



Security Tech Germany

ABUS CMS SOFTWARE – Benutzerhandbuch V1.0

Inhalt

Kapitel 3 Geräteverwaltung	1
3.1 Geräte aktivieren	1
3.2 Gerät hinzufügen	2
3.2.1 Einzelne oder mehrere Online-Geräte hinzufügen	3
3.2.2 Gerät nach IP-Adresse oder Domänenname hinzufügen	6
3.2.3 Geräte nach IP-Segment hinzufügen	9
3.2.4 Geräte in einem Stapel importieren	12
3.3 Gerätepasswort wiederherstellen/zurücksetzen	15
3.3.1 Gerätepasswort zurücksetzen	15
3.3.2 Das Standardpasswort des Geräts wiederherstellen	16
3.4 Upgrade der Geräte-Firmware-Version	17
3.5 Hinzugefügte Geräte verwalten	19
3.6 Verwaltung der Gruppe	20
3.6.1 Ressourcen der Gruppe	20
3.6.2 Ressourcenparameter bearbeiten	22
Kapitel 4 ABUS Link Station	24
4.1 Registrierung eines ABUS Link Stationskontos	24
4.2 Anmeldung bei ABUS Link Station Konto	25
Kapitel 5 Live-Ansicht	27
5.1 Symbolleiste der Live-Ansicht	27
5.2 Benutzerdefinierte Ansicht hinzufügen	28
5.3 Live-Ansicht starten	29
5.4 Automatisches Umschalten in der Live-Ansicht	31
5.4.1 Automatisches Umschalten von Kameras in einer Gruppe	31
5.4.2 Automatisches Umschalten aller Kameras	33
5.4.3 Benutzerdefinierte Ansichten automatisch umschalten	35
5.5 PTZ-Steuerung	37
5.5.1 PTZ-Bedienfeld	37
5.5.2 Voreinstellung, Patrouille und Muster einstellen	40

5.6 Anpassen der Fensteraufteilung.....	42
5.7 Manuelles Aufzeichnen und Erfassen.....	45
5.7.1 Manuelles Aufzeichnen von Videos	45
5.7.2 Lokale Videos anzeigen	45
5.7.3 Bilder Snapshot	46
5.7.4 Aufgenommene Bilder ansehen	47
5.8 Sofortige Wiedergabe	48
5.9 Live-Ansicht für Fisheye-Kamera	49
5.9.1 Live-Ansicht im Fischaugenmodus durchführen	49
5.9.2 PTZ-Steuerung im Fisheye-Modus.....	51
5.9.3 Eine Voreinstellung und eine Patrouille festlegen.....	51
5.11 Live-Ansicht für Wärmebildkamera.....	52
5.11.1 Anzeigen von Brandherdinformationen während der Live-Ansicht	52
5.11.2 Temperaturinformationen in der Live-Ansicht anzeigen	54
5.11.3 Manuelles Messen der Temperatur	55
5.11.4 Anzeige des Brandherd-Erkennungsschildes	56
5.13 Weitere Funktionen	57
Kapitel 6 Fernwiedergabe.....	60
6.2 Konfiguration des Speichers	60
6.2.1 Bild und Video auf DVR, NVR oder Netzwerkkamera speichern.....	60
6.2.3 Bild und zusätzliche Informationen auf dem lokalen PC speichern	62
6.2.4 Aufzeichnungszeitplanvorlage konfigurieren	63
6.2.5 Erfassungszeitplanvorlage konfigurieren	64
6.3 Symbolleiste für die Wiedergabe	65
6.4 Normale Wiedergabe	67
6.4.1 Videomaterial suchen	68
6.4.2 Videomaterial abspielen	70
6.5 Wiedergabe von Alarmeingängen	72
6.5.1 Videomaterial suchen	72
6.5.2 Videomaterial abspielen	74
6.6 Wiedergabe von Ereignissen.....	75

6.6.1 Suche nach Videomaterial/Bildern.....	75
6.6.2 Videomaterial/Bild anzeigen	76
6.9 VCA-Wiedergabe	77
6.10 Synchrone Wiedergabe	79
6.11 Videowiedergabe der Fisheye-Kamera	80
6.13 Videomaterial herunterladen	82
6.13.1 Videomaterial nach Datum herunterladen	82
6.13.2 Download für mehrere Kameras	83
Kapitel 7 Ereigniskonfiguration.....	85
7.1 Ereignis für Kamera konfigurieren.....	85
7.2 Ereignis für Alarমেingang konfigurieren	87
7.3 Ereignis für Kodiergerät konfigurieren	89
Kapitel 8 Veranstaltungszentrum.....	91
8.1 Aktivieren des Empfangs von Ereignissen von Geräten	91
8.2 Echtzeit-Ereignisse anzeigen	92
8.3 Suche nach historischen Ereignissen	94
8.4 Ereignisse vom Gerät abrufen.....	98
8.5 Pop-up-Ereignisinformationen anzeigen.....	99
Kapitel 9 Kartenverwaltung	100
9.1 Karte hinzufügen	100
9.2 Kartenmaßstab bearbeiten	101
9.3 Kalibrierung von Längen- und Breitengraden	102
9.4 Hot Spot verwalten	103
9.4.1 Kamera als Hot Spot hinzufügen	103
9.4.2 Alarমেingang als Hot Spot hinzufügen	105
9.4.3 Alarmausgang als Hot Spot hinzufügen.....	106
9.4.4 Zone als Hot Spot hinzufügen	108
9.4.5 Zugangspunkt als Hot Spot hinzufügen	110
Kapitel 10 Statistik	111
10.1.1 Personenzählungsbericht nach Kodiergerät	111
10.2 Bericht zur Personenzählung an Kreuzungen anzeigen	115

10.4 Wärmekartenbericht.....	116
10.7 Temperaturkarte	118
Kapitel 11 Datenabruf	121
11.1 Fahrzeug-Abruf.....	121
Kapitel 14 Personenverwaltung.....	122
14.1 Organisation hinzufügen	123
14.2 Einzelperson hinzufügen	123
14.2.1 Grundlegende Informationen konfigurieren	124
14.2.2 Ausstellung einer Karte für eine Person.....	126
14.2.3 Hochladen eines Gesichtsfotos vom lokalen PC	128
14.2.4 Ein Foto über den Client aufnehmen.....	129
14.2.5 Gesicht über Zutrittskontrollgerät erfassen.....	130
14.2.10 Konfigurieren der Zugriffskontrollinformationen.....	131
14.2.11 Anpassen von Personeninformationen.....	133
14.2.12 Anwohnerinformationen konfigurieren.....	134
14.2.13 Zusätzliche Informationen konfigurieren.....	135
14.3 Import und Export von personenidentifizierenden Informationen	135
14.3.1 Personendaten importieren	135
14.3.2 Personenbilder importieren	136
14.3.3 Informationen zur Person exportieren.....	137
14.3.4 Personenbilder exportieren.....	137
14.4 Abrufen von Personeninformationen vom Zutrittskontrollgerät	138
14.5 Personen zu einer anderen Organisation versetzen.....	139
14.6 Ausgabe von Karten an Personen im Stapel	139
14.7 Berichtskarte Verlust.....	140
14.8 Ressourcenstatistiken anzeigen.....	141
Kapitel 15 Zugangskontrolle	142
15.2 Zeitplan und Vorlage konfigurieren.....	142
15.2.1 Urlaub hinzufügen	142
15.2.2 Vorlage hinzufügen	143
15.3 Zugriffsgruppe festlegen, um Personen eine Zugriffsberechtigung zuzuweisen	145

15.4 Zugriffsgruppe suchen.....	147
15.5 Erweiterte Funktionen konfigurieren.....	148
15.5.1 Geräteparameter konfigurieren.....	148
15.5.2 Verbleibende Entsperrung/Sperrung konfigurieren.....	157
15.5.3 Konfigurieren der Multi-Faktor-Authentifizierung.....	159
15.5.4 Benutzerdefinierte Wiegand-Regel konfigurieren.....	161
15.5.5 Konfigurieren von Kartenleser-Authentifizierungsmodus und Zeitplan.....	162
15.5.6 Personenauthentifizierungsmodus konfigurieren.....	166
15.5.8 Konfigurieren der ersten Person in.....	166
15.5.9 Anti-Passback konfigurieren.....	168
15.5.10 Konfigurieren der Mehrtürverriegelung.....	169
15.5.11 Authentifizierungscode konfigurieren.....	170
15.6.3 Geräteerfassungsparameter einstellen.....	170
15.6.4 Parameter für Gesichtserkennungsterminal einstellen.....	172
15.6.5 Aktivieren der M1-Kartenverschlüsselung.....	173
15.6.6 RS-485-Parameter einstellen.....	173
15.6.7 Wiegand-Parameter einstellen.....	174
15.7 Konfigurieren von Verknüpfungsaktionen für die Zugriffskontrolle.....	175
15.7.1 Client-Aktionen für Zugriffseignis konfigurieren.....	175
15.7.2 Geräteaktionen für Zugriffseignis konfigurieren.....	176
15.7.3 Geräteaktionen für das Durchziehen von Karten konfigurieren.....	178
15.7.4 Geräte-Aktionen für Personen-ID konfigurieren.....	179
15.8.1 Status der Kontrolltür.....	181
15.8.3 Echtzeit-Zugangsdaten prüfen.....	182
Kapitel 19 Logsuche.....	184
Kapitel 20 Benutzerverwaltung.....	185
20.1 Benutzer hinzufügen.....	185
20.2 Passwort des Benutzers ändern.....	186
Kapitel 21 Systemkonfiguration.....	188
21.1 Allgemeine Parameter einstellen.....	188
21.2 Live-Ansicht und Wiedergabeparameter einstellen.....	189

21.3 Bildparameter einstellen	191
21.4 Bildspeicherung einstellen	192
21.5 Alarmton einstellen	192
21.6 Einstellen der Parameter für die Zugangskontrolle und die Videosprechanlage	193
21.7 Dateispeicherpfad festlegen	194
21.8 In der Symbolleiste angezeigte Symbole einstellen	194
21.9 Tastatur- und Joystick-Verknüpfungen festlegen	196
21.10 E-Mail-Parameter festlegen	196
21.11 Verwalten der Sicherheitsauthentifizierung	197
21.11.1 Zertifikat aus dem Service Management exportieren	198
21.11.2 Zertifikat in den Client importieren	198
21.11.3 Zertifikatsüberprüfung bei Übertragungsverschlüsselung	199
Kapitel 22 Betrieb und Wartung	200
A. Benutzerdefinierte Wiegand-Regelbeschreibungen	202
D. Fehlercode	204

Kapitel 3 Geräteverwaltung

3.1 Geräte aktivieren

Für die inaktiven Geräte müssen Sie ein Kennwort erstellen, um sie zu aktivieren, bevor sie der Software hinzugefügt werden und ordnungsgemäß funktionieren können.

Bevor Sie beginnen

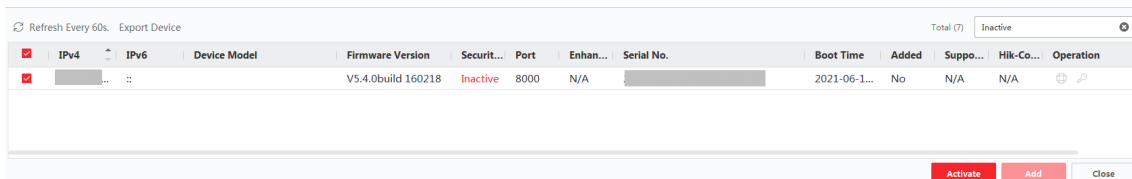
Vergewissern Sie sich, dass das zu aktivierende Gerät mit dem Netzwerk verbunden ist und sich im selben Subnetz befindet wie der PC, auf dem der Client läuft.

Schritte

Hinweis

Diese Funktion sollte von dem Gerät unterstützt werden.

1. Rufen Sie die Seite Geräteverwaltung auf.
2. Klicken Sie oben im rechten Fenster auf **Gerät**.
3. Klicken Sie auf **Online-Gerät**, um die Liste der Online-Geräte unten auf der Seite anzuzeigen.
Die gesuchten Online-Geräte werden in der Liste angezeigt.
4. Überprüfen Sie den Gerätestatus (angezeigt in der Spalte **Sicherheitsstufe**) und wählen Sie ein inaktives Gerät aus.





IPV4	IPV6	Device Model	Firmware Version	Securit...	Port	Enhan...	Serial No.	Boot Time	Added	Suppo...	Hik-Co...	Operation
...	::		V5.4.0build 160218	Inactive	8000	N/A		2021-06-1...	No	N/A	N/A	 

Abbildung 3-1 Online inaktive Geräte

5. Klicken Sie auf **Aktivieren**, um den Aktivierungsdialog zu öffnen.
6. Erstellen Sie ein Passwort im Passwortfeld und bestätigen Sie das Passwort.

Vorsicht

Die Passwortstärke des Geräts kann automatisch überprüft werden. Wir empfehlen Ihnen dringend, das Passwort Ihrer Wahl zu ändern (mit mindestens 8 Zeichen, darunter mindestens drei Arten der folgenden Kategorien: Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen), um die Sicherheit Ihres Produkts zu erhöhen. Und wir empfehlen Ihnen, Ihr Passwort regelmäßig zu ändern, vor allem im Hochsicherheitssystem kann eine monatliche oder wöchentliche Änderung des Passworts Ihr Produkt besser schützen.

Die ordnungsgemäße Konfiguration aller Kennwörter und anderer Sicherheitseinstellungen liegt in der Verantwortung des Installateurs und/oder des Endbenutzers.


Hinweis

Für das NVR-Gerät müssen Sie ein Kennwort im Feld **Standardkennwort für Netzwerkkameras** erstellen und das Kennwort bestätigen, um die an den NVR angeschlossene(n) Netzwerkkamera(s) zu aktivieren.

7. Optional: Aktivieren Sie den Dienst ABUS Link Station bei der Aktivierung des Geräts, wenn das Gerät dies unterstützt.
 - 1) Markieren Sie **Cloud P2P aktivieren**, um den Notizendialog zu öffnen.
 - 2) Erstellen Sie einen Verifizierungscode und bestätigen Sie den Verifizierungscode.
 - 3) Klicken Sie auf **Nutzungsbedingungen** und **Datenschutzrichtlinien**, um die Anforderungen zu lesen.
 - 4) Klicken Sie auf **OK**, um den Dienst ABUS Link Station zu aktivieren.
 8. Klicken Sie auf **OK**, um das Gerät zu aktivieren.
-

Hinweis

Wenn das Gerät das Zurücksetzen des Passworts über die reservierte E-Mail, die Sicherheitsfrage oder die GUID unterstützt, können Sie diese nach der Aktivierung des Geräts konfigurieren.

9. Optional: Klicken Sie auf  in der Spalte Betrieb, um die Netzwerkinformationen (einschließlich IP-Adresse, Portnummer, Gateway usw.) für das Online-Gerät zu bearbeiten.

3.2 Gerät hinzufügen

Der Client bietet verschiedene Modi zum Hinzufügen von Geräten, einschließlich IP/Domäne, IP-Segment und ABUS Link Station. Der Client unterstützt auch das Importieren mehrerer Geräte in

einem Stapel, wenn eine große Anzahl von Geräten hinzugefügt werden soll.

3.2.1 Einzelne oder mehrere Online-Geräte hinzufügen

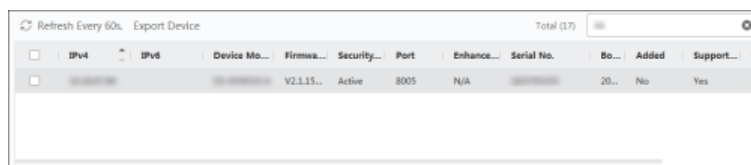
Der Client kann Online-Geräte erkennen, die sich im selben Netzwerk befinden wie der PC, auf dem der Client läuft. Sie können ein erkanntes Online-Gerät auswählen, das in der Liste der Online-Geräte angezeigt wird, und es zum Client hinzufügen. Bei erkannten Online-Geräten, die denselben Benutzernamen und dasselbe Passwort haben, können Sie diese in einem Stapel zum Client hinzufügen.

Bevor Sie beginnen

- Das/die hinzuzufügende(n) Gerät(e) befinden sich im selben Netzwerk wie der PC, auf dem der Client läuft.
- Das/die hinzuzufügende(n) Gerät(e) wurde(n) aktiviert.

Schritte

1. Klicken Sie auf **Geräteverwaltung** → **Gerät** → **Gerät**.
2. Klicken Sie auf **Online-Gerät**, um den Online-Gerätebereich anzuzeigen.
Die gesuchten Online-Geräte werden in der Liste angezeigt.



<input type="checkbox"/>	IPV4	IPV6	Device Mo...	Firmwa...	Security...	Port	Enhance...	Serial No.	Bo...	Added	Support...
<input type="checkbox"/>			V2.1.15...	Active		8005	N/A		20...	No	Yes

Abbildung 3-2 Online Gerät

3. Markieren Sie im Bereich **Online-Gerät** ein oder mehrere Online-Geräte, und klicken Sie auf **Hinzufügen**, um das Fenster zum Hinzufügen von Geräten zu öffnen.

Add [X]

Name

IP Address

Transmission Encryptio...

Port

User Name

Password

Synchronize Time

Import to Group

i Set the device name as the group name and add all the channels connected to the device to the group.

Add **Cancel**

Abbildung 3-3 Einzelne Online-Geräte hinzufügen

Add [X]

User Name

Password

Synchronize Time

Import to Group

i Set the device name as the group name and add all the channels connected to the device to the group.

Add **Cancel**

Abbildung 3-4 Mehrere Online-Geräte hinzufügen

4. Geben Sie die erforderlichen Informationen ein.

Name

Geben Sie einen beschreibenden Namen für das Gerät ein.

IP-Adresse

Geben Sie die IP-Adresse des Geräts ein. Die IP-Adresse des Geräts wird in diesem Hinzufügemodus automatisch ermittelt.

Hafen

Sie können die Anschlussnummer anpassen. Die Portnummer des Geräts wird in diesem Hinzufügungsmodus automatisch ermittelt.

Hinweis

Bei einigen Gerätetypen können Sie als Anschlussnummer **80** eingeben. Diese Funktion sollte von dem Gerät unterstützt werden.

Name des Benutzers

Standardmäßig lautet der Benutzername **admin** für TVVR/HDCC/NVR und **installer** für IPCs

Passwort

Geben Sie das Gerätepasswort ein.

Vorsicht

Die Passwortstärke des Geräts kann automatisch überprüft werden. Wir empfehlen Ihnen dringend, das Passwort Ihrer Wahl zu ändern (mit mindestens 8 Zeichen, darunter mindestens drei Arten der folgenden Kategorien: Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen), um die Sicherheit Ihres Produkts zu erhöhen. Und wir empfehlen Ihnen, Ihr Passwort regelmäßig zu ändern, vor allem im Hochsicherheitssystem kann eine monatliche oder wöchentliche Änderung des Passworts Ihr Produkt besser schützen. Die ordnungsgemäße Konfiguration aller Kennwörter und anderer Sicherheitseinstellungen liegt in der Verantwortung des Installateurs und/oder des Endbenutzers.

5. Optional: Aktivieren Sie die Option **Übertragungsverschlüsselung (TLS)**, um die Übertragungsverschlüsselung mit dem TLS-Protokoll (Transport Layer Security) zu Sicherheitszwecken zu aktivieren.
-

Hinweis

- Diese Funktion sollte von dem Gerät unterstützt werden.
 - Wenn Sie die Zertifikatsüberprüfung aktiviert haben, sollten Sie auf **Zertifikatsverzeichnis öffnen** klicken, um den Standardordner zu öffnen, und die vom Gerät exportierte Zertifikatsdatei in dieses Standardverzeichnis kopieren, um die Sicherheit zu erhöhen. Weitere Informationen zur Aktivierung der Zertifikatsüberprüfung finden Sie unter **Zertifikatsüberprüfung für Übertragungsverschlüsselung**.
 - Sie können sich bei dem Gerät anmelden, um die Zertifikatsdatei über den Webbrowser abzurufen.
-

6. Aktivieren Sie **Zeit synchronisieren**, um die Gerätezeit mit dem PC zu synchronisieren, auf dem der Client läuft, nachdem das Gerät zum Client hinzugefügt wurde.
-

7. Optional: Markieren Sie **In Gruppe importieren**, um eine Gruppe mit dem Gerätenamen zu erstellen und alle Kanäle des Geräts in diese Gruppe zu importieren.

Beispiel

Bei Codiergeräten werden die Codierkanäle und Alarmeingänge/-ausgänge in diese Gruppe importiert.

Für ein Zutrittskontrollgerät werden dessen Zutrittspunkte, Alarmeingänge/-ausgänge und Codierkanäle (falls vorhanden) in diese Gruppe importiert.

8. Klicken Sie auf **Hinzufügen**.
9. Optional: Klicken Sie auf **Gerät exportieren**, wählen Sie den Speicherpfad und den Gerätetyp aus, und klicken Sie auf **OK**, um die Geräteinformationen auf Ihren PC zu exportieren.



Hinweis

Derzeit unterstützt die Plattform nur den Export der Informationen von Video-Sprechanlagen, einschließlich Türstationen, Innenstationen und Hauptstationen.

3.2.2 Gerät nach IP-Adresse oder Domänenname hinzufügen

Wenn Sie die IP-Adresse oder den Domännennamen des hinzuzufügenden Geräts kennen, können Sie dem Client Geräte hinzufügen, indem Sie die IP-Adresse (oder den Domännennamen), den Benutzernamen, das Passwort usw. angeben.

Schritte

1. Rufen Sie das Modul Geräteverwaltung auf.
2. Klicken Sie oben im rechten Fenster auf die Registerkarte **Gerät**.
Die hinzugefügten Geräte werden auf der rechten Seite angezeigt.

Abbildung 3-5 Gerät nach IP-Adresse oder Domänenname hinzufügen

3. Klicken Sie auf **Hinzufügen**, um das Fenster Hinzufügen zu öffnen, und wählen Sie dann **IP/Domäne** als Hinzufügungsmodus.
4. Geben Sie die erforderlichen Informationen ein.

Name

Erstellen Sie einen beschreibenden Namen für das Gerät. Sie können zum Beispiel einen Spitznamen verwenden, der den Standort oder die Funktion des Geräts angibt.

Adresse

Die IP-Adresse oder der Domänenname des Geräts.

Hafen

Die hinzuzufügenden Geräte haben die gleiche Anschlussnummer. Der Standardwert ist **8000**.

Hinweis

Bei einigen Gerätetypen können Sie als Anschlussnummer **80** eingeben. Diese Funktion sollte von dem Gerät unterstützt werden.

Name des Benutzers

Geben Sie den Benutzernamen des Geräts ein. Der Standardbenutzername ist **admin**.

Passwort

Geben Sie das Gerätepasswort ein.

Vorsicht

Die Passwortstärke des Geräts kann automatisch überprüft werden. Wir empfehlen Ihnen dringend, das Passwort Ihrer Wahl zu ändern (mit mindestens 8 Zeichen, darunter mindestens drei Arten der folgenden Kategorien: Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen), um die Sicherheit Ihres Produkts zu erhöhen. Und wir empfehlen Ihnen, Ihr Passwort regelmäßig zu ändern, vor allem im Hochsicherheitssystem kann eine monatliche oder wöchentliche Änderung des Passworts Ihr Produkt besser schützen. Die ordnungsgemäße Konfiguration aller Kennwörter und anderer Sicherheitseinstellungen liegt in der Verantwortung des Installateurs und/oder des Endbenutzers.

5. Optional: Fügen Sie die Offline-Geräte hinzu.

- 1) Markieren Sie **Offline-Gerät hinzufügen**.
 - 2) Geben Sie die erforderlichen Informationen ein, darunter die Kanalnummer des Geräts und die Nummer des Alarmeingangs.
-

Hinweis

Nach dem Hinzufügen des Offline-Geräts zum Client wird der Netzwerkstatus des Geräts als "Offline" angezeigt. Sobald das Gerät online ist, wechselt der Netzwerkstatus des Geräts zu "Online", und der Client stellt automatisch eine Verbindung her.

6. Optional: Aktivieren Sie die Option **Übertragungsverschlüsselung (TLS)**, um die Übertragungsverschlüsselung mit dem TLS-Protokoll (Transport Layer Security) zu Sicherheitszwecken zu aktivieren.

Hinweis

- Diese Funktion sollte von dem Gerät unterstützt werden.
 - Wenn Sie die Zertifikatsüberprüfung aktiviert haben, sollten Sie auf **Zertifikatsverzeichnis öffnen** klicken, um den Standardordner zu öffnen, und die vom Gerät exportierte Zertifikatsdatei in dieses Standardverzeichnis kopieren, um die Sicherheit zu erhöhen. Weitere Informationen zur Aktivierung der Zertifikatsüberprüfung finden Sie unter **Zertifikatsüberprüfung für Übertragungsverschlüsselung**.
 - Sie können sich bei dem Gerät anmelden, um die Zertifikatsdatei über den Webbrowser abzurufen.
-



7. Aktivieren Sie **Zeit synchronisieren**, um die Gerätezeit mit dem PC zu synchronisieren, auf dem der Client läuft, nachdem das Gerät zum Client hinzugefügt wurde.
8. Optional: Markieren Sie **In Gruppe importieren**, um eine Gruppe nach dem Gerätenamen zu erstellen und alle Kanäle des Geräts in diese Gruppe zu importieren.


Beispiel


Bei Codiergeräten werden die Codierkanäle und Alarmeingänge/-ausgänge in diese Gruppe importiert.


Für ein Zutrittskontrollgerät werden dessen Zutrittspunkte, Alarmeingänge/-ausgänge und Codierkanäle (falls vorhanden) in diese Gruppe importiert.

9. Beenden Sie das Hinzufügen des Geräts.
 - Klicken Sie auf **Hinzufügen**, um das Gerät hinzuzufügen und zur Seite mit der Geräteliste zurückzukehren.
 - Klicken Sie auf **Hinzufügen und Neu**, um die Einstellungen zu speichern und mit dem Hinzufügen weiterer Geräte fortzufahren.
10. Optional: Führen Sie die folgende(n) Operation(en) durch.

Ferngesteuerte Konfiguration Klicken Sie auf der Seite mit der Geräteliste in der Spalte Vorgang auf , um eine Fernkonfiguration für ein Gerät durchzuführen.  befindet sich in der Spalte ganz rechts auf der Seite "Gerät". Weitere Informationen finden Sie im Benutzerhandbuch des Geräts.

Gerätstatus Klicken Sie auf  in der Spalte "Betrieb", um den Gerätstatus, einschließlich Kameras, Aufzeichnungsstatus, Signalstatus, Hardwarestatus usw. anzuzeigen.

Geräteinformationen bearbeiten Klicken Sie in der Spalte Betrieb auf , um die Geräteinformationen wie IP-Adresse, Benutzername und Passwort zu bearbeiten.

Online Benutzer prüfen Klicken Sie auf  in der Spalte "Betrieb", um die Online-Benutzer zu überprüfen, die auf das Gerät zugreifen, z. B. Benutzername, Benutzertyp, IP-Adresse des Benutzers und Anmeldezeit.

Aktualisieren Klicken Sie in der Spalte Betrieb auf , um die neuesten Geräteinformationen abzurufen.

Gerät löschen Wählen Sie ein oder mehrere Geräte aus und klicken Sie auf **Löschen**, um die ausgewählten Geräte aus dem Client zu löschen.

3.2.3 Geräte nach IP-Segment hinzufügen

Wenn die Geräte dieselbe Portnummer, denselben Benutzernamen und dasselbe Passwort haben und ihre IP-Adressbereiche im selben IP-Segment liegen, können Sie sie zum Client hinzufügen, indem Sie die Start- und End-IP-Adresse, die Portnummer, den Benutzernamen, das Passwort usw.

der Geräte angeben.

Schritte

1. Klicken Sie im Bereich Wartung und Verwaltung auf der rechten Seite des Clients auf **Geräteverwaltung**.
2. Klicken Sie auf die Registerkarte **Gerät** oben im linken Fenster.
Die hinzugefügten Geräte werden auf der rechten Seite angezeigt.
3. Klicken Sie auf **Hinzufügen**, um das Fenster Hinzufügen zu öffnen.

Hinzufügen ✕

Modus hinzufügen IP/Domäne IP-Segment ABUS Link Sta...

Batch-Import

Offline-Gerät hinzufügen

* Start IP:

* End IP:

Übertragungsverschlüs...

* Port

* Benutzername

* Passwort

Zeit synchronisieren

In Gruppe importieren

ⓘ Gruppe mit der Geräte-IP erstellen

Hinzufügen ... **Hinzufügen** **Abbrechen**

Abbildung 3-6 Gerät nach IP-Segment hinzufügen

4. Wählen Sie **IP-Segment** als Hinzufügemodus.
5. Geben Sie die erforderlichen Informationen ein.

Start IP

Geben Sie eine Start-IP-Adresse ein.

Ende IP

Geben Sie eine End-IP-Adresse ein, die sich im gleichen Netzwerksegment wie die Start-IP befindet.

Hafen

Geben Sie die Geräteanschlussnummer ein. Der Standardwert ist **8000**.

Hinweis

Bei einigen Gerätetypen können Sie als Anschlussnummer **80** eingeben. Diese Funktion sollte von dem Gerät unterstützt werden.

Name des Benutzers

Der Standardbenutzername ist **admin**.

Passwort

Geben Sie das Gerätepasswort ein.

Vorsicht

Die Passwortstärke des Geräts kann automatisch überprüft werden. Wir empfehlen Ihnen dringend, das Passwort Ihrer Wahl zu ändern (mit mindestens 8 Zeichen, darunter mindestens drei Arten der folgenden Kategorien: Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen), um die Sicherheit Ihres Produkts zu erhöhen. Und wir empfehlen Ihnen, Ihr Passwort regelmäßig zu ändern, vor allem im Hochsicherheitssystem kann eine monatliche oder wöchentliche Änderung des Passworts Ihr Produkt besser schützen. Die ordnungsgemäße Konfiguration aller Kennwörter und anderer Sicherheitseinstellungen liegt in der Verantwortung des Installateurs und/oder des Endbenutzers.

6. Optional: Fügen Sie die Offline-Geräte hinzu.

- 1) Markieren Sie **Offline-Gerät hinzufügen**.
 - 2) Geben Sie die erforderlichen Informationen ein, darunter die Kanalnummer des Geräts und die Nummer des Alarmeingangs.
-

Hinweis

Nach dem Hinzufügen des Offline-Geräts zum Client wird der Netzwerkstatus des Geräts als "Offline" angezeigt. Sobald das Gerät online ist, wechselt der Netzwerkstatus des Geräts zu "Online", und der Client stellt automatisch eine Verbindung her.

7. Optional: Aktivieren Sie **Übertragungsverschlüsselung (TLS)**, um die Übertragungsverschlüsselung mit dem TLS-Protokoll (Transport Layer Security) zu aktivieren.







Hinweis

- Diese Funktion sollte von dem Gerät unterstützt werden.
 - Wenn Sie die Zertifikatsüberprüfung aktiviert haben, sollten Sie auf **Zertifikatsordner öffnen** klicken, um den Standardordner zu öffnen, und die vom Gerät exportierte Zertifikatsdatei in
-

dieses Standardverzeichnis kopieren, um die Sicherheit zu erhöhen. Weitere Informationen zur Aktivierung der Zertifikatsüberprüfung finden Sie unter **Zertifikatsüberprüfung für Übertragungsverschlüsselung**.

- Sie können sich bei dem Gerät anmelden, um die Zertifikatsdatei über den Webbrowser abzurufen.
-

8. Aktivieren Sie **Zeit synchronisieren**, um die Gerätezeit mit dem PC zu synchronisieren, auf dem der Client läuft, nachdem das Gerät zum Client hinzugefügt wurde.
9. Optional: Markieren Sie **In Gruppe importieren**, um eine Gruppe nach dem Gerätenamen zu erstellen und alle Kanäle des Geräts in die Gruppe zu importieren.
10. Beenden Sie das Hinzufügen des Geräts.
 - Klicken Sie auf **Hinzufügen**, um das Gerät hinzuzufügen und zur Seite mit der Geräteliste zurückzukehren.
 - Klicken Sie auf **Hinzufügen und Neu**, um die Einstellungen zu speichern und mit dem Hinzufügen weiterer Geräte fortzufahren.
11. Optional: Führen Sie die folgende(n) Operation(en) durch.

Ferngesteuerte Konfiguration	Klicken Sie auf der Seite mit der Geräteliste in der Spalte Vorgang auf  , um eine Fernkonfiguration für ein Gerät durchzuführen.  befindet sich in der Spalte ganz rechts auf der Seite "Gerät". Weitere Informationen finden Sie im Benutzerhandbuch des Geräts.
Gerätstatus	Klicken Sie auf  in der Spalte "Betrieb", um den Gerätstatus, einschließlich Kameras, Aufzeichnungsstatus, Signalstatus, Hardwarestatus usw. anzuzeigen.
Geräteinformationen bearbeiten	Klicken Sie in der Spalte Betrieb auf  , um die Geräteinformationen wie IP-Adresse, Benutzername und Passwort zu bearbeiten.
Online Benutzer prüfen	Klicken Sie auf  in der Spalte "Betrieb", um die Online-Benutzer zu überprüfen, die auf das Gerät zugreifen, z. B. Benutzername, Benutzertyp, IP-Adresse des Benutzers und Anmeldezeit.
Aktualisieren	Klicken Sie in der Spalte Betrieb auf  , um die neuesten Geräteinformationen abzurufen.
Gerät löschen	Wählen Sie ein oder mehrere Geräte aus und klicken Sie auf Löschen , um die ausgewählten Geräte aus dem Client zu löschen.

3.2.4 Geräte in einem Stapel importieren

Sie können dem Client mehrere Geräte in einem Stapel hinzufügen, indem Sie die

Geräteparameter in eine vordefinierte CSV-Datei eingeben.

Schritte

1. Rufen Sie das Modul Geräteverwaltung auf.
2. Klicken Sie oben im rechten Fenster auf die Registerkarte **Gerät**.
3. Klicken Sie auf **Hinzufügen**, um das Fenster Hinzufügen zu öffnen, und wählen Sie **Batch-Import** als Hinzufügemodus.

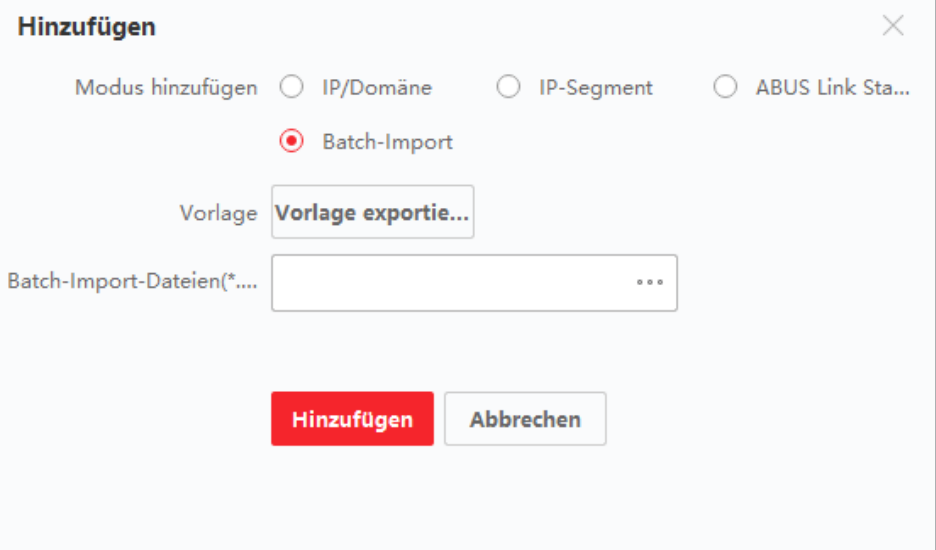


Abbildung 3-7 Geräte in einem Stapel hinzufügen

4. Klicken Sie auf **Vorlage exportieren** und speichern Sie dann die vordefinierte Vorlage (CSV-Datei) auf Ihrem PC.
5. Öffnen Sie die exportierte Vorlagendatei und geben Sie die erforderlichen Informationen zu den hinzuzufügenden Geräten in der entsprechenden Spalte ein.

Hinweis

Eine ausführliche Beschreibung der erforderlichen Felder finden Sie in den Einleitungen der Vorlage.

Hinzufügen von Modus

Geben Sie **0** oder **1** oder **2** ein.

Adresse

Bearbeiten Sie die Adresse des Geräts.

Hafen

Geben Sie die Portnummer des Geräts ein. Die Standard-Portnummer ist **8000**.

Name des Benutzers

Geben Sie den Benutzernamen des Geräts ein. Der Standardbenutzername ist **admin**.

Passwort

Geben Sie das Gerätepasswort ein.

Vorsicht

Die Passwortstärke des Geräts kann automatisch überprüft werden. Wir empfehlen Ihnen dringend, das Passwort Ihrer Wahl zu ändern (mit mindestens 8 Zeichen, darunter mindestens drei Arten der folgenden Kategorien: Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen), um die Sicherheit Ihres Produkts zu erhöhen. Und wir empfehlen Ihnen, Ihr Passwort regelmäßig zu ändern, vor allem im Hochsicherheitssystem kann eine monatliche oder wöchentliche Änderung des Passworts Ihr Produkt besser schützen. Die ordnungsgemäße Konfiguration aller Kennwörter und anderer Sicherheitseinstellungen liegt in der Verantwortung des Installateurs und/oder des Endbenutzers.

Offline-Gerät hinzufügen

Geben Sie **1** ein, um das Hinzufügen eines Offline-Geräts zu aktivieren.

Nach dem Hinzufügen des Offline-Geräts zum Client wird der Netzwerkstatus des Geräts als "Offline" angezeigt. Wenn das Gerät online geht, wechselt der Netzwerkstatus des Geräts zu "Online", und der Client verbindet es automatisch. Geben Sie **0** ein, um das Hinzufügen eines Offline-Geräts zu deaktivieren.

In Gruppe importieren


Geben Sie **1** ein, um eine Gruppe nach dem Gerätenamen zu erstellen. Alle Kanäle des Geräts werden standardmäßig in die entsprechende Gruppe importiert. Geben Sie **0** ein, um diese Funktion zu deaktivieren.

Kanalnummer



Wenn Sie **Offline-Gerät hinzufügen** aktivieren, geben Sie die Kanalnummer des Geräts ein. Wenn Sie **Offline-Gerät hinzufügen** deaktivieren, ist dieses Feld nicht erforderlich.

Alarめingang Nummer


Wenn Sie **Offline-Gerät hinzufügen** aktivieren, geben Sie die Alarめingangnummer des Geräts ein. Wenn Sie **Offline-Gerät hinzufügen** deaktivieren, ist dieses Feld nicht erforderlich.




6. Klicken Sie auf  und wählen Sie die Vorlagendatei aus.
7. Klicken Sie auf **Hinzufügen**, um die Geräte zu importieren.
8. Optional: Führen Sie die folgende(n) Operation(en) durch.

Ferngesteuerte Konfiguration

Klicken Sie auf der Seite mit der Geräteliste in der Spalte Vorgang auf , um eine Fernkonfiguration für ein Gerät durchzuführen.  befindet sich in der Spalte ganz rechts auf der Seite "Gerät". Weitere Informationen finden Sie im Benutzerhandbuch des Geräts.

Gerätstatus

Klicken Sie auf  in der Spalte "Betrieb", um den Gerätstatus, einschließlich Kameras, Aufzeichnungsstatus, Signalstatus, Hardwarestatus usw. anzuzeigen.

Geräteinformationen bearbeiten	Klicken Sie in der Spalte Betrieb auf  , um die Geräteinformationen wie IP-Adresse, Benutzername und Passwort zu bearbeiten.
Online Benutzer prüfen	Klicken Sie auf  in der Spalte "Betrieb", um die Online-Benutzer zu überprüfen, die auf das Gerät zugreifen, z. B. Benutzername, Benutzertyp, IP-Adresse des Benutzers und Anmeldezeit.
Aktualisieren	Klicken Sie in der Spalte Betrieb auf  , um die neuesten Geräteinformationen abzurufen.
Gerät löschen	Wählen Sie ein oder mehrere Geräte aus und klicken Sie auf Löschen , um die ausgewählten Geräte aus dem Client zu löschen.


3.3 Gerätepasswort wiederherstellen/zurücksetzen

Wenn Sie das Kennwort der erkannten Online-Geräte vergessen haben, können Sie das Standardkennwort des Geräts wiederherstellen oder das Kennwort des Geräts über den Client zurücksetzen.

3.3.1 Gerätepasswort zurücksetzen

Wenn Sie das Passwort der erkannten Online-Geräte vergessen haben, können Sie das Gerätepasswort über den Client zurücksetzen.

Schritte

1. Rufen Sie die Seite Geräteverwaltung auf.
2. Klicken Sie oben im rechten Fenster auf die Registerkarte **Gerät**.
3. Klicken Sie auf **Online-Gerät**, um den Online-Gerätebereich anzuzeigen.
Alle Online-Geräte, die dasselbe Subnetz nutzen, werden in der Liste angezeigt.
4. Wählen Sie das Gerät aus der Liste aus und klicken Sie auf  in der Spalte Betrieb.
5. Setzen Sie das Gerätepasswort zurück.
 - **Klicken** Sie auf Exportieren, um die Gerätedatei auf Ihrem PC zu speichern, und senden Sie die Datei dann an unseren technischen Support.

Hinweis

Für die folgenden Vorgänge zum Zurücksetzen des Passworts wenden Sie sich bitte an unseren technischen Support, insofern ihr Gerät keinen Hardware-Reset-Knopf hat.

- Klicken Sie auf **Erzeugen**, um das QR-Code-Fenster zu öffnen, und klicken Sie auf **Herunterladen**, um den QR-Code auf Ihrem PC zu speichern. Sie können auch ein Foto des QR-Codes machen, um ihn auf Ihrem Handy zu speichern. Senden Sie das Bild an unseren technischen Support.

 **Hinweis**

Für die folgenden Vorgänge zum Zurücksetzen des Passworts wenden Sie sich bitte an unseren technischen Support.

- Wählen Sie den abgesicherten Modus je nach Bedarf.
-

 **Hinweis**

Für die folgenden Vorgänge zum Zurücksetzen des Passworts wenden Sie sich bitte an unseren technischen Support.

 **Vorsicht**


Die Passwortstärke des Geräts kann automatisch überprüft werden. Wir empfehlen Ihnen dringend, das Passwort Ihrer Wahl zu ändern (mit mindestens 8 Zeichen, darunter mindestens drei Arten der folgenden Kategorien: Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen), um die Sicherheit Ihres Produkts zu erhöhen. Und wir empfehlen Ihnen, Ihr Passwort regelmäßig zu ändern, vor allem im Hochsicherheitssystem kann eine monatliche oder wöchentliche Änderung des Passworts Ihr Produkt besser schützen.

Die ordnungsgemäße Konfiguration aller Kennwörter und anderer Sicherheitseinstellungen liegt in der Verantwortung des Installateurs und/oder des Endbenutzers.

3.3.2 Das Standardpasswort des Geräts wiederherstellen

Wenn Sie das Passwort der erkannten Online-Geräte vergessen haben, können Sie deren Standardpasswort über den Client wiederherstellen.

Schritte

1. Rufen Sie die Seite Geräteverwaltung auf.
 2. Klicken Sie oben im rechten Fenster auf die Registerkarte **Gerät**.
 3. Klicken Sie auf **Online-Gerät**, um den Online-Gerätebereich unten auf der Seite anzuzeigen. Alle Online-Geräte, die dasselbe Subnetz nutzen, werden in der Liste angezeigt.
 4. Wählen Sie ein Gerät aus und klicken Sie in der Spalte Vorgang auf  , um das Fenster Passwort zurücksetzen zu öffnen.
 5. Stellen Sie das Gerätepasswort wieder her.
 - Geben Sie den Sicherheitscode ein, und stellen Sie das Standardkennwort des ausgewählten Geräts wieder her.
-

 **Hinweis**

Um den Sicherheitscode zu erhalten, wenden Sie sich an unseren technischen Support.

- **Klicken** Sie auf Exportieren, um die Gerätedatei auf Ihrem PC zu speichern und die Datei an unseren technischen Support zu senden.
-

Hinweis

Für die folgenden Vorgänge zum Zurücksetzen des Passworts wenden Sie sich bitte an unseren technischen Support.

Was ist als nächstes zu tun?

Das Standardkennwort (12345) für das Administratorkonto ist nur für die erstmalige Anmeldung vorgesehen. Sie müssen dieses Standardkennwort ändern, um sich besser gegen Sicherheitsrisiken zu schützen, wie z. B. den unbefugten Zugriff anderer auf das Produkt, der die ordnungsgemäße Funktion des Produkts verhindern und/oder zu anderen unerwünschten Folgen führen kann.

Vorsicht

Die Passwortstärke des Geräts kann automatisch überprüft werden. Wir empfehlen Ihnen dringend, das Passwort Ihrer Wahl zu ändern (mit mindestens 8 Zeichen, darunter mindestens drei Arten der folgenden Kategorien: Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen), um die Sicherheit Ihres Produkts zu erhöhen. Und wir empfehlen Ihnen, Ihr Passwort regelmäßig zu ändern, vor allem im Hochsicherheitssystem kann eine monatliche oder wöchentliche Änderung des Passworts Ihr Produkt besser schützen.

Die ordnungsgemäße Konfiguration aller Kennwörter und anderer Sicherheitseinstellungen liegt in der Verantwortung des Installateurs und/oder des Endbenutzers.

3.4 Upgrade der Geräte-Firmware-Version

Wenn eine neue Firmware-Version für das hinzugefügte Gerät verfügbar ist, können Sie dessen Firmware-Version über den Client aktualisieren.

Hinweis

- Das Gerät sollte diese Funktion unterstützen.
 - Sie können den Aktualisierungsmodus in der Systemkonfiguration konfigurieren. Weitere Informationen finden Sie unter **Allgemeine Parameter festlegen**.
-

Rufen Sie das Modul Geräteverwaltung auf, und klicken Sie auf die Registerkarte **Gerät**, um die Geräteliste anzuzeigen.

Führen Sie die folgenden Vorgänge entsprechend den verschiedenen Aktualisierungsmodi durch.

Hinweis

Der Fortschritt der Aktualisierung wird angezeigt. Wenn die Aktualisierung abgeschlossen ist, wechselt der Status in der Spalte "Firmware-Upgrade" des Geräts zu **"Aktualisiert"**.

Bei Download und Upgrade auffordern

Wenn eine neue Firmware-Version verfügbar ist, wird ein Fenster mit einer Aufforderung angezeigt. Klicken Sie auf **Alle aktualisieren**, um das Herunterladen und Aktualisieren zu starten.

Herunterladen und Aufforderung zum Upgrade

Nach dem Herunterladen des Pakets mit der neuen Version wird ein Dialogfeld angezeigt, in dem Sie auswählen können, ob ein Upgrade durchgeführt werden soll. Klicken Sie auf **Alle aktualisieren**, um die Aktualisierung der Gerätefirmware zu starten.

Hinweis

Nachdem Sie auf **Alle aktualisieren** geklickt haben, wird eine Aufforderung zur Anzeige von Details angezeigt. Wenn Sie sich nicht auf der Seite Geräteverwaltung befinden, klicken Sie auf **Details anzeigen**, um zur Seite Geräteverwaltung zu wechseln; wenn Sie sich auf der Seite Geräteverwaltung befinden, schließen Sie die Aufforderung.

Upgrade-Status

Auf der Geräteverwaltungsseite wird der folgende Aktualisierungsstatus in der Spalte Firmware-Upgrade angezeigt.

Keine verfügbare Version

Keine neue Firmware-Version verfügbar.

Warten

Das Gerät wartet auf ein Upgrade.

Aktualisieren von

Die Aktualisierung der Geräte-Firmware ist im Gange.

Verbessert

Bewegen Sie den Mauszeiger auf "**Aktualisiert**", um die Version nach der Aktualisierung anzuzeigen.









Upgrading fehlgeschlagen

Wenn das Upgrade fehlschlägt, wird eine Aufforderung zur Anzeige von Details angezeigt. Wenn Sie sich nicht auf der Seite Geräteverwaltung befinden, klicken Sie auf **Details anzeigen**, um zur Seite Geräteverwaltung zu wechseln; wenn Sie sich auf der Seite Geräteverwaltung befinden, schließen Sie die Aufforderung. Bewegen Sie den Mauszeiger auf **Upgrade fehlgeschlagen**, um die Fehlerdetails anzuzeigen, und klicken Sie auf **Upgrade erneut**, um es erneut zu versuchen.

3.5 Hinzugefügte Geräte verwalten

Nachdem Sie Geräte zur Geräteliste hinzugefügt haben, können Sie die hinzugefügten Geräte verwalten, einschließlich der Bearbeitung von Geräteparametern, der Fernkonfiguration, der Anzeige des Gerätestatus usw.

Tabelle 3-1 Verwalten hinzugefügter Geräte

Gerät bearbeiten	Klicken Sie auf  , um Geräteinformationen wie Gerätename, Adresse, Benutzername, Passwort usw. zu bearbeiten.
Gerät löschen	Markieren Sie ein oder mehrere Geräte, und klicken Sie auf Löschen , um die ausgewählten Geräte zu löschen.
Ferngesteuerte Konfiguration	Klicken Sie auf der Seite mit der Geräteliste in der Spalte Vorgang auf  , um eine Fernkonfiguration für ein Gerät durchzuführen.  befindet sich in der Spalte ganz rechts auf der Seite "Gerät". Weitere Informationen finden Sie im Benutzerhandbuch des Geräts.
Gerätestatus anzeigen	<p>Klicken Sie auf  , um den Gerätestatus anzuzeigen, einschließlich Kameras, Aufzeichnungsstatus, Signalstatus, Hardwarestatus usw.</p> <hr/> <p> Hinweis</p> <p>Für verschiedene Geräte werden unterschiedliche Informationen zum Gerätestatus angezeigt.</p> <hr/>
Online-Ansicht Benutzer	Klicken Sie auf  , um die Details der Online-Benutzer anzuzeigen, die auf das Gerät zugreifen, einschließlich Benutzername, Benutzertyp, IP-Adresse und Anmeldezeit.
Geräteinformationen aktualisieren	Klicken Sie auf  , um die neuesten Geräteinformationen zu erhalten.
QR-Code generieren	<p>Markieren Sie ein oder mehrere Geräte, und klicken Sie auf QR-Code, um einen QR-Code für das/die hinzugefügte(n) Gerät(e) zu generieren. Sie können Geräte zum Mobile Client hinzufügen, indem Sie den QR-Code scannen.</p> <hr/> <p> Hinweis</p> <p>Geräte, die durch ISUP oder ABUS Link Station hinzugefügt werden, können keinen QR-Code erzeugen.</p> <hr/>
Upgrade-Gerät	Zeigen Sie den Gerätestatus in der Spalte Firmware-Upgrade an, markieren Sie ein oder mehrere aktualisierbare Geräte und klicken Sie

	auf Gerätefirmware aktualisieren , um die ausgewählten Geräte zu aktualisieren. Weitere Informationen finden Sie unter <u>Gerätefirmware-Version aktualisieren</u> .
Ereignisse vom Gerät abrufen	Markieren Sie ein Gerät, und klicken Sie auf Ereignisse vom Gerät abrufen , um Ereignisse zu synchronisieren. Einzelheiten finden Sie unter <u>Ereignisse vom Gerät abrufen</u> .

3.6 Verwaltung der Gruppe

Der Client bietet Gruppen zur Verwaltung der hinzugefügten Ressourcen in verschiedenen Gruppen. Sie können die Ressourcen je nach Standort der Ressourcen in verschiedene Gruppen einteilen.

Beispiel

In der 1. Etage sind beispielsweise 64 Kameras, 16 Türen, 64 Alarmeingänge und 16 Alarmausgänge installiert. Sie können diese Ressourcen zur bequemen Verwaltung in einer Gruppe (mit dem Namen 1st Floor) organisieren. Sie können die Live-Ansicht aufrufen, die Videodateien wiedergeben, den Türstatus kontrollieren und einige andere Vorgänge der Geräte durchführen, nachdem Sie die Ressourcen nach Gruppen verwaltet haben.

3.6.1 Ressourcen der Gruppe

Der Client bietet zwei Methoden zum Hinzufügen einer Gruppe: Anpassen einer Gruppe oder Erstellen einer Gruppe nach Gerätenamen. Nachdem Sie eine Gruppe angepasst haben, müssen Sie die Ressourcen manuell in diese Gruppe importieren. Nachdem Sie eine Gruppe nach dem Gerätenamen erstellt haben, werden die Ressourcen des Geräts automatisch in die Gruppe importiert. Sie können eine der beiden Methoden wählen, um Ihre Ressourcen nach den tatsächlichen Bedürfnissen zu gruppieren.

Schritte

1. Klicken Sie im Bereich Wartung und Verwaltung auf **Geräteverwaltung** → **Gruppe**, um die Seite zur Gruppenverwaltung aufzurufen.
2. Fügen Sie eine Gruppe hinzu.
 - **Passen Sie eine Gruppe an:** Klicken Sie auf **Gruppe hinzufügen** und vergeben Sie einen Namen für die neue Gruppe.
 - **Eine Gruppe nach Gerätenamen erstellen:** Klicken Sie auf **Gruppe nach Gerätenamen erstellen** und wählen Sie ein hinzugefügtes Gerät aus, um eine neue Gruppe nach dem Namen des ausgewählten Geräts zu erstellen. Nach dem Erstellen einer Gruppe nach dem Gerätenamen werden die Ressourcen (z. B. Codierkanäle, Alarmeingänge, Alarmausgänge und Zugangspunkte) des Geräts automatisch in die Gruppe importiert.

Hinweis

- Es können bis zu 256 Gruppen hinzugefügt werden.
 - Sie können mehrere Gruppen auswählen, indem Sie die Umschalt- oder Strg-Taste auf der Tastatur gedrückt halten.
-


3. Nachdem Sie eine Gruppe hinzugefügt haben, müssen Sie Ressourcen in die Gruppe importieren.
-

Hinweis


Eine Ressource kann zu verschiedenen Gruppen hinzugefügt werden.

- 1) Wählen Sie die Art der zu importierenden Ressourcen und klicken Sie auf **Importieren**.
 - 2) Wählen Sie die zu importierenden Ressourcen aus, und klicken Sie auf **Importieren**, um alle ausgewählten Ressourcen in diese Gruppe zu importieren.
4. Optional: Führen Sie nach dem Hinzufügen einer Gruppe bei Bedarf einen der folgenden Vorgänge aus.

Ressourcenliste erweitern oder falten

Klicken Sie auf  , um die Ressourcenliste in der Gruppe zu erweitern oder zu reduzieren.

Ressource suchen

Geben Sie den Suchbegriff ein und klicken Sie auf  , um nach Zielressourcen zu suchen.

Ressource aus der Gruppe entfernen

Wählen Sie die Ressource(n) aus und klicken Sie auf **Löschen**, um die ausgewählte(n) Ressource(n) aus der Gruppe zu entfernen.

Ressourcenname aktualisieren

Sie können alle Ressourcenamen in einer Gruppe oder in einem Kanal aktualisieren.

- Wählen Sie eine Gruppe aus, und klicken Sie auf **Ressourcenname aktualisieren**, um alle Ressourcenamen in der ausgewählten Gruppe zu aktualisieren.
 - Wählen Sie einen Kanal in einer Gruppe aus, und aktualisieren Sie alle Ressourcenamen in diesem Kanal. Klicken Sie zum Beispiel auf **Codierungskanäle** → **Kameranamen aktualisieren**, um alle Kameranamen in Codierungskanälen zu aktualisieren.
-

Hinweis

Diese Funktion sollte von dem Gerät unterstützt werden.


3.6.2 Ressourcenparameter bearbeiten

Nachdem Sie die Ressourcen in die Gruppe importiert haben, können Sie die Ressourcenparameter bearbeiten. Für den Verschlüsselungskanal können Sie den Kanalnamen, den Stream Typ, den Protokolltyp usw. bearbeiten. Für den Zugangspunkt können Sie den Namen des Zugangspunkts bearbeiten. Für den Alarmeingang können Sie den Namen des Alarmeingangs bearbeiten. Nehmen wir den Verschlüsselungskanal als Beispiel.

Bevor Sie beginnen

Importieren Sie die Ressourcen in die Gruppe.

Schritte

1. Rufen Sie das Modul Geräteverwaltung auf.
2. Klicken Sie auf **Geräteverwaltung** → **Gruppe**, um die Gruppenverwaltungsseite aufzurufen. Alle hinzugefügten Gruppen werden auf der linken Seite angezeigt.
3. Wählen Sie eine Gruppe in der Gruppenliste aus und klicken Sie auf **Codierkanal**. Die in die Gruppe importierten Codierungskanäle werden angezeigt.
4. Klicken Sie auf  in der Spalte Vorgang, um das Fenster Ressource bearbeiten zu öffnen.
5. Bearbeiten Sie die Kamerainformationen, einschließlich des Kameranamens, des Streamtyps usw.

Video-Stream

Wählen Sie den gewünschten Stream Typ für die Live-Ansicht der Kamera.

Hinweis

Sie sollten die Live-Ansicht erneut starten, damit sie wirksam wird.

Wiedergabestromtyp

Wählen Sie den Stream Typ für die Wiedergabe der Kamera wie gewünscht aus.

Hinweis

- Dieses Feld wird angezeigt, wenn das Gerät Dual-Stream unterstützt.
 - Sie sollten die Live-Ansicht erneut starten, damit sie wirksam wird.
-

Drehung Typ

Wählen Sie die Art der Drehung für die Live-Ansicht oder die Wiedergabe der Kamera aus.

Protokoll-Typ

Wählen Sie das Übertragungsprotokoll für die Kamera.

Hinweis

Sie sollten die Live-Ansicht erneut starten, damit sie wirksam wird.

Streaming-Protokoll

Wählen Sie das Protokoll als RTSP oder privat, um den Stream bei der Live-Ansicht abzurufen.

Hinweis

Sie sollten die Live-Ansicht erneut starten, damit sie wirksam wird.

Kopieren nach...

Kopieren Sie die konfigurierten Parameter auf andere Kameras.

Aktualisieren

Holen Sie sich ein neu aufgenommenes Bild für die Live-Ansicht der Kamera.

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

Kapitel 4 ABUS Link Station

Die Client-Software unterstützt auch die Registrierung eines ABUS Link Station-Kontos, die Anmeldung bei Ihrem ABUS Link Station-Konto und die Verwaltung der Geräte, die den ABUS Link Station-Dienst unterstützen.

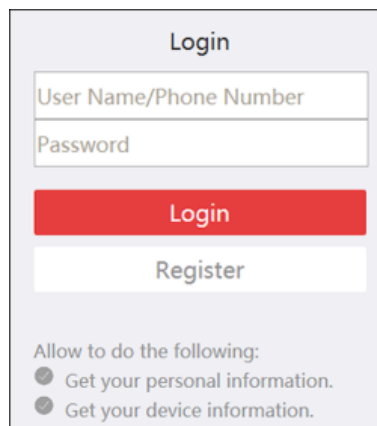
4.1 Registrierung eines ABUS Link Stationskontos

Der Client unterstützt die Registrierung eines ABUS Link Station-Kontos zur Verwaltung von Geräten, die den ABUS Link Station-Dienst unterstützen.

Schritte

1. Rufen Sie die Anmeldeseite der ABUS Link Station auf.
 - Klicken Sie auf **Anmelden in der** oberen rechten Ecke des Clients.
 1. Klicken Sie auf **Geräteverwaltung** → **Gerät**, um die Seite Geräteverwaltung aufzurufen.
 2. Klicken Sie auf **Hinzufügen**, um das Fenster Gerät hinzufügen zu öffnen.
 3. Wählen Sie **ABUS Link Station** als Hinzufügemodus.
 4. Klicken Sie auf **Anmelden**.

Das Anmeldefenster wird geöffnet.



The screenshot shows a login and registration interface. At the top, the word "Login" is centered. Below it are two input fields: "User Name/Phone Number" and "Password". Underneath these fields are two buttons: a red "Login" button and a white "Register" button. At the bottom, there is a section titled "Allow to do the following:" with two checked radio buttons: "Get your personal information." and "Get your device information."

Abbildung 4-1 Anmeldefenster

2. Klicken Sie auf **Registrieren**, um das Fenster Konto registrieren zu öffnen.
3. Geben Sie die erforderlichen Informationen ein, einschließlich Benutzername, Passwort, Passwortbestätigung und Telefonnummer/E-Mail-Adresse.

 **Vorsicht**

Die Passwortstärke des Geräts kann automatisch überprüft werden. Wir empfehlen Ihnen dringend, das Passwort Ihrer Wahl zu ändern (mit mindestens 8 Zeichen, darunter mindestens drei Arten der folgenden Kategorien: Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen), um die Sicherheit Ihres Produkts zu erhöhen. Und wir empfehlen Ihnen, Ihr Passwort regelmäßig zu ändern, vor allem im Hochsicherheitssystem kann eine monatliche oder wöchentliche Änderung des Passworts Ihr Produkt besser schützen.

Die ordnungsgemäße Konfiguration aller Kennwörter und anderer Sicherheitseinstellungen liegt in der Verantwortung des Installateurs und/oder des Endbenutzers.

4. Klicken Sie auf **Nachricht senden**, um einen Verifizierungscode zu erhalten.
Das System sendet einen Verifizierungscode an Ihr Telefon oder Ihre E-Mail.
5. Geben Sie den erhaltenen Verifizierungscode in das Textfeld **Verifizierungscode** ein.
6. **Ich habe die Nutzungsbedingungen gelesen und stimme den Datenschutzbestimmungen zu.**
7. Klicken Sie auf **Registrieren**, um die Registrierung abzuschließen.

4.2 Anmeldung bei ABUS Link Station Konto

Sie können sich über den Client in das ABUS Link Station Konto einloggen, um Geräte zu bedienen, die über das ABUS Link Station Konto verwaltet werden.

Bevor Sie beginnen

Registrieren Sie ein ABUS Link Station Konto.

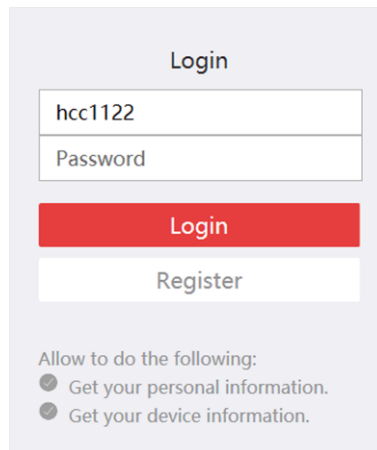
 **Hinweis**

Einzelheiten finden Sie unter **[Registrieren eines ABUS Link Station Kontos.](#)**

Schritte

1. Rufen Sie die Anmeldeseite der ABUS Link Station auf.
 - Klicken Sie auf **Anmelden in der** oberen rechten Ecke des Clients.
 1. Klicken Sie auf **Geräteverwaltung** → **Gerät**, um die Seite Geräteverwaltung aufzurufen.
 2. Klicken Sie auf **Hinzufügen**, um das Fenster Gerät hinzufügen zu öffnen.
 3. Wählen Sie **ABUS Link Station** als Hinzufügemodus.
 4. Klicken Sie auf **Anmelden**.

Das Anmeldefenster wird geöffnet.



Login

hcc1122

Password

Login

Register

Allow to do the following:

- Get your personal information.
- Get your device information.

Abbildung 4-2 Anmeldeseite der ABUS Link Station

2. Geben Sie den Benutzernamen und das Passwort ein.
3. Klicken Sie auf **Anmelden**, um sich bei Ihrem Konto anzumelden.
Log in wird zu **Logged in**.
4. Optional: Klicken Sie auf **Eingeloggt** → **Abmelden**, um sich von Ihrem Konto abzumelden.

Hinweis

- Von der ABUS Link Station hinzugefügte Geräte werden nach dem Abmelden vom ABUS Link Station Service ausgeblendet
 - Alarmbezogene Bilder, die in der ABUS Link Station gespeichert werden, sind 2 Stunden lang gültig.
-












Kapitel 5 Live-Ansicht

Sie können das Live-Video der hinzugefügten Netzwerk-Kameras und Video-Encoder auf der Seite Hauptansicht anzeigen. Außerdem werden einige grundlegende Funktionen unterstützt, z. B. Bildaufnahme, manuelle Aufzeichnung, Fensteraufteilung, PTZ-Steuerung, automatische Umschaltung in der Live-Ansicht usw.

5.1 Symbolleiste der Live-Ansicht

Mit der Symbolleiste für die Live-Ansicht können Sie das Live-Ansichtsfenster bequemer und schneller bedienen und verwalten. Zum Beispiel können Sie mit einem Klick auf die Werkzeuge in der Symbolleiste ein Bild aufnehmen, den Ton aufnehmen, die Lautstärke einstellen und das Fenster teilen.

Tabelle 5-1 Beschreibungen der Symbolleiste

Icon	Funktion Name	Funktionsbeschreibung und Bedienung
	Ansicht speichern	Speichern Sie die Ansicht, die Sie gerade erstellen, um die gewünschten Kameras schnell anzeigen zu können. Klicken Sie auf  , um das Fenster zum Speichern der Ansicht zu öffnen. Wählen Sie Ansicht erstellen oder Aktuelle Ansicht und einen Namen für die Ansicht.
	Live-Ansicht anhalten	Halten Sie alle Live-View-Kameras an.
	Stummschaltung /Stummschaltung aufheben	Klicken Sie auf  , um die Lautstärkeleiste einzublenden, klicken Sie auf  , um die Stummschaltung aufzuheben, und Sie können die Lautstärke einstellen. Klicken Sie auf  , um die Lautstärkeleiste einzublenden, und klicken Sie erneut auf  , um die Live-View-Kameras stumm zu schalten.
	Abteilung Fenster	Wählen Sie die verschiedenen Fensterteilungsmodi für die Live-Ansicht. Klicken Sie auf  , um einen Fensterteilungsmodus auszuwählen (z. B. 9 Fensterteilung). Sie können auch auf Hinzufügen klicken, um einen Fensterteilungsmodus anzupassen.
	Vollbild	Zeigt die Live-Ansicht im Vollbildmodus an. Drücken Sie die Esc-Taste, um den Vollbildmodus zu verlassen.





Icon	Funktion Name	Funktionsbeschreibung und Bedienung
	Konfiguration	Rufen Sie den Einstellmodus für die Live-Ansicht-Parameter auf und konfigurieren Sie Live-Ansicht und Wiedergabe, Bild, Dateien und Symbolleiste.


Tabelle 5-2 Beschreibung der Symbole im Live-View-Fenster

Icon	Funktion Name	Funktionsbeschreibung und Bedienung
	Erfassen Sie	Nehmen Sie die Bilder für das Live-View-Fenster manuell auf.
	Aufnahme starten/Aufnahme stoppen	Klicken Sie beim ersten Mal auf , um die Aufnahme zu starten, und klicken Sie erneut, um die Aufnahme zu beenden. Die Aufnahmedateien werden automatisch in dem von Ihnen festgelegten Pfad gespeichert.
	Umschalten auf sofortige Wiedergabe	Bei der aktuellen Uhrzeit können Sie wählen, ob das Video in den letzten 30 Sekunden, 1 Minute, 3 Minuten, 5 Minuten, 8 Minuten oder 10 Minuten wiedergegeben werden soll.

5.2 Benutzerdefinierte Ansicht hinzufügen

Eine Ansicht ist eine Fensteraufteilung mit Kameras, die für jedes Fenster konfiguriert sind. Im Ansichtsmodus können Sie die Fensteraufteilung und die Zuordnung zwischen Kameras und Fenstern als Favorit speichern, um später schnell auf die entsprechenden Kameras zugreifen zu können. Sie können zum Beispiel Kamera 1, Kamera 2 und Kamera 3 in Ihrem Büro miteinander verknüpfen, um Fenster anzuzeigen, und diese als Ansicht mit dem Namen Büro speichern.

Schritte

1. Rufen Sie die Seite Hauptansicht auf.
2. Klicken Sie auf die Registerkarte **Ressourcen**.
3. Bewegen Sie den Cursor auf die benutzerdefinierte Ansicht im Ressourcenfenster und klicken Sie auf  , um eine neue Ansicht zu erstellen.
4. Geben Sie einen Namen für die Ansicht ein.

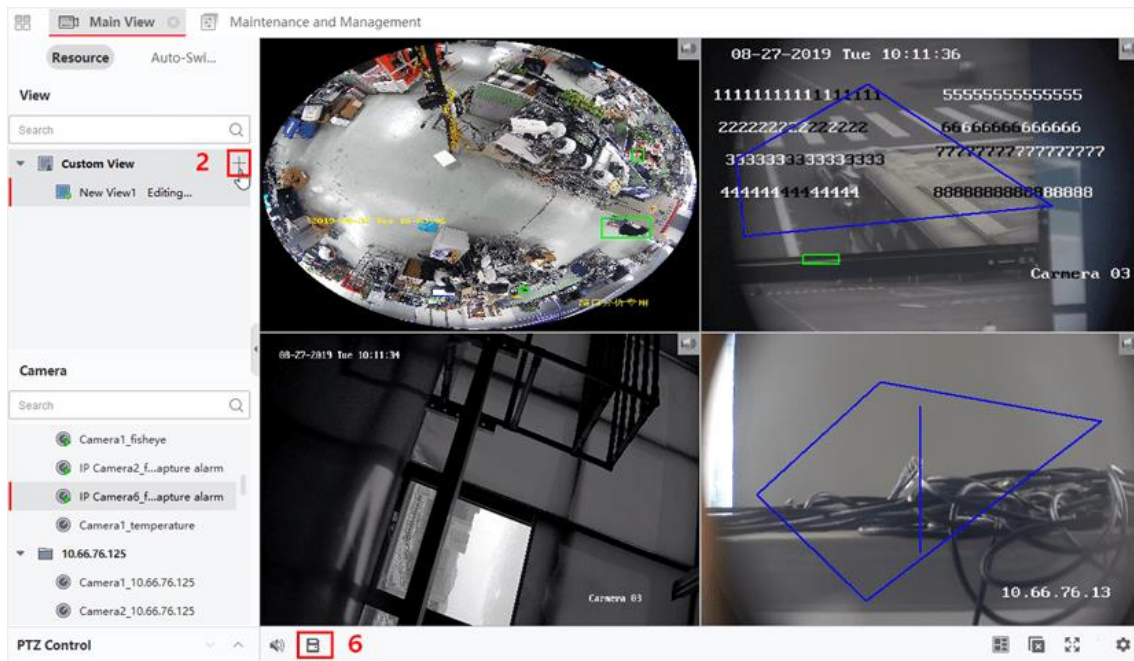





Abbildung 5-1 Benutzerdefinierte Ansicht hinzufügen


5. Optional: Klicken Sie in der Symbolleiste der Live-Ansicht auf  , um den Fensterteilungsmodus für die neue Ansicht festzulegen.
6. Starten Sie die Live-Ansicht für die angegebene Kamera im angegebenen Fenster entsprechend den aktuellen Anforderungen.
7. Klicken Sie auf  , um die aktuelle Ansicht zu speichern oder sie als neue Ansicht zu speichern.

Hinweis

Es können bis zu 16 benutzerdefinierte Ansichten zum Client hinzugefügt werden.

8. Optional: Führen Sie nach dem Hinzufügen der benutzerdefinierten Ansicht die folgenden Vorgänge aus.

Name der Ansicht bearbeiten Bewegen Sie den Cursor über die neue Ansicht und klicken Sie auf  , um den Namen der Ansicht zu bearbeiten.

Ansicht löschen Bewegen Sie den Cursor über die neue Ansicht und klicken Sie auf  , um die Ansicht zu löschen.

Was ist als nächstes zu tun?





Klicken Sie erneut auf  , um die benutzerdefinierte Fensteraufteilung auszuwählen.

5.3 Live-Ansicht starten

Sie können die Live-Ansicht starten, nachdem Sie ein oder mehrere Geräte zum Client hinzugefügt haben, damit Sie den überwachten Bereich gut kennenlernen können. Sie können die Live-Ansicht

für eine Kamera oder für alle Kameras einer Gruppe starten. Sie können die Live-Ansicht auch im benutzerdefinierten Ansichtsmodus starten.

Klicken Sie auf **Hauptansicht** → **Ressource**, um die Seite Hauptansicht zu öffnen. Wählen Sie in der linken Ressourcenliste die Ressource(n) aus und starten Sie die Live-Ansicht auf die folgenden Arten.

Verfügbare Wege	Beschreibung	Operation
Live-Ansicht für eine Kamera starten	Starten Sie die Live-Ansicht von nur einer Kamera in einer Gruppe.	<ul style="list-style-type: none"> • Wählen Sie eine Kamera aus und ziehen Sie sie in das Fenster. • Doppelklicken Sie auf die Kamera in einer Gruppe. • Bewegen Sie den Mauszeiger über den Kameranamen und klicken Sie auf  .
Live-Ansicht für Kameragruppe starten	Starten Sie die Live-Ansicht aller Kameras in einer Gruppe synchron.	<ul style="list-style-type: none"> • Wählen Sie eine Gruppe aus und ziehen Sie sie in das Fenster. • Doppelklicken Sie auf die Gruppe. • Bewegen Sie den Mauszeiger über den Gruppennamen, und klicken Sie auf  , oder klicken Sie auf  → Alle Kameras in der Gruppe anzeigen.
Starten der Live-Ansicht im Modus Benutzerdefinierte Ansicht	Starten Sie die Live-Ansicht der Kameras in der benutzerdefinierten Ansicht.	<ul style="list-style-type: none"> • Wählen Sie eine benutzerdefinierte Ansicht und ziehen Sie sie in das Fenster. • Doppelklicken Sie auf die benutzerdefinierte Ansicht. <hr/> <p> Hinweis</p> <p>Passen Sie eine Ansicht an, die Informationen wie z. B. die Fensteraufteilung, die Kamera und die Entsprechung zwischen Kameras und Fenstern enthält. Siehe <u>Benutzerdefinierte Ansicht hinzufügen</u> für weitere Informationen.</p> <hr/>

 **Hinweis**

Wenn das Gerät die Stream-Verschlüsselung unterstützt und der Stream seiner Live-Ansicht verschlüsselt ist, müssen Sie einen Stream-Schlüssel zur doppelten Überprüfung eingeben.

Abbildung 5-2 Live-Ansicht starten

In der Live-Ansicht können Sie die Bitrate, die Bildrate und die Auflösung des Bildes anzeigen.

5.4 Automatisches Umschalten in der Live-Ansicht

Sie können die Live-Ansicht von Kameras anzeigen oder die benutzerdefinierten Ansichten abwechselnd anzeigen, was als "Auto-Switch" bezeichnet wird. Wenn Sie die Live-Ansicht einer großen Anzahl von Kameras anzeigen möchten, können Sie die ausgewählten Kameras automatisch umschalten. Sie können auch mehrere Ansichten automatisch umschalten.


Bei der automatischen Umschaltung in der Live-Ansicht sind drei Modi verfügbar:

- Automatisches Umschalten aller Kameras in die Standardansicht
- Automatisches Umschalten von Kameras in einer Gruppe
- Benutzerdefinierte Ansichten automatisch umschalten

5.4.1 Automatisches Umschalten von Kameras in einer Gruppe

Der Videostrom der Kameras derselben Gruppe kann automatisch in einem ausgewählten Anzeigefenster umgeschaltet werden. Wenn Sie z. B. die automatische Umschaltung einer Gruppe mit 5 Kameras starten, wird die Live-Ansicht der 5 Kameras abwechselnd in einem konfigurierbaren Intervall angezeigt. Sie können auch auf Wiedergabe umschalten und andere Operationen im Anzeigefenster durchführen.

Schritte

1. Rufen Sie die Seite Hauptansicht auf.
2. Klicken Sie im linken Bereich auf **Auto-Switch** → **Single Window Auto-Switch**, um die Gruppen anzuzeigen.
3. Wählen Sie ein Anzeigefenster auf der rechten Seite.
4. Bewegen Sie den Cursor auf einen Gruppennamen und klicken Sie auf  .

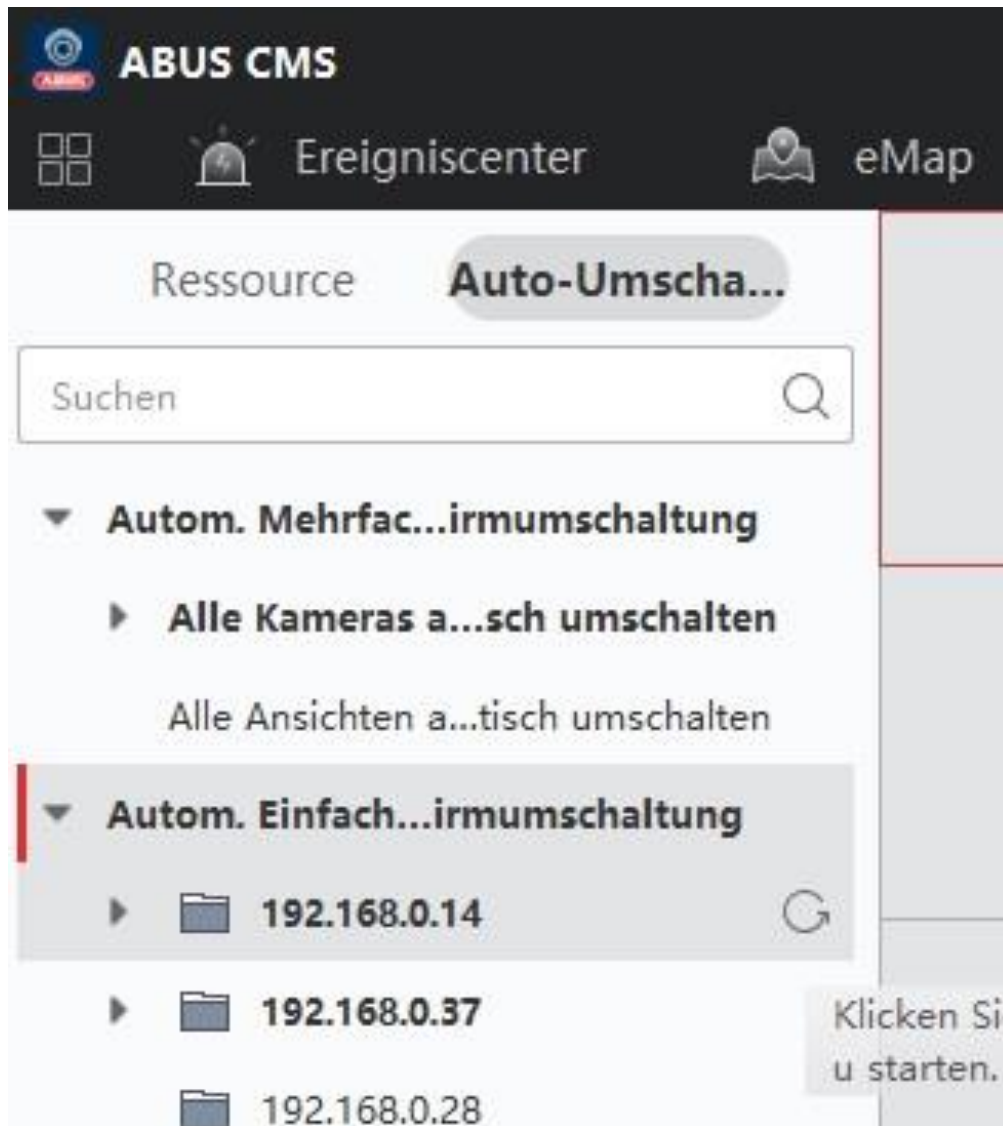






Abbildung 5-3 Start der automatischen Umschaltung von Kameras in einer Gruppe

Die Kameras der ausgewählten Gruppe werden im Anzeigefenster automatisch umgeschaltet.

 **Hinweis**

Der Ton ist nach dem Start der automatischen Umschaltung standardmäßig ausgeschaltet.

5. Optional: Führen Sie die folgenden Vorgänge durch.

Operation	Beschreibung
Pause/Fortsetzen Auto-Switch	Klicken Sie auf  oder  , um die automatische Umschaltung anzuhalten/fortzusetzen.
Zur vorherigen/nächsten Seite gehen	Klicken Sie auf  oder  , um die Kameras der vorherigen/nächsten Gruppe anzuzeigen.


**Verweilzeit
einstellen**

Klicken Sie nach dem Anhalten der aktuellen automatischen Umschaltung auf « oder » , um die Verweilzeit der automatischen Umschaltung zu verringern/erhöhen, oder klicken Sie auf **20s** unten auf der Seite, um die Verweilzeit der automatischen Umschaltung zu ändern. Sie können auch auf **Benutzerdefinierte Verweilzeit** klicken, um die Verweilzeit nach Ihren Bedürfnissen einzustellen. Wenn Sie z. B. ein Intervall von 10 Sekunden einstellen, wird das Bild jeder Gruppe 10 Sekunden lang angezeigt und dann zur nächsten Gruppe gewechselt.

5.4.2 Automatisches Umschalten aller Kameras

Das Video aller Kameras in der Kameraliste kann automatisch in einem selbstanpassenden Modus umgeschaltet werden. Wenn Sie die automatische Umschaltung aller Kameras starten, kann die Live-Ansicht aller Kameras schnell angezeigt werden, was eine effektive Methode für die Live-Ansicht ist. Die automatische Umschaltung erfolgt in einem konfigurierbaren Intervall. Sie können im Auto-Switch-Fenster auch zur Wiedergabe wechseln und andere Aktionen durchführen.

Schritte

1. Rufen Sie die Seite Hauptansicht auf.
2. Klicken Sie im linken Bereich auf **Auto-Switch** → **Multi-Window Auto-Switch**.
3. Bewegen Sie den Mauszeiger auf **Auto-Switch All Cameras** und klicken Sie auf  .

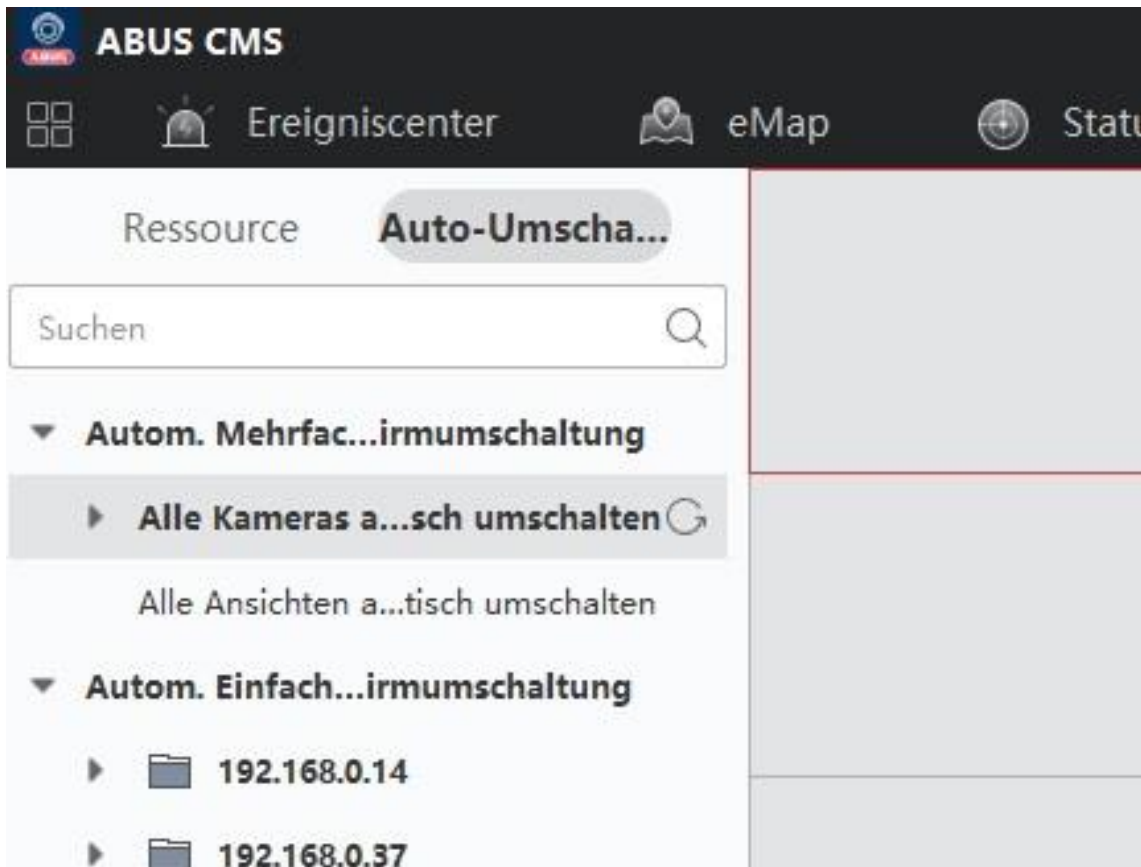


Abbildung 5-4 Auto-Switch für alle Kameras starten

Alle Kameras in der Kameraliste starten die automatische Umschaltung in einem selbstanpassenden Modus.

4. Optional: Führen Sie die folgenden Vorgänge durch.

Operation	Beschreibung
Pause/Fortsetzen Auto-Switch	Klicken Sie auf oder ↺ , um die automatische Umschaltung anzuhalten/fortzusetzen.
Zur vorherigen/nächsten Seite gehen	Klicken Sie auf < oder > , um Kameras auf der vorherigen/nächsten Seite anzuzeigen.
Verweilzeit einstellen	Klicken Sie nach dem Anhalten der aktuellen automatischen Umschaltung auf << oder >> , um die Verweilzeit der automatischen Umschaltung zu verringern/erhöhen, oder klicken Sie auf 20s unten auf der Seite, um die Verweilzeit der automatischen Umschaltung zu ändern. Sie können auch auf Benutzerdefinierte Verweilzeit klicken, um die Verweilzeit nach Ihren Bedürfnissen einzustellen. Wenn Sie zum Beispiel ein Intervall von 10 Sekunden einstellen, wird das Bild jeder Kamera 10 Sekunden lang angezeigt und dann zur nächsten

Kamera umgeschaltet.


5.4.3 Benutzerdefinierte Ansichten automatisch umschalten

Eine Ansicht ist eine Fensteraufteilung mit Ressourcenkanälen (z. B. Kameras), die mit jedem Fenster verknüpft sind. Im Ansichtsmodus können Sie die Fensteraufteilung und die Zuordnung zwischen Kameras und Fenstern als Favoriten speichern, damit Sie später schnell auf diese Kanäle zugreifen können. Wenn Sie eine Ansicht speichern, die alle Kameras auf einer Etage enthält, speichern Sie eine benutzerdefinierte Ansicht, und Sie können die Live-Ansicht aller Kameras auf der Etage nacheinander mit einem Mausklick aufrufen. Auf diese Weise müssen Sie diese Kameras nicht jedes Mal in der Kameraliste suchen, wenn Sie sich anmelden. Die automatische Umschaltung erfolgt in einem Intervall, das manuell konfiguriert werden kann.

Bevor Sie beginnen

Fügen Sie die benutzerdefinierten Ansichten hinzu. Siehe [**Benutzerdefinierte Ansicht hinzufügen**](#) für Details.

Schritte

1. Rufen Sie die Seite Hauptansicht auf.
2. Klicken Sie auf der linken Seite auf **Ressource** → **Multi-Window Auto-Switch**.
3. Bewegen Sie den Mauszeiger auf **Auto-Switch All Views** und klicken Sie auf  .

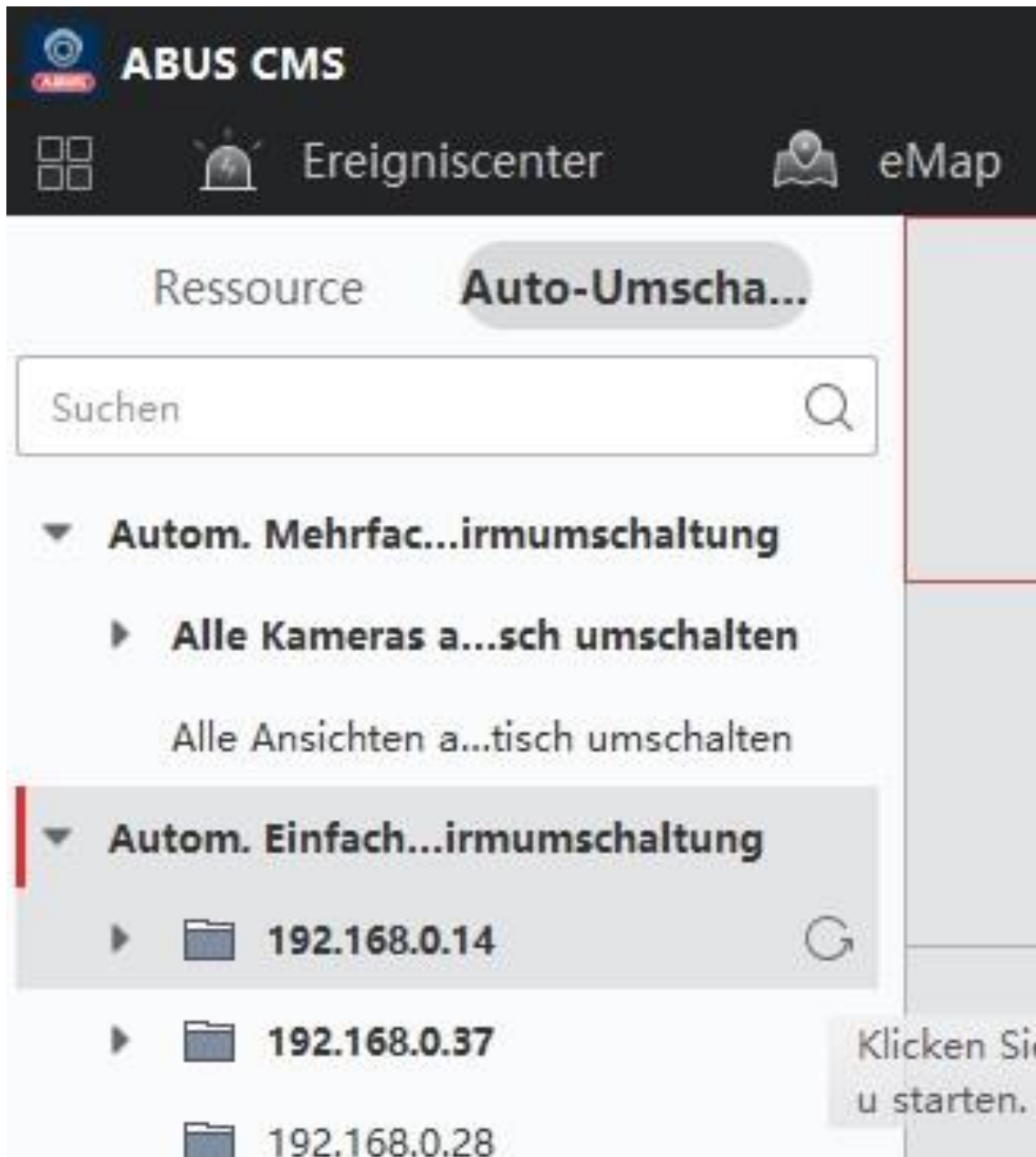


Abbildung 5-5 Automatisches Umschalten einer benutzerdefinierten Ansicht

Alle benutzerdefinierten Ansichten werden automatisch umgeschaltet.

4. Optional: Führen Sie die folgenden Vorgänge durch.

Operation	Beschreibung
Pause/Fortsetzen Auto-Switch	Klicken Sie auf II oder ↺ , um die automatische Umschaltung anzuhalten/fortzusetzen.
Zur vorherigen/nächsten Seite gehen	Klicken Sie auf < oder > , um die vorherige/nächste Ansicht anzuzeigen.

Verweilzeit einstellen

Klicken Sie nach dem Anhalten der aktuellen automatischen Umschaltung auf « oder » , um die Verweilzeit der automatischen Umschaltung zu verringern/erhöhen, oder klicken Sie auf **20s** unten auf der Seite, um die Verweilzeit der automatischen Umschaltung zu ändern. Sie können auch auf **Benutzerdefinierte Verweilzeit** klicken, um die Verweilzeit nach Ihren Bedürfnissen einzustellen. Wenn Sie z. B. ein Intervall von 10 Sekunden einstellen, wird das Bild jeder Ansicht 10 Sekunden lang angezeigt und dann zur nächsten Ansicht gewechselt.

5.5 PTZ-Steuerung

Die Software bietet PTZ-Steuerung für Kameras mit Schwenk-/Neige-/Zoom-Funktion. Während der PTZ-Steuerung können Sie Voreinstellungen, Patrouillen und Muster festlegen und ein neues Fenster zur Steuerung des PTZ öffnen.



Vorsicht

- Einige Funktionen sollten von dem Gerät unterstützt werden.

5.5.1 PTZ-Bedienfeld

Die Software bietet PTZ-Steuerungsfunktionen über das Bedienfeld, z. B. Erkennung, Geschwindigkeit, Vergrößern, Verkleinern usw. Sie können auch ein neues Fenster zur Steuerung des PTZ öffnen.




Hinweis











Die ABUS Link Station unterstützt nur PTZ-Bewegungen in die Richtungen nach oben, unten, links und rechts.







Rufen Sie das Modul **Hauptansicht** auf, und wählen Sie **PTZ-Steuerung**, um das PTZ-Steuerungsfeld zu öffnen.







Die folgenden Symbole sind auf dem PTZ-Bedienfeld verfügbar.

Tabelle 5-3 Icons auf dem PTZ-Bedienfeld

Icon	Name	Beschreibung
	Richtungs-Schaltflächen	Klicken Sie mit der linken Maustaste oder halten Sie sie gedrückt, um das PTZ-Gerät zu drehen. Klicken Sie, um die PTZ horizontal und kontinuierlich zu drehen; klicken Sie erneut,

Icon	Name	Beschreibung
		um die Drehung zu beenden.
	Geschwindigkeitskontrolle	Ziehen Sie den Schieberegler, um die PTZ-Bewegungsgeschwindigkeit anzupassen.
	Vergrößern/Verkleinern	Vergrößern Sie das Bild, um Details zu sehen, verkleinern Sie es, um ein Panoramabild zu sehen.
	Fokus +/-	Klicken Sie auf Fokus + , um den Fokuspunkt nach vorne zu verschieben, und auf Fokus - , um den Fokuspunkt nach hinten zu verschieben.
	Blende +/-	Dient zur Einstellung der Leuchtdichte des Bildes. Je größer die Blende ist, desto mehr Licht fällt ein, und desto heller wird das Bild.
	3D-Positionierung	Klicken Sie mit der linken Maustaste auf die gewünschte Position im Videobild und ziehen Sie einen rechteckigen Bereich in die untere rechte Richtung, dann verschiebt das Dome-System die Position in die Mitte und lässt den rechteckigen Bereich einzoomen. Ziehen Sie mit der linken Maustaste einen rechteckigen Bereich in die obere linke Richtung, um die Position in die Mitte zu verschieben und den rechteckigen Bereich zu verkleinern.
	Zusätzlicher Fokus	Klicken Sie auf , um automatisch zu fokussieren.
	Initialisierung des Objektivs	Initialisieren Sie das Objektiv und stellen Sie erneut scharf, um ein klares Bild zu erhalten.
	Licht	Klicken Sie auf , um Licht zu füllen. <hr/>  Hinweis Diese Funktion muss von dem Gerät unterstützt werden. <hr/>
	Wischer	Verwenden Sie den Wischer, um den Staub auf dem Kameraobjektiv zu entfernen.








Icon	Name	Beschreibung
	Manuelle Verfolgung	Bei Speed Dome-Kameras mit Auto-Tracking-Funktion aktivieren Sie das Auto-Tracking (über das Rechtsklickmenü) und klicken Sie auf das Symbol, um das Ziel manuell zu verfolgen, indem Sie auf das Video klicken.
	Menü	Bei einer analogen Speed Dome-Kamera klicken Sie auf das Symbol, um das lokale Menü anzuzeigen. Detaillierte Informationen zur Bedienung des Menüs finden Sie im Benutzerhandbuch der Speed Dome-Kamera.
	One-Touch-Patrouille	Bei Speed Domes mit One-Touch-Streifenfunktion klicken Sie auf das Symbol, und die Speed Dome-Kamera beginnt nach einer gewissen Zeit der Inaktivität (Parkzeit) mit dem Streifengang von der vordefinierten Voreinstellung Nr. 1 bis zur Voreinstellung Nr. 32. Informationen zur Einstellung der Parkzeit finden Sie im Benutzerhandbuch der Speed Dome-Kamera.
	Parken mit einem Tastendruck	Bei der Speed Dome-Kamera mit One-Touch-Park-Funktion klicken Sie auf das Symbol, und die Speed Dome-Kamera speichert die aktuelle Ansicht unter der Voreinstellung Nr. 32. Das Gerät beginnt nach einer gewissen Zeit der Inaktivität (Parkzeit) automatisch mit dem Parken auf der voreingestellten Nr. 32. Informationen zum Einstellen der Parkzeit finden Sie im Benutzerhandbuch der Speed Dome-Kamera.
	Manuelles Objektiv-Enteisungsheizgerät einschalten	<p>Aktivieren Sie diese Funktion, um die Leistung der Kamera durch Erwärmung zu gewährleisten.</p> <hr/> <p> Hinweis</p> <p>Wir empfehlen Ihnen, diese Funktion zu aktivieren, wenn die Umgebungstemperatur unter 0 °C liegt, da sonst die hohen Temperaturen die Arbeit der Kamera beeinträchtigen können.</p> <hr/>

Icon	Name	Beschreibung
	Manuelle PT-Enteisung einschalten	Aktivieren Sie diese Funktion, um die Kameraleistung zu gewährleisten, indem Sie das an der PTZ-Kamera haftende Eis abwischen.
	Manuelle Gesichtserfassung	Klicken Sie auf diese Schaltfläche und halten Sie die linke Maustaste gedrückt, um ein Gesicht im Bild auszuwählen und es zu erfassen. Das Bild wird zur Ansicht auf den Server hochgeladen.
	FOV synchronisieren	Bei Wärmebildkameras klicken Sie auf das Symbol, um das Sichtfeld des optischen Kanals mit dem des Wärmebildkanals zu synchronisieren.
	Regionale Exposition	Klicken Sie bei Speed Domes auf das Symbol und ziehen Sie ein Rechteck auf das Bild, um den Belichtungseffekt in diesem Bereich zu optimieren.
	Regionaler Schwerpunkt	Klicken Sie bei Speed Domes auf das Symbol und ziehen Sie ein Rechteck auf das Bild, um den Fokuseffekt in diesem Bereich zu optimieren.
	Scharfschalten und Verfolgen	Bei Kameras, die das Scharfstellen und Verfolgen unterstützen, klicken Sie auf das Symbol und wählen Sie das Ziel (Person oder Fahrzeug) in der Live-Ansicht aus, um dieses Ziel scharfzustellen und zu verfolgen.

5.5.2 Voreinstellung, Patrouille und Muster einstellen

Die PTZ-Steuerung unterstützt das Einstellen und Aufrufen einer Voreinstellung, einer Patrouille und eines Musters.

Klicken Sie auf der Startseite auf **Hauptansicht** → **PTZ-Steuerung**, um das Bedienfeld PTZ-Steuerung anzuzeigen.

Aufgabe	Definition	Operation
Voreinstellung	<p>Eine Voreinstellung verknüpft die Schlüsselregionen mit der Position und dem Status der mobilen PTZ. Das Überwachungspersonal kann damit schnell zu den Schlüsselregionen gelangen. Durch Senden eines Voreinstellungsbefehls zeichnet die mobile PTZ die Position und den Status von Zoom, Fokus und Blende auf. Beim Ausführen des Voreinstellungsbefehls fährt die mobile PTZ schnell zur eingestellten Position und kehrt zum eingestellten Status zurück.</p>	<p>Einstellen: Wählen Sie eine Voreinstellung aus der Voreinstellungsliste, drehen Sie die Kamera in die gewünschte Position und klicken Sie auf  .</p> <hr/> <p>So rufen Sie an:  .</p>
Muster	<p>Mit dem Aufzeichnungsmuster können der Bewegungspfad und die Verweildauer an einer bestimmten Position genau aufgezeichnet werden. Durch den Aufruf des Musters beginnt die mobile PTZ mit der Bewegung entsprechend dem aufgezeichneten Pfad.</p>	<p>Einstellen: Klicken Sie auf  , um mit der Aufnahme eines Musters zu beginnen, klicken Sie auf die Richtungstasten, um das Muster zu formen, klicken Sie auf  .</p> <hr/> <p>So rufen Sie an:  .</p>
Streife	<p>Patrouille ist die Funktion, mit der der Benutzer eine Abtastspur mit einer Gruppe von definierten Voreinstellungen festlegt. Die Patrouille zwischen zwei Voreinstellungen wird mit der eingestellten Geschwindigkeit und Zeit durchgeführt.</p>	<p>Einstellen: Klicken Sie auf  → wählen Sie die Voreinstellungen und stellen Sie Geschwindigkeit und Zeit ein → klicken Sie auf OK.</p> <hr/> <p>Wie Sie anrufen können:  anklicken.</p>

 **Hinweis**

Sie sollten vorher mindestens zwei Voreinstellungen vornehmen.

5.6 Anpassen der Fensteraufteilung

Die Client-Software bietet mehrere Arten von vordefinierten Fenstereinteilungen. Sie können die Fensteraufteilung auch nach Ihren Wünschen einstellen.

Schritte

 **Hinweis**

Bis zu 5 Fensterteilungen können individuell gestaltet werden.


1. Öffnen Sie die Seite Hauptansicht oder Fernwiedergabe.
2. Klicken Sie in der Symbolleiste der Live-Ansicht oder der Wiedergabe auf  , um das Fenstereinteilungsfeld zu öffnen.



Abbildung 5-6 Benutzerdefinierte Fensterteilung hinzufügen

3. Klicken Sie auf **Hinzufügen**, um das Dialogfeld Benutzerdefinierte Fensterteilung hinzufügen zu öffnen.
4. Geben Sie die Fensternummern in der horizontalen und vertikalen Dimension in das Feld Dimension ein und drücken Sie dann die **Eingabetaste** auf Ihrer Tastatur.

 **Hinweis**

Bei der Fernwiedergabe können bis zu 16 Fenster gleichzeitig wiedergegeben werden, so dass die benutzerdefinierte Fenstereinteilung mit mehr als 16 Fenstern ungültig ist.

5. Optional: Ziehen Sie die Maus, um die benachbarten Fenster auszuwählen, und klicken Sie auf **"Verbinden"**, um sie zu einem ganzen Fenster zusammenzufügen.

Benutzerdefinierte Fensterteilung hinzufügen

Name

Abmessungen X

Fensteraufteilung Ver... Wieder...

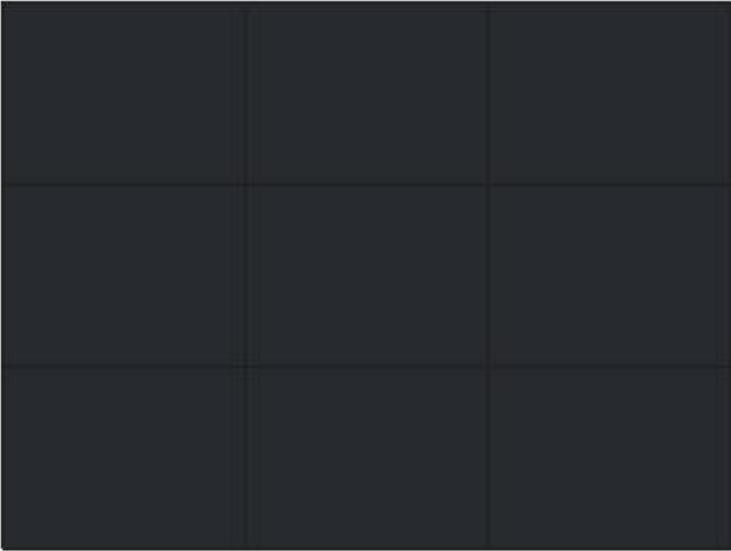



Abbildung 5-7 Fenster "Benutzerdefinierte Fensterteilung hinzufügen"

6. Optional: Wählen Sie das Verbindungsfenster aus und klicken Sie auf **Wiederherstellen**, um die Verbindung aufzuheben.
7. Klicken Sie auf **Speichern**.
8. Optional: Klicken oder ziehen Sie einen Teilungsmodus auf das Anzeigefenster, um den Modus für die Anzeige anzuwenden.
9. Optional: Bearbeiten Sie einen benutzerdefinierten Fensterteilungsmodus.
 - 1) Klicken Sie in der Symbolleiste der Live-Ansicht oder der Wiedergabe auf  , um das Fenstereinteilungsfeld zu öffnen.
 - 2) Klicken Sie auf **Bearbeiten**, um die Abteilung Benutzerdefiniertes Fenster hinzufügen zu öffnen.
 - 3) Wählen Sie einen benutzerdefinierten Teilungsmodus und führen Sie Operationen wie Umbenennung, Einstellen von Maßen, Zusammenfügen/Aufheben des Zusammenfügens von Fenstern durch.

5.7 Manuelles Aufzeichnen und Erfassen

Während der Live-Ansicht können Sie Videos und Bilder manuell aufzeichnen und dann die aufgezeichneten Videodateien und aufgenommenen Bilder auf dem lokalen PC anzeigen.






5.7.1 Manuelles Aufzeichnen von Videos

Mit der manuellen Aufnahmefunktion können Sie das Live-Video auf der Hauptansichtsseite manuell aufzeichnen und die Videodateien auf dem lokalen PC speichern.

Schritte

Hinweis

Die manuelle Aufzeichnung wird von der ABUS Link Station während der Live-Ansicht nicht unterstützt.

1. Öffnen Sie die Seite Hauptansicht.
2. Starten Sie die Live-Ansicht.
3. Führen Sie einen der folgenden Schritte aus, um die manuelle Aufnahme zu starten.
 - Bewegen Sie den Cursor auf das Anzeigefenster in der Live-Ansicht, um die Symbolleiste einzublenden, und klicken Sie auf  in der Symbolleiste.
 - Klicken Sie mit der rechten Maustaste auf das Anzeigefenster und klicken Sie im Rechtsklickmenü auf **Aufzeichnung starten**.
Das Symbol  wird zu . In der oberen rechten Ecke des Anzeigefensters erscheint eine Anzeige .
4. Klicken Sie auf , um die manuelle Aufnahme zu beenden.
Die aufgezeichnete Videodatei wird automatisch auf dem lokalen PC gespeichert, und ein kleines Fenster mit den Informationen zum Speicherpfad wird in der unteren rechten Ecke des Desktops angezeigt.

Hinweis

Der Speicherpfad für die aufgezeichneten Videodateien kann auf der Seite Systemkonfiguration festgelegt werden. Siehe [**Dateispeicherpfad festlegen**](#) für weitere Informationen.


5.7.2 Lokale Videos anzeigen

Sie können die aufgezeichneten Videodateien, die auf Ihrem lokalen PC gespeichert sind, ansehen.

Bevor Sie beginnen

Nehmen Sie das Live-Video auf.

Schritte

1. Klicken Sie auf  → **Datei** → **Videodatei öffnen** in der oberen rechten Ecke, um die Seite Videodateien zu öffnen.
2. Wählen Sie aus der Liste der Kameragruppen die Kamera aus, mit der Sie die aufgezeichneten Videodateien suchen möchten.
3. Geben Sie die Start- und Endzeit für die Suche in der unteren linken Ecke an.
4. Klicken Sie auf **Suchen**.
Die Videodateien, die zwischen der Start- und der Endzeit aufgezeichnet wurden, werden auf der Seite im Miniaturformat angezeigt.
5. Optional: Führen Sie die folgende(n) Operation(en) nach der Suche durch.

Videodatei löschen Wählen Sie die Videodatei aus, und klicken Sie auf **Löschen**, um die Videodatei zu löschen.

E-Mail senden Wählen Sie die Videodatei aus, und klicken Sie auf **E-Mail**, um eine E-Mail-Benachrichtigung mit der ausgewählten Videodatei im Anhang zu senden.

Hinweis

Um eine E-Mail-Benachrichtigung zu senden, müssen die E-Mail-Einstellungen konfiguriert werden, bevor Sie fortfahren können. Einzelheiten finden Sie unter ***E-Mail-Parameter festlegen***.

Lokales Video speichern Wählen Sie die Videodatei aus, und klicken Sie auf **Speichern unter**, um eine neue Kopie der Videodatei zu speichern.


Wiedergabe Doppelklicken Sie auf die Videodatei, um die lokale Wiedergabe zu starten.

5.7.3 Bilder Snapshot

Sie können während der Live-Ansicht Bilder aufnehmen.

Führen Sie diese Aufgabe aus, wenn Sie während der Live-Ansicht Bilder aufnehmen möchten.

Schritte

1. Öffnen Sie die Seite Hauptansicht und starten Sie die Live-Ansicht einer Kamera.
2. Führen Sie einen der folgenden Schritte aus, um Bilder aufzunehmen.
 - Bewegen Sie den Cursor auf das Anzeigefenster in der Live-Ansicht, um die Symbolleiste einzublenden, und klicken Sie auf  in der Symbolleiste.
 - Klicken Sie mit der rechten Maustaste auf das Anzeigefenster und klicken Sie im Rechtsklickmenü auf **Erfassen**.

Das aufgenommene Bild wird automatisch auf dem lokalen PC gespeichert, und ein kleines

Fenster mit der Bildvorschau und den Informationen zum Speicherpfad wird in der unteren rechten Ecke des Desktops angezeigt.

Hinweis

Der Speicherpfad für die aufgenommenen Bilder kann auf der Seite Systemkonfiguration festgelegt werden. Einzelheiten finden Sie unter **Festlegen des Dateispeicherpfads**.

5.7.4 Aufgenommene Bilder ansehen

Die in der Live-Ansicht aufgenommenen Bilder werden auf dem PC gespeichert, auf dem die Software läuft. Sie können die aufgenommenen Bilder bei Bedarf ansehen.

Bevor Sie beginnen

Nehmen Sie Bilder in der Live-Ansicht auf.

Schritte


1. Klicken Sie auf  → **Datei** → **Erfasstes Bild öffnen** in der oberen rechten Ecke, um die Seite Erfasstes Bild zu öffnen.
2. Wählen Sie aus der Liste der Kameragruppen die Kamera aus, mit der Sie die aufgenommenen Bilder suchen möchten.
3. Geben Sie die Start- und Endzeit für die Suche in der unteren linken Ecke an.
4. Klicken Sie auf **Suchen**.
Die Bilder, die zwischen der Start- und der Endzeit aufgenommen wurden, werden auf der Seite im Miniaturformat angezeigt.
5. Optional: Führen Sie die folgende(n) Operation(en) nach der Suche durch.

Bild vergrößern	Doppelklicken Sie auf die Miniaturansicht des Bildes, um es zu vergrößern und besser sehen zu können.
Bild drucken	Wählen Sie das aufgenommene Bild aus, und klicken Sie auf Drucken , um das ausgewählte Bild zu drucken.
Bild löschen	Wählen Sie das aufgenommene Bild aus, und klicken Sie auf Löschen , um das ausgewählte Bild zu löschen.
E-Mail senden	Wählen Sie das erfasste Bild aus, und klicken Sie auf E-Mail , um eine E-Mail-Benachrichtigung mit dem ausgewählten Bild als Anhang zu senden.
Bild speichern	Wählen Sie das erfasste Bild aus, und klicken Sie auf Speichern unter , um eine neue Kopie des ausgewählten Bildes zu speichern.



5.8 Sofortige Wiedergabe

Die Sofortwiedergabe zeigt einen Teil des Videos, der bemerkenswert ist oder der auf den ersten Blick unklar ist. So können Sie die Videodateien sofort auf der Hauptansichtsseite abspielen und bei Bedarf eine sofortige Überprüfung vornehmen.

Bevor Sie beginnen


Zeichnen Sie die Videodateien auf und speichern Sie sie auf den Speichergeräten, z. B. auf den SD/SDHC-Karten und Festplatten der DVRs, NVRs, Netzwerkkameras usw., oder auf den Speicherservern.


Schritte

1. Öffnen Sie die Seite Hauptansicht und starten Sie die Live-Ansicht.
2. Führen Sie einen der folgenden Vorgänge aus, um die Liste der Vorspieldauern für die sofortige Wiedergabe anzuzeigen.
 - Bewegen Sie den Cursor auf das Anzeigefenster, um die Symbolleiste einzublenden, und klicken Sie auf  .
 - Klicken Sie mit der rechten Maustaste auf das Anzeigefenster und wählen Sie im Rechtsklick-Menü die Option **Auf sofortige Wiedergabe umschalten**.
 - Bewegen Sie den Cursor auf den Knoten "Standardansicht" oder "Benutzerdefinierte Ansicht" im Bedienfeld "Ansicht" und klicken Sie auf  .Eine Liste mit Vorspieldauern von 30s, 1 min, 3 min, 5 min, 8 min und 10 min wird angezeigt.
3. Wählen Sie einen Zeitraum aus der angezeigten Liste aus, um die Sofortwiedergabe zu starten.

Beispiel

Wenn Sie 3 Minuten auswählen und die aktuelle Uhrzeit der Live-Ansicht 09:30:00 ist, beginnt die Sofortwiedergabe um 09:27:00.

Während der Sofortwiedergabe erscheint in der oberen rechten Ecke des Anzeigefensters die Anzeige  .

5. Optional: Klicken Sie erneut auf  , um die Sofortwiedergabe zu beenden und zur Live-Ansicht zurückzukehren.

5.9 Live-Ansicht für Fisheye-Kamera

Bei Fisheye-Kameras können Sie die Live-Ansicht im Fisheye-Modus starten, Voreinstellungen und Patrouillen festlegen und PTZ-Steuerung durchführen.


5.9.1 Live-Ansicht im Fischaugenmodus durchführen

Bei der Live-Ansicht von Fisheye-Kameras wird die gesamte verzerrte Weitwinkelansicht angezeigt. Es kann jedoch schwierig sein, einige Details zu erkennen. Um dieses Problem zu lösen, können Sie die Live-Videos im Fisheye-Erweiterungsmodus abspielen. Die Fisheye-Erweiterung kann Bilder in verschiedenen Modi erweitern: 180°-Panorama, 360°-Panorama, PTZ, Halbkugel, usw. So können Sie das Bild deutlich sehen.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie die Microsoft DirectX-Komponente installiert haben.

Schritte

1. Öffnen Sie die Seite Hauptansicht und starten Sie die Live-Ansicht der Fisheye-Kamera.
2. Rufen Sie den Modus Fischaugenerweiterung auf.
 - Klicken Sie mit der rechten Maustaste auf das Video und wählen Sie **Fischaugenerweiterung**.
 - Klicken Sie in der Symbolleiste auf . Weitere Informationen zum Einstellen der Symbolleiste finden Sie unter **Symbole in der Symbolleiste festlegen**.

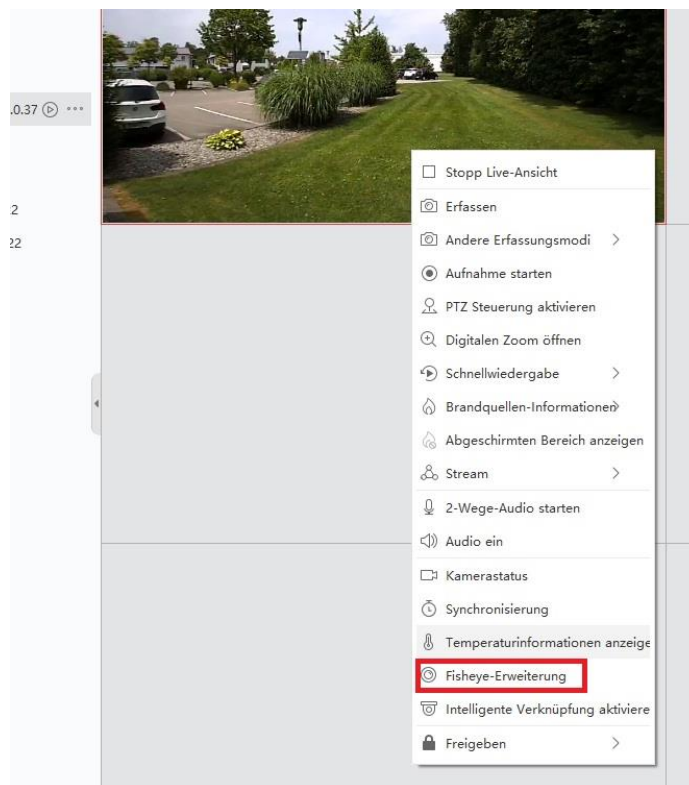





Abbildung 5-8 Live-Ansicht im Fischaugenmodus

–

 wendet sich an .

3. Klicken Sie auf  in der linken unteren Ecke des Anzeigefensters, um das Auswahlfenster für die Montageart und den Erweiterungsmodus zu öffnen.
4. Wählen Sie die Montageart der Fischaugenkamera entsprechend ihrer tatsächlichen Montageposition.
5. Wählen Sie den gewünschten Erweiterungsmodus für die Live-Ansicht.

Fisheye

Im Fisheye-Ansichtsmodus wird die gesamte Weitwinkelansicht der Kamera angezeigt. Dieser Ansichtsmodus wird Fisheye genannt, weil er der Sicht des konvexen Auges eines Fisches ähnelt. Das Objektiv erzeugt gekrümmte Bilder eines großen Bereichs, wobei die Perspektive und die Winkel der Objekte im Bild verzerrt werden.

Panorama

Im Panoramamodus wird das verzerrte Fisheye-Bild durch einige Kalibrierungsmethoden in ein normales perspektivisches Bild umgewandelt.

PTZ

Die PTZ-Ansicht ist die Nahaufnahme eines bestimmten Bereichs in der Fischaugen- oder Panorama-Ansicht und unterstützt die elektronische PTZ-Funktion, die auch als e-PTZ bezeichnet wird.



Hinweis

Jede PTZ-Ansicht ist in der Fischaugenansicht und der Panoramaansicht mit einem speziellen Navigationsfeld gekennzeichnet. Sie können das Navigationsfeld auf der Fischaugen- oder Panorama-Ansicht ziehen, um die PTZ-Ansicht anzupassen, oder die PTZ-Ansicht ziehen, um die Ansicht auf den gewünschten Winkel einzustellen.

Halbkugel

Im Halbkugelmodus können Sie das Bild ziehen und um den Durchmesser zentrieren, um die Ansicht an den gewünschten Winkel anzupassen.

AR-Halbkugel

Der AR-Halbkugelmodus überlagert Bilder in der Ferne und in der Nähe, so dass Sie ein dimensionales Bild in einem weiten Winkel betrachten können.

Zylinder

Im Zylindermodus wird das Bild zu einer Zylinderseite geformt.

6. Optional: Führen Sie die folgende(n) Operation(en) aus, nachdem Sie die Live-Ansicht im Fischaugen-Modus gestartet haben.

Erfassen Sie Klicken Sie mit der rechten Maustaste auf das Fenster und wählen Sie **Erfassen**, um das Bild in der Liveansicht zu erfassen.

Vollbild eingeben Klicken Sie mit der rechten Maustaste auf ein Wiedergabefenster und

schalten Sie das ausgewählte Fenster in den Vollbildmodus.





5.9.2 PTZ-Steuerung im Fisheye-Modus

Im Fischaugenmodus können Sie den PTZ steuern, um das PTZ-Fenster anzupassen.

 **Hinweis**



Das PTZ-Bedienfeld ist je nach Gerät unterschiedlich.



Die folgenden Funktionen sind auf dem PTZ-Bedienfeld verfügbar.

- Wählen Sie ein PTZ-Fenster aus, und klicken Sie auf die Richtungstasten, um den Blickwinkel einzustellen. Oder ziehen Sie die Bezeichnung Nr. im Fischaugen- oder Panoramafenster, um den Blickwinkel des PTZ-Fensters zu ändern.
- Wählen Sie ein PTZ-Fenster aus, klicken Sie auf  , um den automatischen Scan zu starten (die Kamera dreht sich in horizontaler Richtung), und klicken Sie erneut, um den automatischen Scan zu beenden.
- Ziehen Sie den Schieberegler auf  , um die Geschwindigkeit der PTZ-Bewegung anzupassen.
- Klicken Sie auf   , oder drehen Sie das Mausrad, um das ausgewählte PTZ-Fenster zu vergrößern oder zu verkleinern.

5.9.3 Eine Voreinstellung und eine Patrouille festlegen

PTZ unterstützt das Konfigurieren und Aufrufen einer Voreinstellung und eines Rundgangs. Rufen Sie die Seite **Hauptansicht** auf, und wählen Sie **Fischaugenerweiterung**, nachdem Sie mit der rechten Maustaste auf eine Kamera geklickt haben.

Aufgabe	Definition	Operation
Voreinstellung	Eine Voreinstellung verknüpft die Schlüsselregionen mit der Position und dem Status der mobilen PTZ. Das Überwachungspersonal kann damit schnell zu den Schlüsselregionen gelangen. Durch Senden eines Voreinstellungsbefehls zeichnet die mobile PTZ die Position und den Status von Zoom, Fokus und Blende auf. Beim Ausführen des Voreinstellungsbefehls fährt	Einstellen: Wählen Sie eine Voreinstellung aus der Voreinstellungsliste, drehen Sie die Kamera in die gewünschte Position und klicken Sie auf  . Wie Sie aufrufen können:  anklicken.

Aufgabe	Definition	Operation
	die mobile PTZ schnell zur eingestellten Position und kehrt zum eingestellten Status zurück.	
Streife	Patrouille ist eine Funktion, mit der der Benutzer eine Abtastspur mit einer Gruppe von definierten Voreinstellungen festlegen kann. Die Patrouille zwischen zwei Voreinstellungen wird mit der eingestellten Geschwindigkeit und Zeit durchgeführt.	Einstellen: Klicken Sie auf  → wählen Sie die Voreinstellungen und stellen Sie Geschwindigkeit und Zeit ein → klicken Sie auf OK .
		Wie Sie anrufen können:  anklicken.

5.11 Live-Ansicht für Wärmebildkamera

Bei der Wärmebildkamera können Sie die Informationen zur Feuerquelle und die Temperatur in der Live-Ansicht anzeigen. Sie können die Temperatur auch manuell messen, um Temperaturinformationen in der Live-Ansicht zu erhalten.

5.11.1 Anzeigen von Brandherdinformationen während der Live-Ansicht

Während der Live-Ansicht können Sie die Informationen zur erkannten Brandquelle anzeigen.

Bevor Sie beginnen

Konfigurieren Sie die Alarmregeln für das Thermogerät, Einzelheiten finden Sie im Benutzerhandbuch des Geräts.

Schritte

1. Rufen Sie die Seite Hauptansicht auf und starten Sie die Live-Ansicht einer Wärmebildkamera.

Hinweis

Informationen zum Starten der Live-Ansicht finden Sie unter **Live-Ansicht starten**.

2. Klicken Sie mit der rechten Maustaste auf das Live-View-Bild und wählen Sie im Rechtsklick-Menü die Option **Dateiquellinformationen**, um die Liste der Informationstypen anzuzeigen.

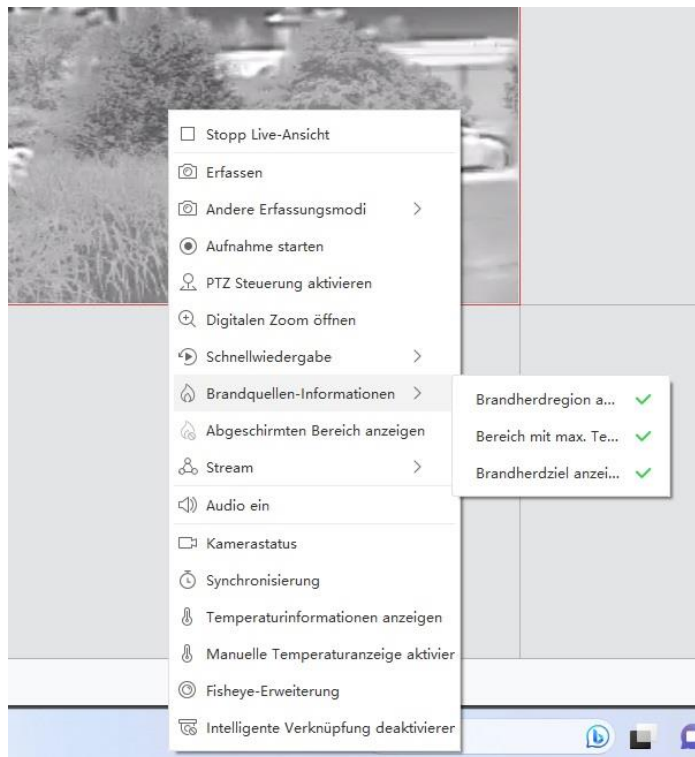


Abbildung 5-9 Ansicht der Brandherdinformationen

3. Wählen Sie eine Informationsart aus der Liste aus, um die Informationen anzuzeigen.

Anzeige der Brandherdregion

Der Bereich, in dem die Temperatur höher ist als die konfigurierte Alarmschwelle.

Suchen Sie die Max. Temperatur Region

Markieren Sie den Bereich, in dem die Temperatur in der Brandherdregion am höchsten ist. Sie ist grün markiert.

Anzeige Feuerquelle Ziel

Der Abstand zwischen dem Gerät und der Feuerquelle.

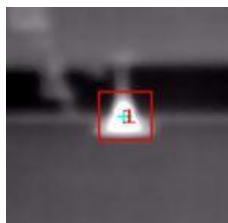


Abbildung 5-10 Informationen zur Feuerquelle in der Live-Ansicht

5.11.2 Temperaturinformationen in der Live-Ansicht anzeigen

Sie können die Echtzeit-Temperaturinformationen der Überwachungsszene beim Betrachten des Live-Videos ein- oder ausblenden.

Bevor Sie beginnen

- Schalten Sie den VCA-Quellentyp des Geräts auf **Temperaturmessung + Erkennung abnormaler Ereignisse** um.
- Aktivieren Sie die Temperaturmessfunktion des Geräts und legen Sie die Regeln für die Temperaturmessung fest; Einzelheiten hierzu finden Sie im Benutzerhandbuch des Geräts.

Führen Sie diese Aufgabe aus, wenn Sie die Temperaturdaten in der Live-Ansicht anzeigen möchten.

Schritte

1. Rufen Sie die Seite Hauptansicht auf und starten Sie die Live-Ansicht einer Wärmebildkamera.

Hinweis

Informationen zum Starten der Live-Ansicht finden Sie unter **Live-Ansicht starten**.

2. Stellen Sie die Szene auf den mit der Temperaturmessregel konfigurierten Bereich ein.
3. Klicken Sie mit der rechten Maustaste auf das Live-Bild und wählen Sie im Rechtsklick-Menü die Option **Temperaturinformationen anzeigen**.
Die Temperatur wird in der Live-Ansicht angezeigt.
4. Klicken Sie auf das Bild, um die detaillierten Temperaturinformationen anzuzeigen.

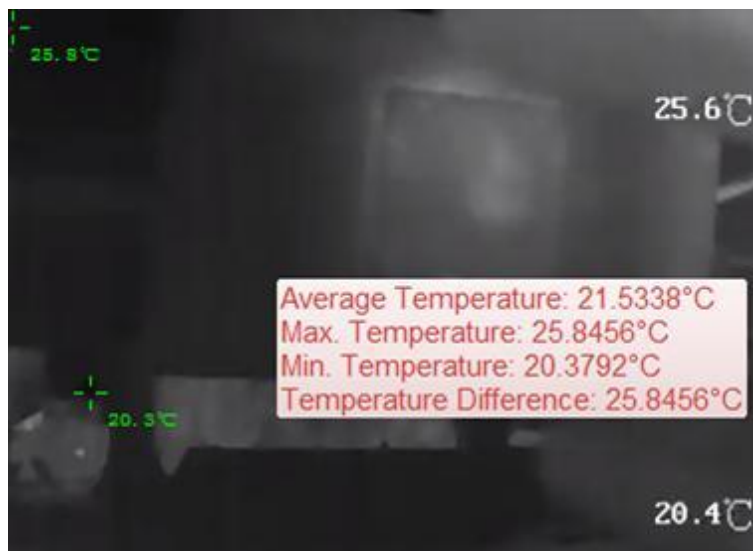


Abbildung 5-11 Temperaturinformationen in der Live-Ansicht

5. Optional: Klicken Sie mit der rechten Maustaste auf das Bild der Live-Ansicht und wählen Sie **Temperaturinformationen ausblenden**, um die Temperaturinformationen auszublenden.

5.11.3 Manuelles Messen der Temperatur

Während der Live-Ansicht der Wärmebildkamera können Sie auf eine beliebige Stelle des Live-Bildes klicken, um die Temperatur an verschiedenen Punkten anzuzeigen und so die Brandherde schnell zu lokalisieren.

Schritte

Hinweis

- Die gemessene Temperatur wird für 5 Sekunden auf dem Bild angezeigt.
 - Es kann nur die Temperatur eines Punktes angezeigt werden.
 - Wenn mehrere Clients das Live-Video einer Kamera abrufen, ist die Live-Ansicht der anderen Clients betroffen, wenn ein Client die Messpunkte hinzufügt oder löscht. Die Messpunkte werden gelöscht, wenn alle Benutzer die Live-Ansicht der Kamera beenden.
-

1. Rufen Sie die Seite Hauptansicht auf und starten Sie die Live-Ansicht einer Wärmebildkamera.
-

Hinweis

Informationen zum Starten der Live-Ansicht finden Sie unter [**Live-Ansicht starten**](#).

2. Klicken Sie mit der rechten Maustaste auf das Bild in der Live-Ansicht und wählen Sie **Temperaturinformationen anzeigen**.
3. Klicken Sie auf das Bild der Live-Ansicht, um die Temperatur dieser Position anzuzeigen. Die Temperatur der angeklickten Punkte wird auf dem Bild angezeigt.

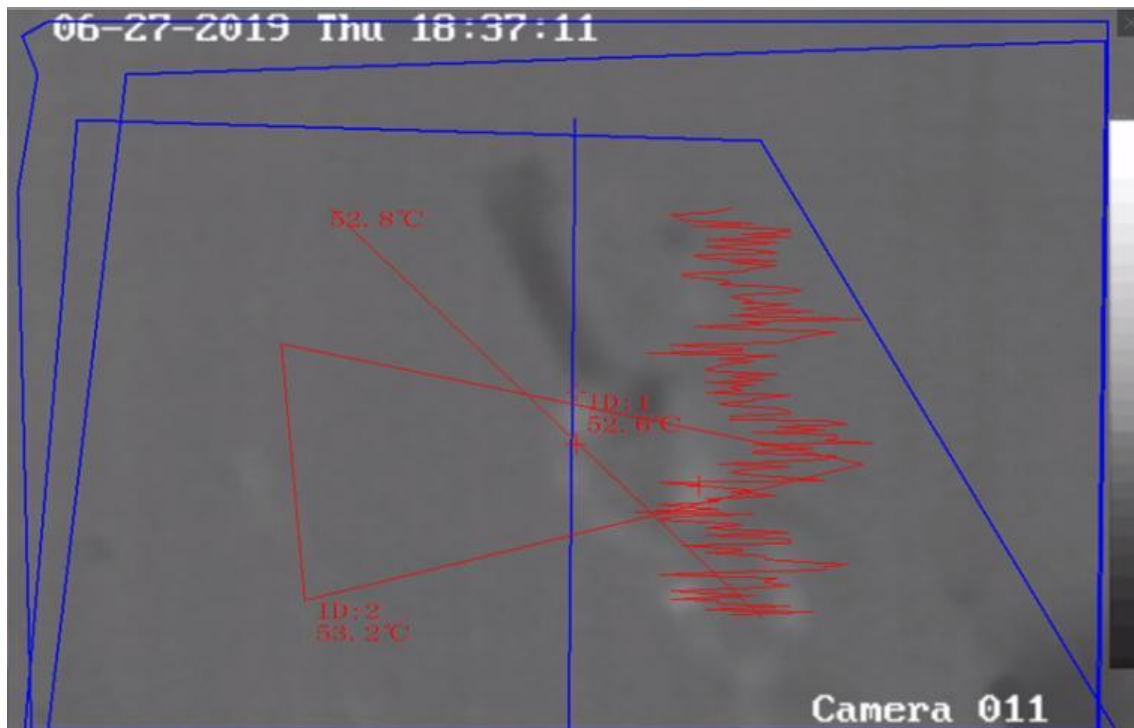


Abbildung 5-12 Manuelle Temperaturmessung an Punkten

4. Optional: Klicken Sie mit der rechten Maustaste auf das Bild der Live-Ansicht und wählen Sie im Menü die Option **Temperaturinformationen ausblenden**.

5.11.4 Anzeige des Brandherd-Erkennungsschildes

Der Brandherd-Erkennungsschutzbereich ist ein vordefinierter Bereich, der bei der Brandherd-Erkennung vor der Erkennung geschützt werden kann. Während der Live-Ansicht können Sie den Bereich auf dem Bild anzeigen.

Klicken Sie mit der rechten Maustaste auf ein Live-Ansichtsbild und wählen Sie **Abschirmbereich anzeigen**. Der Schutzbereich wird auf dem Wärmebild der Kamera angezeigt.

Hinweis

- Diese Funktion muss vom Gerät unterstützt werden.
- Vergewissern Sie sich, dass Sie die Funktion Brandherd-Erkennungsschild für das Gerät aktiviert und konfiguriert haben. Einzelheiten finden Sie im Benutzerhandbuch des Geräts.



Abbildung 5-13 Brandherd-Abschirmbereich

5.13 Weitere Funktionen

In der Live-Ansicht werden noch weitere Funktionen unterstützt, darunter die Vorschau auf dem Hilfsbildschirm, Digitalzoom, Kanal-Nullstellung, Zwei-Wege-Audio, Kamerastatus und Synchronisierung.

Hilfsbildschirm Vorschau

Zeigen Sie das Live-Video auf verschiedenen Zusatzbildschirmen an, um eine bequeme Vorschau mehrerer Überwachungsszenen zu ermöglichen.

Hinweis

Es werden bis zu 3 Hilfsbildschirme unterstützt.

Digitaler Zoom

Ziehen Sie die Maus, um einen rechteckigen Bereich in Richtung rechts unten/ links oben zu zeichnen, um den gezeichneten Bereich zu vergrößern oder zu verkleinern. Oder verwenden Sie

das Mausrad, um die Ansicht im digitalen Zoom-Modus zu vergrößern oder zu verkleinern.

Kanal-Null

Halten Sie für den Kanal Null des Geräts die Strg-Taste gedrückt und doppelklicken Sie darauf, um den entsprechenden Kanal anzuzeigen. Halten Sie die **Strg-Taste gedrückt** und doppelklicken Sie erneut, um die Anzeige wiederherzustellen.

Zwei-Wege-Audio

Die Zwei-Wege-Audiofunktion ermöglicht die Sprachübertragung der Kamera. Sie können nicht nur das Live-Video, sondern auch das Echtzeit-Audio von der Kamera erhalten. Wenn das Gerät über mehrere Zwei-Wege-Audiokanäle verfügt, können Sie einen Kanal auswählen, um Zwei-Wege-Audio zu starten.



Hinweis

- Die Zwei-Wege-Audiofunktion kann nur für eine Kamera gleichzeitig verwendet werden.
 - Die ABUS Link Station unterstützt nicht die Auswahl des Kanals bei Zwei-Wege-Audio.
-

Kamera-Status

Der Kamerastatus, wie z. B. Aufzeichnungsstatus, Signalstatus, Verbindungsnummer usw., kann erkannt und zur Überprüfung angezeigt werden. Die Statusinformationen werden alle 10 Sekunden aktualisiert.

Synchronisierung

Die Synchronisationsfunktion bietet eine Möglichkeit, die Geräteuhr mit dem PC zu synchronisieren, auf dem die Client-Software läuft.

Stream-Typ festlegen

Automatisches Ändern des Stream-Typs

Die Kamera wählt den Stream-Typ entsprechend der Größe des Anzeigefensters. Wenn die Teilungszahl des Fensters kleiner als 9 ist, wird der Stream Typ Hauptstream gewählt, ansonsten Substream.

Für die Einstellung des Streamtyps gibt es drei Möglichkeiten:

- Bewegen Sie den Mauszeiger in der Ressourcenliste über den Namen einer Kamera und klicken Sie auf **...** → **Stream**, um einen Stream-Typ auszuwählen, oder klicken Sie auf **Stream-Typ automatisch ändern**. Sie können diesen Vorgang auch für eine Gerätegruppe durchführen, um den Stream Typ für alle Geräte in dieser Gruppe festzulegen.
- Klicken Sie in der Symbolleiste der Live-Ansicht auf und wählen Sie einen Stream Typ aus. Weitere Informationen zur Bearbeitung der Symbolleiste finden Sie unter **Symbole in der Symbolleiste festlegen**.
- Klicken Sie mit der rechten Maustaste auf ein Live-Ansichtsfenster und klicken Sie auf **Stream**, um einen Stream Typ für die Kamera auszuwählen.

Hinweis

Diese Funktion muss vom Gerät unterstützt werden.

Client im Vollbildmodus sperren

Drücken Sie **Strg** und **L** auf Ihrer Tastatur, um den Client zu sperren, nachdem Sie den Vollbildmodus aktiviert haben. Nachdem Sie den Client gesperrt haben, können Sie den Client nicht mehr bedienen, auch nicht die anderen Fenster im aktuellen Fensterteilungsmodus. Klicken Sie oben auf **Entsperren**, geben Sie das Anmeldekennwort für den Client ein und klicken Sie auf **Entsperren**, um den Client zu entsperren.

Kapitel 6 Fernwiedergabe

Hinweis

Es gibt zwei Wiedergabemodi: zum einen die sofortige Wiedergabe im Hauptansichtsmodul (siehe **Sofortige Wiedergabe**), zum anderen die Suche nach Videodateien und die Wiedergabe der Videodateien im Fernwiedergabemodul. In diesem Kapitel wird nur die Wiedergabe im Fernwiedergabemodul vorgestellt.

6.2 Konfiguration des Speichers

Die Videodateien und aufgenommenen Bilder können auf den HDDs, Net HDDs oder SD/SDHC-Karten des lokalen Geräts oder auf dem angeschlossenen Speicherserver gespeichert werden.

Hinweis

Diese Funktion sollte von dem Gerät unterstützt werden.

6.2.1 Bild und Video auf DVR, NVR oder Netzwerkkamera speichern

Einige lokale Geräte, einschließlich DVRs, NVRs und Netzwerk-Kameras, bieten Speichergeräte wie HDDs, Net HDDs und SD/SDHC-Karten für Video- und Bilddateien. Sie können für die Kanäle der lokalen Geräte einen Aufzeichnungs- oder Aufnahmezeitplan festlegen.

Bevor Sie beginnen

Vergewissern Sie sich, dass die neu installierten Speichergeräte formatiert wurden. Weitere Informationen finden Sie unter **Formatieren der Festplatte des Speicherservers**.

Führen Sie diese Aufgabe aus, wenn Sie die Bild- und Videodateien auf dem Kodierungsgerät wie DVR, NVR oder Netzwerkkamera speichern müssen.

Schritte

Hinweis

Die über den Aufnahmeplan aufgenommenen Bilder werden auf dem lokalen Gerät gespeichert und können auf der Fernkonfigurationsseite des Geräts durchsucht werden.

1. Rufen Sie das Modul "Speicherplan" auf.
 2. Wählen Sie die Kamera in der Liste Kameragruppe aus.
 3. Stellen Sie den Schalter für den **Aufzeichnungszeitplan** oder den **Aufzeichnungszeitplan** im Bereich "**Storage on Encoding Device**" auf ON, um die lokale Aufzeichnung oder Erfassung am Gerät zu aktivieren.
-

4. Wählen Sie die Aufzeichnungs- oder Aufnahmeplanvorlage aus der Dropdown-Liste aus.

Ganztägige Vorlage

Ganztägige kontinuierliche Aufzeichnung.

Wochentag Vorlage

Kontinuierliche Aufzeichnung der Arbeitszeiten von 8:00 bis 20:00 Uhr.

Ereignis-Vorlage

Ganztägige ereignisgesteuerte Aufzeichnung.

Vorlage 01 bis 08

Feste Vorlagen für bestimmte Zeitpläne. Sie können die Vorlagen bei Bedarf bearbeiten.

Benutzerdefiniert

Passen Sie eine Vorlage nach Belieben an.



Hinweis

Wenn Sie die Vorlage bearbeiten oder anpassen müssen, lesen Sie den Abschnitt **Aufzeichnungszeitplanvorlage konfigurieren** oder **Aufzeichnungszeitplanvorlage konfigurieren**.

5. Klicken Sie auf **Erweitert** des Aufzeichnungsplans, um die erweiterten Aufzeichnungsparameter einzustellen.



Hinweis

Die angezeigten Elemente variieren je nach Gerät.

Voraufzeichnung

Wird normalerweise für die ereignisgesteuerte Aufzeichnung verwendet, wenn Sie aufzeichnen möchten, bevor das Ereignis eintritt.

Nachaufzeichnung

Nach Beendigung des Ereignisses kann das Video auch für eine bestimmte Zeit aufgezeichnet werden.

Videodateien aufbewahren für

Die Zeit, in der die Videodateien auf dem Speichermedium verbleiben; sobald sie überschritten wird, werden die Dateien gelöscht. Wenn der Wert auf 0 gesetzt wird, werden die Dateien dauerhaft gespeichert.

Redundante Aufzeichnung

Speichern Sie die Videodateien nicht nur auf der R/W-Festplatte, sondern auch auf der redundanten Festplatte.

Audio aufzeichnen

Nehmen Sie die Videodateien mit oder ohne Ton auf.

Video-Stream

Wählen Sie den Stream Typ für die Aufzeichnung aus.



Hinweis

Für bestimmte Gerätetypen können Sie **Dual-Stream** auswählen, um sowohl den Hauptstream als auch den Substream der Kamera aufzuzeichnen. In diesem Modus können Sie den Stream Typ während der Fernwiedergabe umschalten. Siehe **Normale Wiedergabe** für die Stream-Umschaltung während der Wiedergabe.

6. Klicken Sie auf **Erweitert** des Erfassungszeitplans, um die erweiterten Parameter für die Erfassung festzulegen.

Auflösung

Wählen Sie die Auflösung für die Serien- oder Ereignisbilder.

Bildqualität

Stellen Sie die Qualität für Serien- oder Ereignisaufnahmen ein.

Intervall

Wählen Sie das Intervall, das sich auf die Zeitspanne zwischen zwei Erfassungsaktionen bezieht.

Erfasste Bildnummer

Legen Sie die Bildnummer für die Ereignisaufnahme fest.

7. Optional: Klicken Sie auf **Kopieren nach...**, um die Einstellungen des Aufnahmeplans auf andere Kanäle zu kopieren.
8. Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

6.2.3 Bild und zusätzliche Informationen auf dem lokalen PC speichern

Sie können die Bilder und die zusätzlichen Informationen, wie z. B. die Wärmekarte, die Personenzählungsdaten und die Straßenverkehrsdaten, auf dem lokalen PC speichern.

Führen Sie diese Aufgabe aus, wenn Sie Bilder und zusätzliche Informationen auf dem lokalen PC speichern möchten.

Schritte

1. Geben Sie das Modul "**Speicherplan**" ein.
2. Wählen Sie die Kamera in der Liste Kameragruppe aus.



Hinweis

Diese Funktion sollte von dem Gerät unterstützt werden.

3. Wählen Sie den Speicherinhalt.

Bildspeicherung

Speichern Sie die Alarmbilder der Kamera, wenn ein Ereignis eintritt. Sie können auf **Systemkonfiguration** → **Datei** klicken, um den Speicherpfad der Bilder zu ändern.

Zusätzliche Informationen Lagerung

Speichern Sie die zusätzlichen Informationen (z. B. Heatmap, Personenzählungsdaten usw.) auf einem lokalen PC.

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

6.2.4 Aufzeichnungszeitplanvorlage konfigurieren

Sie können die Aufzeichnungsplanvorlage bearbeiten oder eine Aufzeichnungsplanvorlage anpassen.


Schritte

1. Rufen Sie das Modul "Speicherplan" auf.


2. Öffnen Sie das Fenster mit den Vorlageneinstellungen.

Wählen Sie **Vorlage 01** bis **Vorlage 08** aus der Dropdown-Liste und klicken Sie auf **Bearbeiten**.

Wählen Sie **Benutzerdefiniert** aus der Dropdown-Liste.

3. Ziehen Sie auf der Zeitleiste, um die Zeiträume für die ausgewählte Vorlage festzulegen, wenn der Cursor auf  wechselt.


Kontinuierlich

Normale und kontinuierliche Aufzeichnung. Die Zeitleiste ist mit  gekennzeichnet.

Ereignisaufzeichnung

Die Aufnahme wird durch ein Ereignis ausgelöst. Die Zeitleiste ist mit  gekennzeichnet.

Befehl


Die Aufzeichnung wird durch einen Befehl ausgelöst. Die Zeitleiste ist mit  gekennzeichnet.

Hinweis


Für jeden Tag können bis zu 8 Zeiträume im Aufzeichnungsplan festgelegt werden.

4. Optional: Nachdem Sie die Zeiträume festgelegt haben, können Sie eine oder mehrere der folgenden Aktionen durchführen:

Verschieben




Ziehen Sie eine Zeitspanne, um sie zu verschieben, wenn der Cursor auf  wechselt.

Verlängern oder Verkürzen

Wählen Sie eine Zeitspanne aus und verlängern oder verkürzen Sie sie, wenn der Cursor auf  wechselt.

Genaue Zeit

Klicken Sie auf einen Zeitraum, um die genaue Start- und Endzeit des

einstellen	Zeitraums festzulegen.
Löschen	Wählen Sie die konfigurierte Zeitspanne aus und klicken Sie auf  , um sie zu löschen.
Alle löschen	Klicken Sie auf  , um alle konfigurierten Zeiträume zu löschen.
Kopie an	Wählen Sie ein Datum aus und klicken Sie auf  , um die Einstellungen für den Zeitraum dieses Datums auf die anderen Daten zu übertragen.

5. Optional: Für die Vorlagen 01 bis 08 können Sie den Vorlagennamen nach Belieben bearbeiten.
6. Klicken Sie auf **OK**, um die Einstellungen zu speichern.


 **Hinweis**

Wenn Sie zum Anpassen einer Vorlage die Option **Benutzerdefiniert** wählen, können Sie auf **Als Zeitplanvorlage speichern** klicken. Die benutzerdefinierte Vorlage kann dann als Vorlage 01 bis 08 gespeichert werden.

6.2.5 Erfassungszeitplanvorlage konfigurieren

Sie können die Aufnahmeplanvorlage bearbeiten oder eine Aufnahmeplanvorlage anpassen.

Schritte

1. Rufen Sie das Modul "Speicherplan" auf.
2. Öffnen Sie das Fenster mit den Vorlageneinstellungen.
Wählen Sie **Vorlage 01** bis **Vorlage 08** aus der Dropdown-Liste und klicken Sie auf **Bearbeiten**.
Wählen Sie **Benutzerdefiniert** aus der Dropdown-Liste.
3. Ziehen Sie auf der Zeitleiste, um Zeiträume für die ausgewählte Vorlage festzulegen, wenn der Cursor auf  wechselt.



Kontinuierliche Erfassung


Normale und kontinuierliche Erfassung. Die Zeitleiste ist mit  gekennzeichnet.


Ereignis-Erfassung


Die Erfassung wird durch ein Ereignis ausgelöst. Die Zeitleiste ist mit  gekennzeichnet.

4. Optional: Nachdem Sie den Zeitraum festgelegt haben, können Sie eine oder mehrere der folgenden Aktionen durchführen

Verschieben	Wenn der Cursor auf  wechselt, können Sie den gerade bearbeiteten Zeitraum verschieben. Sie können auch den angezeigten Zeitpunkt bearbeiten, um den genauen Zeitraum festzulegen.
Verlängern oder Verkürzen	Wenn der Cursor auf  steht, können Sie den ausgewählten Zeitraum verlängern oder verkürzen.

- Löschen** Wählen Sie einen Zeitraum aus und klicken Sie auf  , um ihn zu löschen.

- Alle löschen** Klicken Sie auf  , um alle konfigurierten Zeiträume zu löschen.

- Kopie an** Wählen Sie ein Datum aus und klicken Sie auf  , um die Einstellungen für den Zeitraum dieses Datums auf die anderen Daten zu übertragen.

5. Optional: Für die Vorlagen 01 bis 08 können Sie den Vorlagennamen nach Belieben bearbeiten.
6. Klicken Sie auf **OK**, um die Einstellungen zu speichern.

 **Hinweis**

Wenn Sie zum Anpassen einer Vorlage die Option **Benutzerdefiniert** wählen, können Sie auf **Als Zeitplanvorlage speichern** klicken. Die benutzerdefinierte Vorlage kann dann als Vorlage 01 bis 08 gespeichert werden.

6.3 Symbolleiste für die Wiedergabe

Bei der Videowiedergabe auf dem Remote Playback Modul können Sie die Werkzeuge in der Symbolleiste verwenden, um verschiedene Funktionen zu implementieren.

 **Hinweis**

Die Werkzeuge in den verschiedenen Wiedergabemodi können unterschiedlich sein. In diesem Abschnitt werden die Werkzeuge im Kamerawiedergabemodul vorgestellt.

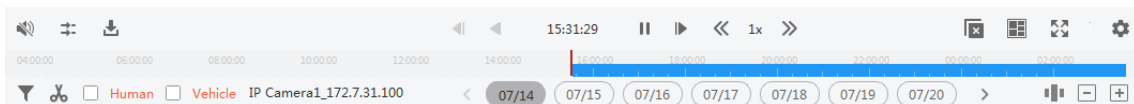




















Abbildung 6-2 Symbolleiste für die Wiedergabe

Tabelle 6-1 Symbolleiste für die Wiedergabe

Icon	Icon Name	Beschreibungen
	Rückwärts abspielen	Geben Sie die Videodatei(en) in umgekehrter Reihenfolge wieder.
	Pause/Wiedergabe	Pause/Wiedergabe der Videodatei(en).
	Alle schließen	Schließen Sie alle abgespielten Videodateien.
	Einzelbild(Rückw	Spielen Sie die Videodatei(en) bildweise in umgekehrter


Icon	Icon Name	Beschreibungen
	ärts)	Reihenfolge ab.
	Einzelbild	Spielen Sie die Videodatei(en) bildweise ab.
	Langsam Vorwärts/Schnell Vorwärts	Legen Sie die Abspielgeschwindigkeit fest, und geben Sie die Videodatei(en) je nach Geschwindigkeit langsam oder schnell wieder.
	Band	Klicken Sie auf dieses Symbol, um den Ton zu öffnen/zu schließen und die Lautstärke einzustellen.
	Clip	Legen Sie die Start- und Endzeit für das Clipping fest und laden Sie die geschnittene Videodatei auf die lokale Festplatte herunter.
	Download für mehrere Kameras	Legen Sie die Start- und Endzeit für mehrere Kameras fest und laden Sie die Videodateien mehrerer Kameras gleichzeitig herunter.
	Abteilung Fenster	Legen Sie die Fensteraufteilung fest.
	Vollbild	Wiedergabe der Videodatei(en) im Vollbildmodus. Drücken Sie ESC zum Beenden.
	Asynchrones Abspielen/Synchrones Abspielen	<p>Wechseln Sie in den asynchronen/synchronen Wiedergabemodus.</p> <hr/> <p> Hinweis</p> <p>Einzelheiten dazu finden Sie unter <u>Synchrone Wiedergabe.</u></p> <hr/>
	Einstellungen	Rufen Sie das Modul Videoparameter-Einstellungen auf und konfigurieren Sie die Parameter für Live-Ansicht und -Wiedergabe, Bild, Dateien und Symbolleiste.
	Filter	Filtern Sie die Videodateien nach dem Aufzeichnungstyp.
	Genauere Positionierung	Stellen Sie die genaue Zeit für die Wiedergabe der Videodatei(en) ein.
	Video Datum	<p>Das Datum der aktuell wiedergegebenen Videodatei(en). Sie können schnell zur Wiedergabe der Videodatei(en) an einem anderen Datum wechseln.</p> <p>Wenn Sie z. B. das Datum auf 30.07. ändern, wird das Video automatisch ab 00:00 Uhr am 30. Juli angezeigt</p>

Icon	Icon Name	Beschreibungen
		(sofern zu diesem Zeitpunkt ein Video vorhanden ist).
<input type="checkbox"/> Human <input type="checkbox"/> Vehicle	Menschen- oder fahrzeugbezogene Videos filtern	<p>Markieren Sie Mensch oder Fahrzeug, um die Videos zu filtern, in denen ein menschlicher Körper oder ein Fahrzeug erkannt wurde. Die Videos, die sich auf Menschen oder Fahrzeuge beziehen, werden in der Zeitleiste orange markiert, und Sie können das Video in der Zeitleiste schnell auffinden.</p> <hr/> <p> Hinweis</p> <p>Diese Funktion sollte von dem Gerät unterstützt werden, andernfalls ist der Mensch oder das Fahrzeug grau und kann nicht überprüft werden.</p> <hr/>

6.4 Normale Wiedergabe

Sie können Videodateien nach Kamera oder Gruppe für die normale Wiedergabe suchen und gefundene Videodateien auf den lokalen PC herunterladen. Sie können auch einen Tag hinzufügen, um wichtiges Videomaterial zu markieren, usw.

Sie können mit der rechten Maustaste auf das Wiedergabefenster klicken, um die gewünschten Funktionen aus dem Kontextmenü auszuwählen. Einige davon sind im Folgenden aufgeführt:

Name	Beschreibung
Temperaturinformationen ein-/ausblenden	<p>Temperaturinformationen ein-/ausblenden</p> <hr/> <p> Hinweis</p> <p>Das Overlay der Temperaturinformationen wird nur von der Wärmebildkamera unterstützt.</p> <hr/>
Tag Kontrolle	<p>Fügen Sie ein Standard-Tag (der Standard-Tag-Name ist TAG) oder ein benutzerdefiniertes Tag (der Tag-Name ist benutzerdefiniert) für die Videodatei hinzu, um den wichtigen Videopunkt zu markieren. Sie können das Tag auch bearbeiten oder bequem zur Tag-Position gehen.</p>
Andere Aufnahmemodi	<ul style="list-style-type: none"> ● Erfasstes Bild drucken: Nehmen Sie ein Bild auf und drucken Sie es.

Name	Beschreibung
	<ul style="list-style-type: none">● E-Mail senden: Erfassen Sie das aktuelle Bild und senden Sie dann eine E-Mail-Benachrichtigung an einen oder mehrere Empfänger. Das erfasste Bild kann angehängt werden.● Benutzerdefinierte Aufnahme: Nimmt das aktuelle Bild auf. Sie können den Namen des Bildes bearbeiten und es dann speichern.


Hinweis

- Die ABUS Link Station unterstützt nur die normale Wiedergabe und nicht die Funktionen der Rückwärtswiedergabe, des langsamen oder schnellen Vorlaufs und des Hinzufügens von Tags.
 - Bei einem NVR, der mit einem anderen Benutzernamen (außer admin) zum Client hinzugefügt wurde, müssen Sie bei aktivierter **Doppelverifizierung** den Benutzernamen und das Passwort für die Doppelverifizierung eingeben, wenn Sie Videos auf dem Client abspielen. Weitere Informationen zur doppelten Verifizierung finden Sie im Benutzerhandbuch des NVR.
-

6.4.1 Videomaterial suchen

Sie können das Videomaterial nach Datum durchsuchen, und Sie können auch ein Stichwort eingeben, um die Ergebnisse für die normale Wiedergabe zu filtern.

Schritte

1. Rufen Sie das Remote Playback Modul auf.
2. Klicken Sie links auf  , um die Seite "Kamerawiedergabe" aufzurufen.

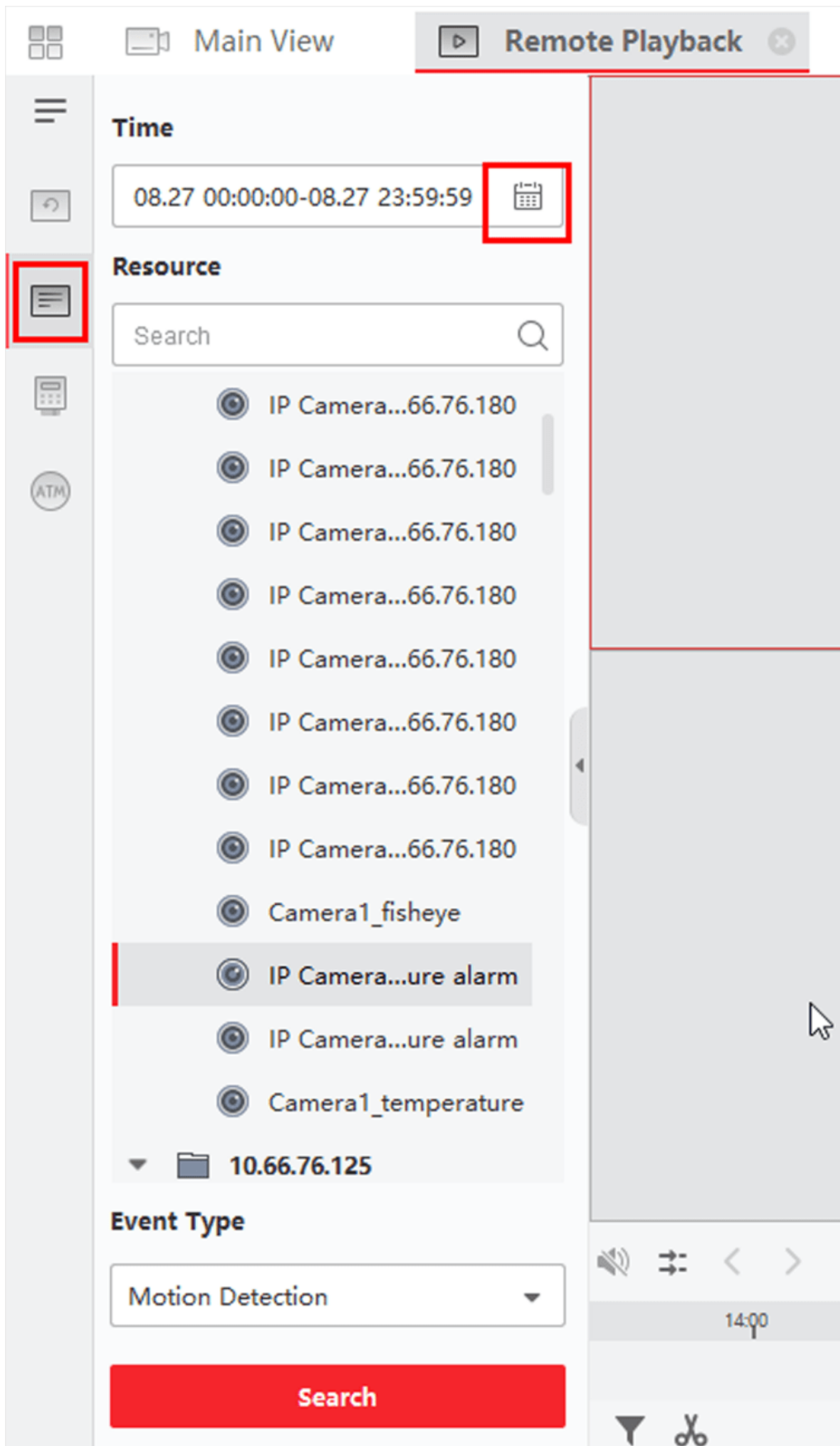





Abbildung 6-3 Videodateien suchen

3. Optional: Klicken Sie auf  , um das Startdatum und das Enddatum des Suchzeitraums festzulegen.

Hinweis

Im Kalender wird das Datum, an dem Videomaterial nach Zeitplan aufgezeichnet wurde, mit  markiert, und das Datum, an dem Videomaterial aufgrund eines Ereignisses aufgezeichnet wurde, mit  markiert.

4. Starten Sie die Wiedergabe der Kamera(s), um das Videomaterial der ausgewählten Kamera(s) zu durchsuchen. Sie können eine der folgenden Möglichkeiten nutzen, um die Wiedergabe zu starten.

Hinweis

Es können bis zu 16 Kameras gleichzeitig durchsucht werden.

- Ziehen Sie die Kamera oder Gruppe in ein Anzeigefenster.
- Wählen Sie ein Anzeigefenster aus und doppelklicken Sie auf die Kamera oder Gruppe, um die Wiedergabe im ausgewählten Fenster zu starten.
- Doppelklicken Sie nacheinander auf die Kameras, um das Anzeigefenster automatisch auszuwählen und die Wiedergabe in den Fenstern zu starten.

6.4.2 Videomaterial abspielen

Nachdem Sie das Videomaterial für die normale Wiedergabe durchsucht haben, können Sie das Video über die Zeitleiste abspielen.

Schritte

1. Rufen Sie das Remote Playback Modul auf.
2. Durchsuchen Sie das Videomaterial.
3. Video über Zeitleiste abspielen.

Sie können auf **Stream** → **Main Stream / Sub Stream** klicken, um den Stream Typ für die Wiedergabe nach Ihren Bedürfnissen zu wechseln.

Das Videomaterial wird automatisch abgespielt. Sie können auf die Zeitleiste klicken, um das gewünschte Videosegment der angegebenen Zeit für die normale Wiedergabe zu positionieren.

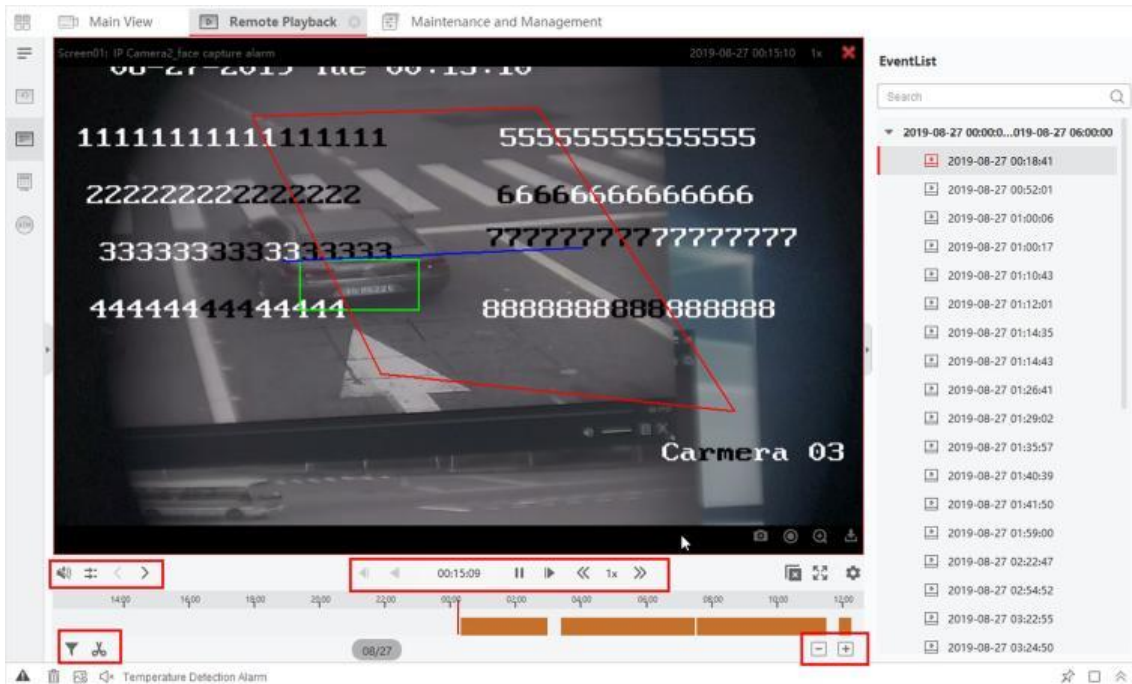


Abbildung 6-4 Videomaterial abspielen

Hinweis




- Die Zeitleiste zeigt die Zeitdauer des Videomaterials an, und die verschiedenen Arten von Videomaterial sind farblich gekennzeichnet. Während der Wiedergabe können Sie die Informationen zu Bitrate, Bildrate und Auflösung auf dem Bild anzeigen.
- Sie können das Mausrad benutzen oder auf klicken, um die Zeitleiste zu vergrößern oder zu verkleinern.

4. Optional: Führen Sie die folgenden Operationen in der Symbolleiste aus, um die Wiedergabe zu steuern.

- | | |
|-------------------------------------|---|
| Einzelbild (rückwärts) | Klicken Sie auf oder rollen Sie mit dem Mausrad nach unten, um das Videomaterial Bild für Bild (in umgekehrter Reihenfolge) abzuspielen. |
| Audio-Steuerung | Klicken Sie auf oder , um den Ton ein-/auszuschalten. Sie können auch die Lautstärke beim Einschalten einstellen. |
| Download für mehrere Kameras | Klicken Sie auf , um Videomaterial von mehreren Kameras gleichzeitig herunterzuladen. |

Hinweis

Weitere Einzelheiten finden Sie unter [Download für mehrere Kameras.](#)

Videodateien nach Datum herunterladen	Klicken Sie auf  , um das Videomaterial der Kamera nach Datum und Uhrzeit herunterzuladen und auf dem lokalen PC zu speichern. Der Fortschritt des Herunterladens wird in der rechten oberen Ecke der Seite angezeigt, und Sie können das Herunterladen manuell unterbrechen.
Genauere Positionierung	Klicken Sie auf  , um den genauen Zeitpunkt für die Wiedergabe der Videodatei festzulegen.
Zum Bild eines Thumbnails springen	Klicken Sie auf  in der unteren rechten Ecke, um die Miniaturfunktion zu aktivieren, und setzen Sie den Cursor auf die Zeitleiste, um die Miniatur des Punktes anzuzeigen. Klicken Sie auf die Miniaturansicht, um zum Bild des Punktes zu springen.

 **Hinweis**

Diese Funktion muss von den Geräten unterstützt werden.

6.5 Wiedergabe von Alarmeingängen

Wenn der Alarmeingang ausgelöst wird, kann das verknüpfte Video nach der Wiedergabe des Alarmeingangs durchsucht werden. Diese Funktion erfordert die Unterstützung durch das angeschlossene Gerät.

Eine Beschreibung der Symbolleiste für die Wiedergabe des Alarmeingangs und des Rechtsklick-Menüs im Anzeigefenster finden Sie unter **Normale Wiedergabe**.


 **Hinweis**

Einige Symbole sind bei der Wiedergabe von Alarmeingängen möglicherweise nicht verfügbar.

6.5.1 Videomaterial suchen

Sie können das Videomaterial nach Datum durchsuchen, und Sie können auch ein Schlüsselwort eingeben, um die Ergebnisse für die Wiedergabe des Alarmeingangs zu filtern.

Schritte

1. Rufen Sie das Remote Playback Modul auf.
2. Klicken Sie links auf  , um die Seite für die Ereigniswiedergabe aufzurufen.

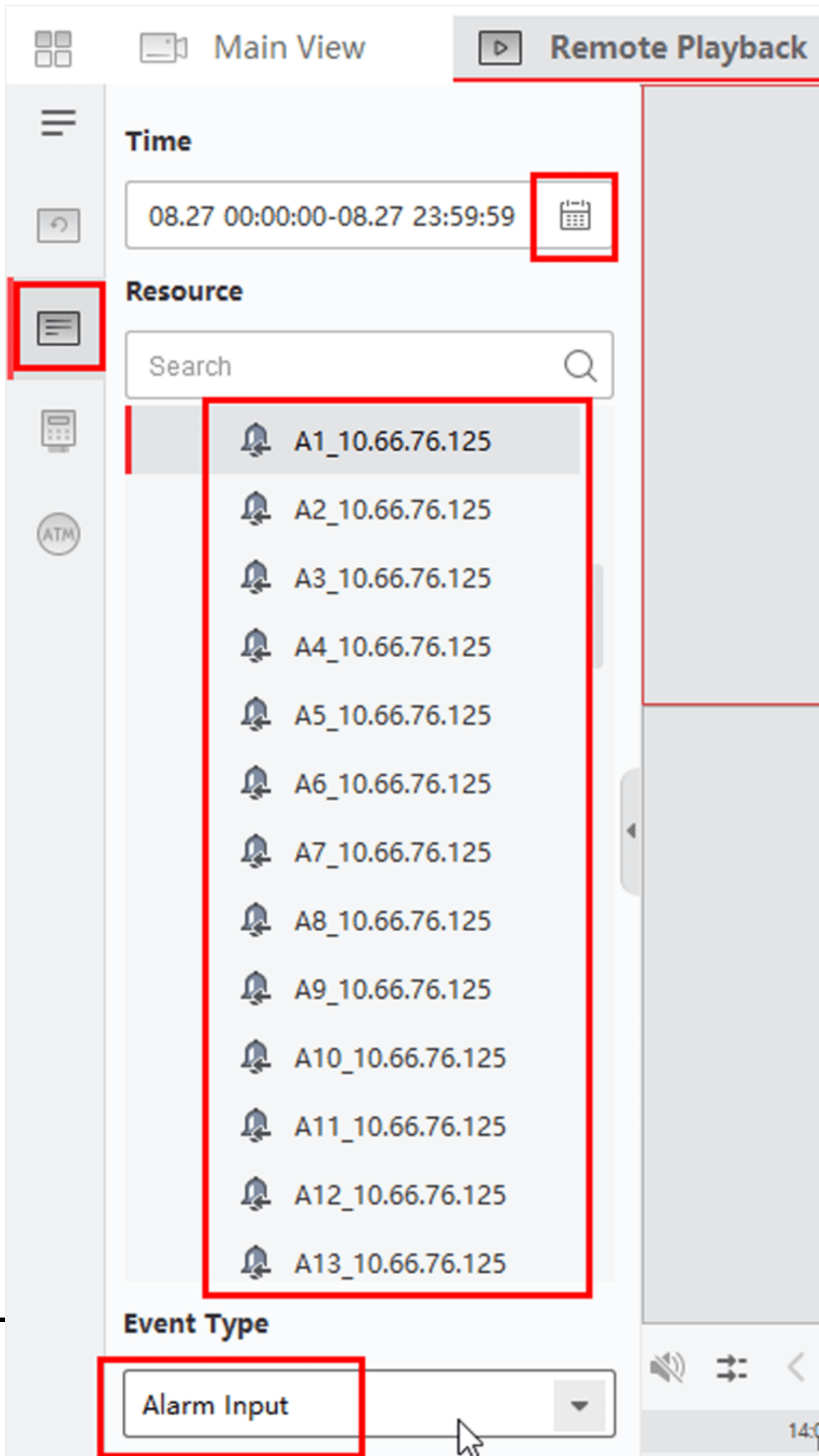




Abbildung 6-5 Videodateien suchen

3. Wählen Sie einen Alarmeingangskanal auf der linken Seite.
4. Optional: Klicken Sie auf  , um das Startdatum und das Enddatum des Suchzeitraums festzulegen.
5. Wählen Sie als Ereignistyp "**Alarmeingang**" aus der Dropdown-Liste aus.
6. Klicken Sie auf **Suchen**, um die Suche zu starten.
Das passende Videomaterial des ausgewählten Alarmeingangs wird auf der rechten Seite in chronologischer Reihenfolge angezeigt. Standardmäßig wird das erste Video automatisch abgespielt.
7. Wahlweise: Geben Sie ein Stichwort in das Suchfeld ein, um die Ergebnisse zu filtern.

6.5.2 Videomaterial abspielen

Nach dem Durchsuchen des Videomaterials für die Wiedergabe des Alarmeingangs können Sie das Video über die Dateiliste oder die Zeitleiste wiedergeben.

Schritte


1. Rufen Sie das Remote Playback Modul auf.
2. Klicken Sie links auf  , um die Seite für die Ereigniswiedergabe aufzurufen.
3. Durchsuchen Sie das Videomaterial des Alarmeingangs.

Hinweis

Weitere Informationen zum Durchsuchen von Videomaterial des Alarmeingangs finden Sie unter ***Suchen von Videomaterial***.

4. Video über Dateiliste oder Zeitleiste abspielen.
 - Doppelklicken Sie auf das Videomaterial, um das Video im Wiedergabefenster abzuspielen.
 - Klicken Sie auf die Zeitleiste, um das gewünschte Videosegment der angegebenen Zeit für die Wiedergabe des Alarmeingangs zu positionieren.

Hinweis

- Die Zeitleiste zeigt die Dauer des Videomaterials an, und die verschiedenen Arten von Videomaterial sind farblich gekennzeichnet.
 - Sie können das Mausrad benutzen oder auf  klicken, um die Zeitleiste zu vergrößern oder zu verkleinern.
-

6.6 Wiedergabe von Ereignissen

Die aufgezeichneten Videodateien, die durch ein Ereignis ausgelöst wurden, wie z. B. Bewegungserkennung, VCA-Erkennung oder Erkennung eines abnormalen Ereignisses, können für die Ereigniswiedergabe durchsucht werden. Diese Funktion erfordert die Unterstützung durch das angeschlossene Gerät.

Eine Beschreibung der Symbolleiste für die Ereigniswiedergabe und des Rechtsklick-Menüs des Anzeigefensters finden Sie unter "**Normale Wiedergabe**".



Hinweis

Einige Symbole sind möglicherweise für die Wiedergabe von Ereignissen nicht verfügbar.



6.6.1 Suche nach Videomaterial/Bildern

Sie können Videos/Bilder von Veranstaltungen nach Datum und Art der Veranstaltung suchen.

Schritte

1. Rufen Sie das Remote Playback Modul auf.
2. Klicken Sie links auf  , um die Seite für die Ereigniswiedergabe aufzurufen.
3. Klicken Sie auf  , um das Startdatum und das Enddatum der Suche festzulegen.

Hinweis

Im Kalender wird das Datum, an dem Videomaterial nach Zeitplan aufgezeichnet wurde, mit  markiert, und das Datum, an dem Videomaterial aufgrund eines Ereignisses aufgezeichnet wurde, mit  markiert.

4. Wählen Sie **Video** oder **Bild** als den zu suchenden Inhalt.
5. Wählen Sie eine Kamera aus der Ressourcenliste aus.
6. Wählen Sie einen Ereignistyp aus der Dropdown-Liste **Ereignistyp** aus.
7. Klicken Sie auf **Suchen**.
 - Wenn Sie **Video** als gesuchten Inhalt auswählen, wird das gefundene Videomaterial auf der rechten Seite in chronologischer Reihenfolge angezeigt. Und standardmäßig wird die erste Videodatei automatisch abgespielt.
 - Wenn Sie "**Bild**" als gesuchten Inhalt auswählen, werden die passenden Bilder automatisch auf der rechten Seite angezeigt.
 -


6.6.2 Videomaterial/Bild anzeigen

Wenn die Kamera Ereignisse erkennt (z. B. Linienüberquerung, Bewegungserkennung und Erkennung ungewöhnlicher Ereignisse) oder die Außenstation ein Videogespräch führt, löst sie die Videoaufzeichnung oder Bildaufnahme der verknüpften Kamera aus. Sie können das Videomaterial oder die Bilder durchsuchen und die Videos über die Dateiliste oder die Zeitleiste abspielen und die Bilder der Reihe nach ansehen.



Schritte

Hinweis





Für die Außenstation unterstützt nur die DS-KV8123-M die folgenden Funktionen.

1. Rufen Sie das Remote Playback Modul auf.
 2. Klicken Sie links auf , um die Seite für die Ereigniswiedergabe aufzurufen.
 3. Durchsuchen Sie das aufgezeichnete Videomaterial oder die Bilder nach einem bestimmten Ereignis.
 4. Videomaterial oder Bilder ansehen.
 - Doppelklicken Sie auf das Videomaterial, um das Video im Wiedergabefenster abzuspielen.
 - Die gesuchten Bilder werden automatisch wiedergegeben.
-

Hinweis



- Die Zeitleiste zeigt die Dauer der Videodateien an, und die Videodateien verschiedener Typen sind farblich gekennzeichnet.
 - Sie können das Mausrad verwenden oder auf   klicken, um die Zeitleiste zu vergrößern oder zu verkleinern.
-

5. Optional: Führen Sie bei Bedarf die folgenden Vorgänge durch.


Filmmaterial aus einer bestimmten Zeit abspielen	Klicken Sie auf die Zeitleiste, um ein Videosegment der angegebenen Zeit für die Ereigniswiedergabe anzuzeigen.
Filmmaterial mit Mensch und/oder Fahrzeug anzeigen	Markieren Sie unter der Zeitleiste die Option Mensch und/oder Fahrzeug , um Material anzuzeigen, das Menschen oder Fahrzeuge enthält.
Bilder wechseln	Klicken Sie auf  oder  , um zum vorherigen oder nächsten Bild zu gelangen.
Intervall für die Bildanzeige einstellen	Klicken Sie auf  , um das Intervall der Bildanzeige einzustellen.
Bilder im	Klicken Sie auf  , um Bilder im Vollbildmodus anzuzeigen.

Vollbildmodus anzeigen


Bilder im Listenmodus anzeigen

Klicken Sie auf  , um Bilder im Listenmodus anzuzeigen.
Klicken Sie auf  , um in den Miniaturbildmodus zu wechseln.

Bilder herunterladen

Klicken Sie auf  , prüfen Sie die Bilder und klicken Sie auf **Herunterladen**, um die ausgewählten Bilder auf Ihren PC herunterzuladen.

Videos herunterladen

Klicken Sie auf  , wählen Sie mehrere Videodateien aus und klicken Sie auf **Download**, um die Videodateien auf Ihren PC herunterzuladen.

6.9 VCA-Wiedergabe

Für die durchsuchten Videodateien können Sie eine VCA-Regel festlegen, um das Videomaterial zu finden, bei dem ein VCA-Ereignis auftritt, wie z. B. Bewegungserkennung, Erkennung von Linienüberquerungen und Einbruchserkennung. Diese Funktion hilft bei der Suche nach dem Video, das Sie mehr beunruhigen könnte, und markiert es mit roter Farbe.

Bevor Sie beginnen

Stellen Sie sicher, dass das Gerät mit VCA-Funktion installiert ist.

Schritte

 **Hinweis**

Die VCA-Wiedergabe wird nur in einem einzigen Fenster unterstützt, synchrone und asynchrone Wiedergabe werden nicht unterstützt.



1. Rufen Sie das Remote Playback Modul auf.
2. Klicken Sie links auf  , um die Seite "Kamerawiedergabe" aufzurufen.
3. Wählen Sie die Kamera aus und starten Sie die Videowiedergabe der Kamera.



Abbildung 6-9 VCA-Wiedergabe

4. Rufen Sie das Menü VCA-Suche auf.
 - Klicken Sie mit der rechten Maustaste auf das Wiedergabefenster, um das Kontextmenü aufzurufen, und klicken Sie dann auf **VCA-Suche**.
 - Klicken Sie auf  in der unteren rechten Ecke des Wiedergabefensters.
5. Aktivieren Sie den VCA-Typ, zeichnen Sie den Erfassungsbereich und stellen Sie die Empfindlichkeit ein.

Bewegungserkennung

Wenn sich die Sicht auf das Video ändert (z. B. wenn eine Person vorbeigeht oder das Objektiv bewegt wird), wird das Videomaterial in der Zeitleiste rot markiert, was für die automatische Alarmszene oder die Nicht-Wach-Szene verwendet wird.

Erkennung von Linienkreuzungen

Sie können eine virtuelle Linie auf dem Video zeichnen, und das Videomaterial wird als rote Farbe auf der Zeitleiste markiert, wenn der Client bidirektional Personen, Fahrzeuge und andere bewegliche Objekte erkennt, die die virtuelle Linie überqueren.

Intrusion Detection


Sie können einen virtuellen Bereich auf dem Video einzeichnen, und das Videomaterial wird auf der Zeitleiste rot markiert, wenn Personen, Fahrzeuge oder andere bewegliche Objekte in den vordefinierten Bereich eindringen.

VCA-Einstellungen

Legen Sie die Empfindlichkeit fest und filtern Sie die gesuchten Videodateien, indem Sie die Zielzeichen einstellen. Das Videomaterial wird in der Zeitleiste rot markiert, wenn eine Person (deren Attribute mit den eingestellten Attributen übereinstimmen) im Video vorkommt.

Hinweis

Je höher die Empfindlichkeit, desto genauer ist der Abgleich der Person.

6. Optional: Klicken Sie auf  , um das Startdatum und das Enddatum des Suchzeitraums festzulegen.

7. Starten Sie die VCA-Wiedergabe.

Die im definierten Bereich aufgetretenen VCA-Ereignisse werden in der Zeitleiste rot markiert.

Hinweis

- Standardmäßig ist die Wiedergabegeschwindigkeit des betroffenen Videos 1X und die Wiedergabegeschwindigkeit des nicht betroffenen Videos 8X.
 - Sie können in der Systemkonfiguration festlegen, dass das nicht betroffene Video während der VCA-Wiedergabe übersprungen werden soll, und das nicht betroffene Video wird während der VCA-Wiedergabe nicht wiedergegeben. Weitere Informationen finden Sie unter **Einstellen von Live-Ansicht und Wiedergabeparametern**.
 - Wenn Sie die VCA-Wiedergabe deaktivieren müssen, klicken Sie mit der rechten Maustaste auf das VCA-Wiedergabefenster und dann auf **VCA-Suche**, um die VCA-Wiedergabe zu deaktivieren.
-

6.10 Synchrone Wiedergabe

Standardmäßig spielt der Client die Videodateien mehrerer Kameras im asynchronen Wiedergabemodus ab: Die Wiedergabezeit der verschiedenen Videodateien kann unterschiedlich sein. Bei der synchronen Wiedergabe können die Videodateien synchronisiert wiedergegeben werden.


Schritte

Hinweis

- Videodateien von bis zu 16 Kameras können gleichzeitig wiedergegeben werden.
 - Synchrone und asynchrone Wiedergabe werden im ATM-Video-Wiedergabemodus und im VCA-Wiedergabemodus nicht unterstützt.
 - Die Videowiedergabe von Ereignissen und die POS-Videowiedergabe unterstützen nur die synchrone Wiedergabe. Um mehrere Kameras zu verknüpfen, rufen Sie **Wartung und Verwaltung** → **Ereignisverwaltung** auf und aktivieren die verknüpfte Kamera je nach Ereignistyp.
-

1. Rufen Sie das Remote Playback Modul auf.

2. Starten Sie die Wiedergabe von mindestens zwei Kameras.

3. Klicken Sie in der Symbolleiste auf  , um die synchrone Wiedergabe zu aktivieren.

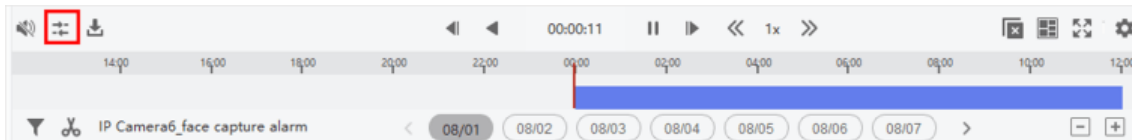


Abbildung 6-10 Synchroner Wiedergabe deaktivieren

Die Kamera, die sich in der Wiedergabe befindet, startet die synchrone Wiedergabe.

4. Klicken Sie auf  , um die synchrone Wiedergabe zu deaktivieren.

6.11 Videowiedergabe der Fisheye-Kamera

Bei der Wiedergabe des Videos der Fisheye-Kamera kann es zu Verzerrungen in der Ansicht kommen. Um die Details besser beobachten zu können, können Sie die Fischaugen-Erweiterungsfunktion aktivieren, um die Ansicht als unverzerrte Ansicht zu korrigieren. Der Client unterstützt mehrere Fisheye-Erweiterungsmodi, z. B. Panorama, Halbkugel, PTZ, Fisheye+PTZ-Modus.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie die Microsoft DirectX-Komponente installiert haben.

Schritte


Hinweis

Weitere Anweisungen zur Wiedergabesteuerung finden Sie unter **"Normale Wiedergabe"**. Einige Symbole sind bei der Fischaugen-Wiedergabe möglicherweise nicht verfügbar.

1. Rufen Sie das Remote Playback Modul auf.
2. Wählen Sie eine Fisheye-Kamera aus, um die Wiedergabe zu starten.



Hinweis

Ausführliche Informationen zur Konfiguration der Wiedergabe und der Wiedergabesteuerung finden Sie unter **Normale Wiedergabe**.

3. Rufen Sie den Modus Fischaugenerweiterung auf.
 - Klicken Sie mit der rechten Maustaste auf das Anzeigefenster und wählen Sie **Fisheye Expansion**.
 - Klicken Sie in der Symbolleiste auf  . Weitere Informationen zum Einstellen der Symbolleiste finden Sie unter **Symbole in der Symbolleiste festlegen**.

Hinweis

Die Montageart bei der Wiedergabe der Fischaugenerweiterung wird entsprechend der Montageart in der Live-Ansicht eingestellt. Einzelheiten finden Sie unter **Live-Ansicht im Fischaugen-Modus durchführen**

 wendet sich an  .

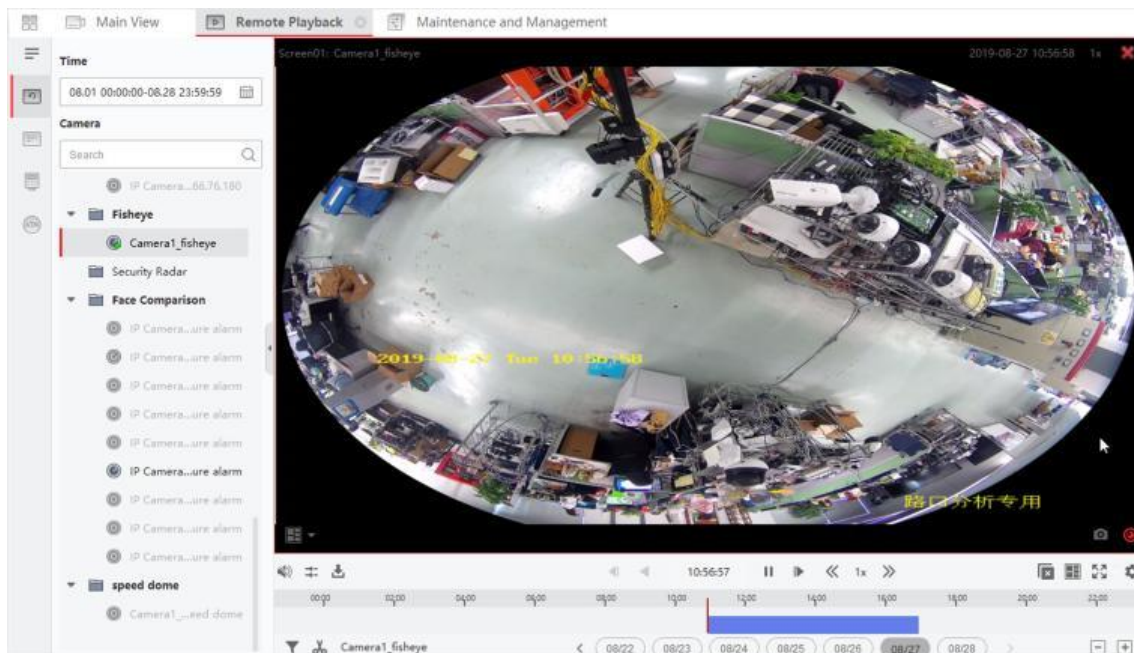



Abbildung 6-11 Videowiedergabe der Fisheye-Kamera

4. Klicken Sie auf  in der unteren linken Ecke des Anzeigebereichs, um den gewünschten Erweiterungsmodus für die Wiedergabe auszuwählen.

Fisheye

Im Fisheye-Ansichtsmodus wird die gesamte Weitwinkelansicht der Kamera angezeigt. Dieser Ansichtsmodus wird **Fisheye** genannt, weil er der Sicht des konvexen Auges eines Fisches ähnelt. Das Objektiv erzeugt gekrümmte Bilder eines großen Bereichs, wobei die Perspektive und die Winkel der Objekte im Bild verzerrt werden.

Panorama / Doppel-180° Panorama / 360° Panorama

Im Panoramamodus wird das verzerrte Fisheye-Bild durch einige Kalibrierungsmethoden in ein normales perspektivisches Bild umgewandelt.

PTZ

Die PTZ-Ansicht ist die Nahaufnahme eines bestimmten Bereichs in der Fischaugen- oder Panorama-Ansicht und unterstützt die elektronische PTZ-Funktion, die auch als e-PTZ bezeichnet wird.

Hinweis

Jede PTZ-Ansicht ist in der Fischaugenansicht und der Panoramaansicht mit einem speziellen Navigationsfeld gekennzeichnet. Sie können das Navigationsfeld auf der Fischaugen- oder Panorama-Ansicht ziehen, um die PTZ-Ansicht anzupassen, oder die PTZ-Ansicht ziehen, um die Ansicht auf den gewünschten Winkel einzustellen.

Halbkugel

Im Halbkugelmodus können Sie das Bild ziehen und um den Durchmesser zentrieren, um die Ansicht an den gewünschten Winkel anzupassen.

AR-Halbkugel

Der AR-Halbkugelmodus überlagert Bilder in der Ferne und in der Nähe, so dass Sie ein dimensionales Bild in einem weiten Winkel betrachten können.

Zylinder

Im Zylindermodus wird das Bild zu einer Zylinderseite geformt, und Sie können das Bild flexibel in jede Richtung ziehen, um den gesamten Erfassungsbereich zu sehen.

5. Optional: Klicken Sie mit der rechten Maustaste auf ein Wiedergabefenster in der Fischaugenansicht, um das ausgewählte Fenster in den Vollbildmodus zu schalten.

Hinweis

Sie können mit der rechten Maustaste auf das Fenster klicken und "**Vollbildmodus beenden**" wählen, um den Vollbildmodus zu beenden.

6.13 Videomaterial herunterladen

Während der Wiedergabe können Sie die Videodateien einer Kamera oder mehrerer Kameras auf den lokalen PC herunterladen.

6.13.1 Videomaterial nach Datum herunterladen

Während der Wiedergabe können Sie das Videomaterial der Kamera herunterladen und auf dem lokalen PC speichern.

Schritte

1. Rufen Sie die Seite "Fernwiedergabe" auf und wählen Sie eine Kamera aus, um die Wiedergabe zu starten.

Hinweis

Einzelheiten zum Starten der Wiedergabe finden Sie unter [Fernwiedergabe](#).

2. Klicken Sie mit der rechten Maustaste auf das Bild und dann auf **Herunterladen**.

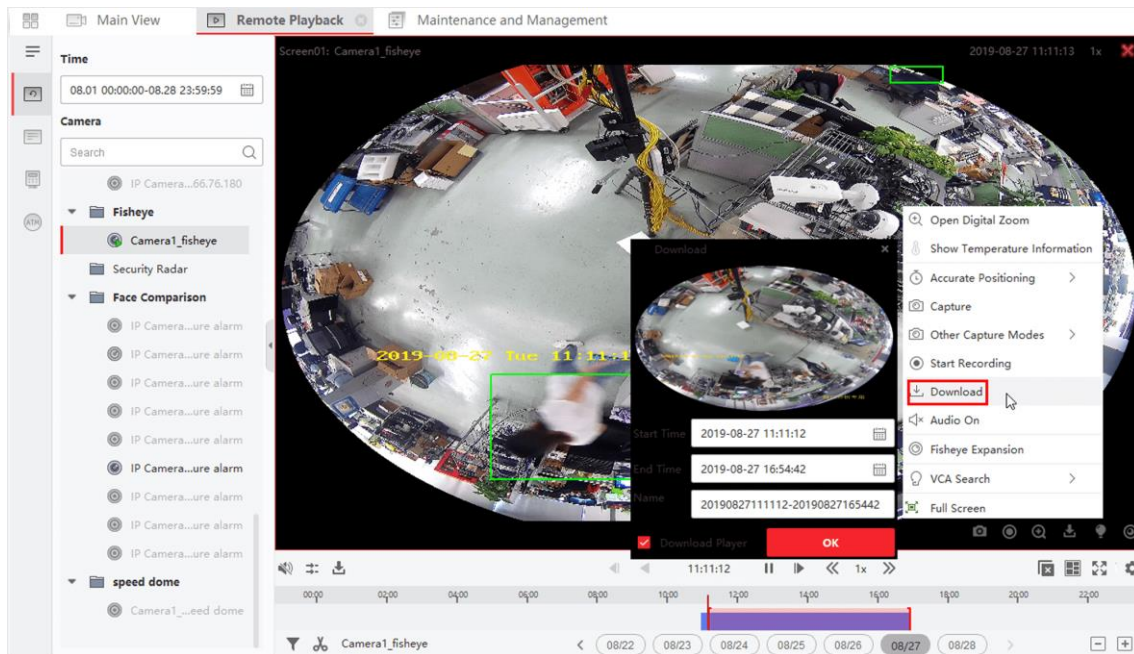


Abbildung 6-12 Herunterladen von Videomaterial nach Datum

3. Legen Sie die Start- und Endzeit des herunterzuladenden Videomaterials fest.
4. Geben Sie einen Namen für das Videomaterial ein.
5. Klicken Sie auf **OK**, um das Herunterladen des Videomaterials auf den lokalen PC zu starten.

6.13.2 Download für mehrere Kameras

Während der Wiedergabe von mehreren Kameras können Sie die Videodateien mehrerer Kameras gleichzeitig nach Datum herunterladen.

Schritte

1. Rufen Sie die Seite "Fernwiedergabe" auf und wählen Sie mehrere Kameras aus, um die Wiedergabe zu starten.

Hinweis

Einzelheiten zum Starten der Wiedergabe finden Sie unter **Fernwiedergabe**.

2. Klicken Sie auf  , um das Fenster Download für mehrere Kameras zu öffnen.

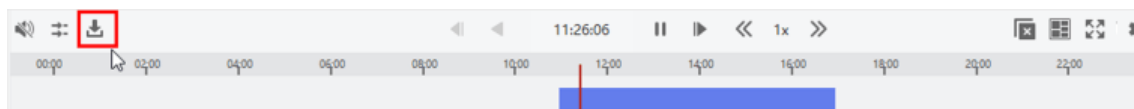


Abbildung 6-13 Symbolleiste

3. Wählen Sie die Kameras aus, für die Sie Videodateien herunterladen möchten.
4. Stellen Sie die Start- und Endzeit der Videodauer für jede Kamera ein.

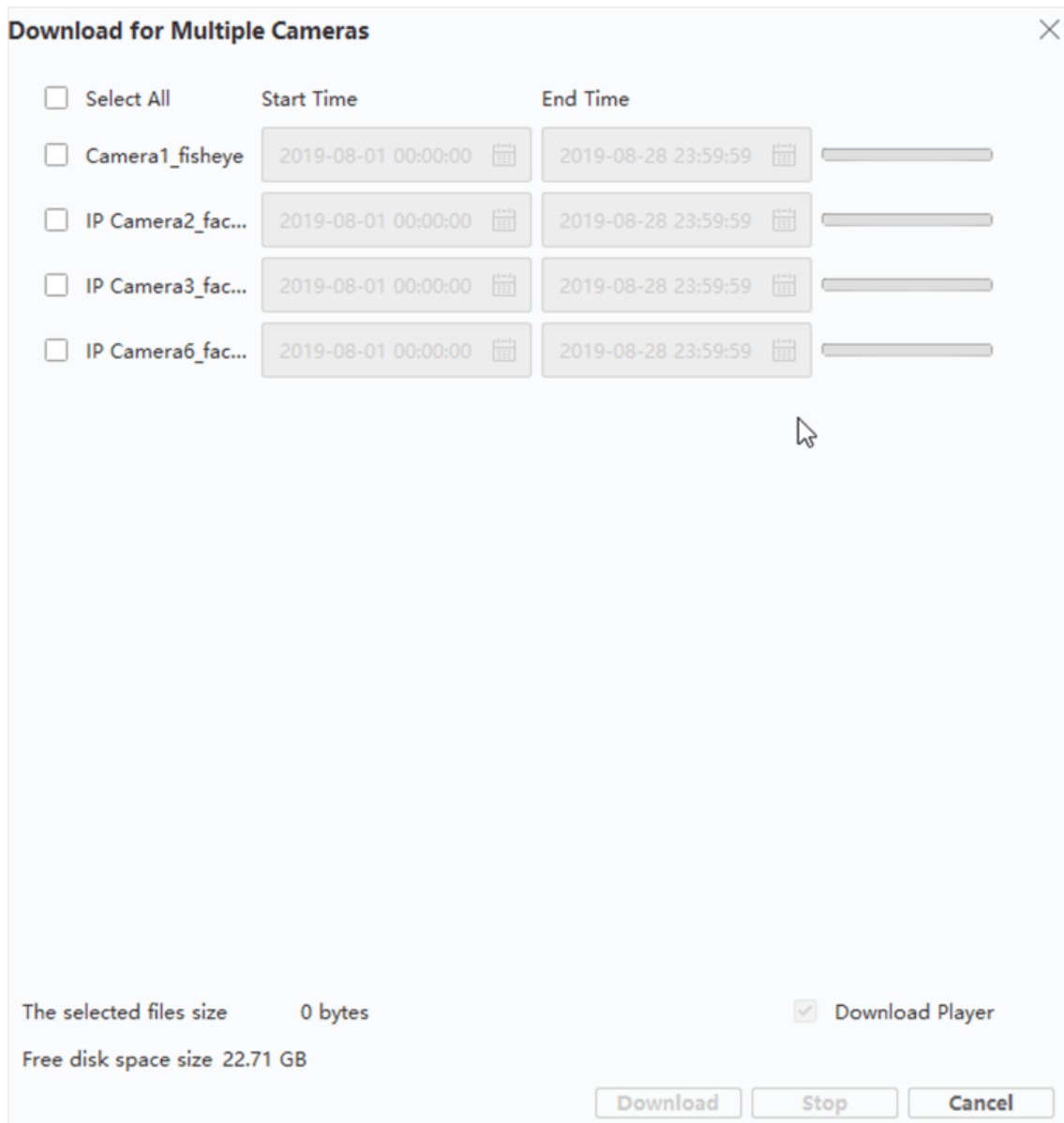


Abbildung 6-14 Kameras auswählen

5. Optional: Markieren Sie **Player herunterladen**, um den Player herunterzuladen.
6. Klicken Sie auf **Herunterladen**, um das Herunterladen der Videodateien der konfigurierten Dauer(n) auf den lokalen PC zu starten.
Der Fortschrittsbalken zeigt das Herunterladen der Videodateien der einzelnen Kameras an.
7. Optional: Klicken Sie auf **Stopp**, um das Herunterladen manuell zu beenden.

 **Hinweis**

Die Videodateien von bis zu 16 Kameras können gleichzeitig heruntergeladen werden.

Kapitel 7 Ereigniskonfiguration

Das Ereignis wird verwendet, um das Sicherheitspersonal über eine bestimmte Situation zu benachrichtigen, was dazu beiträgt, die Situation sofort zu bewältigen. Ein Ereignis kann eine Reihe von Verknüpfungsaktionen (z. B. akustische Warnung und E-Mail-Versand) zur Benachrichtigung und Ereignisbehandlung auslösen. Sie können das Ereignis aktivieren und Verknüpfungsaktionen für die zum Client hinzugefügten Ressourcen festlegen. Wenn die ausgewählten Ereignisse eintreten, erhält der Client Ereignisbenachrichtigungen in Echtzeit und Sie können die Details überprüfen und die Ereignisse entsprechend behandeln.

Video-Veranstaltung

Die Videoereignisse beziehen sich auf spezielle Ereignisse, die durch eine Videoausnahme, eine Ausnahme des Überwachungsbereichs, einen Alarmeingang, eine Ausnahme des Codiergeräts usw. ausgelöst werden. Weitere Einzelheiten finden Sie unter [Ereignis für Kamera konfigurieren](#), [Ereignis für Alarmeingang konfigurieren](#) und [Ereignis für Kodiergerät konfigurieren](#).

Ereignis der Zugangskontrolle

Die Zutrittskontrollereignisse beziehen sich auf die speziellen Ereignisse, die an den Zutrittskontrollgeräten, Türen, Kartenlesern, Aufzügen, Video-Gegensprechanlagen usw. ausgelöst werden. Weitere Einzelheiten finden Sie unter [Konfigurieren von Client-Aktionen für Zutrittsereignisse](#) und [Konfigurieren von Ereignissen der Videosprechanlage](#).

7.1 Ereignis für Kamera konfigurieren

Das Ereignis für die Kamera bezieht sich auf die Videoausnahme oder die Ereignisse, die im Überwachungsbereich der Kamera erkannt werden, wie z. B. Bewegungserkennung, Videoverlust, Leitungsüberschreitung usw. Sie können ein Ereignis für die Kameras im Client aktivieren. Wenn das Ereignis auf der Kamera ausgelöst wird, kann der Client das Ereignis zur Überprüfung empfangen und aufzeichnen und eine Reihe von Verknüpfungsaktionen (z. B. das Senden einer E-Mail) zur Benachrichtigung auslösen.

Schritte

1. Klicken Sie auf **Ereigniskonfiguration** → **Videoereignis** → **Kamera**.

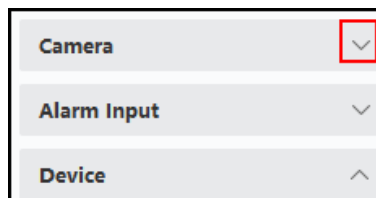


Abbildung 7-1 Anzeige der Kamera-Ressource

2. Klappen Sie die Gruppe auf und wählen Sie eine Kamera als Ereignisquelle aus.

 **Hinweis**

Stellen Sie sicher, dass die Ressource online ist.

Alle Ereignistypen, die von der ausgewählten Kamera unterstützt werden, werden angezeigt.

<input type="checkbox"/>	Event Type	Priority	Trigger Client Action	Linked Camera	Enable
<input type="checkbox"/>	Audio Input Exception...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_10.6.113.250	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Face Detection Alarm	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_10.6.113.250	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Intrusion Detection Al...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_10.6.113.250	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Line Crossing Detectio...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_10.6.113.250	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Motion Detection Alar...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_10.6.113.250	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Region Entrance Dete...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_10.6.113.250	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Region Exiting Detecti...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_10.6.113.250	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Video Loss Alarm	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_10.6.113.250	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Video Tampering Det...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_10.6.113.250	<input checked="" type="checkbox"/>

Abbildung 7-2 Ereignisse für die Kamera konfigurieren

- Optional: Geben Sie Schlüsselwörter in das Feld **Filter** ein, um das gewünschte Ereignis schnell zu finden.
- Optional: Aktivieren Sie den Schalter in der Spalte Aktivieren, um den Ereignistyp zu aktivieren, oder klicken Sie auf **Alle aktivieren**, um alle Ereignistypen für diese Kamera zu aktivieren.

 **Hinweis**


Nach der Aktivierung kann das Ereignis vom Client empfangen werden und die Verknüpfungsaktion(en) auslösen. Sie können auch einen Ereignistyp oder alle Ereignistypen deaktivieren.

- Wahlweise: Wählen Sie das/die Ereignis(e) aus und führen Sie dann die folgenden Vorgänge aus.

Priorität bearbeiten Klicken Sie auf **Priorität bearbeiten**, um die Priorität des Ereignisses/der Ereignisse festzulegen.
Die Priorität steht für den Notfallgrad des Ereignisses.

Ereigniskopplung bearbeiten Klicken Sie auf **Ereignisverknüpfung bearbeiten**, um die Verknüpfungsaktion(en) für das/die Ereignis(e) festzulegen.

Akustische Warnung

Lösen Sie die akustische Warnung des Kunden aus, wenn das Ereignis ausgelöst wird. Sie können die Audiodatei in der Dropdown-Liste auswählen oder auf **Hinzufügen** klicken, um eine neue Audiodatei (im WAV-Format) hinzuzufügen. Sie können auf  klicken, um die ausgewählte Audiodatei anzuhören.

E-Mail senden


Senden Sie eine E-Mail-Benachrichtigung mit den Alarminformationen an einen oder mehrere Empfänger.

Einzelheiten zum Festlegen von E-Mail-Parametern finden Sie unter **Festlegen von E-Mail-Parametern**.

Pop-up-Fenster

Popup-Fenster zur Anzeige der ereignisbezogenen Informationen (einschließlich Ereignisdetails, Live-Video der Quellkamera, aufgenommene Bilder der verknüpften Kamera) auf dem Client, wenn das Ereignis ausgelöst wird. Sie können auch Anmerkungen zur Behandlung des Ereignisses eingeben.

Anzeige auf der Karte

Wenn die Ereignisquelle als Hotspot auf der Karte hinzugefügt wird, wird der Hotspot mit  blinkend angezeigt, wenn das Ereignis ausgelöst wird, was dem Sicherheitspersonal hilft, den Ort des Ereignisses zu erkennen.

Sie können auch auf den Hotspot klicken, um die Ereignisdetails und das Live-Video der verknüpften Kamera anzuzeigen.

Verknüpfte Kamera

Verknüpfen Sie die ausgewählte Kamera, um ein Bild oder ein Video aufzunehmen, wenn das Ereignis ausgelöst wird.

Was ist als nächstes zu tun?

Sie müssen das Gerät, zu dem die Kamera gehört, scharfschalten, sonst kann der Client die konfigurierten Ereignisse nicht empfangen. Details finden Sie unter **Aktivieren des Empfangs von Ereignissen von Geräten**.

7.2 Ereignis für Alarmeingang konfigurieren

Das Ereignis für den Alarmeingang bezieht sich auf das durch den Alarmeingang ausgelöste Ereignis. Sie können ein Ereignis für die Alarmeingänge im Client aktivieren. Wenn der Alarmeingang ausgelöst wird, kann der Client das Ereignis zur Überprüfung empfangen und aufzeichnen und eine Reihe von Verknüpfungsaktionen (z. B. das Senden einer E-Mail) zur Benachrichtigung auslösen.

Schritte

1. Klicken Sie auf **Ereigniskonfiguration** → **Videoereignis** → **Alarmeingang**.

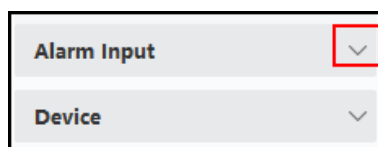


Abbildung 7-3 Anzeige der Alarmeingangsressource

2. Klappen Sie die Gruppe aus und wählen Sie einen Alarmeingang als Ereignisquelle.

Hinweis

Stellen Sie sicher, dass die Ressource online ist.

Es werden alle Ereignistypen angezeigt, die von dem ausgewählten Alarmeingang unterstützt werden.

3. Optional: Geben Sie Schlüsselwörter in das Feld **Filter** ein, um das gewünschte Ereignis schnell zu finden.
 4. Optional: Aktivieren Sie den Schalter in der Spalte Aktivieren, um den Ereignistyp zu aktivieren, oder klicken Sie auf **Alle aktivieren**, um alle Ereignistypen für diesen Alarmeingang zu aktivieren.
-

Hinweis

Nach der Aktivierung kann das Ereignis vom Client empfangen werden und die Verknüpfungsaktion(en) auslösen. Sie können auch einen Ereignistyp oder alle Ereignistypen deaktivieren.

5. Wahlweise: Wählen Sie das/die Ereignis(e) aus und führen Sie dann die folgenden Vorgänge aus.


Priorität bearbeiten Klicken Sie auf **Priorität bearbeiten**, um die Priorität des Ereignisses/der Ereignisse festzulegen.
Die Priorität steht für den Notfallgrad des Ereignisses.

Ereigniskopplung bearbeiten Klicken Sie auf **Ereignisverknüpfung bearbeiten**, um die Verknüpfungsaktion(en) für das/die Ereignis(e) festzulegen.

Akustische Warnung

Lösen Sie die akustische Warnung des Kunden aus, wenn das Ereignis ausgelöst wird.

Sie können die Audiodatei in der Dropdown-Liste auswählen oder auf **Hinzufügen** klicken, um eine neue Audiodatei (im WAV-Format) hinzuzufügen.

Sie können auf  klicken, um die ausgewählte Audiodatei anzuhören.

E-Mail senden


Senden Sie eine E-Mail-Benachrichtigung mit den Alarminformationen an einen oder mehrere Empfänger.

Einzelheiten zum Festlegen von E-Mail-Parametern finden Sie unter **Festlegen von E-Mail-Parametern**.

Pop-up-Fenster

Popup-Fenster zur Anzeige der ereignisbezogenen Informationen (einschließlich Ereignisdetails, Live-Video der Quellkamera, aufgenommene Bilder der verknüpften Kamera) auf dem Client, wenn das Ereignis ausgelöst wird. Sie können auch Anmerkungen zur Behandlung des Ereignisses eingeben.

Anzeige auf der Karte

Wenn die Ereignisquelle als Hotspot auf der Karte hinzugefügt wird, wird der Hotspot mit  blinkend angezeigt, wenn das Ereignis ausgelöst wird, was dem Sicherheitspersonal hilft, den Ort

des Ereignisses zu erkennen.

Sie können auch auf den Hotspot klicken, um die Ereignisdetails und das Live-Video der verknüpften Kamera anzuzeigen.

Verknüpfte Kamera

Verknüpfen Sie die ausgewählte Kamera, um ein Bild oder ein Video aufzunehmen, wenn das Ereignis ausgelöst wird.

Was ist als nächstes zu tun?

Sie müssen das Gerät, zu dem der Alarmeingang gehört, scharfschalten, sonst kann der Client die konfigurierten Ereignisse nicht empfangen. Details finden Sie unter **Aktivieren des Empfangs von Ereignissen von Geräten**.

7.3 Ereignis für Kodiergerät konfigurieren

Das Ereignis für das Kodiergerät bezieht sich auf eine Ausnahme des Kodiergeräts, z. B. Gerät offline. Sie können ein Ereignis für die im Client hinzugefügten Kodiergeräte aktivieren. Wenn das Ereignis auf dem Gerät ausgelöst wird, kann der Client das Ereignis zur Überprüfung empfangen und aufzeichnen und eine Reihe von Verknüpfungsaktionen (z. B. das Senden einer E-Mail) zur Benachrichtigung auslösen.

Schritte

1. Klicken Sie auf **Ereigniskonfiguration** → **Videoereignis** → **Gerät**.

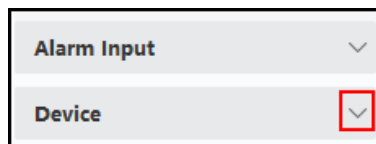


Abbildung 7-4 Ressource Anzeigegerät

2. Wählen Sie ein Gerät als Ereignisquelle aus.

Hinweis

Stellen Sie sicher, dass die Ressource online ist.

Es werden alle vom ausgewählten Gerät unterstützten Ereignistypen angezeigt.

3. Optional: Geben Sie Schlüsselwörter in das Feld **Filter** ein, um das gewünschte Ereignis schnell zu finden.
4. Optional: Aktivieren Sie den Schalter in der Spalte "Aktivieren", um den Ereignistyp zu aktivieren, oder klicken Sie auf "**Alle aktivieren**", um alle Ereignistypen dieses Geräts zu aktivieren.


Hinweis

Nach der Aktivierung kann das Ereignis vom Client empfangen werden und die Verknüpfungsaktion(en) auslösen. Sie können auch einen Ereignistyp oder alle Ereignistypen deaktivieren.

5. Wahlweise: Wählen Sie das/die Ereignis(e) aus und führen Sie dann die folgenden Vorgänge aus.

- | | |
|------------------------------------|--|
| Priorität bearbeiten | Klicken Sie auf Priorität bearbeiten , um die Priorität des Ereignisses/der Ereignisse festzulegen.
Die Priorität steht für den Notfallgrad des Ereignisses. |
| Ereigniskopplung bearbeiten | Klicken Sie auf Ereignisverknüpfung bearbeiten , um die Verknüpfungsaktion(en) für das/die Ereignis(e) festzulegen. |

Akustische Warnung

Lösen Sie die akustische Warnung des Kunden aus, wenn das Ereignis ausgelöst wird. Sie können die Audiodatei in der Dropdown-Liste auswählen oder auf **Hinzufügen** klicken, um eine neue Audiodatei (im WAV-Format) hinzuzufügen. Sie können auf  klicken, um die ausgewählte Audiodatei anzuhören.

E-Mail senden

Senden Sie eine E-Mail-Benachrichtigung mit den Alarminformationen an einen oder mehrere Empfänger.

Einzelheiten zum Festlegen von E-Mail-Parametern finden Sie unter **Festlegen von E-Mail-Parametern**.

Klicken Sie auf **Kopieren**, um die Ereigniseinstellungen dieses Geräts auf andere Geräte zu kopieren.

Hinweis

Sie können die Ereigniseinstellungen nur auf die Ressource(n) desselben Typs kopieren.

Was ist als nächstes zu tun?

Sie müssen dieses Gerät scharfschalten, sonst kann der Client die konfigurierten Ereignisse nicht empfangen. Einzelheiten finden Sie unter **Aktivieren des Empfangs von Ereignissen von Geräten**.


Kapitel 8 Veranstaltungszentrum

Die vom Client empfangenen Ereignisinformationen (z. B. "Gerät offline") werden angezeigt. Im Ereigniszentrum können Sie die detaillierten Informationen der Echtzeit- und historischen Ereignisse prüfen, das mit dem Ereignis verknüpfte Video ansehen, die Ereignisse bearbeiten usw. Bevor der Client die Ereignisinformationen vom Gerät empfangen kann, müssen Sie zunächst die Ereignisse der Ressource aktivieren und das Gerät scharfschalten. Einzelheiten hierzu finden Sie unter **Ereigniskonfiguration** und **Aktivieren des Empfangs von Ereignissen von Geräten**. Bevor Sie die Pop-up-Alarminformationen anzeigen können, müssen Sie das durch ein Ereignis ausgelöste Pop-up-Bild in der Ereigniszentrale aktivieren. Weitere Informationen finden Sie unter **Pop-up-Ereignisinformationen anzeigen**.

8.1 Aktivieren des Empfangs von Ereignissen von Geräten

Bevor die Client-Software Ereignisbenachrichtigungen vom Gerät empfangen kann, müssen Sie das Gerät zunächst scharfschalten.

Schritte

1. Klicken Sie auf  → **Tool** → **Device Arming Control**, um die Seite Device Arming Control zu öffnen.
Alle hinzugefügten Geräte werden auf dieser Seite angezeigt.
2. Optional: Wenn es zu viele Geräte gibt, geben Sie die Schlüsselwörter im Feld Filter ein, um die gewünschten Geräte zu filtern.

Hinweis

Für die gefilterten Geräte können Sie auf **Alle aktivieren** oder **Alle deaktivieren** klicken, um den Empfang von Ereignissen für diese Geräte zu aktivieren.

3. Schalten Sie in der Spalte Auto-Arming den Schalter ein, um die automatische Scharfschaltung zu aktivieren.

Abbildung 8-1 Armvorrichtung

Nach dem Einschalten werden die Geräte scharfgeschaltet. Benachrichtigungen über Ereignisse, die durch das/die aktivierte(n) Gerät(e) ausgelöst werden, werden automatisch und in Echtzeit an die Client-Software gesendet.

8.2 Echtzeit-Ereignisse anzeigen

Die vom Client der angeschlossenen Ressourcen empfangenen Echtzeit-Ereignisinformationen werden angezeigt. Sie können die Echtzeit-Ereignisinformationen überprüfen, einschließlich Ereignisquelle, Ereigniszeit, Priorität usw.

Bevor Sie beginnen

Aktivieren Sie das Empfangen von Ereignissen von Geräten, bevor der Client Ereignisse vom Gerät empfangen kann. Weitere Informationen finden Sie unter **Aktivieren des Empfangs von Ereignissen von Geräten.**

Schritte

1. Klicken Sie auf **Event Center** → **Echtzeitergebnis**, um die Seite für Echtzeitergebnisse aufzurufen, und Sie können die vom Client empfangenen Echtzeitergebnisse anzeigen.

Ereignis Zeit

Bei Kodiergeräten ist die Ereigniszeit der Client-Zeitpunkt, an dem das Ereignis empfangen wird. Bei anderen Gerätetypen ist die Ereigniszeit die Zeit, zu der das Ereignis ausgelöst wird.

Priorität

Die Priorität steht für den Notfallgrad des Ereignisses.

2. Filtern Sie die Ereignisse.

Filter nach Gerätetyp und (oder) Priorität Wählen Sie Gerätetyp(en) und (oder) Prioritäten, um Ereignisse zu filtern.

Nach Stichworten filtern Geben Sie die Schlüsselwörter ein, um die Ereignisse zu filtern.

3. Optional: Klicken Sie mit der rechten Maustaste auf den Tabellenkopf der Ereignisliste, um die in der Ereignisliste anzuzeigenden ereignisbezogenen Elemente anzupassen.
4. Wählen Sie ein Ereignis in der Ereignisliste aus, um die Ereignisdetails anzuzeigen.

Hinweis

Wenn **Bilder im Strukturdatenformat speichern** aktiviert ist, werden keine Bilder in den Ereignisdetails im Ereignis-Center angezeigt. Einzelheiten zum **Speichern von Bildern im Strukturdatenformat** finden Sie unter **Allgemeine Parameter festlegen.**

Hinweis

- Zu den Ereignisdetails gehören das aufgenommene Bild bzw. die aufgenommenen Bilder, das Video (aufgezeichnetes Video, das durch das Ereignis ausgelöst wurde, oder Live-Ansicht des Geräts) und andere Ereignisbeschreibungen.
 - Um das aufgezeichnete Video, das durch das Ereignis ausgelöst wurde, anzuzeigen, sollten Sie die Kamera(s) mit dem Gerät in der Ereigniskonfiguration verknüpfen. Weitere Informationen finden Sie unter **Ereigniskonfiguration.**
-

- Um die aufgenommenen Bilder anzusehen, müssen Sie die Bildspeicherung im Speicherplan konfigurieren.
-

5. Optional: Führen Sie bei Bedarf die folgenden Vorgänge durch.

Einzelereignis behandeln

Klicken Sie auf **Handle**, um den Verarbeitungsvorschlag einzugeben, und klicken Sie dann auf **OK**.

Hinweis

Nachdem ein Ereignis bearbeitet wurde, wird die Schaltfläche "**Bearbeiten**" zu "**Bemerkung hinzufügen**". Klicken Sie auf **Bemerkung hinzufügen**, um weitere Bemerkungen zu diesem behandelten Ereignis hinzuzufügen.

Ereignisse in einem Stapel verarbeiten

Wählen Sie die zu verarbeitenden Ereignisse aus und klicken Sie dann auf **Im Stapel verarbeiten**. Geben Sie den Verarbeitungsvorschlag ein und klicken Sie dann auf **OK**.

Aktivieren/Deaktivieren des Alarmtons

Klicken Sie auf **Audio ein/stumm**, um den Ton des Ereignisses zu aktivieren/deaktivieren.

Automatisch das letzte Ereignis auswählen

Aktivieren Sie das Kontrollkästchen **Letztes Ereignis automatisch auswählen**, um das letzte Ereignis automatisch auszuwählen, und die Details zu den Ereignissen werden angezeigt.

Ereignisse löschen

Klicken Sie auf **Löschen**, um alle Ereignisse in der Ereignisliste zu löschen.

E-Mail senden

Wählen Sie ein Ereignis aus und klicken Sie dann auf **E-Mail senden**, um die Informationen zu diesem Ereignis per E-Mail zu versenden.


Hinweis


Sie sollten zuerst die E-Mail-Parameter konfigurieren, siehe **[E-Mail-Parameter festlegen](#)** für weitere Informationen.

Auto-Play Video

Aktivieren Sie **Auto-Play Video**, um bei der Anzeige von Ereignisdetails automatisch ein Video abzuspielen.

Video oder Bild vergrößern

- Doppelklicken Sie auf das Videobild, um das Video in einem größeren Fenster anzuzeigen.
- Setzen Sie den Cursor auf das Bild, und klicken Sie auf  , um das Bild in einem größeren Fenster zu sehen.

Gefangenes Bild herunterladen	Bewegen Sie den Mauszeiger auf das aufgenommene Bild, und klicken Sie auf das Download-Symbol in der unteren rechten Ecke des Bildes, um es auf den lokalen PC herunterzuladen.
Ereignisgesteuertes Video herunterladen	Bewegen Sie den Mauszeiger auf das aufgezeichnete Video und klicken Sie auf  , um das durch das Ereignis ausgelöste Video herunterzuladen (30 Sekunden vor Eintritt des Ereignisses).

8.3 Suche nach historischen Ereignissen

Sie können historische Ereignisse suchen und anzeigen, indem Sie Suchbedingungen wie Zeit, Gerätetyp und Priorität im Client festlegen. Die gesuchten Ereignisse können Sie bearbeiten und exportieren.

Bevor Sie beginnen

Aktivieren Sie das Empfangen von Ereignissen von Geräten, bevor der Client Ereignisinformationen vom Gerät empfangen kann; Einzelheiten finden Sie unter **Aktivieren des Empfangs von Ereignissen von Geräten**.

Schritte

1. Klicken Sie auf **Veranstaltungscenter** → **Veranstaltungssuche**, um die Seite für die Veranstaltungssuche aufzurufen.
2. Stellen Sie die Filterbedingungen so ein, dass nur die gewünschten Ereignisse angezeigt werden.

Zeit

Die Uhrzeit, zu der das Ereignis beginnt.

Suche nach

Gerät

Suchen Sie die Ereignisse nach Gerät oder nach den Ressourcenkanälen des Geräts. Wenn Sie nach Gerät suchen, müssen Sie folgende Einstellungen vornehmen:

- **Unterknoten einbeziehen:** Durchsucht die Ereignisse des Geräts und alle Ressourcenkanäle.
- **Gerätetyp:** Wählen Sie das Gerät aus, auf dem Sie nach Ereignissen suchen möchten.

Gruppe

Suchen Sie die Ereignisse nach Ressourcenkanälen in der Gruppe.

Hinweis

- Für die Video-Gegensprechanlage müssen Sie den Suchbereich auswählen: Alle und Protokoll sperren.
- Für das Zutrittskontrollgerät können Sie auf **Mehr anzeigen** klicken, um weitere Bedingungen festzulegen: Status, Ereignistyp, Kartenlesertyp, Personennamen,

Kartenummer und Organisation.

Priorität

Die Priorität umfasst niedrig, mittel, hoch und nicht kategorisiert, was den Notfallgrad des Ereignisses angibt.

Veranstaltungstyp

Wählen Sie aus der Dropdown-Liste einen oder mehrere zu durchsuchende Ereignistypen aus.

Hinweis

Sie können ein Schlüsselwort (unterstützt unscharfe Suche) in das Suchfeld eingeben, um die Zielereignisart(en) zu suchen.

Status

Der Bearbeitungsstatus des Ereignisses.

Suche nach Schlüsselwort

Geben Sie ein Schlüsselwort ein (unterstützt unscharfe Suche), um schnell die gewünschten historischen Ereignisse zu finden. Sie können z. B. den Namen einer Person eingeben, um die mit dieser Person verbundenen Ereignisse zu suchen.

3. Klicken Sie auf **Suchen**, um die Ereignisse entsprechend den von Ihnen festgelegten Bedingungen zu suchen.

Hinweis

Wenn **Bilder im Strukturdatenformat speichern** aktiviert ist, werden keine Bilder im Feld Ereignisdetails im Ereignis-Center angezeigt. Einzelheiten zum **Speichern von Bildern im Strukturdatenformat** finden Sie unter [Allgemeine Parameter festlegen](#).

The screenshot displays a web-based interface for managing events. At the top, there are buttons for 'Handle in Batch', 'Export', and 'Export All'. Below this is a table with the following columns: Index, Device Name, Event Type, Event Time, Device Type, Group Name, Object Name, Object Type, Priority, and Event Details. The table contains eight rows of data, all for 'Detector Work Status' events on 'Camera 1' from 'Encoding Device' 'F5' on '2020-03-13'. Each row has a checkbox on the left and a 'Priority' button labeled 'Uncategorized'. Below the table, there is a pagination control showing 'Total 319 Record(s)' and a dropdown set to '50', along with navigation arrows and a page indicator '1 / 7 Page(s)'. Below the table is an 'Event Details' section with buttons for 'Send Email', 'Handle', and 'Hide'. It is divided into two panels: 'Picture' and 'Handling records', both showing 'No picture' and 'No handling record.' respectively.

Index	Device Name	Event Type	Event Time	Device Type	Group Name	Object Name	Object Type	Priority	Event Details	
<input type="checkbox"/>	2	101	Smoke Detection Alarm	2020-03-13 18:59:32	Encoding Device	F5	Camera 1	Camera	Uncategorized	Linked Camera: Camera 1
<input type="checkbox"/>	3	101	Detector Work Status	2020-03-13 18:59:22	Encoding Device	F5	Camera 1	Camera	Uncategorized	Linked Camera: Camera 1,
<input type="checkbox"/>	4	101	Detector Work Status	2020-03-13 18:59:12	Encoding Device	F5	Camera 1	Camera	Uncategorized	Linked Camera: Camera 1,
<input type="checkbox"/>	5	101	Detector Work Status	2020-03-13 18:59:03	Encoding Device	F5	Camera 1	Camera	Uncategorized	Linked Camera: Camera 1,
<input type="checkbox"/>	6	101	Detector Work Status	2020-03-13 18:59:03	Encoding Device	F5	Camera 1	Camera	Uncategorized	Linked Camera: Camera 1,
<input type="checkbox"/>	7	101	Detector Work Status	2020-03-13 18:59:03	Encoding Device	F5	Camera 1	Camera	Uncategorized	Linked Camera: Camera 1,
<input type="checkbox"/>	8	101	Detector Work Status	2020-03-13 18:58:49	Encoding Device	F5	Camera 1	Camera	Uncategorized	Linked Camera: Camera 1,

Abbildung 8-2 Suche nach historischen Ereignissen

4. Optional: Klicken Sie mit der rechten Maustaste auf den Tabellenkopf der Ereignisliste, um die in der Ereignisliste anzuzeigenden ereignisbezogenen Elemente anzupassen.
5. Wählen Sie ein Ereignis in der Ereignisliste aus, um die Ereignisdetails anzuzeigen.

Hinweis

- Zu den Ereignisdetails gehören das aufgenommene Bild bzw. die aufgenommenen Bilder, das Video (aufgezeichnetes Video, das durch das Ereignis ausgelöst wurde, oder Live-Ansicht des Geräts) und andere Ereignisbeschreibungen.
- Um das aufgezeichnete Video, das durch das Ereignis ausgelöst wurde, anzuzeigen, sollten Sie die Kamera(s) mit dem Gerät in der Ereigniskonfiguration verknüpfen. Weitere Informationen finden Sie unter **Ereigniskonfiguration**.
- Um die aufgenommenen Bilder anzusehen, müssen Sie die Bildspeicherung im Speicherplan konfigurieren.

6. Wahlweise: Führen Sie einen der folgenden Vorgänge aus.

Einzelereignis behandeln

Einzelnes Ereignis behandeln: Wählen Sie ein Ereignis aus, das behandelt werden muss, und klicken Sie dann auf der Seite mit den Ereignisinformationen auf **Behandeln**, und geben Sie den Behandlungsvorschlag ein.

 **Hinweis**

Nachdem ein Ereignis bearbeitet wurde, wird die Schaltfläche "**Bearbeiten**" zu "**Bemerkung hinzufügen**". Klicken Sie auf "**Bemerkung hinzufügen**", um weitere Bemerkungen zu diesem bearbeiteten Ereignis hinzuzufügen.

Stapelverarbeitung von Ereignissen

Ereignisse in einem Stapel behandeln: Wählen Sie die zu bearbeitenden Ereignisse aus, klicken Sie auf **Im Batch bearbeiten** und geben Sie einen Vorschlag für die Bearbeitung ein.


 **Hinweis**

Nachdem ein Ereignis bearbeitet wurde, wird die Schaltfläche "**Bearbeiten**" zu "**Bemerkung hinzufügen**". Klicken Sie auf "**Bemerkung hinzufügen**", um weitere Bemerkungen zu diesem bearbeiteten Ereignis hinzuzufügen.

Auto-Play Video

Aktivieren Sie **Auto-Play Video**, um bei der Anzeige von Ereignisdetails automatisch ein Video abzuspielen.

Video oder Bild vergrößern

- Doppelklicken Sie auf das Videobild, um das Video in einem größeren Fenster anzuzeigen.
- Setzen Sie den Cursor auf das Bild, und klicken Sie auf  , um das Bild in einem größeren Fenster zu betrachten.

E-Mail senden

Wählen Sie ein Ereignis aus und klicken Sie dann auf **E-Mail senden**, um die Informationen zu diesem Ereignis per E-Mail zu versenden.

 **Hinweis**


Sie sollten zuerst die E-Mail-Parameter konfigurieren, siehe **[E-Mail-Parameter festlegen](#)** für weitere Informationen.

Ereignisinformationen exportieren

Klicken Sie auf **Exportieren**, um das Ereignisprotokoll oder die Ereignisbilder als CSV/Excel-Datei auf den lokalen PC zu exportieren. Sie können den Speicherpfad manuell festlegen.

Gefangenes Bild herunterladen

Bewegen Sie den Mauszeiger auf das aufgenommene Bild, und klicken Sie auf das Download-Symbol in der unteren rechten Ecke des Bildes, um es auf den lokalen PC herunterzuladen.

Ereignisgesteuertes Video herunterladen Bewegen Sie den Mauszeiger auf das aufgezeichnete Video und klicken Sie auf  , um das durch das Ereignis ausgelöste Video herunterzuladen (30 Sekunden vor Eintritt des Ereignisses).

8.4 Ereignisse vom Gerät abrufen

In einigen Fällen (z. B. wenn der Client nicht gestartet werden kann, das Zutrittskontrollgerät von einem anderen Client aktiviert wurde usw.) sind die vom Client empfangenen und vom Zutrittskontrollgerät ausgelösten Ereignisse nicht konsistent. Sie können Ereignisse vom Gerät aus der Ferne abrufen, um die Ereignisse vom Gerät mit dem Event Center des Clients zu synchronisieren.

Klicken Sie auf **Geräteverwaltung** → **Gerät** → **Gerät**, wählen Sie das/die Zugangskontrollgerät(e) aus, und klicken Sie auf **Ereignisse vom Gerät abrufen**.

Synchronisieren Sie die Ereignisse auf die beiden Arten:

- **Online:** Wenn das Gerät online ist und mit dem Client in Echtzeit kommunizieren kann, können Sie **Online** auswählen und die Start- und Endzeit festlegen, um die Ereignisse während dieses Zeitraums abzurufen.
- **Datei importieren:** Wenn das Netzwerk nicht gut ist oder das Gerät nicht in Echtzeit mit dem Client kommunizieren kann, können Sie die Ereignisdatei zunächst aus dem ausgewählten Gerät exportieren und diese exportierte Datei später auf den Client importieren, indem Sie **Datei importieren** wählen und das Kennwort der verschlüsselten Datei eingeben.

Hinweis

- Aus Gründen der Datensicherheit sollten Sie die Datei beim Exportieren auf dem Gerät verschlüsseln. In der Zwischenzeit sollte das ausgewählte Zugangskontrollgerät dasjenige sein, von dem Sie die Datei exportiert haben.
- Die Funktion sollte von dem Gerät unterstützt werden.

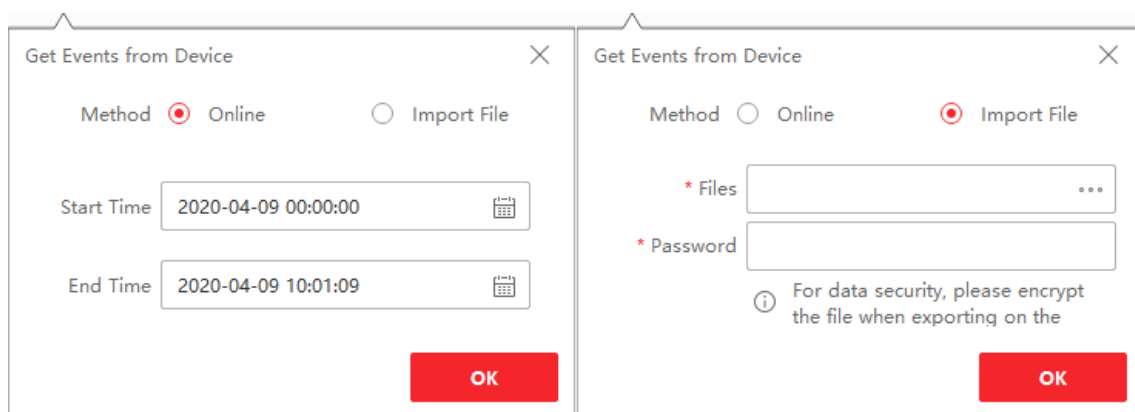


Abbildung 8-3 Ereignisse vom Gerät abrufen

 **Hinweis**

Wenn Sie nur die Ereignisse im Zusammenhang mit der Anwesenheit abrufen möchten, können Sie auch **Zeit & Anwesenheit** → **Anwesenheitsstatistik** → **Anwesenheitsdatensätze** aufrufen, auf **Ereignisse vom Gerät abrufen** klicken und **Online** oder **Datei importieren** auswählen, um die Ereignisse abzurufen.

8.5 Pop-up-Ereignisinformationen anzeigen

Wenn Sie die Ereignisbenachrichtigung aktiviert und als Verknüpfungsaktion "Ereignis ausgelöstes Pop-up-Bild" festgelegt haben, wird bei Eintreten des Ereignisses ein Fenster mit den Ereignisinformationen, zugehörigen Bildern und Videos angezeigt.

Gehen Sie zu **Ereignis-Center** → **Echtzeit-Ereignis** und klicken Sie dann auf **Alarm ausgelöstes Pop-up-Bild aktivieren**, um die Funktion zu aktivieren.

Sie können das ereignisbezogene Videomaterial (von 30 Sekunden vor dem Ereignis bis zum Ende des Ereignisses), das bei Eintritt des Ereignisses aufgenommene Bild sowie die Ereignisdetails wie Ereignisquelle, verknüpfte Kamera, Ereignistyp usw. anzeigen.

 **Hinweis**

- Wenn das Fenster nicht geschlossen ist, sollten Sie auf **Weiter** klicken, um die neuen Ereignisinformationen anzuzeigen, wenn ein neues Ereignis ausgelöst wurde.
 - Wenn Sie die Ereignisinformationen nicht gelöscht haben, können Sie auf **Zurück** klicken, um die vorherigen Ereignisinformationen anzuzeigen.
 - Wenn die Option **Bilder im Strukturdatenformat speichern** aktiviert ist, werden die Bilder nicht in den Ereignisinformationen angezeigt. Weitere Einzelheiten finden Sie unter **Allgemeine Parameter festlegen**.
-

Sie können das Kontrollkästchen **Ereignis automatisch aktualisieren** aktivieren, damit das Fenster automatisch zu den neuesten Ereignisinformationen wechselt, wenn ein neues Ereignis ausgelöst wird.

Kapitel 9 Kartenverwaltung

Die E-Map-Funktion bietet einen visuellen Überblick über die Standorte und Verteilungen der installierten Kameras und Alarmeingabegeräte. Sie können die Live-Ansicht der Kameras auf der Karte sehen und erhalten eine Benachrichtigung auf der Karte, wenn ein Alarm ausgelöst wird. Eine E-Map ist ein statisches Bild (es muss sich nicht um geografische Karten handeln, obwohl dies oft der Fall ist. Je nach den Bedürfnissen Ihrer Organisation können auch Fotos und andere Arten von Bilddateien als E-Maps verwendet werden), die Ihnen einen visuellen Überblick über die Standorte und die Verteilung der Hot Spots (Ressourcen (z. B. Kamera, Alarmeingang), die auf der Karte platziert sind, werden als Hot Spots bezeichnet) gibt. Sie können die physischen Standorte der Kameras und Alarmeingänge sehen und in welche Richtung die Kameras zeigen. Mit der Funktion der Hot Spots können E-Maps in Hierarchien organisiert werden, um von großen Perspektiven zu detaillierten Perspektiven zu navigieren, z. B. von der Etageebene zur Raumebene.

9.1 Karte hinzufügen

Sie sollten eine Karte als übergeordnete Karte für die Hot Spots und Hot Regions hinzufügen.

Schritte

 **Hinweis**

Es kann nur eine Karte zu einer Gruppe hinzugefügt werden.

1. Öffnen Sie die E-Map-Seite.
 2. Wählen Sie eine Gruppe aus, für die Sie eine Karte hinzufügen möchten.
-

 **Hinweis**

Einzelheiten zum Einrichten der Gruppe finden Sie unter **Gruppenverwaltung**.

3. Klicken Sie auf **Karte hinzufügen**, um das Fenster zum Hinzufügen von Karten zu öffnen.

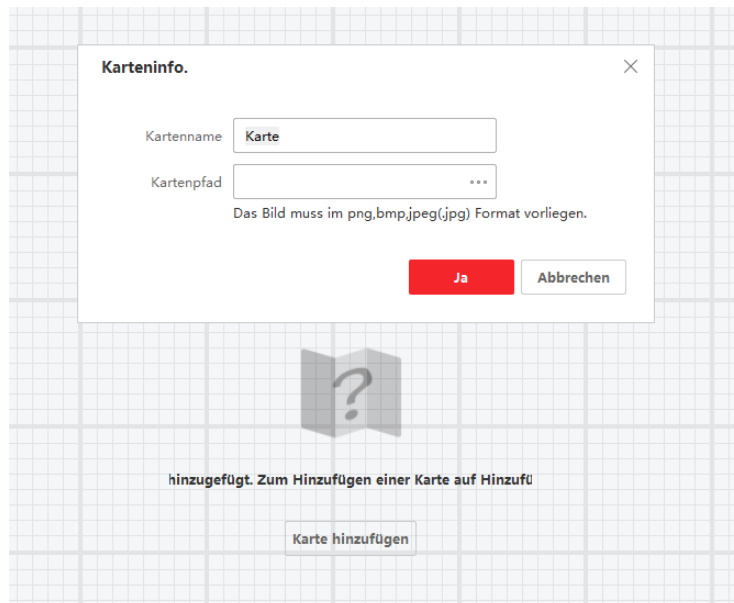


Abbildung 9-1 Karte hinzufügen

4. Geben Sie einen beschreibenden Namen für die hinzugefügte Karte ein.
5. Wählen Sie ein Kartenbild aus dem lokalen Pfad aus.

Hinweis

Das Bildformat der Karte kann nur PNG, JPEG oder BMP sein.

6. Klicken Sie auf **OK**.
7. Optional: Führen Sie nach dem Hinzufügen der Karte die folgenden Aufgaben aus.

Vergrößern/Verkleinern Verwenden Sie das Mausrad oder klicken Sie auf + oder -, um die Karte zu vergrößern oder zu verkleinern.

Kartenbereich anpassen Ziehen Sie das gelbe Fenster in der unteren rechten Ecke oder verwenden Sie die Richtungstasten und die Zoomleiste, um den Kartenbereich für die Ansicht anzupassen.


9.2 Kartenmaßstab bearbeiten

Der Maßstab einer Karte ist das Verhältnis zwischen einer Entfernung auf der Karte und der entsprechenden Entfernung auf dem Boden. Der Client kann die Entfernung zweier Orte auf der Karte anhand der Entfernung am Boden berechnen. Ein genauer Kartenmaßstab ist für die Festlegung des Überwachungsbereichs des Radars unerlässlich.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie eine Karte hinzugefügt haben. Siehe **Karte hinzufügen** für Details. Führen Sie diese Aufgabe aus, wenn Sie der Karte ein Sicherheitsradar hinzufügen möchten.

Schritte

1. Geben Sie das E-Map-Modul ein.
2. Klicken Sie in der E-Map-Symbolleiste auf "**Bearbeiten**", um den Bearbeitungsmodus der Karte aufzurufen.
3. Klicken Sie auf **Kartenkalibrierung** → **Maßstab bearbeiten**, um zwei Stellen auf der Karte auszuwählen.
Der Cursor wird zu  , wenn Sie mit ihm über die Karte fahren.

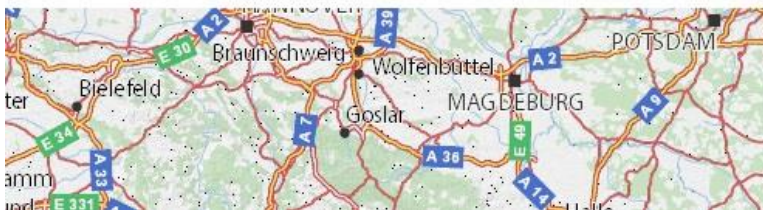


Abbildung 9-2 Kartenmaßstab bearbeiten

4. Klicken Sie auf die Karte, um zwei Standorte auszuwählen.
Das Fenster "Skala bearbeiten" wird eingeblendet.
5. Geben Sie den Bodenabstand zwischen den beiden Standorten ein, und klicken Sie auf **OK**.
Der Client berechnet den Kartenmaßstab automatisch.

9.3 Kalibrierung von Längen- und Breitengraden

Nachdem Sie die Längen- und Breitengrade von zwei Punkten auf der E-Karte kalibriert haben, können Sie das Radar in der Gruppe auf die E-Karte ziehen. Das Radar wird automatisch an die richtige Position auf der E-Karte entsprechend dem Ergebnis der Längen- und Breitengradkalibrierung verschoben.

Bevor Sie beginnen

1. Stellen Sie sicher, dass Sie Radar auf dem Client hinzugefügt haben. Weitere Informationen finden Sie unter **Einzelne oder mehrere Online-Geräte hinzufügen**.
2. Vergewissern Sie sich, dass Sie die Parameter für Längen- und Breitengrad des Radars im Webbrowser eingestellt haben.

Schritte

1. Geben Sie das E-Map-Modul ein.
2. Klicken Sie in der E-Map-Symbolleiste auf "**Bearbeiten**", um den Bearbeitungsmodus der Karte aufzurufen.
3. Klicken Sie auf **Kartenkalibrierung** → **Längen-/Breitengradkalibrierung**.
4. Klicken Sie auf **Kalibrierungspunkt hinzufügen**.
5. Klicken Sie auf einen Punkt auf der Karte, geben Sie den Längen- und Breitengrad des Punktes in das Popup-Fenster ein und klicken Sie dann auf **Speichern**.
6. Klicken Sie auf **Kalibrierungspunkt hinzufügen** und wiederholen Sie den vorherigen Schritt, um den zweiten Kalibrierungspunkt hinzuzufügen.
7. Ziehen Sie den Radar in der linken Ressourcengruppe auf die Karte.
Das Radargerät bewegt sich automatisch an die richtige Position auf der Karte entsprechend der Längen- und Breitengradkalibrierung von zwei Punkten.

9.4 Hot Spot verwalten

Die der Karte hinzugefügten Geräte werden als Hotspots bezeichnet. Die Hotspots zeigen die Standorte der Geräte an, und Sie können über die Hotspots auch die Live-Ansicht oder Alarminformationen der Überwachungsszenarien abrufen.

9.4.1 Kamera als Hot Spot hinzufügen

Sie können der Karte Kameras als Hotspots hinzufügen.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie dem Client eine E-Map und eine Kamera hinzugefügt haben. Weitere Informationen finden Sie unter **Karte hinzufügen** und **Geräteverwaltung**.

Schritte

1. Rufen Sie die E-Map-Seite auf.
2. Klicken Sie auf **Bearbeiten** in der oberen rechten Ecke, um den Bearbeitungsmodus der Karte aufzurufen.
3. Klicken Sie auf **Hotspot hinzufügen** → **Kamera-Hotspot**, um das Fenster Hotspot hinzufügen zu öffnen.

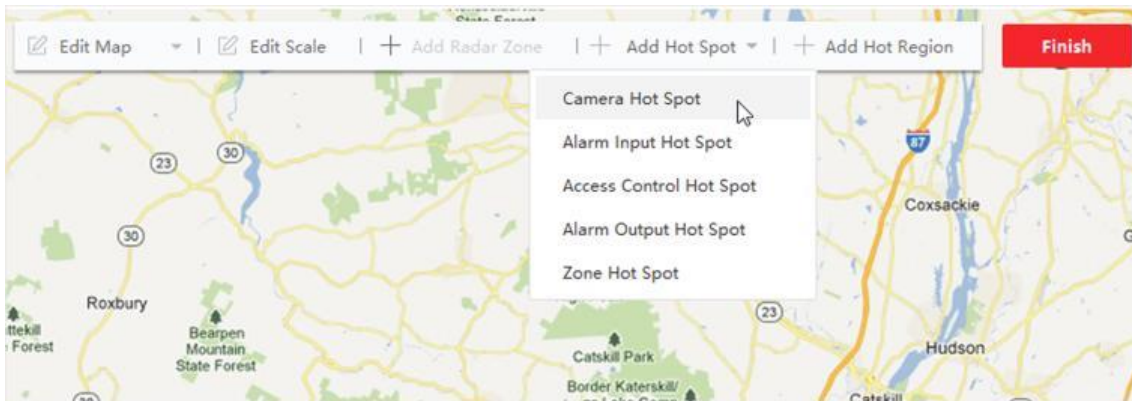


Abbildung 9-3 Hotspot hinzufügen

4. Wählen Sie die Kameras aus, die dem Lageplan hinzugefügt werden sollen.
5. Optional: Bearbeiten Sie den Hotspot-Namen, wählen Sie die Farbe des Namens und das Hotspot-Symbol aus.
6. Klicken Sie auf **OK**, um die Einstellungen zu speichern.

Hinweis

Sie können auch die Kamerasymbole aus der Gruppenliste direkt auf die Karte ziehen, um die Hotspots hinzuzufügen.

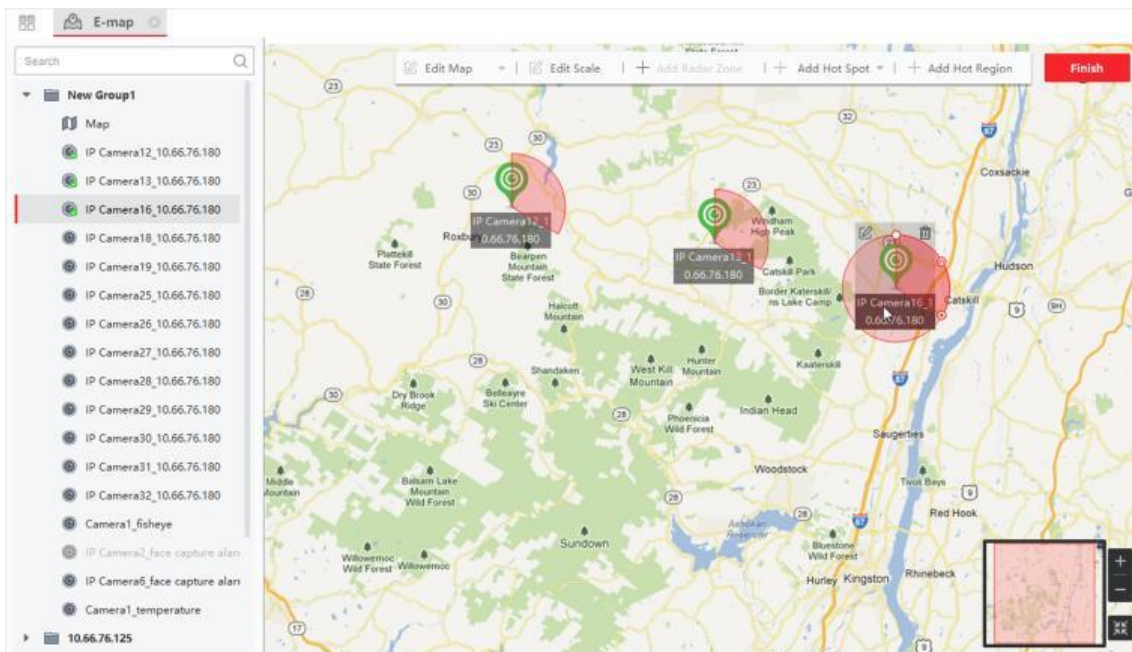






Abbildung 9-4 Hinzugefügter Kamera-Hotspot

Die Kamerasymbole werden auf der Karte als Hotspots hinzugefügt, und die Symbole der hinzugefügten Kameras ändern sich von  zu . Der Sektor zeigt das Sichtfeld der Kamera an.

7. Führen Sie die folgende(n) Operation(en) durch.

- | | |
|---------------------------------|---|
| Verschieben des Hotspots | Ziehen Sie den Hotspot, um ihn an eine bestimmte Position zu verschieben. |
| Ändern des FOV-Winkels | Ziehen Sie /  und drehen Sie, um das Sichtfeld der Kamera zu ändern. |
| Ändern Sie die FOV-Größe | Ziehen Sie  , um die FOV-Größe zu ändern. |

9.4.2 Alarমেingang als Hot Spot hinzufügen

Sie können die Alarমেingänge als Hotspots in die Karte einfügen.

Schritte

1. Geben Sie das E-Map-Modul ein.
2. Klicken Sie auf **Bearbeiten** in der oberen rechten Ecke, um den Bearbeitungsmodus der Karte aufzurufen.
3. Klicken Sie auf **Hotspot hinzufügen** → **Alarমেingangs-Hotspot**, um das Fenster Hotspot hinzufügen zu öffnen.

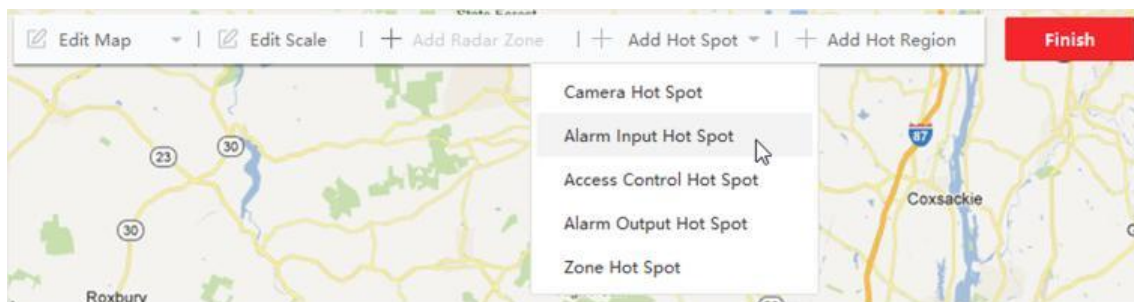


Abbildung 9-5 Alarমেingang als Hotspot hinzufügen

4. Wählen Sie die Alarমেingänge aus, die der Karte hinzugefügt werden sollen.
5. Optional: Bearbeiten Sie den Hotspot-Namen, wählen Sie die Namensfarbe und wählen Sie das Hotspot-Symbol durch Doppelklick auf das entsprechende Feld.
6. Klicken Sie auf **OK**.

Hinweis

Sie können auch die Alarmeingangssymbole aus der Gruppenliste direkt auf die Karte ziehen, um den Hotspot hinzuzufügen.

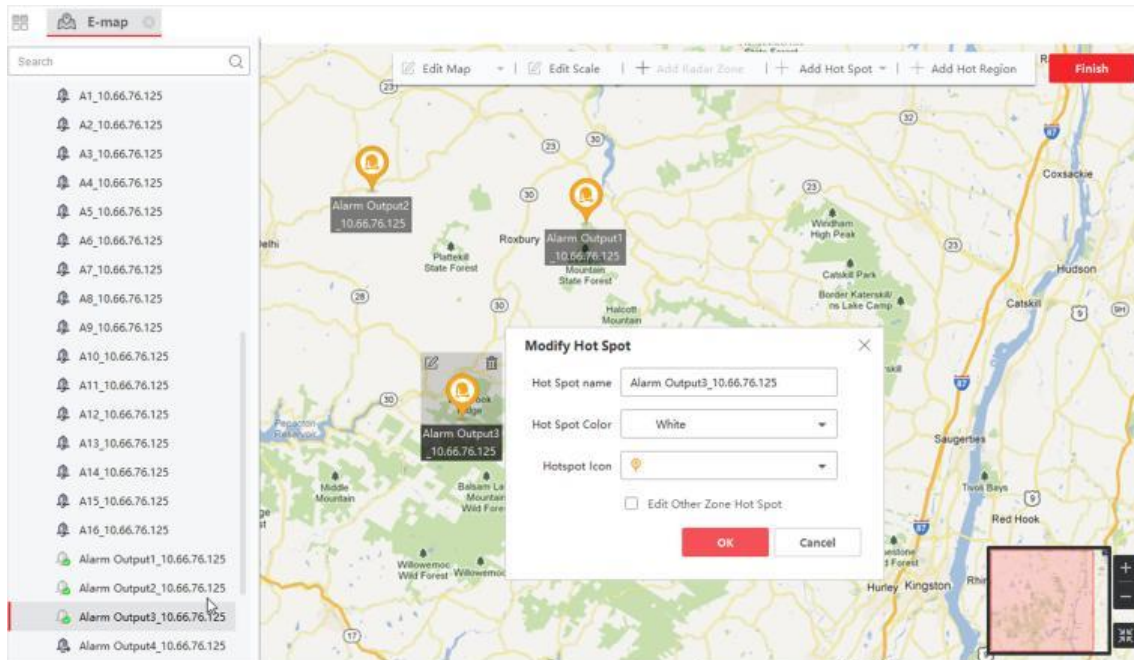




Abbildung 9-6 Hinzugefügter Alarmeingangs-Hotspot

Die Alarmeingangssymbole werden der Karte als Hotspots hinzugefügt und die Symbole der hinzugefügten Alarmeingänge in der Gruppenliste ändern sich von  auf .

7. Optional: Ziehen Sie den Hotspot, um ihn an eine bestimmte Position zu verschieben.

9.4.3 Alarmausgang als Hot Spot hinzufügen

Sie können Alarmausgänge auf der Karte als Hotspots für die Verwaltung hinzufügen. Danach können Sie sie schnell aktivieren oder deaktivieren. Wenn Sie einen Alarmausgang auf der Karte aktivieren, werden die daran angeschlossenen Sicherheitskontrollgeräte (z. B. Sirenen, Klingeln) alarmiert.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie dem Client eine E-Map und einen Alarmausgang hinzugefügt haben. Siehe **Karte hinzufügen** und **Gerätemanagement** für weitere Details.

Schritte

1. Geben Sie das E-Map-Modul ein.
2. Klicken Sie in der E-Map-Symbolleiste auf "**Bearbeiten**", um den Bearbeitungsmodus der Karte aufzurufen.

3. Klicken Sie auf **Hotspot hinzufügen** → **Alarmausgangshotspot**, um das Fenster Hotspot hinzufügen zu öffnen.

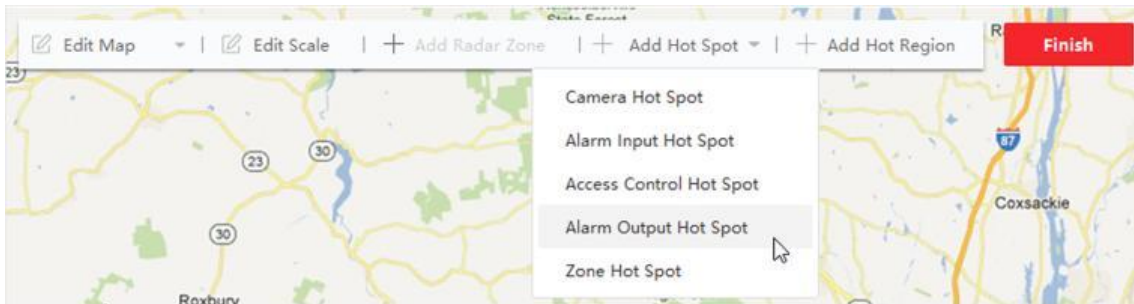


Abbildung 9-7 Alarmausgang als Hot Spot hinzufügen

4. Wählen Sie den Alarmausgang aus, der der Karte hinzugefügt werden soll.
5. Optional: Bearbeiten Sie den Hotspot-Namen, wählen Sie die Farbe des Namens und wählen Sie das Hotspot-Symbol.
6. Klicken Sie auf **OK**.

Hinweis

Sie können auch ein Alarmausgangssymbol aus der Alarmausgangsliste auf die Karte ziehen, um den Hotspot hinzuzufügen.

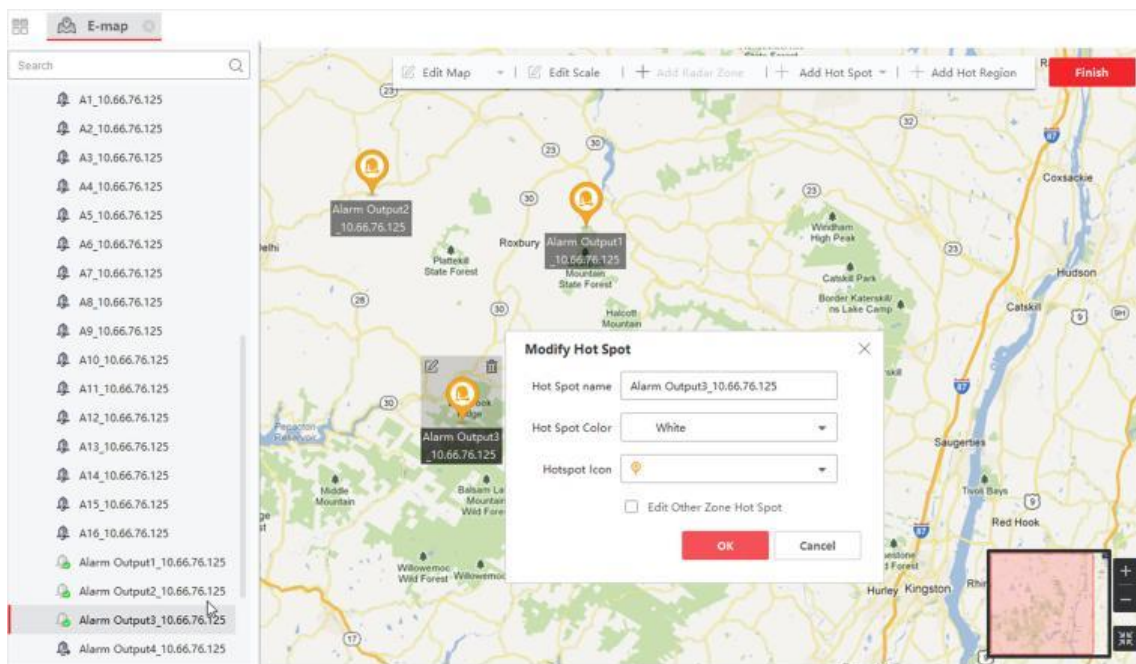




Abbildung 9-8 Hinzugefügter Alarmausgang-Hotspot

Der Alarmausgang wird der Karte als Hotspot hinzugefügt und sein Symbol in der Gruppenliste ändert sich von  zu  .

7. Optional: Ziehen Sie den Alarmausgang, um ihn an eine bestimmte Position zu verschieben.

9.4.4 Zone als Hot Spot hinzufügen

Sie können der Karte Zonen hinzufügen, damit Sie die Zone im Falle eines Alarms schnell lokalisieren können.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie dem Client eine Karte und eine Zone hinzugefügt haben. Siehe [Karte hinzufügen](#) und [Gerät hinzufügen](#) für weitere Informationen.

Schritte

1. Geben Sie das E-Map-Modul ein.
2. Klicken Sie in der E-Map-Symbolleiste auf "**Bearbeiten**", um den Bearbeitungsmodus der Karte aufzurufen.
3. Klicken Sie auf **Hot-Spot hinzufügen** → **Zonen-Hot-Spot**, um das Fenster Hot-Spot hinzufügen zu öffnen.

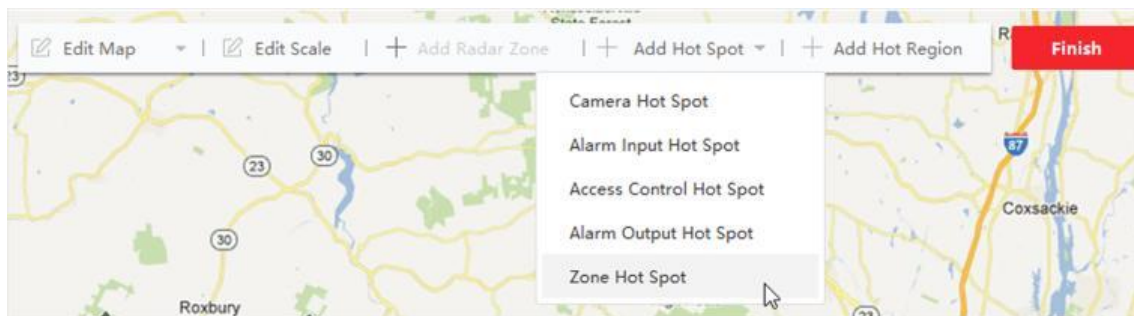


Abbildung 9-9 Zone als Hotspot hinzufügen

4. Wählen Sie die Zone(n) aus, die der Karte hinzugefügt werden soll(en).
5. Optional: Bearbeiten Sie den Hotspot-Namen, wählen Sie die Farbe des Namens und wählen Sie das Hotspot-Symbol.
6. Klicken Sie auf **OK**.

 **Hinweis**

Sie können auch die Alarmausgangssymbole aus der Alarmausgangsliste auf die Karte ziehen, um den Hotspot hinzuzufügen.

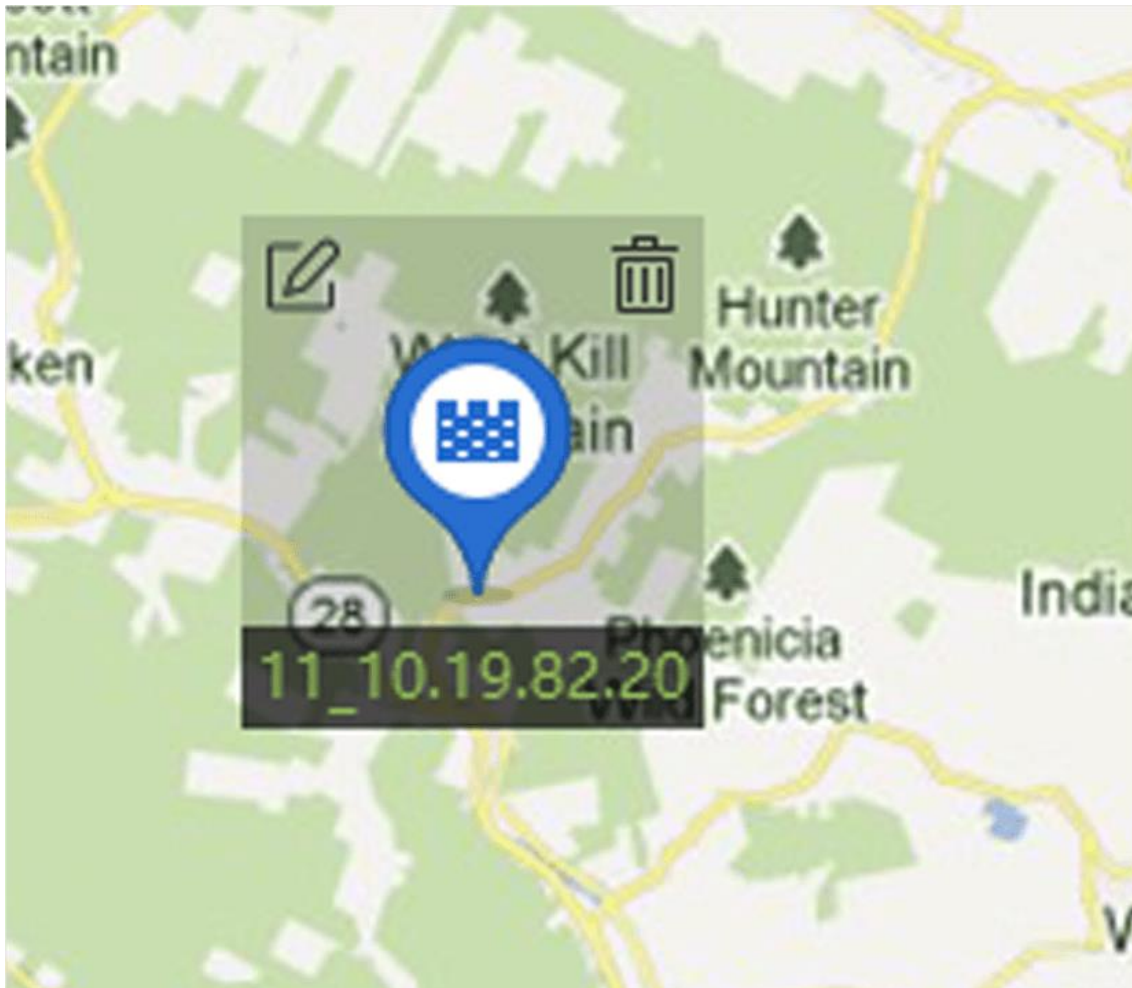




Abbildung 9-10 Zone auf der Karte

Die Zone wird der Karte als Hotspot hinzugefügt und ihr Symbol in der Gruppenliste ändert sich von  zu  .

7. Optional: Ziehen Sie den Zonen-Hotspot, um ihn an eine bestimmte Position zu verschieben. Wenn Alarme ausgelöst werden, wird die Nummer des neuesten Alarms auf dem Symbol der Zone angezeigt. Sie können auf die Nummer klicken, um die Details der Alarme zu sehen.

 **Hinweis**

Es können nicht mehr als 10 neueste Alarme angezeigt werden.

8. Optional: Klicken Sie auf **Alarmlöschen**, um die Alarmlisten der Zonen auf der aktuellen Karte als gelesen zu markieren.

9.4.5 Zugangspunkt als Hot Spot hinzufügen

Sie können Zugangspunkte auf der Karte als Hotspots hinzufügen, so dass Sie die Hotspots finden und deren Status und Alarmnummern anzeigen können.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie dem Client eine Karte und einen Zugangspunkt hinzugefügt haben. Siehe **Karte hinzufügen** und **Gerät hinzufügen** für weitere Informationen.

Schritte

1. Geben Sie das E-Map-Modul ein.
2. Klicken Sie in der E-Map-Symbolleiste auf **"Bearbeiten"**, um den Bearbeitungsmodus der Karte aufzurufen.
3. Klicken Sie auf **Add Hot Spot** → **Access Point Hot Spot**, um das Fenster Add Hot Spot zu öffnen.

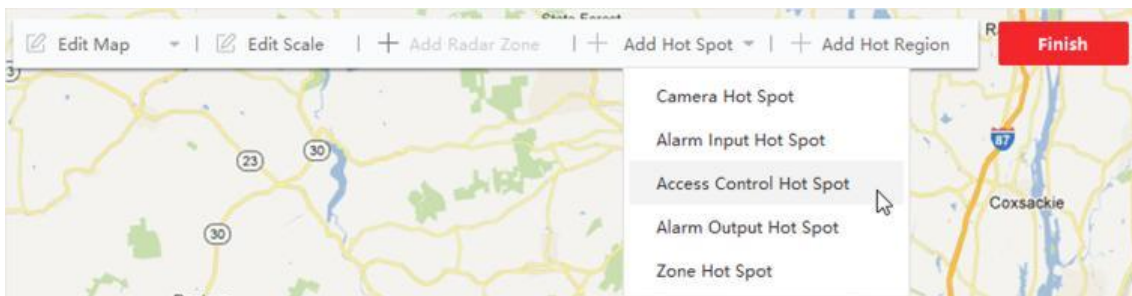




Abbildung 9-11 Zugangspunkt als Hotspot hinzufügen

4. Wählen Sie den/die Zugangspunkt(e) aus, die der Karte hinzugefügt werden sollen.
5. Optional: Bearbeiten Sie den Hotspot-Namen, wählen Sie die Farbe des Namens und wählen Sie das Hotspot-Symbol.
6. Klicken Sie auf **OK**.

Hinweis

Sie können auch ein Zugangspunktsymbol aus der Zugangspunktliste auf die Karte ziehen.

Abbildung 9-12 Zugangspunkt auf der Karte

Der Zugangspunkt wird der Karte als Hotspot hinzugefügt und sein Symbol in der Gruppenliste ändert sich von  zu .

7. Optional: Ziehen Sie den Hotspot des Zugangspunkts, um ihn an eine bestimmte Position zu verschieben.

Wenn Alarmlisten ausgelöst werden, wird die Nummer des neuesten Alarms auf dem Hotspot-

Symbol angezeigt. Sie können auf die Nummer klicken, um die Details des Alarms zu sehen.

 **Hinweis**

Es können nicht mehr als 10 neueste Alarme angezeigt werden.

Kapitel 10 Statistik

10.1.1 Personenzählungsbericht nach Kodiergerät

Der Personenzählungsbericht nach Codiergerät zeigt die von den Codiergeräten erfassten Personenzählungsdaten an. Sie können die Personenzählungsdaten in verschiedenen Dimensionen suchen.

Bevor Sie beginnen

Fügen Sie der Software ein Codiergerät mit Personenzählfunktion hinzu und konfigurieren Sie den entsprechenden Bereich und die Personenzählregel ordnungsgemäß. Weitere Informationen zum Hinzufügen von Geräten zur Personenzählung finden Sie unter **Gerät hinzufügen**.

Schritte

1. Klicken Sie auf **Bericht** → **Personenzählung**, um die Seite Personenzählung aufzurufen.
2. Wählen Sie als **Gerätetyp Kodiergerät**.
3. Wählen Sie als Berichtstyp Tagesbericht, Wochenbericht, Monatsbericht oder Jahresbericht.

Täglicher Bericht

Der Tagesbericht zeigt Daten auf Tagesbasis. Das System berechnet die Anzahl der Personen in jeder Stunde eines Tages.

Wöchentlicher Bericht, monatlicher Bericht und Jahresbericht


Im Vergleich zum Tagesbericht können Wochen-, Monats- und Jahresberichte weniger zeitaufwendig sein, da sie nicht jeden Tag vorgelegt werden müssen. Das System berechnet die Anzahl der Personen an jedem Tag einer Woche, an jedem Tag eines Monats und in jedem Monat eines Jahres.

Benutzerdefinierter Bericht

Die Benutzer können die Tage im Bericht anpassen, um die Anzahl der Personen an jedem Tag oder Monat des benutzerdefinierten Zeitintervalls zu analysieren.

Hinweis

Sie können nicht mehr als 31 Tage im Kalender auswählen.

4. Wählen Sie die Art der Statistikzeit und klicken Sie auf  , um die Zeit einzustellen.

Eine Periode

Erstellen Sie die Statistiken in einem Zeitraum.

Mehrere Perioden

Erstellen Sie die Statistiken für zwei Zeiträume, um den Personenfluss und die Anzahl der Personen in zwei Zeiträumen zu vergleichen.

Wenn Sie z. B. den Berichtstyp als Monatsbericht und die Monate März und April als Statistikzeitpunkt festlegen, werden die Ergebnisse der Personenzählung im März und April in demselben Diagramm mit unterschiedlicher Farbe angezeigt, und Sie können die Daten an den verschiedenen Tagen der einzelnen Monate vergleichen.

5. Wählen Sie **Statistik-Typ**.

Anzeige nach Gerät

Anzeige des Berichts nach Gerät.

Wenn Sie z. B. einen NVR auswählen (mit 4 Personen, die Kameras zählen), zeigt der Bericht die Gesamtzahl der Personen an, die durch die 4 Personen, die Kameras zählen, summiert werden.

Anzeige nach Kamera

Zeigen Sie den Bericht nach Kamera an.

Wenn Sie z. B. einen NVR auswählen (mit 4 Kameras, die von Personen gezählt werden), zeigt der Bericht die Statistiken für jede einzelne Kamera an, und zwar in 4/8 Farben (wobei eine oder zwei Farben jeweils eine Kamera darstellen).

Anzeige nach Gruppierung Statistik

Zeigen Sie den Bericht nach gruppierten Statistiken an.

Wenn Sie beispielsweise eine Gerätegruppe auswählen (die Gruppe wird auf dem Client erstellt), zeigt der Bericht die Gesamtzahl der Personen an, die durch die Gesamtzahl der Personen, die Kameras in der Gruppe zählen, summiert wird.

Hinweis

- Einzelheiten zur Gerätegruppe finden Sie unter **Gruppenressourcen**.
 - Diese Funktion sollte von dem Gerät unterstützt werden.
-

6. Wählen Sie den Filterungsmodus.

Kanal

Anzeige von Personenzählungsdaten, die von Kanälen eines Codiergeräts erfasst wurden.

Region

Anzeige der Anzahl der Personen in ausgewählten Bereichen einer Kamera.

Hinweis

Sie müssen zuvor Regionen für die Kamera konfigurieren. Einzelheiten dazu finden Sie im Benutzerhandbuch des Geräts.

- Wählen Sie die Kamera(s) oder die Region(en) aus der Kameraliste aus.
- Legen Sie den Inhalt fest, der angezeigt werden soll.

Richtung

Berechnen Sie die Anzahl der Personen in verschiedenen Richtungen, z. B. Eingang, Ausgang oder Eingang und Ausgang.

Eingabe

Die eingetragenen Personen werden gezählt.

Ausfahrt

Die ausgetretenen Personen werden gezählt.

Betreten und Verlassen

Es werden sowohl die ein- als auch die ausgetretenen Personen gezählt.

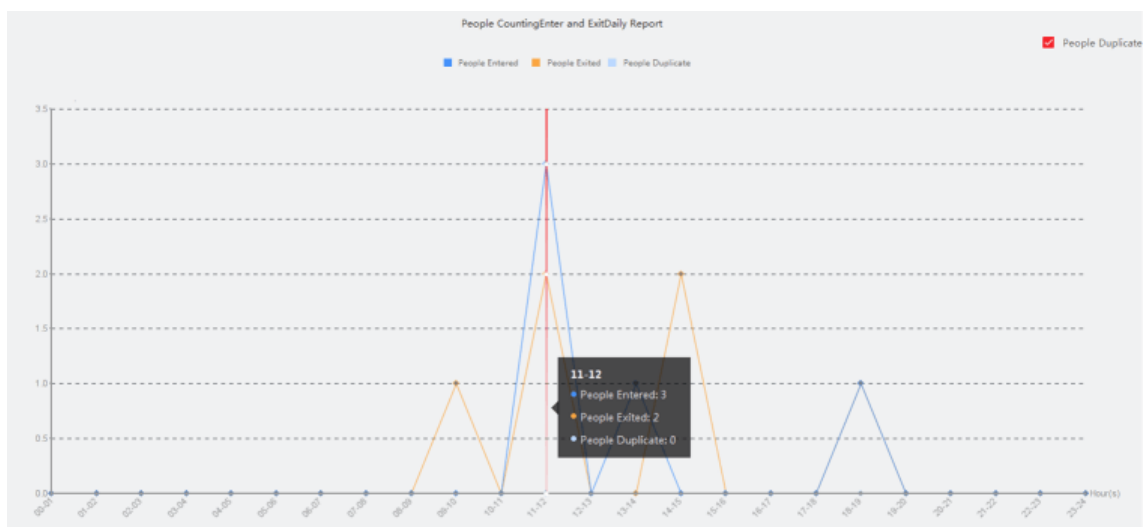


Abbildung 10-1 Personenzählung nach Richtung

Gesichtszüge

Erstellen Sie den Bericht auf der Grundlage des Gesichtsmerkmals.

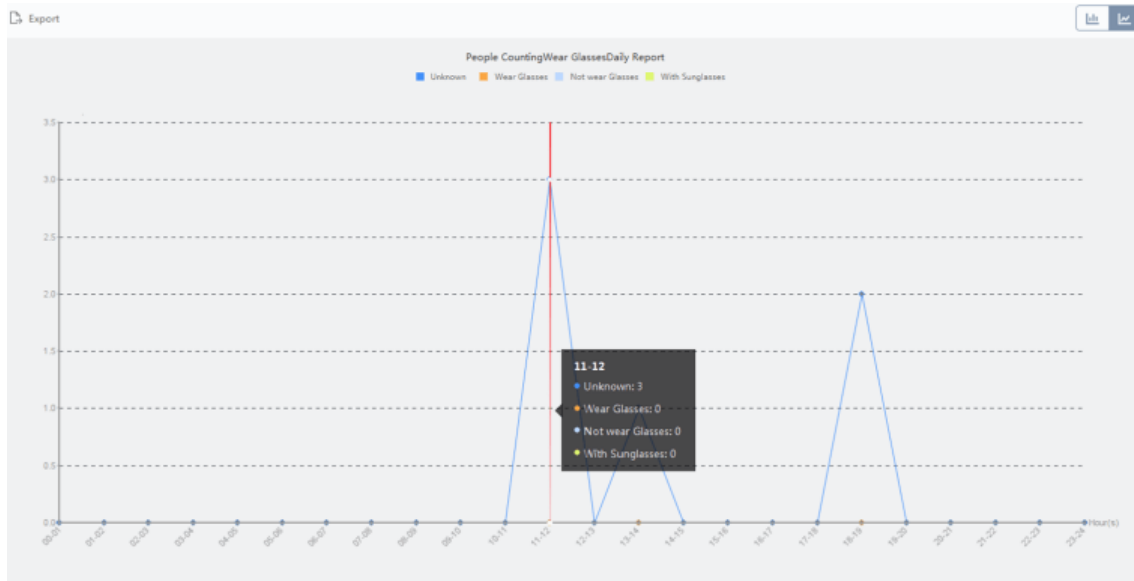


Abbildung 10-2 Personenzählung nach Gesichtsmerkmalen

9. Optional: Markieren Sie **Nur Kinder**, um einen Bericht über die erkannten Kinder zu erstellen.

Hinweis

- Der Client zählt erkannte Personen, die kleiner als eine vordefinierte Größe sind, die auf der Fernkonfigurationsseite des Geräts konfiguriert werden kann. Einzelheiten zur Konfiguration des Hörschwellenwerts finden Sie im Benutzerhandbuch des Geräts.
- Diese Funktion muss von dem Gerät unterstützt werden.

10. Klicken Sie auf "**Suchen**", um die Statistik der Personenzählung und detaillierte Daten für jede Stunde, jeden Tag oder jeden Monat zu erhalten.

Standardmäßig wird die Statistik in Form eines Histogramms angezeigt.

11. Optional: Für den Bericht nach Richtung können Sie in der rechten oberen Ecke der Berichtsseite ein Häkchen bei "**Doppelte Personen**" setzen, um die Anzahl der doppelten Personen anzuzeigen.

Hinweis

Die Anzahl der doppelten Personen wird von dem Gerät berechnet. Wenn dasselbe Gesicht mehr als einmal erkannt wird, wird es als doppelte Person berechnet. Wenn zum Beispiel ein Kassierer den Supermarkt mehr als einmal betritt oder verlässt, wird er/sie als doppelte Person berechnet. Auf diese Weise kann der Supermarkt die tatsächliche Anzahl von Personen ermitteln, die einkaufen.

12. Optional: Führen Sie nach der Suche die folgenden Operationen durch.

Zum Liniendiagramm wechseln Klicken Sie auf [↔](#), um das Diagramm in ein Liniendiagramm umzuwandeln.

 **Hinweis**

Standardmäßig werden die Statistiken in einem Balkendiagramm angezeigt.

**Zum
Balkendiagramm
wechseln**

Klicken Sie auf [☰](#) , um das Diagramm in ein Balkendiagramm umzuwandeln.

**Auf lokalem PC
speichern**

Klicken Sie auf **Exportieren**, um die detaillierten Daten der Personenzählung auf Ihrem PC zu speichern.

10.2 Bericht zur Personenzählung an Kreuzungen anzeigen

Die Kreuzungsanalyse dient zur Überwachung des Personenflusses und der Personenanzahl in einer kreuzungsähnlichen Szene. Die Pfeile im Bild beziehen sich auf verschiedene Richtungen. Wenn Sie eine Richtung (z. B. A) als Eingang auswählen, werden die anderen Richtungen standardmäßig als Ausgänge festgelegt, so dass mehrere Wege entstehen (z. B. A nach A, A nach B, A nach C und A nach D). Sie können sich die Anzahl der Personen anzeigen lassen, die die einzelnen Pfade passiert haben, was dem Ladenbesitzer helfen kann, den Personenfluss an verschiedenen Türen zu analysieren. Das Ergebnis der Statistik kann in einem täglichen, wöchentlichen, monatlichen und jährlichen Bericht angezeigt werden.

Bevor Sie beginnen

Vergewissern Sie sich, dass eine Fischaugenkamera, die die Schnittpunktanalysefunktion unterstützt, ordnungsgemäß konfiguriert wurde und zur Software hinzugefügt wurde. Siehe [Gerät hinzufügen](#) für Details zum Hinzufügen des Geräts.

Schritte

 **Hinweis**

Es können bis zu 10 Kreuzungen analysiert werden.

1. Klicken Sie auf **Bericht** → **Kreuzungsanalyse**, um das Modul Kreuzungsanalyse aufzurufen.
2. Wählen Sie als Berichtstyp Tagesbericht, Wochenbericht, Monatsbericht oder Jahresbericht.

Täglicher Bericht

Der Tagesbericht zeigt Daten auf täglicher Basis. Das System berechnet die Anzahl der Personen im Kreuzungsbericht in jeder Stunde eines Tages.

Wöchentlicher Bericht, monatlicher Bericht und Jahresbericht

Im Vergleich zum Tagesbericht können Wochen-, Monats- und Jahresberichte weniger

zeitaufwändig sein, da sie nicht jeden Tag vorgelegt werden müssen. Das System berechnet die Anzahl der Personen im Kreuzungsbericht an jedem Tag einer Woche, an jedem Tag eines Monats und an jedem Monat eines Jahres.

3. Legen Sie die Startzeit für den Bericht fest.
4. Wählen Sie die Kamera für die Erstellung des Berichts aus.
5. Wählen Sie eine Richtung als Eingang aus der Dropdown-Liste im Feld **Fluss in**.
6. Klicken Sie auf **Suchen**, um das Ergebnis der Statistik zu erhalten.

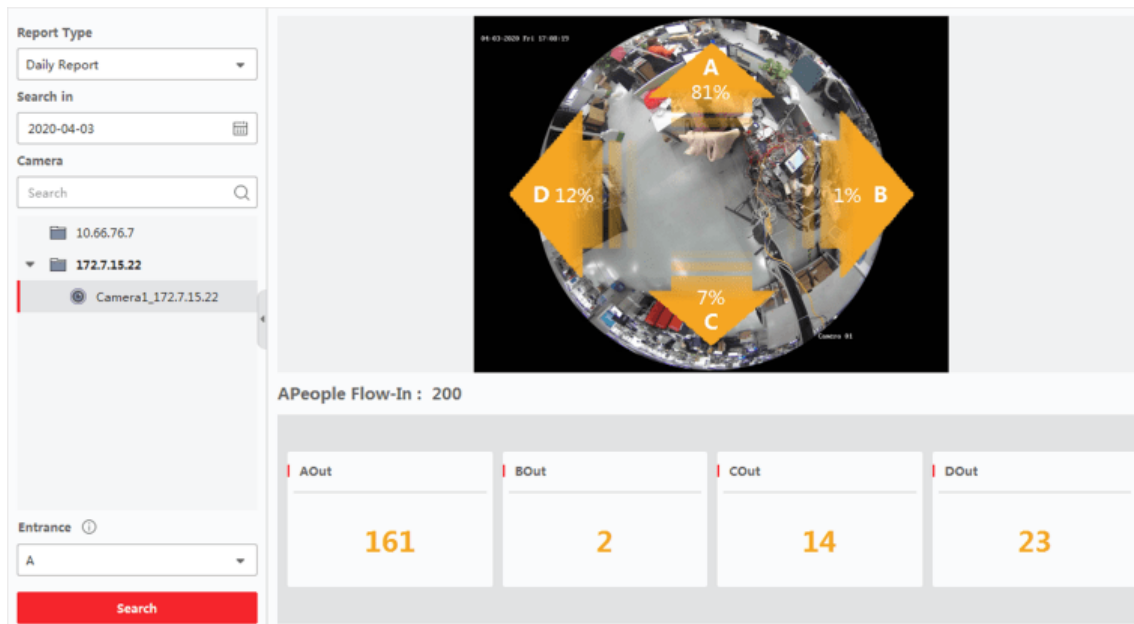


Abbildung 10-4 Ergebnisse

Die Personennummer für jeden Pfad wird auf der rechten Seite angezeigt.

10.4 Wärmekartenbericht

Heatmap ist eine grafische Darstellung von Daten, die durch Farben dargestellt werden, und die Heatmap-Daten können in einem Liniendiagramm angezeigt werden. Sie können die Heatmap-Funktion der Kamera verwenden, um die Besuchszeiten und die Verweildauer der Kunden in einem konfigurierten Bereich zu analysieren, was dem Ladenbesitzer helfen kann, den interessierten Bereich der Kunden zu analysieren und die Anordnung der Waren vorzunehmen.

Bevor Sie beginnen

Fügen Sie der Software eine Netzwerkkamera mit Wärmebildkarte hinzu und konfigurieren Sie den entsprechenden Bereich ordnungsgemäß. Die hinzugefügte Kamera sollte mit einer Heatmap-Regel konfiguriert worden sein. Siehe [Gerät hinzufügen](#) für Details zum Hinzufügen von Heatmap-Netzwerk-Kameras.

Schritte

1. Klicken Sie auf **Bericht** → **Heatmap**, um die Heatmap-Seite aufzurufen.

2. Wählen Sie als Berichtstyp

Tagesbericht/Wochenbericht/Monatsbericht/Jahresbericht/Benutzerdefinierter **Bericht**.

Täglicher Bericht

Der Tagesbericht zeigt Daten auf täglicher Basis. Das System berechnet die Daten der Heatmap in jeder Stunde eines Tages.

Wöchentlicher Bericht, monatlicher Bericht und Jahresbericht

Im Vergleich zu Tagesberichten sind Wochen-, Monats- und Jahresberichte weniger zeitaufwändig, da sie nicht jeden Tag vorgelegt werden müssen. Das System berechnet die Daten der Heatmap für jeden Tag einer Woche, für jeden Tag eines Monats und für jeden Monat eines Jahres.

Benutzerdefinierter Bericht

Sie können die Tage im Bericht anpassen, um die Verweildauer oder den Crowd-Trend an jedem Tag oder Monat des benutzerdefinierten Zeitintervalls zu analysieren.



Hinweis

Der Zeitraum im benutzerdefinierten Bericht sollte nicht mehr als 31 Tage betragen.

3. Wählen Sie als Statistiktyp **Nach Verweildauer** oder **Nach Crowd-Trend**.

Nach Verweildauer

Das System berechnet den Heatmap-Wert (den Ordinatenwert im Liniendiagramm oder die Farbe in Bildern) entsprechend der Verweildauer der Besucher.

Von Crowd Trend

Das System berechnet den Heatmap-Wert (den Ordinatenwert im Liniendiagramm oder die Farbe in Bildern) entsprechend der Anzahl der erkannten Personen.

4. Legen Sie den Zeitraum für die Suche fest.

5. Wählen Sie eine Wärmebildkamera in der Kameraliste aus.

6. Klicken Sie auf **Heatmap generieren**, um die Heatmap der Kamera anzuzeigen.

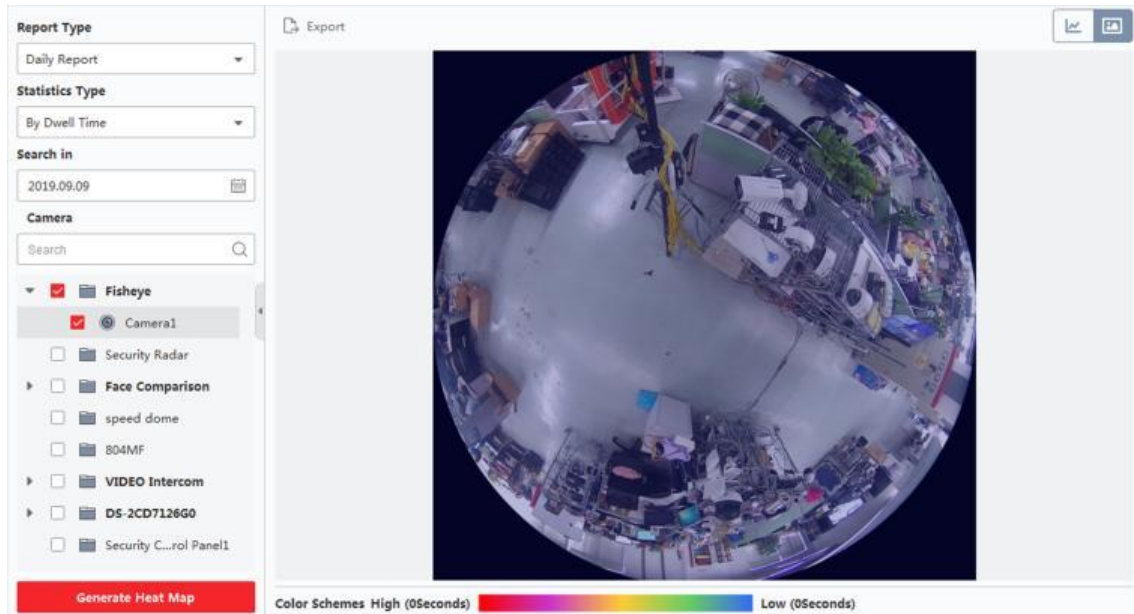




Abbildung 10-9 Ergebnisse

7. Optional: Nach der Erstellung des Heatmap-Berichts können Sie die folgenden Vorgänge durchführen.

Anzeige im Liniendiagramm

Klicken Sie auf  , um die Statistiken in einem Liniendiagramm anzuzeigen.

Anzeige im Bildmodus

Klicken Sie auf  , um die Statistik im Bildmodus anzuzeigen. Der rote Farbblock (255, 0, 0) kennzeichnet den beliebtesten Bereich und der blaue Farbblock (0, 0, 255) den weniger beliebten Bereich.

Statistikdaten speichern

Klicken Sie auf **Exportieren**, um die detaillierten Daten der Heatmap auf Ihrem PC zu speichern.

10.7 Temperaturkarte

Eine Temperaturkarte zeigt den Temperaturtrend einer Region während eines bestimmten Tages an. Wenn Sie Temperaturüberwachungsregionen konfiguriert haben, können Sie eine Temperaturkarte für bestimmte Regionen erstellen, um einen Überblick über den Temperaturtrend der einzelnen Regionen zu erhalten.

Bevor Sie beginnen

- Stellen Sie sicher, dass Sie auf der Gerätekonfigurationsseite Bereiche für die Temperaturkarte eingezeichnet haben. Einzelheiten finden Sie im Benutzerhandbuch des Geräts.
- Stellen Sie sicher, dass Sie dem Client mindestens ein Gerät für die Temperaturkarte hinzugefügt haben. Siehe **Gerät hinzufügen** für Details.

Schritte

Hinweis

Diese Funktion sollte vom Gerät unterstützt werden.

1. Klicken Sie auf **Bericht** → **Temperaturkarte**.
2. Wählen Sie ein Datum aus dem Kalender aus.
3. Wählen Sie in der Liste Kamera eine Kamera aus.

Hinweis

Sie können ein Stichwort in das Suchfeld eingeben, um eine Kamera zu suchen.

4. Wählen Sie eine Einheit.
5. Wählen Sie eine Voreinstellung.

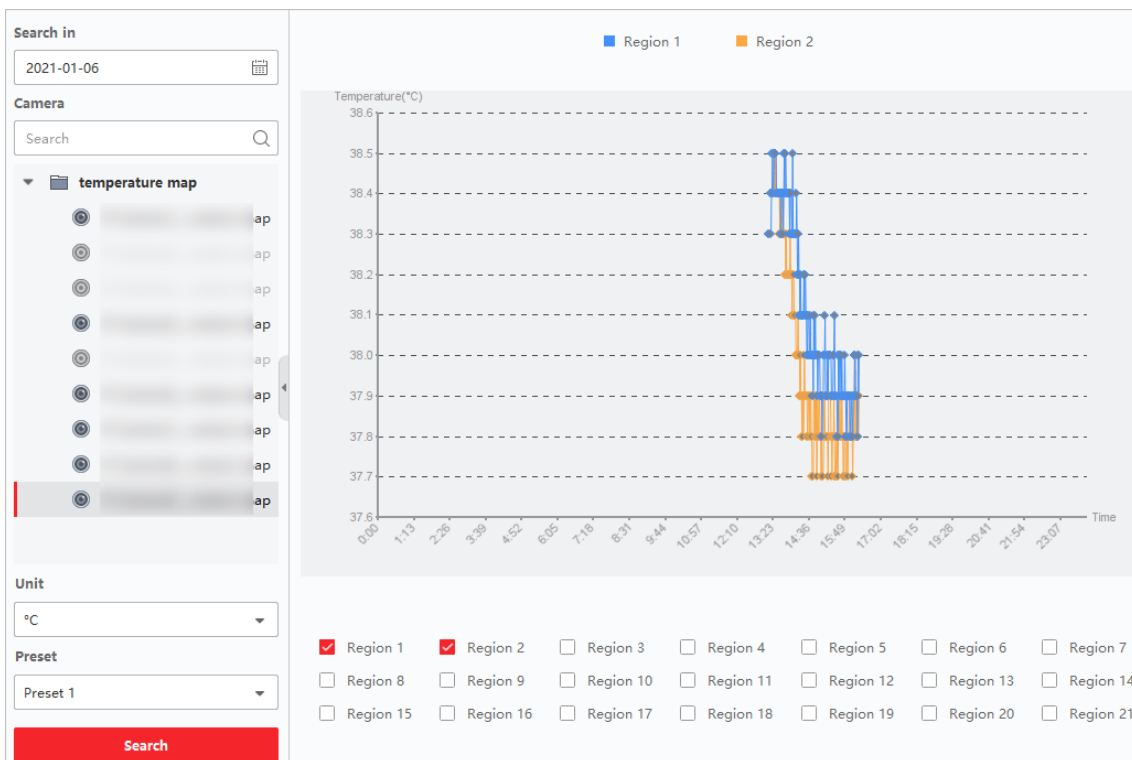


Abbildung 10-12 Temperaturkarte

6. Markieren Sie im rechten Feld die Region(en), für die der Bericht erstellt werden soll.

Hinweis

Es können nicht mehr als 8 Regionen angekreuzt werden.

7. Klicken Sie auf **Suchen**.

Die Temperaturkarte wird in einem Liniendiagramm angezeigt, wobei jede Linie eine Region

darstellt.

8. Wahlweise: Wählen Sie eine andere Einheit, um die Temperaturkarte in einer anderen Einheit anzuzeigen.

Kapitel 11 Datenabruf

Im Modul Datenabruf können Sie nach Aufzeichnungen von Autos und menschlichen Objekten suchen. Das Gerät muss die Funktion "Auto" oder "Mensch" unterstützen.


11.1 Fahrzeug-Abruf

Bei Geräten, die die Fahrzeugsuche unterstützen, können Sie die zugehörigen Fahrzeugbilder und -videos suchen, indem Sie die Suchbedingungen wie Kennzeichen und Aufnahmezeit einstellen.

Bevor Sie beginnen

Fügen Sie das Gerät, das den Fahrzeugabruf unterstützt, zum Client hinzu und konfigurieren Sie die entsprechenden Einstellungen ordnungsgemäß. Siehe **Gerät hinzufügen** für Details zum Hinzufügen des Geräts.

Schritte

1. Klicken Sie auf **Datenabruf** → **Fahrzeugabruf**, um die Seite für den Fahrzeugabruf aufzurufen.
2. Klicken Sie auf , um die Startzeit und die Endzeit für die Suche festzulegen.
3. Wählen Sie den Suchtyp.

Fahrzeug

Suche und Anzeige der erfassten Fahrzeugbilder durch Eingabe des Kfz-Kennzeichens.

Erkennung von Mischverkehr

Suchen Sie nach Bildern eines bestimmten Fahrzeugs und zeigen Sie diese an, indem Sie das Nummernschild des Fahrzeugs eingeben.

Hinweis

Die Kamera sollte die Erkennung von Mischverkehr unterstützen.

4. Wählen Sie ein Gerät aus der Kameraliste aus.
-

6. Wahlweise: Geben Sie das Nummernschild für die Suche ein (unterstützt unscharfe Suche).
7. Optional: Legen Sie die maximale Anzahl der anzuzeigenden Suchergebnisse fest.
8. Klicken Sie auf **Suchen**, um die Suche zu starten.

Die aufgenommenen Bilder, die die Suchbedingungen erfüllen, werden auf der rechten Seite angezeigt. Es können bis zu 30 Bilder auf einer Seite angezeigt werden.

9. Optional: Führen Sie bei Bedarf die folgenden Vorgänge durch.

Bild exportieren

Sie können ein oder mehrere gesuchte Bilder exportieren.


1. Klicken Sie auf **Bild exportieren**.
2. Kreuzen Sie ein oder mehrere Bilder an, oder wählen Sie auf der Seite unten **Alle auswählen**.

3. Klicken Sie auf **Exportieren**, um die ausgewählten Bilder auf den lokalen PC zu exportieren.

Details zum Capture anzeigen

Klicken Sie auf ein Bild, um die Aufnahmedetails wie Aufnahmezeit und Kameraname anzuzeigen.





Hinweis

Sie können auf  klicken, um ein vergrößertes Bild zu sehen.


Zugehöriges Video abspielen

Klicken Sie auf **Wiedergabe**, um die zum Bild gehörende Videodatei (5 Sekunden vor und 5 Sekunden nach der Aufnahme) im Ansichtsfenster abzuspielen.

Hinweis

- Sie können auf  klicken, um das Video in einem größeren Fenster zu sehen.
 - Sie können auf  klicken, um die Wiedergabegeschwindigkeit anzupassen, auf  , um die Videodatei Bild für Bild wiederzugeben, und auf  , um den Ton zu aktivieren.
-

Einzelnen Datensatz exportieren

Klicken Sie auf der Seite mit dem vergrößerten Bild auf  und dann auf **Bild exportieren**, **Videodatei exportieren** oder **Details exportieren**, um das Bild, die Videodatei und die Aufnahmedetails einer einzelnen Aufnahme auf einen lokalen PC zu exportieren.

Kapitel 14 Personenverwaltung

Sie können dem System Personeninformationen für weitere Vorgänge wie Zutrittskontrolle, Videogegensprechanlage, Zeiterfassung usw. hinzufügen. Sie können die hinzugefügten Personen verwalten, z. B. Karten in einem Stapel ausstellen, Personendaten in einem Stapel importieren und exportieren, usw.

Wichtiger Hinweis: Für die detaillierte Konfiguration z.B. für ABUS Intercom Systeme oder ABUS

Face Access Module lesen Sie bitte das entsprechende Handbuch zum passenden Produkt.

14.1 Organisation hinzufügen

Sie können eine Organisation hinzufügen und Personeninformationen in die Organisation importieren, um die Personen effektiv zu verwalten. Sie können auch eine untergeordnete Organisation für die hinzugefügte Organisation hinzufügen.


Schritte


1. Geben Sie das Modul **Person** ein.
2. Wählen Sie eine übergeordnete Organisation in der linken Spalte aus und klicken Sie auf **Hinzufügen** in der oberen linken Ecke, um eine Organisation hinzuzufügen.
3. Erstellen Sie einen Namen für die hinzugefügte Organisation.

Hinweis

Es können bis zu 10 Ebenen von Organisationen hinzugefügt werden.

4. Optional: Führen Sie die folgende(n) Operation(en) durch.

Organisation bearbeiten Bewegen Sie den Mauszeiger auf eine hinzugefügte Organisation und klicken Sie auf  , um ihren Namen zu bearbeiten.

Organisation löschen Bewegen Sie den Mauszeiger auf eine hinzugefügte Organisation und klicken Sie auf  , um sie zu löschen.

Hinweis

- Wenn Sie eine Organisation löschen, werden auch die untergeordneten Organisationen gelöscht.
 - Vergewissern Sie sich, dass keine Person unter der Organisation hinzugefügt wurde, sonst kann die Organisation nicht gelöscht werden.
-

Personen in Unterorganisation anzeigen Markieren Sie **Personen in Unterorganisationen anzeigen** und wählen Sie eine Organisation aus, um die Personen in ihren Unterorganisationen anzuzeigen.

14.2 Einzelperson hinzufügen

Sie können der Client-Software nach und nach Personen hinzufügen. Die Personeninformationen enthalten grundlegende Informationen, detaillierte Informationen, Profile,

Zugangskontrollinformationen, Berechtigungsnachweise, benutzerdefinierte Informationen, usw.

14.2.1 Grundlegende Informationen konfigurieren

Sie können dem Client eine Person nach der anderen hinzufügen und die grundlegenden Informationen der Person wie Name, E-Mail, Telefonnummer usw. konfigurieren.

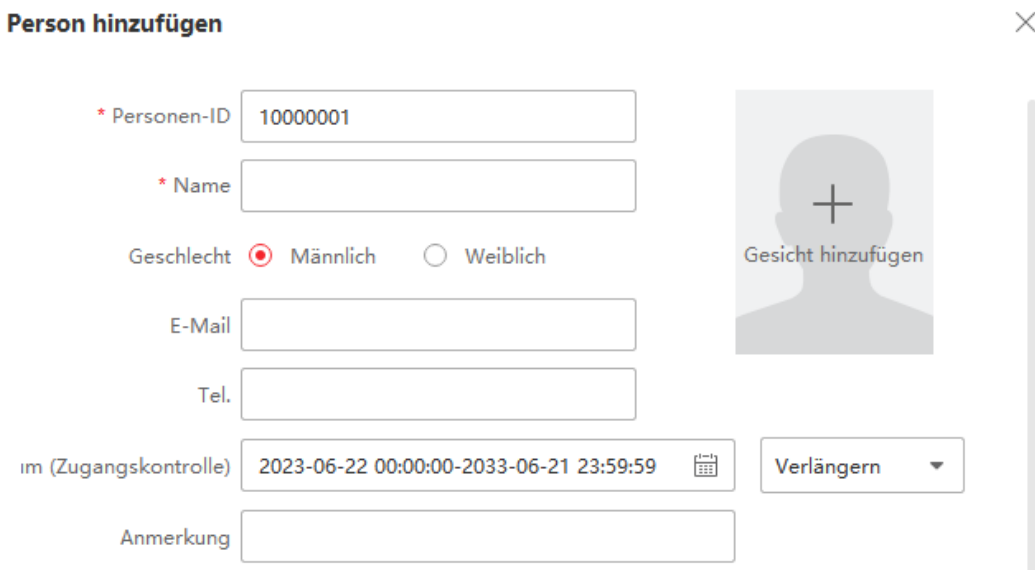
Schritte

1. Geben Sie das Modul **Person** ein.

Hinweis

Wenn Sie das Personenmodul zum ersten Mal aufrufen, erscheint ein Fenster, in dem Sie Regeln für die Generierung von Personen-IDs (Buchstaben und Zahlen unterstützt) beim Hinzufügen von Personen festlegen können. Wenn beim Abrufen von Personeninformationen vom Gerät keine Personen-IDs vorhanden sind, werden die Personen-IDs entsprechend der Regel generiert.

2. Wählen Sie eine Organisation in der Organisationsliste aus, um die Person hinzuzufügen.
3. Klicken Sie auf **Hinzufügen**, um das Fenster zum Hinzufügen von Personen zu öffnen.
Die Personen-ID wird automatisch generiert.
4. Geben Sie die grundlegenden Informationen wie Name, Telefonnummer, E-Mail-Adresse, Gültigkeitsdauer usw. ein.



Das Bild zeigt ein Dialogfenster mit dem Titel 'Person hinzufügen' und einem Schließen-Symbol (X) oben rechts. Das Fenster enthält folgende Eingabefelder und Elemente:

- * Personen-ID: Textfeld mit dem Wert '10000001'.
- * Name: Leeres Textfeld.
- Geschlecht: Radio-Knopf für 'Männlich' (aktiviert) und 'Weiblich'.
- E-Mail: Leeres Textfeld.
- Tel.: Leeres Textfeld.
- im (Zugangskontrolle): Zeitbereich '2023-06-22 00:00:00-2033-06-21 23:59:59' mit einem Kalender-Symbol und einem 'Verlängern' Button mit einem Dropdown-Pfeil.
- Anmerkung: Leeres Textfeld.
- Rechts daneben befindet sich ein Platzhalter für ein Profilbild mit einem Plus-Symbol und der Beschriftung 'Gesicht hinzufügen'.

Abbildung 14-1 Grundlegende Informationen konfigurieren

Hinweis

Wenn der Gültigkeitszeitraum abgelaufen ist, werden die Anmeldeinformationen und Zugriffskontrolleinstellungen der Person ungültig, und die Person hat keine Berechtigung für den Zugriff auf die Türen. Sie können auf **Verlängern** klicken, um die Gültigkeitsdauer der Person um 1 Monat, 3 Monate, 6 Monate oder 1 Jahr zu verlängern.

5. Bestätigen Sie, um die Person hinzuzufügen.
 - Klicken Sie auf **Hinzufügen**, um die Person hinzuzufügen, und schließen Sie das Fenster Person hinzuzufügen.
 - Klicken Sie auf **Hinzufügen und Neu**, um die Person hinzuzufügen, und fahren Sie fort, weitere Personen hinzuzufügen.
6. Registriertes Gesichtsbild löschen

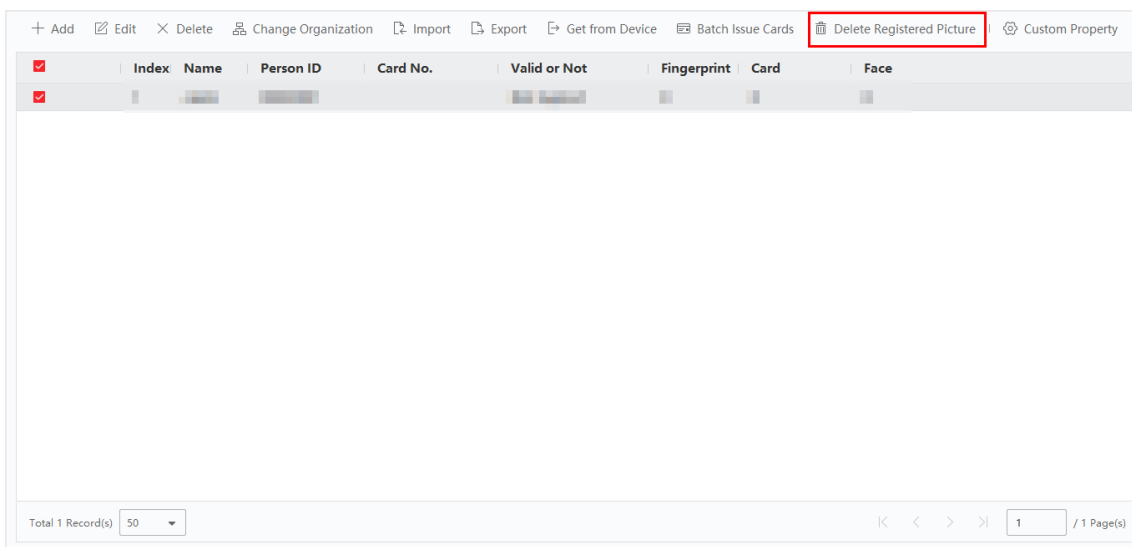


Abbildung 14-2 Registriertes Bild löschen

Hinweis

Wenn "**Bilder im Strukturdatenformat speichern**" aktiviert ist, wird die Schaltfläche "**Registriertes Bild löschen**" auf der Personenseite hinzugefügt. Im Allgemeinen wird das registrierte Gesichtsbild automatisch gelöscht, sobald die Informationen der Person auf das Gerät angewendet werden. Wenn Sie auf die Person doppelklicken, öffnet sich das Fenster **Person bearbeiten, in dem** Sie überprüfen können, ob das registrierte Gesichtsbild gelöscht wurde. Falls nicht, können Sie die Person auswählen und auf **Registriertes Bild löschen** klicken, um das Bild manuell zu löschen.

14.2.2 Ausstellung einer Karte für eine Person

Wenn Sie eine Person hinzufügen, können Sie ihr eine Karte als Zugangsberechtigung für die Tür(en) ausstellen. Bevor Sie einer Person eine Karte ausstellen, müssen Sie den Kartenausgabemodus einstellen, um die Kartenummer zu erhalten. Neben der manuellen Eingabe der Kartenummer bietet der Client auch die beiden anderen Modi zum Ablesen der Kartenummer: im lokalen Modus (über die Kartenregistrierungsstation) oder im Fernmodus (über den Kartenleser des Zutrittskontrollgeräts).

Hinweis

Es können bis zu fünf Karten an eine Person ausgegeben werden.

Ausstellen einer Karte durch Eingabe der Kartenummer


Wenn kein Gerät (Kartenerfassungsstation/Kartenleser) zum Lesen der Kartenummer zur Verfügung steht, können Sie eine Karte durch manuelle Eingabe der Kartenummer ausstellen.

Schritte

1. Geben Sie das Modul **Person** ein.
 2. Wählen Sie eine Organisation in der Organisationsliste aus, um die Person hinzuzufügen, und klicken Sie auf **Hinzufügen**, um das Fenster Person hinzufügen zu öffnen.
-

Hinweis

Geben Sie zunächst die Basisinformationen der Person ein. Einzelheiten zur Konfiguration der Basisinformationen einer Person finden Sie unter **[Basisinformationen konfigurieren](#)**.

3. Klicken Sie im Bereich **Berechtigung** → **Karte** auf  .
4. Geben Sie die Kartenummer auf der Seite "Hinzufügen" manuell ein.
5. Klicken Sie auf **Hinzufügen**.
Die Karte wird der Person ausgestellt.

Ausstellen einer Karte im lokalen Modus


Wenn eine Kartenregistrierungsstation verfügbar ist, können Sie eine Karte im lokalen Modus ausgeben. Um die Kartenummer abzulesen, müssen Sie die Kartenregistrierungsstation über die USB-Schnittstelle oder COM mit dem PC verbinden, auf dem der Client läuft, und die Karte auf die Kartenregistrierungsstation legen.

Schritte

1. Geben Sie das Modul **Person** ein.
2. Wählen Sie eine Organisation in der Organisationsliste aus, um die Person hinzuzufügen, und klicken Sie auf **Hinzufügen**, um das Fenster Person hinzufügen zu öffnen.

Hinweis

Geben Sie zunächst die Basisinformationen der Person ein. Einzelheiten zur Konfiguration der Basisinformationen einer Person finden Sie unter **[Basisinformationen konfigurieren](#)**.

3. Klicken Sie im Bereich **Berechtigung** → **Karte** auf  .
4. Klicken Sie auf **Einstellungen**, um die Seite Einstellungen aufzurufen.
5. Wählen Sie **Lokal** als Kartenausgabemodus.
6. Stellen Sie andere zugehörige Parameter ein.

Station für die Kartenregistrierung

Wählen Sie ein Modell der Kartenregistrierungsstation aus der Dropdown-Liste. Sie können die Kartenregistrierungsstation an den PC anschließen und die grundlegenden Informationen über die hinzugefügte Person über USB zwischen den beiden Geräten übertragen.

Karte Typ

Wählen Sie den Kartentyp als EM-Karte oder Mifare-Karte entsprechend dem tatsächlichen Kartentyp.

Brummen

Aktivieren oder deaktivieren Sie den Signalton, wenn die Kartenummer erfolgreich gelesen wurde.

Karte Nr. Typ

Wählen Sie die Art der Kartenummer entsprechend den tatsächlichen Bedürfnissen.

M1 Kartenverschlüsselung

Wenn es sich um eine M1-Karte handelt, können Sie die Funktion M1-Kartenverschlüsselung aktivieren und den zu verschlüsselnden Sektor der Karte auswählen.

7. Klicken Sie auf **OK**, um den Vorgang zu bestätigen.
8. Legen Sie die Karte auf die Kartenerfassungsstation und klicken Sie auf **Lesen**, um die Kartenummer abzurufen.
Die Kartenummer wird automatisch im Feld Karten-Nr. angezeigt.
9. Klicken Sie auf **Hinzufügen**.
Die Karte wird der Person ausgestellt.

Ausstellen einer Karte im Remote-Modus

Abgesehen von der Ausgabe einer Karte im lokalen Modus können Sie die Karte auch über den Kartenleser des hinzugefügten Zugangskontrollgeräts ziehen, um die Kartenummer zu erhalten. Dies ist möglich, wenn sich der Kunde und die Personen, die Karten ausstellen müssen, nicht am selben Ort befinden. So können Sie z. B. Karten für Mitarbeiter in einer Zweigstelle im Remote-Modus über den Client ausgeben.

Schritte

1. Geben Sie das Modul **Person** ein.

2. Wählen Sie eine Organisation in der Organisationsliste aus, um die Person hinzuzufügen, und klicken Sie auf **Hinzufügen**, um den Bereich Person hinzuzufügen zu öffnen.

Hinweis

Geben Sie zunächst die Basisinformationen der Person ein. Einzelheiten zur Konfiguration der Basisinformationen einer Person finden Sie unter **[Basisinformationen konfigurieren](#)**.

3. Klicken Sie im Bereich **Berechtigung** → **Karte** auf **+** .
4. Klicken Sie auf **Einstellungen**, um die Seite Einstellungen aufzurufen.
5. Wählen Sie **Kartenleser** als Kartenausgabemodus.
6. Wählen Sie ein im Client hinzugefügtes Zugangskontrollgerät aus.
7. Wählen Sie ein hinzugefügtes Zutrittskontrollgerät oder die Anmeldestation aus der Dropdown-Liste aus.

Hinweis

- Wenn Sie ein Zugangskontrollgerät auswählen, stellen Sie sicher, dass Sie die Geräte aktiviert haben.
 - Wenn Sie die Anmeldestation auswählen, sollten Sie auf **Anmelden** klicken, um die entsprechenden Parameter des Geräts wie IP-Adresse, Portnummer, Benutzername und Kennwort einzustellen. Außerdem sollten Sie den/die RF-Kartentyp(en) nach Bedarf überprüfen.
-

8. Klicken Sie auf **OK**, um den Vorgang zu bestätigen.
9. Legen Sie die Karte auf den Kartenleser und klicken Sie auf **Lesen**, um die Kartenummer abzurufen.
Die Kartenummer wird automatisch im Feld Karten-Nr. angezeigt.
10. Klicken Sie auf **Hinzufügen**.
Die Karte wird der Person ausgestellt.

14.2.3 Hochladen eines Gesichtsfotos vom lokalen PC

Wenn Sie eine Person hinzufügen, können Sie ein auf dem lokalen PC gespeichertes Gesichtsfoto als Profil der Person in den Client hochladen.

Schritte

1. Geben Sie das Modul **Person** ein.
2. Wählen Sie eine Organisation in der Organisationsliste aus, um die Person hinzuzufügen, und klicken Sie auf **Hinzufügen**.

Hinweis

Geben Sie zunächst die Basisinformationen der Person ein. Einzelheiten zur Konfiguration der Basisinformationen einer Person finden Sie unter **[Basisinformationen konfigurieren](#)**.

3. Klicken Sie im Bereich Basisinformationen auf **Gesicht hinzufügen**.
4. Wählen Sie **Hochladen**.
5. Wählen Sie ein Bild von dem PC aus, auf dem der Client läuft.

Hinweis

Das Bild sollte im JPG- oder JPEG-Format vorliegen und kleiner als 200 KB sein.

6. Optional: Aktivieren Sie **Verify by Device**, um zu prüfen, ob das im Client verwaltete Gesichtserkennungsgerät das Gesicht auf dem Foto erkennen kann.

Hinweis

Diese Funktion wird je nach Kapazität des Geräts ein- oder ausgeblendet.

7. Bestätigen Sie, um die Person hinzuzufügen.
 - Klicken Sie auf **Hinzufügen**, um die Person hinzuzufügen, und schließen Sie das Fenster Person hinzufügen.
 - Klicken Sie auf **Hinzufügen und Neu**, um die Person hinzuzufügen und fahren Sie fort, weitere Personen hinzuzufügen.

14.2.4 Ein Foto über den Client aufnehmen

Wenn Sie eine Person hinzufügen, können Sie ein Foto der Person mit der integrierten Kamera des Clients, der USB-Kamera oder der Anmeldestation aufnehmen und dieses Foto als Profil der Person festlegen.

Bevor Sie beginnen

Stellen Sie sicher, dass der PC, auf dem der Client läuft, eine der folgenden Bedingungen erfüllt:

- Der Kunde hat eine Kamera.
- Sie haben eine USB-Kamera an den PC angeschlossen.
- Sie haben die Enrollment Station über die USB-Schnittstelle mit dem PC verbunden.

Schritte

1. Geben Sie das Modul **Person** ein.
2. Wählen Sie eine Organisation in der Organisationsliste aus, um die Person hinzuzufügen, und klicken Sie auf **Hinzufügen**, um das Fenster Person hinzufügen zu öffnen.

Hinweis

Geben Sie zunächst die Basisinformationen der Person ein. Weitere Informationen finden Sie unter **Grundlegende Informationen konfigurieren**.

3. Klicken Sie im Bereich Basisinformationen auf **Gesicht hinzufügen**.
4. Wählen Sie **Foto aufnehmen**, um das Fenster Foto aufnehmen aufzurufen.
5. Klicken Sie auf ▾ , um die integrierte Kamera oder die Anmeldestation aus der Dropdown-Liste auszuwählen.
6. Optional: Aktivieren Sie die Option **Nach Gerät überprüfen**, um zu prüfen, ob das aufgenommene Gesichtsfoto die Anforderungen für das Hochladen erfüllt.

Hinweis

Diese Funktion wird je nach Kapazität des Geräts ein- oder ausgeblendet.



7. Machen Sie ein Foto.
 - 1) Blicken Sie in die Kamera und achten Sie darauf, dass sich Ihr Gesicht in der Mitte des Aufnahmefensters befindet.
 - 2) Klicken Sie auf  , um ein Gesichtsfoto aufzunehmen.
 - 3) Optional: Klicken Sie auf  , um erneut zu erfassen.
 - 4) Klicken Sie auf **OK**, um das aufgenommene Foto zu speichern.

Abbildung 14-3 Ein Foto über den Client aufnehmen

8. Bestätigen Sie, um die Person hinzuzufügen.
 - Klicken Sie auf **Hinzufügen**, um die Person hinzuzufügen, und schließen Sie das Fenster Person hinzufügen.
 - Klicken Sie auf **Hinzufügen und Neu**, um die Person hinzuzufügen, und fahren Sie fort, weitere Personen hinzuzufügen.

14.2.5 Gesicht über Zutrittskontrollgerät erfassen

Wenn Sie eine Person hinzufügen, können Sie das Gesicht der Person über ein Zugangskontrollgerät erfassen, das dem Client hinzugefügt wurde und die Funktion der Gesichtserkennung unterstützt.

Schritte

1. Geben Sie das Modul **Person** ein.
2. Wählen Sie eine Organisation in der Organisationsliste aus, um die Person hinzuzufügen, und klicken Sie auf **Hinzufügen**.

Hinweis

Geben Sie zunächst die Basisinformationen der Person ein. Einzelheiten zur Konfiguration der Basisinformationen einer Person finden Sie unter **[Basisinformationen konfigurieren](#)**.

3. Klicken Sie im Bereich Basisinformationen auf **Gesicht hinzufügen**.
4. Wählen Sie **Fernabholung**.

5. Wählen Sie ein hinzugefügtes Zutrittskontrollgerät oder die Anmeldestation aus der Dropdown-Liste aus.

Hinweis

Wenn Sie die Anmeldestation auswählen, sollten Sie auf **Anmelden** klicken, um die entsprechenden Parameter des Geräts wie IP-Adresse, Portnummer, Benutzername und Kennwort festzulegen. Außerdem können Sie **Face Anti-Spoofing** prüfen und die Aktivitätsstufe **Niedrig**, **Mittel** oder **Hoch** wählen.

Gesicht Anti-Spoofing


Wenn Sie diese Funktion aktivieren, kann das Gerät erkennen, ob das zu erfassende Gesicht echt ist.

6. Optional: Klicken Sie auf **Kartenleser**, wählen Sie die ID des Kartenlesers und klicken Sie auf **OK**.

Hinweis

Diese Funktion sollte vom Gerät unterstützt werden.

7. Gesicht sammeln.

- 1) Stellen Sie sich vor die Kamera des ausgewählten Zugangskontrollgeräts und achten Sie darauf, dass sich Ihr Gesicht in der Mitte des Erfassungsfensters befindet.
- 2) Klicken Sie auf  , um ein Foto aufzunehmen.
- 3) Klicken Sie auf **OK**, um das aufgenommene Foto zu speichern.


8. Bestätigen Sie, um die Person hinzuzufügen.

- Klicken Sie auf **Hinzufügen**, um die Person hinzuzufügen, und schließen Sie das Fenster **Person hinzufügen**.
- Klicken Sie auf **Hinzufügen und Neu**, um die Person hinzuzufügen und fahren Sie fort, weitere Personen hinzuzufügen.

14.2.10 Konfigurieren der Zugriffskontrollinformationen

Wenn Sie eine Person hinzufügen, können Sie deren Zugangskontrollinformationen festlegen, z. B. eine Zugangskontrollgruppe mit der Person verbinden, den PIN-Code konfigurieren, die Person als Besucher, Blocklistenperson oder Superuser festlegen usw.

Schritte

1. Geben Sie das Modul **Person** ein.
2. Wählen Sie eine Organisation in der Organisationsliste aus, um die Person hinzuzufügen, und klicken Sie auf **Hinzufügen**.
3. Klicken Sie im Bereich **Zugriffskontrolle** auf  , um die Zugriffsgruppe(n) für die Person auszuwählen.

 **Hinweis**

Einzelheiten finden Sie unter **Zugriffsgruppe festlegen, um Personen eine Zugriffsberechtigung zuzuweisen.**

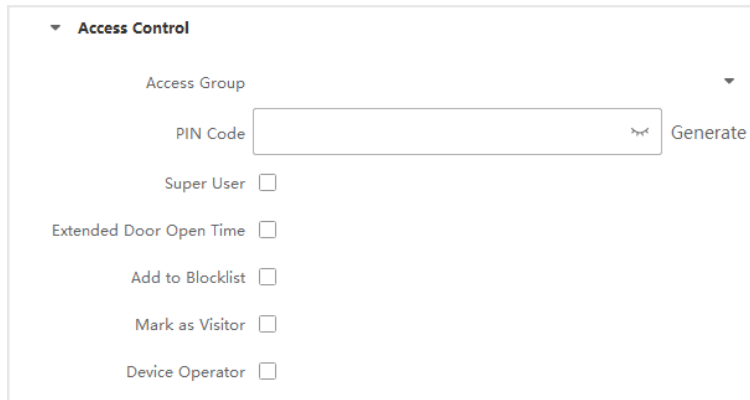


Abbildung 14-4 Konfigurieren der Zugriffskontrollinformationen

4. Legen Sie einen eindeutigen PIN-Code für die Person fest, der für die Zugangsauthentifizierung verwendet werden kann.
- Geben Sie manuell einen PIN-Code mit 4 bis 8 Ziffern ein.

 **Hinweis**

Die PIN-Codes der Personen können nicht wiederholt werden.

- Klicken Sie auf **Erzeugen**, um einen 6-stelligen, nicht wiederholten PIN-Code nach dem Zufallsprinzip zu erzeugen.

 **Hinweis**

Bei wiederholten PIN-Codes wird auf dem Client eine Aufforderung angezeigt. Der Administrator kann einen neuen PIN-Code generieren, um den wiederholten PIN-Code zu ersetzen und die betroffenen Personen zu benachrichtigen.

5. Überprüfen Sie die Betriebserlaubnis der Person.

Super-Benutzer

Wenn die Person als Superuser eingestellt ist, hat sie die Berechtigung, alle Türen/Etagen zu betreten und ist von den übrigen Schließungsbeschränkungen, allen Anti-Passback-Regeln und der Berechtigung der ersten Person ausgenommen.

Verlängerte Türöffnungszeit

Verwenden Sie diese Funktion für Personen mit eingeschränkter Mobilität. Beim Zugang zur Tür hat die Person mehr Zeit als andere, um die Türen zu passieren.

Einzelheiten zum Einstellen der Öffnungsdauer der Tür finden Sie unter **Konfigurieren der Parameter für Tür/Aufzug**.

Zur Blockliste hinzufügen

Fügen Sie die Person der Sperrliste hinzu, und wenn die Person versucht, sich Zugang zu Türen/Etagen zu verschaffen, wird ein Ereignis ausgelöst und an den Client gesendet, um das Sicherheitspersonal zu benachrichtigen.

Als Besucher markieren

Wenn die Person ein Besucher ist, sollten Sie die für sie geltenden Besuchszeiten festlegen.

Hinweis

Die gültigen Zeiten für den Besuch liegen zwischen 1 und 100. Sie können auch **Kein Limit** ankreuzen, dann gibt es für den Besucher keine begrenzten Zeiten für den Zugang zu Türen/Etagen.

Gerät Operator

Die Person mit der Rolle des Gerätebedieners ist berechtigt, die Zugangskontrollgeräte zu bedienen.

Hinweis

Die Funktionen Superuser, Erweiterte Türöffnungszeit, Zur Blockliste hinzufügen und Als Besucher markieren können nicht gleichzeitig aktiviert werden. Wenn z. B. eine Person als Superuser eingestellt ist, können Sie für sie nicht die erweiterte Türöffnungszeit aktivieren, sie zur Blockliste hinzufügen oder sie als Besucher markieren.

6. Bestätigen Sie, um die Person hinzuzufügen.
 - Klicken Sie auf **Hinzufügen**, um die Person hinzuzufügen, und schließen Sie das Fenster Person hinzufügen.
 - Klicken Sie auf **Hinzufügen und Neu**, um die Person hinzuzufügen, und fahren Sie fort, weitere Personen hinzuzufügen.

14.2.11 Anpassen von Personeninformationen

Sie können die Personeneigenschaften, die im Client nicht vordefiniert sind, an Ihre tatsächlichen Bedürfnisse anpassen, z. B. den Geburtsort. Nach dem Anpassen können Sie beim Hinzufügen einer Person die benutzerdefinierten Informationen eingeben, um die Personendaten zu vervollständigen.

Schritte

1. Geben Sie das Modul **Person** ein.
2. Legen Sie die Felder für die benutzerdefinierten Informationen fest.
 - 1) Klicken Sie auf **Benutzerdefinierte Eigenschaft**.
 - 2) Klicken Sie auf **Hinzufügen**, um eine neue Eigenschaft hinzuzufügen.

- 3) Geben Sie den Eigenschaftsnamen ein.
 - 4) Klicken Sie auf **OK**.
3. Legen Sie die benutzerdefinierten Informationen fest, wenn Sie eine Person hinzufügen.
- 1) Wählen Sie eine Organisation in der Organisationsliste aus, um die Person hinzuzufügen, und klicken Sie auf **Hinzufügen**.
-

 **Hinweis**

Geben Sie zunächst die Basisinformationen der Person ein. Einzelheiten zur Konfiguration der Basisinformationen einer Person finden Sie unter **Basisinformationen konfigurieren**.

- 2) Geben Sie im Bereich **Benutzerdefinierte Informationen** die Informationen zur Person ein.
- 3) Klicken Sie auf **Hinzufügen**, um die Person hinzuzufügen und das Fenster Person hinzufügen zu schließen, oder klicken Sie auf **Hinzufügen und Neu**, um die Person hinzuzufügen und mit dem Hinzufügen anderer Personen fortzufahren.

14.2.12 Anwohnerinformationen konfigurieren

Wenn es sich bei der Person um einen Bewohner handelt, müssen Sie für die Video-Gegensprechanlage die Zimmernummer für ihn/sie festlegen und eine Innenstation binden. Nach dem Einbinden können Sie diese Person anrufen, indem Sie die Innenstation anrufen und mit ihr eine Video-Gegensprechverbindung herstellen.

Schritte

1. Geben Sie das Modul **Person** ein.
 2. Wählen Sie eine Organisation in der Organisationsliste aus, um die Person hinzuzufügen, und klicken Sie auf **Hinzufügen**.
-

 **Hinweis**

Geben Sie zunächst die Basisinformationen der Person ein. Einzelheiten zur Konfiguration der Basisinformationen einer Person finden Sie unter **Basisinformationen konfigurieren**.

3. Wählen Sie im Bereich **Bewohnerinformationen** die Innenstation aus, um sie mit der Person zu verbinden.
-

 **Hinweis**

Wenn Sie **Analoge Innenstation** wählen, wird das Feld **Türstation** angezeigt und Sie müssen die Türstation auswählen, die mit der analogen Innenstation kommunizieren soll.

4. Geben Sie die Etagen- und Zimmernummer der Person ein.
 5. Bestätigen Sie, um die Person hinzuzufügen.
 - Klicken Sie auf **Hinzufügen**, um die Person hinzuzufügen, und schließen Sie das Fenster Person hinzufügen.
 - Klicken Sie auf **Hinzufügen und Neu**, um die Person hinzuzufügen, und fahren Sie fort,
-

weitere Personen hinzuzufügen.

14.2.13 Zusätzliche Informationen konfigurieren

Wenn Sie eine Person hinzufügen, können Sie die zusätzlichen Informationen für die Person konfigurieren, wie z. B. den Identitätstyp, die Identitätsnummer, das Land usw., je nach Bedarf.

Schritte

1. Geben Sie das Modul **Person** ein.
2. Wählen Sie eine Organisation in der Organisationsliste aus, um die Person hinzuzufügen, und klicken Sie auf **Hinzufügen**.

Hinweis

Geben Sie zunächst die Basisinformationen der Person ein. Einzelheiten zur Konfiguration der Basisinformationen einer Person finden Sie unter **Basisinformationen konfigurieren**.

3. Geben Sie im Feld "**Zusätzliche Informationen**" die zusätzlichen Informationen zur Person ein, z. B. den ID-Typ, die ID-Nr., die Berufsbezeichnung usw., je nach Bedarf.
4. Bestätigen Sie, um die Person hinzuzufügen.
 - Klicken Sie auf **Hinzufügen**, um die Person hinzuzufügen, und schließen Sie das Fenster Person hinzufügen.
 - Klicken Sie auf **Hinzufügen und Neu**, um die Person hinzuzufügen und fahren Sie fort, weitere Personen hinzuzufügen.

14.3 Import und Export von personenidentifizierenden Informationen

Sie können die Informationen und Bilder mehrerer Personen in einem Stapel in die Client-Software importieren. In der Zwischenzeit können Sie die Personendaten und Bilder auch exportieren und auf Ihrem PC speichern.

14.3.1 Personendaten importieren

Sie können die Informationen mehrerer Personen in eine vordefinierte Vorlage (CSV/Excel-Datei) eingeben, um die Informationen in einem Stapel in den Client zu importieren.

Schritte

1. Geben Sie das Modul Person ein.
2. Wählen Sie eine hinzugefügte Organisation in der Liste aus, oder klicken Sie auf **Hinzufügen** in der oberen linken Ecke, um eine Organisation hinzuzufügen, und wählen Sie sie dann aus.
3. Klicken Sie auf **Importieren**, um das Fenster Importieren zu öffnen.
4. Wählen Sie **Personendaten** als Importmodus.

5. Klicken Sie auf **Vorlage für den Import von Personen herunterladen**, um die Vorlage herunterzuladen.
6. Geben Sie die Personendaten in die heruntergeladene Vorlage ein.

Hinweis

- Wenn die Person mehrere Karten hat, trennen Sie die Kartenummer mit einem Semikolon.
 - Die mit einem Sternchen versehenen Angaben sind erforderlich.
 - Standardmäßig wird als Einstellungsdatum das aktuelle Datum verwendet.
-

7. Klicken Sie auf **...**, um die CSV/Excel-Datei mit den Personeninformationen vom lokalen PC auszuwählen.
8. Klicken Sie auf **Importieren**, um den Import zu starten.

Hinweis

- Wenn eine Personnummer bereits in der Datenbank des Kunden vorhanden ist, löschen Sie die vorhandenen Informationen vor dem Import.
 - Sie können die Daten von höchstens 2.000 Personen importieren.
-

14.3.2 Personenbilder importieren

Nach dem Import von Gesichtsbildern für die hinzugefügten Personen in den Client können die Personen auf den Bildern durch ein hinzugefügtes Gesichtserkennungsterminal identifiziert werden. Sie können die Personenbilder entweder einzeln oder mehrere Bilder auf einmal importieren, je nach Bedarf.

Bevor Sie beginnen

Vergewissern Sie sich, dass Sie dem Kunden vorher Informationen über die Person geliefert haben.

Schritte

1. Geben Sie das Modul Person ein.
2. Wählen Sie eine hinzugefügte Organisation in der Liste aus, oder klicken Sie auf **Hinzufügen** in der oberen linken Ecke, um eine Organisation hinzuzufügen, und wählen Sie sie dann aus.
3. Klicken Sie auf **Importieren**, um das Fenster Importieren zu öffnen und das **Gesicht zu** überprüfen.
4. Optional: Aktivieren Sie **Verify by Device**, um zu prüfen, ob das auf dem Client verwaltete Gesichtserkennungsgerät das Gesicht auf dem Foto erkennen kann.
5. Klicken Sie auf **...**, um eine Gesichtsbilddatei auszuwählen.

Hinweis

- Der (Ordner mit) Gesichtsbildern sollte im ZIP-Format vorliegen.
 - Jede Bilddatei sollte im JPG-Format vorliegen und nicht größer als 200 KB sein.
 - Jede Bilddatei sollte als "Person ID_Name" benannt werden. Die Personen-ID sollte mit derjenigen der importierten Personendaten übereinstimmen.
-

6. Klicken Sie auf **Importieren**, um den Import zu starten.
Der Fortschritt und das Ergebnis des Imports werden angezeigt.

14.3.3 Informationen zur Person exportieren

Sie können die Informationen der hinzugefügten Personen als CSV/Excel-Datei auf einen lokalen PC exportieren.

Bevor Sie beginnen

- Stellen Sie sicher, dass Sie Personen zu einer Organisation hinzugefügt haben.
- Vergewissern Sie sich, dass Sie die Funktion **Personendaten exportieren** aktiviert haben, damit die Schaltfläche **Exportieren** angezeigt wird. Weitere Informationen finden Sie unter **Allgemeine Parameter festlegen**.

Schritte

1. Geben Sie das Modul Person ein.
2. Wahlweise: Wählen Sie eine Organisation aus der Liste aus.



Wenn Sie keine Organisation auswählen, werden die Informationen aller Personen exportiert.

3. Klicken Sie auf **Exportieren**.
4. Geben Sie den Superuser-Namen und das Passwort zur Überprüfung ein.
Das Fenster Exportieren wird angezeigt.
5. Markieren Sie **Personeninformationen** als zu exportierenden Inhalt.
6. Markieren Sie die gewünschten zu exportierenden Elemente.
7. Klicken Sie auf **Exportieren**, um die exportierte Datei als CSV/Excel-Datei auf Ihrem PC zu speichern.

14.3.4 Personenbilder exportieren

Sie können die Gesichtsbilddatei der hinzugefügten Personen exportieren und auf Ihrem PC speichern.

Bevor Sie beginnen

- Vergewissern Sie sich, dass Sie Personen und deren Gesichtsbilder zu einer Organisation hinzugefügt haben.
- Vergewissern Sie sich, dass Sie die Funktion **Personendaten exportieren** aktiviert haben, damit die Schaltfläche **Exportieren** angezeigt wird. Weitere Informationen finden Sie unter **Allgemeine Parameter festlegen**.

Schritte

1. Geben Sie das Modul Person ein.
2. Wahlweise: Wählen Sie eine Organisation aus der Liste aus.

 **Hinweis**

Wenn Sie keine Organisation auswählen, werden die Gesichtsbilder aller Personen exportiert.

3. Klicken Sie in der oberen Menüleiste auf **Exportieren**.
 4. Geben Sie den Superuser-Namen und das Passwort zur Überprüfung ein.
Das Fenster Exportieren wird angezeigt.
 5. Markieren Sie **Gesicht** als den zu exportierenden Inhalt.
 6. Klicken Sie auf **Exportieren** und legen Sie einen Verschlüsselungscode fest, um die exportierte Datei zu verschlüsseln.
-

 **Hinweis**

- Die exportierte Datei liegt im ZIP-Format vor.
 - Das exportierte Gesichtsbild wird als "Person ID_Name_0" bezeichnet
-

14.4 Abrufen von Personeninformationen vom Zutrittskontrollgerät

Wenn das Zutrittskontrollgerät mit Personeninformationen konfiguriert wurde (einschließlich Personendaten, Fingerabdruck und Karteninformationen), können Sie die Personeninformationen von dem hinzugefügten Gerät abrufen und für weitere Vorgänge in den Client importieren.

Schritte

 **Hinweis**

- Wenn der im Gerät gespeicherte Personennamen leer ist, wird der Personennamen nach dem Importieren in den Client mit der ausgestellten Kartennummer gefüllt.
 - Personen werden standardmäßig **männlich** sein.
 - Wenn die auf dem Gerät gespeicherte Kartennummer oder Personen-ID (Mitarbeiter-ID) bereits in der Client-Datenbank vorhanden ist, wird die Person mit dieser Kartennummer oder Personen-ID nicht in den Client importiert.
-

1. Geben Sie das Modul **Person** ein.
 2. Wählen Sie eine Organisation aus, um die Personen zu importieren.
 3. Klicken Sie auf **Vom Gerät holen**.
 4. Wählen Sie ein hinzugefügtes Zutrittskontrollgerät oder die Anmeldestation aus der Dropdown-Liste aus.
-

 **Hinweis**

Wenn Sie die Anmeldestation auswählen, sollten Sie auf **Login** klicken und IP-Adresse, Portnummer, Benutzername und Passwort des Geräts eingeben.

5. Wählen Sie den **Abrufmodus**.

 **Hinweis**

Der Abrufmodus variiert je nach Gerät. Das Zutrittskontrollgerät unterstützt das Abrufen von Personeninformationen über die Mitarbeiter-ID. Es können jeweils bis zu 5 Mitarbeiter-IDs angegeben werden.

6. Klicken Sie auf **Importieren**, um den Import der Personendaten in den Client zu starten.

 **Hinweis**

Es können bis zu 2.000 Personen und 5.000 Karten importiert werden.

Die Personendaten, einschließlich der Personendetails, der Fingerabdruckdaten der Person (falls konfiguriert) und der verknüpften Karten (falls konfiguriert), werden in die ausgewählte Organisation importiert.

14.5 Personen zu einer anderen Organisation versetzen

Sie können die hinzugefügten Personen bei Bedarf in eine andere Organisation verschieben.

Bevor Sie beginnen

- Stellen Sie sicher, dass Sie mindestens zwei Organisationen hinzugefügt haben.
- Vergewissern Sie sich, dass Sie die Personendaten importiert haben.

Schritte

1. Geben Sie das Modul **Person** ein.
2. Wählen Sie im linken Bereich eine Organisation aus.
Die Personen, die der Organisation unterstehen, werden im rechten Bereich angezeigt.
3. Wählen Sie die zu verschiebende Person aus.
4. Klicken Sie auf **Organisation ändern**.
5. Wählen Sie die Organisation aus, in die Personen verschoben werden sollen.
6. Klicken Sie auf **OK**.

14.6 Ausgabe von Karten an Personen im Stapel

Der Client bietet eine bequeme Möglichkeit, Karten an mehrere Personen in einem Stapel auszugeben.

Schritte


1. Geben Sie das Modul **Person** ein.
2. Klicken Sie auf **Karten im Stapel ausgeben**.
Alle hinzugefügten Personen, für die keine Karte ausgestellt wurde, werden im rechten Feld angezeigt.


3. Wahlweise: Geben Sie Schlüsselwörter (Name oder Personen-ID) in das Eingabefeld ein, um die Person(en) herauszufiltern, die Karten ausstellen müssen.
4. Optional: Klicken Sie auf **Einstellungen**, um die Parameter für die Kartenausgabe festzulegen. Einzelheiten finden Sie unter ***Eine Karte an eine Person ausgeben***.
5. Klicken Sie auf **Initialisieren**, um die Kartenerfassungsstation oder den Kartenleser zu initialisieren, damit sie für die Ausgabe von Karten bereit sind.
6. Klicken Sie auf die Spalte **Karten-Nr.** und geben Sie die Kartenummer ein.
 - Legen Sie die Karte auf die Kartenerfassungsstation.
 - Ziehen Sie die Karte über den Kartenleser.
 - Geben Sie die Kartenummer von Hand ein und drücken Sie die Eingabetaste.Die in der Liste aufgeführte(n) Person(en) erhält/erhalten eine Karte.

14.7 Berichtskarte Verlust

Wenn die Person ihre Karte verloren hat, können Sie den Verlust der Karte melden, damit die zugehörige Zugangsberechtigung inaktiv wird.

Schritte

1. Geben Sie das Modul **Person** ein.
2. Wählen Sie die Person aus, für die Sie den Kartenverlust melden möchten, und klicken Sie auf **Bearbeiten**, um das Fenster Person bearbeiten zu öffnen.
3. Klicken Sie im Fenster **Berechtigungsnachweis** → **Karte** auf  , um die hinzugefügte Karte als verlorene Karte zu kennzeichnen.

Nach der Meldung des Kartenverlustes wird die Zugangsberechtigung dieser Karte ungültig und inaktiv. Eine andere Person, die diese Karte erhält, kann die Türen nicht durch Durchziehen dieser verlorenen Karte öffnen.
4. Optional: Wenn die verlorene Karte gefunden wird, können Sie auf  klicken, um den Verlust zu stornieren.

Nach der Löschung des Kartenverlustes bleibt die Zugangsberechtigung der Person gültig und aktiv.
4. Wenn die verlorene Karte einer Zutrittsgruppe hinzugefügt wurde und die Zutrittsgruppe bereits auf das Gerät angewendet wurde, erscheint nach der Meldung des Kartenverlusts oder der Stornierung des Kartenverlusts ein Fenster, das Sie auffordert, die Änderungen auf das Gerät anzuwenden. Nach der Anwendung auf das Gerät können diese Änderungen auf dem Gerät wirksam werden.

14.8 Ressourcenstatistiken anzeigen

Nachdem Sie Personen und Zugangskontrolldaten (einschließlich Gesichter, Karten und Fingerabdrücke) auf das Gerät angewendet haben, können Sie Ressourcenstatistiken auf dem Client und auf dem Gerät anzeigen, um zu erfahren, ob die Ressourcen erfolgreich angewendet wurden.

Sie haben dem Gerät Personen und Berechtigungsnachweise zugewiesen. Einzelheiten finden Sie unter **Zugriffsgruppe festlegen, um Personen eine Zugriffsberechtigung zuzuweisen**.

Klicken Sie auf **Personenverwaltung** → **Ressourcenstatistik**, um das Fenster Ressourcenstatistik zu öffnen.

Abbildung 14-5 Übersicht auf dem Client

Wählen Sie im Bereich **Übersicht auf dem Gerät** ein Gerät aus der Dropdown-Liste aus, und klicken Sie auf **Zählen**, um die Geräteressourcen einschließlich Personen, Gesichter, Karten und Fingerabdrücke anzuzeigen. Durch den Vergleich der Ressourcen auf dem Client und auf dem Gerät können Sie feststellen, ob die Client-Ressourcen auf das Gerät angewendet wurden.

Abbildung 14-6 Auf das Gerät angewendete Client-Ressourcen



Hinweis

Diese Funktion sollte vom Gerät unterstützt werden. Wenn das Gerät die Gesichts- oder Fingerabdruckerkennung nicht unterstützt, wird in der unteren rechten Ecke des PC-Desktops eine Aufforderung angezeigt.

Kapitel 15 Zugangskontrolle

Das Zutrittskontrollmodul ist für Zutrittskontrollgeräte und Videosprechanlagen geeignet. Es bietet mehrere Funktionen, darunter die Konfiguration von Zutrittsgruppen, Video-Gegensprechanlagen und andere erweiterte Funktionen.

Hinweis

Benutzer mit Zugriffskontrollmodul-Berechtigungen können das Zugriffskontrollmodul aufrufen und die Zugriffskontrolleinstellungen konfigurieren. Informationen zum Einstellen der Benutzerberechtigung für das Zugriffskontrollmodul finden Sie unter **Benutzer hinzufügen**.

15.2 Zeitplan und Vorlage konfigurieren

Sie können die Vorlage einschließlich Urlaubs- und Wochenplan konfigurieren. Nach der Einstellung der Vorlage können Sie die konfigurierte Vorlage bei der Einstellung der Zutrittsgruppen übernehmen, so dass die Zutrittsgruppe in den Zeiträumen der Vorlage wirksam wird.

Hinweis

Die Einstellungen für die Zugriffsgruppen finden Sie unter **Zugriffsgruppe festlegen, um Personen eine Zugriffsberechtigung zuzuweisen**.

15.2.1 Urlaub hinzufügen

Sie können Feiertage erstellen und die Tage in den Feiertagen festlegen, einschließlich des Start- und Enddatums und der Dauer des Feiertags an einem Tag.

Schritte

Hinweis

Sie können bis zu 64 Feiertage in das Softwaresystem aufnehmen.

1. Klicken Sie auf **Zugriffskontrolle** → **Zeitplan** → **Urlaub**, um die Seite Urlaub aufzurufen.
 2. Klicken Sie im linken Bereich auf **Hinzufügen**.
 3. Erfinden Sie einen Namen für den Feiertag.
 4. Wahlweise: Geben Sie in das Feld Bemerkung die Beschreibungen oder einige Hinweise zu diesem Feiertag ein.
 5. Fügen Sie einen Urlaubszeitraum zur Urlaubsliste hinzu und konfigurieren Sie die Urlaubsdauer.
-






Hinweis

Einem Urlaub können bis zu 16 Urlaubszeiträume hinzugefügt werden.

- 1) Klicken Sie im Feld Urlaubsliste auf **Hinzufügen**.
 - 2) Ziehen Sie den Cursor, um die Zeitdauer einzuzeichnen, die bedeutet, dass die konfigurierte Zutrittsgruppe in dieser Zeitspanne aktiviert ist.
-

Hinweis

Einem Urlaubszeitraum können bis zu 8 Zeitspannen zugeordnet werden.

- 3) Optional: Führen Sie die folgenden Operationen durch, um die Zeitdauern zu bearbeiten.
 - Bewegen Sie den Cursor auf die Zeitdauer und ziehen Sie die Zeitdauer in der Zeitleiste an die gewünschte Position, wenn der Cursor auf  wechselt.
 - Klicken Sie auf die Zeitdauer und bearbeiten Sie die Start-/Endzeit direkt im erscheinenden Dialog.
 - Bewegen Sie den Cursor an den Anfang oder das Ende der Zeitdauer und ziehen Sie, wenn der Cursor auf  wechselt, um die Zeitdauer zu verlängern oder zu verkürzen.
 - 4) Optional: Wählen Sie die zu löschende(n) Zeitdauer(n) aus und klicken Sie dann in der Spalte Vorgang auf , um die ausgewählte(n) Zeitdauer(n) zu löschen.
 - 5) Optional: Klicken Sie auf  in der Spalte Vorgang, um alle Zeitdauer(n) in der Zeitleiste zu löschen.
 - 6) Optional: Klicken Sie in der Spalte Vorgang auf , um den hinzugefügten Urlaubszeitraum aus der Urlaubsliste zu löschen.
6. Klicken Sie auf **Speichern**.

15.2.2 Vorlage hinzufügen

Die Vorlage enthält einen Wochenplan und einen Feiertag. Sie können einen Wochenplan festlegen und die Zeitdauer der Zugriffsberechtigung für verschiedene Personen oder Gruppen zuweisen. Sie können auch den/die zusätzlichen Feiertag(e) für die Vorlage auswählen.

Schritte

Hinweis

Sie können bis zu 255 Vorlagen in das Softwaresystem aufnehmen.

1. Klicken Sie auf **Zugriffskontrolle** → **Zeitplan** → **Vorlage**, um die Seite Vorlage zu öffnen.
-

Hinweis

Es gibt zwei Standardvorlagen: All-Day Authorized und All-Day Denied, die nicht bearbeitet oder gelöscht werden können.

Ganztägig autorisiert

Die Zugangsberechtigung ist an jedem Wochentag gültig und hat keinen Feiertag.



Ganztägig verweigert

Die Zugangsberechtigung ist an jedem Wochentag ungültig und es gibt keinen Feiertag.

2. Klicken Sie im linken Bereich auf **Hinzufügen**, um eine neue Vorlage zu erstellen.
 3. Erstellen Sie einen Namen für die Vorlage.
 4. Geben Sie in das Feld Bemerkung eine Beschreibung oder einen Hinweis zu dieser Vorlage ein.
 5. Bearbeiten Sie den Wochenplan, um ihn auf die Vorlage anzuwenden.
 - 1) Klicken Sie in der unteren Leiste auf die Registerkarte **Wochenplan**.
 - 2) Wählen Sie einen Wochentag und zeichnen Sie die Zeitdauer(n) auf der Zeitleiste ein.
-

Hinweis

Für jeden Tag im Wochenplan können bis zu 8 Zeitdauer(n) eingestellt werden.

- 3) Optional: Führen Sie die folgenden Operationen durch, um die Zeitdauern zu bearbeiten.
 - Bewegen Sie den Cursor auf die Zeitdauer und ziehen Sie die Zeitdauer in der Zeitleiste an die gewünschte Position, wenn der Cursor auf  wechselt.
 - Klicken Sie auf die Zeitdauer und bearbeiten Sie die Start-/Endzeit direkt im erscheinenden Dialog.
 - Bewegen Sie den Cursor an den Anfang oder das Ende der Zeitdauer und ziehen Sie, wenn der Cursor auf  wechselt, um die Zeitdauer zu verlängern oder zu verkürzen.
 - 4) Wiederholen Sie die beiden obigen Schritte, um weitere Zeitdauern an den anderen Wochentagen zu zeichnen.
 6. Fügen Sie einen Feiertag hinzu, um ihn auf die Vorlage anzuwenden.
-


Hinweis

Bis zu 4 Feiertage können zu einer Vorlage hinzugefügt werden.

- 1) Klicken Sie auf die Registerkarte **Urlaub**.
 - 2) Wählen Sie einen Feiertag in der linken Liste aus und er wird der ausgewählten Liste auf der rechten Seite hinzugefügt.
 - 3) Wahlweise: Klicken Sie auf **Hinzufügen**, um einen neuen Feiertag hinzuzufügen.
-

Hinweis

Einzelheiten zum Hinzufügen eines Feiertags finden Sie unter **Feiertag hinzufügen**.

- 4) Optional: Wählen Sie einen ausgewählten Feiertag in der rechten Liste aus und klicken Sie auf , um den ausgewählten Feiertag zu entfernen, oder klicken Sie auf **Löschen**, um alle ausgewählten Feiertage in der rechten Liste zu löschen.
 7. Klicken Sie auf **Speichern**, um die Einstellungen zu speichern und das Hinzufügen der Vorlage abzuschließen.
-

15.3 Zugriffsgruppe festlegen, um Personen eine Zugriffsberechtigung zuzuweisen

Nachdem Sie die Person hinzugefügt und ihre Anmeldedaten konfiguriert haben, können Sie die Zutrittsgruppen erstellen, um festzulegen, welche Person(en) Zugang zu welchen Türen erhalten kann (können), und dann die Zutrittsgruppe auf das Zutrittskontrollgerät anwenden, damit sie wirksam wird.

Bevor Sie beginnen

- Person zum Kunden hinzufügen.
- Fügen Sie dem Client und den Gruppenzugangspunkten ein Zugangskontrollgerät hinzu. Weitere Informationen finden Sie unter **Gruppenverwaltung**.
- Vorlage hinzufügen.

Schritte

Wenn die Zugriffsgruppeneinstellungen geändert werden, müssen Sie die Zugriffsgruppen erneut auf die Geräte anwenden, damit sie wirksam werden. Zu den Änderungen der Zugangsgruppen gehören Änderungen der Vorlage, der Einstellungen der Zugangsgruppen, der Einstellungen der Person für die Zugangsgruppen und der zugehörigen Personendaten (einschließlich Kartenummer, Fingerabdruck, Gesichtsbild, Verknüpfung zwischen Kartenummer und Fingerabdruck, Verknüpfung zwischen Kartenummer und Fingerabdruck, Kartenpasswort, Gültigkeitsdauer der Karte usw.).

1. Klicken Sie auf **Zugriffskontrolle** → **Berechtigung** → **Zugriffsgruppe**, um die Oberfläche der Zugriffsgruppe aufzurufen.
2. Klicken Sie auf **Hinzufügen**, um das Fenster Hinzufügen zu öffnen.
3. Geben Sie im Textfeld **Name** einen beliebigen Namen für die Zugangsgruppe ein.
4. Wählen Sie eine Vorlage für die Zugangsgruppe.

Hinweis

Sie sollten die Vorlage vor den Zugriffsgruppeneinstellungen konfigurieren. Weitere Informationen finden Sie unter **Konfigurieren von Zeitplan und Vorlage**.

5. Wählen Sie in der linken Liste des Feldes Person auswählen die Person(en) aus, der/denen Sie eine Zugriffsberechtigung zuweisen möchten.
6. Wählen Sie in der linken Liste des Feldes Zugangspunkt wählen die Tür(en), Türstation(en) oder Etage(n) aus, zu denen die ausgewählten Personen Zugang haben sollen.
7. Klicken Sie auf **Speichern**.
Sie können die ausgewählte(n) Person(en) und den/die ausgewählten Zugangspunkt(e) auf der rechten Seite der Benutzeroberfläche anzeigen.

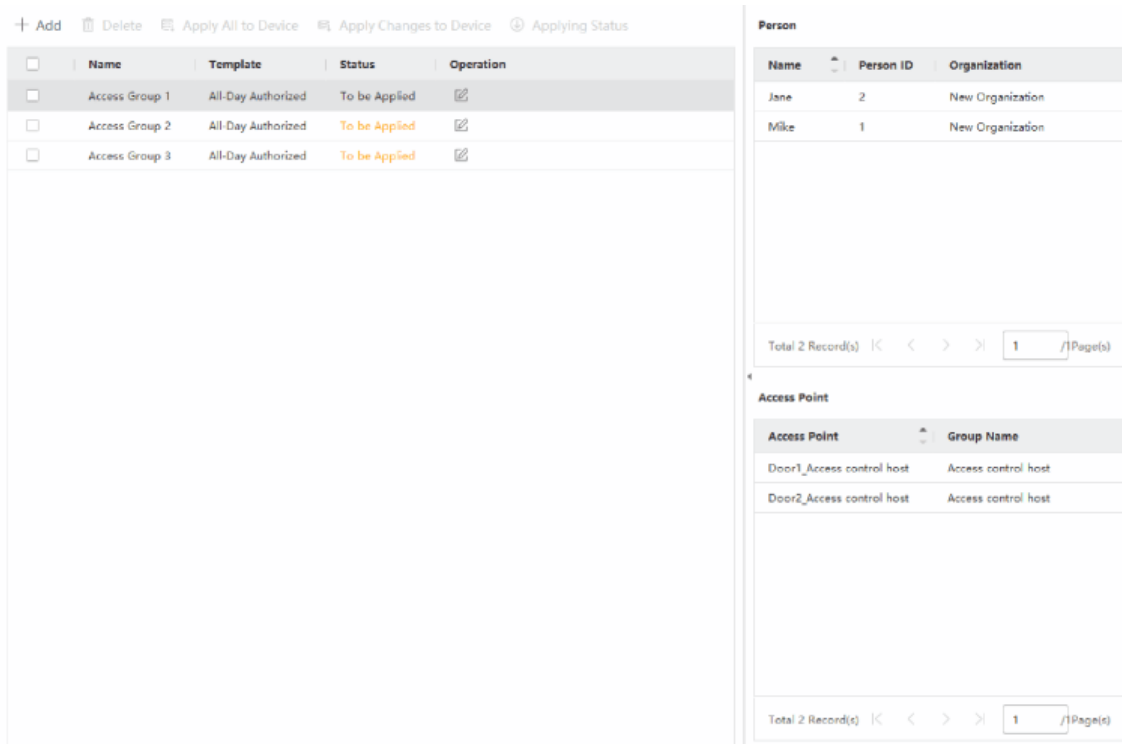


Abbildung 15-2 Anzeige der ausgewählten Person(en) und Zugangspunkt(e)

8. Nachdem Sie die Zugangsgruppen hinzugefügt haben, müssen Sie sie auf das Zugangskontrollgerät anwenden, damit sie wirksam werden.
 - 1) Wählen Sie die Zutrittsgruppe(n) aus, die für das Zutrittskontrollgerät gelten sollen.
 - 2) Klicken Sie auf **Apply All to Devices**, um alle ausgewählten Zutrittsgruppen auf das Zutrittskontrollgerät oder die Türstation anzuwenden.
 - 3) Klicken Sie auf **Alle auf Geräte anwenden** oder **Änderungen auf Geräte anwenden**.

Alle auf Geräte anwenden

Dieser Vorgang löscht alle bestehenden Zugangsgruppen der ausgewählten Geräte und wendet dann die neue Zugangsgruppe auf das Gerät an.

Änderungen auf Geräte anwenden

Dieser Vorgang löscht nicht die bestehenden Zugangsgruppen der ausgewählten Geräte, sondern wendet nur den geänderten Teil der ausgewählten Zugangsgruppe(n) auf das/die Gerät(e) an.

- 4) Zeigen Sie den Anwendungsstatus in der Spalte Status an oder klicken Sie auf **Anwendungsstatus**, um alle angewendeten Zugangsgruppen anzuzeigen.

Hinweis

Sie können das Kontrollkästchen **Nur Fehler anzeigen** aktivieren, um die Anwendungsergebnisse zu filtern.

Die ausgewählten Personen in den beantragten Zutrittsgruppen haben die Berechtigung, die ausgewählten Türen/Türstationen mit ihren verknüpften Karten oder Fingerabdrücken zu

betreten/verlassen.

9. Optional: Klicken Sie auf  , um die Zugriffsgruppe zu bearbeiten, falls erforderlich.

 **Hinweis**

Wenn Sie die Zugangsdaten der Personen oder andere zugehörige Informationen ändern, wird in der rechten Ecke des Clients die Aufforderung "**Access Group to Be Applied**" angezeigt. Sie können auf die Aufforderung klicken, um die geänderten Daten auf das Gerät zu übertragen. Sie können entweder **Jetzt anwenden** oder **Später anwenden** wählen.

15.4 Zugriffsgruppe suchen

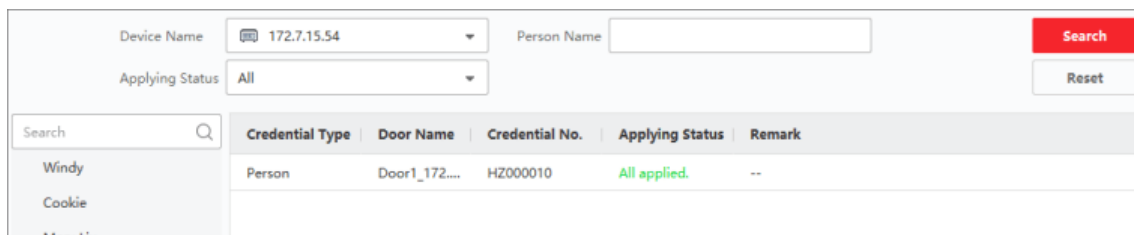
Nachdem Sie eine Zugangsgruppe festgelegt und den Personen eine Zugangsberechtigung zugewiesen haben, können Sie die Zugangsgruppe, zu der die Person gehört, suchen und andere zugehörige Informationen wie Berechtigungsnachweisnummer, Berechtigungstyp, Antragsstatus usw. anzeigen.

 **Hinweis**

Vergewissern Sie sich, dass Sie die Zugriffsgruppe zur Zuweisung der Zugriffsberechtigung an die vorgesehenen Personen festgelegt und angewendet haben. Einzelheiten finden Sie unter **Zugriffsgruppe festlegen, um Personen eine Zugriffsberechtigung zuzuweisen**.

Klicken Sie auf **Zugriffskontrolle** → **Berechtigung** → **Suchen**. Wählen Sie einen Gerätenamen aus und legen Sie die Suchbedingungen fest (einschließlich Personennamen und Anwendungsstatus, optional) und klicken Sie dann auf **Suchen**.

Sie können die Zutrittsgruppe, zu der die gesuchte Person gehört, sowie weitere Informationen wie Berechtigungsnachweisart, Türname, Berechtigungsnachweisnummer, Antragsstatus, Bemerkung usw. anzeigen.




Device Name	<input type="text" value="172.7.15.54"/>	Person Name	<input type="text"/>	<input type="button" value="Search"/>
Applying Status	<input type="text" value="All"/>	<input type="button" value="Reset"/>		
Search	<input type="text"/>			
Windy				
Cookie				
Mary Liu				
Credential Type	Door Name	Credential No.	Applying Status	Remark
Person	Door1_172...	HZ000010	All applied.	--

Abbildung 15-3 Zugriffsgruppe suchen

15.5 Erweiterte Funktionen konfigurieren

Sie können die erweiterten Funktionen der Zugangskontrolle konfigurieren, um spezielle Anforderungen in verschiedenen Bereichen zu erfüllen, z. B. Multi-Faktor-Authentifizierung, Anti-Passback usw.

Hinweis

- Für die kartenbezogenen Funktionen (Art der Zugangskontrollkarte/Multifaktor-Authentifizierung) werden beim Hinzufügen von Karten nur die Karte(n) mit angewandter Zugangsgruppe aufgelistet.
 - Die erweiterten Funktionen sollten von dem Gerät unterstützt werden.
 - Bewegen Sie den Mauszeiger auf die erweiterte Funktion und klicken Sie auf  , um die anzuzeigende(n) erweiterte(n) Funktion(en) anzupassen.
-

15.5.1 Geräteparameter konfigurieren

Nach dem Hinzufügen des Zutrittskontrollgeräts können Sie die Parameter des Zutrittskontrollgeräts (Zutrittskontrolle), der Zutrittskontrollpunkte (Tür oder Etage), der Alarmeingänge, der Alarmausgänge, der Kartenleser und der Fahrspurkontrolle konfigurieren.

Parameter für Zugangskontrollgerät konfigurieren

Nach dem Hinzufügen des Zugangskontrollgeräts können Sie dessen Parameter konfigurieren, z. B. das Einblenden von Benutzerinformationen auf dem Bild, das Hochladen von Bildern nach der Aufnahme, das Speichern aufgenommener Bilder usw.


Bevor Sie beginnen

Fügen Sie dem Client ein Zugangskontrollgerät hinzu.

Schritte

1. Klicken Sie auf **Zugriffskontrolle** → **Erweiterte Funktion** → **Geräteparameter**.

Hinweis

Wenn Sie den Geräteparameter nicht in der Liste der erweiterten Funktionen finden können, bewegen Sie den Cursor auf die erweiterte Funktion und klicken Sie dann auf  , um den anzuzeigenden Geräteparameter auszuwählen.

2. Wählen Sie ein Zugangsgerät aus, um dessen Parameter auf der rechten Seite anzuzeigen.
3. Stellen Sie den Schalter auf ON, um die entsprechenden Funktionen zu aktivieren.

Hinweis

- Die angezeigten Parameter können bei verschiedenen Zugangskontrollgeräten variieren.
 - Einige der folgenden Parameter sind auf der Seite Basisinformationen nicht aufgeführt. Klicken Sie auf **Mehr**, um die Parameter zu bearbeiten.
-

RS-485-Komm. Redundanz

Sie sollten diese Funktion aktivieren, wenn Sie den RS-485-Kartenleser redundant mit dem Zutrittskontrollgerät verkabeln.

Anzeige Erkanntes Gesicht

Bei der Authentifizierung ein Gesichtsbild anzeigen.

Kartenummer anzeigen

Anzeige der Karteninformationen bei der Authentifizierung.

Informationen zur Person anzeigen

Anzeige der Personeninformationen bei der Authentifizierung.

Überlagerung von Personeninformationen auf dem Bild

Zeigen Sie die Personeninformationen auf dem aufgenommenen Bild an.

Spracheingabeaufforderung

Wenn Sie diese Funktion aktivieren, wird die Sprachansage im Gerät aktiviert. Sie können die Sprachansage bei der Bedienung des Geräts hören.

Bild hochladen. Nach verlinkter Aufnahme

Laden Sie die von der verknüpften Kamera aufgenommenen Bilder automatisch in das System hoch.

Bild speichern. Nach verknüpftem Capture

Wenn Sie diese Funktion aktivieren, können Sie das von der verknüpften Kamera aufgenommene Bild auf dem Gerät speichern.

Taste zur Eingabe der Kartenummer drücken

Wenn Sie diese Funktion aktivieren, können Sie die Kartenummer durch Drücken der Taste eingeben.

Wi-Fi-Sonde

Wenn Sie diese Funktion aktivieren, kann das Gerät die MAC-Adresse der umliegenden Kommunikationsgeräte abfragen und die MAC-Adresse in das System hochladen. Wenn die MAC-Adresse mit der angegebenen MAC-Adresse übereinstimmt, kann das System einige Verknüpfungsaktionen auslösen.

3G/4G

Wenn Sie diese Funktion aktivieren, kann das Gerät im 3G/4G-Netz kommunizieren.

NFC Anti-Cloning

Wenn Sie diese Funktion aktivieren, können Sie die geklonte Karte nicht zur Authentifizierung verwenden und die Sicherheit weiter erhöhen.

4. Klicken Sie auf **OK**.
5. Optional: Klicken Sie auf **Kopieren nach** und wählen Sie dann das/die Zugangskontrollgerät(e) aus, um die Parameter auf der Seite auf das/die ausgewählte(n) Gerät(e) zu kopieren.


Parameter für Tür/Aufzug konfigurieren

Nachdem Sie das Zutrittskontrollgerät hinzugefügt haben, können Sie die Parameter für den Zugangspunkt (Tür oder Etage) konfigurieren.

Bevor Sie beginnen

Fügen Sie dem Client ein Zugangskontrollgerät hinzu.

Schritte

1. Klicken Sie auf **Zugriffskontrolle** → **Erweiterte Funktion** → **Geräteparameter**.
2. Wählen Sie auf der linken Seite ein Zutrittskontrollgerät aus, und klicken Sie dann auf  , um die Türen oder Etagen des ausgewählten Geräts anzuzeigen.
3. Wählen Sie eine Tür oder Etage aus, um deren Parameter auf der rechten Seite anzuzeigen.
4. Bearbeiten Sie die Tür- oder Bodenparameter.

Hinweis

- Die angezeigten Parameter können bei verschiedenen Zugangskontrollgeräten variieren.
 - Einige der folgenden Parameter sind auf der Seite Basisinformationen nicht aufgeführt. Klicken Sie auf **Mehr**, um die Parameter zu bearbeiten.
-

Name

Bearbeiten Sie den Namen des Kartenlesers wie gewünscht.

Türkontakt

Sie können den Türsensor als "geschlossen" oder "offen" einstellen. Normalerweise bleibt er geschlossen.

Typ der Beenden-Taste

Sie können festlegen, ob die Ausfahrtstaste geschlossen oder offen bleiben soll. Normalerweise bleibt sie offen.

Tür verriegelt Zeit

Nach dem Durchziehen der normalen Karte und dem Betätigen des Relais beginnt die

Zeitschaltuhr für die Verriegelung der Tür zu arbeiten.

Verlängerte Öffnungsdauer

Der Türkontakt kann mit einer angemessenen Verzögerung aktiviert werden, nachdem die Person mit erweitertem Zugangsbedarf ihre Karte gezogen hat.

Timeout-Alarm bei offener Tür

Der Alarm kann ausgelöst werden, wenn die Tür innerhalb einer konfigurierten Zeitspanne nicht geschlossen wurde. Ist er auf 0 eingestellt, wird kein Alarm ausgelöst.

Tür verriegeln, wenn die Tür geschlossen ist

Die Tür kann verriegelt werden, sobald sie geschlossen ist, auch wenn die **Türverriegelungszeit** nicht erreicht ist.

Code der Bedrohung

Die Tür kann durch Eingabe des Nötigungscodes geöffnet werden, wenn eine Nötigung vorliegt. Gleichzeitig kann der Kunde das Nötigungsereignis melden.

Super-Passwort

Die betreffende Person kann die Tür öffnen, indem sie das Superpasswort eingibt.

Code verwerfen

Erstellen Sie einen Entlassungscode, mit dem der Summer des Kartenlesers ausgeschaltet werden kann (durch Eingabe des Entlassungscodes auf dem Tastenfeld).

Hinweis

- Der Nötigungscodes, der Supercode und der Entlassungscode sollten unterschiedlich sein.
 - Der Nötigungscodes, das Superpasswort und der Entlassungscode sollten sich vom Authentifizierungspasswort unterscheiden.
 - Die Länge des Nötigungscodes, des Superpassworts und des Entlassungscodes richtet sich nach dem Gerät, in der Regel sollte er 4 bis 8 Ziffern enthalten.
-

5. Klicken Sie auf **OK**.

6. Optional: Klicken Sie auf **Kopieren nach** und wählen Sie dann die Tür/Etage(n) aus, um die Parameter auf der Seite auf die ausgewählten Türen/Etage(n) zu kopieren.

Hinweis

Die Einstellungen für die Statusdauer der Tür oder Etage werden auch auf die ausgewählte(n) Tür(en) oder Etage(n) übertragen.

Parameter für Kartenleser konfigurieren


Nachdem Sie das Zutrittskontrollgerät hinzugefügt haben, können Sie die Parameter des

Kartenlesers konfigurieren.

Bevor Sie beginnen

Fügen Sie dem Client ein Zugangskontrollgerät hinzu.

Schritte

1. Klicken Sie auf **Zugriffskontrolle** → **Erweiterte Funktion** → **Geräteparameter**.
2. Klicken Sie in der Geräteliste auf der linken Seite auf , um die Tür zu erweitern, wählen Sie einen Kartenleser aus und bearbeiten Sie die Parameter des Kartenlesers auf der rechten Seite.
3. Bearbeiten Sie die Basisparameter des Kartenlesers auf der Seite Basisinformationen.

Hinweis

- Die angezeigten Parameter können bei verschiedenen Zugangskontrollgeräten variieren. Ein Teil der Parameter ist wie folgt aufgelistet. Weitere Einzelheiten entnehmen Sie bitte dem Benutzerhandbuch des Geräts.
 - Einige der folgenden Parameter sind auf der Seite Basisinformationen nicht aufgeführt. Klicken Sie auf **Mehr**, um die Parameter zu bearbeiten.
-

Name

Bearbeiten Sie den Namen des Kartenlesers wie gewünscht.

OK-LED Polarität/Fehler-LED Polarität/Summer Polarität

Stellen Sie die Polarität der OK-LED/Fehler-LED/Summer-LED der Hauptplatine entsprechend den Parametern des Kartenlesers ein. Im Allgemeinen werden die Standardeinstellungen übernommen.

Mindestintervall für den Karteneinzug

Wenn das Intervall zwischen den Kartendurchzügen derselben Karte kleiner als der eingestellte Wert ist, ist der Kartendurchzug ungültig. Sie können den Wert auf 0 bis 255 einstellen.

Max. Intervall bei der Eingabe von PWD

Wenn Sie das Kennwort am Kartenleser eingeben und der Abstand zwischen dem Drücken zweier Ziffern größer ist als der eingestellte Wert, werden die zuvor gedrückten Ziffern automatisch gelöscht.

Alarm von Max. Fehlversuche

Aktivieren Sie diese Option, um einen Alarm zu melden, wenn die Kartenleseversuche den eingestellten Wert erreichen.

Max. Zeiten des Kartenversagens

Legen Sie die maximalen Fehlversuche beim Lesen der Karte fest.

Erkennung von Manipulationen

Aktivieren Sie die Manipulationserkennung für den Kartenleser.

Kommunikation mit dem Controller Jedes

Wenn das Zutrittskontrollgerät länger als die eingestellte Zeit keine Verbindung mit dem Kartenleser herstellen kann, schaltet sich der Kartenleser automatisch ab.

Brummende Zeit

Stellen Sie die Summzeit des Kartenlesers ein. Die verfügbare Zeit reicht von 0 bis 5.999 Sekunden. 0 steht für einen Dauersignalton.

Kartenleser Typ/Kartenleser Beschreibung

Ermittelt Typ und Beschreibung des Kartenlesers. Sie sind schreibgeschützt.

Fingerabdruck-Erkennungsstufe

Wählen Sie die Stufe der Fingerabdruckerkennung in der Dropdown-Liste aus.

Standard-Authentifizierungsmodus des Kartenlesers

Zeigen Sie den Standard-Authentifizierungsmodus des Kartenlesers an.

Kapazität der Fingerabdrücke

Zeigen Sie die maximale Anzahl der verfügbaren Fingerabdrücke an.

Vorhandene Fingerabdrucknummer

Anzeige der Anzahl der vorhandenen Fingerabdrücke auf dem Gerät.

Ergebnis

Das Gerät bewertet das aufgenommene Bild anhand des Gierwinkels, des Neigungswinkels und der Pupillendistanz. Liegt die Bewertung unter dem konfigurierten Wert, wird die Gesichtserkennung fehlschlagen.

Zeitüberschreitung bei der Gesichtserkennung

Wenn die Erkennungszeit länger als die eingestellte Zeit ist, erinnert Sie das Gerät daran.

Intervall der Gesichtserkennungsfunktion

Das Zeitintervall zwischen zwei kontinuierlichen Gesichtserkennungen bei der Authentifizierung. Standardmäßig beträgt es 2s.

Gesicht 1:1 Übereinstimmungsschwellenwert

Legen Sie den Abgleichsschwellenwert für die Authentifizierung im 1:1-Abgleichsmodus fest. Je größer der Wert ist, desto geringer ist die Falschakzeptanzrate und desto größer ist die Falschrückweisungsrate bei der Authentifizierung.

1:N Sicherheitsstufe

Legen Sie die Sicherheitsstufe für die Authentifizierung über den 1:N-Abgleichsmodus fest. Je größer der Wert ist, desto geringer ist die Falschakzeptanzrate und desto größer ist die Falschrückweisungsrate bei der Authentifizierung.

Live-Gesichtserkennung

Aktivieren oder deaktivieren Sie die Funktion zur Erkennung eines lebenden Gesichts. Wenn

Sie die Funktion aktivieren, kann das Gerät erkennen, ob es sich um eine lebende Person handelt oder nicht.

Live-Gesichtserkennung Sicherheitsstufe

Nachdem Sie die Funktion Live-Gesichtserkennung aktiviert haben, können Sie die entsprechende Sicherheitsstufe für die Live-Gesichtsauthentifizierung festlegen.

Max. Fehlversuche für Face Auth.

Legen Sie die maximale Anzahl der Fehlversuche bei der Live-Gesichtserkennung fest. Das System sperrt das Gesicht des Benutzers für 5 Minuten, wenn die Live-Gesichtserkennung mehr als die konfigurierte Anzahl von Fehlversuchen aufweist. Derselbe Benutzer kann sich innerhalb von 5 Minuten nicht mit dem falschen Gesicht authentifizieren. Innerhalb der 5 Minuten kann sich der Benutzer zweimal kontinuierlich mit dem echten Gesicht authentifizieren, um die Sperre aufzuheben.

Sperrern Authentifizierung fehlgeschlagen Gesicht

Nach Aktivierung der Funktion Live-Gesichtserkennung sperrt das System das Gesicht des Benutzers für 5 Minuten, wenn die Live-Gesichtserkennung mehr als die konfigurierte Anzahl von Versuchen fehlschlägt. Derselbe Benutzer kann sich innerhalb von 5 Minuten nicht mit dem falschen Gesicht authentifizieren. Innerhalb dieser 5 Minuten kann sich der Benutzer zweimal kontinuierlich mit dem echten Gesicht authentifizieren, um die Sperre aufzuheben.

Anwendungsmodus

Sie können je nach Umgebung einen Innenraum- oder einen anderen Anwendungsmodus wählen.

4. Klicken Sie auf **OK**.
5. Optional: Klicken Sie auf **Kopieren nach** und wählen Sie dann das/die Kartenlesegerät(e) aus, um die Parameter auf der Seite auf das/die ausgewählte(n) Kartenlesegerät(e) zu kopieren.

Parameter für Alarmeingang konfigurieren

Nachdem Sie das Zutrittskontrollgerät hinzugefügt haben, können Sie die Parameter für seine Alarmeingänge konfigurieren.

Bevor Sie beginnen


Fügen Sie dem Client ein Zugangskontrollgerät hinzu, und stellen Sie sicher, dass das Gerät Alarmeingaben unterstützt.

Schritte

Hinweis

Wenn der Alarmeingang aktiviert ist, können Sie seine Parameter nicht bearbeiten. Entschärfen Sie ihn zuerst.

1. Klicken Sie auf **Zugriffskontrolle** → **Erweiterte Funktion** → **Geräteparameter** .

2. Klicken Sie in der Geräteliste auf der linken Seite auf  , um die Tür zu erweitern, wählen Sie einen Alarmeingang aus und bearbeiten Sie die Parameter des Alarmeingangs auf der rechten Seite.
3. Stellen Sie die Parameter für den Alarmeingang ein.

Name

Bearbeiten Sie den Namen des Alarmeingangs wie gewünscht.

Detektor Typ

Der Detektortyp des Alarmeingangs.

Zone Typ

Stellen Sie den Zonentyp für den Alarmeingang ein.

Empfindlichkeit

Nur wenn die Dauer des vom Detektor erkannten Signals die eingestellte Zeit erreicht, wird der Alarmeingang ausgelöst. Wenn Sie zum Beispiel die Empfindlichkeit auf 10 ms eingestellt haben, wird der Alarmeingang nur dann ausgelöst, wenn die Dauer des vom Detektor erfassten Signals 10 ms erreicht.

Alarmausgang auslösen

Wählen Sie den/die auszulösenden Alarmausgang(e).

4. Klicken Sie auf **OK**.
5. Optional: Klicken Sie auf den Schalter in der oberen rechten Ecke, um den Alarmeingang zu aktivieren oder zu deaktivieren.


Konfigurieren der Parameter für den Alarmausgang

Nach dem Hinzufügen des Zugangskontrollgeräts können Sie, wenn das Gerät mit Alarmausgängen verbunden ist, die Parameter konfigurieren.

Bevor Sie beginnen

Fügen Sie dem Client ein Zugangskontrollgerät hinzu, und stellen Sie sicher, dass das Gerät die Alarmausgabe unterstützt.

Schritte

1. Klicken Sie auf **Zugangskontrolle** → **Erweiterte Funktion** → **Geräteparameter**, um die Konfigurationsseite der Zugangskontrollparameter aufzurufen.
2. Klicken Sie in der Geräteliste auf der linken Seite auf  , um die Tür zu erweitern, wählen Sie einen Alarmeingang aus und bearbeiten Sie die Parameter des Alarmeingangs auf der rechten Seite.
3. Stellen Sie die Parameter für den Alarmausgang ein.

Name

Bearbeiten Sie den Namen des Kartenlesers wie gewünscht.

Aktivzeit des Alarmausgangs

Wie lange der Alarmausgang nach der Auslösung anhält.

4. Klicken Sie auf **OK**.
5. Optional: Stellen Sie den Schalter in der oberen rechten Ecke auf **ON**, um den Alarmausgang auszulösen.

Parameter für den Lane Controller konfigurieren

Nachdem Sie den Spurcontroller zum Client hinzugefügt haben, können Sie seine Parameter für das Passieren der Spur konfigurieren.

Bevor Sie beginnen

Fügen Sie dem Client ein Zugangskontrollgerät hinzu.

Schritte

1. Klicken Sie auf **Zugangskontrolle** → **Erweiterte Funktion** → **Geräteparameter**, um die Seite Parametereinstellungen aufzurufen.
2. Wählen Sie in der Geräteliste auf der linken Seite einen Lane Controller aus und Sie können die Parameter des Lane Controllers auf der rechten Seite bearbeiten.
3. Bearbeiten Sie die Parameter.

Passing-Modus

Wählen Sie den Controller aus, der den Schrankenstatus des Geräts steuern soll.

- Wenn Sie **Gemäß den DIP-Einstellungen des Fahrspur-Controllers** wählen, folgt das Gerät den DIP-Einstellungen des Fahrspur-Controllers, um die Schranke zu steuern. Die Einstellungen in der Software sind dann ungültig.
- Wenn Sie **Gemäß den Einstellungen des Hauptcontrollers** wählen, folgt das Gerät den Einstellungen der Software zur Steuerung der Schranke. Die DIP-Einstellungen des Fahrbahnreglers sind dann ungültig.

Authentifizierung bei freiem Durchgang

Wenn Sie diese Funktion aktivieren, müssen sich die Fußgänger jedes Mal authentifizieren, wenn sie die Fahrspur passieren, wenn der Schrankenmodus für die Ein- und Ausfahrt auf Offen bleibt. Andernfalls wird ein Alarm ausgelöst.

Öffnen/Schließen der Schranke Geschwindigkeit

Stellen Sie die Öffnungs- und Schließgeschwindigkeit der Schranke ein. Sie können zwischen 1 und 10 wählen. Je höher der Wert, desto schneller die Geschwindigkeit.



Hinweis

Der empfohlene Wert ist 6.

Dauer der akustischen Aufforderung

Legen Sie fest, wie lange der Ton dauern soll, der bei Auslösung eines Alarms abgespielt wird.

Hinweis

0 bedeutet, dass der Alarmton so lange abgespielt wird, bis der Alarm beendet ist.

Temperatur Einheit

Wählen Sie die Temperatureinheit, die im Gerätestatus angezeigt wird.

4. Klicken Sie auf **OK**.

15.5.2 Verbleibende Entsperrung/Sperrung konfigurieren

Sie können den Status der Tür als unverriegelt oder verriegelt festlegen und die Aufzugsteuerung als frei und kontrolliert einstellen. Sie können zum Beispiel festlegen, dass die Tür während des Urlaubs verriegelt bleibt und dass die Tür während des festgelegten Zeitraums des Arbeitstages unverriegelt bleibt.

Bevor Sie beginnen

Fügen Sie die Zugangskontrollgeräte zum System hinzu.

Schritte

1. Klicken Sie auf **Zugriffskontrolle** → **Erweiterte Funktion** → **Gesperrt/Entsperrt bleiben**, um die Seite **Gesperrt/Entsperrt bleiben** aufzurufen.
2. Wählen Sie auf der linken Seite die Tür- oder Aufzugsteuerung aus, die konfiguriert werden soll.
3. Um den Status der Tür- oder Aufzugsteuerung während des Arbeitstages einzustellen, klicken Sie auf den **Wochenplan** und führen Sie die folgenden Schritte aus.
 - 1) Klicken Sie für die Tür auf **Unverriegelt bleiben**, **Verriegelt bleiben**, **Induktiv-Modus** oder **Barrierefrei-Modus**.

Hinweis



- **Induktiver Modus:** Das Öffnen und Schließen der Tür wird durch die Infrarot-Induktion des menschlichen Körpers ausgelöst.
 - **Barrierefreier Modus:** Wenn eine große Anzahl von Personen die Tür passieren muss, bleibt die Tür offen (ohne häufige Authentifizierung), wenn der Personen- und ID-Vergleich erfolgreich ist. Nur wenn der Personen- und ID-Vergleich fehlschlägt, wird die Tür geschlossen.
 - Der induktive Modus und der barrierefreie Modus sollten vom Gerät unterstützt werden.
-

- 2) Klicken Sie für die Aufzugssteuerung auf **Frei** oder **Gesteuert**.
 - 3) Ziehen Sie den Cursor, um die Zeitdauer einzuzeichnen, die bedeutet, dass die konfigurierte Zutrittsgruppe in dieser Zeitspanne aktiviert ist.
-

Hinweis

Für jeden Tag im Wochenplan können bis zu 8 Zeitdauern eingestellt werden.

- 4) Optional: Führen Sie die folgenden Operationen durch, um die Zeitdauern zu bearbeiten.

- Bewegen Sie den Cursor auf die Zeitdauer und ziehen Sie die Zeitdauer in der Zeitleiste an die gewünschte Position, wenn der Cursor auf  wechselt.
- Klicken Sie auf die Zeitdauer und bearbeiten Sie die Start-/Endzeit direkt im erscheinenden Dialog.
- Bewegen Sie den Cursor an den Anfang oder das Ende der Zeitdauer und ziehen Sie, wenn der Cursor auf  wechselt, um die Zeitdauer zu verlängern oder zu verkürzen.

5) Klicken Sie auf **Speichern**.

Verwandte Operationen





- | | |
|---------------------------------|---|
| Auf ganze Woche kopieren | Wählen Sie eine Dauer in der Zeitleiste aus und klicken Sie auf In ganze Woche kopieren , um alle Dauereinstellungen in dieser Zeitleiste auf andere Wochentage zu übertragen. |
| Ausgewählte löschen | Wählen Sie eine Dauer in der Zeitleiste aus und klicken Sie auf Markierte löschen , um diese Dauer zu löschen. |
| Klar | Klicken Sie auf Löschen , um alle Dauereinstellungen im Wochenplan zu löschen. |


4. Um den Türstatus während des Feiertags einzustellen, klicken Sie auf den **Feiertag** und führen Sie die folgenden Schritte aus.

- 1) Klicken Sie auf **Entriegelt bleiben, Verriegelt bleiben, Induktivmodus** oder **Barrierefreier Modus**.
- 2) Klicken Sie auf **Hinzufügen**.
- 3) Geben Sie das Anfangs- und Enddatum ein.
- 4) Ziehen Sie den Cursor, um die Zeitdauer einzuzeichnen, die bedeutet, dass die konfigurierte Zutrittsgruppe in dieser Zeitspanne aktiviert ist.

Hinweis

Einem Urlaubszeitraum können bis zu 8 Zeitspannen zugeordnet werden.

- 5) Führen Sie die folgenden Schritte aus, um die Zeitdauern zu bearbeiten.
 - Bewegen Sie den Cursor auf die Zeitdauer und ziehen Sie die Zeitdauer in der Zeitleiste an die gewünschte Position, wenn der Cursor auf  wechselt.
 - Klicken Sie auf die Zeitdauer und bearbeiten Sie die Start-/Endzeit direkt im erscheinenden Dialog.
 - Bewegen Sie den Cursor an den Anfang oder das Ende der Zeitdauer und ziehen Sie, wenn der Cursor auf  wechselt, um die Zeitdauer zu verlängern oder zu verkürzen.
- 6) Optional: Wählen Sie die zu löschende(n) Zeitdauer(n) aus und klicken Sie dann in der Spalte Vorgang auf  , um die ausgewählte(n) Zeitdauer(n) zu löschen.
- 7) Optional: Klicken Sie auf  in der Spalte Vorgang, um alle Zeitdauer(n) in der Zeitleiste zu löschen.

- 8) Optional: Klicken Sie auf  in der Spalte Vorgang, um den hinzugefügten Urlaubszeitraum aus der Urlaubsliste zu löschen.
- 9) Klicken Sie auf **Speichern**.
5. Optional: Klicken Sie auf **Kopieren**, um die TürstatusEinstellungen dieser Tür auf andere Türen zu übertragen.

15.5.3 Konfigurieren der Multi-Faktor-Authentifizierung

Sie können die Personen nach Gruppen verwalten und die Authentifizierung für mehrere Personen an einem Zutrittskontrollpunkt (Tür) einstellen.

Bevor Sie beginnen

Legen Sie die Zutrittsgruppe fest und wenden Sie die Zutrittsgruppe auf das Zutrittskontrollgerät an. Einzelheiten finden Sie unter **Zugriffsgruppe festlegen, um Personen eine Zugriffsberechtigung zuzuweisen**.

Führen Sie diese Aufgabe aus, wenn Sie Authentifizierungen für mehrere Karten eines Zugangskontrollpunkts (Tür) festlegen möchten.

Schritte

1. Klicken Sie auf **Zugriffskontrolle** → **Erweiterte Funktion** → **Multi-Faktor-Authentifizierung**.
2. Wählen Sie ein Zutrittskontrollgerät in der Geräteliste auf der linken Seite aus.
3. Fügen Sie eine Personen-/Kartengruppe für das Zutrittskontrollgerät hinzu.
 - 1) Klicken Sie im rechten Bereich auf **Hinzufügen**.
 - 2) Geben Sie der Gruppe einen Namen nach Wunsch.
 - 3) Geben Sie die Startzeit und die Endzeit des Gültigkeitszeitraums für die Person/Kartengruppe an.
 - 4) Wählen Sie die Mitglieder und die Karte(n) in der Liste Verfügbar aus, und die ausgewählten Mitglieder und Karten werden der Liste Ausgewählt hinzugefügt.

Hinweis

Vergewissern Sie sich, dass Sie der Person eine Karte ausgestellt haben.
Vergewissern Sie sich, dass Sie die Zugangsgruppe festgelegt haben und wenden Sie die Zugangsgruppe erfolgreich auf das Zugangskontrollgerät an.

- 5) Klicken Sie auf **Speichern**.
- 6) Optional: Wählen Sie die Person/Kartengruppe(n) aus, und klicken Sie dann auf **Löschen**, um sie zu löschen.
- 7) Optional: Wählen Sie die Personen-/Kartengruppe(n) aus und klicken Sie dann auf **Anwenden**, um die Zugangsgruppe, die zuvor nicht auf das Zugangskontrollgerät angewendet werden konnte, erneut anzuwenden.
4. Wählen Sie einen Zugangskontrollpunkt (Tür) des ausgewählten Geräts auf dem linken Bedienfeld.
5. Geben Sie bei der Passworteingabe das maximale Intervall ein.
6. Fügen Sie eine Authentifizierungsgruppe für den ausgewählten Zugangskontrollpunkt hinzu.

- 1) Klicken Sie im Bereich Authentifizierungsgruppen auf **Hinzufügen**.
- 2) Wählen Sie in der Dropdown-Liste eine konfigurierte Vorlage als Authentifizierungsvorlage aus.

Hinweis

Informationen zum Einstellen der Vorlage finden Sie unter [Zeitplan und Vorlage konfigurieren](#).

- 3) Wählen Sie in der Dropdown-Liste die Authentifizierungsart **Lokale Authentifizierung, Lokale Authentifizierung und Remote Open Door** oder **Lokale Authentifizierung und Superpasswort** aus.

Lokale Authentifizierung

Authentifizierung durch das Zugangskontrollgerät.

Lokale Authentifizierung und ferngesteuertes Öffnen der Tür

Authentifizierung durch das Zugangskontrollgerät und durch den Kunden. Wenn die Person die Karte am Gerät durchzieht, öffnet sich ein Fenster. Sie können die Tür über den Client entriegeln.

Abbildung 15-4 Ferngesteuert geöffnete Tür

Hinweis

Sie können **Offline-Authentifizierung** aktivieren, um die Superpasswort-Authentifizierung zu aktivieren, wenn die Verbindung zwischen dem Zugangskontrollgerät und dem Client unterbrochen ist.

Lokale Authentifizierung und Superpasswort

Authentifizierung durch das Zugangskontrollgerät und durch das Superpasswort.

- 4) Wählen Sie die hinzugefügte Personen-/Kartengruppe in der linken Liste unten aus, und sie wird der Liste ausgewählt auf der rechten Seite als Authentifizierungsgruppe hinzugefügt.
- 5) Klicken Sie auf die hinzugefügte Authentifizierungsgruppe in der rechten Liste, um die Authentifizierungszeiten in der Spalte Authentifizierungszeiten festzulegen.

Hinweis

- Die Authentifizierungszeiten sollten größer als 0 und kleiner als die addierte Personalmenge in der Personalgruppe sein.
 - Der Höchstwert für die Authentifizierungszeiten beträgt 16.
-

- 6) Klicken Sie auf **Speichern**.

Hinweis

- Für jeden Zugangskontrollpunkt (Tür) können bis zu vier Authentifizierungsgruppen

hinzugefügt werden.

- Für die Authentifizierungsgruppe, deren Authentifizierungstyp **Lokale Authentifizierung** ist, können bis zu 8 Personen-/Kartengruppen zur Authentifizierungsgruppe hinzugefügt werden.
 - Für die Authentifizierungsgruppe, deren Authentifizierungstyp **Lokale Authentifizierung und Superkennwort** oder **Lokale Authentifizierung und Tür ferngesteuert öffnen** ist, können bis zu 7 Personen-/Kartengruppen zur Authentifizierungsgruppe hinzugefügt werden.
-

7. Klicken Sie auf **Speichern**.

15.5.4 Benutzerdefinierte Wiegand-Regel konfigurieren

Basierend auf dem Wissen der Upload-Regel für den Drittanbieter-Wiegand können Sie mehrere benutzerdefinierte Wiegand-Regeln für die Kommunikation zwischen dem Gerät und den Kartenlesern von Drittanbietern festlegen.

Bevor Sie beginnen

Verbinden Sie die Kartenleser von Drittanbietern mit dem Gerät.

Schritte

Hinweis

- Standardmäßig deaktiviert das Gerät die benutzerdefinierte Wiegand-Funktion. Wenn das Gerät die benutzerdefinierte Wiegand-Funktion aktiviert, verwenden alle Wiegand-Schnittstellen des Geräts das benutzerdefinierte Wiegand-Protokoll.
 - Es können bis zu 5 benutzerdefinierte Wiegands eingestellt werden.
 - Einzelheiten zum benutzerdefinierten Wiegand finden Sie unter **Beschreibung der benutzerdefinierten Wiegand-Regel**.
-

1. Klicken Sie auf **Access Control** → **Advanced Function** → **Custom Wiegand**, um die Seite Custom Wiegand aufzurufen.
 2. Wählen Sie auf der linken Seite einen benutzerdefinierten Wiegand aus.
 3. Erstellen Sie einen Wiegand-Namen.
-

Hinweis

Für den benutzerdefinierten Wiegand-Namen sind bis zu 32 Zeichen zulässig.

4. Klicken Sie auf **Gerät auswählen**, um das Zugangskontrollgerät für die Einstellung des benutzerdefinierten Wiegand auszuwählen.
 5. Stellen Sie den Paritätsmodus entsprechend den Eigenschaften des Kartenlesegeräts des Drittanbieters ein.
-

Hinweis

- In der Gesamtlänge sind bis zu 80 Bits erlaubt.
 - Das Startbit der ungeraden Parität, die Länge der ungeraden Parität, das Startbit der geraden
-

Parität und die Länge der geraden Parität reichen von 1 bis 80 Bit.

- Das Startbit der Karten-ID, der Herstellercode, der Standortcode und der OEM sollten zwischen 1 und 80 Bit liegen.
-

6. Legen Sie die Transformationsregel für die Ausgabe fest.

- 1) Klicken Sie auf **Regel festlegen**, um das Fenster Regeln für die Ausgabeumwandlung festlegen zu öffnen.

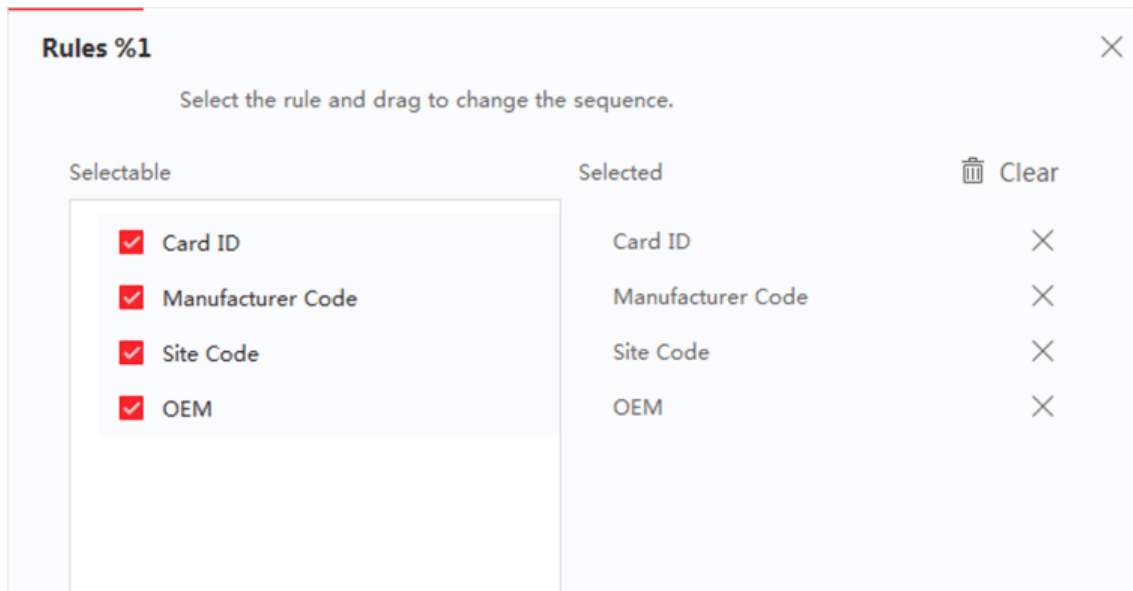


Abbildung 15-5 Transformationsregel für die Ausgabe festlegen

- 2) Wählen Sie in der linken Liste Regeln aus.

Die ausgewählten Regeln werden der rechten Liste hinzugefügt.

- 3) Optional: Ziehen Sie die Regeln, um die Reihenfolge der Regeln zu ändern.

- 4) Klicken Sie auf **OK**.

- 5) Legen Sie auf der Registerkarte Custom Wiegand das Startbit, die Länge und die Dezimalstelle der Regel fest.

7. Klicken Sie auf **Speichern**.

15.5.5 Konfigurieren von Kartenleser-Authentifizierungsmodus und Zeitplan

Sie können die Durchgangsregeln für den Kartenleser des Zugangskontrollgeräts entsprechend Ihren tatsächlichen Bedürfnissen festlegen.

Schritte

1. Klicken Sie auf **Zugriffskontrolle** → **Erweiterte Funktion** → **Authentifizierung**, um die Konfigurationsseite für den Authentifizierungsmodus aufzurufen.
2. Wählen Sie auf der linken Seite einen Kartenleser aus, den Sie konfigurieren möchten.
3. Stellen Sie den Authentifizierungsmodus des Kartenlesers ein.

1) Klicken Sie auf **Konfiguration**.

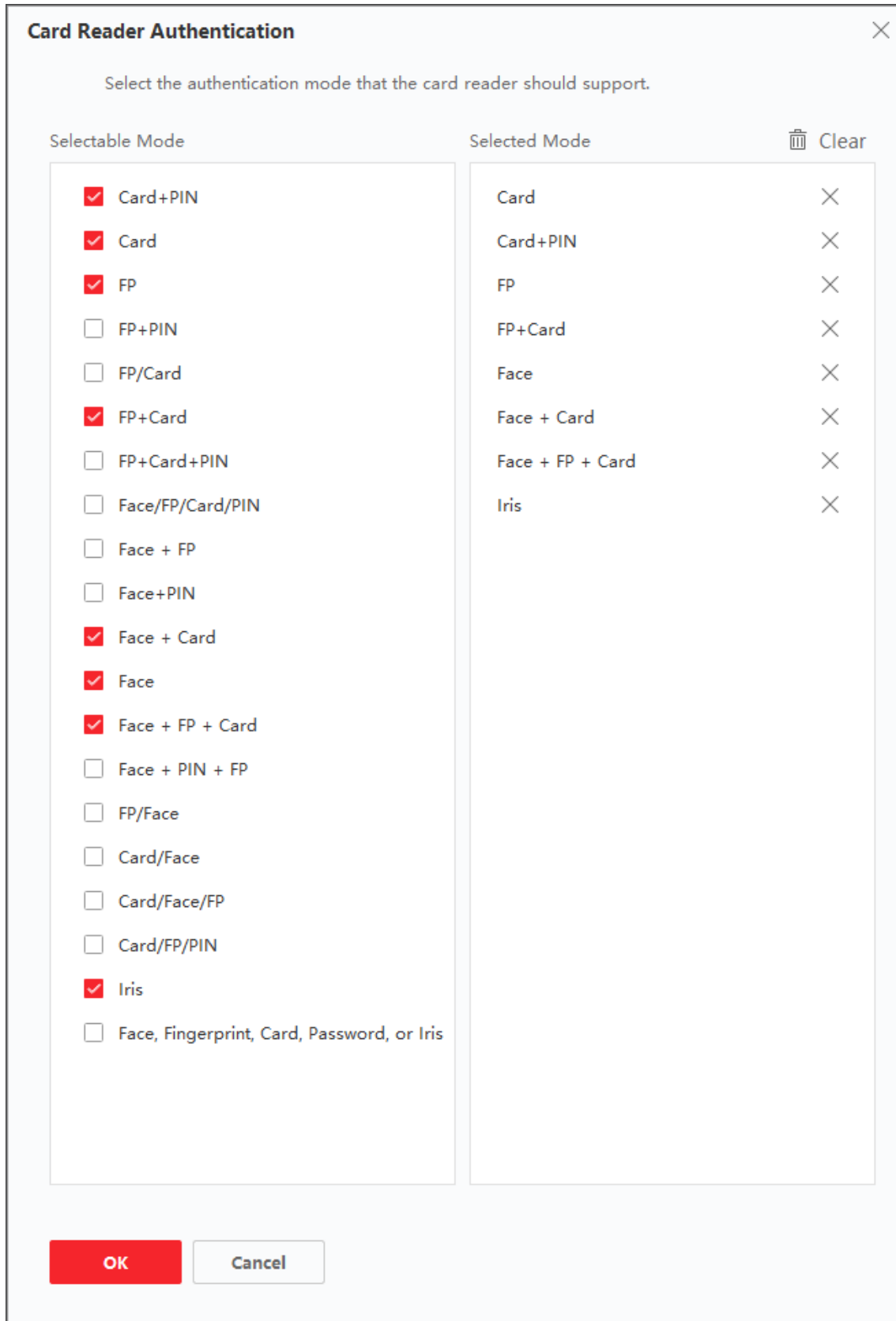


Abbildung 15-6 Auswahl des Kartenleser-Authentifizierungsmodus

Hinweis

PIN bezieht sich auf den zum Öffnen der Tür festgelegten PIN-Code. Siehe **Zugangskontrollinformationen konfigurieren**.

- 2) Markieren Sie die Modi in der Liste Verfügbare Modi und sie werden der Liste der ausgewählten Modi hinzugefügt.
- 3) Klicken Sie auf **OK**.
Nach der Auswahl der Modi werden die ausgewählten Modi als Symbole mit unterschiedlicher Farbe angezeigt.
4. Klicken Sie auf das Symbol, um einen Kartenleser-Authentifizierungsmodus auszuwählen, und ziehen Sie den Cursor, um einen Farbbalken auf dem Zeitplan zu zeichnen, was bedeutet, dass die Kartenleser-Authentifizierung in diesem Zeitraum gültig ist.
5. Wiederholen Sie den obigen Schritt, um andere Zeiträume einzustellen.

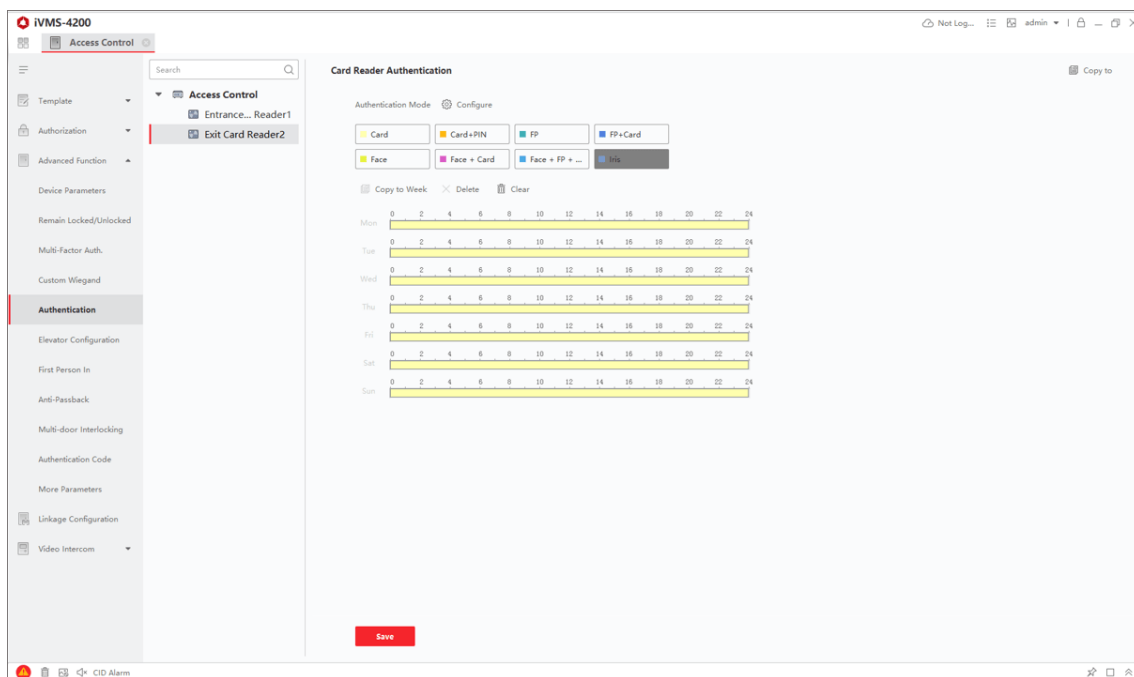


Abbildung 15-7 Authentifizierungsmodi für Kartenleser festlegen

6. Optional: Wählen Sie einen konfigurierten Tag aus und klicken Sie auf **In Woche kopieren**, um die gleichen Einstellungen für die gesamte Woche zu übernehmen.
7. Optional: Klicken Sie auf **Kopieren**, um die Einstellungen auf andere Kartenleser zu übertragen.
8. Klicken Sie auf **Speichern**.

15.5.6 Personenauthentifizierungsmodus konfigurieren

Sie können die Regeln für den Zutritt von Personen zum angegebenen Zutrittskontrollgerät entsprechend Ihren tatsächlichen Bedürfnissen festlegen.

Bevor Sie beginnen

- Fügen Sie dem Client ein Zugangskontrollgerät hinzu, und stellen Sie sicher, dass das Zugangskontrollgerät die Funktion der Personenauthentifizierung unterstützt.
- Fügen Sie eine Person hinzu und weisen Sie ihr eine Zugangsberechtigung zu. Einzelheiten finden Sie unter Personenverwaltung und Zugriffsgruppe festlegen, um Personen eine Zugriffsberechtigung zuzuweisen.

Schritte

1. Klicken Sie auf **Zugriffskontrolle** → **Erweiterte Funktion** → **Authentifizierung**.
2. Wählen Sie ein Zugangskontrollgerät (das die Funktion der Personenauthentifizierung unterstützt) im linken Bereich aus, um die Seite für den Personenauthentifizierungsmodus aufzurufen.
3. Klicken Sie auf **Hinzufügen**, um das Fenster Hinzufügen zu öffnen.
4. Wählen Sie auf der linken Seite die Person(en) aus, die konfiguriert werden müssen. Die ausgewählte(n) Person(en) wird (werden) dem rechten Fenster hinzugefügt.
5. Wählen Sie den Authentifizierungsmodus in der Dropdown-Liste **Authentifizierungsmodus** aus.
6. Klicken Sie auf **OK**.

Abbildung 15-8 Authentifizierungsmodi für Personen festlegen

7. Optional: Wählen Sie auf der Seite Personenauthentifizierungsmodus die Person(en) aus und klicken Sie dann auf **Übernehmen**, um den Personenauthentifizierungsmodus auf das Gerät anzuwenden.

Hinweis

Die Personenauthentifizierung hat höhere Priorität als andere Authentifizierungsmodi. Wenn für das Zugangskontrollgerät der Personenauthentifizierungsmodus konfiguriert wurde, sollte sich die Person an diesem Gerät über den Personenauthentifizierungsmodus authentifizieren.

15.5.8 Konfigurieren der ersten Person in

Sie können mehrere erste Personen für einen Zugangskontrollpunkt festlegen. Nachdem die erste Person autorisiert wurde, ermöglicht sie mehreren Personen den Zugang zur Tür oder andere Authentifizierungsaktionen.

Bevor Sie beginnen

- Fügen Sie dem Client ein Zugangskontrollgerät hinzu, und stellen Sie sicher, dass das Gerät die Funktion "Erste Person" unterstützt.

- Fügen Sie eine Person hinzu und weisen Sie ihr eine Zugangsberechtigung zu. Einzelheiten finden Sie unter **Personenverwaltung** und **Zugriffsgruppe festlegen, um Personen eine Zugriffsberechtigung zuzuweisen**.

Schritte

1. Klicken Sie auf **Zugriffskontrolle** → **Erweiterte Funktion** → **Erste Person In**, um die Seite Erste Person In zu öffnen.
2. Wählen Sie ein Zutrittskontrollgerät in der Liste auf der linken Seite aus.
3. Wählen Sie in der Dropdown-Liste für jeden Zugangskontrollpunkt des ausgewählten Geräts den aktuellen Modus "**Nach erster Person geöffnet bleiben**", "**Nach erster Person geöffnet bleiben**" oder "**Autorisierung durch erste Person**" aus.

Offenbleiben nach der ersten Person aktivieren

Die Tür bleibt nach der Autorisierung der ersten Person für die konfigurierte Zeitdauer geöffnet, bis die Offenhaltezeit endet. Wenn Sie diesen Modus wählen, sollten Sie die aufeinanderfolgenden Authentifizierungszeiten und das Intervall der aufeinanderfolgenden Authentifizierung einstellen.

Hinweis

Die Offenhaltungsdauer sollte zwischen 0 und 1440 Minuten liegen. Standardmäßig beträgt die Offenhaltungsdauer 10 Minuten.

Offenbleiben nach der ersten Person deaktivieren

Deaktivieren Sie die Funktion der Erstanmeldung, d. h. die normale Authentifizierung.

Autorisierung durch die erste Person

Alle Authentifizierungen (mit Ausnahme der Authentifizierungen von Superkarte, Superpasswort, Nötigungskarte und Nötigungscodes) sind erst nach der Autorisierung durch die erste Person zulässig.

Hinweis

Sie können sich erneut mit der ersten Person authentifizieren, um den Modus der ersten Person zu deaktivieren.

4. Klicken Sie auf **Hinzufügen** im Feld Erste Person Liste.
5. Wählen Sie die Person(en) in der linken Liste aus und die Person(en) werden als erste Person(en) der Türen zu den ausgewählten Personen hinzugefügt.
Die hinzugefügte(n) erste(n) Person(en) werden in der Liste der ersten Person(en) aufgeführt.
6. Optional: Wählen Sie eine erste Person aus der Liste aus und klicken Sie auf **Löschen**, um die Person aus der Liste der ersten Personen zu entfernen.
7. Klicken Sie auf **Speichern**.

15.5.9 Anti-Passback konfigurieren

Die Anti-Passback-Funktion wurde entwickelt, um den Missbrauch oder die betrügerische Verwendung von Zugangsdaten zu minimieren, wie z. B. die Rückgabe der Karte an eine unbefugte Person oder die Erschleichung des Zugangs. Die Anti-Passback-Funktion legt eine bestimmte Reihenfolge fest, in der die Zugangsdaten verwendet werden müssen, um Zugang zu gewähren. Sie können die Reihenfolge entsprechend dem tatsächlichen Pfad über den Client einstellen, und wenn die Person die Zugangsdaten in der falschen Reihenfolge verwendet, können Sie die Anti-Passback-Datensätze auch zurücksetzen.


Bevor Sie beginnen

Fügen Sie dem Client ein Zugangskontrollgerät hinzu und aktivieren Sie die Anti-Passing-Back-Funktion des Zugangskontrollgeräts.

Schritte

Hinweis

Für ein Zutrittskontrollgerät kann entweder die Anti-Passing-Back- oder die Multitürverriegelungsfunktion gleichzeitig konfiguriert werden. Informationen zur Konfiguration der Mehrtürverriegelung finden Sie unter **Konfigurieren der Mehrtürverriegelung**.

1. Klicken Sie auf **Zugriffskontrolle** → **Erweiterte Funktion** → **Anti-Passback**, um die Seite Anti-Passback-Einstellungen aufzurufen.
 2. Wählen Sie auf der linken Seite ein Zutrittskontrollgerät aus.
 3. Wählen Sie im Feld **Erster Kartenleser** einen Kartenleser als Beginn des Pfades aus.
 4. Klicken Sie auf  des ausgewählten ersten Kartenlesers in der Spalte **Kartenleser danach**, um den Dialog Kartenleser auswählen zu öffnen.
 5. Wählen Sie die nachfolgenden Kartenleser für den ersten Kartenleser aus.
-

Hinweis

Bis zu vier nachgeschaltete Kartenleser können als nachgeschaltete Kartenleser für einen Kartenleser hinzugefügt werden.

6. Klicken Sie im Dialogfeld auf **OK**, um die Auswahlen zu speichern.
7. Klicken Sie auf der Seite Anti-Passback-Einstellungen auf **Speichern**, um die Einstellungen zu speichern und in Kraft zu setzen.

Beispiel

Pfad für das Durchziehen von Karten festlegen: Wenn Sie Leser In_01 als Anfang und Leser In_02, Leser Out_04 als verknüpfte Kartenleser auswählen. Dann können Sie den Zugangskontrollpunkt nur passieren, indem Sie die Karte in der Reihenfolge Leser In_01, Leser In_02 und Leser Out_04 durchziehen.

8. Klicken Sie auf **Anti-Passback zurücksetzen** und wählen Sie die Person(en) aus, um die entsprechenden Anti-Passback-Datensätze über die Person(en) auf dem Gerät zu löschen.

 **Hinweis**

Diese Funktion sollte von dem Gerät unterstützt werden.

15.5.10 Konfigurieren der Mehrtürverriegelung

Sie können die Mehrfachtürverriegelung zwischen mehreren Türen desselben Zutrittskontrollgeräts einstellen. Um eine der Türen zu öffnen, müssen die anderen Türen geschlossen bleiben. Das bedeutet, dass in der verriegelten kombinierten Türgruppe bis zu einer Tür gleichzeitig geöffnet werden kann.

Bevor Sie beginnen

Fügen Sie dem Client ein Zutrittskontrollgerät hinzu und vergewissern Sie sich, dass das Gerät die Funktion der Mehrfachtürverriegelung unterstützt.

Schritte

 **Hinweis**

- Die Funktion "Multi-door Interlocking" wird nur von Zutrittskontrollgeräten unterstützt, die über mehr als einen Zutrittskontrollpunkt (Türen) verfügen.
 - Für ein Zutrittskontrollgerät kann entweder die Anti-Passback- oder die Multi-Tür-Verriegelungsfunktion gleichzeitig konfiguriert werden. Informationen zur Konfiguration der Anti-Passback-Funktion finden Sie unter **Konfigurieren der Anti-Passback-Funktion**.
-

1. Klicken Sie auf **Zutrittskontrolle** → **Erweiterte Funktion** → **Multitürverriegelung**.
 2. Wählen Sie auf der linken Seite ein Zutrittskontrollgerät aus.
 3. Klicken Sie auf **Hinzufügen** in der Multitür-Verriegelungsliste, um das Fenster Zugangskontrollpunkt hinzufügen zu öffnen.
 4. Wählen Sie mindestens zwei Zugangskontrollpunkte (Türen) aus der Liste aus.
-

 **Hinweis**

Bis zu vier Türen können in einer Multitür-Verriegelungskombination hinzugefügt werden.

5. Klicken Sie auf **OK**, um die ausgewählte(n) Zugangskontrollstelle(n) für die Verriegelung hinzuzufügen.
Die konfigurierte Kombination von Mehrfachtürverriegelungen wird in der Liste der Mehrfachtürverriegelungen aufgeführt.
 6. Optional: Wählen Sie eine hinzugefügte Mehrtür-Verriegelungskombination aus der Liste aus und klicken Sie auf **Löschen**, um die Kombination zu löschen.
 7. Klicken Sie auf **Übernehmen**, um die Einstellungen auf das Zugangskontrollgerät anzuwenden.
-

15.5.11 Authentifizierungscode konfigurieren

Sie können den Authentifizierungscode auf dem Client konfigurieren. Danach können Sie die Tür durch Eingabe des Authentifizierungscodes öffnen, wenn Sie vergessen haben, die Karte mitzunehmen.

Bevor Sie beginnen

Fügen Sie dem Client ein Zugangskontrollgerät hinzu, und stellen Sie sicher, dass das Gerät den Authentifizierungscode als Authentifizierungsmodus unterstützt.

Schritte

1. Klicken Sie auf **Zugriffskontrolle** → **Erweiterte Funktion** → **Authentifizierungscode**, um die Konfigurationsseite für den Authentifizierungscode aufzurufen.
2. Wählen Sie ein Zutrittskontrollgerät in der Liste des Controller-Listenfeldes aus. Alle angelegten Karten und Personen werden in der Kartenliste angezeigt.

Hinweis

Informationen zum Festlegen und Anwenden der Berechtigungen auf das Gerät finden Sie unter **Zugriffsgruppe festlegen, um Personen eine Zugriffsberechtigung zuzuweisen**.

3. Klicken Sie auf das Feld jeder Karte in der Spalte Authentifizierungscode, um den Authentifizierungscode einzugeben.

Hinweis

Der Authentifizierungscode sollte 4 bis 8 Ziffern enthalten.

4. Klicken Sie in der oberen rechten Ecke der Seite Authentifizierungscode auf **Speichern**, um die Einstellungen zu speichern.
Die Authentifizierungscode-Funktion der Karte wird automatisch aktiviert.

Was ist als nächstes zu tun?

Sie sollten den Kartenleser-Authentifizierungsmodus des Zugangskontrollgeräts auf **Karte/Authentifizierungscode** einstellen. Weitere Informationen finden Sie unter **Konfigurieren von Kartenleser-Authentifizierungsmodus und Zeitplan**.

15.6.3 Geräteerfassungsparameter einstellen

Sie können die Erfassungsparameter des Zugangskontrollgeräts konfigurieren, einschließlich der manuellen Erfassung und der ereignisgesteuerten Erfassung.

Hinweis

- Die Aufnahmefunktion sollte vom Gerät unterstützt werden.
 - Bevor Sie die Aufnahmeparameter einstellen, sollten Sie zunächst den Bildspeicher festlegen, um zu definieren, wo die ereignisgesteuerten Bilder gespeichert werden. Weitere Informationen finden Sie unter **Festlegen des Bildspeichers**.
-

Ausgelöste Erfassungsparameter festlegen

Wenn ein Ereignis eintritt, kann die Kamera des Zugangskontrollgeräts ausgelöst werden, um ein oder mehrere Bilder aufzunehmen, um aufzuzeichnen, was bei Eintreten des Ereignisses passiert. Sie können die aufgenommenen Bilder ansehen, wenn Sie die Ereignisdetails im Ereigniszentrum überprüfen. Zuvor müssen Sie die Parameter für die Aufnahme festlegen, z. B. die Anzahl der Bilder, die zu einem bestimmten Zeitpunkt aufgenommen werden.

Bevor Sie beginnen

Bevor Sie die Aufnahmeparameter einstellen, sollten Sie zunächst den Bildspeicher einstellen, um festzulegen, wo die aufgenommenen Bilder gespeichert werden. Einzelheiten finden Sie unter **Festlegen des Bildspeichers**.

Schritte

Hinweis

Diese Funktion sollte von dem Gerät unterstützt werden

1. Rufen Sie das Modul Zugangskontrolle auf.
2. Wählen Sie in der linken Navigationsleiste **Erweiterte Funktion** → **Weitere Parameter** → **Aufnehmen**.
3. Wählen Sie ein Zutrittskontrollgerät in der Geräteliste aus und wählen Sie **Verknüpftes Capture**.
4. Stellen Sie die Bildgröße und -qualität ein.
5. Legen Sie die Aufnahmezeiten fest, sobald die Kamera ausgelöst wurde, um festzulegen, wie viele Bilder pro Zeiteinheit aufgenommen werden sollen.
6. Wenn die Erfassungszeiten mehr als 1 betragen, legen Sie das Intervall für jede Erfassung fest.
7. Klicken Sie auf **Speichern**.

Manuelle Erfassungsparameter einstellen

Im Modul Statusüberwachung können Sie ein Bild der Kamera des Zugangskontrollgeräts manuell aufnehmen, indem Sie auf eine Schaltfläche klicken. Zuvor müssen Sie die Parameter für die Aufnahme festlegen, z. B. die Bildqualität.

Bevor Sie beginnen

Bevor Sie die Aufnahmeparameter einstellen, sollten Sie zuerst den Speicherpfad festlegen, um zu definieren, wo die aufgenommenen Bilder gespeichert werden. Einzelheiten finden Sie unter **Festlegen des Dateispeicherpfads**.

Schritte

Hinweis

Diese Funktion sollte von dem Gerät unterstützt werden

1. Rufen Sie das Modul Zugangskontrolle auf.
2. Wählen Sie in der linken Navigationsleiste **Erweiterte Funktion** → **Weitere Parameter** → **Aufnehmen**.
3. Wählen Sie ein Zutrittskontrollgerät in der Geräteliste und wählen Sie **Manuelle Erfassung**.
4. Wählen Sie die Auflösung der aufgenommenen Bilder aus der Dropdown-Liste.
5. Wählen Sie die Bildqualität als **Hoch**, **Mittel** oder **Niedrig**. Je höher die Bildqualität ist, desto größer wird das Bild sein.
6. Klicken Sie auf **Speichern**.

15.6.4 Parameter für Gesichtserkennungsterminal einstellen

Für das Gesichtserkennungsterminal können Sie die Parameter wie Gesichtsbilddatenbank, QR-Code-Authentifizierung usw. einstellen.

Schritte

Hinweis

Diese Funktion sollte von dem Gerät unterstützt werden.

1. Rufen Sie das Modul Zugangskontrolle auf.
2. Geben Sie in der Navigationsleiste links **Erweiterte Funktion** → **Weitere Parameter** ein.
3. Wählen Sie ein Zutrittskontrollgerät in der Geräteliste aus und klicken Sie auf **Gesichtserkennungsterminal**.
4. Stellen Sie die Parameter ein.

Hinweis

Diese angezeigten Parameter variieren je nach Gerätemodell.

COM

Wählen Sie einen COM-Anschluss für die Konfiguration. COM1 bezieht sich auf die RS-485-Schnittstelle und COM2 bezieht sich auf die RS-232-Schnittstelle.

Gesichtsbild-Datenbank

wählen Sie Deep Learning als Gesichtsbilddatenbank.

Authentifizierung per QR-Code

Wenn diese Funktion aktiviert ist, kann die Gerätekamera den QR-Code zur Authentifizierung scannen. Standardmäßig ist die Funktion deaktiviert.

Blocklisten-Authentifizierung

Wenn diese Option aktiviert ist, vergleicht das Gerät die Person, die Zugang erhalten möchte, mit den Personen in der Sperrliste.

Bei Übereinstimmung (die Person befindet sich in der Sperrliste) wird der Zugang verweigert und das Gerät lädt einen Alarm auf den Client hoch.

Bei Nichtübereinstimmung (die Person ist nicht in der Sperrliste enthalten) wird der Zugang gewährt.

Authentifizierendes Gesichtsbild speichern

Wenn aktiviert, wird das bei der Authentifizierung aufgenommene Gesichtsbild auf dem Gerät gespeichert.

MCU-Version

Anzeige der MCU-Version des Geräts.

5. Klicken Sie auf **Speichern**.

15.6.5 Aktivieren der M1-Kartenverschlüsselung

Die M1-Kartenverschlüsselung kann das Sicherheitsniveau der Authentifizierung verbessern.

Schritte



Die Funktion sollte von der Zutrittskontrollvorrichtung und dem Kartenleser unterstützt werden.

1. Rufen Sie das Modul Zugangskontrolle auf.
2. Geben Sie in der Navigationsleiste links **Erweiterte Funktion** → **Weitere Parameter** ein.
3. Wählen Sie ein Zutrittskontrollgerät in der Geräteliste aus und klicken Sie auf **M1 Card Encryption**, um die Seite M1 Card Encryption aufzurufen.
4. Stellen Sie den Schalter auf on, um die Verschlüsselungsfunktion der M1-Karte zu aktivieren.
5. Stellen Sie die Sektor-ID ein.

Die Sektor-ID reicht von 1 bis 100.

6. Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

15.6.6 RS-485-Parameter einstellen

Sie können die RS-485-Parameter des Zugangskontrollgeräts einstellen, einschließlich der Baudrate, des Datenbits, des Stoppbits, des Paritätstyps, der Flusssteuerungsart, des Kommunikationsmodus, des Arbeitsmodus und des Verbindungsmodus.

Bevor Sie beginnen

Fügen Sie dem Client ein Zugangskontrollgerät hinzu, und stellen Sie sicher, dass das Gerät die RS-485-Schnittstelle unterstützt.

Schritte

1. Rufen Sie das Modul Zugangskontrolle auf.
2. Geben Sie in der Navigationsleiste links **Erweiterte Funktion** → **Weitere Parameter** ein.

3. Wählen Sie ein Zutrittskontrollgerät in der Geräteliste und klicken Sie auf **RS-485**, um die Seite RS-485-Einstellungen aufzurufen.
4. Wählen Sie die Nummer der seriellen Schnittstelle aus der Dropdown-Liste, um die RS-485-Parameter einzustellen.
5. Stellen Sie die Baudrate, das Datenbit, das Stoppbit, den Paritätstyp, den Kommunikationsmodus, den Arbeitsmodus und den Verbindungsmodus in der Dropdown-Liste ein.

Hinweis

Wenn der Verbindungsmodus "**Zugangskontrollgerät verbinden**" lautet, können Sie als Ausgabotyp "**Kartenummer**" oder "**Personen-ID**" wählen.

6. Klicken Sie auf **Speichern**.
 - Die konfigurierten Parameter werden automatisch auf das Gerät angewendet.
 - Wenn Sie den Arbeitsmodus oder den Verbindungsmodus ändern, wird das Gerät automatisch neu gestartet.

15.6.7 Wiegand-Parameter einstellen

Sie können den Wiegand-Kanal des Zugangskontrollgeräts und den Kommunikationsmodus einstellen. Nach der Einstellung der Wiegand-Parameter kann das Gerät über die Wiegand-Kommunikation eine Verbindung zum Wiegand-Kartenleser herstellen.

Bevor Sie beginnen

Fügen Sie dem Client ein Zugangskontrollgerät hinzu, und stellen Sie sicher, dass das Gerät Wiegand unterstützt.

Schritte

1. Rufen Sie das Modul Zugangskontrolle auf.
2. Geben Sie in der Navigationsleiste links **Erweiterte Funktion** → **Weitere Parameter** ein.
3. Wählen Sie ein Zutrittskontrollgerät in der Geräteliste aus und klicken Sie auf **Wiegand**, um die Seite Wiegand-Einstellungen aufzurufen.
4. Stellen Sie den Schalter auf on, um die Wiegand-Funktion für das Gerät zu aktivieren.
5. Wählen Sie die Wiegand-Kanal-Nr. und den Kommunikationsmodus aus der Dropdown-Liste.

Hinweis

Wenn Sie die **Kommunikationsrichtung** auf **Senden** einstellen, müssen Sie den **Wiegand-Modus** auf **Wiegand 26** oder **Wiegand 34** einstellen.

6. Klicken Sie auf **Speichern**.
 - Die konfigurierten Parameter werden automatisch auf das Gerät angewendet.
 - Nach dem Wechsel der Kommunikationsrichtung wird das Gerät automatisch neu gestartet.

15.7 Konfigurieren von Verknüpfungsaktionen für die Zugriffskontrolle

Sie können verschiedene Verknüpfungsaktionen für das vom Zugangskontrollgerät erkannte Ereignis konfigurieren. Danach werden die Verknüpfungsaktionen ausgelöst, sobald das Ereignis eintritt. Dieser Mechanismus wird verwendet, um das Sicherheitspersonal über das Ereignis zu benachrichtigen oder eine automatische Zugangskontrolle in Echtzeit auszulösen.

Es werden zwei Arten von Verknüpfungsaktionen unterstützt:

- **Client-Aktionen:** Wenn das Ereignis erkannt wird, werden Aktionen auf dem Client ausgelöst, wie z. B. ein akustisches Warnsignal des Clients.
- **Geräte-Aktionen:** Wenn das Ereignis erkannt wird, löst es die Aktionen eines bestimmten Geräts aus, z. B. das Summieren eines Kartenlesers und das Öffnen/Schließen einer Tür.

15.7.1 Client-Aktionen für Zugriffseignis konfigurieren

Auch wenn Sie weit von einem Zugangspunkt entfernt sind, können Sie über den Client erfahren, was passiert und wie dringend das Ereignis ist, indem Sie Client-Aktionen für das Zugangseignis konfigurieren. Mit Client-Aktionen sind hier die Aktionen gemeint, die automatisch vom Client selbst ausgeführt werden, wie z. B. ein akustisches Warnsignal und das Senden einer E-Mail. Sobald ein Ereignis ausgelöst wird, benachrichtigt der Client das Sicherheitspersonal, so dass dieses das Ereignis rechtzeitig bearbeiten kann.

Bevor Sie beginnen

Fügen Sie dem Client ein Zugangskontrollgerät hinzu.

Schritte

1. Klicken Sie auf **Ereigniskonfiguration** → **Zugriffskontrollereignis**.
Die hinzugefügten Zutrittskontrollgeräte werden in der Geräteliste angezeigt.
2. Wählen Sie eine Ressource (einschließlich Gerät, Alarmeingang, Tür/Aufzug und Kartenleser) aus der Geräteliste aus.
Es erscheinen die Ereignistypen, die die ausgewählte Ressource unterstützt.
3. Wählen Sie das/die Ereignis(e) und klicken Sie auf **Priorität bearbeiten**, um die Priorität für das/die Ereignis(e) festzulegen, die zum Filtern von Ereignissen im Event Center verwendet werden kann.
4. Legen Sie die Verknüpfungsaktionen des Ereignisses fest.
 - 1) Wählen Sie das/die Ereignis(e) und klicken Sie auf **Verknüpfung bearbeiten**, um die Client-Aktionen festzulegen, wenn das/die Ereignis(e) ausgelöst werden.

Akustische Warnung

Die Client-Software gibt eine akustische Warnung aus, wenn das Ereignis ausgelöst wird. Sie können einen Alarmton für die akustische Warnung auswählen.

 **Hinweis**

Einzelheiten zum Einstellen des Alarmtons finden Sie unter **Alarmton einstellen**.

E-Mail senden

Senden Sie eine E-Mail-Benachrichtigung über das Ereignis an einen oder mehrere Empfänger.

Einzelheiten zum Festlegen von E-Mail-Parametern finden Sie unter **Festlegen von E-Mail-Parametern**.

Pop-up-Fenster

Pop-up-Fenster zur Anzeige der Ereignisinformationen (einschließlich der Ereignisdetails, des ereignisbezogenen Videomaterials und des ereignisbezogenen Bildes) auf dem Software-Client, wenn das Ereignis ausgelöst wird.

Anzeige auf der Karte

Wenn die Ereignisquelle als Hotspot auf der Karte hinzugefügt wird, wird der Hotspot mit einer roten Zahl (die die Anzahl der Ereignisse angibt, maximal 10) an der Seite angezeigt, wenn das Ereignis ausgelöst wird, was dem Sicherheitspersonal hilft, den Ort des Ereignisses zu sehen.

Sie können auch auf den Hotspot klicken, um die Ereignisdetails und das Live-Video der verknüpften Kamera anzuzeigen.

Verknüpfte Kamera

Verknüpfen Sie die ausgewählte Kamera, um ein Bild aufzunehmen, wenn das Zugangsereignis ausgelöst wird.

Wählen Sie die Kamera in der Dropdown-Liste aus.

2) Klicken Sie auf **OK**.

5. Aktivieren Sie das Ereignis, so dass bei Erkennung des Ereignisses ein Ereignis an den Client gesendet wird und die Verknüpfungsaktionen ausgelöst werden.

6. Optional: Klicken Sie auf **Kopieren**, um die Ereigniseinstellungen auf ein anderes Zutrittskontrollgerät, einen Alarmeingang, eine Tür/einen Aufzug oder einen Kartenleser zu kopieren.

15.7.2 Geräteaktionen für Zugriffseignis konfigurieren

Sie können die Verknüpfungsaktionen des Zugangskontrollgeräts für das ausgelöste Ereignis des Zugangskontrollgeräts festlegen. Wenn dann ein Ereignis ausgelöst wird, kann es den Alarmausgang, den Summer am Zutrittskontrollgerät und andere Aktionen auslösen.

Schritte

 **Hinweis**

Die Verknüpfungsaktionen sollten von dem Gerät unterstützt werden.

1. Klicken Sie auf **Zugriffskontrolle** → **Verknüpfungskonfiguration**.
2. Wählen Sie das Zugangskontrollgerät aus der Liste auf der linken Seite aus.
3. Klicken Sie auf **Hinzufügen**, um eine neue Verknüpfung hinzuzufügen.
4. Wählen Sie **Ereignisverknüpfung** als Ereignisquelle.
5. Wählen Sie den Ereignistyp und das detaillierte Ereignis, um die Verknüpfung festzulegen.
6. Legen Sie im Bereich Verknüpfungsziel die Eigenschaft Ziel fest, um diese Aktion zu aktivieren.

Summer am Controller

Das akustische Warnsignal der Zutrittskontrollvorrichtung wird ausgelöst.

Erfassen Sie

Ein ereignisbezogenes Bild wird aufgenommen, wenn das ausgewählte Ereignis eintritt.

Aufnahme

Ein ereignisbezogenes Bild wird aufgenommen, wenn das ausgewählte Ereignis eintritt.



Hinweis

Das Gerät sollte die Aufzeichnung unterstützen.

Buzzer am Lesegerät

Der akustische Warnton des Kartenlesers wird ausgelöst.

Alarm Ausgang

Der Alarmausgang wird zur Benachrichtigung ausgelöst, wenn das ausgewählte Ereignis eintritt

Alarm-Eingang

Schalten Sie den Alarmeingang scharf oder unscharf.



Hinweis

Das Gerät sollte die Funktion des Alarmeingangs unterstützen.

Zugangspunkt

Es wird der Türstatus offen, geschlossen, offen bleiben oder geschlossen bleiben ausgelöst.



Hinweis

Die Zieltür und die Quelltür können nicht dieselbe sein.

Hörspiel

Die Audio-Eingabeaufforderung wird ausgelöst. Der ausgewählte Audioindex wird entsprechend dem konfigurierten Wiedergabemodus abgespielt.

7. Klicken Sie auf **Speichern**.

8. Optional: Nachdem Sie die Geräteverknüpfung hinzugefügt haben, können Sie eine oder mehrere der folgenden Aktionen durchführen:

Verknüpfungseinstellungen bearbeiten Wählen Sie die konfigurierten Verknüpfungseinstellungen in der Geräteliste aus, und Sie können die Parameter der Ereignisquelle bearbeiten, einschließlich Ereignisquelle und Verknüpfungsziel.

Verknüpfungseinstellungen löschen Wählen Sie die konfigurierten Verknüpfungseinstellungen in der Geräteliste aus und klicken Sie auf **Löschen**, um sie zu löschen.

15.7.3 Geräteaktionen für das Durchziehen von Karten konfigurieren

Sie aktivieren die Verknüpfungsaktionen des Zutrittskontrollgeräts (z. B. das Unscharfschalten einer Zone und das Auslösen einer akustischen Aufforderung) für das Durchziehen einer bestimmten Karte. Auf diese Weise können Sie das Verhalten und den Aufenthaltsort des Karteninhabers überwachen.

Schritte

Hinweis

Sie sollte vom Gerät unterstützt werden.

1. Klicken Sie auf **Zugriffskontrolle** → **Verknüpfungskonfiguration**.
2. Wählen Sie das Zugangskontrollgerät aus der Liste auf der linken Seite aus.
3. Klicken Sie auf **Hinzufügen**, um eine neue Verknüpfung hinzuzufügen.
4. Wählen Sie **Card Linkage** als Ereignisquelle.
5. Geben Sie die Kartenummer ein oder wählen Sie die Karte aus der Dropdown-Liste aus.
6. Wählen Sie den Kartenleser aus, bei dem die Karte eingezogen wird.
7. Legen Sie im Bereich Verknüpfungsziel die Eigenschaft Ziel fest, um diese Aktion zu aktivieren.

Summer am Controller

Das akustische Warnsignal der Zutrittskontrollvorrichtung wird ausgelöst.

Buzzer am Lesegerät

Der akustische Warnton des Kartenlesers wird ausgelöst.

Erfassen Sie

Ein ereignisbezogenes Bild wird aufgenommen, wenn das ausgewählte Ereignis eintritt.

Aufnahme

Ein ereignisbezogenes Bild wird aufgenommen, wenn das ausgewählte Ereignis eintritt.

 **Hinweis**

Das Gerät sollte die Aufzeichnung unterstützen.

Alarm Ausgang

Der Alarmausgang wird zur Benachrichtigung ausgelöst.

Alarm-Eingang

Schalten Sie den Alarmeingang scharf oder unscharf.

 **Hinweis**

Das Gerät sollte die Funktion des Alarmeingangs unterstützen.

Zugangspunkt

Es wird der Türstatus offen, geschlossen, offen bleiben oder geschlossen bleiben ausgelöst.

Hörspiel

Die Audio-Eingabeaufforderung wird ausgelöst. Der ausgewählte Audioindex wird entsprechend dem konfigurierten Wiedergabemodus abgespielt.

8. Klicken Sie auf **Speichern**.

Wenn die Karte (konfiguriert in Schritt 5) über den Kartenleser (konfiguriert in Schritt 6) gezogen wird, kann sie die damit verbundenen Aktionen (konfiguriert in Schritt 7) auslösen.

9. Optional: Nachdem Sie die Geräteverknüpfung hinzugefügt haben, können Sie eine oder mehrere der folgenden Aktionen durchführen:

Verknüpfungseinstellungen löschen Wählen Sie die konfigurierten Verknüpfungseinstellungen in der Geräteliste aus und klicken Sie auf **Löschen**, um sie zu löschen.

Verknüpfungseinstellungen bearbeiten Wählen Sie die konfigurierten Verknüpfungseinstellungen in der Geräteliste aus, und Sie können die Parameter der Ereignisquelle bearbeiten, einschließlich Ereignisquelle und Verknüpfungsziel.

15.7.4 Geräte-Aktionen für Personen-ID konfigurieren

Sie können die Verknüpfungsaaktionen des Zutrittskontrollgeräts für die angegebene Personen-ID festlegen. Wenn das Zutrittskontrollgerät die angegebene Personen-ID erkennt, kann es den Alarmausgang, den Summer auf dem Kartenleser und andere Aktionen auslösen, um eine spezielle Überwachung der angegebenen Person zu realisieren.

Schritte

 **Hinweis**

Sie sollte vom Gerät unterstützt werden.

1. Klicken Sie auf **Zugriffskontrolle** → **Verknüpfungskonfiguration**.
2. Wählen Sie das Zugangskontrollgerät aus der Liste auf der linken Seite aus.
3. Klicken Sie auf **Hinzufügen**, um eine neue Verknüpfung hinzuzufügen.
4. Wählen Sie **Personenverknüpfung** als Ereignisquelle.
5. Geben Sie die Mitarbeiternummer ein oder wählen Sie die Person aus der Dropdown-Liste aus.
6. Wählen Sie den Kartenleser aus, bei dem die Karte eingezogen wird.
7. Legen Sie im Bereich Verknüpfungsziel die Eigenschaft Ziel fest, um diese Aktion zu aktivieren.

Summer am Controller

Das akustische Warnsignal der Zutrittskontrollvorrichtung wird ausgelöst.

Buzzer am Lesegerät

Der akustische Warnton des Kartenlesers wird ausgelöst.

Erfassen Sie

Ein ereignisbezogenes Bild wird aufgenommen, wenn das ausgewählte Ereignis eintritt.

Aufnahme

Ein ereignisbezogenes Bild wird aufgenommen, wenn das ausgewählte Ereignis eintritt.



Hinweis

Das Gerät sollte die Aufzeichnung unterstützen.

Alarm Ausgang

Der Alarmausgang wird zur Benachrichtigung ausgelöst.

Alarm-Eingang

Schalten Sie den Alarmeingang scharf oder unscharf.



Hinweis

Das Gerät sollte die Zonenfunktion unterstützen.

Zugangspunkt

Es wird der Türstatus offen, geschlossen, offen bleiben oder geschlossen bleiben ausgelöst.

Hörspiel

Die Audio-Eingabeaufforderung wird ausgelöst. Der ausgewählte Audioindex wird entsprechend dem konfigurierten Wiedergabemodus abgespielt.

8. Klicken Sie auf **Speichern**.
9. Optional: Nachdem Sie die Geräteverknüpfung hinzugefügt haben, können Sie eine oder mehrere der folgenden Aktionen durchführen:

Verknüpfungseinstell Wählen Sie die konfigurierten Verknüpfungseinstellungen in der

ungen löschen	Geräteliste aus und klicken Sie auf Löschen , um sie zu löschen.
Verknüpfungseinstellungen bearbeiten	Wählen Sie die konfigurierten Verknüpfungseinstellungen in der Geräteliste aus, und Sie können die Parameter der Ereignisquelle bearbeiten, einschließlich Ereignisquelle und Verknüpfungsziel.

15.8.1 Status der Kontrolltür

Sie können den Status für die Tür(en) steuern, einschließlich Tür entriegeln, Tür verriegeln, Tür unverriegelt lassen, Tür verriegelt lassen, alles unverriegelt lassen usw.

Bevor Sie beginnen

- Fügen Sie eine Person hinzu und weisen Sie ihr eine Zugangsberechtigung zu. Die Person hat dann die Zugangsberechtigung zu den Zugangspunkten (Türen). Weitere Informationen finden Sie unter **Personenverwaltung** und **Zugriffsgruppe festlegen, um Personen eine Zugriffsberechtigung zuzuweisen**.
- Vergewissern Sie sich, dass der Betriebsbenutzer die Berechtigung für die Zugangspunkte (Türen) hat. Einzelheiten dazu finden Sie unter **Benutzer hinzufügen**.

Schritte

1. Klicken Sie auf **Überwachung**, um die Seite zur Statusüberwachung aufzurufen.
2. Wählen Sie eine Zugangspunktgruppe in der oberen rechten Ecke aus.

Hinweis

Informationen zur Verwaltung der Zugangspunktgruppe finden Sie unter **Gruppenverwaltung**.

Die Türen der ausgewählten Zutrittskontrollgruppe werden angezeigt.

3. Klicken Sie auf ein Türsymbol, um eine Tür auszuwählen, oder drücken Sie die **Strg-Taste** und wählen Sie mehrere Türen aus.

Hinweis

Bei den Optionen "**Alles entriegelt lassen**" und "**Alles verriegelt lassen**" können Sie diesen Schritt ignorieren.

4. Klicken Sie auf die folgenden Schaltflächen, um die Tür zu steuern.

freischalten

Wenn die Tür verriegelt ist, entriegeln Sie sie und sie wird einmalig geöffnet. Nach Ablauf der Öffnungszeit wird die Tür automatisch geschlossen und wieder verriegelt.

Schloss

Wenn die Tür entriegelt ist, verriegeln Sie sie und sie wird geschlossen. Die Person, die die Zugangsberechtigung hat, kann die Tür mit einem Ausweis öffnen.

Unverriegelt bleiben

Die Tür wird entriegelt (unabhängig davon, ob sie geschlossen oder geöffnet ist). Alle Personen können die Tür betreten, ohne sich ausweisen zu müssen.

Verschlossen bleiben

Die Tür wird geschlossen und verriegelt. Mit Ausnahme der Superuser kann keine Person die Tür öffnen, selbst wenn sie über die entsprechenden Berechtigungsnachweise verfügt.

Bleiben Sie alle freigeschaltet

Alle Türen in der Gruppe werden entriegelt (unabhängig davon, ob sie geschlossen oder geöffnet sind). Alle Personen können die Türen betreten, ohne dass ein Ausweis erforderlich ist.

Bleiben Sie alle verschlossen

Alle Türen in der Gruppe werden geschlossen und verriegelt. Mit Ausnahme der Superuser kann niemand die Türen betreten, selbst wenn er/sie über die entsprechenden Berechtigungsnachweise verfügt.

Erfassen Sie

Nehmen Sie ein Bild manuell auf.



Hinweis

Die Schaltfläche **Aufnehmen** ist verfügbar, wenn das Gerät die Aufnahmefunktion unterstützt. Das Bild wird auf dem PC gespeichert, auf dem der Client läuft. Informationen zum Festlegen des Speicherpfads finden Sie unter **Festlegen des Dateispeicherpfads**.

Ergebnis

Das Symbol der Türen ändert sich in Echtzeit entsprechend dem Vorgang, wenn der Vorgang erfolgreich war.

15.8.3 Echtzeit-Zugangsdaten prüfen

Die Echtzeit-Zugangsdaten können auf dem Client angezeigt werden, einschließlich der Daten zum Durchziehen der Karte, zur Gesichtserkennung, zur Hautoberflächentemperatur usw. Außerdem können Sie die Personeninformationen und das während des Zutritts aufgenommene Bild anzeigen.

Bevor Sie beginnen

Sie haben dem Client Person(en) und Zutrittskontrollgerät(e) hinzugefügt. Weitere Informationen finden Sie unter **Personenverwaltung** und **Gerät hinzufügen**.

Schritte

1. Klicken Sie auf **Überwachung**, um das Überwachungsmodul aufzurufen.

Die Echtzeit-Zugangsdaten werden unten auf der Seite angezeigt. Sie können die Details der Aufzeichnungen einsehen, einschließlich Kartenummer, Name der Person, Zeitpunkt des

Ereignisses, Standort der Tür, Temperatur, Authentifizierungsart usw.

Abbildung 15-12 Echtzeit-Zugriffsdatensätze

Hinweis

Sie können mit der rechten Maustaste auf den Spaltennamen der Zugriffsereignistabelle klicken, um die Spalte je nach Bedarf ein- oder auszublenden.

2. Optional: Wählen Sie eine Zugangspunktgruppe aus der Dropdown-Liste in der oberen rechten Ecke aus, um die Echtzeit-Zugangsdaten der ausgewählten Gruppe anzuzeigen.
 3. Wahlweise: Überprüfen Sie den Ereignistyp und den Ereignisstatus.
Die erkannten Ereignisse mit geprüftem Typ und Status werden in der Liste unten angezeigt.
 4. Optional: Markieren Sie **Letztes Ereignis anzeigen**, um den letzten Zugriffsdatensatz anzuzeigen.
Die Liste der Aufzeichnungen wird in umgekehrter chronologischer Reihenfolge aufgeführt.
 5. Optional: Aktivieren Sie das Kontrollkästchen **Eingabeaufforderung für abnormale Temperatur**, um die Eingabeaufforderung für abnormale Hautoberflächentemperaturen zu aktivieren.
-


Hinweis

Wenn diese Funktion aktiviert ist, erscheint beim Aufrufen des Überwachungsmoduls ein Fenster "Abnormale Temperatur", in dem das Bild der Person, die Hautoberflächentemperatur, die Kartenummer, der Name der Person usw. angezeigt werden, wenn Informationen über abnormale Temperaturen vorliegen.


6. Wahlweise: Klicken Sie auf ein Ereignis, um Bilder der Person (einschließlich aufgenommenem Bild und Profil) anzuzeigen.
-

Hinweis

Im Feld **Verknüpftes Bild aufnehmen** können Sie auf das aufgenommene Bild doppelklicken, um eine vergrößerte Ansicht zu erhalten.

7. Optional: Klicken Sie auf , um Überwachungsdetails (einschließlich detaillierter Informationen zur Person und des aufgenommenen Bildes) anzuzeigen.
-


Hinweis

In dem Pop-up-Fenster können Sie auf  klicken, um die Überwachungsdetails im Vollbildmodus anzuzeigen.

Kapitel 19 Logsuche

Es gibt zwei Protokolltypen: Betriebsprotokoll und Systemprotokoll. Die Betriebsprotokolle beziehen sich auf die normalen Vorgänge, die der Benutzer auf dem Client durchgeführt hat, z. B. Hinzufügen eines Geräts, Zurücksetzen des Passworts, Starten der Live-Ansicht usw., während die Systemprotokolle die Systeminformationen aufzeichnen, z. B. Anmeldung, Abmeldung, Sperren und Entsperrungen usw. Sie können die Protokolldateien durchsuchen und die Protokolldetails, einschließlich Zeit, Benutzer usw., anzeigen.

Schritte

1. Rufen Sie das Modul Log Search auf.
2. Klicken Sie auf  , um die Start- und Endzeit anzugeben.


Hinweis

Sie können die Protokolle innerhalb eines Monats durchsuchen.

3. Wählen Sie einen Benutzer aus, um die Protokolldateien zu durchsuchen, die erzeugt werden, wenn dieser Benutzer auf dem Client arbeitet.
4. Wählen Sie **Betriebsprotokoll** oder **Systemprotokoll** als Protokolltyp.
5. Klicken Sie auf **Suchen**.

Die Protokolldateien zwischen der Startzeit und der Endzeit werden in der Liste angezeigt. Sie können die Betriebszeit, den Typ und andere Informationen zu den Protokollen überprüfen.

6. Optional: Führen Sie die folgenden Operationen durch, wenn zu viele Protokolldateien vorhanden sind.

- Klicken Sie auf  auf jede Tabellenüberschrift und wählen Sie, um die Protokolle zu filtern.

Sortieren

Klicken Sie auf den Tabellenkopf, um die Protokolle nach Zeit oder Buchstabenfolge zu sortieren.

Kapitel 20 Benutzerverwaltung

Um die Sicherheit des Systems zu erhöhen, sollte der Administrator verschiedene Konten für verschiedene Benutzer einrichten und ihnen unterschiedliche Berechtigungen zuweisen. Um zu vermeiden, dass verschiedene Personen dasselbe Benutzerkonto verwenden, empfehlen wir, die Benutzerkonten regelmäßig zu verwalten.

20.1 Benutzer hinzufügen

Der Superuser und der Administrator können neue Benutzer hinzufügen und bei Bedarf unterschiedliche Berechtigungen für verschiedene Benutzer vergeben.

Führen Sie diese Aufgabe aus, um ein Benutzerkonto hinzuzufügen.

Schritte

Hinweis

Das Benutzerkonto, das Sie für die Anmeldung bei der Software registriert haben, ist als Superuser festgelegt.

1. Rufen Sie das Modul Benutzerverwaltung auf.
2. Klicken Sie auf **Benutzer hinzufügen**, um den Benutzerinformationsbereich anzuzeigen.
3. Wählen Sie den Benutzertyp aus der Dropdown-Liste aus.

Verwalter

Das Administratorkonto verfügt standardmäßig über alle Berechtigungen und kann die Passwörter und Berechtigungen aller Betreiber und seines eigenen Kontos ändern.

Betreiber

Das Betreiberkonto hat standardmäßig keine Berechtigung und Sie können die Berechtigungen manuell zuweisen. Ein Betreiber kann nur die Passwörter seines eigenen Kontos und der Konten, die er hinzugefügt hat, ändern.

4. Geben Sie den Benutzernamen, das Kennwort und das Bestätigungskennwort wie gewünscht ein.

 **Vorsicht**

Die Passwortstärke des Geräts kann automatisch überprüft werden. Wir empfehlen Ihnen dringend, das Passwort Ihrer Wahl zu ändern (mit mindestens 8 Zeichen, darunter mindestens drei Arten der folgenden Kategorien: Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen), um die Sicherheit Ihres Produkts zu erhöhen. Und wir empfehlen Ihnen, Ihr Passwort regelmäßig zu ändern, vor allem im Hochsicherheitssystem kann eine monatliche oder wöchentliche Änderung des Passworts Ihr Produkt besser schützen. Die ordnungsgemäße Konfiguration aller Kennwörter und anderer Sicherheitseinstellungen liegt in der Verantwortung des Installateurs und/oder des Endbenutzers.

5. Aktivieren Sie die Kontrollkästchen, um dem erstellten Benutzer die Berechtigungen zuzuweisen.
 6. Optional: Klicken Sie auf **Standardwert**, um die Standardberechtigungen für diesen Benutzer wiederherzustellen.
 7. Klicken Sie auf **Speichern**.
-

 **Hinweis**

Es können bis zu 50 Benutzerkonten für die Client-Software hinzugefügt werden.

Nachdem das Benutzerkonto erfolgreich erstellt wurde, wird es zur Benutzerliste auf der Seite Kontoverwaltung hinzugefügt.

8. Optional: Führen Sie nach der Erstellung des Benutzerkontos die folgenden Vorgänge aus.

Benutzer bearbeiten Klicken Sie auf einen Benutzer in der Liste, um die Benutzerinformationen zu bearbeiten.

 **Hinweis**

Nur das Passwort des Superusers kann bearbeitet werden.

Benutzer löschen Wählen Sie den Benutzer in der Liste aus und klicken Sie auf **Benutzer löschen**.

 **Hinweis**

Sie können den Superuser nicht löschen.

20.2 Passwort des Benutzers ändern

Der Administrator kann das Kennwort eines normalen Benutzers ändern, ohne das alte Kennwort einzugeben, während der Administrator das alte Kennwort eingeben sollte, wenn er das eigene

Kennwort ändert.

Bevor Sie beginnen

Benutzer zum Software-Client hinzufügen.

Schritte

1. Rufen Sie das Modul Benutzerverwaltung auf.
2. Wählen Sie den Benutzer, dessen Passwort geändert werden soll, und klicken Sie auf **Ändern**.
3. Wahlweise: Geben Sie das alte Passwort ein.

Hinweis

Wenn Sie das Administratorkennwort ändern, müssen Sie zuerst das alte Kennwort eingeben.

4. Geben Sie das neue Passwort ein und bestätigen Sie das Passwort.
5. Klicken Sie auf **OK**.

Kapitel 21 Systemkonfiguration

21.1 Allgemeine Parameter einstellen

Sie können die häufig verwendeten Parameter konfigurieren, z. B. die Ablaufzeit des Protokolls, die Netzwerkleistung usw.

Schritte

1. Rufen Sie das Modul Systemkonfiguration auf.
2. Klicken Sie auf die Registerkarte **Allgemein**, um die Seite Allgemeine Einstellungen aufzurufen.
3. Konfigurieren Sie die allgemeinen Parameter.

Datumsformat / Zeitformat

Die Art der Anzeige von Datum und Uhrzeit auf den entsprechenden Seiten.

Aufbewahrungsfrist für Protokolle

Die Zeit für die Aufbewahrung der Protokolldateien. Bei Überschreitung werden die Dateien gelöscht.

Maximaler Modus

Wählen Sie **Maximieren** oder **Vollbild** als maximalen Modus. Im Modus **Maximieren** können Sie die Anzeige maximieren und die Taskleiste einblenden. Im Vollbildmodus kann der Client im Vollbildmodus angezeigt werden.

Leistung des Netzes

Stellen Sie die Netzbedingungen auf **Normal**, **Besser** oder **Bestens** ein.

Bilder im Strukturdatenformat speichern

- Nachdem das **Speichern von Bildern im Strukturdatenformat** aktiviert wurde, ist das Modul **Registriertes Bild** in **Person löschen** verfügbar. Wenn die Informationen einer Person erfolgreich auf das/die Gerät(e) angewendet wurden, wird das Bild der Person automatisch gelöscht und kein Bild wird in den Basisinformationen angezeigt. In der Spalte "**Gesicht**" im Modul "**Person**" wird die Nummer des/der hinzugefügten Gesichtsbildes/Gesichtsbilder angezeigt.
- Wenn "**Bilder im Strukturdatenformat speichern**" aktiviert ist, werden im Feld "Ereignisdetails" im Ereignis-Center keine Bilder angezeigt.

Tastatur und Joystick einschalten

Aktivieren Sie die Tastatur oder den Joystick. Nach der Aktivierung können Sie die Tastenkombinationen für die Tastatur und den Joystick festlegen.

Hinweis

Einzelheiten finden Sie unter **Tastatur- und Joystick-Kurzbefehle festlegen.**

Informationen zur Person exportieren

Wenn Sie dies aktivieren, wird die Schaltfläche **Exportieren** zum Exportieren von Personendaten auf der Seite Personenverwaltung angezeigt. Achten Sie bitte auf die Sicherheit der Personendaten.

Aufbewahrungsfrist für Ereignisse

Der Zeitraum, in dem die Ereignisinformationen aufbewahrt werden. Wenn die Aufbewahrungsfrist abgelaufen ist, wird der Ereignisdatensatz automatisch gelöscht.

Automatische Zeitsynchronisation

Automatische Synchronisierung der Uhrzeit der hinzugefügten Geräte mit der Uhrzeit des PCs, auf dem der Client läuft, zu einem bestimmten Zeitpunkt.

Auto-Upgrade Gerät

Legen Sie den Aktualisierungsmodus fest, nachdem die neue Version des Geräts erkannt wurde.

Deaktivieren Sie

Nach der Aktivierung lädt der Client das Firmware-Paket nicht herunter und führt kein Upgrade durch, selbst wenn der Client eine neue Version des Clients erkennt.

Bei Download und Upgrade auffordern

Nachdem der Client eine neue Version des Geräts erkannt hat, fragt er den Benutzer, ob er das Firmware-Paket herunterladen und aktualisieren möchte.

Herunterladen und Aufforderung zum Upgrade

Nachdem der Client die neue Version des Geräts erkannt hat, lädt er das Firmware-Paket automatisch herunter und fragt den Benutzer, ob er ein Upgrade durchführen möchte.

Automatisch herunterladen und auffordern

Nachdem der Client die neue Version der Geräte erkannt hat, lädt er das Firmware-Paket herunter und aktualisiert die neue Version automatisch.

Im Feld **Upgrade-Zeitpunkt** müssen Sie einen Zeitplan festlegen, in dem der Client die neue Version automatisch aktualisiert.

Land/Region

Wählen Sie die Region des Servers für ABUS Link Station, Sie können die Region auswählen, zu der Sie gehören oder die nächstgelegene Region.

4. Klicken Sie auf **Speichern**.

21.2 Live-Ansicht und Wiedergabeparameter einstellen

Sie können die Parameter für die Live-Ansicht und die Wiedergabe einstellen, z. B. das Bildformat,

die Vorspieldauer usw.

Schritte

1. Rufen Sie das Modul Systemkonfiguration auf.
2. Klicken Sie auf die Registerkarte "**Live-Ansicht**" und "**Wiedergabe**".
3. Konfigurieren Sie die Parameter für die Live-Ansicht und die Wiedergabe.

Bildformat

Wählen Sie **JPEG** oder **BMP** als Bildformat zum Speichern von Bildern.

Hinweis

Wenn der Schalter **Temperatur bei aufgenommenen Bildern anzeigen** auf EIN steht, wird standardmäßig JPEG als Bildformat gewählt und kann nicht geändert werden.

Video-Format

Wählen Sie **MP4/AVI** als Format für die aufgezeichneten Videos.

Heruntergeladene Videodateien zusammenführen

Legen Sie die maximale Größe der zusammengeführten Videodatei für das Herunterladen der Videodatei nach Datum fest.

Durchsuchen von Videodateien, die in

Durchsuchen Sie die Videodateien, die auf dem lokalen Gerät, auf dem Speicherserver oder sowohl auf dem Speicherserver als auch auf dem lokalen Gerät gespeichert sind, nach Wiedergabemöglichkeiten.

Vorspiel für

Legen Sie die Vorspielzeit für die Ereigniswiedergabe fest. Standardmäßig beträgt sie 30s.

Priorisierung der Wiedergabe von Videodateien auf dem Speicherserver

Geben Sie bevorzugt die auf dem Speicherserver aufgezeichneten Videodateien wieder. Andernfalls geben Sie die auf dem lokalen Gerät aufgezeichneten Videodateien wieder.

Aktuellen Status der Live-Ansicht nach Neustart wiederherstellen

Setzen Sie den letzten Status der Live-Ansicht fort, nachdem Sie sich erneut beim Client angemeldet haben.

Trennen von Hintergrundvideos in der Einzel-Live-Ansicht

Im Modus für die Teilung in mehrere Fenster doppelklicken Sie auf ein Live-Video, um es im Modus für die Teilung in ein Fenster anzuzeigen, und die anderen Live-Videos werden angehalten, um die Ressourcen zu schonen.

Aktivieren Sie das Rad für den Zoom

Verwenden Sie das Mausrad zum Vergrößern oder Verkleinern des Videos im PTZ-Modus bzw. zum Vergrößern oder Wiederherstellen des Videos im Digitalzoom-Modus. Auf diese Weise können Sie direkt in das Live-Video hinein- oder herauszoomen (oder es wiederherstellen), indem Sie mit der Maus scrollen.

Überspringen nicht betroffener Videos während der VCA-Wiedergabe

Das nicht betroffene Video wird während der VCA-Wiedergabe übersprungen und das nicht betroffene Video wird während der VCA-Wiedergabe nicht wiedergegeben.

4. Klicken Sie auf **Speichern**.

21.3 Bildparameter einstellen

Die Bildparameter des Clients können konfiguriert werden, z. B. der Maßstab der Ansicht, die Wiedergabeleistung usw.

Schritte

1. Öffnen Sie die Seite Systemkonfiguration.
2. Klicken Sie auf die Registerkarte **Bild**, um die Schnittstelle für die Bildeinstellungen zu öffnen.
3. Konfigurieren Sie die Bildparameter.

Ansicht Skala

Der Ansichtsmaßstab des Videos in der Live-Ansicht oder bei der Wiedergabe. Er kann auf **Vollbild, 4:3, 16:9** oder **Originalauflösung** eingestellt werden.

Hinweis

Sie können den Ansichtsmaßstab auch im Live-View-Modul einstellen. Einzelheiten dazu finden Sie unter [Live-Ansicht](#).

Leistung spielen

Die Wiedergabeleistung des Live-Videos. Sie kann als **kürzeste Verzögerung, ausgeglichen** oder **fließend** eingestellt werden.

Sie können auch die Option **Benutzerdefiniert** wählen und die Bildrate entsprechend Ihren Bedürfnissen konfigurieren.

Hardware-Dekodierung bevorzugt

Wählen Sie **D3D9** oder **D3D11**, um die Hardware-Dekodierung für Live-Ansicht und Wiedergabe zu aktivieren. Die Hardware-Dekodierung kann eine bessere Dekodierleistung und eine geringere CPU-Auslastung bei der Wiedergabe von HD-Videos in der Live-Ansicht oder bei der Wiedergabe bieten.

Hervorhebung einschalten

Markieren Sie die erkannten Objekte mit grünen Rechtecken in der Live-Ansicht und bei der Wiedergabe.

Transaktionsinformationen anzeigen

Zeigen Sie die Transaktionsinformationen in der Live-Ansicht an.

VCA-Regel

Zeigen Sie die VCA-Regel in der Live-Ansicht an.

Aktivieren des Frame-Extrahierens für High-Speed-Wiedergabe

Bei der Wiedergabe von Videos mit hoher Geschwindigkeit (8-fache Geschwindigkeit und höher) können Sie diese Funktion deaktivieren, um das Bild bei der Wiedergabe flüssiger zu machen und die Details besser erkennen zu können.

Muster des Ziels anzeigen

Nach der Aktivierung können Sie die Bewegungsspur der Zielperson im Ansichtsfenster anzeigen.

Überlagerungsregeln für das aufgenommene Bild

Stellen Sie für das Wärmebildgerät ein, dass die Temperaturinformationen und die Informationen zur Brandquelle auf den aufgenommenen Bildern angezeigt werden.

Hinweis

Nachdem Sie diese Funktion aktiviert haben, wird das unter **Systemkonfiguration** → **Live-Ansicht und Wiedergabe** eingestellte Bildformat auf JPEG geändert und kann nicht mehr bearbeitet werden.

Rauschunterdrückung

Rauschunterdrückungsmodus, der auf **Deaktivieren**, **Selbstanpassung** oder **Aktivieren** eingestellt werden kann.

4. Klicken Sie auf **Speichern**.

21.4 Bildspeicherung einstellen

Die aufgenommenen Bilder, die durch die Ereignisse an den Geräten ausgelöst werden, können auf dem PC, auf dem der ABUS CMS Service läuft, gespeichert werden. Den Speicherort der Bilder können Sie hier manuell einstellen.

Schritte





1. Rufen Sie das Modul Systemkonfiguration auf.
2. Klicken Sie auf **Ereignisbildspeicher**.
3. Stellen Sie den Schalter **Bilder im Server speichern** auf Ein.
Es werden alle Festplatten des PCs angezeigt, auf dem der ABUS CMS-Dienst läuft.
4. Wählen Sie den Datenträger zum Speichern der Bilder.
5. Klicken Sie auf **Speichern**.

21.5 Alarmton einstellen

Wenn das Ereignis ausgelöst wird, kann der Client eine akustische Warnung ausgeben, um das Sicherheitspersonal zu benachrichtigen. Sie können den Ton der akustischen Warnung in diesem

Abschnitt einstellen.

Schritte

1. Öffnen Sie die Seite Systemkonfiguration.
2. Klicken Sie auf die Registerkarte **Alarmton**, um die Seite Alarmtoneinstellungen aufzurufen.
3. Optional: Klicken Sie auf  und wählen Sie die Audiodateien aus dem lokalen Pfad für verschiedene Ereignisse aus.
4. Optional: Fügen Sie einen individuellen Alarmton hinzu.
 - 1) Klicken Sie auf **Hinzufügen**, um einen individuellen Alarmton hinzuzufügen.
 - 2) Doppelklicken Sie auf das Feld **Typ**, um den Namen des Alarmsignals nach Wunsch anzupassen.
 - 3) Klicken Sie auf  und wählen Sie die Audiodateien aus dem lokalen Pfad für verschiedene Alarme aus.
5. Optional: Klicken Sie auf  für einen Test der Audiodatei.
6. Optional: Klicken Sie auf  in der Spalte Vorgang, um den benutzerdefinierten Sound zu löschen.
7. Klicken Sie auf **Speichern**.

Hinweis

Das Format der Audiodatei kann nur WAV sein.



21.6 Einstellen der Parameter für die Zugangskontrolle und die Videosprechanlage

Sie können die Parameter für die Zugangskontrolle und die Video-Gegensprechanlage entsprechend Ihren Bedürfnissen konfigurieren.

Schritte

1. Öffnen Sie die Seite Systemkonfiguration.
2. Klicken Sie auf die Registerkarte **Zutrittskontrolle & Videosprechanlage**.
3. Geben Sie die erforderlichen Informationen ein.

Klingelton

Klicken Sie auf  und wählen Sie die Audiodatei aus dem lokalen Pfad für den Klingelton der Innenstation. Optional können Sie auf  klicken, um die Audiodatei zu testen.

Max. Ring Dauer

Geben Sie die Sekunden an, die das Klingeln maximal dauern soll. Die maximale Klingeldauer kann von 15s bis 60s eingestellt werden.

Max. Gesprächsdauer mit Innenstation

Geben Sie die Sekunden an, die das Gespräch mit der Innenstation maximal dauern soll. Die maximale Gesprächsdauer zwischen Innenstation und Client kann zwischen 120s und 600s

eingestellt werden.

Max. Gesprächsdauer mit Türstation

Geben Sie die Sekunden an, die das Gespräch mit der Türstation maximal dauern soll. Die maximale Gesprächsdauer zwischen Türstation und Client kann von 90s bis 120s eingestellt werden.

Max. Gesprächsdauer mit Zugangskontrolle

Geben Sie die Sekunden an, die das Gespräch mit dem Zutrittskontrollgerät maximal dauern soll. Die maximale Gesprächsdauer zwischen dem Zutrittskontrollgerät und dem Client kann von 90s bis 120s eingestellt werden.

4. Klicken Sie auf **Speichern**.

21.7 Dateispeicherpfad festlegen

Das Videomaterial (manuell während der Live-Ansicht aufgezeichnet und während der Wiedergabe ausgeschnitten) und die aufgenommenen Bilder werden auf dem lokalen PC gespeichert. Der Speicherpfad für diese Dateien kann festgelegt werden.

Schritte

1. Öffnen Sie die Seite Systemkonfiguration.
2. Klicken Sie auf die Registerkarte **Datei**, um die Seite Einstellungen für den Dateispeicherpfad aufzurufen.
3. Klicken Sie auf*** und wählen Sie einen lokalen Pfad für die Dateien.
4. Klicken Sie auf **Speichern**.

21.8 In der Symbolleiste angezeigte Symbole einstellen

Die Symbole und die Reihenfolge in der Symbolleiste in der Live-Ansicht und im Wiedergabefenster können angepasst werden. Sie können einstellen, welche Symbole angezeigt werden sollen und die Reihenfolge der Symbole festlegen.

Führen Sie die folgende Aufgabe aus, wenn Sie die in der Symbolleiste angezeigten Symbole einstellen möchten.

Schritte

1. Rufen Sie das Modul Systemkonfiguration auf.
2. Klicken Sie auf die Registerkarte **Symbolleiste**, um die Seite Symbolleisteneinstellungen aufzurufen.
3. Stellen Sie den Schalter **Bildschirm-Symbolleistenanzeige aktivieren** auf EIN, damit die Symbolleiste in der Live-Ansicht und im Wiedergabefenster angezeigt wird.
4. Klicken Sie auf das gewünschte Symbol, um es in der Symbolleiste anzuzeigen.
5. Optional: Ziehen Sie das Symbol, um die Reihenfolge der Symbole auf der Symbolleiste festzulegen.

Tabelle 21-1 Symbole in der Symbolleiste der Live-Ansicht















	Live-Ansicht anhalten	Halten Sie die Live-Ansicht im Anzeigefenster an.
	Erfassen Sie	Nehmen Sie das Bild im Live-View-Verfahren auf. Das aufgenommene Bild wird auf dem PC gespeichert.
	Datensatz	Starten Sie die manuelle Aufnahme. Die Videodatei wird auf dem PC gespeichert.
	PTZ-Steuerung	Starten Sie den PTZ-Modus für Speed Dome. Klicken und ziehen Sie in der Ansicht, um die PTZ-Steuerung durchzuführen.
	Zwei-Wege-Audio	Starten Sie die Zwei-Wege-Audioübertragung mit dem Gerät in der Live-Ansicht.
	Digitaler Zoom	Aktivieren Sie die Digitalzoomfunktion. Klicken Sie erneut, um die Funktion zu deaktivieren.
	Sofortige Wiedergabe	Wechseln Sie in den Sofortwiedergabemodus.
	Ferngesteuerte Konfiguration	Öffnen Sie die Fernkonfigurationsseite der Kamera in der Live-Ansicht.

Tabelle 21-2 Symbole in der Symbolleiste für die Wiedergabe

	Erfassen Sie	Nehmen Sie das Bild im Live-View-Verfahren auf. Das aufgenommene Bild wird auf dem PC gespeichert.
	Datensatz	Starten Sie die manuelle Aufnahme. Die Videodatei wird auf dem PC gespeichert.
	Digitaler Zoom	Aktivieren Sie die Digitalzoomfunktion. Klicken Sie erneut, um die Funktion zu deaktivieren.
	Herunterladen	Laden Sie die Videodateien der Kamera herunter, und die Videodateien werden auf dem PC gespeichert.
	VCA-Wiedergabe	Legen Sie die VCA-Regeln fest. Weitere Einzelheiten finden Sie unter <u>VCA-Wiedergabe</u> .
	Tag Kontrolle	Fügen Sie Standard- oder benutzerdefinierte Tags für die Videodateien hinzu, um den wichtigen Videopunkt zu markieren. Sie können das Tag auch bearbeiten.

6. Klicken Sie auf **Speichern**.

21.9 Tastatur- und Joystick-Verknüpfungen festlegen

Die Tastatur kann an den Client angeschlossen werden und zur Steuerung der PTZ-Kameras verwendet werden. Sie können Tastenkombinationen für die Tastatur und den Joystick festlegen, um einen schnellen und bequemen Zugriff auf die am häufigsten verwendeten Aktionen zu erhalten.

Führen Sie diese Aufgabe aus, wenn Sie Tastatur- und Joystick-Kurzbeefehle festlegen müssen.

Schritte

Hinweis

Diese Konfigurationsseite wird angezeigt, nachdem Tastatur und Joystick in den Allgemeinen Einstellungen aktiviert wurden. Einzelheiten finden Sie unter **Allgemeine Parameter einstellen**.

1. Rufen Sie das Modul Systemkonfiguration auf.
 2. Klicken Sie auf **Tastatur und Joystick**, um den Bereich Einstellungen für Tastatur- und Joystick-Kurzbeefehle anzuzeigen.
 3. Wählen Sie den COM-Port aus der Dropdown-Liste für die Tastatur aus, wenn die Tastatur an den mit dem Client installierten PC angeschlossen ist.
-

Hinweis

Sie können den Gerätemanager des PCs aufrufen, um den COM-Port zu überprüfen, an den die Tastatur angeschlossen ist.

4. Legen Sie Tastenkombinationen für Tastatur und Joystick fest.
 - 1) Wählen Sie einen bestimmten Funktionsnamen in der Spalte Funktion.
 - 2) Doppelklicken Sie auf das Elementfeld unter der Spalte PC-Tastatur, USB-Joystick oder USB-Tastatur.
 - 3) Wählen Sie die Funktion der zusammengesetzten Tasten oder die Nummer aus der Dropdown-Liste aus, um sie als Tastenkürzel für die Funktion der Tastatur oder des USB-Joysticks festzulegen.
5. Klicken Sie auf **Speichern**.

Beispiel

Wenn Sie für die Funktion **Fokus (+)** die Tasten **Home**, **1** und **F1** als Tastenkombinationen für die PC-Tastatur, den USB-Joystick und die USB-Tastatur festlegen, können Sie die Home-Taste auf der PC-Tastatur drücken, den Joystick in Richtung 1 steuern oder die Taste F1 auf der USB-Tastatur drücken, um die Ansicht zu vergrößern.

21.10 E-Mail-Parameter festlegen

Wenn ein Ereignis ausgelöst wird und Sie **E-Mail senden** als Verknüpfungsaktion für dieses Ereignis

festlegen können, sendet der Client eine E-Mail zur Benachrichtigung an die Empfänger. In diesem Abschnitt müssen Sie die E-Mail-Einstellungen festlegen und die Zielempfänger angeben.

Schritte

1. Rufen Sie das Modul Systemkonfiguration auf.
2. Klicken Sie auf die Registerkarte **E-Mail**, um die Schnittstelle für die E-Mail-Einstellungen zu öffnen.
3. Geben Sie die erforderlichen Informationen ein.

SMTP-Server

Die IP-Adresse des SMTP-Servers oder der Hostname (z. B. smtp.263xmail.com)

Verschlüsselungstyp

Sie können das Kontrollkästchen aktivieren, um **unverschlüsselt**, **SSL** oder **STARTTLS** auszuwählen.

Hafen

Geben Sie den für SMTP verwendeten Kommunikationsport ein. Der Port ist standardmäßig 25.

Adresse des Absenders

Die E-Mail Adresse des Absenders.

Sicherheitszertifikat (optional)

Wenn Ihr E-Mail-Server eine Authentifizierung erfordert, aktivieren Sie dieses Kontrollkästchen, um die Authentifizierung für die Anmeldung beim Server zu verwenden, und geben Sie den Login-Benutzernamen und das Passwort Ihres E-Mail-Kontos ein.

Name des Benutzers

Geben Sie den Benutzernamen der Absender-E-Mail-Adresse ein, wenn die **Server-Authentifizierung** aktiviert ist.

Passwort

Geben Sie das Passwort der Absender-E-Mail-Adresse ein, wenn die **Server-Authentifizierung** aktiviert ist.

Empfänger 1 bis 3

Geben Sie die E-Mail-Adresse des Empfängers ein. Es können bis zu 3 Empfänger eingestellt werden.

4. Optional: Klicken Sie auf **Test-E-Mail senden**, um eine E-Mail zum Test an den Empfänger zu senden.
5. Klicken Sie auf **Speichern**.

21.11 Verwalten der Sicherheitsauthentifizierung

Aus Gründen der Datensicherheit sollten die Sicherheitszertifikate von Clients und hinzugefügten Servern identisch sein. Sie können festlegen, ob ein Verifizierungszertifikat erforderlich ist oder

nicht, wenn Sie die Verschlüsselung der Übertragung mit dem TLS-Protokoll (Transport Layer Security) aktivieren.

Bevor Sie einen Server zum Client hinzufügen, sollten Sie das Dienstzertifikat aus dem Client-Dienst exportieren und in den Server importieren. Wenn mehrere Clients denselben Server verwenden, sollten Sie die Sicherheitszertifikate der Clients und des Servers aufeinander abstimmen.

21.11.1 Zertifikat aus dem Service Management exportieren

Sie können das Sicherheitszertifikat aus dem aktuellen Client-Dienst exportieren und die exportierte Zertifikatsdatei in andere Clients importieren.

Schritte

1. Geben Sie das Service Management ein.
2. Klicken Sie auf **Exportieren**, um die Zertifikatsdatei auf dem lokalen PC zu speichern.

Hinweis

Die Zertifikatsdatei liegt im XML-Format vor.

Was ist als nächstes zu tun?

Nach dem Exportieren des Zertifikats können Sie das Zertifikat auf den PC kopieren, auf dem der Client installiert ist, und es in andere Clients importieren.

21.11.2 Zertifikat in den Client importieren

Wenn es mehrere Clients gibt, die auf denselben Steam-Medienserver zugreifen, sollten Sie dasselbe Zertifikat für die Clients und den Server importieren.

Bevor Sie beginnen

Vergewissern Sie sich, dass Sie das Sicherheitszertifikat von einem der Client-Dienste exportiert haben.

Hinweis

Einzelheiten finden Sie unter ***Zertifikat aus Service Management exportieren***.

Schritte

1. Kopieren Sie die vom anderen Client exportierte Zertifikatsdatei auf den lokalen PC.
2. Rufen Sie das Modul Systemkonfiguration auf.
3. Klicken Sie auf die Registerkarte **Sicherheitsauthentifizierung**, um die Schnittstelle für die Einstellung der Sicherheitsauthentifizierung zu öffnen.
4. Klicken Sie auf **Importieren**.
5. Wählen Sie die Zertifikatsdatei von Ihrem lokalen PC aus und klicken Sie auf **Öffnen**.

 **Hinweis**

Bitte starten Sie den Client neu, damit er wirksam wird.

21.11.3 Zertifikatsüberprüfung bei Übertragungsverschlüsselung

Auf der Seite Sicherheitsauthentifizierung können Sie festlegen, ob die Überprüfung des Gerätezertifikats für die Verschlüsselung der Übertragung erforderlich ist oder nicht.

Klicken Sie auf **Systemkonfiguration** → Sicherheitsauthentifizierung, **um** die Schnittstelle für die Sicherheitsauthentifizierung aufzurufen. Wählen Sie die Option Zertifikat überprüfen als **Ja** oder **Nein**.

Ja


Wenn Sie beim Hinzufügen eines Geräts die Übertragungsverschlüsselung aktivieren, müssen Sie das Gerätezertifikat in das vorgesehene Verzeichnis einfügen. Das Gerät wird dann mit Übertragungsverschlüsselung hinzugefügt und das Zertifikat wird überprüft, was das Sicherheitsniveau erhöht.

Nein

Das Gerätezertifikat ist nicht erforderlich, wenn Sie beim Hinzufügen des Geräts die Übertragungsverschlüsselung aktivieren. Und das Gerät wird mit Übertragungsverschlüsselung hinzugefügt.

Kapitel 22 Betrieb und Wartung

Im Menü können Sie Wartungsarbeiten durchführen, um eine reibungslose und komfortable Nutzung des Clients zu gewährleisten.

Klicken Sie in der oberen rechten Ecke des Clients auf  → **Datei** → **System** → **Werkzeug** und führen Sie die folgenden Schritte aus.

Logdatei öffnen

Sie können eine auf Ihrem lokalen PC gespeicherte Protokolldatei oder Protokolldateien des Clients öffnen.

Konfigurationsdatei importieren/exportieren

Sie können bei Bedarf Konfigurationsdateien vom lokalen PC auf den Client importieren und umgekehrt.

Automatische Sicherung

Wählen Sie Tag und Uhrzeit für die Sicherung von Konfigurationsdateien und Daten in der Datenbank oder die Wiederherstellung der gesicherten Daten.

Sendung

Markieren Sie ein oder mehrere Geräte, um die Broadcast-Funktion der Geräte zu aktivieren.

Batch-Wischer-Steuerung

Stapelweise Ein-/Ausschalten des Scheibenwischers.

1 VS 1 Gesichtsvergleich

Wählen Sie zwei Gesichtsbilder auf dem lokalen PC zum Vergleich aus. Die Ähnlichkeit zwischen

den beiden Bildern wird angezeigt.

Hinweis

Diese Funktion kann zur Identitätsprüfung verwendet werden und sollte vom DeepinMind-Gerät unterstützt werden.

Batch Time Sync

Synchronisieren Sie die Zeit ausgewählter Geräte mit Ihrer PC-Zeit.

Nachrichten-Warteschlange

Nach der Konfiguration der E-Mail-Verknüpfung werden hier das/die ausgelöste(n) Ereignis(e) angezeigt. Wählen Sie ein Ereignis aus und brechen Sie den Versand einer E-Mail an den Empfänger ab.

A. Benutzerdefinierte Wiegand-Regelbeschreibungen

Nehmen Sie Wiegand 44 als Beispiel. Die Einstellwerte auf der Registerkarte Custom Wiegand lauten wie folgt:

Benutzerdefinierter Wiegand-Name	Wiegand 44				
Gesamtlänge	44				
Transformationsregel (Dezimalziffer)	byFormatRule[4]=[1][4][0][0]				
Paritätsmodus	XOR-Parität				
Ungerade Parität Startbit		Länge			
Gerade Parität Startbit		Länge			
XOR Parität Startbit	0	Länge pro Gruppe	4	Gesamtlänge	40
Karten-ID Startbit	0	Länge	32	Dezimalziffer	10
Site Code Start Bit		Länge		Dezimalziffer	
OEM Start Bit		Länge		Dezimalziffer	
Hersteller Code Start Bit	32	Länge	8	Dezimalziffer	3

Wiegand-Daten

Wiegand-Daten = Gültige Daten + Paritätsdaten

Gesamtlänge

Länge der Wiegand-Daten.

Transport-Regel

4 Bytes. Zeigen Sie die Kombinationstypen der gültigen Daten an. Im Beispiel wird die Kombination aus Karten-ID und Herstellercode angezeigt. Die gültigen Daten können eine einzelne Regel oder eine Kombination aus mehreren Regeln sein.

Paritätsmodus

Gültige Parität für Wiegand-Daten. Sie können entweder ungerade oder gerade Parität wählen.

Ungerade Parität, Startbit und Länge

Wenn Sie Ungerade Parität wählen, sind diese Optionen verfügbar. Wenn das Startbit für die ungerade Parität 1 ist und die Länge 12 beträgt, beginnt das System die Berechnung der ungeraden Parität mit Bit 1. Es wird 12 Bits berechnet. Das Ergebnis steht in Bit 0. (Bit 0 ist das erste Bit.)

Gerade Parität, Startbit und Länge

Wenn Sie gerade Parität wählen, sind diese Optionen verfügbar. Wenn das Startbit der geraden Parität 12 ist und die Länge 12 beträgt, beginnt das System die Berechnung der geraden Parität mit Bit 12. Es wird 12 Bits berechnet. Das Ergebnis wird im letzten Bit angezeigt.

XOR Paritätsstartbit, Länge pro Gruppe und Gesamtlänge

Wenn Sie XOR-Parität wählen, sind diese Optionen verfügbar. Gemäß der oben angezeigten Tabelle ist das Startbit 0, die Länge pro Gruppe ist 4 und die Gesamtlänge ist 40. Das bedeutet, dass das System mit Bit 0 beginnt, alle 4 Bits berechnet und insgesamt 40 Bits berechnet (insgesamt 10 Gruppen). Das Ergebnis steht in den letzten 4 Bits. (Die Ergebnislänge ist die gleiche wie die Länge pro Gruppe.)

Karten-ID Startbit, Länge und Dezimalziffer

Wenn Sie die Transformationsregel verwenden, sind diese Elemente verfügbar. Gemäß der oben angezeigten Tabelle ist das Startbit der Karten-ID 0, die Länge beträgt 32 und die Dezimalziffer ist 10. Dies bedeutet, dass die Karten-ID ab Bit 0 aus 32 Bits besteht. (Die Länge wird hier bitweise berechnet.) Und die Länge der Dezimalziffer beträgt 10 Bit.

Startbit, Länge und Dezimalziffer des Standortcodes

Wenn Sie die Transformationsregel verwenden, sind diese Elemente verfügbar. Ausführliche Informationen finden Sie in der Erläuterung der Karten-ID.

OEM Startbit, Länge und Dezimalziffer

Wenn Sie die Transformationsregel verwenden, sind diese Elemente verfügbar. Ausführliche Informationen finden Sie in der Erläuterung der Karten-ID.

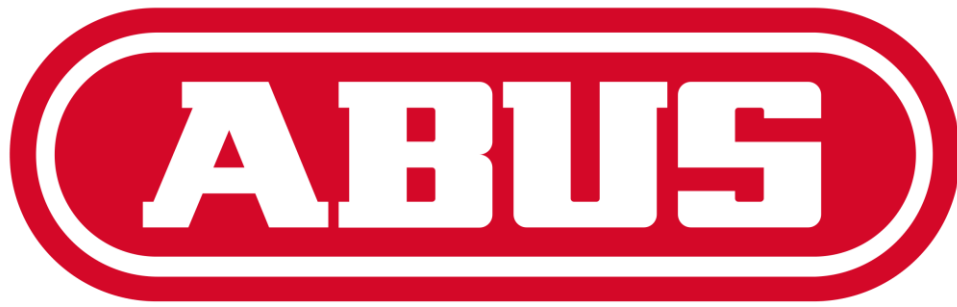
Hersteller Code Startbit, Länge und Dezimalziffer

Wenn Sie die Transformationsregel verwenden, sind diese Elemente verfügbar. Aus der obigen Tabelle geht hervor, dass das Startbit des Herstellercodes 32, die Länge 8 und die Dezimalziffer 3 ist. Das bedeutet, dass es ab Bit 32 8 Bits Herstellercode gibt. (Die Länge wird hier nach Bit berechnet.) Und die Dezimalstelle ist 3.

D. Fehlercode

Cod e	Fehler Name	Beschreibung
ABUS CMS		
317	Keine Videos.	Es wird eine Aufforderung angezeigt, wenn der Benutzer keine Berechtigung zum Abspielen hat.
HCNetSDK.dll		
1	Ungültiger Benutzername oder ungültiges Passwort.	
2	Keine Genehmigung.	Der Benutzer des Geräts hat keine ausreichende Berechtigung.
4	Ungültige Kanalnummer.	Sie werden in der Live-Ansicht der Bildschirmfernsteuerung dazu aufgefordert.
5	Es können keine weiteren Geräte angeschlossen werden.	
7	Das Gerät konnte nicht angeschlossen werden.	
23	Nicht unterstützt.	
29	Operation fehlgeschlagen.	
43	Kein Puffer.	Sie werden dazu aufgefordert, wenn Sie ein Gerät hinzufügen und der Geräteport durch einen Webserver belegt ist.
55	Ungültige IP-Adresse.	
56	Ungültige MAC-Adresse.	
91	Der Kanal unterstützt diesen Vorgang nicht.	Wenn der Sub-Stream nicht abgerufen werden kann, werden Sie dazu aufgefordert.
96	Das Gerät ist nicht im DDNS registriert.	
153	Der Benutzer ist gesperrt.	
250	Das Gerät ist nicht aktiviert.	
404	Kanal Nr. Fehler oder das Gerät unterstützt den Sub-Stream	Es wird eine Meldung angezeigt, wenn der Sub-Stream nicht abgerufen werden kann oder nicht

Cod e	Fehler Name	Beschreibung
	nicht.	vorhanden ist.
424	Die Daten für RTSP SETUP konnten nicht empfangen werden.	Sie wird beim Hinzufügen der Live-Ansicht für die Software DVS über ein externes Netzwerk abgefragt.
800	Es kann keine Bandbreite mehr genutzt werden.	
Playctrl.dll		
2		Der Stream ist kein Video- und Audiostream.
6		Das Wiedergabefenster wird schwarz, wenn H.265 in einem 64-Bit-Betriebssystem angenommen wird.



Security Tech Germany

ABUS CMS – User manual V1.0

Contents

Chapter 3 Device Management	1
3.1 Activate Devices	1
3.2 Add Device	2
3.2.1 Add Single or Multiple Online Devices	3
3.2.2 Add Device by IP Address or Domain Name	6
3.2.3 Add Devices by IP Segment	9
3.2.4 Import Devices in a Batch	12
3.3 Restore/Reset Device Password	15
3.3.1 Reset Device Password	15
3.3.2 Restore Device's Default Password	16
3.4 Upgrade Device Firmware Version	17
3.5 Manage Added Devices	18
3.6 Group Management	20
3.6.1 Group Resources	20
3.6.2 Edit Resource Parameters	21
Chapter 4 ABUS Link Station	23
4.1 Register a ABUS Link Station Account	23
4.2 Log into ABUS Link Station Account	24
Chapter 5 Live View	26
5.1 Live View Toolbar	26
5.2 Add Custom View	27
5.3 Start Live View	28
5.4 Auto-Switch in Live View	29
5.4.1 Auto-Switch Cameras in a Group	29
5.4.2 Auto-Switch All Cameras	31
5.4.3 Auto-Switch Custom Views	33
5.5 PTZ Control	35
5.5.1 PTZ Control Panel	35
5.5.2 Set Preset, Patrol, and Pattern	38

5.6 Customize Window Division	39
5.7 Manually Record and Capture	42
5.7.1 Manually Record Video	42
5.7.2 View Local Videos.....	42
5.7.3 Capture Pictures	43
5.7.4 View Captured Pictures.....	43
5.8 Instant Playback	44
5.9 Live View for Fisheye Camera	45
5.9.1 Perform Live View in Fisheye Mode	45
5.9.2 PTZ Control in Fisheye Mode	47
5.9.3 Set a Preset and Patrol	47
5.11 Live View for Thermal Camera	48
5.11.1 View Fire Source Information during Live View.....	48
5.11.2 Show Temperature Information on Live View Image.....	50
5.11.3 Manually Measure Temperature.....	51
5.11.4 Display Fire Source Detection Shield Area	52
5.13 More Functions.....	53
Chapter 6 Remote Playback.....	55
6.2 Remote Storage Configuration	55
6.2.1 Store Picture and Video on DVR, NVR, or Network Camera	55
6.2.3 Store Picture and Additional Information on Local PC	57
6.2.4 Configure Recording Schedule Template	58
6.2.5 Configure Capture Schedule Template.....	59
6.3 Toolbar for Playback	60
6.4 Normal Playback.....	61
6.4.1 Search Video Footage.....	62
6.4.2 Play Video Footage.....	64
6.5 Alarm Input Playback	66
6.5.1 Search Video Footage.....	66
6.5.2 Play Video Footage.....	68
6.6 Event Playback.....	68

6.6.1 Search Video Footage/Picture	69
6.6.2 View Video Footage/Picture	69
6.9 VCA Playback	70
6.10 Synchronous Playback	72
6.11 Fisheye Camera's Video Playback	73
6.13 Download Video Footage	75
6.13.1 Download Video Footage by Date	75
6.13.2 Download for Multiple Cameras	76
Chapter 7 Event Configuration	78
7.1 Configure Event for Camera	78
7.2 Configure Event for Alarm Input	80
7.3 Configure Event for Encoding Device	81
Chapter 8 Event Center	83
8.1 Enable Receiving Event from Devices	83
8.2 View Real-Time Events	84
8.3 Search Historical Events	86
8.4 Get Events from Device	89
8.5 View Pop-up Event Information	90
Chapter 9 Map Management	92
9.1 Add Map	92
9.2 Edit Map Scale	93
9.3 Longitude and Latitude Calibration	94
9.4 Manage Hot Spot	95
9.4.1 Add Camera as Hot Spot	95
9.4.2 Add Alarm Input as Hot Spot	96
9.4.3 Add Alarm Output as Hot Spot	98
9.4.4 Add Zone as Hot Spot	99
9.4.5 Add Access Point as Hot Spot	101
Chapter 10 Statistics	103
10.1.1 People Counting Report by Encoding Device	103
10.2 View People Counting in Intersections Report	107

10.4 Heat Map Report	108
10.7 Temperature Map	110
Chapter 11 Data Retrieval	112
11.1 Vehicle Retrieval.....	112
Chapter 14 Person Management	113
14.1 Add Organization.....	113
14.2 Add Single Person.....	114
14.2.1 Configure Basic Information	114
14.2.2 Issue a Card to One Person	116
14.2.3 Upload a Face Photo from Local PC.....	119
14.2.4 Take a Photo via Client.....	119
14.2.5 Collect Face via Access Control Device.....	120
14.2.10 Configure Access Control Information	121
14.2.11 Customize Person Information	123
14.2.12 Configure Resident Information	124
14.2.13 Configure Additional Information	124
14.3 Import and Export Person Identify Information	125
14.3.1 Import Person Information	125
14.3.2 Import Person Pictures	125
14.3.3 Export Person Information	126
14.3.4 Export Person Pictures	127
14.4 Get Person Information from Access Control Device	127
14.5 Move Persons to Another Organization.....	128
14.6 Issue Cards to Persons in Batch	129
14.7 Report Card Loss.....	129
14.8 View Resource Statistics	129
Chapter 15 Access Control	131
15.2 Configure Schedule and Template.....	131
15.2.1 Add Holiday	131
15.2.2 Add Template	132
15.3 Set Access Group to Assign Access Authorization to Persons	133

15.4 Search Access Group	135
15.5 Configure Advanced Functions	136
15.5.1 Configure Device Parameters	136
15.5.2 Configure Remaining Unlocked/Locked	144
15.5.3 Configure Multi-Factor Authentication	146
15.5.4 Configure Custom Wiegand Rule	148
15.5.5 Configure Card Reader Authentication Mode and Schedule	149
15.5.6 Configure Person Authentication Mode	151
15.5.8 Configure First Person In	152
15.5.9 Configure Anti-Passback	153
15.5.10 Configure Multi-door Interlocking	154
15.5.11 Configure Authentication Code	155
15.6.3 Set Device Capture Parameters	156
15.6.4 Set Parameters for Face Recognition Terminal	157
15.6.5 Enable M1 Card Encryption	158
15.6.6 Set RS-485 Parameters	159
15.6.7 Set Wiegand Parameters	159
15.7 Configure Linkage Actions for Access Control	160
15.7.1 Configure Client Actions for Access Event	160
15.7.2 Configure Device Actions for Access Event	161
15.7.3 Configure Device Actions for Card Swiping	163
15.7.4 Configure Device Actions for Person ID	164
15.8.1 Control Door Status	166
15.8.3 Check Real-Time Access Records	167
Chapter 19 Log Search	169
Chapter 20 User Management	170
20.1 Add User	170
20.2 Change User's Password	171
Chapter 21 System Configuration	172
21.1 Set General Parameters	172
21.2 Set Live View and Playback Parameters	173

21.3 Set Image Parameters	175
21.4 Set Picture Storage	176
21.5 Set Alarm Sound	176
21.6 Set Access Control and Video Intercom Parameters	177
21.7 Set File Saving Path	177
21.8 Set Icons Shown on Toolbar.....	177
21.9 Set Keyboard and Joystick Shortcuts.....	179
21.10 Set Email Parameters	179
21.11 Manage Security Authentication.....	180
21.11.1 Export Certificate from Service Management	180
21.11.2 Import Certificate to Client.....	181
21.11.3 Certificate Verification for Transmission Encryption.....	181
Chapter 22 Operation and Maintenance	183
A. Custom Wiegand Rule Descriptions	185
D. Error Code	187

Chapter 3 Device Management

3.1 Activate Devices

For the inactive devices, you are required to create a password to activate them before they can be added to the software and work properly.

Before You Start

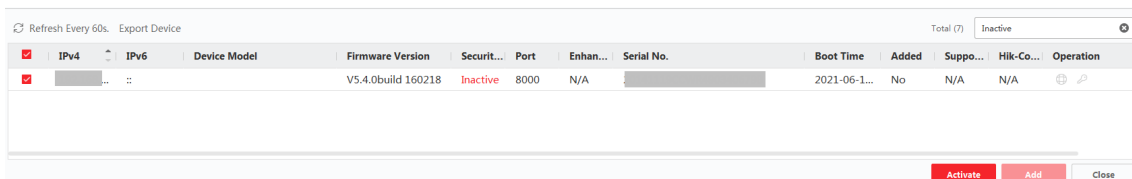
Make sure the device to be activated is connected to the network and on the same subnet with the PC where the client runs.

Steps



This function should be supported by the device.

1. Enter the Device Management page.
2. Click **Device** on the top of the right panel.
3. Click **Online Device** to show the online device list at the bottom of the page.
The searched online devices are displayed in the list.
4. Check the device status (shown on **Security Level** column) and select an inactive device.



IPv4	IPv6	Device Model	Firmware Version	Securit...	Port	Enhan...	Serial No.	Boot Time	Added	Suppo...	Hik-Co...	Operation
...	::		V5.4.0build 160218	Inactive	8000	N/A		2021-06-1...	No	N/A	N/A	⊕

Activate Add Close

Figure 3-1 Online Inactive Devices

5. Click **Activate** to open the Activation dialog.
6. Create a password in the password field, and confirm the password.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.


Note

For the NVR device, you are required to create a password in **Network Cameras' Default Password** field and confirm the password for activating network camera(s) connected to the NVR.

7. Optional: Enable ABUS Link Station service when activating the device if the device supports.
 - 1) Check **Enable Cloud P2P** to open the Note dialog.
 - 2) Create a verification code, and confirm the verification code.
 - 3) Click **Terms of Service** and **Privacy Policy** to read the requirements.
 - 4) Click **OK** to enable the ABUS Link Station service.
 8. Click **OK** to activate the device.
-

Note

If the device supports resetting password via the reserved email, security question, or GUID, you can configure them after activating the device.

9. Optional: Click  in the Operation column to edit the network information (including IP address, port number, gateway, etc.) for the online device.

3.2 Add Device

The client provides various device adding modes including IP/domain, IP segment, ABUS Link Station. The client also supports importing multiple devices in a batch when there are large

amount of devices to be added.

3.2.1 Add Single or Multiple Online Devices

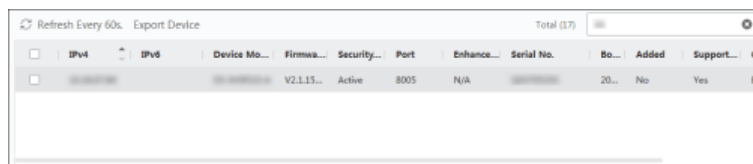
The client can detect online devices which are in the same network as the PC running the client. You can select a detected online device displayed in the online device list and add it to the client. For detected online devices sharing the same user name and password, you can add them to the client in a batch.

Before You Start

- The device(s) to be added are in the same network as the PC running the client.
- The device(s) to be added have been activated.

Steps

1. Click **Device Management** → **Device** → **Device**.
2. Click **Online Device** to show the online device area.
The searched online devices are displayed in the list.



The screenshot shows a table with columns for device information. The table has a header row and one data row. The header row includes columns for checkboxes, IPv4, IPv6, Device Mo..., Firmwa..., Security..., Port, Enhance..., Serial No., Bo..., Added, Support..., and a gear icon. The data row contains a checked checkbox, a device name, V2.1.15..., Active, 8005, N/A, a serial number, 20..., No, Yes, and Er.

<input type="checkbox"/>	IPv4	IPv6	Device Mo...	Firmwa...	Security...	Port	Enhance...	Serial No.	Bo...	Added	Support...	
<input checked="" type="checkbox"/>				V2.1.15...	Active	8005	N/A		20...	No	Yes	Er

Figure 3-2 Online Device

3. In the **Online Device** area, check one or more online device(s), and click **Add** to open the device adding window.

Add [Close]

Name

IP Address

Transmission Encryption...

Port

User Name

Password

Synchronize Time

Import to Group

i Set the device name as the group name and add all the channels connected to the device to the group.

Add **Cancel**

Figure 3-3 Add Single Online Device

Add [Close]

User Name

Password

Synchronize Time

Import to Group

i Set the device name as the group name and add all the channels connected to the device to the group.

Add **Cancel**

Figure 3-4 Add Multiple Online Devices

4. Enter the required information.

Name

Enter a descriptive name for the device.

IP Address

Enter the device's IP address. The IP address of the device is obtained automatically in this adding mode.

Port

You can customize the port number. The port number of the device is obtained automatically in this adding mode.

Note

For some device types, you can enter **80** as the port No. This function should be supported by the device.

User Name

By default, the user name is **admin** for TVVR/HDCC/NVR and **installer** for IPCs

Password

Enter the device password.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

5. Optional: Check **Transmission Encryption (TLS)** to enable transmission encryption using TLS (Transport Layer Security) protocol for security purpose.

Note

- This function should be supported by the device.
 - If you have enabled Certificate Verification, you should click **Open Certificate Directory** to open the default folder, and copy the certificate file exported from the device to this default directory to strengthen the security. See **Certificate Verification for Transmission Encryption** for details about enabling certificate verification.
 - You can log into the device to get the certificate file by web browser.
-

6. Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
7. Optional: Check **Import to Group** to create a group by the device name, and import all the channels of the device to this group.

Example

For encoding device, its encoding channels and alarm inputs/outputs will be imported to this

group.

For access control device, its access points, alarm inputs/outputs, and encoding channels (if exist) will be imported to this group.

8. Click **Add**.
9. Optional: Click **Export Device**, select the saving path and device type, and click **OK** to export the device information to your PC.

Note

Currently, the platform only supports exporting the information of video intercom devices, including door stations, indoor stations, and main stations.

3.2.2 Add Device by IP Address or Domain Name

If you know the IP address or domain name of the device to add, you can add devices to the client by specifying the IP address (or domain name), user name, password, etc.

Steps

1. Enter Device Management module.
2. Click **Device** tab on the top of the right panel.
The added devices are displayed on the right panel.

Figure 3-5 Add Device by IP Address or Domain Name

3. Click **Add** to open the Add window, and then select **IP/Domain** as the adding mode.
4. Enter the required information.

Name

Create a descriptive name for the device. For example, you can use a nickname that can show the location or feature of the device.

Address

The IP address or domain name of the device.

Port

The devices to add share the same port number. The default value is **8000**.

Note

For some device types, you can enter **80** as the port No. This function should be supported by the device.

User Name

Enter the device user name. By default, the user name is **admin**.

Password

Enter the device password.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

5. Optional: Add the offline devices.

- 1) Check **Add Offline Device**.
 - 2) Enter the required information, including the device channel number and alarm input number.
-

Note

After adding the offline device to the client, the device network status will be displayed as "Offline"; When the device comes online, the device network status will turn to "Online", and the client will connect it automatically.

6. Optional: Check **Transmission Encryption (TLS)** to enable transmission encryption using TLS (Transport Layer Security) protocol for security purpose.

Note

- This function should be supported by the device.
 - If you have enabled Certificate Verification, you should click **Open Certificate Directory** to open the default folder, and copy the certificate file exported from the device to this default directory to strengthen the security. See **Certificate Verification for Transmission Encryption** for details about enabling certificate verification.
 - You can log into the device to get the certificate file by web browser.
-

7. Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.







8. Optional: Check **Import to Group** to create a group by the device name, and import all the channels of the device to this group.

Example

For encoding device, its encoding channels and alarm inputs/outputs will be imported to this group.

For access control device, its access points, alarm inputs/outputs, and encoding channels (if exist) will be imported to this group.

9. Finish adding the device.
- Click **Add** to add the device and back to the device list page.
 - Click **Add and New** to save the settings and continue to add other device.
10. Optional: Perform the following operation(s).

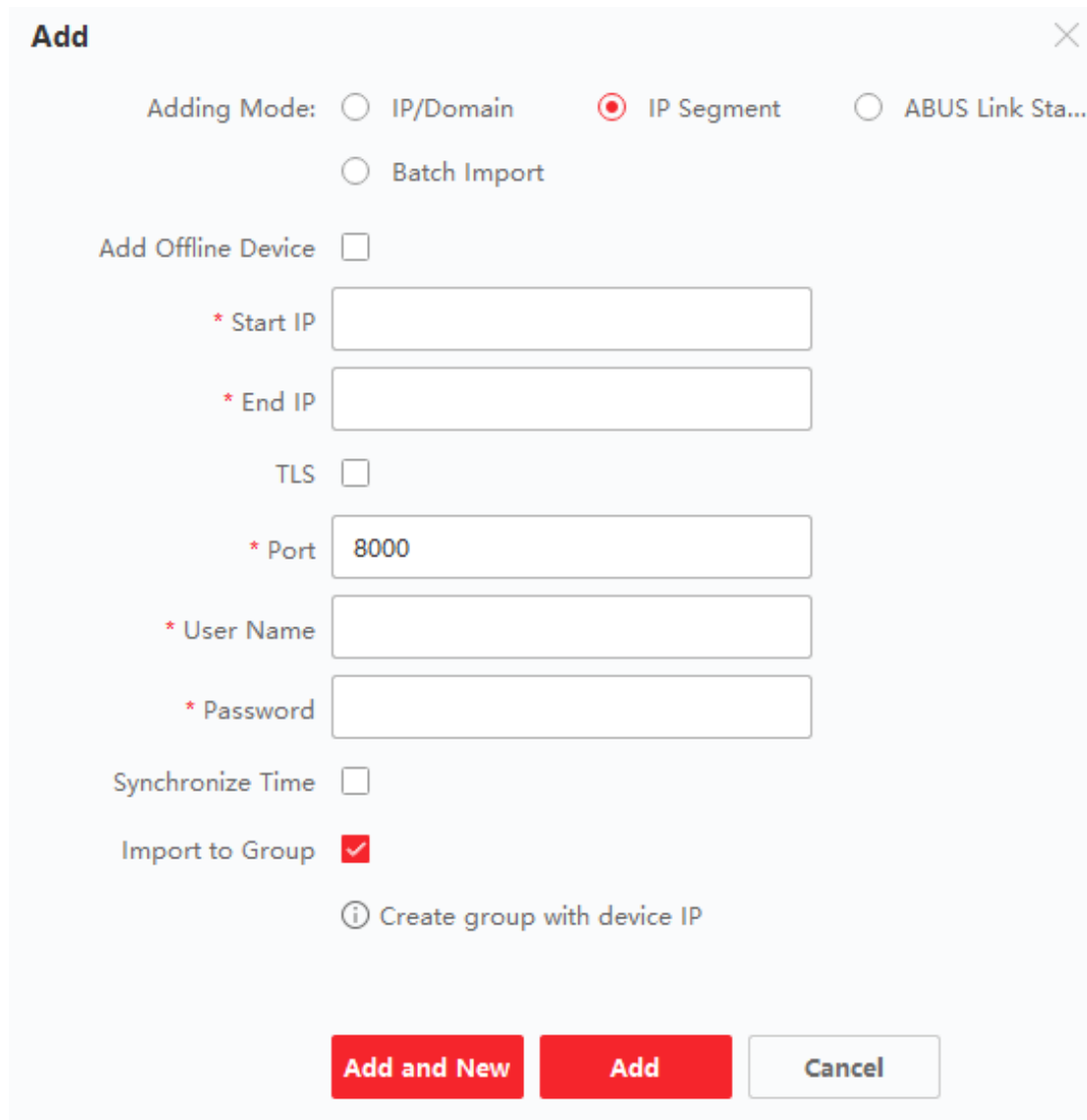
Remote Configuration	On the device list page, click  in the Operation column to perform remote configuration for a device. The  is in the rightmost column of the Device page. For details, refer to the user manual of device.
Device Status	Click  in the Operation column to view device status, including cameras, recording status, signal status, hardware status, etc.
Edit Device Information	Click  in the Operation column to edit the device information, such as IP address, user name, and password.
Check Online User	Click  in the Operation column to check the online users who access the device, such as user name, user type, user's IP address, and login time.
Refresh	Click  in the Operation column to get the latest device information.
Delete Device	Select one or multiple devices and click Delete to delete the selected device(s) from the client.

3.2.3 Add Devices by IP Segment

If the devices share the same port No., user name and password, and their IP addresses ranges in the same IP segment, you can add them to the client by specifying the start IP address and the end IP address, port No., user name, password, etc of the devices.

Steps

1. On the Maintenance and Management panel on the right side of the Client, Click **Device Management**.
2. Click **Device** tab on the top of the left panel.
The added devices are displayed on the right panel.
3. Click **Add** to open the Add window.



Add ✕

Adding Mode: IP/Domain IP Segment ABUS Link Sta...

Batch Import

Add Offline Device

* Start IP

* End IP

TLS

* Port

* User Name

* Password

Synchronize Time

Import to Group

ⓘ Create group with device IP

Add and New **Add** Cancel

Figure 3-6 Add Device by IP Segment

4. Select **IP Segment** as the adding mode.
5. Enter the required information.

Start IP

Enter a start IP address.

End IP

Enter an end IP address in the same network segment with the start IP.

Port

Enter the device port No. The default value is **8000**.

Note

For some device types, you can enter **80** as the port No. This function should be supported by the device.

User Name

By default, the user name is **admin**.

Password

Enter the device password.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

6. Optional: Add the offline devices.

- 1) Check **Add Offline Device**.
 - 2) Enter the required information, including the device channel number and alarm input number.
-

Note

After adding the offline device to the client, the device network status will be displayed as "Offline"; When the device comes online, the device network status will turn to "Online", and the client will connect it automatically.

7. Optional: Check **Transmission Encryption (TLS)** to enable transmission encryption using TLS (Transport Layer Security) protocol for security purpose .

Note

- This function should be supported by the device.
 - If you have enabled Certificate Verification, you should click **Open Certificate Folder** to open the default folder, and copy the certificate file exported from the device to this default directory to strengthen the security. See **Certificate Verification for Transmission Encryption** for details about enabling certificate verification.
 - You can log into the device to get the certificate file by web browser.
-







8. Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.

9. Optional: Check **Import to Group** to create a group by the device name, and import all the channels of the device to the group.

10. Finish adding the device.

- Click **Add** to add the device and back to the device list page.
- Click **Add and New** to save the settings and continue to add other device.

11. Optional: Perform the following operation(s).

Remote Configuration	On the device list page, click  in the Operation column to perform remote configuration for a device. The  is in the rightmost column of the Device page. For details, refer to the user manual of device.
Device Status	Click  in the Operation column to view device status, including cameras, recording status, signal status, hardware status, etc.
Edit Device Information	Click  in the Operation column to edit the device information, such as IP address, user name, and password.
Check Online User	Click  in the Operation column to check the online users who access the device, such as user name, user type, user's IP address, and login time.
Refresh	Click  in the Operation column to get the latest device information.
Delete Device	Select one or multiple devices and click Delete to delete the selected device(s) from the client.

3.2.4 Import Devices in a Batch

You can add multiple devices to the client in a batch by entering the device parameters in a pre-defined CSV file.

Steps

1. Enter the Device Management module.
2. Click **Device** tab on the top of the right panel.
3. Click **Add** to open the Add window, and then select **Batch Import** as the adding mode.

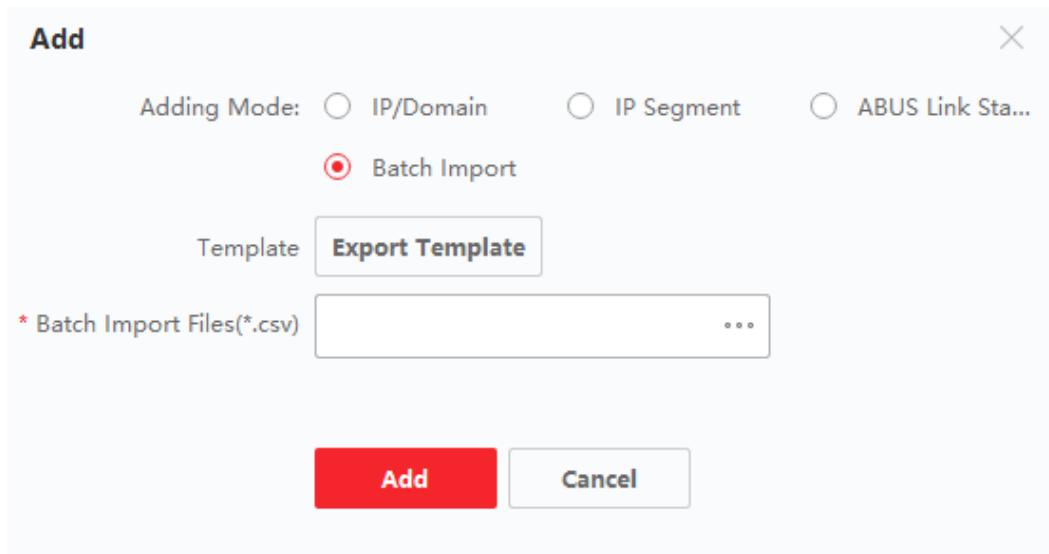


Figure 3-7 Add Devices in a Batch

4. Click **Export Template** and then save the pre-defined template (CSV file) on your PC.
5. Open the exported template file and enter the required information of the devices to be added on the corresponding column.

 **Note**

For detailed description of the required fields, refer to the introductions in the template.

Adding Mode

Enter **0** or **1** or **2**.

Address

Edit the address of the device.

Port

Enter the device port number. The default port number is **8000**.

User Name

Enter the device user name. By default, the user name is **admin**.

Password

Enter the device password.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

Add Offline Device

Enter **1** to enable adding an offline device.

After adding the offline device to the client, the device network status will be displayed as "Offline"; When the device comes online, the device network status will turn to "Online", and the client will connect it automatically. Enter **0** to disable adding an offline device.

Import to Group


Enter **1** to create a group by the device name. All the channels of the device will be imported to the corresponding group by default. Enter **0** to disable this function.






Channel Number


If you enable **Add Offline Device**, enter the channel number of the device. If you disable **Add Offline Device**, this field is not required.

Alarm Input Number

If you enable **Add Offline Device**, enter the alarm input number of the device. If you disable **Add Offline Device**, this field is not required.

6. Click  and select the template file.
7. Click **Add** to import the devices.
8. Optional: Perform the following operation(s).

Remote Configuration	On the device list page, click  in the Operation column to perform remote configuration for a device. The  is in the rightmost column of the Device page. For details, refer to the user manual of device.
Device Status	Click  in the Operation column to view device status, including cameras, recording status, signal status, hardware status, etc.
Edit Device Information	Click  in the Operation column to edit the device information, such as IP address, user name, and password.
Check Online User	Click  in the Operation column to check the online users who access the device, such as user name, user type, user's IP address, and login time.

Refresh	Click  in the Operation column to get the latest device information.
Delete Device	Select one or multiple devices and click Delete to delete the selected device(s) from the client.


3.3 Restore/Reset Device Password

If you forgot the password of the detected online devices, you can restore the device's default password or reset the device's password through the client.

3.3.1 Reset Device Password

If you forgot the password of the detected online devices, you can reset the device password via the client.

Steps

1. Enter Device Management page.
2. Click **Device** tab on the top of the right panel.
3. Click **Online Device** to show the online device area.
All the online devices sharing the same subnet will be displayed in the list.
4. Select the device from the list and click  on the Operation column.
5. Reset the device password.
 - Click **Export** to save the device file on your PC and then send the file to our technical support.

Note

For the following operations for resetting the password, contact our technical support.

- Click **Generate** to pop up the QR Code window and click **Download** to save the QR code to your PC. You can also take a photo of the QR code to save it to your phone. Send the picture to our technical support.
-

Note

For the following operations for resetting the password, contact our technical support.

- Select the Safe Mode according to actual needs.
-

Note

For the following operations for resetting the password, contact our technical support.

 **Caution**


The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

3.3.2 Restore Device's Default Password

If you forget the password of the detected online devices, you can restore their default password via the client.

Steps

1. Enter Device Management page.
2. Click **Device** tab on the top of the right panel.
3. Click **Online Device** to show the online device area at the bottom of the page.
All the online devices sharing the same subnet will be displayed in the list.
4. Select a device and click  on the Operation column to open the Reset Password window.
5. Restore the device password.
 - Enter the security code, and then you can restore the default password of the selected device.

 **Note**

For getting the security code, contact our technical support.

- Click **Export** to save the device file on your PC and send the file to our technical support.
-

 **Note**

For the following operations for resetting the password, contact our technical support.

What to do next

The default password (12345) for the admin account is for first-time login purposes only. You must change this default password to better protect against security risks, such as the unauthorized access by others to the product that may prevent the product from functioning properly and/or lead to other undesirable consequences.

 **Caution**

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

3.4 Upgrade Device Firmware Version

When there is a new firmware version available for the added device, you can upgrade its firmware version via the client.

 **Note**

- The device should support this function.
 - You can configure upgrading mode in System Configuration. See [***Set General Parameters***](#) for details.
-

Enter the Device Management module, and then click **Device** tab to show the device list. Perform the following operations according to different upgrading modes.

Disable

On the Device for Management panel, if there is a new firmware version available, the status in the Firmware Upgrade column of the device will turn to **Upgradeable**.

Select the upgradeable device and click **Upgrade** to start upgrading the device firmware.

 **Note**

The upgrade progress will show. When the upgrade is completed, the status in the Firmware Upgrade column of the device will turn to **Upgraded**.

Prompt Me If Download and Upgrade

If there is a new firmware version available, a prompt window will pop up. Click **Upgrade All** to start downloading and upgrading.

Download and Prompt Me If Upgrade

A dialog will pop up for selecting whether to upgrade after downloading package of new version. Click **Upgrade All** to start upgrading the device firmware.

 **Note**

After clicking **Upgrade All**, a prompt will pop up for viewing details. If you are not in Device Management page, click **View Details** to jump to Device Management page; if you are in Device Management page, close the prompt.

Upgrade Status

On the device management page, the following upgrade status will be shown in the Firmware Upgrade column.


No Available Version

No new firmware version available.

Upgradeable

A new firmware version available.

 **Note**

Move the cursor on  to view the current version, latest version, and upgrade content of the firmware version.

Waiting

The device is waiting for upgrade.

Downloading

The client is downloading the package of the new firmware version.

Upgrading

The upgrading of the device firmware is going on.

Upgraded

Hover the cursor on **Upgraded** to show the version after upgrading.

Upgrading Failed









When the upgrade fails, a prompt will pop up for viewing details. If you are not in Device Management page, click **View Details** to jump to Device Management page; if you are in Device Management page, close the prompt. Hover the cursor on **Upgrading Failed** to show the error details, and click **Upgrade Again** to try again.

3.5 Manage Added Devices

After adding devices to device list, you can manage the added devices including editing device

parameters, remote configuration, viewing device status, etc.

Table 3-1 Manage Added Devices

Edit Device	Click  to edit device information including device name, address, user name, password, etc.
Delete Device	Check one or more devices, and click Delete to delete the selected devices.
Remote Configuration	On the device list page, click  in the Operation column to perform remote configuration for a device. The  is in the rightmost column of the Device page. For details, refer to the user manual of device.
View Device Status	<p>Click  to view device status, including cameras, recording status, signal status, hardware status, etc.</p> <hr/> <p> Note For different devices, you will view different information about device status.</p> <hr/>
View Online User	Click  to view the details of online user who access the device, including user name, user type, IP address and login time.
Refresh Device Information	Click  to refresh and get the latest device information.
Generate QR Code	<p>Check one or more devices, and click QR Code to generate a QR code of the added device(s). You can add device(s) to the Mobile Client via scanning the QR code.</p> <hr/> <p> Note Devices added by ISUP or ABUS Link Station cannot generate a QR code.</p> <hr/>
Upgrade Device	View device status in the Firmware Upgrade column, check one or more upgradable devices, and click Upgrade Device Firmware to upgrade the selected devices. For details, refer to <u>Upgrade Device Firmware Version</u> .
Get Events from Device	Check one device, and click Get Events from Device to synchronize events. For details, refer to <u>Get Events from Device</u> .

3.6 Group Management

The client provides groups to manage the added resources in different groups. You can group the resources into different groups according to the resources' locations.

Example

For example, on the 1st floor, there mounted 64 cameras, 16 doors, 64 alarm inputs, and 16 alarm outputs. You can organize these resources into one group (named 1st Floor) for convenient management. You can get the live view, play back the video files, control door status, and do some other operations of the devices after managing the resources by groups.

3.6.1 Group Resources

The client provides two methods of adding a group: customizing a group or creating a group by device name. After customizing a group, you need to import resources into this group manually. After creating a group by the device name, the resources of the device will be imported into the group automatically. You can choose one method to group your resources according to actual needs.

Steps

1. In the Maintenance and Management area, click **Device Management** → **Group** to enter the group management page.
2. Add a group.
 - **Customize a Group:** Click **Add Group** and create a name for the new group.
 - **Create a Group by Device Name:** Click **Create Group by Device Name** and select an added device to create a new group by the name of the selected device. After creating a group by the device name, the resources (such as encoding channels, alarm inputs, alarm outputs, and access points) of the device will be automatically imported to the group.


Note

- Up to 256 groups can be added.
 - You can select multiple groups by pressing and holding Shift or Ctrl key on the keyboard.
-


3. After adding a group, you need to import resources into the group.

Note

For one resource, it can be added to different groups.

- 1) Select the type of resources to be imported, and click **Import**.
- 2) Select the resources to be imported, and click **Import** to import all the selected resources into this group.
4. Optional: After adding a group, perform one of the following operations if needed.
 - Expand or Fold** Click  to expand or fold the resource list in the group.

Resource List

Search Resource	Enter the keyword and click  to search target resources.
Remove Resource from Group	Select resource(s) and click Delete to remove the selected resource(s) from the group.
Update Resource Name	You can update all the resource names in a group or in a channel. <ul style="list-style-type: none">● Select a group, and click Update Resource Name to update all the resource names in the selected group.● Select a channel in one group, and update all the resource names in this channel. For example, click Encoding Channels → Update Camera Name to update all the camera names in encoding channels.



This function should be supported by the device.


3.6.2 Edit Resource Parameters

After importing the resources to the group, you can edit the resource parameters. For encoding channel, you can edit the channel name, stream type, protocol type, etc. For access point, you can edit the access point name. For alarm input, you can edit the alarm input name. Here we take encoding channel as an example.

Before You Start

Import the resources to group.

Steps

1. Enter the Device Management module.
2. Click **Device Management** → **Group** to enter the group management page.
All the added groups are displayed on the left.
3. Select a group on the group list and click **Encoding Channel**.
The encoding channels imported to the group will display.
4. Click  in the Operation column to open the Edit Resource window.
5. Edit the camera information, including the camera name, the stream type, etc.

Video Stream

Select the stream type for live view of the camera as desired.



You should start live view again to take effect.

Playback Stream Type

Select the stream type for playback of the camera as desired.

Note

- This field will display if the device supports dual-stream.
 - You should start live view again to take effect.
-

Rotation Type

Select the rotate type for the live view or playback of the camera as desired.

Protocol Type

Select the transmission protocol for the camera.

Note

You should start live view again to take effect.

Streaming Protocol

Select the protocol as RTSP or private for getting stream when live view.

Note

You should start live view again to take effect.

Copy to...

Copy the configured parameters to other camera(s).

Refresh

Get a new captured picture for the live view of the camera.

6. Click **OK** to save the new settings.

Chapter 4 ABUS Link Station

The client software also supports to register a ABUS Link Station account, log into your ABUS Link Station account and manage the devices which support the ABUS Link Station service.

4.1 Register a ABUS Link Station Account

The client supports registering a ABUS Link Station account to manage devices which supports ABUS Link Station service.

Steps

1. Enter the login page of ABUS Link Station.
 - Click **Log in** in the upper-right corner of the client.
 1. Click **Device Management** → **Device** to enter the Device Management page.
 2. Click **Add** to open the Add Device panel.
 3. Select **ABUS Link Station** as the adding mode.
 4. Click **Login**.

The Login window pops up.

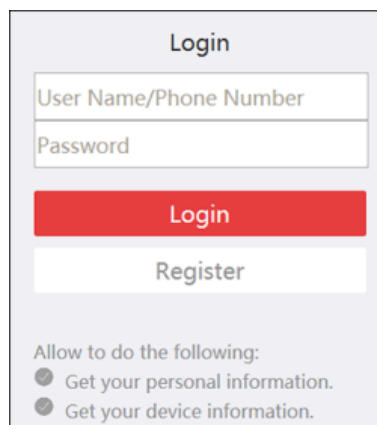


Figure 4-1 Login Window

2. Click **Register** to open the Register Account window.
3. Enter the required information, including user name, password, confirm password, and phone number/email address.

 **Caution**

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

4. Click **Send Message** to get a verification code.
The system will send verification code to your phone or email.
5. Enter the received verification code in the **Verification Code** text field.
6. Check **I have read and agreed Terms of Service Privacy Policy**.
7. Click **Register** to finish the registration.

4.2 Log into ABUS Link Station Account

You can log into ABUS Link Station account via the client, so as to operate devices managed by ABUS Link Station account.

Before You Start

Register a ABUS Link Station account.

 **Note**

For details, refer to [***Register a ABUS Link Station Account***](#).

Steps

1. Enter the login page of ABUS Link Station.
 - Click **Log in** in the upper-right corner of the client.
 1. Click **Device Management** → **Device** to enter the Device Management page.
 2. Click **Add** to open the Add Device panel.
 3. Select **ABUS Link Station** as the adding mode.
 4. Click **Login**.

The Login window pops up.

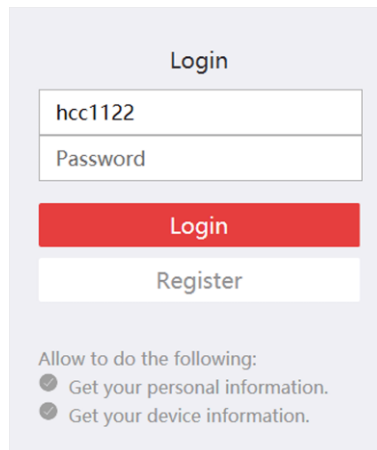


Figure 4-2 Login Page of ABUS Link Station

2. Enter user name and password.
3. Click **Log in** to log into your account.
Log in will turn to **Logged in**.
4. Optional: Click **Logged in** → **Log out** to log out of your account.

 **Note**

- Devices added by ABUS Link Station will be hidden after logging out the ABUS Link Station Service
 - Alarm-related pictures saved in ABUS Link Station will be valid for 2 hours.
-

Chapter 5 Live View

You can view the live video of the added network cameras and video encoders on the Main View page. And some basic operations are supported, including picture capturing, manual recording, window division, PTZ control, Auto-Switch in live view, etc.

5.1 Live View Toolbar

The live-view toolbar can help you operate and manage the live-view window more convenient and quick. For example, you can capture picture, record the audio, adjust the volume, split the window by the one-click of the tools on the toolbar.

Table 5-1 Descriptions of Toolbar
















Icon	Function Name	Function Description and Operation
	Save View	Save the view you create currently, which is convenient for quick viewing the required cameras. Click  to pop up the window of saving view. Select Create View or Current View , and name for the view.
	Stop Live View	Stop the all the live view cameras.
	Mute/Cancel Mute	Click  to pop up the volume bar, click  to cancel the mute and you can adjust the volume. Click  to pop up the volume bar, click  again to set the live-view cameras as mute.
	Window Division	Select the different window division mode for live view. Click  to select one window division mode (e.g. 9 window division). You can also click Add to customize a window division mode.
	Full Screen	Display the live view in full screen. Press Esc key to exit full screen mode.
	Configuration	Enter the live view parameters setting mode, configure for live view and playback, image, files and toolbar.

Table 5-2 Description of Icons on Live View Window


Icon	Function Name	Function Description and Operation
	Capture	Manually capture the pictures for the live view window.

Icon	Function Name	Function Description and Operation
	Start Recording/Stop Recording	Click the first time to start recording and click again to stop recording, and automatically save the recording files to the path you have set.
	Switch to Instant Playback	On the current time, you can select to play back the video in previous 30 s, 1 min, 3 min, 5 min, 8 min, 10 min.

5.2 Add Custom View

A view is a window division with cameras configured to each window; View mode enables you to save the window division and the correspondence between cameras and windows as favorite to quickly access the related cameras later. For example, you can link camera 1, camera 2, and camera 3 located in your office to display windows and save them as a view called office.

Steps

1. Enter the Main View page.
2. Click **Resource** tab.
3. Move the cursor to the Custom View in the resource panel and click  to create a new view.
4. Enter a name for the view.

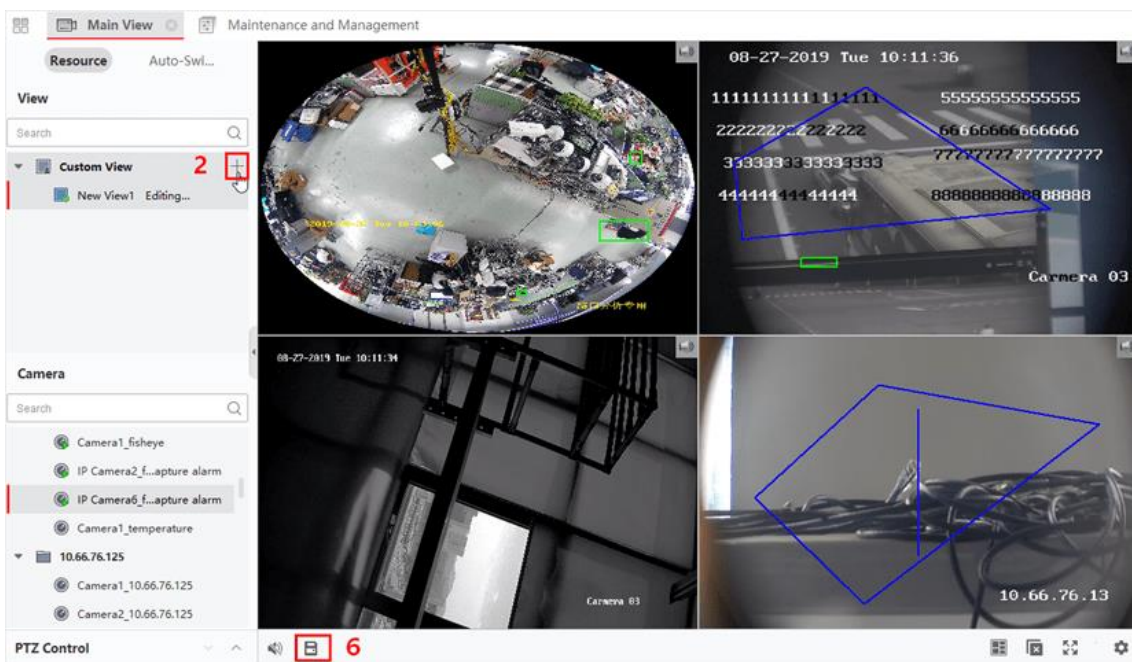





Figure 5-1 Add Custom View


5. Optional: Click  in the live view toolbar to set window division mode for the new view.
6. Start live view for specified camera in specified window according to actual needs.
7. Click  to save the current view or save it as a new view.

 **Note**

Up to 16 custom views are allowed to add to the client.

8. Optional: Perform the following operations after adding the custom view.

Edit View Name Move the cursor over the new view and click  to edit the view name.

Delete View Move the cursor over the new view and click  to delete the view.




What to do next


Click  again to select the custom window division.

5.3 Start Live View

You can start live view after adding device(s) to the client so that you can get to know the monitored area well. You can start the live view of one camera or all cameras in a group. You can also start the live view in custom view mode.

Click **Main View** → **Resource** to enter Main View page. On the left resource list, select resource(s) and start live view by the following ways.

Available Ways	Description	Operation
Start Live View for One Camera	Start the live view of only one camera in a group.	<ul style="list-style-type: none"> ● Select a camera and drag it to the window. ● Double-click the camera in a group. ● Move your cursor over the camera name, and click .
Start Live View for Camera Group	Start the live view of all cameras in one group synchronously.	<ul style="list-style-type: none"> ● Select a group and drag it to the window. ● Double-click the group. ● Move your cursor over the group name, and click , or click  → View All Cameras in Group.
Start Live View in Custom View Mode	Start the live view of the cameras in the custom view.	<ul style="list-style-type: none"> ● Select a custom view and drag it to the window. ● Double-click the custom view.

Available Ways	Description	Operation
		<hr/>  Note Customize a view which containing information such as window division, camera and correspondence between cameras and windows. See <i>Add Custom View</i> for details. <hr/>

 **Note**

If the device supports stream encryption, and the stream of its live view is encrypted, you are required to enter a stream key for double verification.

Figure 5-2 Start Live View

During live view, you can view the bitrate, frame rate and resolution information on the image.

5.4 Auto-Switch in Live View

You can display live view of cameras or display the custom views in turn, which is called "auto-switch". If you want to perform live view of a large amount of cameras, you can auto-switch the selected cameras, which means the client will automatically switch live view of the cameras in the display window. You can also auto-switch multiple views.

When auto-switching in live view, three modes are available:


- Auto-Switch All Cameras in Default View
- Auto-Switch Cameras in a Group
- Auto-Switch Custom Views

5.4.1 Auto-Switch Cameras in a Group

The video stream of the cameras from the same group can switch automatically in a selected display window. For example, if you start auto-switch of a group containing 5 cameras, the live view of the 5 cameras will be displayed in turn with an interval which can be configured. You can also switch to playback and perform other operations on the display window.

Steps

1. Enter the Main View page.

2. Click **Auto-Switch** → **Single Window Auto-Switch** on the left panel to show the groups.
3. Select a display window on the right panel.
4. Hover the cursor on a group name and click .

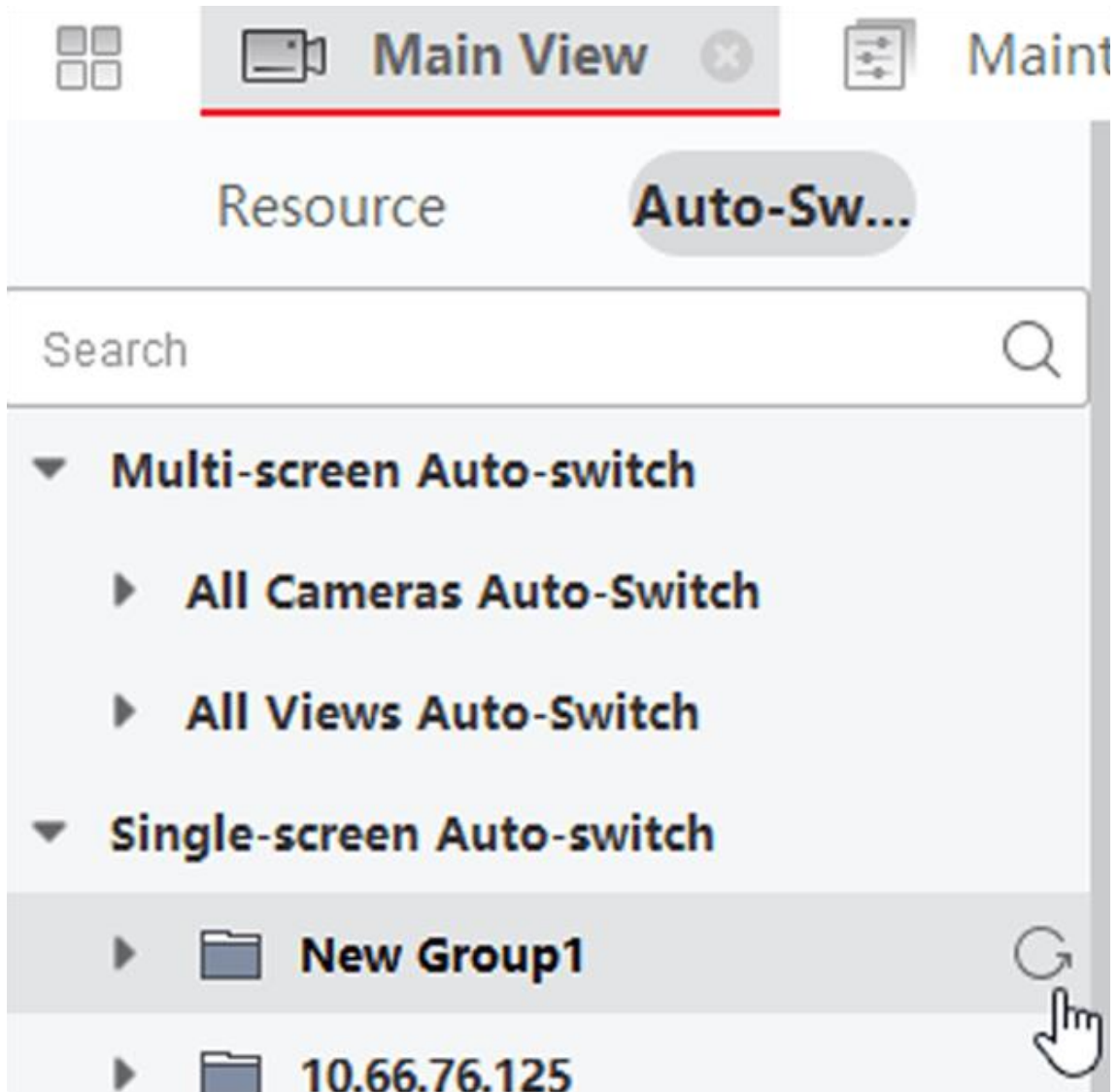




Figure 5-3 Start Auto-Switch of Cameras in a Group

The cameras in the selected group starts auto-switch in the display window.

 **Note**

The audio is off by default after auto-switch starts.

5. Optional: Perform the following operations.

Operation	Description
Pause/Resume Auto-Switch	Click  or  to pause/resume auto-switch.

Go to Previous/Next Page Click < or > to display cameras of the previous/next group.

Set Dwell Time After stopping the current auto-switch, click << or >> to decrease/increase auto-switch dwell time, or click **20s** at the bottom of the page to change the auto-switch dwell time. You can also click **Custom Dwell Time** to set the dwell time according to your need. For example, if you set the interval as 10 seconds, the image of each group will be displayed for 10 seconds and then switch to next group.

5.4.2 Auto-Switch All Cameras

The video of all the cameras in the camera list can switch automatically in a self-adaptive mode. If you start auto-switch of all cameras, the live view of all cameras can be displayed quickly, which is an effective way for live view. The auto-switch is performed with an interval which can be configured. You can also switch to playback and perform other operations on the auto-switch window.

Steps

1. Enter the Main View page.
2. Click **Auto-Switch** → **Multi-Window Auto-Switch** on the left panel.
3. Hover the cursor on **Auto-Switch All Cameras**, and then click .

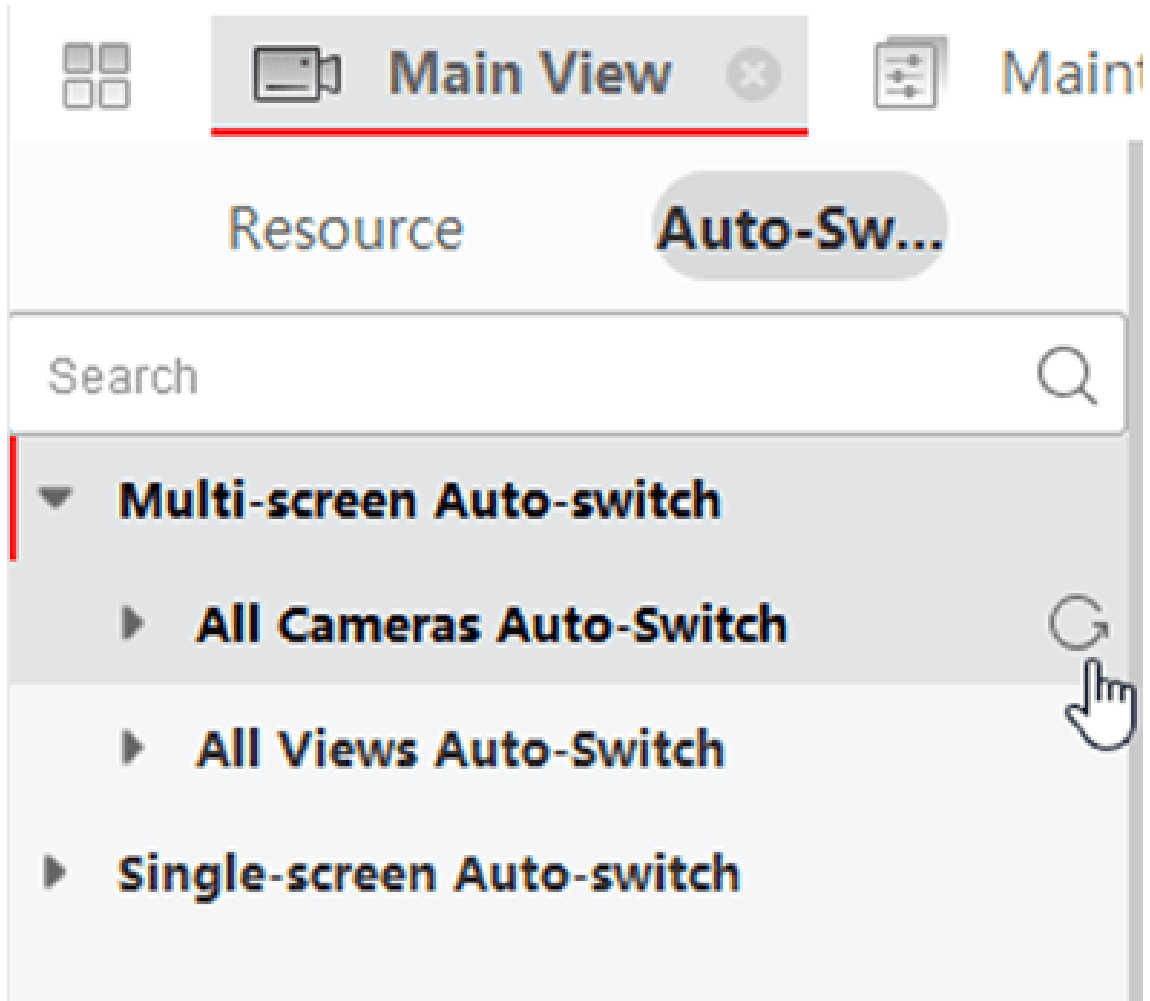


Figure 5-4 Start Auto-Switch of All Cameras

All cameras in the camera list start auto-switching in a self-adaptive mode.

4. Optional: Perform the following operations.

Operation	Description
Pause/Resume Auto-Switch	Click or ↺ to pause/resume auto-switch.
Go to Previous/Next Page	Click < or > to display cameras on the previous/next page.
Set Dwell Time	After stopping the current auto-switch, click << or >> to decrease/increase auto-switch dwell time, or click 20s at the bottom of the page to change the auto-switch dwell time. You can also click Custom Dwell Time to set the dwell time according to your need. For example, if you set the interval as 10 seconds, the image of each camera will be displayed for 10 seconds and then switch to next camera.

5.4.3 Auto-Switch Custom Views

A view is a window division with resource channels (e.g., cameras) linked to each window. View mode enables you to save the window division and the correspondence between cameras and windows as favorite so that you can quickly access these channels later. If you save a view containing all cameras on a floor, you save a custom view, and you can view the live view of all the cameras on the floor in turn by a one-click operation. In this way, you do not have to search these cameras in the camera list every time you login. The auto-switch performs with an interval which can be configured manually.

Before You Start

Add the custom views. See [**Add Custom View**](#) for details.

Steps

1. Enter the Main View page.
2. Click **Resource** → **Multi-Window Auto-Switch** on the left panel.
3. Hover the cursor on **Auto-Switch All Views** and click .

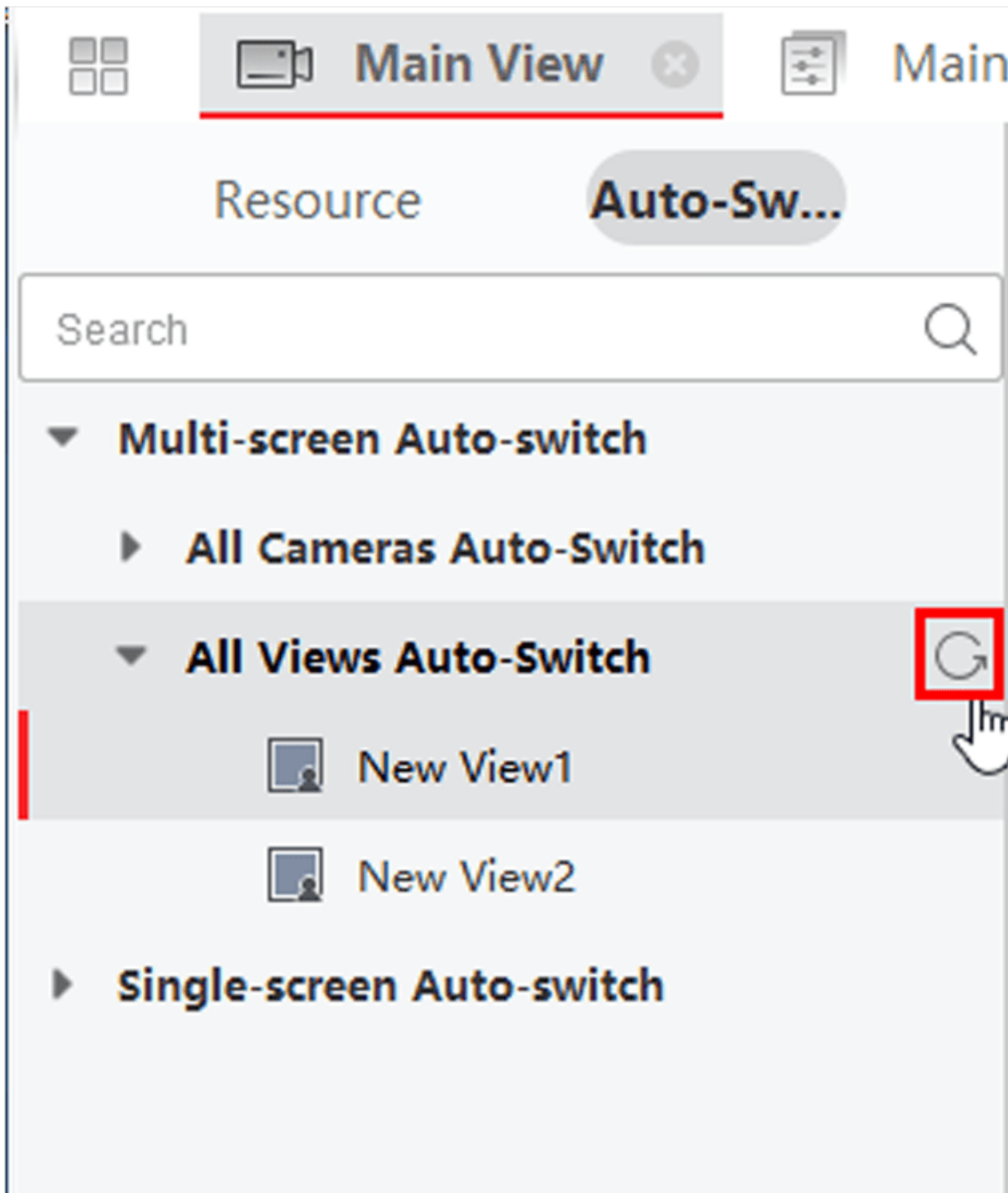


Figure 5-5 Auto-Switch a Custom View

All custom views starts auto-switching.

4. Optional: Perform the following operations.

Operation	Description
Pause/Resume Auto-Switch	Click or ↺ to pause/resume auto-switch.
Go to Previous/Next	Click < or > to display the previous/next view.

Page

Set Dwell Time

After stopping the current auto-switch, click **«** or **»** to decrease/increase auto-switch dwell time, or click **20s** at the bottom of the page to change the auto-switch dwell time. You can also click **Custom Dwell Time** to set the dwell time according to your need. For example, if you set the interval as 10 seconds, the image of each view will be displayed for 10 seconds and then switch to next view.

5.5 PTZ Control

The software provides PTZ control for cameras with pan/tilt/zoom functionality. During the PTZ control, you can set preset, patrol, and pattern, and you can also open a new window for controlling the PTZ.

 **Caution**

- Some functions should be supported by the device.

5.5.1 PTZ Control Panel




The software provides PTZ control operations via control panel, such as detection, speed, zoom in, zoom out, etc. You can also open a new window for controlling the PTZ.











 **Note**









ABUS Link Station device only supports the PTZ movements to the directions of up, down, left, and right.


Enter the **Main View** module, and select **PTZ Control** to open the PTZ control panel. The following icons are available on the PTZ control panel.

Table 5-3 Icons on PTZ Control Panel

Icon	Name	Description
	Direction Buttons	Click or hold the left mouse button to turn the PTZ around. Click to turn around the PTZ horizontally and continuously; click again to stop turning.
	Speed Control	Drag the slider to adjust the PTZ moving speed.
	Zoom in/out	Zoom in to view close image for details; zoom out to view a panoramic image.

Icon	Name	Description
	Focus +/-	Click Focus + move the focal point forward, and click Focus - to move the focal point backward.
	Iris +/-	Used for adjusting the luminance of the image. The larger the iris is, the more the light enters, and the brighter the image will be.
	3D Positioning	Use the left key of mouse to click on the desired position in the video image and drag a rectangle area in the lower right direction, then the dome system will move the position to the center and allow the rectangle area to zoom in. Use the left key of mouse to drag a rectangle area in the upper left direction to move the position to the center and allow the rectangle area to zoom out.
	Auxiliary Focus	Click to focus automatically.
	Lens Initialization	Initialize the lens and focus again for a clear image.
	Light	Click to fill light. <hr/> Note This function needs to be supported by the device. <hr/>
	Wiper	Use the wiper to clear the dust on the camera lens.
	Manual Tracking	For speed dome with auto-tracking function, enable the auto-tracking (via right-click menu) for it and click the icon to manually track the target by clicking on the video.
	Menu	For analog speed dome, click the icon to display its local menu. For detailed operation of the menu, refer to user manual of the speed dome.
	One-Touch Patrol	For speed dome with one-touch patrol function, click the icon and the speed dome








Icon	Name	Description
		starts patrol from the predefined preset No.1 to preset No.32 in order after a period of inactivity (park time). For setting the park time, refer to user manual of the speed dome.
	One-Touch Park	For the speed dome with one-touch park function, click the icon and the speed dome saves the current view to the preset No.32. The device starts to park at preset No. 32 automatically after a period of inactivity (park time). For setting the park time, refer to user manual of the speed dome.
	Enable Manual Lens De-Icing Heater	<p>Enable this function to ensure the camera performance by heating.</p> <hr/> <p> Note We suggest you enable this function when the environment temperature is under 0 °C, otherwise the high temperature may affect the camera work.</p> <hr/>
	Enable Manual PT De-Icing	Enable this function to ensure the camera performance by wiping off the ice adhered on the PTZ camera.
	Manual Face Capture	Click this button, and hold the left mouse button to select a face in the image to capture it. The picture will be uploaded to the server for viewing.
	Synchronize FOV	For thermal cameras, click the icon to synchronize the optical channel's field of view with that of the thermal channel.
	Regional Exposure	For speed domes, click the icon and draw a rectangle on the image to optimize the exposure effect in this region.
	Regional Focus	For speed domes, click the icon and draw a rectangle on the image to optimize the focus effect in this region.

Icon	Name	Description
	Arming and Tracking	For cameras support arming and tracking, click the icon and select the target (person or vehicle) in the live view to arm and track this target.

5.5.2 Set Preset, Patrol, and Pattern

PTZ control supports setting and calling a preset, patrol, and pattern.

On the Home Page, click **Main View** → **PTZ Control** to show the PTZ Control panel.

Task	Definition	Operation
Preset	A preset links the key regions to mobile PTZ position and status. Monitoring people uses it to positioning to key regions rapidly. By sending setting preset command, mobile PTZ records the position and status of zoom, focus, and iris. When executing calling preset command, mobile PTZ rapidly rolls to the set position and resume to set status.	How to Set: select a preset from the preset list→turn the camera to a desired position→click  .
		How to Call: click  .
Pattern	By recording pattern, the movement path and the dwell time in a certain position can be recorded precisely. By calling pattern, mobile PTZ starts move totally according to the recorded path.	How to Set: click  to start recording a pattern→click the direction buttons to shape the pattern→click  .
		How to Call: click  .
Patrol	Patrol is the function that users specify a scan track with a group of defined presets. The patrol between two presets is performed with the set speed and time.	How to Set: click  →select presets, and set speed and time→click OK .
		How to Call: click  .

 **Note**

You should set at least two presets beforehand.


5.6 Customize Window Division

The client software provides multiple kinds of predefined window divisions. You can also set custom the window division as desired.

Steps

 **Note**

Up to 5 window divisions can be customized.

1. Open the Main View or Remote Playback page.
2. Click  on the live view or playback toolbar to open the window division panel.

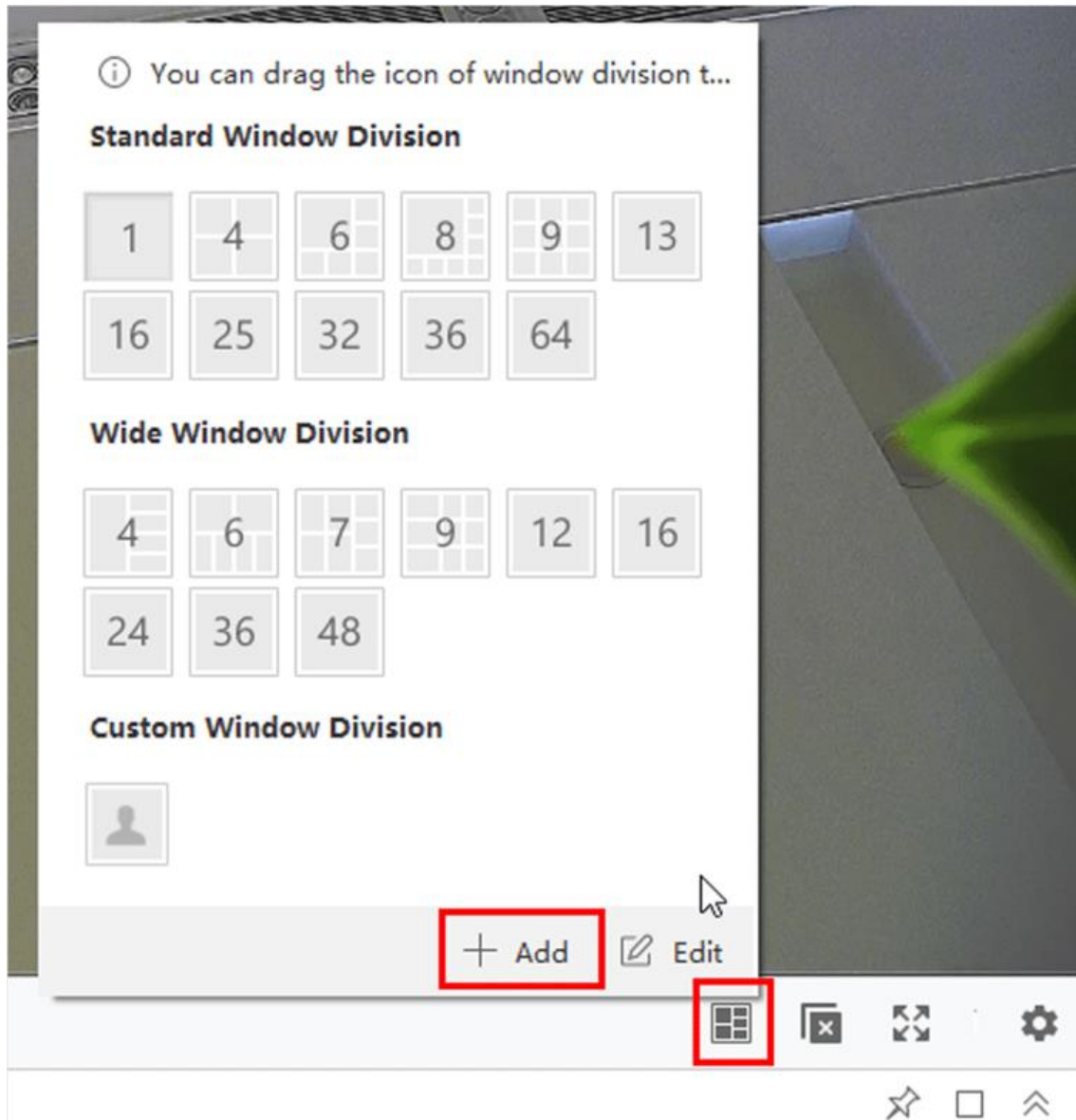


Figure 5-6 Add Custom Window Division

3. Click **Add** to open the Add Custom Window Division dialog.
4. Enter the window numbers in both horizontal and vertical dimension in the Dimension field, and then press **Enter** on your keyboard.

Note

For remote playback, up to 16 windows can be played at the same time, so the custom window division with more than 16 windows is invalid.

5. Optional: Drag your mouse to select the adjacent windows, and click **Joint** to joint them as a whole window.

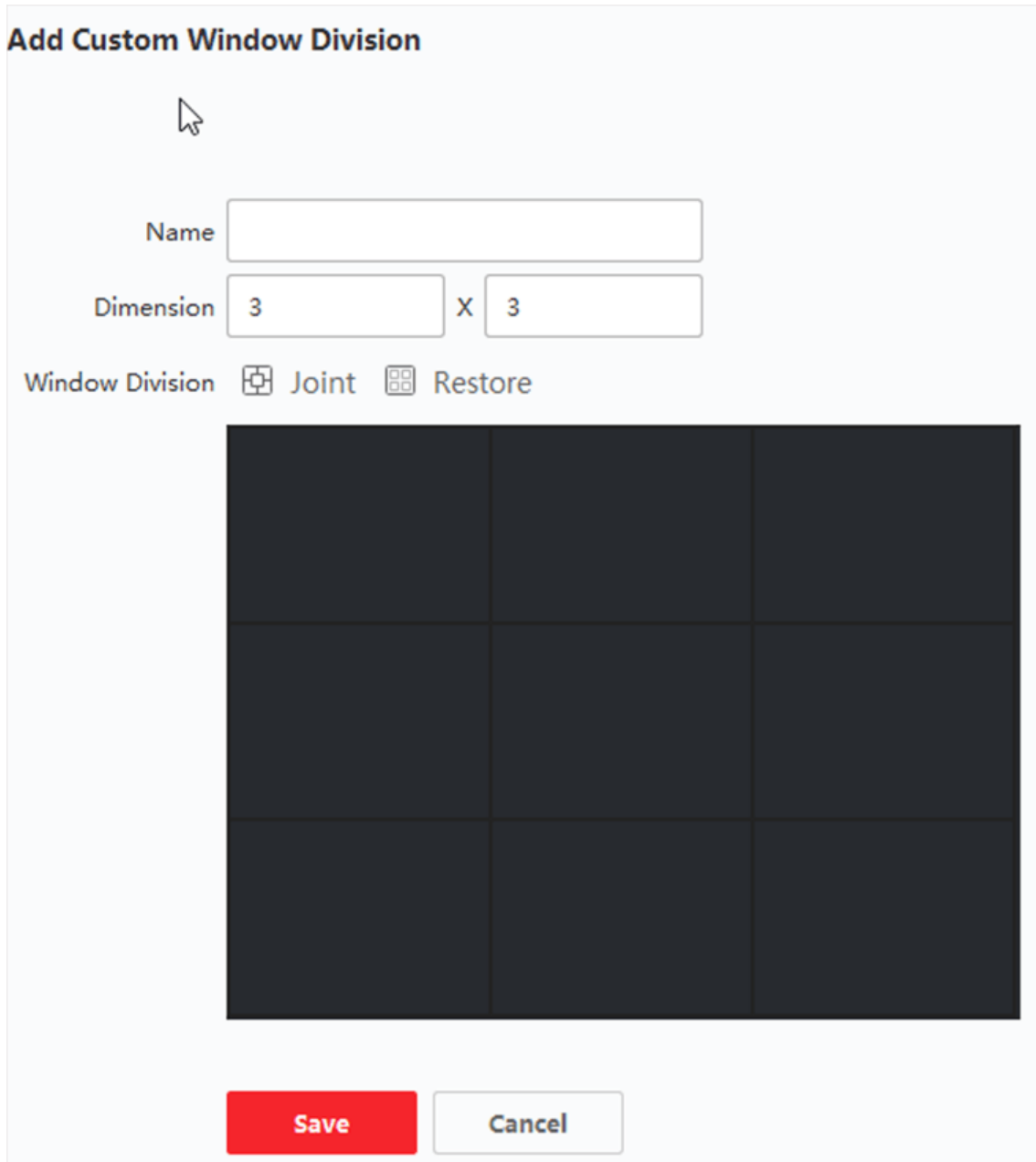



Figure 5-7 Add Custom Window Division Window

6. Optional: Select the joint window and click **Restore** to cancel the joint.
7. Click **Save**.
8. Optional: Click or drag a division mode to the displaying window to apply the mode for displaying.
9. Optional: Edit a customized window division mode.
 - 1) Click  on the live view or playback toolbar to open the window division panel.
 - 2) Click **Edit** to open the Add Custom Window Division.
 - 3) Select a customized division mode and perform operations including renaming, setting dimension, jointing/undo jointing windows.

5.7 Manually Record and Capture

During live view, you can record videos and capture pictures manually, and then view the recorded video files and captured pictures in the local PC.


5.7.1 Manually Record Video





Manual recording function allows to record the live video on the Main View page manually, and you can store the video files in the local PC.

Steps

Note

Manual recording is not supported by ABUS Link Station device during live view.

1. Open the Main View page.
 2. Start the live view.
 3. Perform one of the following operations to start manual recording.
 - Move the cursor to the display window in live view to show the toolbar and click  on the toolbar.
 - Right-click on the display window and click **Start Recording** on the right-click menu.

The icon  turns to . An indicator  appears in the upper-right corner of the display window.
 4. Click  to stop the manual recording.
The recorded video file is automatically saved to the local PC, and a small window with the saving path information appears in the lower-right corner of desktop.
-

Note

The saving path of the recorded video files can be set on the System Configuration page. See [**Set File Saving Path**](#) for details.


5.7.2 View Local Videos

You can view the recorded video files stored in your local PC.

Before You Start

Record the live video.

Steps

1. Click  → **File** → **Open Video File** in the upper-right corner to open the Video Files page.
2. Select the camera to search the recorded video files from the Camera Group list.
3. Specify the start time and end time in the lower-left corner for the searching.
4. Click **Search**.

The video files recorded between the start time and end time displays in thumbnail format on the page.

5. Optional: Perform the following operation(s) after the search.

- | | |
|--------------------------|--|
| Delete Video File | Select the video file, and click Delete to delete the video file. |
| Send Email | Select the video file, and click Email to send an email notification with the selected video file attached. |

Note

To send an email notification, the email settings need to be configured before proceeding. For details, refer to **Set Email Parameters**.


- | | |
|-------------------------|---|
| Save Local Video | Select the video file, and click Save as to save a new copy of the video file. |
| Playback | Double-click the video file to start the local playback. |

5.7.3 Capture Pictures

You can capture pictures during the live view.

Perform this task when you need to capture pictures during the live view.

Steps

1. Open Main View page and start the live view of a camera.
2. Perform one of the following operations to capture pictures.
 - Move the cursor to the display window in live view to show the toolbar and click  on the toolbar.
 - Right-click the display window and click **Capture** on the right-click menu.

The captured picture is automatically saved to the local PC, and a small window with the picture preview and saving path information appears in the lower-right corner of desktop.

Note

The saving path of the captured pictures can be set on the System Configuration page. For details, refer to **Set File Saving Path**.

5.7.4 View Captured Pictures


The pictures captured in the live view are stored in the PC running the software. You can view the

captured pictures if needed.

Before You Start

Capture pictures in the live view.

Steps

1. Click  → **File** → **Open Captured Picture** in the upper-right corner to open the Captured Picture page.
2. Select the camera to search the captured pictures from the Camera Group list.
3. Specify the start time and end time in the lower-left corner for the searching.
4. Click **Search**.

The pictures captured between the start time and end time display in thumbnail format on the page.

5. Optional: Perform the following operation(s) after the search.

Enlarge Picture	Double-click the picture thumbnail to enlarge it for a better view.
Print Picture	Select the captured picture, and click Print to print the selected picture.
Delete Picture	Select the captured picture, and click Delete to delete the selected picture.
Send Email	Select the captured picture, and click Email to send an email notification with the selected picture attached.
Save Picture	Select the captured picture, and click Save as to save a new copy of the selected picture.



5.8 Instant Playback

Instant playback shows a piece of the video which is remarkable, or which is unclear on the first sight. So you can play the video files instantly on the Main View page and get an immediate review if needed.

Before You Start

Record the video files and store them on the storage devices, such as the SD/SDHC cards and HDDs on the DVRs, NVRs, network cameras, etc., or on the storage servers.

Steps


1. Open Main View page and start the live view.
2. Perform one of the following operations to show the pre-play durations' list of instant playback.
 - Move the cursor to the display window to show the toolbar and click .
 - Right-click the display window and select **Switch to Instant Playback** on the right-click menu.
 - Move the cursor to default view or custom view node on the View panel and click .

A list with pre-play durations of 30s, 1 min, 3 min, 5 min, 8 min, and 10 min displays.

3. Select a time period from the appeared list to start the instant playback.

Example

If you select 3 min, and the current time of the live view is 09:30:00, then the instant playback will start from 09:27:00.

During the instant playback, an indicator  appears in the upper-right corner of the display window.

4. Optional: Click  again to stop the instant playback and go back for the live view.

5.9 Live View for Fisheye Camera

For fisheye cameras, you can start the live view in fisheye mode, set presets and patrols, and perform PTZ control.


5.9.1 Perform Live View in Fisheye Mode

During live view of fisheye cameras, the whole wide-angle distorted view will be displayed. But you may have difficulty to view some details. To solve this problem, you can play the live videos in fisheye expansion mode. Fisheye expansion can expand images in various modes: 180° panorama, 360° panorama, PTZ, half sphere, etc. So that you can view the image clearly.

Before You Start

Make sure you have installed Microsoft DirectX component.

Steps

1. Open the Main View page and start the live view of fisheye camera.
2. Enter the Fisheye Expansion mode.
 - Right-click on the video and select **Fisheye Expansion**.
 - Click  in the toolbar. See [Set Icons Shown on Toolbar](#) for details about setting the toolbar.

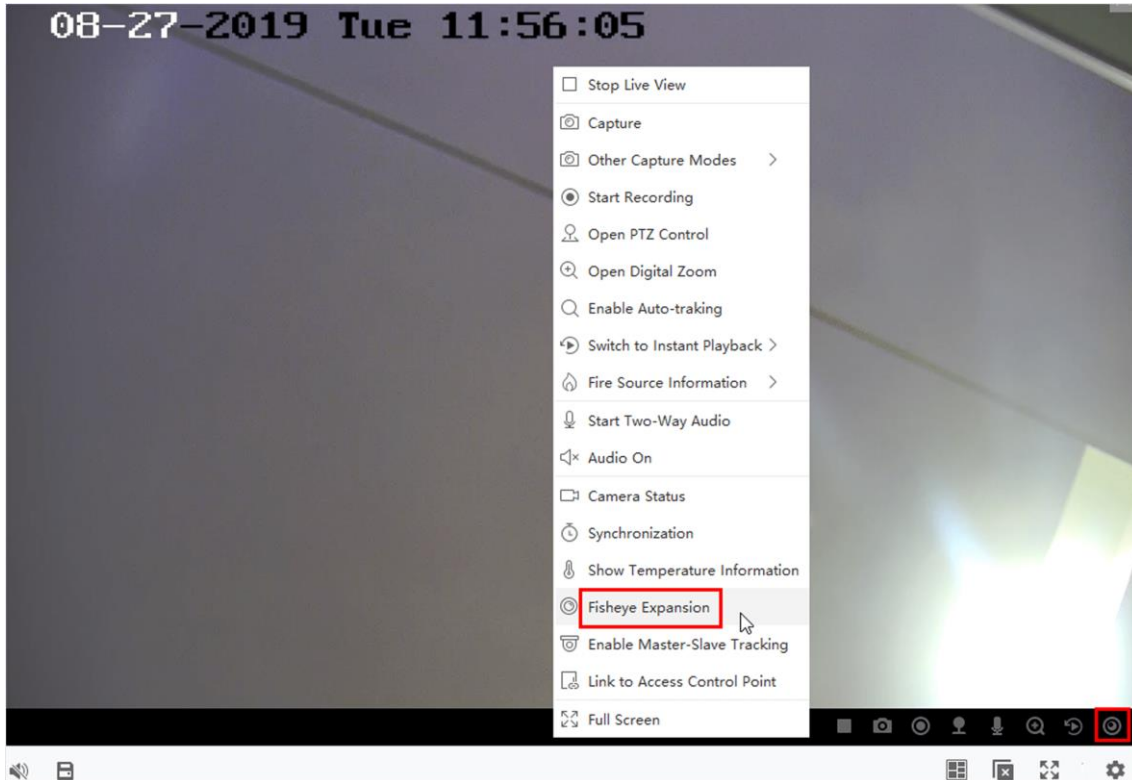



Figure 5-8 Live View in Fisheye Mode

—
 turns to .

3. Click  in the lower-left corner of the displaying window to open the Mounting Type & Expanding Mode Selection panel.
4. Select the mounting type of the fisheye camera according to its actual mounting position.
5. Select the expanding mode for live view as desired.

Fisheye

In the Fisheye view mode, the whole wide-angle view of the camera is displayed. This view mode is called Fisheye because it approximates the vision of a fish's convex eye. The lens produce curvilinear images of a large area, while distort the perspective and angles of objects in the image.

Panorama

In the Panorama view mode, the distorted fisheye image is transformed to normal perspective image by some calibration methods.

PTZ

The PTZ view is the close-up view of some defined area in the Fisheye view or Panorama view, and it supports the electronic PTZ function, which is also called e-PTZ.

 **Note**

Each PTZ view is marked on the Fisheye view and Panorama view with a specific navigation box. You can drag the navigation box on the Fisheye view or Panorama view to adjust the PTZ view, or drag the PTZ view to adjust the view to the desired angle.

Half Sphere

By the half sphere mode, you can drag the image and rotate it centering on the diameter, in order to adjust the view to the desired angle.

AR Half Sphere

AR half sphere mode overlaps images far and near, so that you can view a dimensional image in a wide angle.

Cylinder

In Cylinder mode, the image is formed into a cylinder page.

6. Optional: Perform the following operation(s) after starting live view in fisheye mode.

Capture Right-click on the window and select **Capture** to capture the picture in the live view process.

Enter Full Screen Right-click on a playing window and switch the selected window to full-screen mode.





5.9.2 PTZ Control in Fisheye Mode

In fisheye mode, you can control the PTZ to adjust the PTZ window.

 **Note**

The PTZ panel varies according to different devices.





The following functions are available on the PTZ control panel.

- Select a PTZ window, and click the direction buttons to adjust view angle. Or drag the No. label in the fisheye or panorama window to change the view angle of the PTZ window.
- Select a PTZ window, click  to start auto-scan (the camera rotates in a horizontal direction), and click it again to stop auto-scan.
- Drag the slider on  to adjust the speed for PTZ movement.
- Click  , or scroll the mouse wheel to zoom in or zoom out the selected PTZ window.

5.9.3 Set a Preset and Patrol

PTZ supports configuring and calling a preset and patrol.

Enter the **Main View** page, and select **Fisheye Expansion** after right-clicking a camera.

Task	Definition	Operation
Preset	A preset links the key regions to mobile PTZ position and status. Monitoring people uses it to positioning to key regions rapidly. By sending setting preset command, mobile PTZ records the position and status of zoom, focus, and iris. When executing calling preset command, mobile PTZ rapidly rolls to the set position and resume to set status.	How to Set: select a preset from the preset list→turn the camera to a desired position→click  .
		How to Call: click  .
Patrol	Patrol is the function that users specify a scan track with a group of defined presets. The patrol between two presets is performed with the set speed and time.	How to Set: click  →select presets, and set speed and time→click OK .
		How to Call: click  .

5.11 Live View for Thermal Camera

For thermal camera, you can view the fire source information and temperature during live view. You can also measure the temperature manually to get temperature information in the live view image.

5.11.1 View Fire Source Information during Live View

During the live view, you can view the detected fire source information.

Before You Start

Configure the alarm rules for the thermal device, see the user manual of the device for details.

Steps

1. Enter Main View page and start the live view of a thermal camera.

Note

For starting live view, refer to [Start Live View](#).

2. Right-click on the live view image and select **File Source Information** in the right-click menu to show the list of information types.

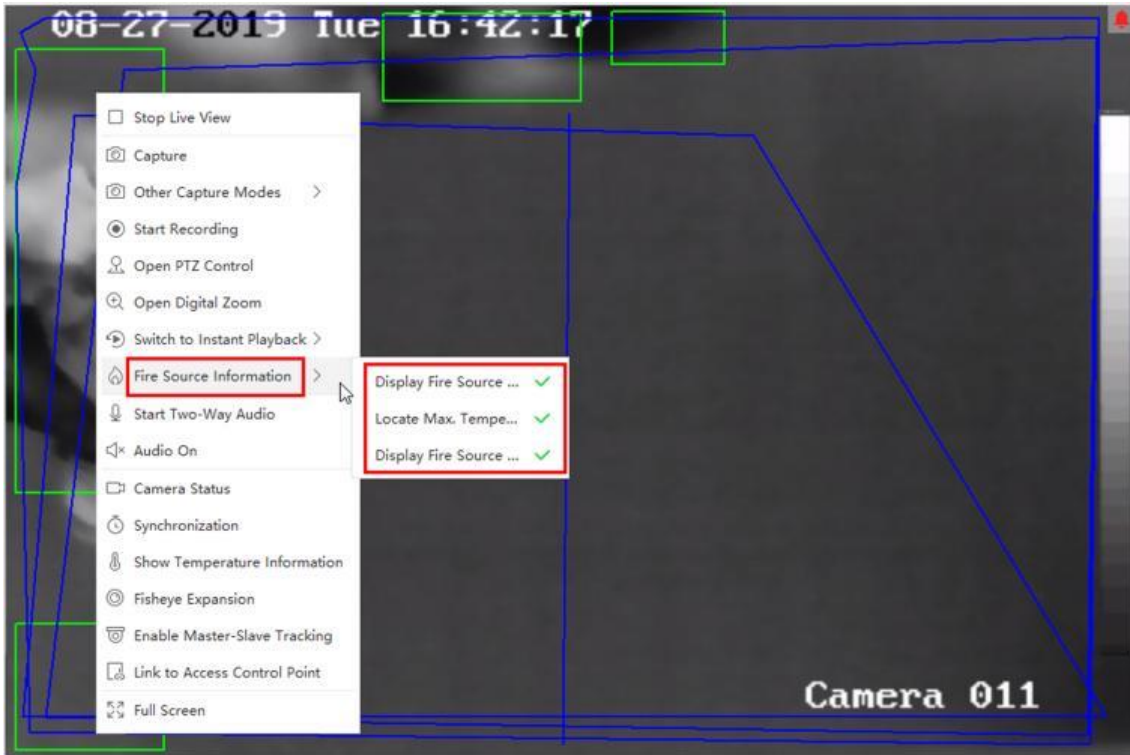


Figure 5-9 View Fire Source Information

3. Select a information type in the list to display the information.

Display Fire Source Region

The region in which the temperature is higher than the configured alarm threshold.

Locate Max. Temperature Region

Mark the region in which the temperature is highest in the fire source region. It is marked in green.

Display Fire Source Target

The distance between the device and fire source.

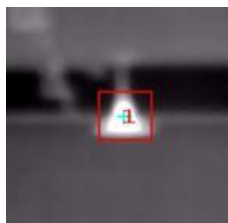


Figure 5-10 Fire Source Information on Live View Image

5.11.2 Show Temperature Information on Live View Image

You can show or hide the real-time temperature information of the monitoring scene when viewing the live video.

Before You Start

- Switch the device VCA source type as **Temperature Measurement + Abnormal Event Detection**.
- Enable the device temperature measurement function and set the temperature measurement rules, see the user manual of the device for details.

Perform this task when you need to show the temperature information on the live view image.

Steps

1. Enter Main View page and start the live view of a thermal camera.

Note

For starting live view, refer to [Start Live View](#).

2. Adjust the scene to the area configured with temperature measurement rule.
3. Right-click on the live view image and select **Show Temperature Information** in the right-click menu.
The temperature displays on the live view image.
4. Click on the image to view the detailed temperature information.



Figure 5-11 Temperature Information on Live View Image

5. Optional: Right-click on the live view image and select **Hide Temperature Information** to hide the temperature information.

5.11.3 Manually Measure Temperature

During the live view of thermal camera, you can click anywhere on the live view image to show the temperature of different points to locate the fire resource quickly.

Steps

 **Note**

- The measured temperature will be displayed on the image for 5 seconds.
- Only one point's temperature can be displayed.
- When multiple clients are getting the live video of one camera, if one client adds or deletes the measurement points, other clients' live view will be affected as well. The measurement points will be cleared if all users stop live view of the camera.

1. Enter Main View page and start the live view of a thermal camera.

 **Note**

For starting live view, refer to [Start Live View](#).

2. Right-click on the live view image and select **Show Temperature Information**.
3. Click on the live view image to show the temperature of this position.
The temperature of the clicked points is shown on the image.

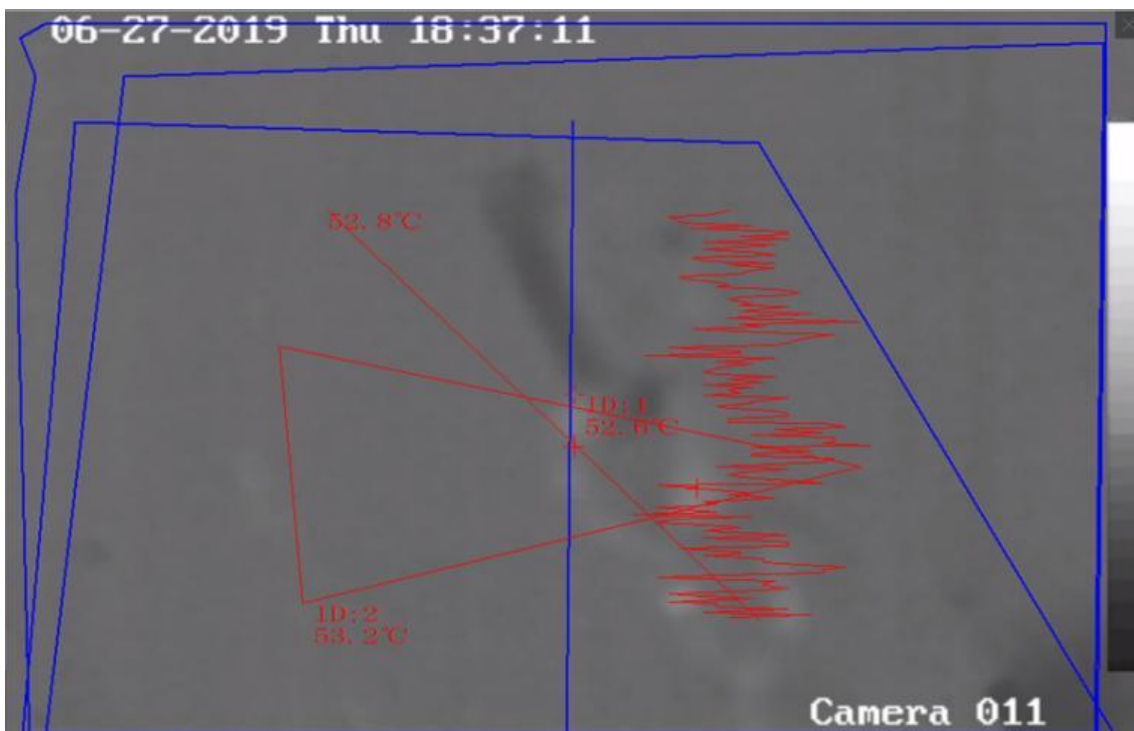


Figure 5-12 Manually Measure Temperature on Points

- Optional: Right-click on the live view image and select **Hide Temperature Information** on the menu.

5.11.4 Display Fire Source Detection Shield Area

Fire source detection shield area is a predefined area that can be shielded from being detected in fire source detection. During live view, you can display the area on the image.

Right-click a live view image and select **Display Shield Area**. The shield area will be displayed on the thermal image of the camera.

Note

- This function needs to be supported by device.
 - Make sure you have enabled and configured Fire Source Detection Shield function for the device. See the device user manual for details.
-



Figure 5-13 Fire Source Shield Area

5.13 More Functions

There are some more functions supported in the live view, including auxiliary screen preview, digital zoom, channel-zero, two-way audio, camera status, and synchronization.

Auxiliary Screen Preview

Display the live video on different auxiliary screens for the convenient preview of multiple monitoring scenes.

Note

Up to 3 auxiliary screens are supported.

Digital Zoom

Drag the mouse to draw a rectangle area in the lower-right/upper-left direction to zoom in or out the drawn area. Or use the mouse wheel to zoom in or out the view in digital zoom mode.

Channel-Zero

For the channel-zero of the device, hold the **Ctrl** key and double-click to display the specific channel. Hold the **Ctrl** key and double-click again to restore.

Two-Way Audio

Two-way audio function enables the voice talk of the camera. You can get not only the live video but also the real-time audio from the camera. If the device has multiple two-way audio channels, you can select a channel to start two-way audio.

Note

- The two-way audio can be used for only one camera at one time.
 - ABUS Link Station device doesn't support selecting channel during two-way audio.
-

Camera Status

The camera status, such as recording status, signal status, connection number, etc., can be detected and displayed for checking. The status information refreshes every 10 seconds.

Synchronization



The synchronization function provides a way to synchronize the device clock with the PC which runs the client software.

Set Stream Type

Auto-Change Stream Type

Camera selects stream type according to its display window size. When the window division number is smaller than 9, the stream type will be main stream, otherwise sub stream.

Three ways are provided for setting stream type:

- In the resource list, hover the cursor on a camera's name and click  → **Stream** to select a stream type, or click **Auto-Change Stream Type**. Or you can perform this operation for a device group to set stream type for all devices in this group.
- Click  in the live view tool bar and select a stream type. See [***Set Icons Shown on Toolbar***](#) for details about editing tool bar.
- Right-click a live view window and click **Stream** to select a stream type for the camera.

Note

This function needs to be supported by device.

Lock Client in Full Screen Mode

Press **Ctrl** and **L** on your keyboard to lock the client after entering the full screen mode. After locking the client, you will be unable to operate the client including the other windows in the current window division mode. Click **Unlock** on the top and enter the login password for the client and click **Unlock** to unlock the client.

Chapter 6 Remote Playback

The device records the video according to the recording schedule. You can view the video files stored in the storage server and the local device, to restore the event occurrence process for postmortem analysis and make the further judgment. Storing the valued video footage can provide basic materials for video analysis and video proof. The client supports multiple playback modes, such as: VCA playback, event playback, etc.

Note

There are two playback modes: one is the instant playback in the Main View module (refer to ***Instant Playback*** for details), another one is searching video files and play the video files in the Remote Playback module. In this chapter, we only introduce the playback in the Remote Playback module.

6.2 Remote Storage Configuration

The video files and captured pictures can be stored on the HDDs, Net HDDs, or SD/SDHC cards on the local device, or on the storage server connected.

Note

This function should be supported by the device.

6.2.1 Store Picture and Video on DVR, NVR, or Network Camera

Some local devices, including the DVRs, NVRs, and Network Cameras, provide storage devices such as the HDDs, Net HDDs and SD/SDHC cards for video and picture files. You can set a recording schedule or capture schedule for the channels of the local devices.

Before You Start

Make sure the newly installed storage devices have be formatted. Refer to ***Format Storage Server's HDD*** for details.

Perform this task when you need to store the picture and video files on the encoding device such as DVR, NVR, or network camera.

Steps

Note

The pictures captured through the capture schedule are stored on the local device and can be searched on the remote configuration page of the device.

1. Enter the Storage Schedule module.
2. Select the camera in the Camera Group list.
3. Set **Recording Schedule** switch or **Capture Schedule** switch to ON on **Storage on Encoding Device** area to enable device local recording or capture.
4. Select the recording or capture schedule template from the drop-down list.

All-day Template

All-day continuous recording.

Weekday Template

Working-hours continuous recording from 8:00 AM to 8:00 PM.

Event Template

All-day event triggered recording.

Template 01 to 08

Fixed templates for specific schedules. You can edit the templates if needed.

Custom

Customize a template as you want.



If you need to edit or customize the template, refer to [**Configure Recording Schedule Template**](#) or [**Configure Capture Schedule Template**](#).

5. Click **Advanced** of Recording Schedule to set the recording advanced parameters.



The displayed items vary according to the devices.

Pre-record

Normally used for the event triggered record, when you want to record before the event happens.

Post-record

After the event finished, the video can also be recorded for a certain time.

Keep Video Files for

The time for keeping the video files in the storage device, once exceeded, the files will be deleted. The files will be saved permanently if the value is set as 0.

Redundant Recording

Save the video files not only in the R/W HDD but also in the redundant HDD.

Record Audio

Record the video files with audio or not.

Video Stream

Select the stream type for the recording.

Note

For specific type of devices, you can select **Dual-Stream** for recording both main stream and sub-stream of the camera. In this mode, you can switch the stream type during remote playback. Refer to ***Normal Playback*** for stream switch during playback.

6. Click **Advanced** of Capture Schedule to set the capture advanced parameters.

Resolution

Select the resolution for the continuous or event captured pictures.

Picture Quality

Set the quality for the continuous or event captured pictures.

Interval

Select the interval which refers to the time period between two capturing actions.

Captured Picture Number

Set the picture number for event capture.

7. Optional: Click **Copy to...** to copy the recording schedule settings to other channels.
8. Click **Save** to save the settings.

6.2.3 Store Picture and Additional Information on Local PC

You can store the pictures and the additional information, such as the heat map, people counting data, and road traffic data, to the local PC.

Perform this task when you need to store pictures and additional information on local PC.

Steps

1. Enter **Storage Schedule** module.
2. Select the camera in the Camera Group list.

Note

This function should be supported by the device.

3. Select storage content.

Picture Storage

Store the alarm pictures of the camera when event occurs. You can click **System Configuration** → **File** to modify the saving path of pictures.

Additional Information Storage

Store the additional information (e.g., heat map, people counting data, etc.) on local PC.

4. Click **Save** to save the settings.

6.2.4 Configure Recording Schedule Template


You can edit the recording schedule template, or customize a recording schedule template.

Steps


1. Enter the Storage Schedule module.

2. Open the template settings window.


Select **Template 01** to **Template 08** from the drop-down list and click **Edit**. Select **Custom** from the drop-down list.

3. Drag on the time-line to set the time periods for the selected template when the cursor turns to .

Continuous

Normal and continuous recording. The schedule time bar is marked with .

Event Recording

The recording is triggered by event. The schedule time bar is marked with .






Command

The recording triggered by command. The schedule time bar is marked with .

Note

Up to 8 time periods can be set for each day in the recording schedule.

4. Optional: After setting the time periods, you can do one or more of the following:

- | | |
|----------------------------|---|
| Move | Drag a time period to move it when the cursors turns to  . |
| Lengthen or Shorten | Select a time period and then lengthen or shorten it when the cursor turns to  . |
| Set Accurate Time | Click a time period to set the accurate start time and end time of the period. |
| Delete | Select the configured schedule time period and click  to delete it. |
| Delete All | Click  to delete all the configured time periods. |
| Copy to | Select one date and click  to copy the date's time period settings to the other dates. |

5. Optional: For template 01 to 08, you can edit the template name as you want.

6. Click **OK** to save the settings.

 **Note**

If you select **Custom** to customize a template, you can click **Save as Schedule Template**, and then the custom template can be saved as template 01 to 08.


6.2.5 Configure Capture Schedule Template

You can edit the capture schedule template, or customize a capture schedule template.

Steps

1. Enter the Storage Schedule module.
2. Open the template settings window.


Select **Template 01** to **Template 08** from the drop-down list and click **Edit**. Select **Custom** from the drop-down list.

3. Drag on the time-line to set time periods for the selected template when the cursor turns to .






Continuous Capture

Normal and continuous capture. The schedule time bar is marked with .

Event Capture

The capture is triggered by event. The schedule time bar is marked with .

4. Optional: After setting the time period, you can do one or more of the followings

- | | |
|----------------------------|--|
| Move | When the cursor turns to  , you can move the time period you just edited. You can also edit the displayed time point to set the accurate time period. |
| Lengthen or Shorten | When the cursor turns to  , you can lengthen or shorten the selected time period. |
| Delete | Select a time period and click  to delete it. |
| Delete All | Click  to delete all the configured time periods. |
| Copy to | Select one date and click  to copy the date's time period settings to the other dates. |

5. Optional: For template 01 to 08, you can edit the template name as you want.
6. Click **OK** to save the settings.

 **Note**

If you select **Custom** to customize a template, you can click **Save as Schedule Template**, and then the custom template can be saved as template 01 to 08.

6.3 Toolbar for Playback

When playing back video on the Remote Playback module, you can operate the tools in the toolbar to implement different functions.

Note

The tools in different playback modes might be different. In this section, you will introduce the tools in the Camera Playback module.

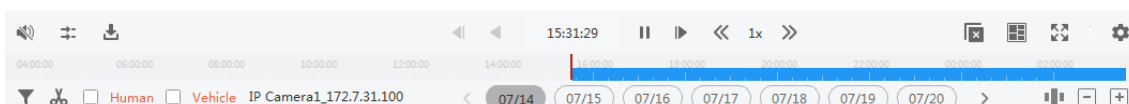

















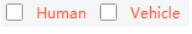



Figure 6-2 Toolbar for Playback

Table 6-1 Toolbar for Playback


Icon	Icon Name	Descriptions
	Reverse Playback	Play back the video file(s) reversely.
	Pause/Play	Pause/play the video file(s).
	Close All	Close all the playing video file(s).
	Single Frame(Reverse)	Play the video file(s) by frame reversely.
	Single Frame	Play the video file(s) by frame.
	Slow Forward/Fast Forward	Set the rate of playing, and play back the video file(s) slowly or fast according to the rate.
	Volume	Click this icon to open/close the audio and adjust the volume.
	Clip	Set the start and end time for clipping and download the clipped video file to the local disk.
	Download for Multiple Cameras	Set the start time and end time for multiple cameras and download the video files of multiple cameras simultaneously.
	Window Division	Set the window division.
	Full Screen	Play back video file(s) in full screen. Press ESC to exit.
	Asynchronous Playback/Synchronous Playback	Switch to asynchronous/synchronous playback mode.

Icon	Icon Name	Descriptions
		<hr/>  Note For details, refer to <i>Synchronous Playback</i> . <hr/>
	Settings	Enter the Video Parameters Settings module, configure the parameters for live view and playback, image, files and toolbar.
	Filter	Filter the video files by the recording type.
	Accurate Positioning	Set the accurate time to play back video file(s).
	Video Date	The date of the playing video file(s) currently. You can switch to play back the video file(s) on the other date quickly. For example, if you switch the date to 07/30, the video will be automatically displayed from 00:00 on July 30 (if there is video at this time).
	Filter Human or Vehicle Related Video	Check Human or Vehicle to filter the video with human body detected or vehicle detected. The human or vehicle related video will be remarked in orange on the time bar, and you can quickly locate the video on the time bar. <hr/>  Note This function should be supported by the device, otherwise the Human or Vehicle is gray and can not be checked. <hr/>

6.4 Normal Playback

You can search video files by camera or group for normal playback and download found video files to local PC. You can also add a tag to mark important video footage, and so on.

You can right-click the playback window to select the required operations from the shortcut menu. Some are listed as follows:

Name	Description
Show/Hide Temperature Information	<p>Show/Hide Temperature Information</p> <hr/> <p> Note</p> <p>The temperature information overlay is only supported by thermal camera.</p> <hr/>
Tag Control	<p>Add default (the default tag name is TAG) or custom tag (the tag name is customized) for the video file to mark the important video point. You can also edit the tag or go to the tag position conveniently.</p>
Other Capture Modes	<ul style="list-style-type: none"> ● Print Captured Picture: Capture a picture and print it. ● Send Email: Capture the current picture and then send an Email notification to one or more receivers. The captured picture can be attached. ● Custom Capture: Capture the current picture. You can edit its name and then save it.


 **Note**

- The ABUS Link Station device only supports normal playback and it also does not support the functions of reverse playback, slow forward or fast forward, and adding tag.
- For NVR which is added to the client by device's other user name (except admin), if **Double Verification** is enabled on this NVR, when playing back videos on the client, you are required to enter the user name and password created for double verification. For details about double verification, refer to the user manual of the NVR.

6.4.1 Search Video Footage

You can search the video footage by date, and you can also enter keyword to filter the matched results for normal playback.

Steps

1. Enter the Remote Playback module.
2. Click  on the left to enter the Camera Playback page.

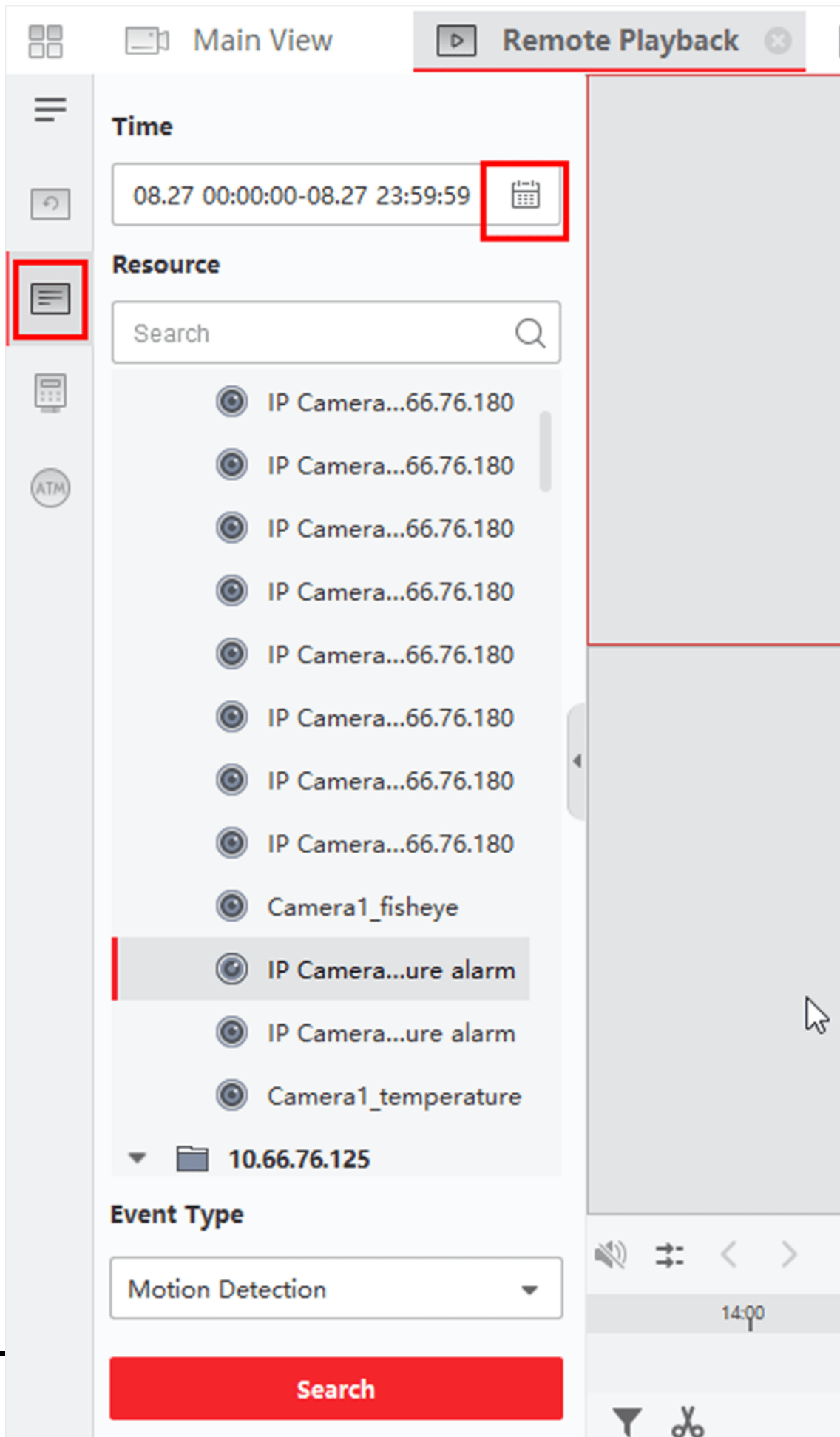




Figure 6-3 Search Video Files

3. Optional: Click  to set the start date and end date of searching time period.

Note

In the calendar, the date which has video footage recorded by schedule will be marked with , and the date which has video footage recorded based on event will be marked with .

4. Start the playback of camera (s) to search the video footage of the selected camera (s). You can do one of the followings to start the playback.

Note

Up to 16 cameras can be searched simultaneously.

- Drag the camera or group to a display window.
- Select a display window and double-click the camera or group to start playback in the selected window.
- Double-click the cameras in turn to select the display window automatically and start playback in the windows.

6.4.2 Play Video Footage

After searching the video footage for the normal playback, you can play the video via time line.

Steps

1. Enter the Remote Playback module.
2. Search the video footage.
3. Play video via time line.

You can click **Stream** → **Main Stream / Sub Stream** to switch the stream type for playback according to your actual need.

The video footage will play automatically. You can click on the time line to position the desired video segment of specified time for normal playback.

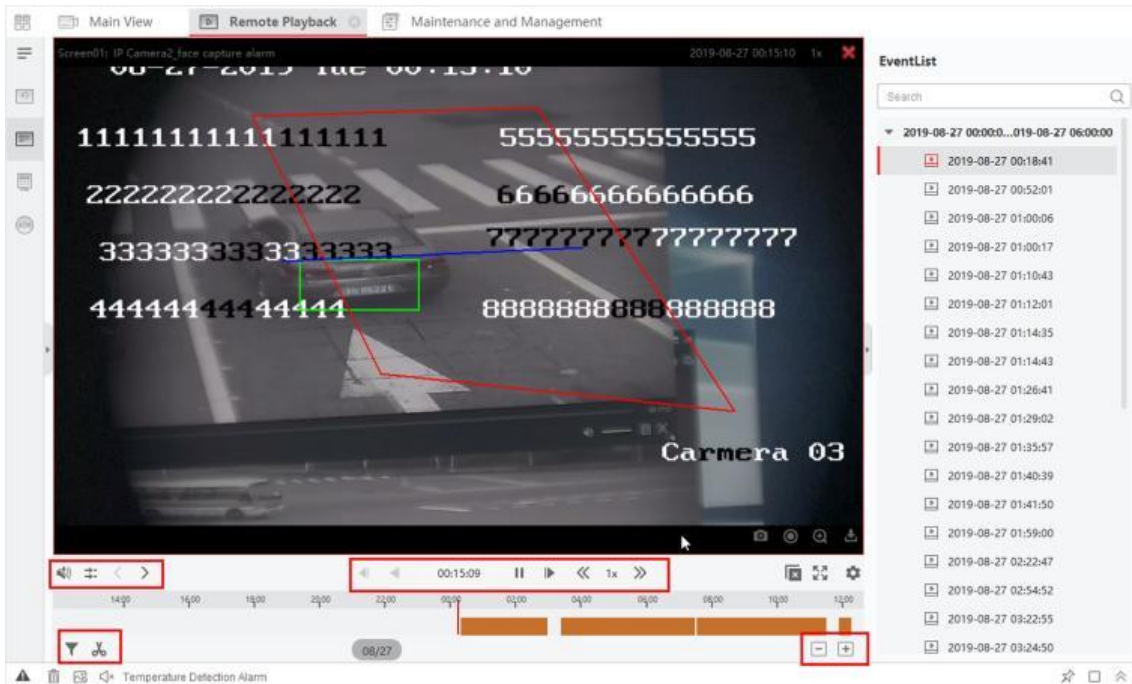


Figure 6-4 Play Video Footage

Note

- The time line indicates the time duration for the video footage, and the video footage of different types are color coded. During playback, you can view the bitrate, frame rate and resolution information on the image.
- You can use mouse wheel or click **+**/**-** to scale up or scale down the time line bar.

4. Optional: Perform the following operations on the toolbar to control the playback.

Single Frame (Reverse) Click **◀** or scroll down the mouse wheel to play the video footage frame by frame (reversely).

Audio Control Click **🔊** or **🔇** to turn off/on the sound. You can also adjust the volume when turning on.


Download for Multiple Cameras Click **📄** to download video footage of multiple cameras at the same time.


Note

For more details, refer to [***Download for Multiple Cameras.***](#)

Download Video Files by Date Click **📅** to download the video footage of the camera by date and time, and store them to local PC. The downloading progress is displayed on the right-upper corner of the page, and you can

manually pause downloading.

Accurate Positioning Click  09:25:46 to set the accurate time point to play the video file.

Jump to the Image of a Thumbnail Click  in the lower-right corner to enable thumbnail function, and put the cursor on the timeline to show the thumbnail of the point. Click the thumbnail to jump to the image of it.



This function needs to be supported by devices.

6.5 Alarm Input Playback

When the alarm input is triggered and the linked video can be searched for alarm input playback. This function requires the support of the connected device.

For the description of the alarm input playback toolbar and right-click menu of display window, refer to ***Normal Playback***.




Some icons may be not available for alarm input playback.

6.5.1 Search Video Footage

You can search the video footage by date, and you can also enter keyword to filter the matched results for alarm input playback.

Steps

1. Enter the Remote Playback module.
2. Click  on the left to enter the Event Playback page.

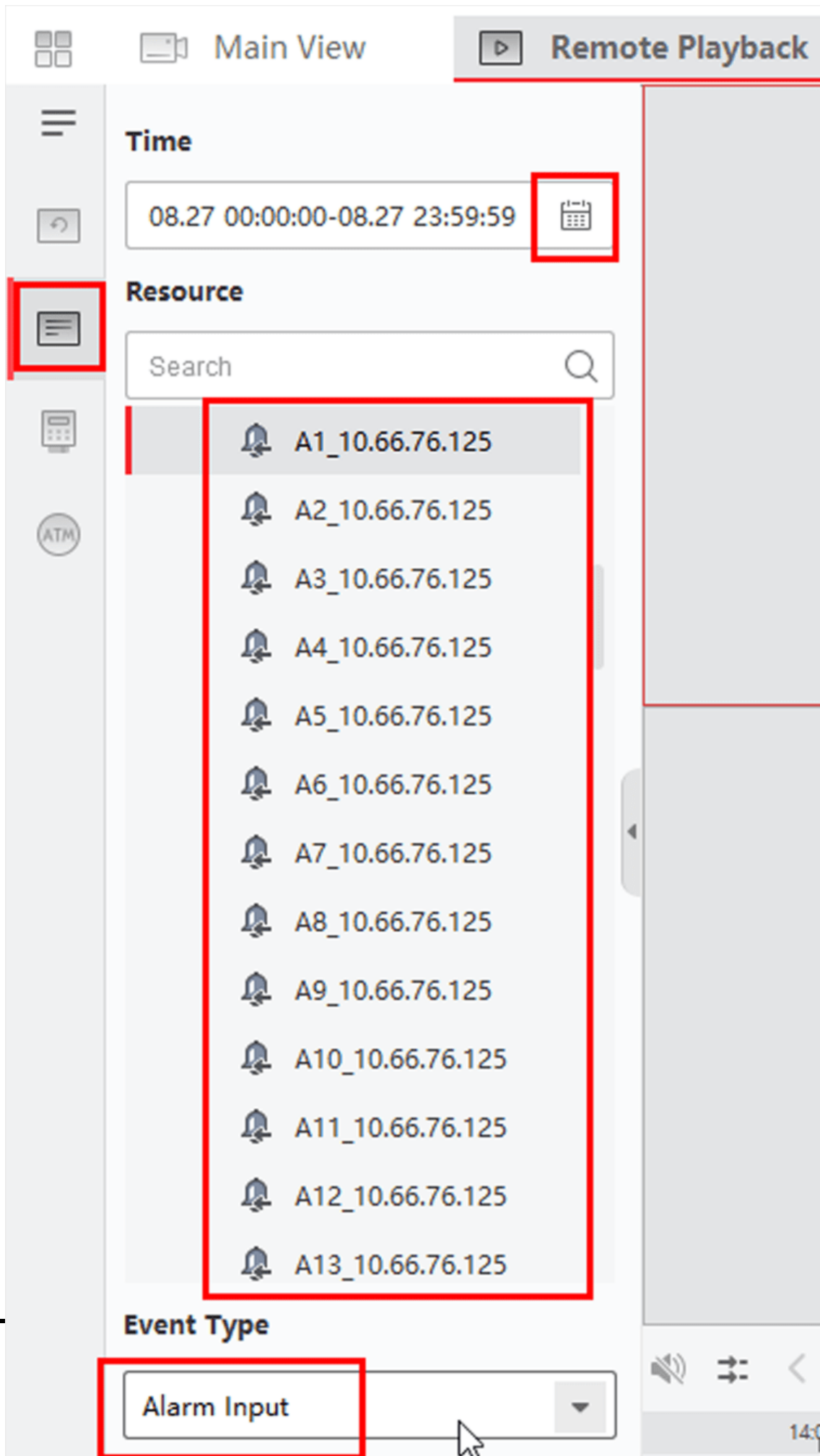




Figure 6-5 Search Video Files

3. Select an alarm input channel at the left.
4. Optional: Click  to set the start date and end date of searching time period.
5. Select **Alarm Input** from the drop-down list as the event type.
6. Click **Search** to start the search.
The matched video footage of the selected alarm input will display on the right page in chronological order. And by default, the first video will play automatically.
7. Optional: Enter keyword in the **Search** field to filter the results.

6.5.2 Play Video Footage

After searching the video footage for the alarm input playback, you can play the video via file list or timeline.

Steps



1. Enter the Remote Playback module.
2. Click  on the left to enter the Event Playback page.
3. Search the video footage of the alarm input.

Note

See [Search Video Footage](#) for details about searching video footage of the alarm input.

4. Play video via file list or timeline.
 - Double-click the video footage to play the video in the playback display window.
 - Click on the timeline to positioning the desired video segment of specified time for alarm input playback.

Note

- The timeline indicates the time duration for the video footage, and the video footage of different types are color coded.
 - You can use mouse wheel or click / to scale up or scale down the timeline bar.
-

6.6 Event Playback

The recorded video files triggered by event, such as motion detection, VCA detection, or abnormal event detection, can be searched for event playback. This function requires the support of the connected device.

For the description of the event playback toolbar and right-click menu of display window, refer to [Normal Playback](#).



 **Note**

Some icons may be not available for event playback.



6.6.1 Search Video Footage/Picture

You can search event videos/pictures by date and event type.

Steps

1. Enter the Remote Playback module.
2. Click  on the left to enter the Event Playback page.
3. Click  to set the start date and end date of searching.

 **Note**

In the calendar, the date which has video footage recorded by schedule will be marked with , and the date which has video footage recorded based on event will be marked with .

4. Select **Video** or **Picture** as the content to search for.
5. Select a camera from the resource list.
6. Select an event type from the **Event Type** drop-down list.
7. Click **Search**.
 - If you select **Video** as the searched content, the matched video footage will display on the right page in chronological order. And by default, the first video file will play automatically.
 - If you select **Picture** as the searched content, the matched pictures will be automatically displayed on the right page.


6.6.2 View Video Footage/Picture

When the camera detects events (such as line crossing, motion detection, and abnormal event detection) happening or the outdoor station performs video talk, it will trigger the linked camera's recording video or capturing pictures. You can search the video footage or pictures and play the videos via file list or timeline and view the pictures in turn.

Steps



 **Note**

For the outdoor station, only DS-KV8123-M supports the following operations.









1. Enter the Remote Playback module.
2. Click  on the left to enter the Event Playback page.
3. Search the video footage or pictures recorded/captured based on event.
4. View video footage or picture.
 - Double-click the video footage to play the video in the playback display window.

- Searched pictures will be automatically played.

 **Note**

- The timeline indicates the time duration for the video files, and the video files of different types are color coded.
 - You can use mouse wheel or click / to scale up or scale down the timeline bar.
-

5. Optional: Perform the following operations if you need.

Play Footage of Certain Time	Click on the timeline to display video segment of specified time for event playback.
Display Footage with Human and/or Vehicle	Under the timeline, check Human and/or Vehicle to display footage contains humans or vehicles.
Switch Pictures	Click  or  to turn to previous or next picture.
Set Picture Displaying Interval	Click  to set the interval of picture display.
Display Pictures in Full Screen	Click  to display pictures in full screen mode.
Display Pictures in List Mode	Click  to display pictures in list mode. Click  to switch to thumbnail mode.
Download Pictures	Click  and check pictures and click Download to download the selected pictures to your PC.
Download Videos	Click  , select multiple video files and click Download to download video files to your PC.

6.9 VCA Playback

For the searched video files, you can set VCA rule to find the video footage that VCA event occurs, such as motion detection, line crossing detection, and intrusion detection. This function helps to search out the video that you may be more concerned and mark it with red color.


Before You Start

Make sure the device with VCA function has been installed.

Steps

Note

VCA playback is only supported in a single window, synchronous and asynchronous playback are not supported.

1. Enter the Remote Playback module.
2. Click  on the left to enter the Camera Playback page.
3. Select the camera and start the camera's video playback.

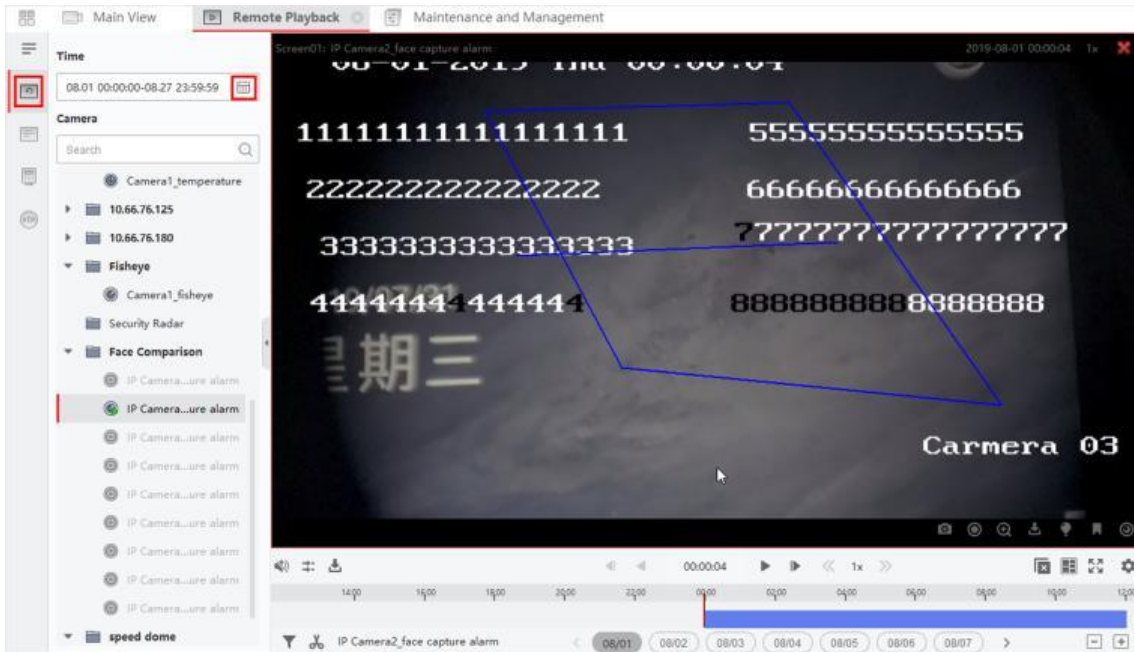



Figure 6-9 VCA Playback

4. Enter the VCA Search menu.
 - Right-click the playback window to pop up the shortcut menu, and then click **VCA Search**.
 - Click  on the lower-right corner of the playback window.
5. Enable the VCA type, draw the detection region and set the sensitivity.

Motion Detection

When the view of the video changes (such as a person passes, the lens is moved), the video footage will be marked as red color on the time line, which is used for the automatic alarm scene or no-guard scene.

Line Crossing Detection

You can draw a virtual line on the video, and the video footage will be marked as red color on the time line when the client bi-directionally detects people, vehicles and other moving objects that cross the virtual line.

Intrusion Detection

You can draw a virtual region on the video, and the video footage will be marked as red color

on the time line when there are people, vehicles and other moving objects intruding into the pre-defined region.

VCA Settings

Set the sensitivity and filter the searched video files by setting the target characters. The video footage will be marked as red color on the time line when a person (whose attributes match the setting attributes) occurs in the video.



The higher the sensitivity, the more accurate the matched person is.

6. Optional: Click  to set the start date and end date of searching time period.

7. Start the VCA playback.

The VCA events occurred in the defined area will be red marked on the timeline.



- By default, the playback speed of concerned video will be 1X, and the playback speed of unconcerned video will be 8X.
 - You can set to skip the unconcerned video during VCA playback in System Configuration and the unconcerned video won't be played during VCA playback. Refer to **Set Live View and Playback Parameters** for details.
 - If you need to disable VCA playback, right-click the VCA playback window and click **VCA Search** to disable VCA playback.
-


6.10 Synchronous Playback

Be default, the client play the video files of multiple cameras in asynchronous playback mode: the playback time of different video files might be different. In synchronous playback, the video files can be played back in synchronization.

Steps



- Video files from up to 16 cameras can be played back simultaneously.
 - Synchronous and asynchronous playback are not supported in ATM video playback and VCA playback mode.
 - Event video playback and POS video playback only support synchronous playback. To link multiple cameras, enter **Maintenance and Management** → **Event Management**, enable the linked camera according to event type.
-

1. Enter the Remote Playback module.
2. Start playback of at least two cameras.
3. Click  in the toolbar to enable the synchronous playback.

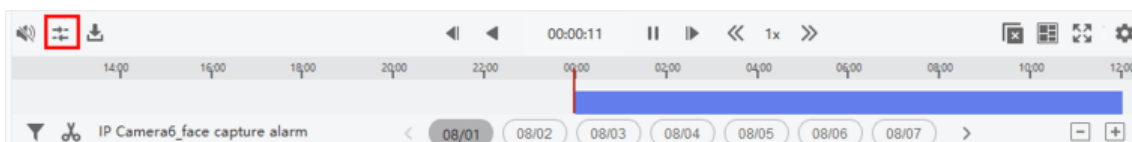



Figure 6-10 Disable Synchronous Playback

The camera under playback will start synchronous playback.

4. Click  to disable the synchronous playback.

6.11 Fisheye Camera's Video Playback

When playing back the fisheye camera's video, there might be distortion in the view. To observe the details better, you can enable the fisheye expansion function, to rectify the view as an undistorted view. The client supports multiple fisheye expansion modes, such as: panorama, half sphere, PTZ, fisheye+PTZ mode.

Before You Start

Make sure you have installed Microsoft DirectX component.

Steps


Note

For other playback control instruction, refer to [Normal Playback](#). Some icons may not be available for fisheye playback.

1. Enter the Remote Playback module.
2. Select a fisheye camera to start playback.

Note

For detailed configuration about playback and playback control, refer to [Normal Playback](#).

3. Enter the Fisheye Expansion mode.
 - Right-click on the display window and select **Fisheye Expansion**.
 - Click  in the toolbar. See [Set Icons Shown on Toolbar](#) for details about setting the toolbar.

Note

The mounting type in playback of fisheye expansion is set according to the mounting type in live view. For details, refer to [Perform Live View in Fisheye Mode](#)

 turns to .

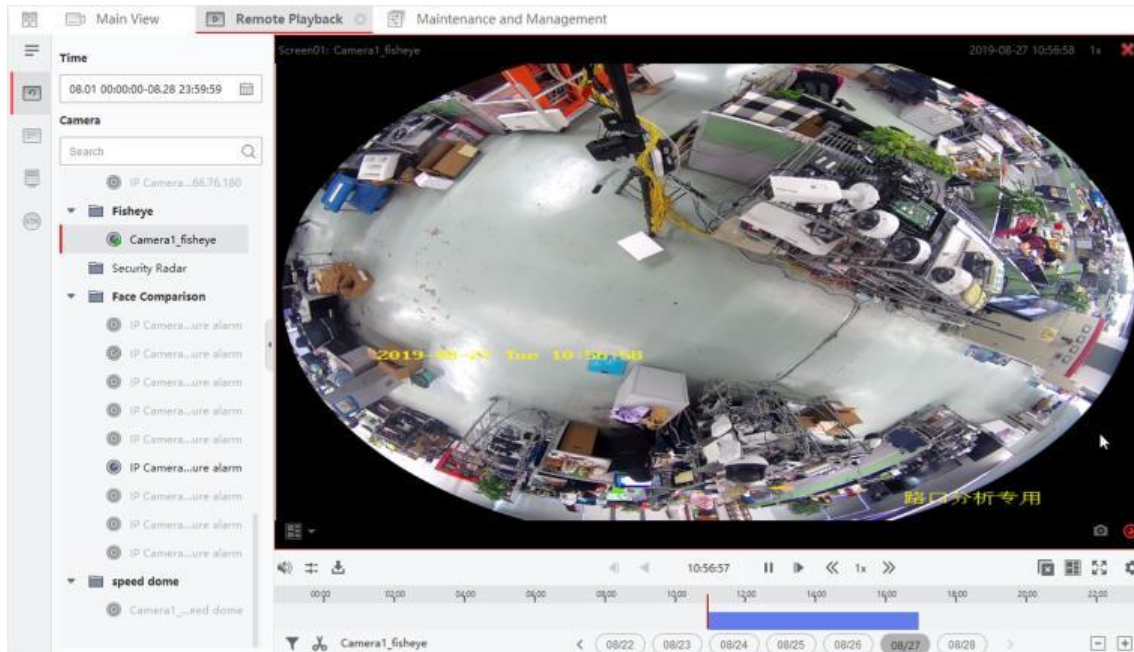



Figure 6-11 Fisheye Camera's Video Playback

4. Click  in the lower-left corner of the display area to select an expanding mode for playback as you desired.

Fisheye

In the Fisheye view mode, the whole wide-angle view of the camera is displayed. This view mode is called **Fisheye** because it approximates the vision of a fish's convex eye. The lens produces curvilinear images of a large area, while distorting the perspective and angles of objects in the image.

Panorama / Dual-180° Panorama / 360° Panorama

In the Panorama view mode, the distorted fisheye image is transformed to normal perspective image by some calibration methods.

PTZ

The PTZ view is the close-up view of some defined area in the Fisheye view or Panorama view, and it supports the electronic PTZ function, which is also called e-PTZ.

Note

Each PTZ view is marked on the Fisheye view and Panorama view with a specific navigation box. You can drag the navigation box on the Fisheye view or Panorama view to adjust the PTZ view, or drag the PTZ view to adjust the view to the desired angle.

Half Sphere

By the half sphere mode, you can drag the image and rotate it centering on the diameter, in order to adjust the view to the desired angle.

AR Half Sphere

AR half sphere mode overlaps images far and near, so that you can view a dimensional image in a wide angle.

Cylinder

In Cylinder mode, the image is formed into a cylinder page, and you can drag the image to any direction flexibly to view everywhere of the detection area.

5. Optional: Right-click on a playing window in the Fisheye view mode and you can switch the selected window to full-screen mode.



You can right-click on the window and select **Quit Full Screen** to exit the full-screen mode.

6.13 Download Video Footage

During playback, you can download the video files of one camera or multiple cameras to the local PC.

6.13.1 Download Video Footage by Date

During playback, you can download the video footage of the camera and save in the local PC.

Steps

1. Enter Remote Playback page and select a camera to start playback.



For details about starting playback, refer to [Remote Playback](#).

2. Right click on the image and click **Download**.

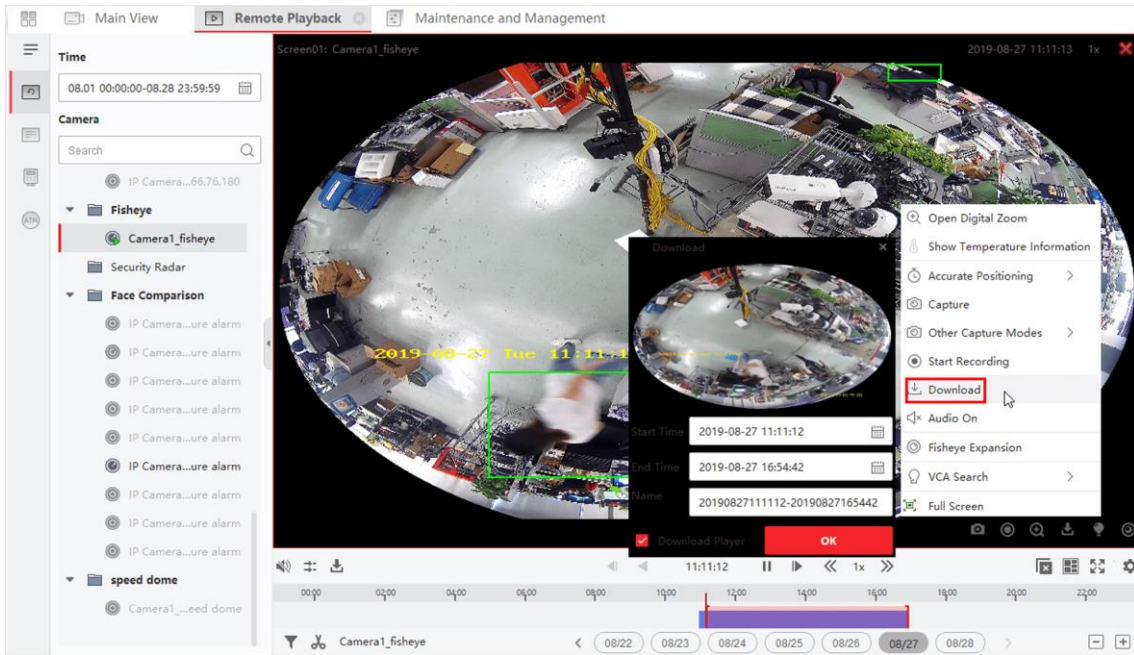


Figure 6-12 Download Video Footage by Date

3. Set the start and end time of the video footage to download.
4. Enter a name for the video footage.
5. Click **OK** to start downloading the video footage to the local PC.

6.13.2 Download for Multiple Cameras

During the playback of multiple cameras, you can download the video files of multiple cameras by date simultaneously.

Steps

1. Enter Remote Playback page and select multiple cameras to start playback.

Note

For details about starting playback, refer to [Remote Playback](#).

2. Click  to open the Download for Multiple Cameras window.

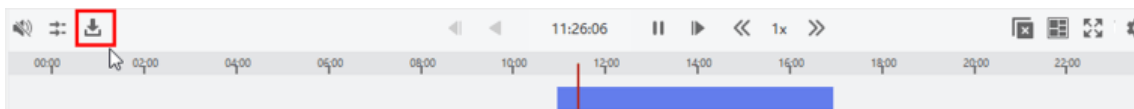


Figure 6-13 Tool Bar

All the cameras in playback will be displayed.

3. Select the cameras you want to download video files for.
4. Set the start time and end time of video duration for each camera.

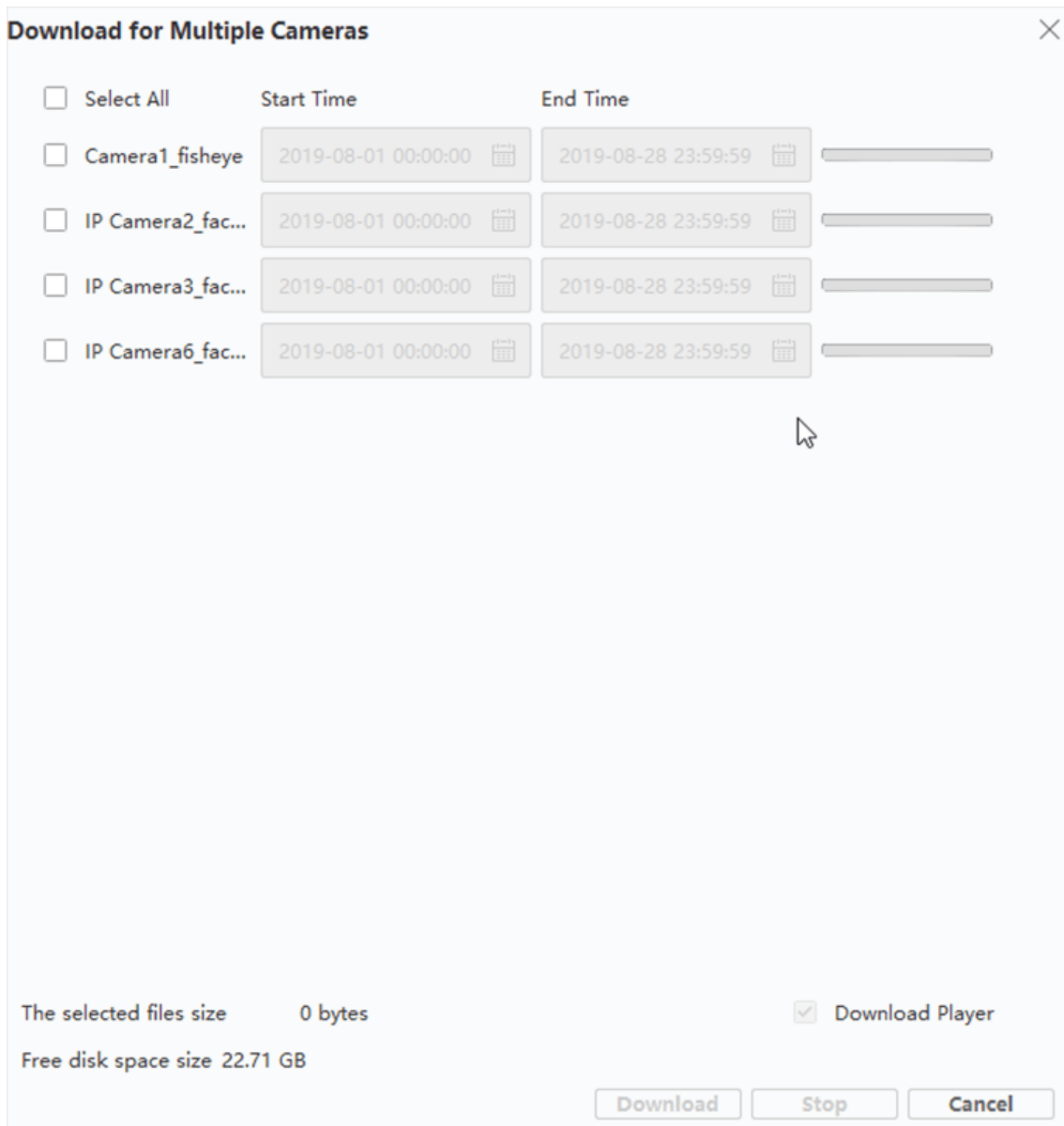


Figure 6-14 Select Cameras

5. Optional: Check **Download Player** to download the player.
6. Click **Download** to start downloading the video files of the configured duration(s) to the local PC.
The progress bar shows the downloading process of each camera's video files.
7. Optional: Click **Stop** to stop downloading manually.

Note

Up to 16 cameras' video files can be downloaded simultaneously.

Chapter 7 Event Configuration

Event is used to notify security personnel of the particular situation which helps handle the situation promptly. Event can trigger a series of linkage actions (e.g., audible warning and sending email) for notification and event handling. You can enable the event and set linkage action(s) for the resources added to the client. If the selected events happen, the client will receive event notifications in real-time and you can check the details and handle the events accordingly.

Video Event

The video events refer to the special events triggered by video exception, monitoring area's exception, alarm input, encoding device's exception, etc. For more details, refer to [Configure Event for Camera](#), [Configure Event for Alarm Input](#), and [Configure Event for Encoding Device](#).

Access Control Event

The access control events refer to the special events triggered at the access control devices, doors, card readers, elevators, video intercom devices, etc. For more details, refer to [Configure Client Actions for Access Event](#) and [Configure Video Intercom Event](#).

7.1 Configure Event for Camera

The event for camera refers to the video exception or the events detected in the monitoring area of the camera, such as motion detection, video loss, line crossing, and so on. You can enable an event for the cameras in the client. When the event is triggered on the camera, the client can receive and record event for checking and trigger a series of linkage actions (e.g., sending email) for notification.

Steps

1. Click **Event Configuration** → **Video Event** → **Camera**.

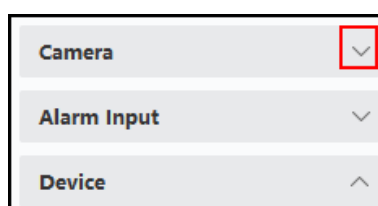


Figure 7-1 Display Camera Resource

2. Unfold the group and select a camera as event source.

Note

Make sure the resource is online.

All the event types supported by the selected camera will appear.

<input type="checkbox"/>	Event Type	Priority	Trigger Client Action	Linked Camera	Enable
<input type="checkbox"/>	Audio Input Exception...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_10.6.113.250	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Face Detection Alarm	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_10.6.113.250	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Intrusion Detection Al...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_10.6.113.250	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Line Crossing Detectio...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_10.6.113.250	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Motion Detection Alar...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_10.6.113.250	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Region Entrance Dete...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_10.6.113.250	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Region Exiting Detecti...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_10.6.113.250	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Video Loss Alarm	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_10.6.113.250	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Video Tampering Det...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_10.6.113.250	<input checked="" type="checkbox"/>

Figure 7-2 Configure Events for Camera

3. Optional: Enter keywords in **Filter** field to locate the desired event quickly.
4. Optional: Turn on the switch on the Enable column to enable the event type, or click **Enable All** to enable all the event types of this camera.

 **Note**

After enabled, the event can be received by the client and trigger the linkage action(s). You can also disable an event type or disable all event types.

5. Optional: Select the event(s), and then perform the following operations.


Edit Priority Click **Edit Priority** to set the priority of the event(s).
Priority represents the emergency degree of the event.

Edit Event Linkage Click **Edit Event Linkage** to set the linkage action(s) of the event(s).

Audible Warning

Trigger the client's audible warning when the event is triggered.

You can select the audio file on the drop-down list, or click **Add** to add new audio file (in WAV format).

You can click  to make an audition of the selected audio file.

Send Email

Send an email notification of the alarm information to one or more receivers.


For details about setting email parameters, refer to **Set Email Parameters**.

Pop-up Window

Pop-up window to display the event related information (including event details, live video of the source camera, captured pictures of the linked camera) on the client when the event is triggered.

You can also enter remarks about how to the handle the event.

Display on Map

When the event source is added as a hot spot on the map, the hot spot will be displayed with 

twinkling aside when the event is triggered, which helps security personnel view the location of the event.

You can also click the hot spot to view the event details and the live video of the linked camera.

Linked Camera

Link the selected camera to capture picture or record video when the event is triggered.

What to do next

You need to arm the device which the camera belongs to, otherwise the client cannot receive the configured events. For details, see [***Enable Receiving Event from Devices***](#).

7.2 Configure Event for Alarm Input

The event for alarm input refers to the event triggered by alarm input. You can enable an event for the alarm inputs in the client. When the alarm input is triggered, the client can receive and record event for checking and trigger a series of linkage actions (e.g., sending email) for notification.

Steps

1. Click **Event Configuration** → **Video Event** → **Alarm Input**.

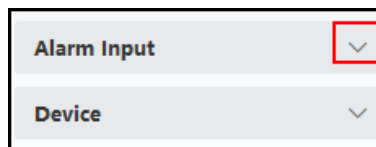


Figure 7-3 Display Alarm Input Resource

2. Unfold the group and select an alarm input as event source.

Note

Make sure the resource is online.

All the event types supported by the selected alarm input will appear.

3. Optional: Enter keywords in **Filter** field to locate the desired event quickly.
4. Optional: Turn on the switch on the Enable column to enable the event type, or click **Enable All** to enable all the event types of this alarm input.

Note

After enabled, the event can be received by the client and trigger the linkage action(s). You can also disable an event type or disable all event types.

5. Optional: Select the event(s), and then perform the following operations.

Edit Priority

Click **Edit Priority** to set the priority of the event(s).
Priority represents the emergency degree of the event.

Edit Event Linkage Click **Edit Event Linkage** to set the linkage action(s) of the event(s).

Audible Warning

Trigger the client's audible warning when the event is triggered.

You can select the audio file on the drop-down list, or click **Add** to add new audio file (in WAV format).

You can click  to make an audition of the selected audio file.

Send Email

Send an email notification of the alarm information to one or more receivers.


For details about setting email parameters, refer to [Set Email Parameters](#).

Pop-up Window

Pop-up window to display the event related information (including event details, live video of the source camera, captured pictures of the linked camera) on the client when the event is triggered.

You can also enter remarks about how to handle the event.

Display on Map

When the event source is added as a hot spot on the map, the hot spot will be displayed with  twinkling aside when the event is triggered, which helps security personnel view the location of the event.

You can also click the hot spot to view the event details and the live video of the linked camera.

Linked Camera

Link the selected camera to capture picture or record video when the event is triggered.

What to do next

You need to arm the device which the alarm input belongs to, otherwise the client cannot receive the configured events. For details, see [Enable Receiving Event from Devices](#).

7.3 Configure Event for Encoding Device

The event for encoding device refers to encoding device's exception, such as device offline. You can enable an event for the encoding devices added in the client. When the event is triggered on the device, the client can receive and record event for checking and trigger a series of linkage actions (e.g., sending email) for notification.

Steps

1. Click **Event Configuration** → **Video Event** → **Device**.

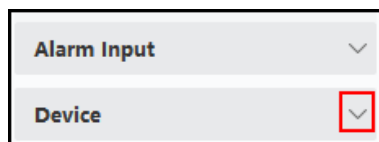


Figure 7-4 Display Device Resource

2. Select a device as event source.

 **Note**

Make sure the resource is online.

All the event types supported by the selected device will appear.

3. Optional: Enter keywords in **Filter** field to locate the desired event quickly.

4. Optional: Turn on the switch on the Enable column to enable the event type, or click **Enable All** to enable all the event types of this device.

 **Note**

After enabled, the event can be received by the client and trigger the linkage action(s). You can also disable an event type or disable all event types.

5. Optional: Select the event(s), and then perform the following operations.

Edit Priority Click **Edit Priority** to set the priority of the event(s).
Priority represents the emergency degree of the event.

Edit Event Linkage Click **Edit Event Linkage** to set the linkage action(s) of the event(s).

Audible Warning

Trigger the client's audible warning when the event is triggered.

You can select the audio file on the drop-down list, or click **Add** to add new audio file (in WAV format).

You can click  to make an audition of the selected audio file.

Send Email

Send an email notification of the alarm information to one or more receivers.

For details about setting email parameters, refer to [**Set Email Parameters**](#).

Click **Copy to** to copy the event settings of this device to other device(s).

 **Note**

You can only copy the event settings to the resource(s) of the same type.

What to do next

You need to arm this device, otherwise the client cannot receive the configured events. For details, see [**Enable Receiving Event from Devices**](#).

Chapter 8 Event Center

The event information (for example, device offline) received by the client displays. In the Event Center, you can check the detailed information of the real-time and historical events, view the event linked video, handle the events, and so on.


Before the client can receive the event information from the device, you need to enable the events of the resource and arm the device first. For details, refer to [Event Configuration](#) and [Enable Receiving Event from Devices](#).

Before the you can view the pop-up alarm information, you need to enable event triggered pop-up image in the event center. For details, refer to [View Pop-up Event Information](#).

8.1 Enable Receiving Event from Devices

Before the client software can receive event notifications from the device, you need to arm the device first.

Steps

1. Click  → **Tool** → **Device Arming Control** to open Device Arming Control page.
All the added devices appear on this page.
2. Optional: If there are too many devices, enter the key words in Filter field to filter the device(s) you want.

Note

For the filtered devices, you can click **Arm All** or **Disarm All** to enable receiving event of these devices.

3. In the Auto-Arming column, turn on the switch to enable auto-arming.

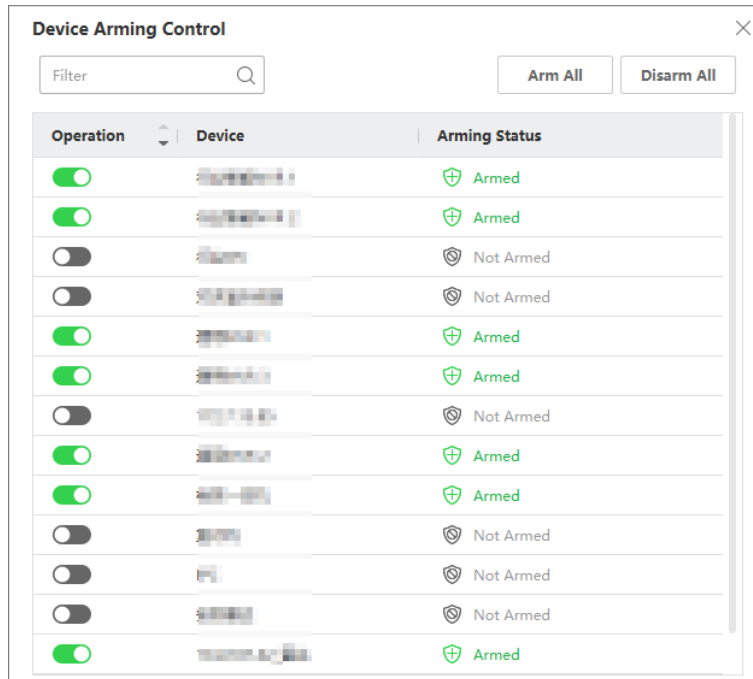


Figure 8-1 Arm Device

After turned on, the device(s) will be armed. And notifications about the events triggered by the armed device(s) will be automatically sent to the client software in real-time.

8.2 View Real-Time Events

The real-time event information received by the client of the connected resources are displayed. You can check the real-time event information, including event source, event time, priority, etc.

Before You Start

Enable receiving events from devices before the client can receive event from the device, see [***Enable Receiving Event from Devices***](#) for details.

Steps

1. Click **Event Center** → **Real-time Event** to enter the real-time event page and you can view the real-time events received by the client.

Event Time

For encoding device, event time is the client time when it receives the event. For other device types, event time is the time when the event is triggered.

Priority

Priority represents the emergency degree of the event.

2. Filter the events.

Filter by Device Type and (or) Priority Select device type(s) and (or) priorities to filter events.

Filter by Keywords Enter the keywords to filter the events.

- Optional: Right-click the table header of the event list to customize the event related items to be displayed in the event list.
- Select an event in the event list to view the event details.

 **Note**

When **Save Pictures in Structure Data Format** is enabled, no pictures will be displayed in Event Details in Event Center. For details about **Save Pictures in Structure Data Format**, refer to [Set General Parameters](#).

 **Note**

- The event details include the captured picture(s), video (recorded video triggered by the event or live view of the device), and other event descriptions.
 - To view the recorded video triggered by the event, you should link camera(s) with the device in event configuration. For details, refer to [Event Configuration](#).
 - To view the captured picture(s), you need to configure picture storage in storage schedule.
-

- Optional: Perform the following operations if necessary.

Handle Single Event Click **Handle** to enter the processing suggestion, and then click **OK**.

 **Note**

After an event is handled, the **Handle** button will become **Add Remark**. Click **Add Remark** to add more remarks for this handled event.

Handle Events in a Batch Select events that need to be processed, and then click **Handle in Batch**. Enter the processing suggestion, and then click **OK**.

Enable/Disable Alarm Audio Click **Audio On/Mute** to enable/disable the audio of the event.



Select the Latest Event Automatically Check **Auto-Select Latest Event** to select the latest event automatically and the event information details is displayed.

Clear Events Click **Clear** to clear the all the events in the event list.

Send Email Select an event and then click **Send Email**, and the information details of this event will be sent by email.



You should configure the email parameters first, see [**Set Email Parameters**](#) for details.

- | | |
|---------------------------------------|---|
| Auto-Play Video | Check Auto-Play Video to automatically play video when displaying event details. |
| Enlarge Video or Picture | <ul style="list-style-type: none">● Double click the video image to view video in a larger window.● Put the cursor on the picture, and click  to view picture in a larger window. |
| Download Captured Picture | Hover the cursor on the captured picture, and click the download icon on the lower right corner of the picture to download it to the local PC. |
| Download Event Triggered Video | Hover the cursor on the recorded video, click  to download the video (30s before the event happens) triggered by the event. |

8.3 Search Historical Events

You can search and view historical events by setting search conditions such as time, device type, and priority in the client. For the searched events, you can handle and export them.

Before You Start

Enable receiving events from devices before the client can receive event information from the device, see [**Enable Receiving Event from Devices**](#) for details.

Steps

1. Click **Event Center** → **Event Search** to enter the event search page.
2. Set the filter conditions to display the required events only.

Time

The time when the event starts.

Search by

Device

Search the events by device or the device's resource channels. If searched by device, you need to set the followings:

- **Include Sub-Node**: Search the events of the device and all resource channels.
- **Device Type**: Select the device from which you want to search events.

Group

Search the events by resource channels in the group.

Note

- For video intercom device, you need to select search scope: All and Locking Log.
 - For access control device, you can click **Show More** to set more conditions: status, event type, card reader type, person name, card No., and organization.
-

Priority

The priority including low, medium, high and uncategorized which indicates the emergency degree of the event.

Event Type

Select one or more event types to be searched from the drop-down list.

Note

You can enter a key word (supports fuzzy search) in the search box to search the target event type(s).

Status

The handling status of the event.

Search by Keyword

Enter a key word (supports fuzzy search) to quickly search the target historical event(s). For example, you can enter a person's name to search the events related with this person.

3. Click **Search** to search the events according the conditions you set.

Note


When **Save Pictures in Structure Data Format** is enabled, no pictures will be displayed in Event Details field in Event Center. For details about **Save Pictures in Structure Data Format**, refer to ***Set General Parameters***.

<input type="checkbox"/>	Index	Device Name	Event Type	Event Time	Device Type	Group Name	Object Name	Object Type	Priority	Event Details
<input type="checkbox"/>	2	101	Smoke Detection Alarm	2020-03-13 18:59:32	Encoding Device	F5	Camera 1	Camera	Uncategorized	Linked Camera: Camera 1
<input type="checkbox"/>	3	101	Detector Work Status	2020-03-13 18:59:22	Encoding Device	F5	Camera 1	Camera	Uncategorized	Linked Camera: Camera 1,
<input type="checkbox"/>	4	101	Detector Work Status	2020-03-13 18:59:12	Encoding Device	F5	Camera 1	Camera	Uncategorized	Linked Camera: Camera 1,
<input type="checkbox"/>	5	101	Detector Work Status	2020-03-13 18:59:03	Encoding Device	F5	Camera 1	Camera	Uncategorized	Linked Camera: Camera 1,
<input type="checkbox"/>	6	101	Detector Work Status	2020-03-13 18:59:03	Encoding Device	F5	Camera 1	Camera	Uncategorized	Linked Camera: Camera 1,
<input type="checkbox"/>	7	101	Detector Work Status	2020-03-13 18:59:03	Encoding Device	F5	Camera 1	Camera	Uncategorized	Linked Camera: Camera 1,
<input type="checkbox"/>	8	101	Detector Work Status	2020-03-13 18:58:49	Encoding Device	F5	Camera 1	Camera	Uncategorized	Linked Camera: Camera 1,

Total 319 Record(s) 50 / 7 Page(s)


Event Details Send Email Handle Hide

Picture



No picture

Handling records



No handling record.

Figure 8-2 Search Historical Events

4. Optional: Right click the table header of the event list to customize the event related items to be displayed in the event list.
5. Select an event in the event list to view the event details.

 **Note**

- The event details include the captured picture(s), video (recorded video triggered by the event or live view of the device), and other event descriptions.
- To view the recorded video triggered by the event, you should link camera(s) with the device in event configuration. For details, refer to ***Event Configuration***.
- To view the captured picture(s), you need to configure picture storage in storage schedule.

6. Optional: Perform one of the following operations.

Handle Single Event

Handle single event: Select one event that needs to be handled, and then click **Handle** in the event information details page, and enter the handling suggestion.

 **Note**

After an event is handled, the **Handle** button will become **Add Remark**, click **Add Remark** to add more remarks for this handled event.

Batch Handle Events

Handle events in a batch: Select the events which need to be handled, and then click **Handle in Batch**, and enter the handling suggestion.



After an event is handled, the **Handle** button will become **Add Remark**, click **Add Remark** to add more remarks for this handled event.

Auto-Play Video Check **Auto-Play Video** to automatically play video when displaying event details.

Enlarge Video or Picture

- Double click the video image to view video in a larger window.
- Put the cursor on the picture, and click to view picture in a larger window.

Send Email Select an event and then click **Send Email**, and the information details of this event will be sent by email.



You should configure the email parameters first, see [Set Email Parameters](#) for details.

Export Event Information Click **Export** to export the event log or event pictures to the local PC in CSV/Excel file. You can set the saving path manually.

Download Captured Picture Hover the cursor on the captured picture, and click the download icon on the lower right corner of the picture to download it to the local PC.

Download Event Triggered Video Hover the cursor on the recorded video, click to download the video (30s before the event happens) triggered by the event.

8.4 Get Events from Device

For some scenarios (e.g., the client cannot start up, access control device has been armed by other client, etc.), the events received by the client and triggered on access control device are not consistent. You can get events from device remotely to synchronize the events from device to Event Center of the client.

Click **Device Management** → **Device** → **Device**, select access control device(s), and click **Get Events from Device**.

Synchronize the events by the two ways:

- **Online:** When the device is online and the device can communicate with client at real time, you

can select **Online** and set the start time and end time to get the events during this period.

- **Import File:** If the network is not good or the device cannot communicate with the client at real time, you can export the event file from the selected device firstly, and import this exported file on the client later by selecting **Import File** and entering the password of the encrypted file.

 **Note**

- For data security, you should encrypt the file when exporting on the device. Meanwhile, the selected access control device should be the one you exported the file from.
 - The function should be supported by the device.
-

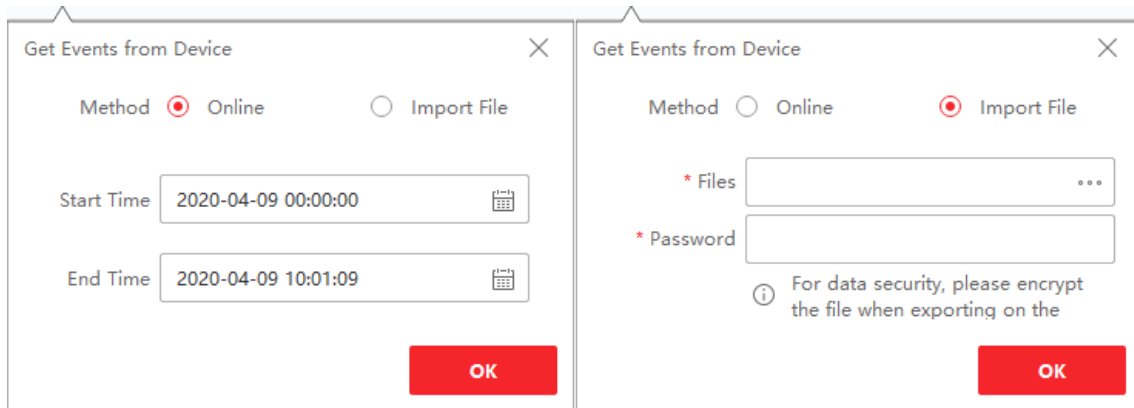


Figure 8-3 Get Events from Device

 **Note**

If you want to get the events related with attendance only, you can also enter **Time & Attendance** → **Attendance Statistics** → **Attendance Records**, click **Get Events from Device** and select **Online** or **Import File** to get the events.

8.5 View Pop-up Event Information

If you have enabled event notification and set Event Triggered Pop-up Image as its linkage action, a window will pop up when the event happens, showing the event information, related pictures, and related videos.

Go to **Event Center** → **Real-Time Event**, and then click **Enable Alarm Triggered Pop-up Image** to enable the function.

You can view the event related video footage (from 30 s before the event to the end of the event), the picture captured when the event happens, as well as the event details such as event source, linked camera, event type, etc.

 **Note**

- When the window is not closed, you should click **Next** to view the new event information if a
-

new event is triggered.

- If you haven't clear the event information, you can click **Previous** to view the previous event information.
 - When **Save Pictures in Structure Data Format** is enabled, pictures will not be displayed in the event information. See [Set General Parameters](#) for more details.
-

You can check **Auto-Update Event** to enable the window to automatically switch to the latest event information when a new event is triggered.

Chapter 9 Map Management

The E-map function gives a visual overview of the locations and distributions of the installed cameras and alarm input devices. You can get the live view of the cameras on the map, and you will get a notification message from the map when alarm is triggered.

E-map is a static image (it do not have to be geographical maps, although they often are). Depending on your organization's needs, photos and other kinds of image files can also be used as e-maps) which gives you a visual overview of the locations and distributions of the hot spots (resources (e.g., camera, alarm input) placed on the map are called hot spots). You can see the physical locations of the cameras and alarm inputs, and in what direction the cameras are pointing. With the function of hot region, e-maps can be organized into hierarchies to navigate from large perspectives to detailed perspectives, e.g., from floor level to room level.

9.1 Add Map

You should add a map as the parent map for the hot spots and hot regions.

Steps

 **Note**

Only one map can be added to one group.

1. Open the E-map page.
2. Select a group for which you want to add a map.

 **Note**

For details about setting the group, refer to [***Group Management***](#).

3. Click **Add Map** to open the map adding window.

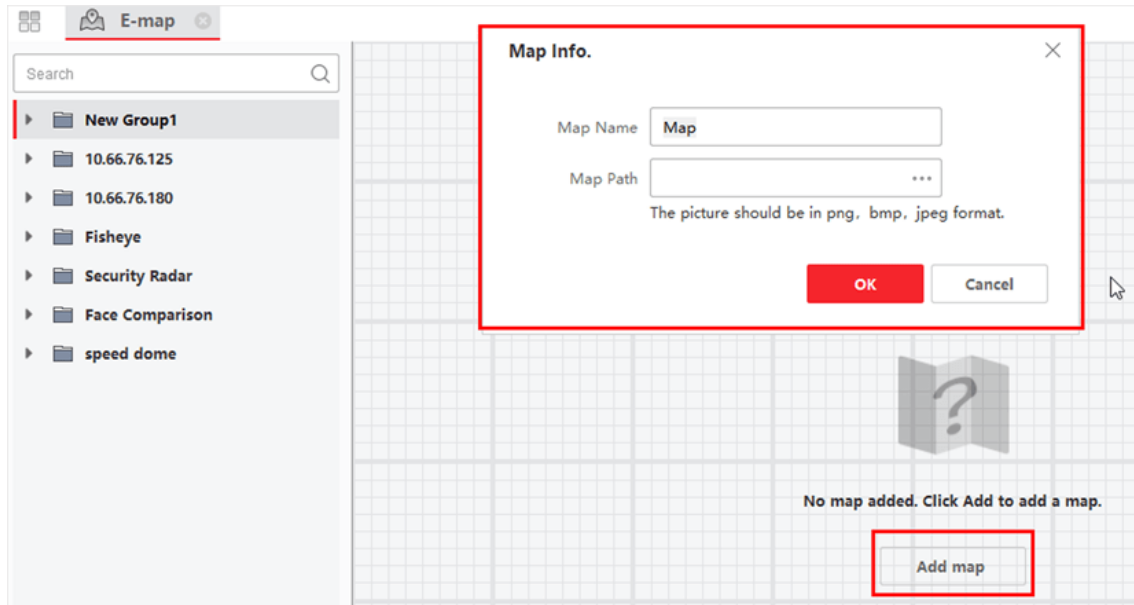


Figure 9-1 Add Map

4. Enter a descriptive name of the added map.
5. Select a map picture from the local path.

Note

The picture format of the map can only be PNG, JPEG or BMP.

6. Click **OK**.
7. Optional: Perform the following tasks after adding the map.

Zoom in/out Use the mouse wheel or click + or - to zoom in or zoom out on the map.

Adjust Map Area Drag the yellow window in the lower-right corner or use the direction buttons and zoom bar to adjust the map area for view.

9.2 Edit Map Scale


The scale of a map is the ratio of a distance on the map to the corresponding distance on the ground. The client can calculate two locations' distance on the map according to the distance on the ground. An accurate map scale is essential for defining radar's monitoring range.

Before You Start

Make sure you have added a map. See [Add Map](#) for details.

Perform this task if you need to add a security radar to the map.

Steps

1. Enter the E-map module.
2. Click **Edit** on the E-map toolbar to enter the map editing mode.
3. Click **Map Calibration** → **Edit Scale** to select two locations on the map.
The cursor will turn to  if you hover it on the map.

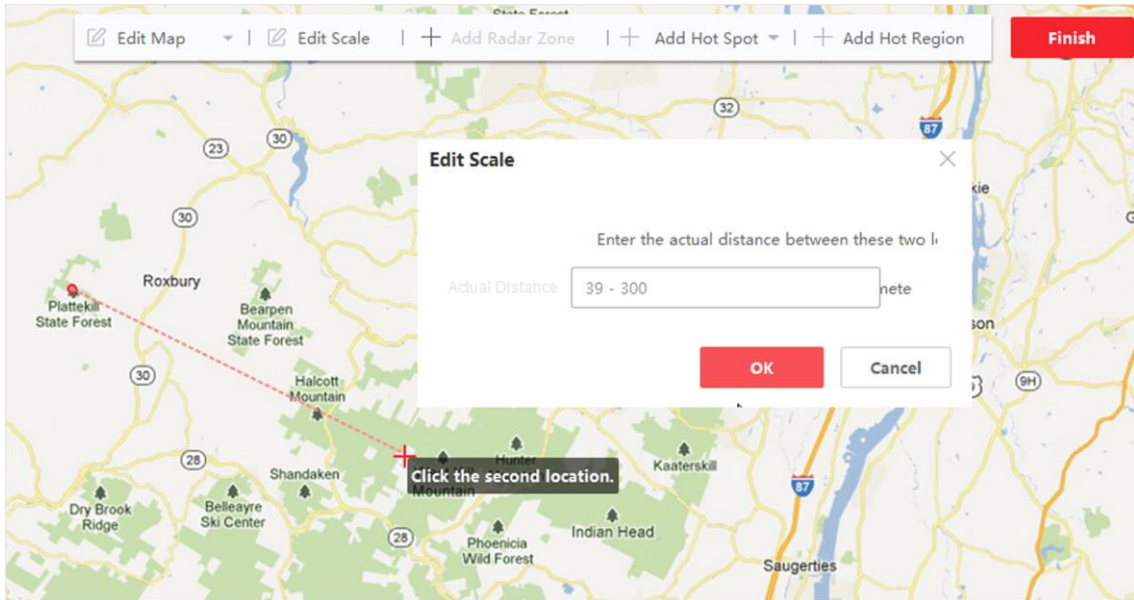


Figure 9-2 Edit Map Scale

4. Click on the map to select two locations.
The Edit Scale window pops up.
5. Enter the ground distance between the two locations, and then click **OK**.
The client will calculate the map scale automatically.

9.3 Longitude and Latitude Calibration

After calibrating the longitude and latitude of two points on the E-map, you can drag the radar in the group to the E-map. The radar will automatically move to the correct position on the E-map according to the longitude and latitude calibrating result.

Before You Start

1. Make sure you have added radar on the Client. For details, refer to [Add Single or Multiple Online Devices](#).
2. Make sure you have set the longitude and latitude parameters of the radar by web browser.

Steps

1. Enter the E-map module.
2. Click **Edit** on the E-map toolbar to enter the map editing mode.
3. Click **Map Calibration** → **LongitudeLatitude Calibration**.

4. Click **Add Calibration Point**.
5. Click a point on the map, enter the longitude and latitude of the point in the pop-up window, and then click **Save**.
6. Click **Add Calibration Point** and repeat the previous step to add the second calibration point.
7. Drag the radar in the left resources group to the map.
The radar will automatically move to the correct position on the map according to the longitude and latitude of two points calibration.

9.4 Manage Hot Spot

The devices added to the map are called hot spots. The hot spots show the locations of the devices, and you can also get the live view or alarm information of the monitoring scenarios through the hot spots.

9.4.1 Add Camera as Hot Spot

You can add cameras to the map as hot spots.

Before You Start

Make sure you have added an e-map and a camera to the client. See [Add Map](#) and [Device Management](#) for details.

Steps

1. Enter the E-map page.
2. Click **Edit** in the upper-right corner to enter the map editing mode.
3. Click **Add Hot Spot** → **Camera Hot Spot** to open the Add Hot Spot window.

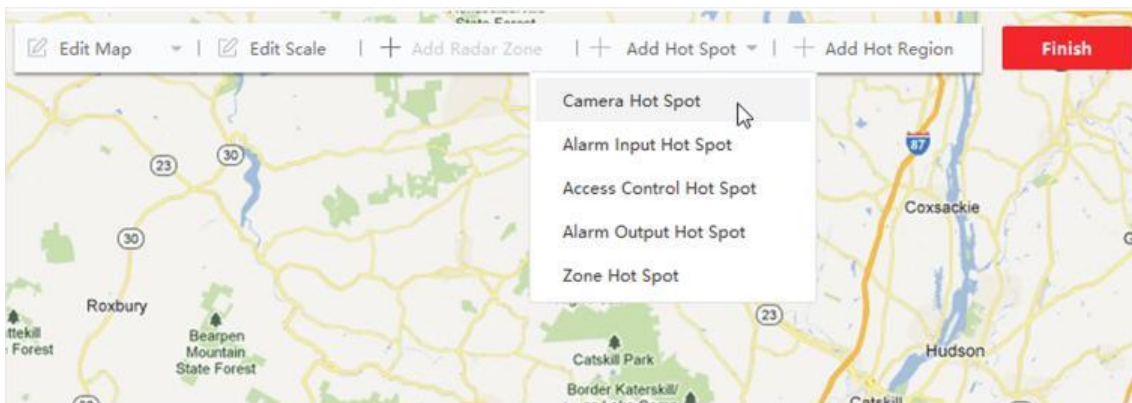


Figure 9-3 Add Hot Spot

4. Select the cameras to be added to the map.
5. Optional: Edit the hot spot name, select the name color and select the hot spot icon.
6. Click **OK** to save the settings.

Note

You can also drag the camera icons from the group list to the map directly to add the hot spots.

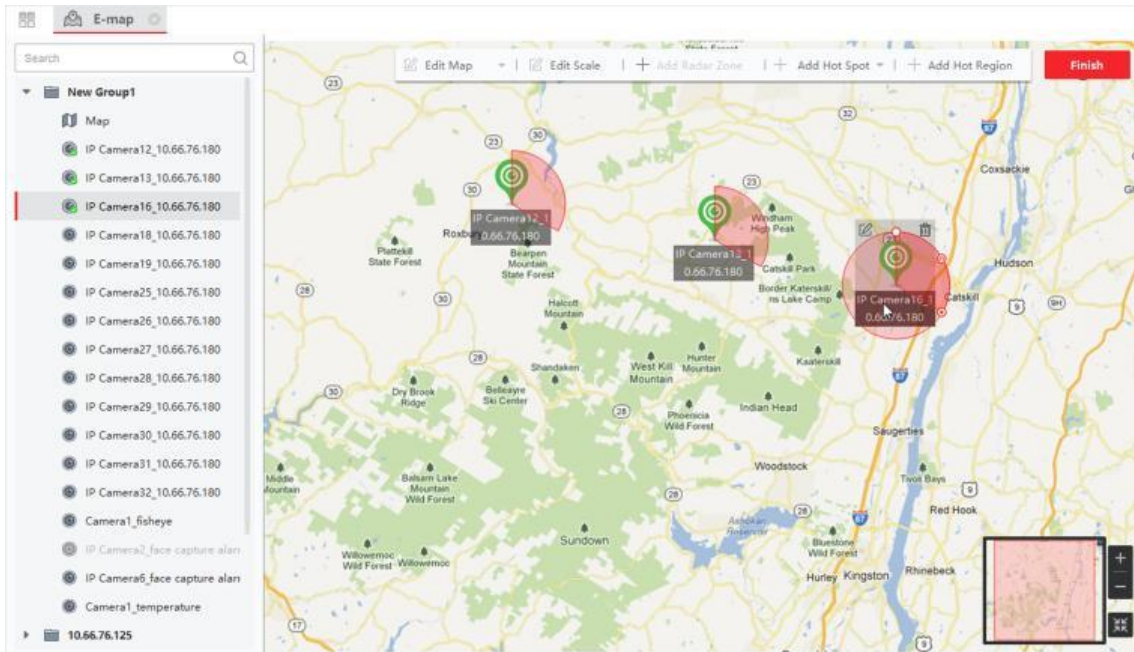


Figure 9-4 Added Camera Hot Spot

The camera icons are added on the map as hot spots and the icons of the added cameras in the group list change from to . The sector indicates the camera's field of view.

7. Perform the following operation(s).

Move the Hot Spot Drag the hot spot to move it to a certain position.

Change the FOV Angle Drag and revolve to change the camera's field of view.

Change the FOV Size Drag to change the FOV size.

9.4.2 Add Alarm Input as Hot Spot

You can add the alarm inputs to the map as hot spots.

Steps

1. Enter the E-map module.
2. Click **Edit** in the upper-right corner to enter the map editing mode.
3. Click **Add Hot Spot** → **Alarm Input Hot Spot** to open the Add Hot Spot window.

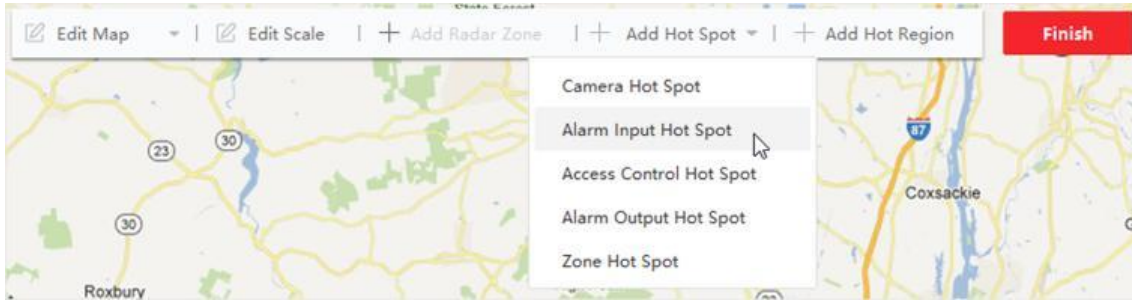


Figure 9-5 Add Alarm Input as Hot Spot

4. Select the alarm inputs to be added to the map.
5. Optional: Edit hot spot name, select the name color and select the hot spot icon by double-clicking the corresponding field.
6. Click **OK**.

Note

You can also drag the alarm input icons from the group list to the map directly to add the hot spot.

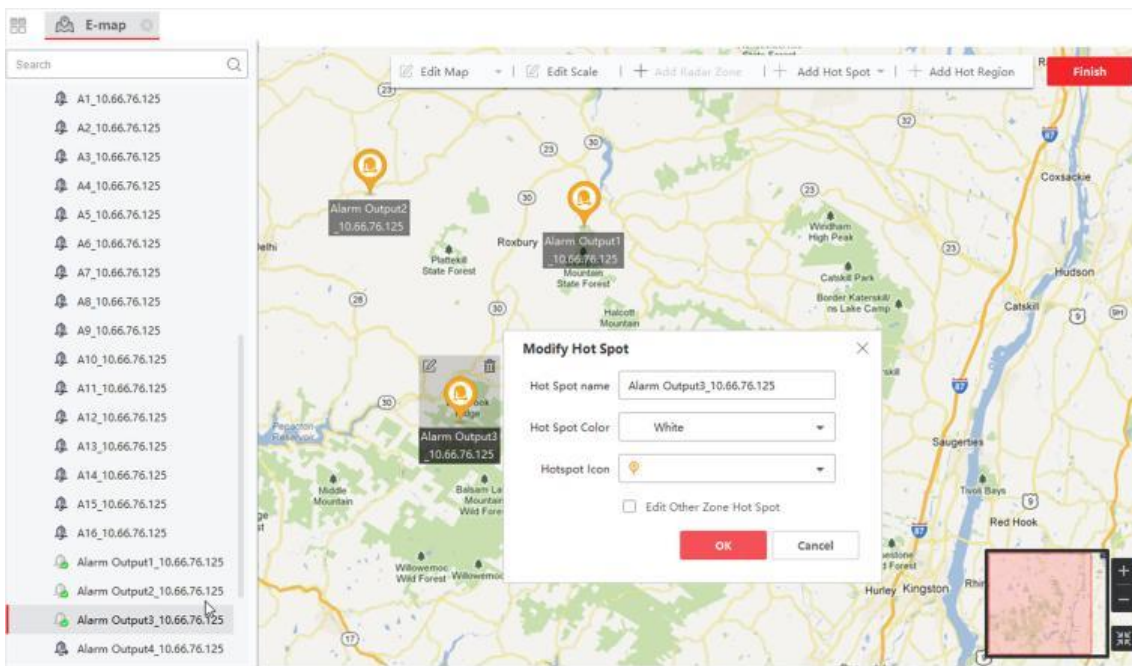




Figure 9-6 Added Alarm Input Hot Spot

The alarm input icons are added to the map as hot spots and the icons of the added alarm inputs in the group list change from  to .

7. Optional: Drag the hot spot to move it to a certain position.

9.4.3 Add Alarm Output as Hot Spot

You can add alarm outputs to the map as hot spots for management. After that, you can enable or disable it in a quick manner. If you enable an alarm output on the map, the security control devices (e.g. sirens, bells) connected to it will alarm for attention.

Before You Start

Make sure you have added an e-map and alarm output to the client. See [Add Map](#) and [Device Management](#) for details.

Steps

1. Enter the E-map module.
2. Click **Edit** on the E-map toolbar to enter the map editing mode.
3. Click **Add Hot Spot** → **Alarm Output Hot Spot** to open the Add Hot Spot panel.

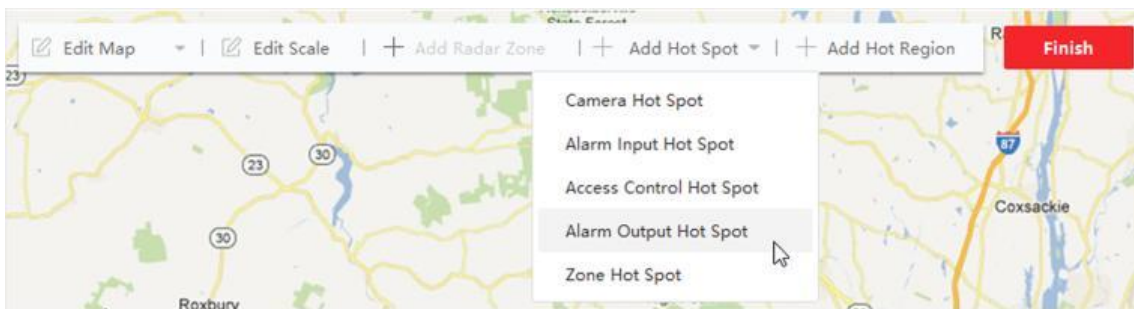


Figure 9-7 Add Alarm Output as Hot Spot

4. Select the alarm output to be added to the map.
5. Optional: Edit the hot spot name, select the name color, and select the hot spot icon.
6. Click **OK**.

Note

You can also drag an alarm output icon from the alarm output list to the map to add the hot spot.

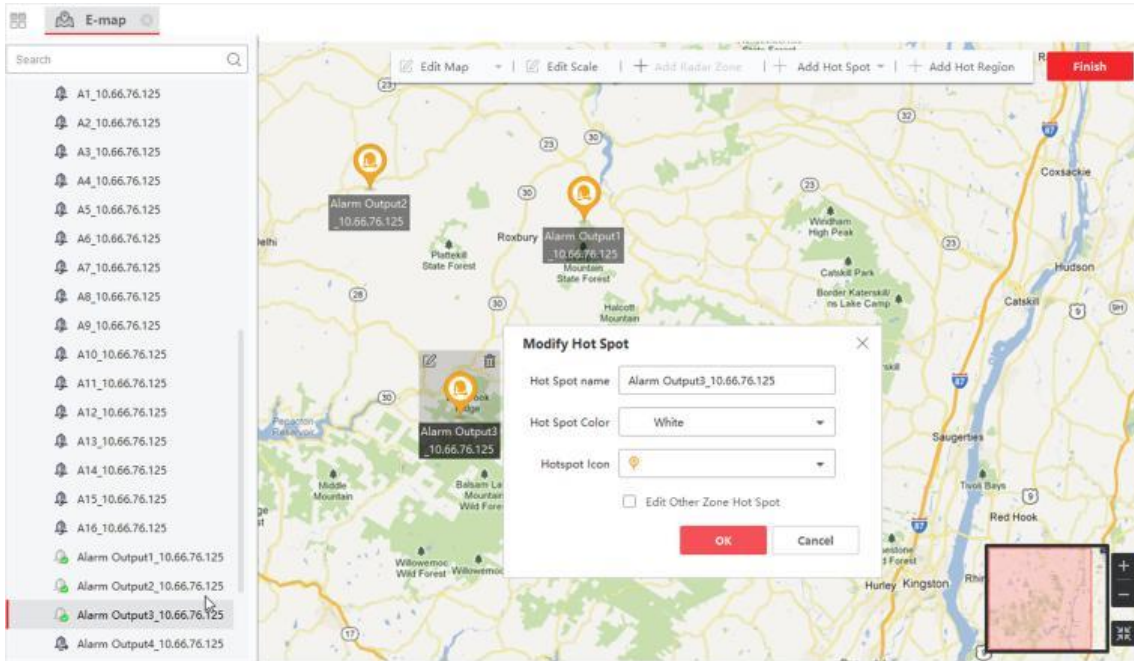




Figure 9-8 Added Alarm Output Hot Spot

The alarm output is added to the map as a hot spot and its icon in the group list changes from  to .

7. Optional: Drag the alarm output to move it to a certain position.

9.4.4 Add Zone as Hot Spot

You can add zones to the map so that you can quickly locate the zone when an alarm is triggered.

Before You Start

Make sure you have added a map and zone to the client. See [Add Map](#) and [Add Device](#) for details.

Steps

1. Enter the E-map module.
2. Click **Edit** on the E-map toolbar to enter the map editing mode.
3. Click **Add Hot Spot** → **Zone Hot Spot** to open the Add Hot Spot panel.

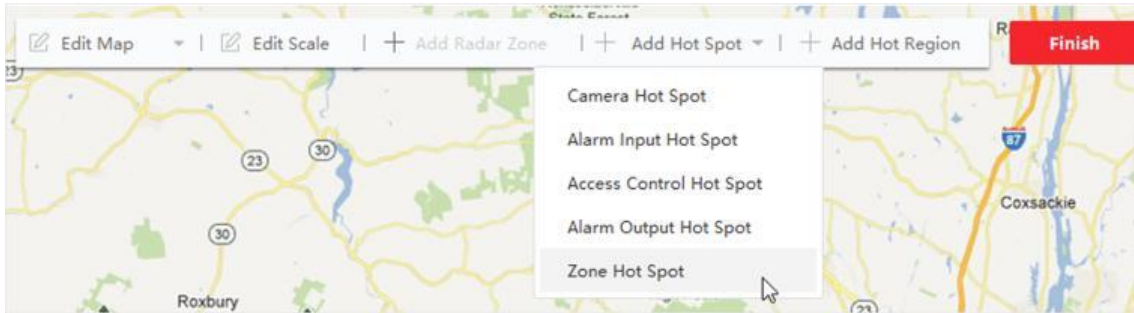


Figure 9-9 Add Zone as Hot Spot

4. Select the zone(s) to be added to the map.
5. Optional: Edit the hot spot name, select the name color, and select the hot spot icon.
6. Click **OK**.

 **Note**

You can also drag the alarm output icons from the alarm output list to the map to add the hot spot.

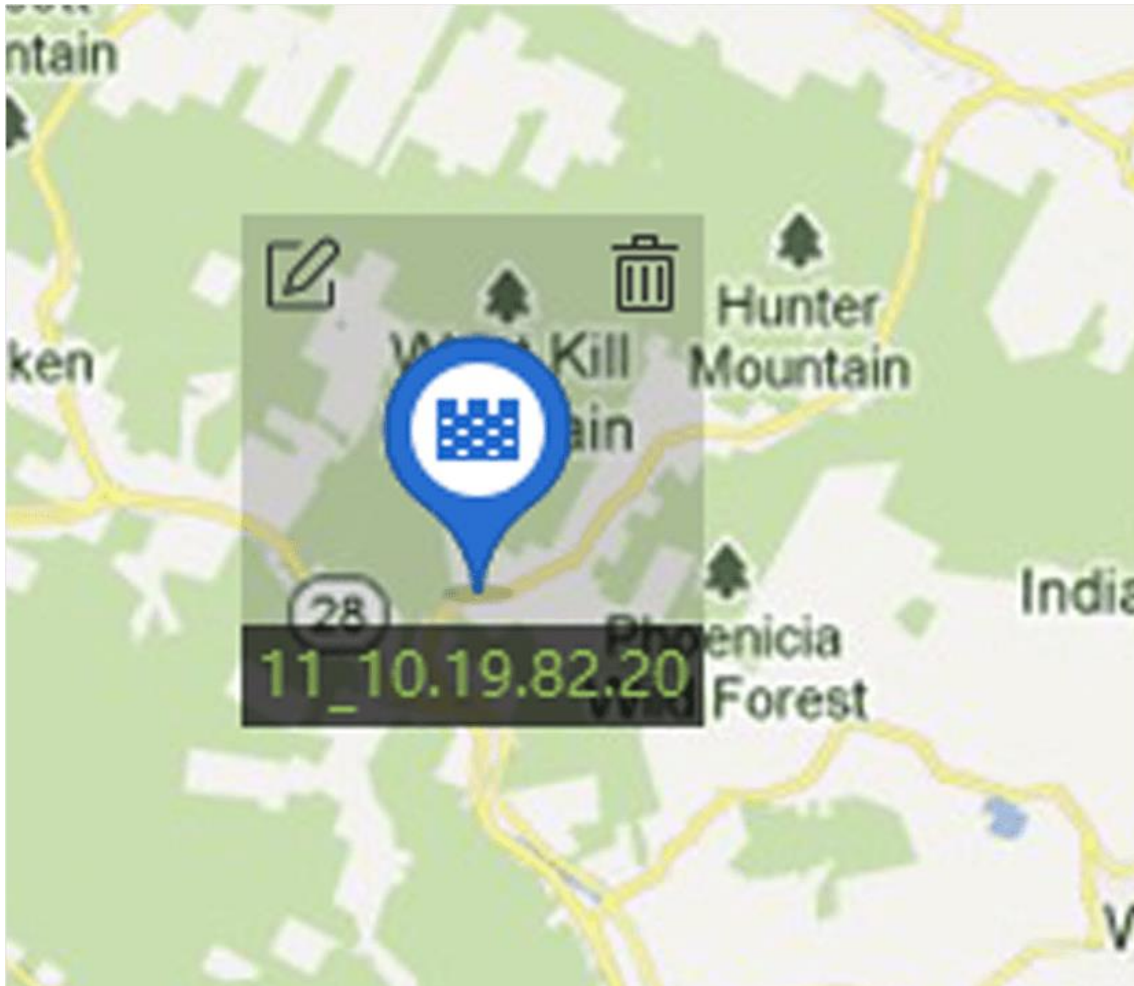




Figure 9-10 Zone on the Map

The zone is added to the map as a hot spot and its icon in the group list changes from  to .

7. Optional: Drag the zone hot spot to move it to a certain position.

When alarms are triggered, the number of the newest alarms will be displayed on the zone's icon. You can click the number to see the alarms details.

 **Note**

No more than 10 newest alarms can be displayed.

8. Optional: Click **Clear Alarms** to mark the alarms of the zones on the current map as read.

9.4.5 Add Access Point as Hot Spot

You can add access points to the map as hot spots, so that you can find the hot spots and view their status and alarm numbers.

Before You Start

Make sure you have added a map and an access point to the client. See [Add Map](#) and [Add Device](#) for details.

Steps

1. Enter the E-map module.
2. Click **Edit** on the E-map toolbar to enter the map editing mode.
3. Click **Add Hot Spot** → **Access Point Hot Spot** to open the Add Hot Spot window.

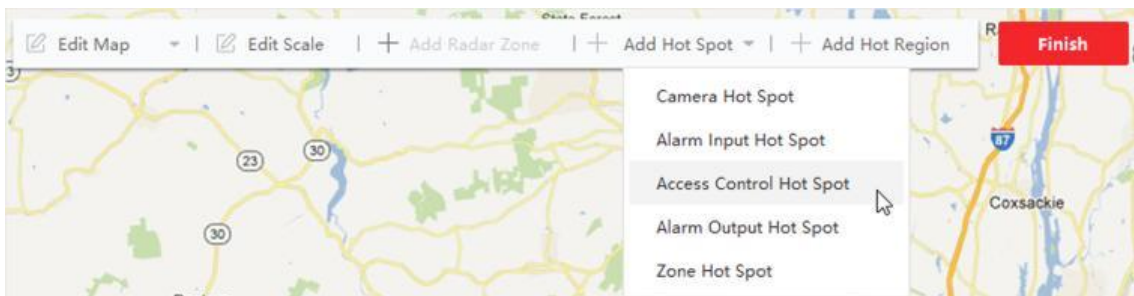


Figure 9-11 Add Access Point as Hot Spot

4. Select the access point(s) to be added to the map.
5. Optional: Edit the hot spot name, select the name color, and select the hot spot icon.
6. Click **OK**.

Note

You can also drag an access point icon from the access point list to the map.

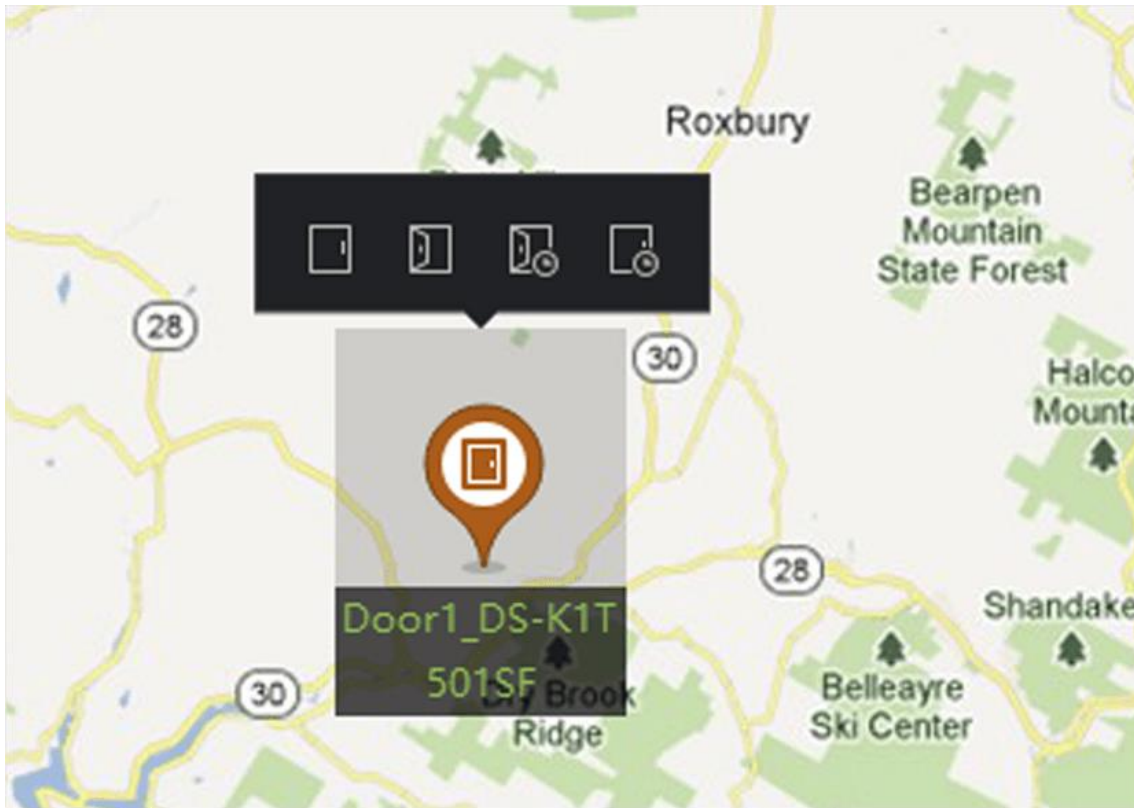




Figure 9-12 Access Point on the Map

The access point is added to the map as a hot spot and its icon in the group list changes from  to .

7. Optional: Drag the access point hot spot to move it to a certain position.

When alarms are triggered, the number of the newest alarms will be displayed on the hot spot icon. You can click the number to see the alarms details.

Note

No more than 10 newest alarms can be displayed.

Chapter 10 Statistics

10.1.1 People Counting Report by Encoding Device

People counting report by encoding device displays people counting data collected by encoding devices. You can search the people counting data in different dimensions.

Before You Start

Add an encoding device with people counting function to the software and properly configure the corresponding area and people counting rule. Refer to [Add Device](#) for details about adding people counting device.

Steps

1. Click **Report** → **People Counting** to enter People Counting page.
2. Select **Encoding Device** as the **Device Type**.
3. Select daily report, weekly report, monthly report, or annual report as the report type.

Daily Report

Daily report shows data on a daily basis. The system will calculate the number of people in each hour of one day.

Weekly Report, Monthly Report and Annual Report

As compared to daily report, weekly report, monthly report and annual report can be less-time consuming, since they are not to be submitted every day. The system will calculate the number of people in each day of one week, in each day of one month, in each month of one year.

Custom Report

Users can customize the days in the report to analyze the number of people in each day or month of the custom time interval.

Note

You can select no more than 31 days on the calendar.

4. Select the statistics time type and click  to set the time.

One Period

Generate the statistics in one time period.

Multiple Periods

Generate the statistics in two time periods, which can help you to compare the people flow and number in two time periods.

For example, if you set the report type as month report, and set the March and April as the statistic time, the people counting results in March and April will be displayed in a same chart with different color, and you can compare the data in different day of each month.

5. Select **Statistics Type**.

Display by Device

Display the report by device.

For example, if you select one NVR (with 4 people counting cameras), the report will display the total number of people summed by the 4 people counting cameras.

Display by Camera

Display the report by camera.

For example, if you select one NVR (with 4 people counting cameras), the report will display the each camera's statistics respectively, namely display the statistics in 4/8 colors (each one or two colors representing one camera).

Display by Grouping Statistics

Display the report by grouping statistics.

For example, if you select one device group (the group is created on the Client), the report will display the total number of people summed by the total people counting cameras in the group.

Note

- For details of device group, refer to **Group Resources**.
 - This function should be supported by the device.
-

6. Select filtering mode.

Channel

Display people counting data collected by channels of an encoding device.

Region

Display number of people in selected regions of a camera.

Note

You need to configure regions for the camera beforehand. See user manual of the device for details.

7. Select camera(s) or region(s) from the **Camera** list.

8. Set the content to be displayed.

Direction

Calculate the number of people in different directions, such as enter, exit, or enter and exit.

Enter

The people entered will be counted.

Exit

The people exited will be counted.

Enter and Exit

Both people entered and exited will be counted.

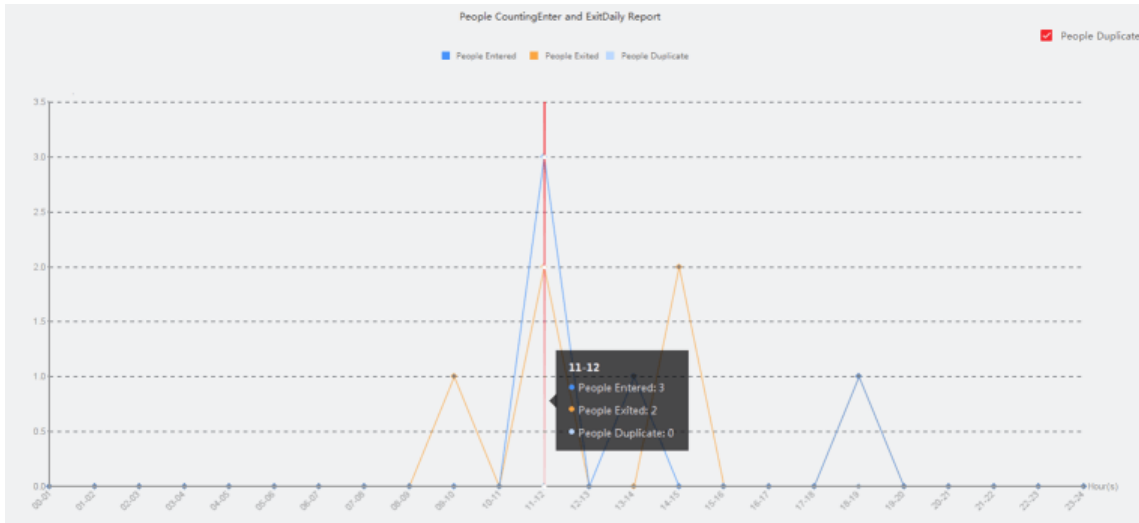


Figure 10-1 People Counting by Direction

Facial Features

Generate the report based on the facial feature.

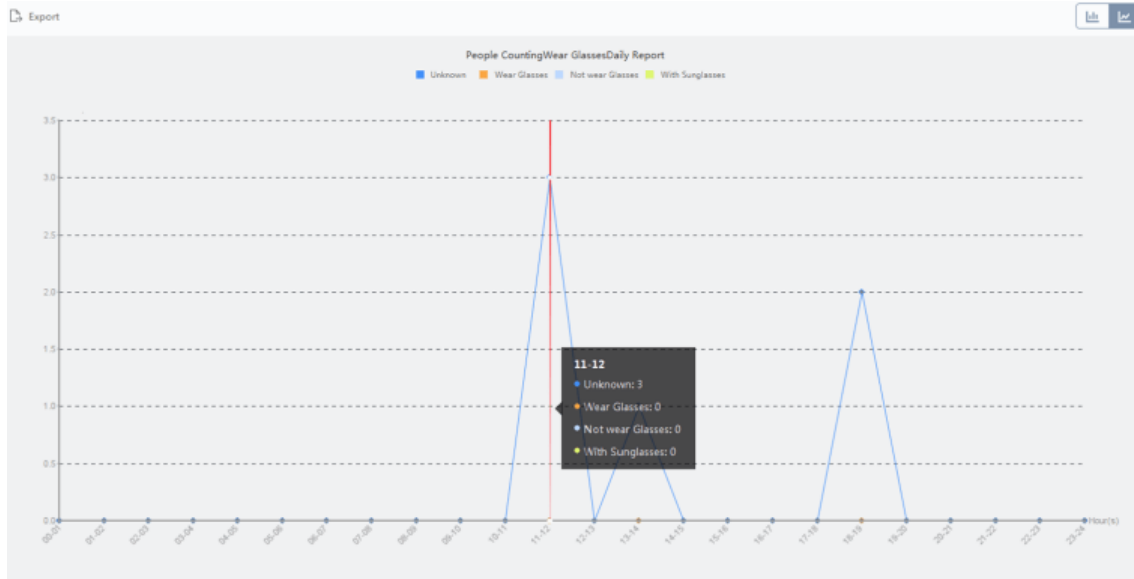


Figure 10-2 People Counting by Facial Features

9. Optional: Check **Children Only** to generate report of recognized children.

Note

- The client counts detected people shorter than a predefined height which can be configured on device's remote configuration page. See the device user manual for details about configuring height threshold.
- This function needs to be supported by the device.

10. Click **Search** to get the people counting statistics and detailed data for each hour, day, or month.

By default, the statistics are shown in histogram form.

11. Optional: For the report by direction, you can check **People Duplicate** on the right-upper corner of the report page to display the number of duplicate people.

Note

The number of duplicate people is calculated by the device. If the same face is recognized more than once, he/she will be calculated as duplicate person.

For example, if a cashier enter or exit the supermarket more than once, he/she will be calculated as duplicate person. In this way, the supermarket can get the actual number of people shopping.

12. Optional: Perform the following operations after search.

Switch to Line Chart Click  to switch it to line chart.



By default, the statistics are shown in bar chart.

Switch to Bar Chart Click  to switch it to bar chart.

Save to Local PC Click **Export** to save the detailed data of people counting to your PC.

10.2 View People Counting in Intersections Report

Intersection analysis is used to monitor people flow and number in an intersection-like scene. The arrows in the image refer to different directions. By selecting one direction (e.g. A) as the entrance, the other directions will be set as the exits by default, so that multiple paths are generated (e.g., A to A, A to B, A to C, and A to D). You can view the people counting who passed by each path, respectively, which can help the shopkeeper to analyze the people flow in different door. The statistics result can show in daily, weekly, monthly, and annual report.

Before You Start

Make sure a fisheye camera which supports intersection analysis function has been configured properly and be added to the software. Refer to [Add Device](#) for details about adding the device.

Steps



Up to 10 intersections can be analyzed.

1. Click **Report** → **Intersection Analysis** to enter the intersection analysis module.
2. Select daily report, weekly report, monthly report, or annual report as the report type.

Daily Report

Daily report shows data on a daily basis. The system will calculate the number of people in intersection report in a each hour of one day.

Weekly Report, Monthly Report and Annual Report

As compared to daily report, weekly report, monthly report and annual report can be less-time consuming, since they are not to be submitted every day. The system will calculate the number of people in intersection report in each day of one week, in each day of one month, in each month of one year.

3. Set the start time for the report.
4. Select the camera for generating the report.
5. Select one direction as the entrance from the drop-down list in the **Flow in** filed.
6. Click **Search** to get the statistics result.

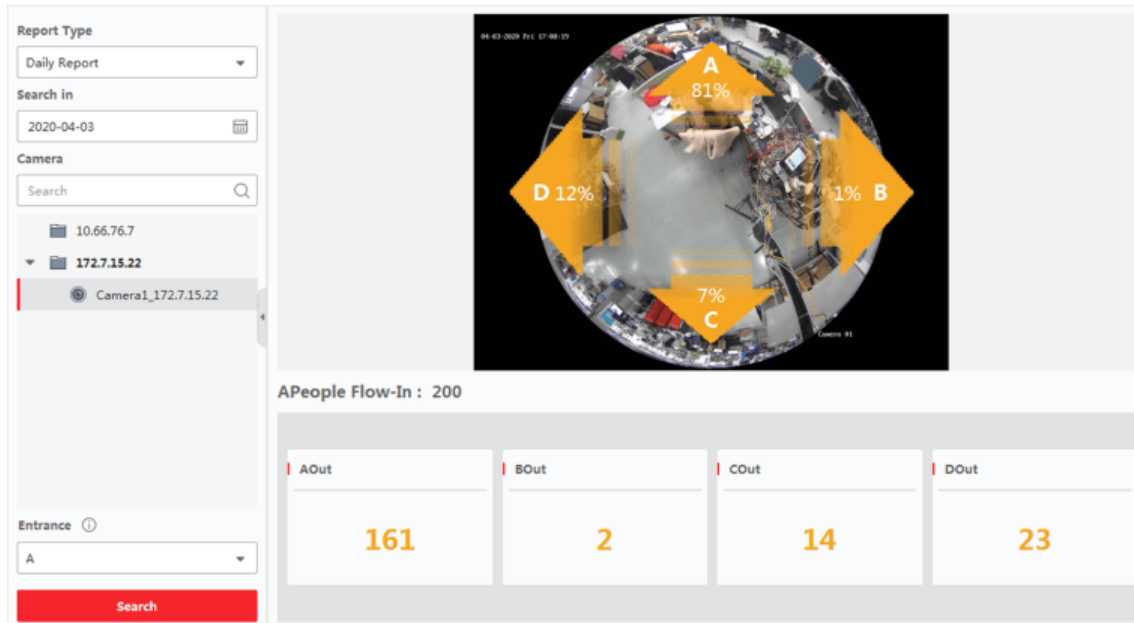


Figure 10-4 Results

The people number for each path will show on the right.

10.4 Heat Map Report

Heat map is a graphical representation of data represented by colors and the heat map data can be displayed in line chart. You can use the heat map function of the camera to analyze the visit times and dwell time of customers in a configured area, which can help the storekeeper analyze the customers' interested area and make the arrangement of goods.

Before You Start

Add a heat map network camera to the software and properly configure the corresponding area. The added camera should have been configured with heat map rule. See [Add Device](#) for details about adding heat map network camera.

Steps

1. Click **Report** → **Heat Map** to enter the heat map page.
2. Select **Daily Report/Weekly Report/Monthly Report/Annual Report/Custom Report** as the report type.

Daily Report

Daily report shows data on a daily basis. The system will calculate the data of heat map in a each hour of one day.

Weekly Report, Monthly Report and Annual Report

As compared to daily report, weekly report, monthly report and annual report can be less-time consuming, since they are not to be submitted every day. The system will calculate the data of heat map in each day of one week, in each day of one month, in each month of one

year.

Custom Report

You can customize the days in the report to analyze the dwell time or crowd trend on each day or month of the custom time interval.

Note

The time period in the custom report should be no more than 31 days.

3. Select **By Dwell Time** or **By Crowd Trend** as the statistics type.

By Dwell Time

The system calculates the heat map value (the ordinate value in the line chart or the color in pictures) according to the people's dwell time.

By Crowd Trend

The system calculates the heat map value (the ordinate value in the line chart or the color in pictures) according to the number of detected people.

4. Set the time period for searching.
5. Select a heat map camera in the camera list.
6. Click **Generate Heat Map** to show the heat map of the camera.

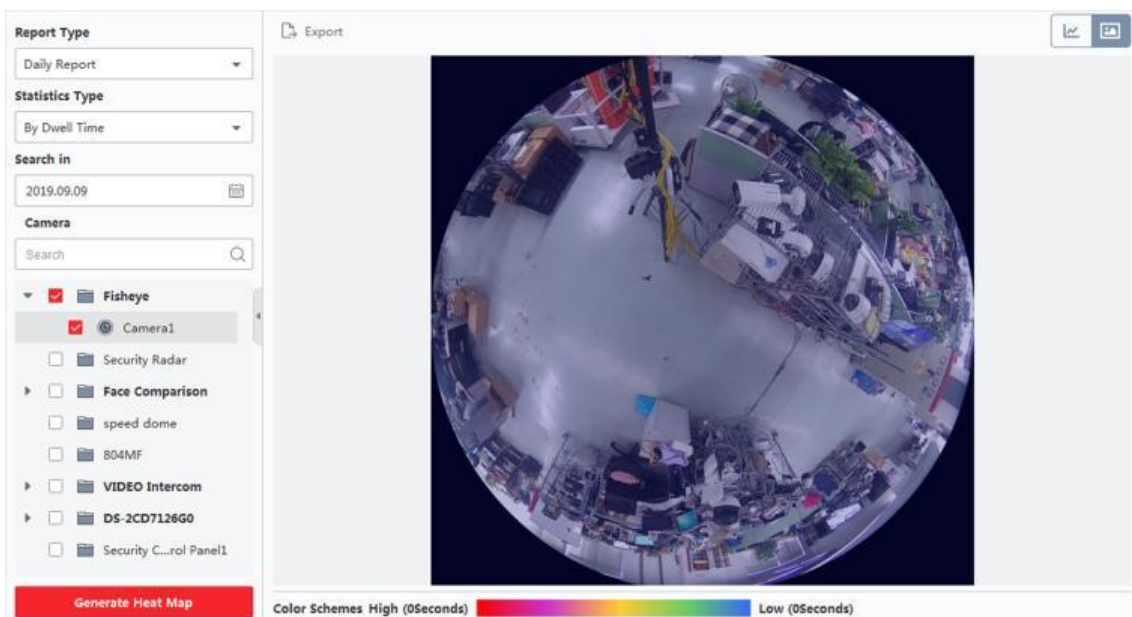



Figure 10-9 Results

7. Optional: After generating heat map report, you can perform the following operations.

Display in Line Chart Click  to display the statistics in line chart.

Display in Picture Mode Click  to display the statistics in picture mode.

The red color block (255, 0, 0) indicates the most welcome area, and

blue color block (0, 0, 255) indicates the less-popular area.

Save Statistics Data Click **Export** to save the detailed data of heat map to your PC.

10.7 Temperature Map

A temperature map displays the temperature trend of a region during a certain day. If you have configured temperature monitoring regions, you can generate temperature map of specific regions to see the overview of each region's temperature trend.

Before You Start

- Make sure you have drawn regions for temperature map on the device configuration page. See user manual of the device for details.
- Make sure you have added at least one device for temperature map to the client. See [**Add Device**](#) for details.

Steps

 **Note**

This function should be supported by device.

1. Click **Report** → **Temperature Map**.
2. Select a date from the calendar.
3. In the Camera list, select a camera.

 **Note**

You can enter a keyword in the searching field to search a camera.

4. Select a unit.
5. Select a preset.

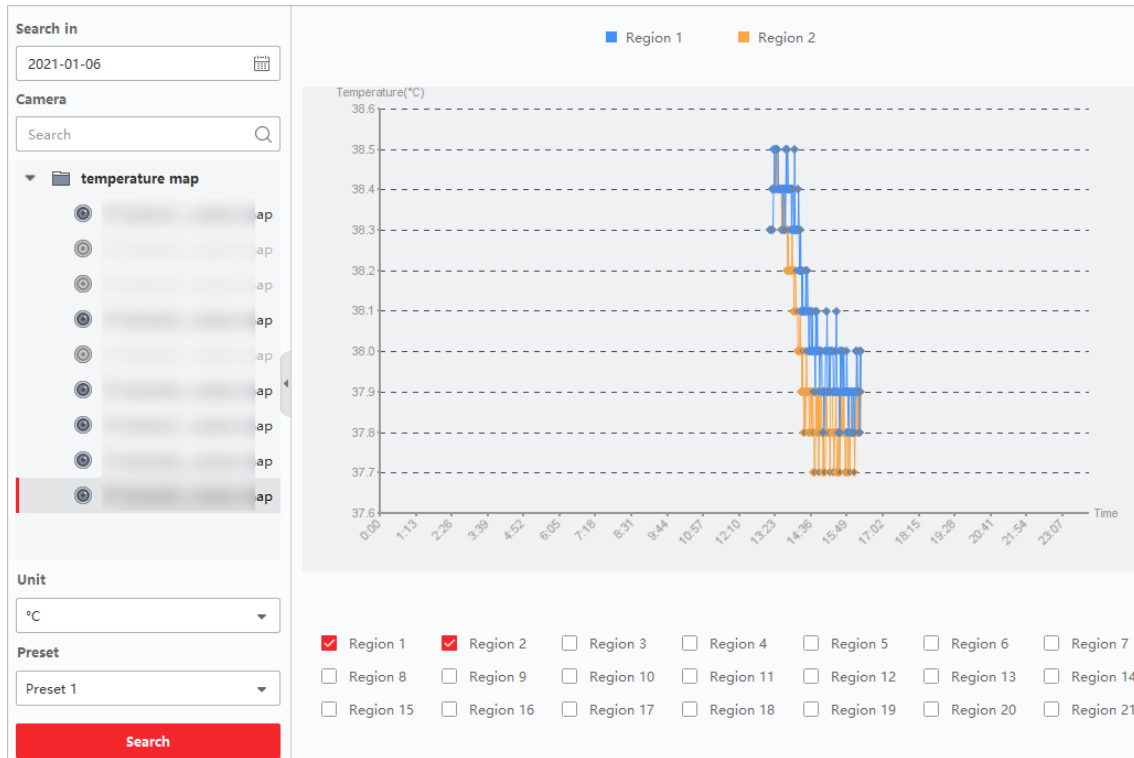


Figure 10-12 Temperature Map

6. On the right panel, check region(s) for generating the report.

Note

No more than 8 regions can be checked.

7. Click **Search**.

The temperature map will be displayed in a line chart with each line representing a region.

8. Optional: Select another unit to display the temperature map in another unit.

Chapter 11 Data Retrieval

In the Data Retrieval module, you can search for car and human object based recordings. The device must support “Car” or “Human” function.


11.1 Vehicle Retrieval

For devices that support vehicle retrieval, you can search the related vehicle pictures and videos by setting the search conditions such as plate number and captured time.

Before You Start

Add the device that supports vehicle retrieval to the client and properly configure the corresponding settings. See [Add Device](#) for details about adding the device.

Steps

1. Click **Data Retrieval** → **Vehicle Retrieval** to enter the vehicle retrieval page.
2. Click  to set the start time and end time for search.
3. Select the search type.

Vehicle

Search and display the captured vehicle pictures by entering the vehicles' license plate number.

Mix-traffic Detection

Search and display the mix-traffic detection related pictures of the specific vehicle by entering the vehicle's license plate number.

Note

The camera should support mix-traffic detection.

4. Select a device from the camera list.
-

6. Optional: Enter the license plate number (support fuzzy search) for search.

7. Optional: Set the maximum number of searched results to be displayed.

8. Click **Search** to start searching.

The captured pictures which meet the search conditions are displayed on the right panel. Up to 30 pictures can be displayed on one page.

9. Optional: Perform the following operations if needed.

Export Picture

You can export one or more searched pictures.

1. Click **Export Picture**.
2. Check one or more picture(s), or check **Select All** on the page

below.

3. Click **Export** to export the selected picture(s) to local PC.





View Capture Details Click a picture to view its capture details such as captured time and camera name.


 **Note**

You can click  to view an enlarged picture.

Play Related Video Click **Playback** to play the picture's related video file (5s before and 5s after the capture) in the view window.

 **Note**

- You can click  to view the video in a larger window.
 - You can click  to adjust the play speed of the playback, click  to play back the video file frame by frame, and click  to enable audio.
-

Export Single Record In the enlarged picture page, click  and then click **Export Picture**, **Export Video File** or **Export Details** to export the picture, video file, and capture details of single record to local PC.

Chapter 14 Person Management

You can add person information to the system for further operations such as access control, video intercom, time and attendance, etc. You can manage the added persons such as issuing cards to them in a batch, importing and exporting person information in a batch, etc.

Important note: For detailed configuration e.g for ABUS Intercom Systems or ABUS Face Access modules, read the corresponding manual to the fitting product.

14.1 Add Organization

You can add an organization and import person information to the organization for effective

management of the persons. You can also add a subordinate organization for the added one.


Steps


1. Enter **Person** module.
2. Select a parent organization in the left column and click **Add** in the upper-left corner to add an organization.
3. Create a name for the added organization.

Note

Up to 10 levels of organizations can be added.

4. Optional: Perform the following operation(s).

Edit Organization Hover the mouse on an added organization and click  to edit its name.

Delete Organization Hover the mouse on an added organization and click  to delete it.

Note

- The lower-level organizations will be deleted as well if you delete an organization.
 - Make sure there is no person added under the organization, or the organization cannot be deleted.
-

Show Persons in Sub Organization Check **Show Persons in Sub Organization** and select an organization to show persons in its sub organizations.

14.2 Add Single Person

You can add persons to the client software one by one. The person information contains basic information, detailed information, profiles, access control information, credentials, custom information, etc.

14.2.1 Configure Basic Information

You can add person to the client one by one and configure the person's basic information such as name, email, phone number, etc.

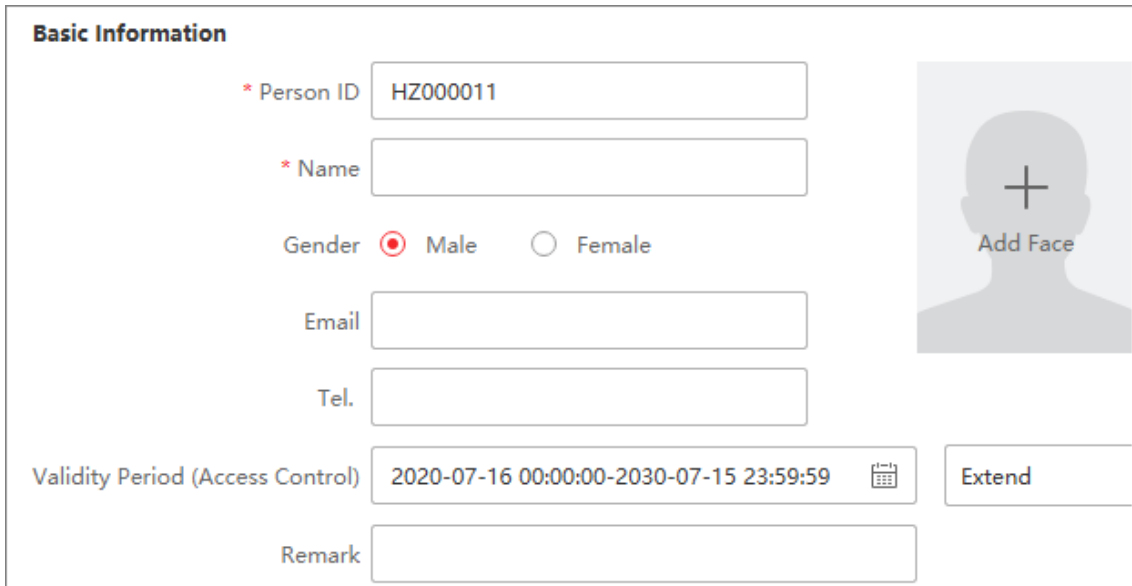
Steps

1. Enter **Person** module.

 **Note**

For the first time you enter **Person** module, a window pops up, and you can set the rules to generate person ID (letters and numbers supported) when adding person. When getting person information from device, if there are no person IDs, the person IDs will be generated according to the rule.

2. Select an organization in the organization list to add the person.
3. Click **Add** to open the adding person window.
The Person ID will be generated automatically.
4. Enter the basic information including person name, telephone number, email address, validity period, etc.



Basic Information


* Person ID

* Name

Gender Male Female

Email

Tel.

Validity Period (Access Control) 

Remark

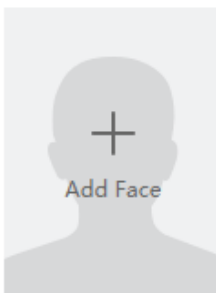


Figure 14-1 Configure Basic Information

 **Note**

Once validity period expired, the credentials and access control settings of the person will be invalid and the person will have no authorization to access the doors\floors. You can click **Extend** to extend the person's validity period for 1 month, 3 months, 6 months, or 1 year.

5. Confirm to add the person.
 - Click **Add** to add the person and close the Add Person window.
 - Click **Add and New** to add the person and continue to add other persons.
6. Delete Registered Face Picture

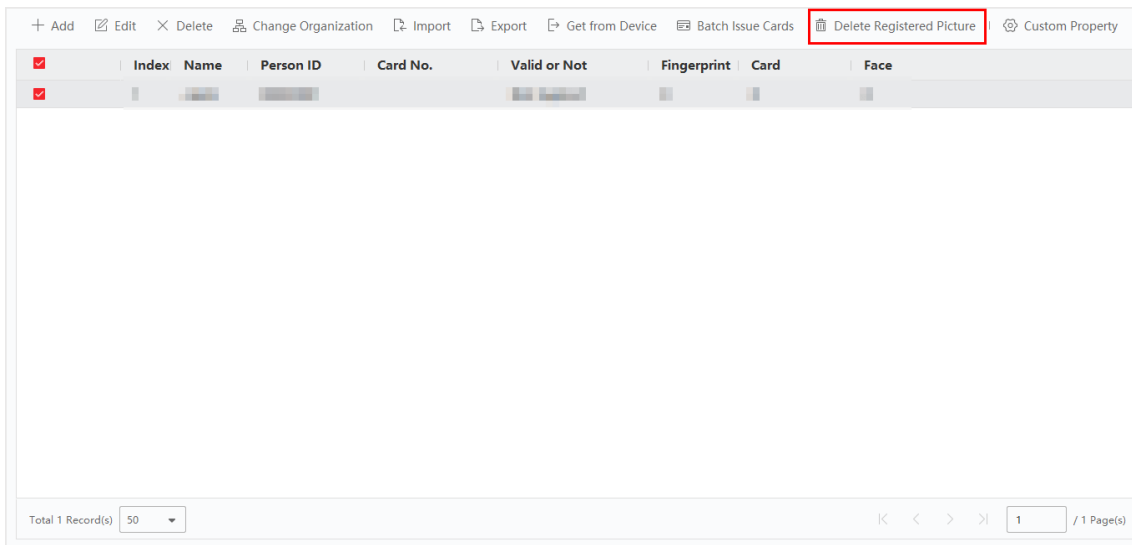


Figure 14-2 Delete Registered Picture

Note

If **Save Pictures in Structure Data Format** is enabled, the **Delete Registered Picture** button will be added to the **Person** page. In general, the registered face picture will be deleted automatically once the person's information is applied to the device. By double clicking the person, the **Edit Person** window will pop up, and you can check whether the registered face picture has been deleted. If not, you can select this person and click **Delete Registered Picture** to delete the picture manually.

14.2.2 Issue a Card to One Person

When adding a person, you can issue a card to him/her as a credential to access the door(s). Before issuing a card to one person, you need to set the card issuing mode to get the card number. Except for manually entering the card number, the client also provides the other two modes for reading the card number: by local mode (via card enrollment station) or by remote mode (via the card reader of the access control device).

Note

Up to five cards can be issued to one person.

Issue a Card by Entering Card Number

When there is no device (card enrollment station/card reader) available to read card number, you


can issue a card by manually entering card number.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add** to enter Add Person panel.

Note

Enter the person's basic information first. For details about configuring person's basic information, refer to [***Configure Basic Information***](#).

3. In the **Credential** → **Card** area, click .
4. Manually enter the card number in the Add page.
5. Click **Add**.
The card will be issued to the person.

Issue a Card by Local Mode


If a card enrollment station is available, you can issue a card by local mode. To read the card number, you should connect the card enrollment station to the PC running the client by USB interface or COM, and place the card on the card enrollment station.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add** to enter Add Person panel.

Note

Enter the person's basic information first. For details about configuring person's basic information, refer to [***Configure Basic Information***](#).

3. In the **Credential** → **Card** area, click .
4. Click **Settings** to enter the Settings page.
5. Select **Local** as the card issuing mode.
6. Set other related parameters.

Card Enrollment Station

Select a model of card enrollment station from the drop-down list. You can connect the card enrollment station to the PC, and transfer the basic information about the added person between the two devices through USB.

Card Type

Select the card type as EM card or Mifare card according to the actual card type.

Buzzing

Enable or disable the buzzing when the card number is read successfully.

Card No. Type

Select the type of the card number according to actual needs.

M1 Card Encryption

If the card is M1 card, then you can enable the M1 Card Encryption function and select the sector of the card to encrypt.

7. Click **OK** to confirm the operation.
8. Place the card on the card enrollment station, and click **Read** to get the card number.
The card number will display in the Card No. field automatically.
9. Click **Add**.
The card will be issued to the person.

Issue a Card by Remote Mode


Except for issuing a card by local mode, you can also swipe the card on the card reader of the added access control device to get the card number. This is applicable when the client and the persons need issuing cards are not in the same location. For example, you can issue cards for employees in the branch company by remote mode via the client.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add** to enter Add Person panel.

Note

Enter the person's basic information first. For details about configuring person's basic information, refer to [***Configure Basic Information***](#).

3. In the **Credential** → **Card** area, click .
4. Click **Settings** to enter the Settings page.
5. Select **Card Reader** as the card issuing mode.
6. Select an access control device added in the client.
7. Select an added access control device or the enrollment station from the drop-down list.

Note

- If you select access control device, make sure you have armed the devices.
 - If you select the enrollment station, you should click **Login** to set related parameters of the device including IP address, port No., user name, and password. Also, you should check RF card type(s) as needed.
-

8. Click **OK** to confirm the operation.
9. Place the card on the card reader, and click **Read** to get the card number.
The card number will display in the Card No. field automatically.

10. Click **Add**.

The card will be issued to the person.

14.2.3 Upload a Face Photo from Local PC

When adding person, you can upload a face photo stored in local PC to the client as the person's profile.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

Note

Enter the person's basic information first. For details about configuring person's basic information, refer to [***Configure Basic Information***](#).

3. Click **Add Face** in the Basic Information panel.
4. Select **Upload**.
5. Select a picture from the PC running the client.

Note

The picture should be in JPG or JPEG format and smaller than 200 KB.

6. Optional: Enable **Verify by Device** to check whether the facial recognition device managed in the client can recognize the face in the photo.

Note

This function is hidden or shown according to the device capacity.

7. Confirm to add the person.
 - Click **Add** to add the person and close the Add Person window.
 - Click **Add and New** to add the person and continue to add other persons .

14.2.4 Take a Photo via Client

When adding a person, you can take a photo of a person by the client integrated camera, USB camera or enrollment station, and set this photo as the person's profile.

Before You Start

Make sure the PC running the client meets one of the following conditions:

- The client has a camera.
- You have connected USB camera to the PC.
- You have connected enrollment station to the PC by USB interface.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add** to enter Add Person window.

Note

Enter the person's basic information first. For details, refer to [**Configure Basic Information**](#).

3. Click **Add Face** in the Basic Information area.
4. Select **Take Photo** to enter Take Photo window.
5. Click ▾ to select the integrated camera or enrollment station from the drop-down list.
6. Optional: Enable **Verify by Device** to check whether the captured face photo can meet the uploading requirements.

Note

This function is hidden or shown according to the device capacity.



7. Take a photo.
 - 1) Face to the camera and make sure your face is in the middle of the collecting window.
 - 2) Click  to capture a face photo.
 - 3) Optional: Click  to capture again.
 - 4) Click **OK** to save the captured photo.

Figure 14-3 Take a Photo via Client

8. Confirm to add the person.
 - Click **Add** to add the person and close the Add Person window.
 - Click **Add and New** to add the person and continue to add other persons.

14.2.5 Collect Face via Access Control Device

When adding person, you can collect the person's face via access control device added to the client which supports facial recognition function.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

 **Note**

Enter the person's basic information first. For details about configuring person's basic information, refer to **Configure Basic Information**.

3. Click **Add Face** in the Basic Information panel.
 4. Select **Remote Collection**.
 5. Select an added access control device or the enrollment station from the drop-down list.
-

 **Note**

If you select the enrollment station, you should click **Login** to set related parameters of the device including IP address, port No., user name, and password. Also, you can check **Face Anti-Spoofing** and select the liveness level as Low, Medium, or High.


Face Anti-Spoofing

If you check this function, then the device can detect whether the face to be collected is an authentic one.

6. Optional: Click **Card Reader**, select the card reader ID, click **OK**.
-

 **Note**


This function should be supported by device.

7. Collect face.
 - 1) Face to the camera of the selected access control device and make sure your face is in the middle of the collecting window.
 - 2) Click  to capture a photo.
 - 3) Click **OK** to save the captured photo.
8. Confirm to add the person.
 - Click **Add** to add the person and close the Add Person window.
 - Click **Add and New** to add the person and continue to add other persons .

14.2.10 Configure Access Control Information

When adding a person, you can set her/his access control information, such as binding an access control group with the person, configuring PIN code, setting the person as a visitor, a blocklist person, or a super user, etc.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.
3. In the **Access Control** area, click  to select access group(s) for the person.

Note

For details, refer to **Set Access Group to Assign Access Authorization to Persons.**

The screenshot shows a configuration window titled 'Access Control'. At the top, there is a dropdown menu labeled 'Access Group'. Below it is a 'PIN Code' input field with a 'Generate' button to its right. Underneath are five checkboxes: 'Super User', 'Extended Door Open Time', 'Add to Blocklist', 'Mark as Visitor', and 'Device Operator'.

Figure 14-4 Configure Access Control Information

4. Set a unique PIN code for the person which can be used for access authentication.
 - Manually enter a PIN code containing 4 to 8 digits.

Note

Persons' PIN codes cannot be repeated.

- Click **Generate** to randomly generate an unrepeated PIN code of 6 digits.

Note

If there are repeated PIN codes, a prompt will pop up on the client. The admin can generate a new PIN code to replace the repeated PIN code and notify related persons.

5. Check the person's operation permissions.

Super User

If the person is set as a super user, he/she will have authorization to access all the doors/floors and will be exempted from remaining closed restrictions, all anti-passback rules, and first person authorization.

Extended Door Open Time

Use this function for persons with reduced mobility. When accessing the door, the person will have more time than others to pass through doors.

For details about setting the door's open duration, refer to **Configure Parameters for Door/Elevator.**

Add to Blocklist

Add the person to the blacklist and when the person tries to access doors/floors, an event will be triggered and sent to the client to notify the security personnel.

Mark as Visitor

If the person is a visitor, you should set the her/his valid times for visit.

Note

The valid times for visit is between 1 and 100. You can also check **No Limit**, then there are no limited times for the visitor to access doors/floors.

Device Operator

For person with device operator role, he/she is authorized to operate on the access control devices.

Note

The Super User, Extended Door Open Time, Add to Blocklist, and Mark as Visitor functions cannot be enabled concurrently. For example, if one person is set as super user, you cannot enable extended door open time for her/him, add her/him to the blacklist, or set her/him as visitor.

6. Confirm to add the person.
 - Click **Add** to add the person and close the Add Person window.
 - Click **Add and New** to add the person and continue to add other persons.

14.2.11 Customize Person Information

You can customize the person properties which are not pre-defined in the client according to actual needs, e.g., place of birth. After customizing, when add a person, you can enter the custom information to make the person information complete.

Steps

1. Enter **Person** module.
2. Set the fields of custom information.
 - 1) Click **Custom Property**.
 - 2) Click **Add** to add a new property.
 - 3) Enter the property name.
 - 4) Click **OK**.
3. Set the custom information when adding a person.
 - 1) Select an organization in the organization list to add the person and click **Add**.

Note

Enter the person's basic information first. For details about configuring person's basic information, refer to **Configure Basic Information**.

- 2) In the **Custom Information** panel, enter the person information.
- 3) Click **Add** to add the person and close the Add Person window, or click **Add and New** to add the person and continue to add other persons.

14.2.12 Configure Resident Information

If the person is resident, for video intercom purpose, you need to set the room number for her/him and bind an indoor station. After bound, you can call this person by calling the indoor station and perform video intercom with her/him.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

Note

Enter the person's basic information first. For details about configuring person's basic information, refer to [***Configure Basic Information***](#).

3. In the **Resident Information** panel, select the indoor station to bind it to the person.

Note

If you select **Analog Indoor Station**, the **Door Station** field will display and you are required to select the door station to communicate with the analog indoor station.

4. Enter the floor No. and room No. of the person.
5. Confirm to add the person.
 - Click **Add** to add the person and close the Add Person window.
 - Click **Add and New** to add the person and continue to add other persons.

14.2.13 Configure Additional Information

When adding person, you can configure the additional information for the person, such as person's identity type, identity No., country, etc., according to actual needs.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

Note

Enter the person's basic information first. For details about configuring person's basic information, refer to [***Configure Basic Information***](#).

3. In the **Additional Information** panel, enter the additional information of the person, including person's ID type, ID No., job title, etc., according to actual needs.
-

4. Confirm to add the person.
 - Click **Add** to add the person and close the Add Person window.
 - Click **Add and New** to add the person and continue to add other persons .

14.3 Import and Export Person Identify Information

You can import the information and pictures of multiple persons to the client software in a batch. Meanwhile, you can also export the person information and pictures and save them in your PC.

14.3.1 Import Person Information


You can enter the information of multiple persons in a predefined template (CSV/Excel file) to import the information to the client in a batch.

Steps

1. Enter the Person module.
2. Select an added organization in the list, or click **Add** in the upper-left corner to add an organization and then select it.
3. Click **Import** to open the Import panel.
4. Select **Person Information** as the importing mode.
5. Click **Download Template for Importing Person** to download the template.
6. Enter the person information in the downloaded template.

Note

- If the person has multiple cards, separate the card No. with semicolon.
- Items with asterisk are required.
- By default, the Hire Date is the current date.

-
7. Click  to select the CSV/Excel file with person information from local PC.
 8. Click **Import** to start importing.

Note

- If a person No. already exists in the client's database, delete the existing information before importing.
 - You can import information of no more than 2,000 persons.
-

14.3.2 Import Person Pictures

After importing face pictures for the added persons to the client, the persons in the pictures can be identified by an added face recognition terminal. You can either import person pictures one by

one, or import multiple pictures at a time according to your need.

Before You Start

Be sure to have imported person information to the client beforehand.

Steps

1. Enter the Person module.
2. Select an added organization in the list, or click **Add** in the upper-left corner to add an organization and then select it.
3. Click **Import** to open the Import panel and check **Face**.
4. Optional: Enable **Verify by Device** to check whether face recognition device managed in the client can recognize the face in the photo.
5. Click **...** to select a face picture file.

Note

- The (folder of) face pictures should be in ZIP format.
- Each picture file should be in JPG format and should be no larger than 200 KB.
- Each picture file should be named as "Person ID_Name". The Person ID should be the same with that of the imported person information.

-
6. Click **Import** to start importing.
The importing progress and result will be displayed.

14.3.3 Export Person Information

You can export the added persons' information to local PC as a CSV/Excel file.

Before You Start

- Make sure you have added persons to an organization.
- Make sure you have enabled the **Export Person Information** function to display the **Export** button. See [Set General Parameters](#) for details.

Steps

1. Enter the Person module.
2. Optional: Select an organization in the list.

Note

All persons' information will be exported if you do not select any organization.

3. Click **Export**.
4. Enter the super user name and password for verification.
The Export panel is displayed.
5. Check **Person Information** as the content to export.
6. Check desired items to export.
7. Click **Export** to save the exported file in CSV/Excel file on your PC.

14.3.4 Export Person Pictures

You can export face picture file of the added persons and save in your PC.

Before You Start

- Make sure you have added persons and their face pictures to an organization.
- Make sure you have enabled the **Export Person Information** function to display the **Export** button. See [Set General Parameters](#) for details.

Steps

1. Enter the Person module.
2. Optional: Select an organization in the list.

Note

All persons' face pictures will be exported if you do not select any organization.

3. Click **Export** on the top menu bar.
4. Enter the super user name and password for verification.
The Export panel is displayed.
5. Check **Face** as the content to export.
6. Click **Export** and set an encryption key to encrypt the exported file.

Note

- The exported file is in ZIP format.
 - The exported face picture is named as "Person ID_Name_0" ("0" is for a full-frontal face).
-

14.4 Get Person Information from Access Control Device

If the access control device has been configured with person information (including person details, fingerprint, and issued card information), you can get the person information from the added device and import them to the client for further operations.

Steps

Note

- If the person name stored in the device is empty, the person name will be filled with the issued card No. after importing to the client.
 - Persons will be **Male** by default.
 - If the card number or person ID (employee ID) stored on the device already exists in the client database, the person with this card number or person ID will not be imported to the client.
-

1. Enter **Person** module.
2. Select an organization to import the persons.

3. Click **Get from Device**.
4. Select an added access control device or the enrollment station from the drop-down list.

Note

If you select the enrollment station, you should click **Login**, and enter IP address, port No., user name and password of the device.

5. Select the **Getting Mode**.

Note

The getting mode varies according to different devices. The access control device supports getting the person information by employee ID. Up to 5 employee IDs can be specified each time.

6. Click **Import** to start importing the person information to the client.

Note

Up to 2,000 persons and 5,000 cards can be imported.

The person information, including person details, person's fingerprint information (if configured), and the linked cards (if configured), will be imported to the selected organization.

14.5 Move Persons to Another Organization

You can move the added persons to another organization if you need.

Before You Start

- Make sure you have added at least two organizations.
- Make sure you have imported person information.

Steps

1. Enter **Person** module.
2. Select an organization in the left panel.
The persons under the organization will be displayed in the right panel.
3. Select the person to move.
4. Click **Change Organization**.
5. Select the organization to move persons to.
6. Click **OK**.

14.6 Issue Cards to Persons in Batch

The client provides a convenient way to issue cards to multiple persons in a batch.



Steps

1. Enter **Person** module.
2. Click **Batch Issue Cards**.
All the added persons with no card issued will be displayed in the right panel.
3. Optional: Enter key words (name or person ID) in the input box to filter the person(s) that need issuing cards.
4. Optional: Click **Settings** to set the card issuing parameters. For details, refer to [Issue a Card to One Person](#).
5. Click **Initialize** to initialize the card enrollment station or card reader to make it ready for issuing cards.
6. Click the **Card No.** column and enter the card number.
 - Place the card on the card enrollment station.
 - Swipe the card on the card reader.
 - Manually enter the card number and press the **Enter** key.
 The person(s) in the list will be issued with card(s).

14.7 Report Card Loss

If the person lost his/her card, you can report the card loss so that the card's related access authorization will be inactive.

Steps

1. Enter **Person** module.
2. Select the person you want to report card loss for and click **Edit** to open the Edit Person window.
3. In the **Credential** → **Card** panel, click  on the added card to set this card as lost card.
After reporting card loss, the access authorization of this card will be invalid and inactive. Other person who gets this card cannot access the doors by swiping this lost card.
4. Optional: If the lost card is found, you can click  to cancel the loss.
After cancelling card loss, the access authorization of the person will be valid and active.
5. If the lost card is added in one access group and the access group is applied to the device already, after reporting card loss or cancelling card loss, a window will pop up to notify you to apply the changes to the device. After applying to device, these changes can take effect on the device.

14.8 View Resource Statistics

After applying persons and access control credentials (including faces, cards, and fingerprints) to device, you can view resource statistics on client and on device to know whether the resources

have been successfully applied.

You have applied persons and credentials to device. For details, refer to **Set Access Group to Assign Access Authorization to Persons**.

Click **Person Management** → **Resource Statistics** to enter Resource Statistics window.

Figure 14-5 Overview on Client

In **Overview on Device** area, select a device from drop-down list, and click **Counting** to view device resources including persons, faces, cards, and fingerprints. By comparing resources on client and that on device, you can know whether the client resources have been applied to device.

Figure 14-6 Client Resources Applied to Device

Note

This function should be supported by device. If the device does not support face or fingerprint, a prompt will pop up on the bottom right corner of the PC desktop.

Chapter 15 Access Control

The Access Control module is applicable to access control devices and video intercom device. It provides multiple functionalities, including access group configuration, video intercom, and other advanced functions.

Note

For the user with access control module permissions, the user can enter the Access Control module and configure the access control settings. For setting the user permission of Access Control module, refer to [***Add User***](#).

15.2 Configure Schedule and Template

You can configure the template including holiday and week schedule. After setting the template, you can adopt the configured template to access groups when setting the access groups, so that the access group will take effect in the time durations of the template.

Note

For access group settings, refer to [***Set Access Group to Assign Access Authorization to Persons***](#).

15.2.1 Add Holiday

You can create holidays and set the days in the holidays, including start date, end date, and holiday duration in one day.

Steps

Note

You can add up to 64 holidays in the software system.

1. Click **Access Control** → **Schedule** → **Holiday** to enter the Holiday page.
 2. Click **Add** on the left panel.
 3. Create a name for the holiday.
 4. Optional: Enter the descriptions or some notifications of this holiday in the Remark box.
 5. Add a holiday period to the holiday list and configure the holiday duration.
-






Note

Up to 16 holiday periods can be added to one holiday.

- 1) Click **Add** in the Holiday List field.
- 2) Drag the cursor to draw the time duration, which means in that duration of time, the configured access group is activated.

 **Note**

Up to 8 time durations can be set to one holiday period.

- 3) Optional: Perform the following operations to edit the time durations.
 - Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to .
 - Click the time duration and directly edit the start/end time in the appeared dialog.
 - Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to .
 - 4) Optional: Select the time duration(s) that need to be deleted, and then click  in the Operation column to delete the selected time duration(s).
 - 5) Optional: Click  in the Operation column to clear all the time duration(s) in the time bar.
 - 6) Optional: Click  in the Operation column to delete this added holiday period from the holiday list.
6. Click **Save**.

15.2.2 Add Template

Template includes week schedule and holiday. You can set week schedule and assign the time duration of access authorization for different person or group. You can also select the added holiday(s) for the template.

Steps

 **Note**

You can add up to 255 templates in the software system.

1. Click **Access Control** → **Schedule** → **Template** to enter the Template page.

 **Note**

There are two default templates: All-Day Authorized and All-Day Denied, and they cannot be edited or deleted.

All-Day Authorized

The access authorization is valid in each day of the week and it has no holiday.

All-Day Denied



The access authorization is invalid in each day of the week and it has no holiday.

2. Click **Add** on the left panel to create a new template.

3. Create a name for the template.
4. Enter the descriptions or some notification of this template in the Remark box.
5. Edit the week schedule to apply it to the template.
 - 1) Click **Week Schedule** tab on the lower panel.
 - 2) Select a day of the week and draw time duration(s) on the timeline bar.

 **Note**

Up to 8 time duration(s) can be set for each day in the week schedule.

- 3) Optional: Perform the following operations to edit the time durations.
 - Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to .
 - Click the time duration and directly edit the start/end time in the appeared dialog.
 - Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to .
 - 4) Repeat the two steps above to draw more time durations on the other days of the week.
6. Add a holiday to apply it to the template.


 **Note**

Up to 4 holidays can be added to one template.

- 1) Click **Holiday** tab.
- 2) Select a holiday in the left list and it will be added to the selected list on the right panel.
- 3) Optional: Click **Add** to add a new holiday.

 **Note**

For details about adding a holiday, refer to [***Add Holiday.***](#)

- 4) Optional: Select a selected holiday in the right list and click  to remove the selected one, or click **Clear** to clear all the selected holiday(s) in the right list.
7. Click **Save** to save the settings and finish adding the template.

15.3 Set Access Group to Assign Access Authorization to Persons

After adding the person and configuring the person's credentials, you can create the access groups to define which person(s) can get access to which door(s) and then apply the access group to the access control device to take effect.

Before You Start

- Add person to the client.
- Add access control device to the client and group access points. For details, refer to [***Group Management.***](#)
- Add template.

Steps

When the access group settings are changed, you need to apply the access groups to the devices again to take effect. The access group changes include changes of template, access group settings, person's access group settings, and related person details (including card number, fingerprint, face picture, linkage between card number and fingerprint, linkage between card number and fingerprint, card password, card effective period, etc).

1. Click **Access Control** → **Authorization** → **Access Group** to enter the Access Group interface.
2. Click **Add** to open the Add window.
3. In the **Name** text field, create a name for the access group as you want.
4. Select a template for the access group.

 **Note**

You should configure the template before access group settings. Refer to [Configure Schedule and Template](#) for details.

5. In the left list of the Select Person field, select person(s) to assign access authority.
6. In the left list of the Select Access Point field, select door(s), door station(s) or floor(s) for the selected persons to access.
7. Click **Save**.

You can view the selected person(s) and the selected access point(s) on the right side of the interface.

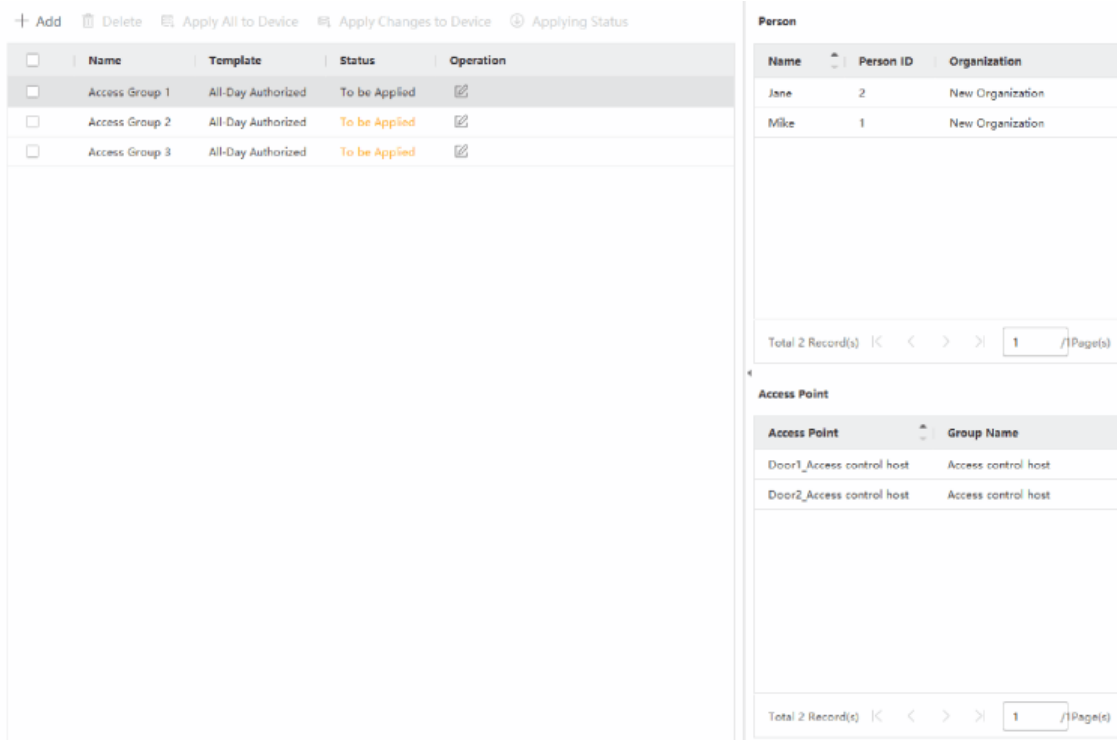


Figure 15-2 Display the Selected Person(s) and Access Point(s)

8. After adding the access groups, you need to apply them to the access control device to take effect.
 - 1) Select the access group(s) to apply to the access control device.
 - 2) Click **Apply All to Devices** start applying all the selected access group(s) to the access control device or door station.
 - 3) Click **Apply All to Devices** or **Apply Changes to Devices**.

Apply All to Devices

This operation will clear all the existed access groups of the selected devices and then apply the new access group to the device.

Apply Changes to Devices


This operation will not clear the existed access groups of the selected devices and only apply the changed part of the selected access group(s) to the device(s).

- 4) View the applying status in the Status column or click **Applying Status** to view all the applied access group(s).

Note

You can check **Display Failure Only** to filter the applying results.

The selected persons in the applied access groups will have the authorization to enter/exit the selected doors/door stations with their linked card(s) or fingerprints.

9. Optional: Click  to edit the access group if necessary.

Note

If you change the persons' access information or other related information, you will view the prompt **Access Group to Be Applied** on the right corner of the client.

You can click the prompt to apply the changed data to the device. You can select either **Apply Now** or **Apply Later**.

15.4 Search Access Group

After setting access group and assigning access authority to persons, you can search the access group that the person belongs to and view other related information including credential No.,

credential type, applying status, etc.

Note

Make sure you have set access group to assign access authorization to designed persons and applied it. For details, refer to **Set Access Group to Assign Access Authorization to Persons**.

Click **Access Control** → **Authorization** → **Search**. Select a device name, and set search condition (including person name and applying status, optional), and then click **Search**.

You can view the access group that the searched person belongs to and other information including the credential type, door name, credential No., applying status, remark, etc.

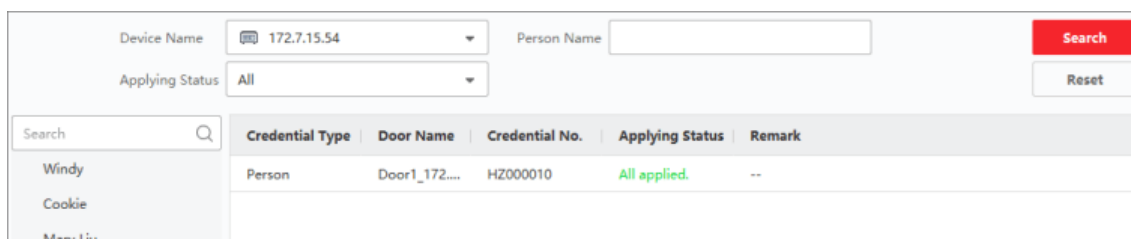



Figure 15-3 Search Access Group

15.5 Configure Advanced Functions

You can configure the advanced functions of access control to meet some special requirements in different scene, such as multi-factor authentication, anti-passback, etc.

Note

- For the card related functions(the type of access control card/multi-factor authentication), only the card(s) with access group applied will be listed when adding cards.
- The advanced functions should be supported by the device.
- Hover the cursor on the Advanced Function, and then Click  to customize the advanced function(s) to be displayed.

15.5.1 Configure Device Parameters

After adding the access control device, you can configure the parameters of access control device (access controller), access control points (door or floor), alarm inputs, alarm outputs, card readers and lane controller.

Configure Parameters for Access Control Device

After adding the access control device, you can configure its parameters, including overlaying user

information on picture, uploading pictures after capturing, saving captured pictures, etc.


Before You Start

Add access control device to the client.

Steps

1. Click **Access Control** → **Advanced Function** → **Device Parameter**.

Note

If you can not find Device Parameter in the Advanced Function list, hover the cursor on the Advanced Function, and then Click  to select the Device Parameter to be displayed.

2. Select an access device to show its parameters on the right page.
3. Turn the switch to ON to enable the corresponding functions.

Note

- The displayed parameters may vary for different access control devices.
 - Some of the following parameters are not listed in the Basic Information page, click **More** to edit the parameters.
-

RS-485 Comm. Redundancy

You should enable this function if you wire the RS-485 card reader to the access control device redundantly.

Display Detected Face

Display face picture when authenticating.

Display Card Number

Display the card information when authenticating.

Display Person Information

Display the person information when authenticating.

Overlay Person Info. on Picture

Display the person information on the captured picture.

Voice Prompt

If you enable this function, the voice prompt is enabled in the device. You can hear the voice prompt when operating in the device.

Upload Pic. After Linked Capture

Upload the pictures captured by linked camera to the system automatically.

Save Pic. After Linked Capture

If you enable this function, you can save the picture captured by linked camera to the device.

Press Key to Enter Card Number

If you enable this function, you can input the card No. by pressing the key.

Wi-Fi Probe

If you enable this function, the device can probe the surrounding communication devices' MAC address and upload the MAC address to the system. If the MAC address match the specified MAC address, the system can trigger some linkage actions.

3G/4G

If you enable this function, the device can communicate in 3G/4G network.

NFC Anti-Cloning

If you enable this function, you cannot use the cloned card for authentication and further enhance security.

4. Click **OK**.
5. Optional: Click **Copy to**, and then select the access control device(s) to copy the parameters in the page to the selected device(s).


Configure Parameters for Door/Elevator

After adding the access control device, you can configure its access point (door or floor) parameters.

Before You Start

Add access control device to the client.

Steps

1. Click **Access Control** → **Advanced Function** → **Device Parameter**.
2. Select an access control device on the left panel, and then click  to show the doors or floors of the selected device.
3. Select a door or floor to show its parameters on the right page.
4. Edit the door or floor parameters.

Note

- The displayed parameters may vary for different access control devices.
 - Some of the following parameters are not listed in the Basic Information page, click **More** to edit the parameters.
-

Name

Edit the card reader name as desired.

Door Contact

You can set the door sensor as remaining closed or remaining open. Usually, it is remaining closed.

Exit Button Type

You can set the exit button as remaining closed or remaining open. Usually, it is remaining open.

Door Locked Time

After swiping the normal card and relay action, the timer for locking the door starts working.

Extended Open Duration

The door contact can be enabled with appropriate delay after person with extended access needs swipes her/his card.

Door Left Open Timeout Alarm

The alarm can be triggered if the door has not been closed in a configured time period. If it is set as 0, no alarm will be triggered.

Lock Door when Door Closed

The door can be locked once it is closed even if the **Door Locked Time** is not reached.

Duress Code

The door can open by inputting the duress code when there is duress. At the same time, the client can report the duress event.

Super Password

The specific person can open the door by inputting the super password.

Dismiss Code

Create a dismiss code which can be used to stop the buzzer of the card reader (by entering the dismiss code on the keypad).

Note

- The duress code, super code, and dismiss code should be different.
- The duress code, super password, and the dismiss code should be different from the authentication password.
- The length of duress code, super password, and the dismiss code is according the device, usually it should contains 4 to 8 digits.

5. Click **OK**.

6. Optional: Click **Copy to** , and then select the door/floor(s) to copy the parameters in the page to the selected doors/floor(s).

 **Note**

The door or floor's status duration settings will be copied to the selected door/floor(s) as well.


Configure Parameters for Card Reader

After adding the access control device, you can configure its card reader parameters.

Before You Start

Add access control device to the client.

Steps

1. Click **Access Control** → **Advanced Function** → **Device Parameter**.
2. In the device list on the left, click  to expand the door, select a card reader and you can edit the card reader's parameters on the right.
3. Edit the card reader basic parameters in the Basic Information page.

 **Note**

- The displayed parameters may vary for different access control devices. There are part of parameters listed as follows. Refer to the user manual of the device for more details.
 - Some of the following parameters are not listed in the Basic Information page, click **More** to edit the parameters.
-

Name

Edit the card reader name as desired.

OK LED Polarity/Error LED Polarity/Buzzer Polarity

Set OK LED Polarity/Error LED Polarity/Buzzer LED Polarity of main board according to the card reader parameters. Generally, adopts the default settings.

Minimum Card Swiping Interval

If the interval between card swiping of the same card is less than the set value, the card swiping is invalid. You can set it as 0 to 255.

Max. Interval When Entering PWD

When you inputting the password on the card reader, if the interval between pressing two digits is larger than the set value, the digits you pressed before will be cleared automatically.

Alarm of Max. Failed Attempts

Enable to report alarm when the card reading attempts reach the set value.

Max. Times of Card Failure

Set the max. failure attempts of reading card.

Tampering Detection

Enable the anti-tamper detection for the card reader.

Communicate with Controller Every

When the access control device cannot connect with the card reader for longer than the set time, the card reader will turn offline automatically.

Buzzing Time

Set the card reader buzzing time. The available time ranges from 0 to 5,999s. 0 represents continuous buzzing.

Card Reader Type/Card Reader Description

Get card reader type and description. They are read-only.

Fingerprint Recognition Level

Select the fingerprint recognition level in the drop-down list.

Default Card Reader Authentication Mode

View the default card reader authentication mode.

Fingerprint Capacity

View the maximum number of available fingerprints.

Existing Fingerprint Number

View the number of existed fingerprints in the device.

Score

The device will score the captured picture according to the yaw angle, pitch angle, and pupillary distance. If the score is less than the configured value, face recognition will be failed.

Face Recognition Timeout Value

If the recognition time is more than the configured time, the device will remind you.

Face Recognition Interval

The time interval between two continuous face recognitions when authenticating. By default, it is 2s.

Face 1:1 Matching Threshold

Set the matching threshold when authenticating via 1:1 matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate when authentication.

1:N Security Level

Set the matching security level when authenticating via 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate when authentication.

Live Face Detection

Enable or disable the live face detection function. If enabling the function, the device can recognize whether the person is a live one or not.

Live Face Detection Security Level

After enabling Live Face Detection function, you can set the matching security level when performing live face authentication.

Max. Failed Attempts for Face Auth.

Set the maximum live face detection failed attempts. The system will lock the user's face for 5 minutes if the live face detection is failed for more than the configured attempts. The same user cannot authenticate via the fake face within 5 minutes. Within the 5 minutes, the user can authenticate via the real face twice continuously to unlock.

Lock Authentication Failed Face

After enabling the Live Face Detection function, the system will lock the user's face for 5 minutes if the live face detection is failed for more than the configured attempts. The same user cannot authenticate via the fake face within 5 minutes. Within the 5 minutes, the user can authenticate via the real face twice continuously to unlock.

Application Mode

You can select indoor or others application modes according to actual environment.

4. Click **OK**.

5. Optional: Click **Copy to**, and then select the card reader(s) to copy the parameters in the page to the selected card reader(s).

Configure Parameters for Alarm Input

After adding the access control device, you can configure the parameters for its alarm inputs.


Before You Start

Add access control device to the client, and make sure the device supports alarm input.

Steps

Note

If the alarm input is armed, you cannot edit its parameters. Disarm it first.

1. Click **Access Control** → **Advanced Function** → **Device Parameter** .
2. In the device list on the left, click  to expand the door, select an alarm input and you can edit the alarm input's parameters on the right.
3. Set the alarm input parameters.

Name

Edit the alarm input name as desired.

Detector Type

The detector type of the alarm input.

Zone Type

Set the zone type for the alarm input.

Sensitivity

Only when the duration of signal detected by the detector reaches the setting time, the alarm input is triggered. For example, you have set the sensitivity as 10ms, only when the duration of signal detected by the detector reach 10ms, this alarm input is triggered.

Trigger Alarm Output

Select the alarm output(s) to be triggered.

4. Click **OK**.
5. Optional: Click the switch on the upper-right corner to arm or disarm the alarm input.


Configure Parameters for Alarm Output

After adding the access control device, if the device links to alarm outputs, you can configure the parameters.

Before You Start

Add access control device to the client, and make sure the device supports alarm output.

Steps

1. Click **Access Control** → **Advanced Function** → **Device Parameter** to enter access control parameter configuration page.
2. In the device list on the left, click  to expand the door, select an alarm input and you can edit the alarm input's parameters on the right.
3. Set the alarm output parameters.

Name

Edit the card reader name as desired.

Alarm Output Active Time

How long the alarm output will last after triggered.

4. Click **OK**.
5. Optional: Set the switch on the upper right corner to **ON** to trigger the alarm output.

Configure Parameters for Lane Controller

After adding the lane controller to the client, you can configure its parameters for passing through the lane.

Before You Start

Add access control device to the client.

Steps

1. Click **Access Control** → **Advanced Function** → **Device Parameter** to enter Parameter Settings page.
2. In the device list on the left, select a lane controller and you can edit the lane controller's parameters on the right.
3. Edit the parameters.

Passing Mode

Select the controller which will control the barrier status of the device.

- If you select **According to Lane Controller's DIP Settings**, the device will follow the lane controller's DIP settings to control the barrier. The settings on the software will be invalid.
- If you select **According to Main Controller's Settings**, the device will follow the settings of the software to control the barrier. The DIP settings of the lane controller will be invalid.

Free Passing Authentication

If you enable this function, when both entrance and exit's barrier mode is Remain Open, the pedestrians should authenticate each time passing through the lane. Or an alarm will be triggered.

Opening/Closing Barrier Speed

Set the barrier's opening and closing speed. You can select from 1 to 10. The greater the value, the faster the speed.

Note

The recommended value is 6.

Audible Prompt Duration

Set how long the audio will last, which is played when an alarm is triggered .

Note

0 refers to the alarm audio will be played until the alarm is ended.

Temperature Unit

Select the temperature unit that displayed in the device status.

4. Click **OK**.

15.5.2 Configure Remaining Unlocked/Locked

You can set the status of the door as unlocked or locked and set the elevator controller as free and controlled. For example, you can set the door remaining locked in the holiday, and set the door remaining unlocked in the specified period of the work day.

Before You Start

Add the access control devices to the system.

Steps

1. Click **Access Control** → **Advanced Function** → **Remain Locked/Unlocked** to enter the Remain Locked/Unlocked page.
2. Select the door or elevator controller that need to be configured on the left panel.
3. To set the door or elevator controller status during the work day, click the **Week Schedule** and perform the following operations.
 - 1) For door, click **Remain Unlocked**, **Remain Locked**, **Inductive Mode**, or **Barrier-Free Mode**.



Note

- **Inductive Mode:** The door opening and closing is triggered by infrared induction of human body.
 - **Barrier-Free Mode:** When a large number of people need to pass the door, the door will remain open (without frequent authentication) if the person and ID comparison succeeds. Only when the person and ID comparison fails, the door will be closed.
 - Inductive mode and barrier-free mode should be supported by device.
-

- 2) For elevator controller, click **Free** or **Controlled**.
 - 3) Drag the cursor to draw the time duration, which means in that duration of time, the configured access group is activated.
-

Note

Up to 8 time durations can be set to each day in the week schedule.

- 4) Optional: Perform the following operations to edit the time durations.
 - Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to .
 - Click the time duration and directly edit the start/end time in the appeared dialog.
 - Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to .
- 5) Click **Save**.

Related Operations

Copy to Whole Week Select one duration on the time bar, click **Copy to Whole Week** to copy all the duration settings on this time bar to other week days.






Delete Selected Select one duration on the time bar, click **Delete Selected** to delete this duration.

Clear Click **Clear** to clear all the duration settings in the week schedule.

4. To set the door status during the holiday, click the **Holiday** and perform the following operations.
 - 1) Click **Remain Unlocked**, **Remain Locked**, **Inductive Mode**, or **Barrier-Free Mode**.
 - 2) Click **Add**.
 - 3) Enter the start date and end date.
 - 4) Drag the cursor to draw the time duration, which means in that duration of time, the configured access group is activated.
-

 **Note**

Up to 8 time durations can be set to one holiday period.

- 5) Perform the following operations to edit the time durations.
 - Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to .
 - Click the time duration and directly edit the start/end time in the appeared dialog.
 - Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to .
 - 6) Optional: Select the time duration(s) that need to be deleted, and then click  in the Operation column to delete the selected time duration(s).
 - 7) Optional: Click  in the Operation column to clear all the time duration(s) in the time bar.
 - 8) Optional: Click  in the Operation column to delete this added holiday period from the holiday list.
 - 9) Click **Save**.
5. Optional: Click **Copy to** to copy the door status settings of this door to other door(s).

15.5.3 Configure Multi-Factor Authentication

You can manage the persons by group and set the authentication for multiple persons of one access control point (door).

Before You Start

Set access group and apply the access group to the access control device. For details, refer to [**Set Access Group to Assign Access Authorization to Persons**](#).

Perform this task when you want to set authentications for multiple cards of one access control point (door).

Steps

1. Click **Access Control** → **Advanced Function** → **Multi-Factor Auth**.
2. Select an access control device in device list on the left panel.
3. Add a person/card group for the access control device.
 - 1) Click **Add** on the right panel.
 - 2) Create a name for the group as desired.
 - 3) Specify the start time and end time of the effective period for the person/card group.
 - 4) Select members(s) and card(s) in the Available list, and the selected member(s) and card(s) will be added to the Selected list.

 **Note**

Make sure you have issue card to the person.

Make sure you have set access group and apply the access group to the access control device successfully.

- 5) Click **Save**.
 - 6) Optional: Select the person/card group(s), and then click **Delete** to delete it(them).
 - 7) Optional: Select the person/card group(s), and then click **Apply** to re-apply access group that failed to be applied previously to the access control device.
 4. Select an access control point (door) of selected device on the left panel.
 5. Enter the maximum interval when entering password.
 6. Add an authentication group for the selected access control point.
 - 1) Click **Add** on the Authentication Groups panel.
 - 2) Select a configured template as the authentication template from the drop-down list.
-

 **Note**

For setting the template, refer to [*Configure Schedule and Template*](#).

- 3) Select the authentication type as **Local Authentication**, **Local Authentication and Remotely Open Door**, or **Local Authentication and Super Password** from the drop-down list.

Local Authentication

Authentication by the access control device.

Local Authentication and Remotely Open Door

Authentication by the access control device and by the client. When the person swipes the card on the device, a window will pop up. You can unlock the door via the client.

Figure 15-4 Remotely Open Door

 **Note**

You can check **Offline Authentication** to enable the super password authentication when the access control device is disconnected with the client.

Local Authentication and Super Password

Authentication by the access control device and by the super password.

- 4) Select the added person/card group in the left list below and it will be added to the Selected list on the right as the authentication group.
 - 5) Click the added authentication group in the right list to set authentication times in the Auth Times column.
-

 **Note**

- The authentication times should be larger than 0 and smaller than the added personnel quantity in the personnel group.
 - The maximum value of authentication times is 16.
-

- 6) Click **Save**.

 **Note**

- For each access control point (door), up to four authentication groups can be added.
 - For the authentication group of which authentication type is **Local Authentication**, up to 8 person/card groups can be added to the authentication group.
 - For the authentication group of which authentication type is **Local Authentication and Super Password** or **Local Authentication and Remotely Open Door**, up to 7 person/card groups can be added to the authentication group.
-

7. Click **Save**.

15.5.4 Configure Custom Wiegand Rule

Based on the knowledge of uploading rule for the third party Wiegand, you can set multiple customized Wiegand rules to communicate between the device and the third party card readers.

Before You Start

Wire the third party card readers to the device.

Steps

 **Note**

- By default, the device disables the custom wiegand function. If the device enables the custom Wiegand function, all wiegand interfaces in the device will use the customized wiegand protocol.
 - Up to 5 custom Wiegands can be set.
 - For details about the custom Wiegand, see [*Custom Wiegand Rule Descriptions*](#).
-

1. Click **Access Control** → **Advanced Function** → **Custom Wiegand** to enter the Custom Wiegand page.
 2. Select a custom Wiegand on the left.
 3. Create a Wiegand name.
-

 **Note**

Up to 32 characters are allowed in the custom Wiegand name.

4. Click **Select Device** to select the access control device for setting the custom wiegand.
 5. Set the parity mode according to the property of the third party card reader.
-

 **Note**

- Up to 80 bits are allowed in the total length.
 - The odd parity start bit, the odd parity length, the even parity start bit and the even parity length range from 1 to 80 bit.
 - The start bit of the card ID, the manufacturer code, the site code, and the OEM should range
-

from 1 to 80 bit.

6. Set output transformation rule.

- 1) Click **Set Rule** to open the Set Output Transformation Rules window.

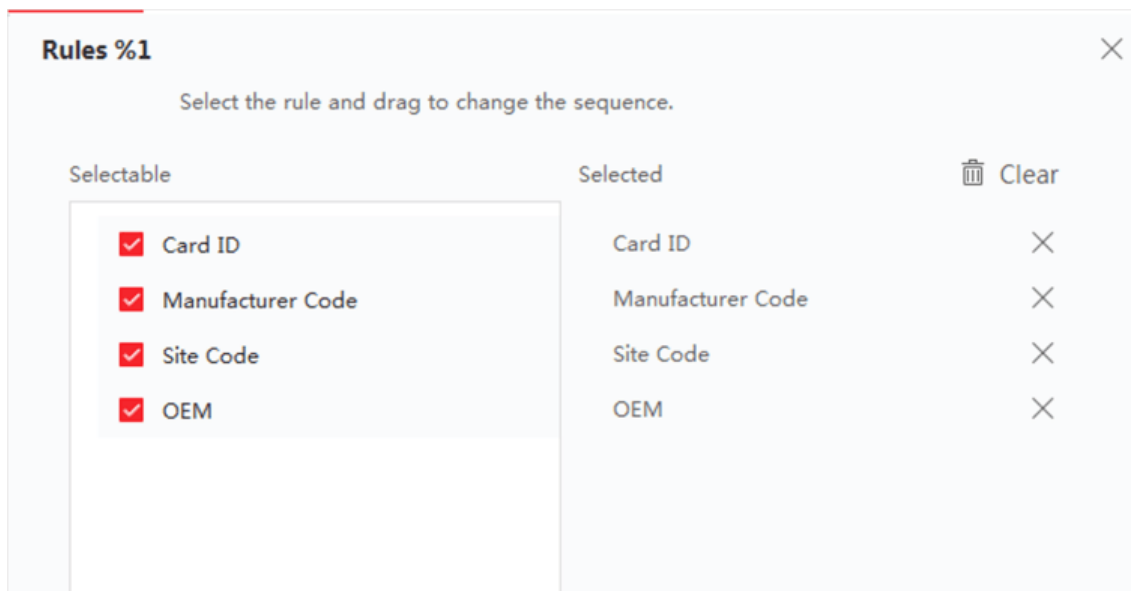


Figure 15-5 Set Output Transformation Rule

- 2) Select rules on the left list.

The selected rules will be added to the right list.

- 3) Optional: Drag the rules to change the rule order.

- 4) Click **OK**.

- 5) In the Custom Wiegand tab, set the rule's start bit, length, and the decimal digit.

7. Click **Save**.

15.5.5 Configure Card Reader Authentication Mode and Schedule

You can set the passing rules for the card reader of the access control device according to your actual needs.

Steps

1. Click **Access Control** → **Advanced Function** → **Authentication** to enter the authentication mode configuration page.
2. Select a card reader on the left to configure.
3. Set card reader authentication mode.
 - 1) Click **Configuration**.

Card Reader Authentication ✕

Select the authentication mode that the card reader should support.

Selectable Mode	Selected Mode	Clear
<input checked="" type="checkbox"/> Card+PIN	Card	✕
<input checked="" type="checkbox"/> Card	Card+PIN	✕
<input checked="" type="checkbox"/> FP	FP	✕
<input type="checkbox"/> FP+PIN	FP+Card	✕
<input type="checkbox"/> FP/Card	Face	✕
<input checked="" type="checkbox"/> FP+Card	Face + Card	✕
<input type="checkbox"/> FP+Card+PIN	Face + FP + Card	✕
<input type="checkbox"/> Face/FP/Card/PIN	Iris	✕
<input type="checkbox"/> Face + FP		
<input type="checkbox"/> Face+PIN		
<input checked="" type="checkbox"/> Face + Card		
<input checked="" type="checkbox"/> Face		
<input checked="" type="checkbox"/> Face + FP + Card		
<input type="checkbox"/> Face + PIN + FP		
<input type="checkbox"/> FP/Face		
<input type="checkbox"/> Card/Face		
<input type="checkbox"/> Card/Face/FP		
<input type="checkbox"/> Card/FP/PIN		
<input checked="" type="checkbox"/> Iris		
<input type="checkbox"/> Face, Fingerprint, Card, Password, or Iris		

OK
Cancel

Figure 15-6 Select Card Reader Authentication Mode

Note

PIN refers to the PIN code set to open the door. Refer to **Configure Access Control Information**.

- 2) Check the modes in the Available Mode list and they will be added to the selected modes list.
- 3) Click **OK**.

After selecting the modes, the selected modes will display as icons with different color.

4. Click the icon to select a card reader authentication mode, and drag the cursor to draw a color bar on the schedule, which means in that period of time, the card reader authentication is valid.
5. Repeat the above step to set other time periods.

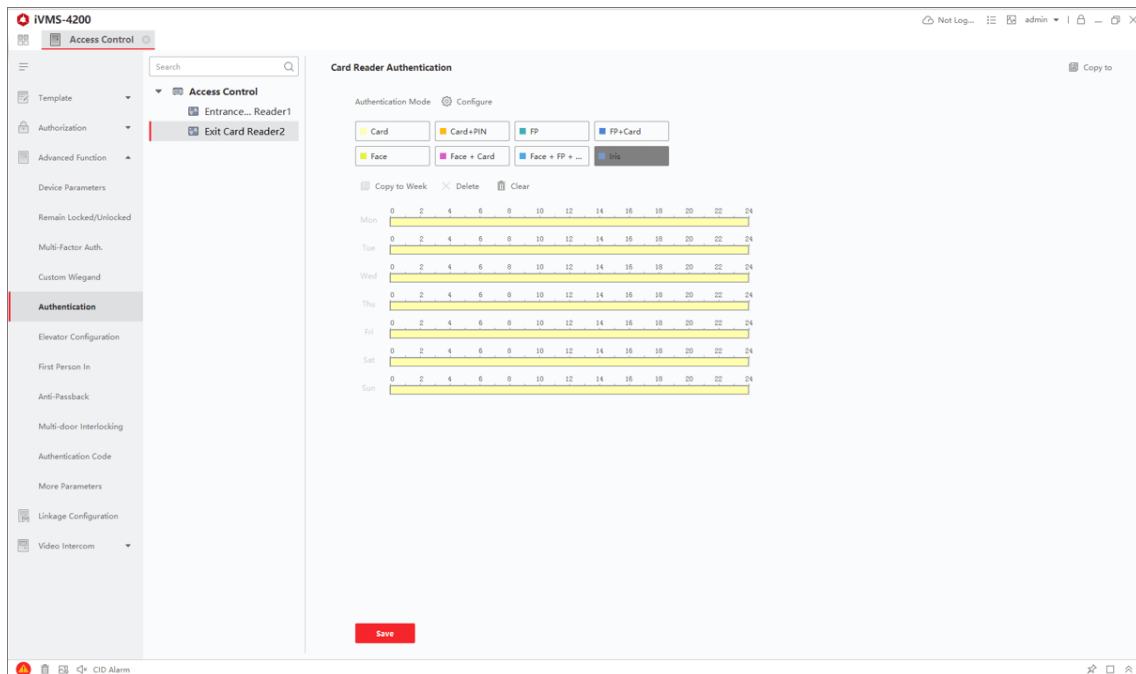


Figure 15-7 Set Authentication Modes for Card Readers

6. Optional: Select a configured day and click **Copy to Week** to copy the same settings to the whole week.
7. Optional: Click **Copy to** to copy the settings to other card readers.
8. Click **Save**.

15.5.6 Configure Person Authentication Mode

You can set the passing rules for person to the specified the access control device according to

your actual needs.

Before You Start

- Add access control device to the client, and make sure the access control device support the function of person authentication.
- Add person and assign access authorization to designed person. For details, refer to [Person Management](#) and [Set Access Group to Assign Access Authorization to Persons](#).

Steps

1. Click **Access Control** → **Advanced Function** → **Authentication**.
2. Select an access control device (support the function of person authentication) on the left panel to enter the person Authentication Mode page.
3. Click **Add** to enter the Add window.
4. Select the person(s) need to be configured on the left panel.
The selected person(s) will be added to the right panel.
5. Select the authentication mode on the drop-down list of **Authentication Mode**.
6. Click **OK**.

Figure 15-8 Set Authentication Modes for Persons

7. Optional: Select person(s) on the Person Authentication mode page, and then click **Apply** to apply the person authentication mode to the device.

Note

Person authentication has higher priority than other authentication mode. When the access control device has been configured person authentication mode, the person should authenticate on this device via person authentication mode.

15.5.8 Configure First Person In

You can set multiple first persons for one access control point. After the first person is authorized, it allows multiple persons access the door or other authentication actions.

Before You Start

- Add access control device to the client, and make sure the device supports the first person in function.
- Add person and assign access authorization to designed person. For details, refer to [Person Management](#) and [Set Access Group to Assign Access Authorization to Persons](#).

Steps

1. Click **Access Control** → **Advanced Function** → **First Person In** to enter the First Person In page.
2. Select an access control device in the list on the left panel.

3. Select the current mode as **Enable Remaining Open after First Person**, **Disable Remaining Open after First Person**, or **Authorization by First Person** from the drop-down list for each access control point of the selected device.

Enable Remaining Open after First Person

The door remains open for the configured time duration after the first person is authorized until the remain open duration ends. If you select this mode, you should set the consecutive authentication times and interval of consecutive authentication.

Note

The remain open duration should be between 0 and 1440 minutes. By default, the remain open duration is 10 minutes.

Disable Remaining Open after First Person

Disable the function of first person in, namely normal authentication.

Authorization by First Person

All authentications (except for the authentications of super card, super password, duress card, and duress code) are allowed only after the first person authorization.

Note

You can authenticate by the first person again to disable the first person mode.

4. Click **Add** on the First Person List panel.
5. Select person(s) in the left list and the person(s) will be add to the selected persons as the first person(s) of the doors.
The added first person(s) will list in the First Person List
6. Optional: Select a first person from the list and click **Delete** to remove the person from the first person list.
7. Click **Save**.

15.5.9 Configure Anti-Passback

The anti-passback feature is designed to minimizes the misuse or fraudulent use of access credentials such as passing back card to an unauthorized person, or tailed access. The anti-passback function establishes a specific sequence in which access credentials must be used in order to grant access. You can set the sequence according to the actual path via the client and if the person uses the credential in wrong sequence, you can also reset the anti-password records.


Before You Start

Add access control device to the client, and enable the anti-passing back function of the access control device.

Steps

Note

Either the anti-passing back or multi-door interlocking function can be configured for an access control device at the same time. For the configuration of multi-door interlocking, refer to ***Configure Multi-door Interlocking***.

1. Click **Access Control** → **Advanced Function** → **Anti-Passback** to enter the Anti-Passpack Settings page.
 2. Select an access control device on the left panel.
 3. Select a card reader as the beginning of the path in the **First Card Reader** field.
 4. Click  of the selected first card reader in the **Card Reader Afterward** column to open the select card reader dialog.
 5. Select the afterward card readers for the first card reader.
-

Note

Up to four afterward card readers can be added as afterward card readers for one card reader.

6. Click **OK** in the dialog to save the selections.
7. Click **Save** in the Anti-Passback Settings page to save the settings and take effect.

Example

Set Card Swiping Path: If you select Reader In_01 as the beginning, and select Reader In_02, Reader Out_04 as the linked card readers. Then you can only get through the access control point by swiping the card in the order as Reader In_01, Reader In_02 and Reader Out_04.

8. Click **Reset Anti-Passback** and select the person(s) to delete the related anti-passback records about the person(s) on the device.
-

Note

This function should be supported by the device.

15.5.10 Configure Multi-door Interlocking

You can set the multi-door interlocking between multiple doors of the same access control device. To open one of the doors, other doors must keep closed. That means in the interlocking combined door group, up to one door can be opened at the same time.

Before You Start

Add access control device to the client, and make sure the device supports the multi-door interlocking function.

Steps

Note

- Multi-door Interlocking function is only supported by the access control device which has more than one access control points (doors).
 - Either the anti-passing back or multi-door interlocking function can be configured for an access control device at the same time. For the configuration of anti-passing back function, refer to [Configure Anti-Passback](#).
-

1. Click **Access Control** → **Advanced Function** → **Multi-door Interlocking**.
 2. Select an access control device on the left panel.
 3. Click **Add** on the Multi-door Interlocking List panel to open Add Access Control Point to open the Add window.
 4. Select at least two access control points(doors) from the list.
-

Note

Up to four doors can be added in one multi-door interlocking combination.

5. Click **OK** to add the selected access control point(s) for interlocking.
The configured multi-door interlocking combination will list on the Multi-door Interlocking List panel.
6. Optional: Select an added multi-door interlocking combination from the list and click **Delete** to delete the combination.
7. Click **Apply** to apply the settings to the access control device.

15.5.11 Configure Authentication Code

You can configure authentication code on the client. And after that, you can open door by entering authentication code when you forget to bring the card with you.

Before You Start

Add access control device to the client, and make sure the device supports authentication code as the authentication mode.

Steps

1. Click **Access Control** → **Advanced Function** → **Authentication Code** to enter the authentication code configuration page.
 2. Select an access control device in the list of Controller List panel.
All the applied cards and persons will display on the Card List panel.
-

Note

For setting and applying the permissions to the device, refer to [Set Access Group to Assign Access Authorization to Persons](#).

3. Click the field of each card in the Authentication Code column to enter the authentication code.

 **Note**

The authentication code should contain 4 to 8 digits.

4. Click **Save** at the upper-right corner of Authentication Code page to save the settings.
The authentication code function of the card will be enabled automatically.

What to do next

You should set the card reader authentication mode of access control device as **Card/Authentication Code**. Refer to [Configure Card Reader Authentication Mode and Schedule](#) for details.

15.6.3 Set Device Capture Parameters

You can configure the capture parameters of the access control device, including manual capture and event triggered capture.

 **Note**

- The capture function should be supported by the device.
 - Before setting the capture parameters, you should set the picture storage first to define where the event triggered pictures are saved. For details, refer to [Set Picture Storage](#).
-

Set Triggered Capture Parameters

When an event occurs, the camera of the access control device can be triggered to capture picture(s) to record what happens when the event occurs. You can view the captured pictures when checking the event details in Event Center. Before that, you need to set the parameters for the capture such as number of pictures captured for one time.

Before You Start

Before setting the capture parameters, you should set the picture storage first to define where the captured pictures are saved. For details, refer to [Set Picture Storage](#).

Steps

 **Note**

This function should be supported by the device

1. Enter the Access Control module.
 2. On the navigation bar on the left, enter **Advanced Function** → **More Parameters** → **Capture**.
 3. Select an access control device in the device list and select **Linked Capture**.
 4. Set the picture size and quality.
-

5. Set the capture times once triggered which defines how many pictures will be captures for one time.
6. If the capture times is more than 1, set the interval for each capture.
7. Click **Save**.

Set Manual Capture Parameters

In Status Monitoring module, you can capture a picture manually the access control device's camera by clicking a button. Before that, you need to set the parameters for the capture such as picture quality.

Before You Start

Before setting the capture parameters, you should set the saving path first to define where the captured pictures are saved. For details, refer to [Set File Saving Path](#).

Steps

 **Note**

This function should be supported by the device

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function** → **More Parameters** → **Capture**.
3. Select an access control device in the device list and select **Manual Capture**.
4. Select the resolution of the captured pictures from the drop-down list.
5. Select the picture quality as **High**, **Medium**, or **Low**. The higher the picture quality is, the larger size the picture will be.
6. Click **Save**.

15.6.4 Set Parameters for Face Recognition Terminal

For face recognition terminal, you can set its parameters including face picture database, QR code authentication, etc.

Steps

 **Note**

This function should be supported by the device.

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function** → **More Parameters**.
3. Select an access control device in the device list and click **Face Recognition Terminal**.
4. Set the parameters.

Note

These parameters displayed vary according to different device models.

COM

Select a COM port for configuration. COM1 refers to the RS-485 interface and COM2 refers to the RS-232 interface.

Face Picture Database

select Deep Learning as the face picture database.

Authenticate by QR Code

If enabled, the device camera can scan the QR code to authenticate. By default, the function is disabled.

Blocklist Authentication

If enabled, the device will compare the person who want to access with the persons in the blocklist.

If matched (the person is in the blocklist), the access will be denied and the device will upload an alarm to the client.

If mismatched (the person is not in the blocklist), the access will be granted.

Save Authenticating Face Picture

If enabled, the captured face picture when authenticating will be saved on the device.

MCU Version

View the device MCU version.

5. Click **Save**.

15.6.5 Enable M1 Card Encryption

M1 card encryption can improve the security level of authentication.

Steps

Note

The function should be supported by the access control device and the card reader.

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function** → **More Parameters**.
3. Select an access control device in the device list and click **M1 Card Encryption** to enter the M1 Card Encryption page.
4. Set the switch to on to enable the M1 card encryption function.
5. Set the sector ID.

The sector ID ranges from 1 to 100.

6. Click **Save** to save the settings.

15.6.6 Set RS-485 Parameters

You can set the access control device's RS-485 parameters including the baud rate, data bit, the stop bit, parity type, flow control type, communication mode, work mode, and connection mode.

Before You Start

Add access control device to the client, and make sure the device supports RS-485 interface.

Steps

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function** → **More Parameters**.
3. Select an access control device in the device list and click **RS-485** to enter the RS-485 Settings page.
4. Select the serial port number from the drop-down list to set the RS-485 parameters.
5. Set the baud rate, data bit, the stop bit, parity type, communication mode, working mode, and connection mode in the drop-down list.



When the connection mode is **Connect Access Control Device**, you can select **Card No.** or **Person ID** as the output type.

6. Click **Save**.
 - The configured parameters will be applied to the device automatically.
 - When you change the working mode or connection mode, the device will reboot automatically.

15.6.7 Set Wiegand Parameters

You can set the access control device's Wiegand channel and the communication mode. After setting the Wiegand parameters, the device can connect to Wiegand card reader via Wiegand communication.

Before You Start

Add access control device to the client, and make sure the device supports Wiegand.

Steps

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function** → **More Parameters**.
3. Select an access control device in the device list and click **Wiegand** to enter the Wiegand Settings page.
4. Set the switch to on to enable the Wiegand function for the device.
5. Select the Wiegand channel No. and the communication mode from the drop-down list.

 **Note**

If you set **Communication Direction** as **Sending**, you are required to set the **Wiegand Mode** as **Wiegand 26** or **Wiegand 34**.

6. Click **Save**.

- The configured parameters will be applied to the device automatically.
- After changing the communication direction, the device will reboot automatically.

15.7 Configure Linkage Actions for Access Control

You can configure different linkage actions for the event detected by the access control device. After that, linkage actions will be triggered once the event happens. This mechanism is used for notifying the security personnel the event, or triggering automatic access control in real time.

Two types of linkage actions are supported:

- **Client Actions:** When the event is detected, it will trigger the actions on the client, such as the client making an audible warning..
- **Device Actions:** When the event is detected, it will trigger the actions of a specific device, such as buzzing of a card reader and, opening/closing of a door, ..

15.7.1 Configure Client Actions for Access Event

Even if you are far away from an access point, you can still know what happens and how urgent the event is via the client by configuring client actions for the access event. Client actions here refer to the actions automatically executed by the client itself, such as making an audible warning and sending an email. Once an event is triggered, the client will notify the security personnel, so that he/she can handle the event in time.

Before You Start

Add access control device to the client.

Steps

1. Click **Event Configuration** → **Access Control Event**.

The added access control devices will display in the device list.

2. Select a resource (including device, alarm input, door/elevator, and card reader) from the device list.

The event types which the selected resource supports appear.

3. Select the event(s) and click **Edit Priority** to define the priority for the event(s), which can be used to filter events in the Event Center.

4. Set the linkage actions of the event.

1) Select the event(s) and click **Edit Linkage** to set the client actions when the event(s) are triggered.

Audible Warning

The client software gives an audible warning when the event is triggered. You can select alarm sound for the audible warning.

Note

For details about setting the alarm sound, refer to [Set Alarm Sound](#).

Send Email

Send an email notification about the event to one or more receivers.

For details about setting email parameters, refer to [Set Email Parameters](#).

Pop-up Window

Pop-up a window to display the event information (including event details, the event-related video footage, the event-related picture) on the software client when the event is triggered.

Display on Map

When the event source is added as a hot spot on the map, the hot spot will be displayed with red number (indicates the number of events, and the maximum number is 10) aside when the event is triggered, which helps the security personnel to view the location of the event.

You can also click the hot spot to view the event details and the live video of the linked camera.

Linked Camera

Link the selected camera to capture a picture when the access event is triggered.

Select the camera in the drop-down list.

2) Click **OK**.

5. Enable the event so that when the event is detected, event will be sent to the client and the linkage actions will be triggered.
6. Optional: Click **Copy to** to copy the event settings to other access control device, alarm input, door/elevator, or card reader.

15.7.2 Configure Device Actions for Access Event

You can set the access control device's linkage actions for the access control device's triggered event. After that, when an event is triggered, it can trigger the alarm output, buzzer on access controller, and other actions.

Steps

Note

The linkage actions should be supported by the device.

1. Click **Access Control** → **Linkage Configuration**.
2. Select the access control device from the list on the left.

3. Click **Add** to add a new linkage.
4. Select **Event Linkage** as the event source.
5. select the event type and detailed event to set the linkage.
6. In the Linkage Target area, set the property target to enable this action.

Buzzer on Controller

The audible warning of access control device will be triggered.

Capture

An event-related picture will be captured when the selected event happens.

Recording

An event-related picture will be captured when the selected event happens.

Note

The device should support recording.

Buzzer on Reader

The audible warning of card reader will be triggered.

Alarm Output

The alarm output will be triggered for notification when the selected event happens

Alarm Input

Arm or disarm the alarm input.

Note

The device should support alarm input function.

Access Point

The door status of open, close, remain open, or remain close will be triggered.

Note

The target door and the source door cannot be the same one.

Audio Play

The audio prompt will be triggered. And the select audio index related audio content will be played according to the configured play mode.

7. Click **Save**.
8. Optional: After adding the device linkage, you can do one or more of the followings:

Edit Linkage Settings	Select the configured linkage settings in the device list and you can edit its event source parameters, including event source and linkage target.
Delete Linkage Settings	Select the configured linkage settings in the device list and click Delete to delete it.

15.7.3 Configure Device Actions for Card Swiping

You enable access control device's linkage actions (such as disarming a zone and triggering audio prompt) for the swiping of a specific card, In this way, you can monitor the card holder's behaviors and whereabouts.

Steps



It should be supported by the device.

1. Click **Access Control** → **Linkage Configuration**.
2. Select the access control device from the list on the left.
3. Click **Add** to add a new linkage.
4. Select **Card Linkage** as the event source.
5. Enter the card number or select the card from the drop-down list.
6. Select the card reader where the card swipes.
7. In the Linkage Target area, set the property target to enable this action.

Buzzer on Controller

The audible warning of access control device will be triggered.

Buzzer on Reader

The audible warning of card reader will be triggered.

Capture

An event-related picture will be captured when the selected event happens.

Recording

An event-related picture will be captured when the selected event happens.



The device should support recording.

Alarm Output

The alarm output will be triggered for notification.

Alarm Input

Arm or disarm the alarm input.

Note

The device should support alarm input function.

Access Point

The door status of open, close, remain open, or remain closed will be triggered.

Audio Play

The audio prompt will be triggered. And the select audio index related audio content will be played according to the configured play mode.

8. Click **Save**.

When the card (configured in Step 5) swipes on the card reader (configured in Step 6), it can trigger the linked actions (configured in step 7).

9. Optional: After adding the device linkage, you can do one or more of the followings:

Delete Linkage Settings Select the configured linkage settings in the device list and click **Delete** to delete it.

Edit Linkage Settings Select the configured linkage settings in the device list and you can edit its event source parameters, including event source and linkage target.

15.7.4 Configure Device Actions for Person ID

You can set the access control device's linkage actions for the specified person ID. When access control device detects the specified person ID, it can trigger the alarm output, buzzer on card reader, and other actions, so as to implement special monitoring on the specified person.

Steps

Note

It should be supported by the device.

1. Click **Access Control** → **Linkage Configuration**.
2. Select the access control device from the list on the left.
3. Click **Add** to add a new linkage.
4. Select **Person Linkage** as the event source.
5. Enter the employee number or select the person from the drop-down list.
6. Select the card reader where the card swipes.

7. In the Linkage Target area, set the property target to enable this action.

Buzzer on Controller

The audible warning of access control device will be triggered.

Buzzer on Reader

The audible warning of card reader will be triggered.

Capture

An event-related picture will be captured when the selected event happens.

Recording

An event-related picture will be captured when the selected event happens.



The device should support recording.

Alarm Output

The alarm output will be triggered for notification.

Alarm Input

Arm or disarm the alarm input.



The device should support zone function.

Access Point

The door status of open, close, remain open, or remain closed will be triggered.

Audio Play

The audio prompt will be triggered. And the select audio index related audio content will be played according to the configured play mode.

8. Click **Save**.

9. Optional: After adding the device linkage, you can do one or more of the followings:

Delete Linkage Settings

Select the configured linkage settings in the device list and click **Delete** to delete it.

Edit Linkage Settings

Select the configured linkage settings in the device list and you can edit its event source parameters, including event source and linkage target.

15.8.1 Control Door Status

You can control the status for the door(s), including unlock door, locking door, remaining the door unlock, remaining the door locked, remain all unlocked, etc.

Before You Start

- Add person and assign access authorization to designed person, and person will have the access authorization to the access points (doors). For details, refer to [Person Management](#) and [Set Access Group to Assign Access Authorization to Persons](#).
- Make sure the operation user has the permission of the access points (doors). For details, refer to [Add User](#).

Steps

1. Click **Monitoring** to enter the status monitoring page.
2. Select an access point group on the upper-right corner.



For managing the access point group, refer to [Group Management](#).

The doors in the selected access control group will display.

3. Click a door icon to select a door, or press **Ctrl** and select multiple doors.



For **Remain All Unlocked** and **Remain All Locked**, ignore this step.

4. Click the following buttons to control the door.

Unlock

When the door is locked, unlock it and it will be open for once. After the open duration, the door will be closed and locked again automatically.

Lock

When the door is unlocked, lock it and it will be closed. The person who has the access authorization can access the door with credentials.

Remain Unlocked

The door will be unlocked (no matter closed or open). All the persons can access the door with no credentials required.

Remain Locked

The door will be closed and locked. No person can access the door even if he/she has the authorized credentials, except the super users.

Remain All Unlocked

All doors in the group will be unlocked (no matter closed or open). All the persons can access the doors with no credentials required.

Remain All Locked

All doors in the group will be closed and locked. No person can access the doors even if he/she has the authorized credentials, except the super users.

Capture

Capture a picture manually.

Note

The **Capture** button is available when the device supports capture function. The picture is saved in the PC running the client. For setting the saving path, refer to **Set File Saving Path**.

Result

The icon of the doors will change in real-time according to the operation if the operation is succeeded.

15.8.3 Check Real-Time Access Records

The real-time access records can be displayed in the client, including card swiping records, face recognition records, skin-surface temperature information, etc. Also, you can view the person information and view the picture captured during access.

Before You Start

You have added person(s) and access control device(s) to the client. For details, refer to **Person Management** and **Add Device**.

Steps

1. Click **Monitoring** to enter monitoring module.
Real-time access records are displayed on the bottom of the page. You can view record details, including card No., person name, event time, door location, temperature, authentication type etc.

Figure 15-12 Real-time Access Records

Note

You can right click the column name of access event table to show or hide the column according to actual needs.

2. Optional: Select an access point group from the drop-down list in the upper-right corner to show the real time access records of the selected group.
3. Optional: Check the event type and event status.

The detected events of checked type and status will be displayed in the list below.

4. Optional: Check **Show Latest Event** to view the latest access record.

The record list will be listed reverse chronologically.

5. Optional: Check **Enable Abnormal Temperature Prompt** to enable abnormal skin-surface temperature prompt.
-


Note

When enabled, if there is abnormal temperature information, an Abnormal Temperature window pops up when you enter Monitoring module, displaying person's picture, skin-surface temperature, card No., person name, etc.

6. Optional: Click an event to view person pictures (including captured picture and profile).
-

Note

In **Linked Capture Picture** field, you can double click the captured picture to view an enlarged picture.

7. Optional: Click  to view monitoring details (including person's detailed information and the captured picture).
-


Note

In the pop-up window, you can click  to view monitoring details in full screen.

Chapter 19 Log Search

Two log types are provided: operation log and system log. The operation logs refer to the normal operations that the user did on the client, such as adding device, resetting password, starting live view, etc.; and the system logs record the system information, such as login, logout, locking and unlocking, etc. You can search the log files and view the log details, including time, user, etc.

Steps


1. Enter the Log Search module.
2. Click  to specify the start time and end time.



Note

You can search the logs within one month.

3. Select a user to search the log files which are generated when this user operate on the client.
4. Select **Operation Log** or **System Log** as log type.
5. Click **Search**.
The log files between the start time and end time will be displayed on the list. You can check the operation time, type and other information of the logs.
6. Optional: Perform the following operations if there are too many log files.

Filter	Click  on each table header and select to filter the logs.
Sort	Click the table header to sort the logs by the time or letter sequence.

Chapter 20 User Management

To improve the system security, the administrator should create different account for different user, and assign different permissions to the user. To avoid different people sharing the same user account, we recommend you manage the user accounts periodically.

20.1 Add User

The super user and administrator can add new users, and assign different permissions for different users if needed.

Perform this task to add an user account.

Steps

Note

The user account you registered to log in the software is set as the super user.

1. Enter the User Management module.
2. Click **Add User** to show user information area.
3. Select the user type from the drop-down list.

Administrator

The administrator account has all permissions by default, and can modify the passwords and permissions of all operators and its own.

Operator

The operator account has no permission by default and you can assign the permissions manually. An operator can only change the passwords of its own account and the accounts which are added by it.

4. Enter the user name, password, and confirm password as desired.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

5. Check the checkboxes to assign the permissions to the created user.
6. Optional: Click **Default Value** to restore the default permissions of this user.
7. Click **Save**.

 **Note**

Up to 50 user accounts can be added for the client software.

After created user account successfully, the user account is added to the user list on the Account Management page.

8. Optional: Perform the following operations after the user account is created.

Edit User

Click a user from the list to edit the user information.

 **Note**

Only the password of the super user can be edited.

Delete User

Select the user from the list and click **Delete User**.

 **Note**

You cannot delete the super user.

20.2 Change User's Password

The administrator can change normal user's password without entering the old password, while the administrator should enter the old password when changing the password of itself.

Before You Start

Add user to the software client.

Steps

1. Enter the User Management module.
 2. Select the user need to be change password, click **Change**.
 3. Optional: Enter the old password.
-

 **Note**

When changing the administrator's password, you need to enter the old password first.

4. Enter the new password and confirm the password.
5. Click **OK**.

Chapter 21 System Configuration

21.1 Set General Parameters

You can configure the frequently-used parameters, including log expired time, network performance, etc.

Steps

1. Enter the System Configuration module.
2. Click **General** tab to enter the General Settings page.
3. Configure the general parameters.

Date Format / Time Format

The display style of date and time on related pages.

Log Retention Period

The time for keeping the log files. Once exceeded, the files will be deleted.

Maximum Mode

Select **Maximize** or **Full Screen** as the maximum mode. **Maximize** mode can maximize the display and show the taskbar. **Full Screen** mode can display the client in full-screen mode.

Network Performance

Set the network conditions to **Normal**, **Better** or **Best**.

Save Pictures in Structure Data Format

- After **Save Pictures in Structure Data Format** is enabled, the **Delete Registered Picture** in **Person** module will be available. If a person's information is applied to the device(s) successfully, the person's picture will be automatically deleted and no picture will be displayed in Basic Information. The **Face** column in **Person** module will display the number of the added face picture(s).
- When **Save Pictures in Structure Data Format** is enabled, no pictures will be displayed in Event Details field in Event Center.

Enable Keyboard and Joystick

Enable the keyboard or joystick. After enabled, you can set the shortcuts for the keyboard and joystick.

Note

For details, refer to [Set Keyboard and Joystick Shortcuts](#).

Export Person Information

If you enable this, the **Export** button for exporting person information will be displayed on

the Person Management page. Please pay attention to person information security.

Event Retention Period

The time period for keeping the event information. When the retention period expires, the event record will be deleted automatically.

Automatic Time Synchronization

Automatically synchronize the time of the added devices with the time of the PC running the client at a specified time point.

Auto-Upgrade Device

Set the upgrading mode after the new version of device are detected.

Disable

After enabled, the client will not download the firmware package and upgrade even if the client detects a new version of the client.

Prompt Me If Download and Upgrade

After the client detects a new version of the device, it will prompt the user whether to download the firmware package and upgrade.

Download and Prompt Me If Upgrade

After the client detects the new version of the device, it will download the firmware package automatically, and prompt the user whether to upgrade.

Download and Prompt Automatically

After the client detects the new version of the devices, it will download the firmware package and upgrade the new version automatically.

You need to set a schedule in the **Upgrade Time** field, during which the client upgrades the new version automatically.

Country/Region

Select the server's region for ABUS Link Station, you can select the region you belong to or the nearest region around.

4. Click **Save**.

21.2 Set Live View and Playback Parameters

You can set the parameters for live view and playback, including picture format, pre-play duration, etc.

Steps

1. Enter the System Configuration module.
2. Click **Live View and Playback** tab.
3. Configure the live view and playback parameters.

Picture Format

Select **JPEG** or **BMP** as the image format for storing pictures.

Note

If **Display Temperature on Captured Pictures** switch is set to ON, JPEG is selected as the image format by default and cannot be changed.

Video Format

Select **MP4/AVI** as the format of recorded videos.

Merge Downloaded Video Files

Set the maximum size of merged video file for downloading the video file by date.

Search Video Files Stored in

Search the video files stored in the local device, in the storage server, or both in the storage server and local device for playback.

Pre-play for

Set the pre-play time for event playback. By default, it is 30s.

Prioritize Playback of Video Files on Storage Server

Play back the video files recorded on the storage server preferentially. Otherwise, play back the video files recorded on the local device.

Resume Latest Live View Status After Restart

Resume the latest live view status after you log into the client again.

Disconnect Background Videos in Single Live View

In multiple-window division mode, double-click a live video to display it in 1-window division mode, and the other live videos will be stopped for saving the resource.

Enable Wheel for Zoom

Use the mouse wheel for zoom in or out of the video in PTZ mode, or for zoom in or restoring of the video in digital zoom mode. In this way, you can directly zoom in or out (or restore) the live video by scrolling the mouse.

Skip Unconcerned Video during VCA Playback

Skip the unconcerned video during VCA playback and the unconcerned video will not be played during VCA playback.

4. Click **Save**.

21.3 Set Image Parameters

The image parameters of the client can be configured, such as view scale, play performance, etc.

Steps

1. Open the System Configuration page.
2. Click **Image** tab to enter the Image Settings interface.
3. Configure the image parameters.

View Scale

The view scale of the video in live view or playback. It can be set as **Full Screen**, **4:3**, **16:9**, or **Original Resolution**.



Note

You can also set the view scale in Live View module. For details, refer to [Live View](#).

Play Performance

The play performance of the live video. It can be set as **Shortest Delay**, **Balanced**, or **Fluency**. You can also select **Custom** and configure the frame rate according to actual needs.

Hardware Decoding Preferred

Select **D3D9** or **D3D11** to enable decoding by hardware for live view and playback. Hardware Decoding can provide better decoding performance and lower CPU usage when playing the HD video during live view or playback.

Enable Highlight

Mark the detected objects with green rectangles in live view and playback.

Display Transaction Information

Display the transaction information on the live view image.

VCA Rule

Display the VCA rule in the live view.

Enable Frame Extracting for High-speed Playback

When playing back the video at high speed (8x speed and above), you can disable this function to make the image of playback more fluent to view the details.

Display Target's Pattern

After enabled, you can view the target person's motion track on the view window.

Overlay Rules on Captured Picture

For the thermal device, set to display the temperature information and fire source information on the captured pictures.

 **Note**

After enabled this function, the Picture Format configured in **System Configuration** → **Live View and Playback** will change to JPEG and is not editable.

Noise Reduction

Noise reduction mode, which can be set as **Disable**, **Self-adaptive**, or **Enable**.

4. Click **Save**.

21.4 Set Picture Storage

The captured pictures triggered by the events on the devices, can be saved in the PC running the ABUS CMS Service. You can set the picture storage location here manually.



Steps

1. Enter the System Configuration module.
2. Click **Event Picture Storage**.
3. Set the **Store Pictures in Server** switch to on.
All the disks of the PC running the ABUS CMS service will show.
4. Select the disk to save the pictures.
5. Click **Save**.

21.5 Set Alarm Sound

When the event is triggered, the client can give an audible warning to notify the security personnel. You can set the sound of the audible warning in this section.

Steps

1. Open the System Configuration page.
2. Click **Alarm Sound** tab to enter the Alarm Sound Settings page.
3. Optional: Click **...** and select the audio files from the local path for different events.
4. Optional: Add customized alarm sound.
 - 1) Click **Add** to add customized alarm sound.
 - 2) Double click the **Type** field to customize the alarm sound name as desired.
 - 3) Click **...** and select the audio files from the local path for different alarms.
5. Optional: Click  for a testing of the audio file.
6. Optional: Click  in the Operation column to delete the custom sound.
7. Click **Save**.

 **Note**

The format of the audio file can only be WAV.

21.6 Set Access Control and Video Intercom Parameters

You can configure the access control and video intercom parameters according to actual needs.

Steps

1. Open the System Configuration page.
2. Click the **Access Control & Video Intercom** tab.
3. Input the required information.

Ringtone

Click and select the audio file from the local path for the ringtone of indoor station. Optionally, you can click for a testing of the audio file.

Max. Ring Duration

Specify the seconds that the ring will last for at most. The maximum ring duration can be set from 15s to 60s.

Max. Speaking Duration with Indoor Station

Specify the seconds that the call with indoor station will last for at most. The maximum speaking duration between indoor station and the client can be set from 120s to 600s.

Max. Speaking Duration with Door Station

Specify the seconds that the call with door station will last for at most. The maximum speaking duration between door station and the client can be set from 90s to 120s.

Max. Speaking Duration with Access Control Device

Specify the seconds that the call with access control device will last for at most. The maximum speaking duration between access control device and the client can be set from 90s to 120s.

4. Click **Save**.

21.7 Set File Saving Path

The video footage (manually recorded during live view and clipped during playback) and captured pictures are stored on the local PC. The saving path of these files can be set.

Steps

1. Open the System Configuration page.
2. Click **File** tab to enter the File Saving Path Settings page.
3. Click **...** and select a local path for the files.
4. Click **Save**.

21.8 Set Icons Shown on Toolbar

The icons and the order on the toolbar in the live view and playback window can be customized.

You can set to display what icons and set the icon order.

Perform the following task when you need to set icons shown on Toolbar.

Steps

1. Enter the System Configuration module.
2. Click **Toolbar** tab to enter the Toolbar Settings page.
3. Set **Enable Screen Toolbar Display** switch to ON to enable displaying the toolbar on in the live view and playback window.
4. Click the required icon to display on the toolbar.
5. Optional: Drag the icon to set the icon order when displaying on the toolbar.

Table 21-1 Icons on Live View Toolbar















	Stop Live View	Stop the live view in the display window.
	Capture	Capture the picture in the live view process. The capture picture is stored in the PC.
	Record	Start manual recording. The video file is stored in the PC.
	PTZ Control	Start PTZ mode for speed dome. Click and drag in the view to perform the PTZ control.
	Two-way Audio	Start the two-way audio with the device in live view.
	Digital Zoom	Enable the digital zoom function. Click again to disable the function.
	Instant Playback	Switch to the instant playback mode.
	Remote Configuration	Open the remote configuration page of the camera in live view.

Table 21-2 Icons on Playback Toolbar

	Capture	Capture the picture in the live view process. The capture picture is stored in the PC.
	Record	Start manual recording. The video file is stored in the PC.
	Digital Zoom	Enable the digital zoom function. Click again to disable the function.
	Download	Download the video files of the camera and the video files are stored in the PC.
	VCA Playback	Set the VCA rules. For more details, refer to <u>VCA Playback</u> .
	Tag Control	Add default or custom tag for the video files to mark the important video point. You can also edit the tag.

6. Click **Save**.

21.9 Set Keyboard and Joystick Shortcuts

The keyboard can be connected to the client and be used to control the PTZ cameras. You can set the shortcuts for keyboard and joystick to get quick and convenient access to the commonly used actions.

Perform this task when you need to set keyboard and joystick shortcuts.

Steps

Note

This configuration page will display after enabling keyboard and joystick in General Settings. For details, refer to [***Set General Parameters***](#).

1. Enter the System Configuration module.
2. Click **Keyboard and Joystick** to show the Keyboard and Joystick Shortcut Settings area.
3. Select the COM port from the drop-down list for keyboard if the keyboard is connected to the PC installed with the client.

Note

You can enter the Device Manger of the PC to check the COM port, which the keyboard is connected to.

4. Set shortcuts for keyboard and joystick.
 - 1) Select a certain function name on Function column.
 - 2) Double-click the item field under the PC Keyboard, USB Joystick or USB Keyboard column.
 - 3) Select the compound keys operation or number from the drop-down list to set it as the shortcuts for the function of the keyboard or USB joystick.
5. Click **Save**.

Example

For the **Focus (+)** function, if you set **Home**, **1**, and **F1** as the shortcuts of the PC Keyboard, USB Joystick and USB Keyboard, you can press the Home key on PC keyboard, control the joystick to the 1 direction, or press F1 key on USB keyboard to zoom in.

21.10 Set Email Parameters

When an event is triggered, if you can set **Send Email** as linkage action for this event, the client will an email to the recipients for notification. You need to set the email settings and specify target

recipients in this section.

Steps

1. Enter the System Configuration module.
2. Click **Email** tab to enter the Email Settings interface.
3. Enter the required information.

STMP Server

The STMP server IP address of host name (e.g., smtp.263xmail.com)

Encryption Type

You can check the radio to select **Non-Encrypted**, **SSL**, or **STARTTLS** .

Port

Enter the communication port used for SMTP. The port is 25 by default.

Sender Address

The email address of the sender.

Security Certificate (Optional)

If your email server requires authentication, check this checkbox to use authentication to log into the server and enter the login user name and password of your email account.

User Name

Enter the user name of the sender email address if **Server Authentication** is checked.

Password

Enter the password of the sender Email address if **Server Authentication** is checked.

Receiver 1 to 3

Enter the email address of the receiver. Up to 3 receivers can be set.

4. Optional: Click **Send Test Email** to send an email to the receiver for test.
5. Click **Save**.

21.11 Manage Security Authentication

For the data security purpose, the security certificate of clients and added servers should be same. You can set the verify certificate is required or not when enabling transmission encryption using TLS (Transport Layer Security) protocol.

Before adding a server to the client, you should export the service certificate from the client service, and import it to the server. If multiple clients use the same server, you should make the security certificates of the clients and the server same with each other.

21.11.1 Export Certificate from Service Management

You can export the security certificate from the current client service and import the exported

certificate file to other clients.

Steps

1. Enter the Service Management.
2. Click **Export** to save the certificate file in the local PC.

Note

The certificate file is in XML format.

What to do next

After exporting the certificate, you can copy the certificate to the PC installed with the client and import it to other clients.

21.11.2 Import Certificate to Client

If there are multiple clients accessing the same steam media server, you should import the same certificate to the clients and server.

Before You Start

Make sure you have exported the security certificate from one of the client service.

Note

For details, refer to [***Export Certificate from Service Management.***](#)

Steps

1. Copy the certificate file exported from other client to the local PC.
2. Enter the System Configuration module.
3. Click **Security Authentication** tab to enter the security authentication setting interface.
4. Click **Import**.
5. Select the certificate file from your local PC and click **Open**.

Note

Please restart the client to take effect.

21.11.3 Certificate Verification for Transmission Encryption

On the Security Authentication page, you can set the device certificate verification is required or not for transmission encryption.

Click **System Configuration** → **Security Authentication** to enter the security authentication interface. Select the Verify Certificate as **Yes** or **No**.

Yes

You must put the device certificate to the designed directory if you enable transmission encryption when adding device. And the device will be added with transmission encryption and the certificate will be verified, which improves the security level.

No

The device certificate is not required if you enable transmission encryption when adding device. And the device will be added with transmission encryption.

Chapter 22 Operation and Maintenance

You can perform maintaining operations in the menu to ensure a smooth and convenient usage of the client.

In the upper-right corner of the client, click  → **File** → **System** → **Tool**, and perform the following operations.

Open Log File

You can open a log file saved in your local PC or log files of the client.

Import/Export Configuration File

You can import configuration files from local PC to the client if needed, and vice versa.

Auto Backup

Select day and time to backup configuration files and data in database, or restore the backed up data.

Broadcast

Check one or more devices to enable the broadcast function of the devices.

Batch Wiper Control

Batch turn on/off the wiper.

1 VS 1 Face Comparison

Select two face pictures from the local PC for comparison. The similarity between the two pictures

will be shown.

 **Note**

This function can be used for identity verification and should be supported by the DeepinMind device.

Batch Time Sync

Synchronize selected devices' time with your PC time.

Message Queue

After configuring email linkage, the triggered event(s) will be displayed here. Select an event and cancel sending the an email to the receiver.

A. Custom Wiegand Rule Descriptions

Take Wiegand 44 as an example, the setting values in the Custom Wiegand tab are as follows:

Custom Wiegand Name	Wiegand 44				
Total Length	44				
Transformation Rule (Decimal Digit)	byFormatRule[4]=[1][4][0][0]				
Parity Mode	XOR Parity				
Odd Parity Start Bit		Length			
Even Parity Start Bit		Length			
XOR Parity Start Bit	0	Length per Group	4	Total Length	40
Card ID Start Bit	0	Length	32	Decimal Digit	10
Site Code Start Bit		Length		Decimal Digit	
OEM Start Bit		Length		Decimal Digit	
Manufacturer Code Start Bit	32	Length	8	Decimal Digit	3

Wiegand Data

Wiegand Data = Valid Data + Parity Data

Total Length

Wiegand data length.

Transportation Rule

4 bytes. Display the combination types of valid data. The example displays the combination of Card ID and Manufacturer Code. The valid data can be single rule, or combination of multiple rules.

Parity Mode

Valid parity for Wiegand data. You can select either odd parity or even parity.

Odd Parity Start Bit, and Length

If you select Odd Parity, these items are available. If the odd parity start bit is 1, and the length is 12, then the system will start odd parity calculation from bit 1. It will calculate 12 bits. The result will be in bit 0. (Bit 0 is the first bit.)

Even Parity Start Bit, and Length

If you select Even Parity, these items are available. If the even parity start bit is 12, and the length is 12, then the system will start even parity calculation from bit 12. It will calculate 12 bits. The result will be in the last bit.

XOR Parity Start Bit, Length per Group, and Total Length

If you select XOR Parity, these items are available. Depending on the table displayed above, the start bit is 0, the length per group is 4, and the total length is 40. It means that the system will calculate from bit 0, calculate every 4 bit, and calculate 40 bits in total (10 groups in total). The result will be in the last 4 bits. (The result length is the same as the length per group.)

Card ID Start Bit, Length, and Decimal Digit

If you use the transformation rule, these items are available. Depending on the table displayed above, the card ID start bit is 0, the length is 32, and the decimal digit is 10. It represents that from bit 0, there are 32 bits represent the card ID. (The length here is calculated by bit.) And the decimal digit length is 10 bits.

Site Code Start Bit, Length, and Decimal Digit

If you use the transformation rule, these items are available. For detailed information, see the explanation of the card ID.

OEM Start Bit, Length, and Decimal Digit

If you use the transformation rule, these items are available. For detailed information, see the explanation of the card ID.

Manufacturer Code Start Bit, Length, and Decimal Digit

If you use the transformation rule, these items are available. Depending on the table displayed above, the manufacturer code start bit is 32, length is 8, and decimal digit is 3. It represents that from bit 32, there are 8 bits are manufacturer code. (The length here is calculated by bit.) And the decimal length is 3.

D. Error Code

Code	Error Name	Description
ABUS CMS		
317	No videos.	It will be prompted when the user has no permission to play back.
HCNetSDK.dll		
1	Invalid user name or password.	
2	No permission.	The user in the device has no enough permission.
4	Invalid channel number.	It will be prompted in the live view of remote screen control.
5	No more devices can be connected.	
7	Failed to connect the device.	
23	Not supported.	
29	Operation failed.	
43	No buffer.	It will be prompted when adding a device and the device port is occupied by a web server.
55	Invalid IP address.	
56	Invalid MAC address.	
91	The channel does not support the operation.	It will be prompted when failed to get the sub stream.
96	The device is not registered on the DDNS.	
153	The user is locked.	
250	The device is not activated.	
404	Channel No. error or the device does not support the sub stream.	It will be prompted when failed to get the sub stream or the sub stream does not exist.
424	Failed to receive the data for RTSP SETUP.	It will be prompted when adding the live view for the software DVS via external network.

Code	Error Name	Description
800	No more bandwidth can be used.	
Playctrl.dll		
2		The stream is not a Video & Audio stream.
6		The playback window turns black when adopting H.265 in the 64-bit operating system.



Security Tech Germany

Gebbruikershandleiding V.1.0
ABUS CMS Software

Inhoud

Hoofdstuk 3 Apparaatbeheer	1
3.1 Apparaten activeren.....	1
3.2 Apparaat toevoegen.....	2
3.2.1 Eén of meerdere online apparaten toevoegen	3
3.2.2 Apparaat toevoegen op IP-adres of domeinnaam.....	6
3.2.3 Apparaten toevoegen per IP-segment	9
3.2.4 Apparaten importeren in een batch.....	12
3.3 Wachtwoord van apparaat herstellen/herstellen	15
3.3.1 Wachtwoord voor apparaat opnieuw instellen	15
3.3.2 Het standaardwachtwoord van het apparaat herstellen	16
3.4 Firmwareversie van apparaat upgraden	17
3.5 Toegevoegde apparaten beheren.....	19
3.6 Groepsmanagement.....	20
3.6.1 Groepsmiddelen	20
3.6.2 Bronparameters bewerken.....	21
Hoofdstuk 4 ABUS Link Station	24
4.1 Een ABUS Link Station Account registreren	24
4.2 Aanmelden bij ABUS Link Station Account	25
Hoofdstuk 5 Liveweergave	27
5.1 Werkbalk Liveweergave	27
5.2 Aangepaste weergave toevoegen	28
5.3 Liveweergave starten	29
5.4 Automatisch schakelen in Liveweergave	31
5.4.1 Automatisch schakelen tussen camera's in een groep.....	31
5.4.2 Alle camera's automatisch schakelen	33
5.4.3 Automatisch schakelen tussen aangepaste weergaven	35
5.5 PTZ-besturing.....	37
5.5.1 PTZ-bedieningspaneel	37
5.5.2 Preset, Patrol en Patroon instellen	40

5.6 Vensterindeling aanpassen	41
5.7 Handmatig opnemen en vastleggen	44
5.7.1 Video handmatig opnemen	44
5.7.2 Lokale video's bekijken	45
5.7.3 Foto's vastleggen	45
5.7.4 Vastgelegde afbeeldingen weergeven	46
5.8 Onmiddellijk afspelen	47
5.9 Liveweergave voor Fisheye-camera	47
5.9.1 Liveweergave in visoogmodus uitvoeren	47
5.9.2 PTZ-besturing in visenoogmodus	49
5.9.3 Een preset en patrouille instellen	50
5.11 Liveweergave voor thermische camera	51
5.11.1 Vuurbroninformatie bekijken tijdens Live weergave	51
5.11.2 Temperatuurinformatie op Live View-beeld tonen	52
5.11.3 Temperatuur handmatig meten	53
5.11.4 Vuurbrondetectiescherm gebied weergeven	55
5.13 Meer functies	56
Hoofdstuk 6 Weergave op afstand	58
6.2 Externe opslagconfiguratie	58
6.2.1 Foto en video opslaan op DVR, NVR of netwerkcamera	58
6.2.3 Afbeelding en extra informatie opslaan op lokale pc	60
6.2.4 Opnameschema sjabloon configureren	61
6.2.5 Vastlegschemasjabloon configureren	62
6.3 Werkbalk voor afspelen	63
6.4 Normaal afspelen	65
6.4.1 Videobeelden zoeken	66
6.4.2 Video afspelen	68
6.5 Alarm ingang afspelen	70
6.5.1 Videobeelden zoeken	70
6.5.2 Videobeelden afspelen	72
6.6 Gebeurtenissen afspelen	72

6.6.1 Videobeelden/foto zoeken	73
6.6.2 Videobeelden/afbeelding bekijken	73
6.9 VCA afspelen.....	74
6.10 Synchroon afspelen	76
6.11 De videoweergave van de Fisheye-camera	77
6.13 Videobeelden downloaden.....	79
6.13.1 Videobeelden downloaden op datum.....	79
6.13.2 Downloaden voor meerdere camera's	80
Hoofdstuk 7 Gebeurtenisconfiguratie	82
7.1 Gebeurtenis voor camera configureren	82
7.2 Gebeurtenis voor alarmingang configureren	84
7.3 Gebeurtenis voor codeerapparaat configureren	86
Hoofdstuk 8 Evenemententerrein.....	88
8.1 Gebeurtenissen van apparaten ontvangen inschakelen	88
8.2 Realtime gebeurtenissen weergeven	89
8.3 Historische gebeurtenissen zoeken	91
8.4 Gebeurtenissen van apparaat ophalen	95
8.5 Pop-up gebeurtenisinformatie weergeven	96
Hoofdstuk 9 Kaartbeheer	98
9.1 Kaart toevoegen	98
9.2 Kaartschaal bewerken.....	99
9.3 Kalibratie van lengtegraad en breedtegraad	100
9.4 Hot Spot beheren	101
9.4.1 Camera toevoegen als hotspot.....	101
9.4.2 Alarmingang toevoegen als hotspot.....	103
9.4.3 Alarmuitgang toevoegen als Hot Spot.....	104
9.4.4 Zone toevoegen als hotspot	106
9.4.5 Toegangspunt toevoegen als hotspot	108
Hoofdstuk 10 Statistieken	110
10.1.1 Rapport over het tellen van personen per codeerapparaat	110
10.2 Rapport over het tellen van personen op kruispunten bekijken	114

10.4 Hittekaartrapport	115
10.7 Temperatuurkaart	117
Hoofdstuk 11 Gegevens ophalen	120
11.1 Ophalen van voertuigen.....	120
Hoofdstuk 14 Persoonsbeheer.....	121
14.1 Organisatie toevoegen	122
14.2 Persoon toevoegen	122
14.2.1 Basisinformatie configureren	123
14.2.2 Een kaart uitgeven aan één persoon.....	124
14.2.3 Een gezichtsfoto uploaden vanaf de lokale pc.....	127
14.2.4 Een foto maken via de client	128
14.2.5 Gezicht verzamelen via toegangscontroleapparaat	129
14.2.10 Informatie over toegangscontrole configureren	130
14.2.11 Persoonsgegevens aanpassen	132
14.2.12 Informatie over de bewoner configureren	133
14.2.13 Extra informatie configureren	133
14.3 Informatie over persoonsidentificatie importeren en exporteren	134
14.3.1 Persoonlijke invoergegevens	134
14.3.2 Afbeeldingen van personen importeren	135
14.3.3 Persoonsgegevens exporteren	135
14.3.4 Afbeeldingen van personen exporteren	136
14.4 Persoonsgegevens ophalen uit toegangscontroleapparaat	137
14.5 Personen verhuizen naar een andere organisatie	138
14.6 Kaarten afgeven aan personen in batch.....	138
14.7 Rapport Verlies.....	138
14.8 Hulpbronstatistieken bekijken	139
Hoofdstuk 15 Toegangscontrole	141
15.2 Schema en sjabloon configureren	141
15.2.1 Vakantie toevoegen	141
15.2.2 Sjabloon toevoegen	142
15.3 Toegangsgroep instellen om toegangsrechten aan personen toe te wijzen	144

15.4 Toegangsgroep zoeken.....	146
15.5 Geavanceerde functies configureren	147
15.5.1 Apparaatparameters configureren.....	147
15.5.2 Resterende vergrendeld/ontgrendeld configureren	156
15.5.3 Multi-Factor Authenticatie configureren	157
15.5.4 Aangepaste Wiegand-regel configureren	159
15.5.5 Kaartlezerauthenticatiemodus en -schema configureren	161
15.5.6 De modus persoonsauthenticatie configureren	164
15.5.8 Eerste persoon in configureren	164
15.5.9 Anti-Passback configureren	165
15.5.10 Multideurvergrendeling configureren.....	167
15.5.11 Authenticatiecode configureren.....	167
15.6.3 Parameters voor apparaatopname instellen	168
15.6.4 Parameters instellen voor gezichtsherkenningsterminal	170
15.6.5 M1-kaartcodering inschakelen	171
15.6.6 RS-485 parameters instellen.....	171
15.6.7 Wiegand-parameters instellen	172
15.7. Koppelingsacties voor toegangscontrole configureren	172
15.7.1 Klantacties voor toegangsgebeurtenis configureren.....	173
15.7.2 Apparaatacties voor toegangsgebeurtenis configureren	174
15.7.3 Apparaatacties voor kaartzwemmen configureren	176
15.7.4 Apparaatacties voor persoon-ID configureren	177
15.8.1 Status besturingsdeur	179
15.8.3 Real-time toegangsrecords controleren.....	180
Hoofdstuk 19 Logboek zoeken	182
Hoofdstuk 20 Gebruikersbeheer	183
20.1 Gebruiker toevoegen	183
20.2 Het wachtwoord van de gebruiker wijzigen	184
Hoofdstuk 21 Systeemconfiguratie	186
21.1 Algemene parameters instellen.....	186
21.2 Liveweergave- en weergaveparameters instellen	187

21.3 Beeldparameters instellen	189
21.4 Beeldopslag instellen	190
21.5 Alarmgeluid instellen	190
21.6 Parameters voor toegangscontrole en video-intercom instellen	191
21.7 Pad voor bestandsopslag instellen	192
21.8 Pictogrammen op werkbalk instellen	192
21.9 Toetsenbord en joystick snelkoppelingen instellen	193
21.10 E-mailparameters instellen	194
21.11 Beveiligingsauthenticatie beheren	195
21.11.1 Certificaat exporteren vanuit Servicebeheer	195
21.11.2 Certificaat importeren naar klant	196
21.11.3 Certificaatverificatie voor transmissie-encryptie	196
Hoofdstuk 22 Bediening en onderhoud	197
A. Aangepaste Wiegand-regelbeschrijvingen	199
D. Foutcode	201

Hoofdstuk 3 Apparaatbeheer

3.1 Apparaten activeren

Voor de inactieve apparaten moet je een wachtwoord aanmaken om ze te activeren voordat ze kunnen worden toegevoegd aan de software en correct kunnen werken.

Voordat u begint

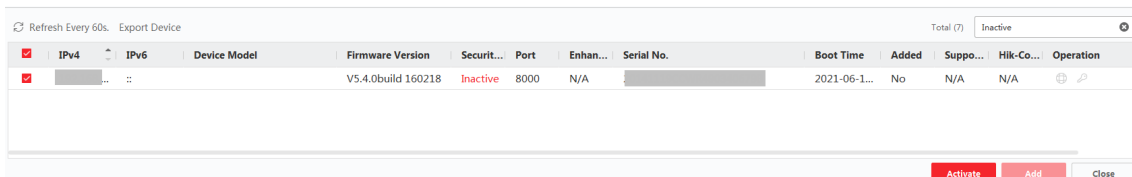
Zorg ervoor dat het te activeren apparaat is aangesloten op het netwerk en zich op hetzelfde subnet bevindt als de pc waarop de client draait.

Stappen

Opmerking

Deze functie moet worden ondersteund door het apparaat.

1. Ga naar de pagina Apparaatbeheer.
2. Klik op **Apparaat** boven in het rechterpaneel.
3. Klik op **Online apparaat** om de lijst met online apparaten onder aan de pagina weer te geven. De gezochte online apparaten worden weergegeven in de lijst.
4. Controleer de apparaatstatus (weergegeven in de kolom **Beveiligingsniveau**) en selecteer een inactief apparaat.



IPV4	IPV6	Device Model	Firmware Version	Securit...	Port	Enhan...	Serial No.	Boot Time	Added	Suppo...	Hik-Co...	Operation
...	::		V5.4.0build 160218	Inactive	8000	N/A		2021-06-1...	No	N/A	N/A	

Afbeelding 3-1 Inactieve apparaten online

5. Klik op **Activeren** om het dialoogvenster Activering te openen.
6. Maak een wachtwoord aan in het wachtwoordveld en bevestig het wachtwoord.

Let op

De wachtwoordsterkte van het apparaat kan automatisch worden gecontroleerd. We raden u ten eerste aan het wachtwoord van uw eigen keuze te wijzigen (met minimaal 8 tekens, waaronder ten minste drie soorten uit de volgende categorieën: hoofdletters, kleine letters, cijfers en speciale tekens) om de beveiliging van uw product te verbeteren. En we raden u aan uw wachtwoord regelmatig te wijzigen, vooral in het hoogbeveiligde systeem kan een maandelijkse of wekelijkse wijziging van het wachtwoord uw product beter beschermen. De juiste configuratie van alle wachtwoorden en andere beveiligingsinstellingen is de verantwoordelijkheid van de installateur en/of eindgebruiker.


Opmerking

Voor het NVR-apparaat moet u een wachtwoord aanmaken in het veld **Standaardwachtwoord netwerkcamera's** en het wachtwoord bevestigen voor het activeren van netwerkcamera('s) die zijn aangesloten op de NVR.

7. Optioneel: Schakel ABUS Link Station service in bij het activeren van het apparaat als het apparaat dit ondersteunt.
 - 1) Vink **Cloud P2P inschakelen** aan om het dialoogvenster Opmerking te openen.
 - 2) Maak een verificatiecode aan en bevestig de verificatiecode.
 - 3) Klik op **Servicevoorwaarden** en **Privacybeleid** om de vereisten te lezen.
 - 4) Klik op **OK** om de ABUS Link Station-service in te schakelen.
 8. Klik op **OK** om het apparaat te activeren.
-

Opmerking

Als het apparaat het resetten van het wachtwoord via de gereserveerde e-mail, beveiligingsvraag of GUID ondersteunt, kunt u deze configureren na het activeren van het apparaat.

9. Optioneel: Klik op  in de kolom Werking om de netwerkinformatie (inclusief IP-adres, poortnummer, gateway, enz.) voor het online apparaat te bewerken.

3.2 Apparaat toevoegen

De client biedt verschillende modi voor het toevoegen van apparaten, waaronder IP/domein, IP-segment en ABUS Link Station. De client ondersteunt ook het importeren van meerdere apparaten

in een batch wanneer er veel apparaten moeten worden toegevoegd.

3.2.1 Eén of meerdere online apparaten toevoegen

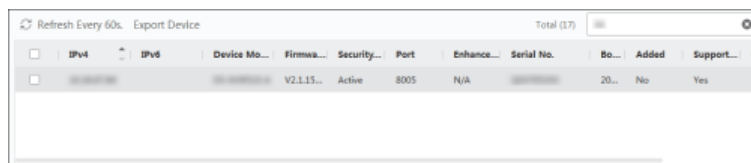
De client kan online apparaten detecteren die zich in hetzelfde netwerk bevinden als de pc waarop de client draait. Je kunt een gedetecteerd online apparaat dat wordt weergegeven in de lijst met online apparaten selecteren en toevoegen aan de client. Voor gedetecteerde online apparaten die dezelfde gebruikersnaam en wachtwoord delen, kun je ze in een batch aan de client toevoegen.

Voordat u begint

- De toe te voegen apparaten bevinden zich in hetzelfde netwerk als de pc waarop de client draait.
- De toe te voegen apparaten zijn geactiveerd.

Stappen

1. Klik op **Apparaatbeheer** → **Apparaat** → **Apparaat**.
2. Klik op **Online apparaat** om het gedeelte Online apparaat weer te geven.
De gezochte online apparaten worden weergegeven in de lijst.



<input type="checkbox"/>	IPv4	IPv6	Device Mo...	Firmwa...	Security...	Port	Enhance...	Serial No.	Bo...	Added	Support...	G
<input type="checkbox"/>				V2.1.15...	Active	8005	N/A		20...	No	Yes	Er

Afbeelding 3-2 Online apparaat

3. Schakel in het gedeelte **Online apparaat** een of meer online apparaten in en klik op **Toevoegen** om het venster voor het toevoegen van apparaten te openen.

Add [X]

Name

IP Address

Transmission Encryption...

Port

User Name

Password

Synchronize Time

Import to Group

i Set the device name as the group name and add all the channels connected to the device to the group.

Add **Cancel**

Afbeelding 3-3 Eén online apparaat toevoegen

Add [X]

User Name

Password

Synchronize Time

Import to Group

i Set the device name as the group name and add all the channels connected to the device to the group.

Add **Cancel**

Figuur 3-4 Meerdere online apparaten toevoegen

4. Voer de vereiste informatie in.

Naam

Voer een beschrijvende naam in voor het apparaat.

IP-adres

Voer het IP-adres van het apparaat in. Het IP-adres van het apparaat wordt automatisch verkregen in deze toevoegmodus.

Haven

Je kunt het poortnummer aanpassen. Het poortnummer van het apparaat wordt automatisch verkregen in deze toevoegmodus.

Opmerking

Voor sommige apparaattypes kunt u **80** invoeren als poortnummer. Deze functie moet ondersteund worden door het apparaat.

Gebruikersnaam

Standaard is de gebruikersnaam **admin** voor TVVR/HDCC/NVR en **installer** voor IPC's.

Wachtwoord

Voer het wachtwoord van het apparaat in.

Let op

De wachtwoordsterkte van het apparaat kan automatisch worden gecontroleerd. We raden u ten eerste aan het wachtwoord van uw eigen keuze te wijzigen (met minimaal 8 tekens, waaronder ten minste drie soorten uit de volgende categorieën: hoofdletters, kleine letters, cijfers en speciale tekens) om de beveiliging van uw product te verbeteren. En we raden u aan uw wachtwoord regelmatig te wijzigen, vooral in het hoogbeveiligde systeem kan een maandelijkse of wekelijkse wijziging van het wachtwoord uw product beter beschermen. De juiste configuratie van alle wachtwoorden en andere beveiligingsinstellingen is de verantwoordelijkheid van de installateur en/of eindgebruiker.

5. Optioneel: Vink **Transmissie-encryptie (TLS)** aan om transmissie-encryptie met behulp van het TLS-protocol (Transport Layer Security) in te schakelen voor beveiligingsdoeleinden.
-

Opmerking

- Deze functie moet worden ondersteund door het apparaat.
 - Als u Certificaatverificatie heeft ingeschakeld, moet u klikken op **Certificaatdirectory openen** om de standaardmap te openen en het certificaatbestand dat van het apparaat is geëxporteerd naar deze standaardmap te kopiëren om de beveiliging te versterken. Zie **Certificaatverificatie voor transmissie-encryptie** voor meer informatie over het inschakelen van certificaatverificatie.
 - U kunt inloggen op het apparaat om het certificaatbestand op te halen via de webbrowser.
-

6. Vink **Tijd synchroniseren** aan om de tijd van het apparaat te synchroniseren met de PC waarop de client draait nadat het apparaat aan de client is toegevoegd.
7. Optioneel: Vink **Importeren naar groep** aan om een groep te maken met de apparaatnaam en alle kanalen van het apparaat naar deze groep te importeren.
-

Voorbeeld

Voor codeerapparaten worden de codeerkanalen en alarmingangen/uitgangen geïmporteerd in deze groep.

Voor toegangscontroleapparaten worden de toegangspunten, alarmingangen/uitgangen en codeerkanalen (indien aanwezig) geïmporteerd in deze groep.

8. Klik op **Toevoegen**.
9. Optioneel: Klik op **Apparaat exporteren**, selecteer het opslagpad en het apparaattype en klik op **OK** om de apparaatinformatie naar uw pc te exporteren.



Opmerking

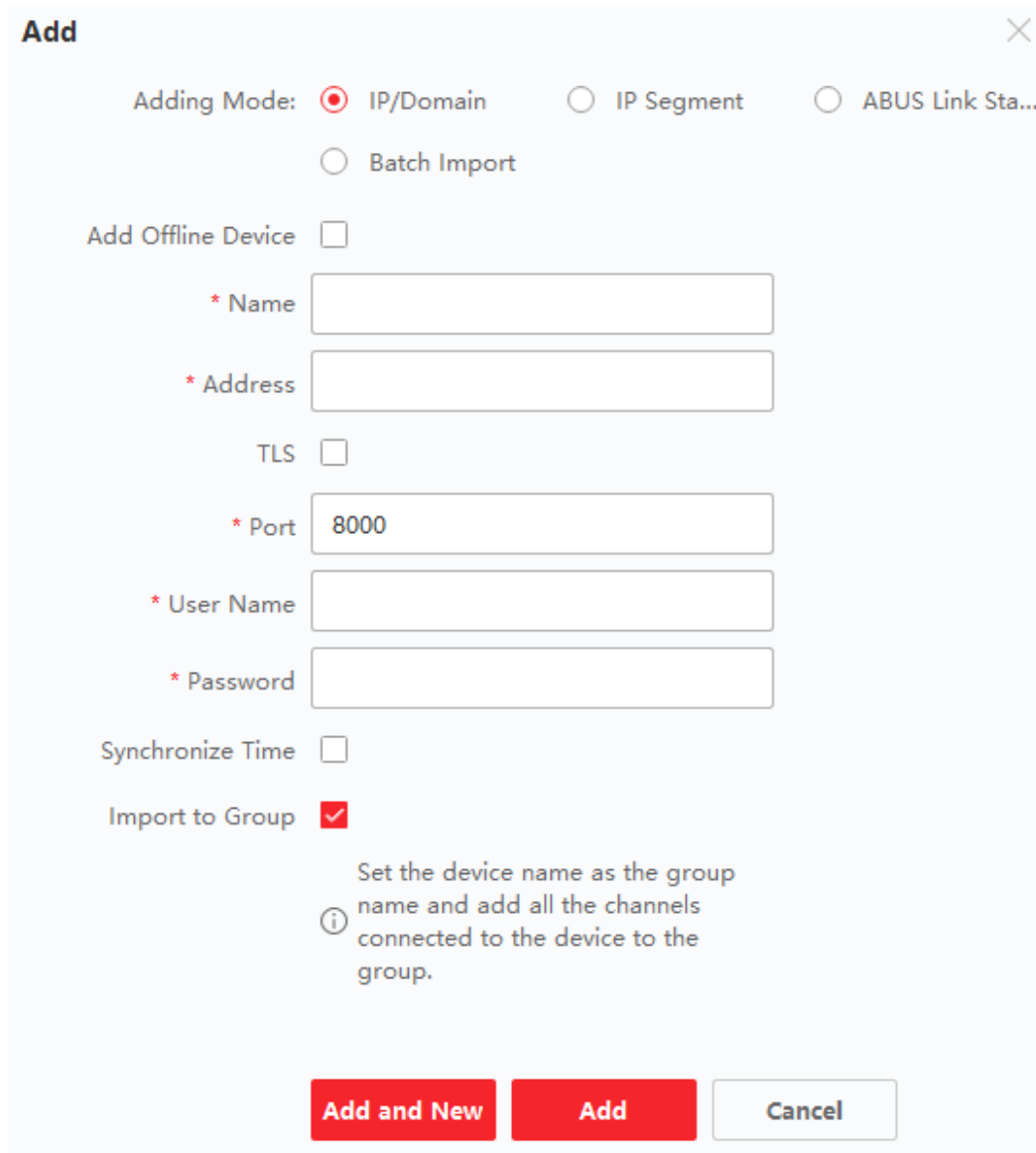
Momenteel ondersteunt het platform alleen het exporteren van informatie van video-intercomapparaten, waaronder deurstations, binnenstations en hoofdstations.

3.2.2 Apparaat toevoegen op IP-adres of domeinnaam

Als je het IP-adres of de domeinnaam van het toe te voegen apparaat weet, kun je apparaten toevoegen aan de client door het IP-adres (of de domeinnaam), de gebruikersnaam, het wachtwoord, enz. op te geven.

Stappen

1. Ga naar de module Apparaatbeheer.
2. Klik op het tabblad **Apparaat** boven in het rechterpaneel.
De toegevoegde apparaten worden weergegeven in het rechterpaneel.



Add

Adding Mode: IP/Domain IP Segment ABUS Link Sta...

Batch Import

Add Offline Device

* Name

* Address

TLS

* Port

* User Name

* Password

Synchronize Time

Import to Group

Set the device name as the group name and add all the channels connected to the device to the group.

Add and New **Add** Cancel

Afbeelding 3-5 Apparaat toevoegen op IP-adres of domeinnaam

3. Klik op **Toevoegen** om het venster Toevoegen te openen en selecteer vervolgens **IP/Domein** als de toevoegmodus.
4. Voer de vereiste informatie in.

Naam

Maak een beschrijvende naam voor het apparaat. Je kunt bijvoorbeeld een bijnaam gebruiken die de locatie of functie van het apparaat weergeeft.

Adres

Het IP-adres of de domeinnaam van het apparaat.

Haven

De toe te voegen apparaten hebben hetzelfde poortnummer. De standaardwaarde is **8000**.

Opmerking

Voor sommige apparaattypes kunt u **80** invoeren als poortnummer. Deze functie moet ondersteund worden door het apparaat.

Gebruikersnaam

Voer de gebruikersnaam van het apparaat in. Standaard is de gebruikersnaam **admin**.

Wachtwoord

Voer het wachtwoord van het apparaat in.

Let op

De wachtwoordsterkte van het apparaat kan automatisch worden gecontroleerd. We raden u ten eerste aan het wachtwoord van uw eigen keuze te wijzigen (met minimaal 8 tekens, waaronder ten minste drie soorten uit de volgende categorieën: hoofdletters, kleine letters, cijfers en speciale tekens) om de beveiliging van uw product te verbeteren. En we raden u aan uw wachtwoord regelmatig te wijzigen, vooral in het hoogbeveiligde systeem kan een maandelijkse of wekelijkse wijziging van het wachtwoord uw product beter beschermen. De juiste configuratie van alle wachtwoorden en andere beveiligingsinstellingen is de verantwoordelijkheid van de installateur en/of eindgebruiker.

5. Optioneel: Voeg de offline apparaten toe.

- 1) Vink **Offline apparaat toevoegen** aan.
 - 2) Voer de vereiste informatie in, waaronder het kanaalnummer van het apparaat en het ingangsnummer van het alarm.
-

Opmerking

Nadat het offline apparaat aan de client is toegevoegd, wordt de netwerkstatus van het apparaat weergegeven als "Offline"; wanneer het apparaat online komt, verandert de netwerkstatus van het apparaat in "Online" en maakt de client automatisch verbinding.

6. Optioneel: Vink **Transmissie-encryptie (TLS)** aan om transmissie-encryptie met behulp van het TLS-protocol (Transport Layer Security) in te schakelen voor beveiligingsdoeleinden.

Opmerking

- Deze functie moet worden ondersteund door het apparaat.
 - Als u certificaatverificatie hebt ingeschakeld, moet u klikken op **Certificaatdirectory openen** om de standaardmap te openen en het certificaatbestand dat van het apparaat is geëxporteerd naar deze standaardmap te kopiëren om de beveiliging te versterken. Zie **Certificaatverificatie voor transmissie-encryptie** voor meer informatie over het inschakelen van certificaatverificatie.
 - U kunt inloggen op het apparaat om het certificaatbestand op te halen via de webbrowser.
-







7. Vink **Tijd synchroniseren** aan om de tijd van het apparaat te synchroniseren met de PC waarop de client draait nadat het apparaat aan de client is toegevoegd.
8. Optioneel: Vink **Importeren naar groep** aan om een groep te maken met de apparaatnaam en alle kanalen van het apparaat naar deze groep te importeren.

Voorbeeld

Voor codeerapparaten worden de codeerkanalen en alarmingangen/uitgangen geïmporteerd in deze groep.

Voor toegangscontroleapparaten worden de toegangspunten, alarmingangen/uitgangen en codeerkanalen (indien aanwezig) geïmporteerd in deze groep.

9. Voltooi het toevoegen van het apparaat.
 - Klik op **Toevoegen** om het apparaat toe te voegen en terug te keren naar de pagina met de apparatenlijst.
 - Klik op **Toevoegen en Nieuw** om de instellingen op te slaan en door te gaan met het toevoegen van andere apparaten.
10. Optioneel: Voer de volgende bewerking(en) uit.

Configuratie op afstand	Klik op de pagina met de apparatenlijst op  in de kolom Bediening om een apparaat op afstand te configureren. De  staat in de meest rechtse kolom van de pagina Apparaat. Raadpleeg de gebruikershandleiding van het apparaat voor meer informatie.
Apparaatstatus	Klik op  in de kolom Bediening om de apparaatstatus te bekijken, inclusief camera's, opnamestatus, signaalstatus, hardwarestatus, enz.
Apparaatinformatie bewerken	Klik op  in de kolom Werking om de apparaatinformatie te bewerken, zoals IP-adres, gebruikersnaam en wachtwoord.
Controleer online gebruiker	Klik op  in de Operation kolom om de online gebruikers te controleren die toegang hebben tot het apparaat, zoals gebruikersnaam, gebruikerstype, IP-adres van de gebruiker en aanmeldtijd.
Vernieuw	Klik op  in de kolom Werking om de meest recente apparaatinformatie te krijgen.
Apparaat verwijderen	Selecteer een of meerdere apparaten en klik op Verwijderen om de geselecteerde apparaten van de client te verwijderen.

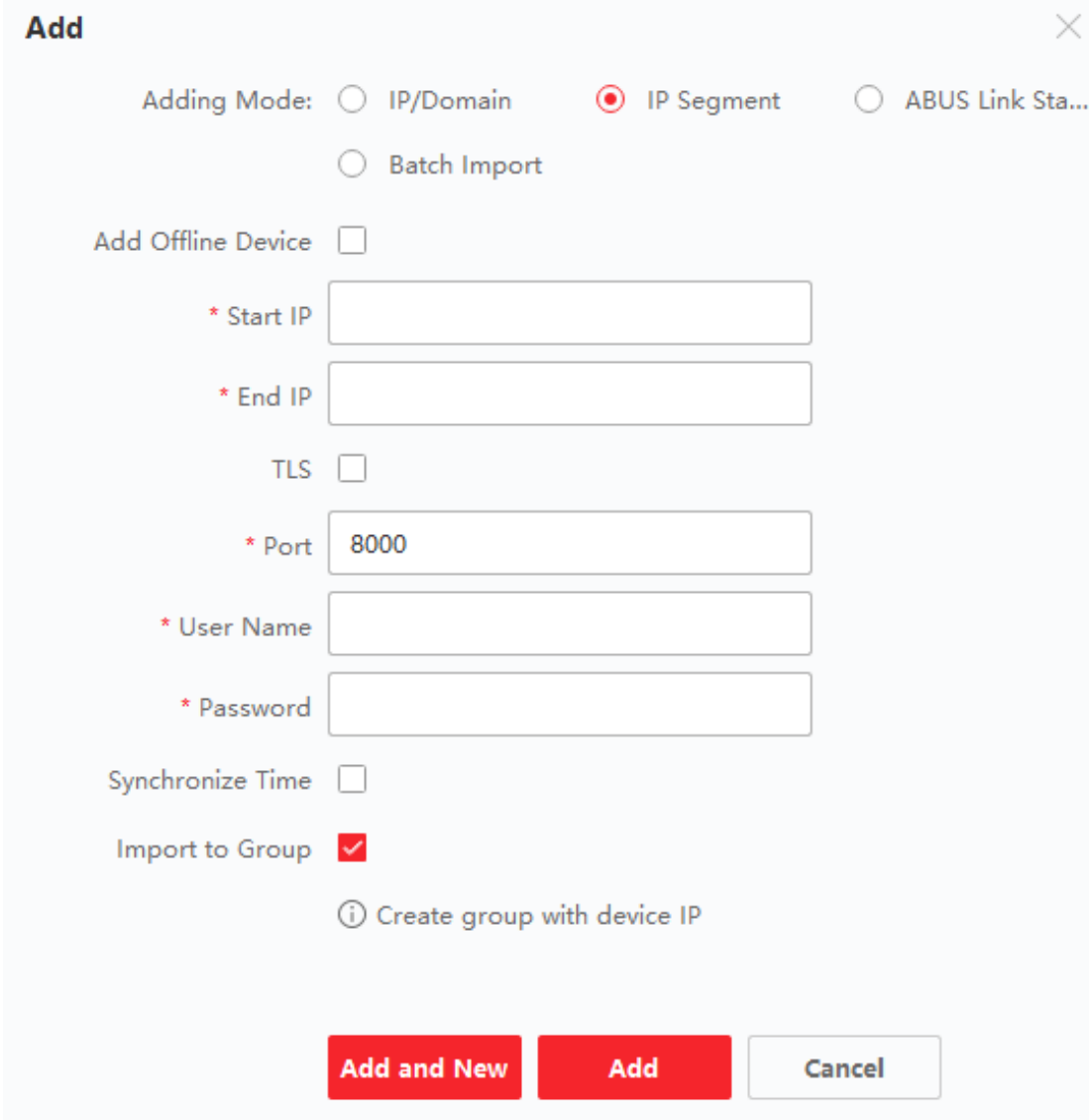
3.2.3 Apparaten toevoegen per IP-segment

Als de apparaten hetzelfde poortnummer, gebruikersnaam en wachtwoord hebben en hun IP-adressen zich in hetzelfde IP-segment bevinden, kun je ze toevoegen aan de client door het begin-IP-adres en het eind-IP-adres, poortnummer, gebruikersnaam, wachtwoord, enz. van de apparaten

op te geven.

Stappen

1. Klik in het paneel Onderhoud en beheer aan de rechterkant van de client op **Apparaatbeheer**.
2. Klik op het tabblad **Apparaat** bovenaan in het linkerpaneel.
De toegevoegde apparaten worden weergegeven in het rechterpaneel.
3. Klik op **Toevoegen** om het venster Toevoegen te openen.



Add ✕

Adding Mode: IP/Domain IP Segment ABUS Link Sta...

Batch Import

Add Offline Device

* Start IP

* End IP

TLS

* Port

* User Name

* Password

Synchronize Time

Import to Group

ⓘ Create group with device IP

Add and New **Add** Cancel

Afbeelding 3-6 Apparaat toevoegen op IP-segment

4. Selecteer **IP Segment** als de toevoegmodus.
5. Voer de vereiste informatie in.

Start IP

Voer een start-IP-adres in.

Einde IP

Voer een eind-IP-adres in hetzelfde netwerksegment in als de start-IP.

Haven

Voer het poortnummer van het apparaat in. De standaardwaarde is **8000**.



Opmerking

Voor sommige apparaattypes kunt u **80** invoeren als poortnummer. Deze functie moet ondersteund worden door het apparaat.

Gebruikersnaam

Standaard is de gebruikersnaam **admin**.

Wachtwoord

Voer het wachtwoord van het apparaat in.



Let op

De wachtwoordsterkte van het apparaat kan automatisch worden gecontroleerd. We raden u ten zeerste aan het wachtwoord van uw eigen keuze te wijzigen (met minimaal 8 tekens, waaronder ten minste drie soorten uit de volgende categorieën: hoofdletters, kleine letters, cijfers en speciale tekens) om de beveiliging van uw product te verbeteren. En we raden u aan uw wachtwoord regelmatig te wijzigen, vooral in het hoogbeveiligde systeem kan een maandelijkse of wekelijkse wijziging van het wachtwoord uw product beter beschermen. De juiste configuratie van alle wachtwoorden en andere beveiligingsinstellingen is de verantwoordelijkheid van de installateur en/of eindgebruiker.

6. Optioneel: Voeg de offline apparaten toe.

- 1) Vink **Offline apparaat toevoegen** aan.
- 2) Voer de vereiste informatie in, waaronder het kanaalnummer van het apparaat en het ingangsnummer van het alarm.



Opmerking

Nadat het offline apparaat aan de client is toegevoegd, wordt de netwerkstatus van het apparaat weergegeven als "Offline"; wanneer het apparaat online komt, verandert de netwerkstatus van het apparaat in "Online" en maakt de client automatisch verbinding.

7. Optioneel: Vink **Transmission Encryption (TLS)** aan om transmissie-encryptie met behulp van TLS (Transport Layer Security) protocol in te schakelen voor beveiligingsdoeleinden .









Opmerking

- Deze functie moet worden ondersteund door het apparaat.
- Als u certificaatverificatie hebt ingeschakeld, moet u op **Certificaatmap openen** klikken om de standaardmap te openen en het certificaatbestand dat van het apparaat is geëxporteerd naar deze standaardmap te kopiëren om de beveiliging te versterken. Zie [Certificaatverificatie voor transmissie-encryptie](#) voor meer informatie over het inschakelen van

certificaatverificatie.

- U kunt inloggen op het apparaat om het certificaatbestand op te halen via de webbrowser.
-

8. Vink **Tijd synchroniseren** aan om de tijd van het apparaat te synchroniseren met de PC waarop de client draait nadat het apparaat aan de client is toegevoegd.
9. Optioneel: Vink **Importeren naar groep** aan om een groep te maken met de apparaatnaam en alle kanalen van het apparaat naar de groep te importeren.
10. Voltooi het toevoegen van het apparaat.
 - Klik op **Toevoegen** om het apparaat toe te voegen en terug te keren naar de pagina met de apparatenlijst.
 - Klik op **Toevoegen en Nieuw** om de instellingen op te slaan en door te gaan met het toevoegen van andere apparaten.
11. Optioneel: Voer de volgende bewerking(en) uit.

Configuratie op afstand	Klik op de pagina met de apparatenlijst op  in de kolom Bediening om een apparaat op afstand te configureren. De  staat in de meest rechtse kolom van de pagina Apparaat. Raadpleeg de gebruikershandleiding van het apparaat voor meer informatie.
Apparaatstatus	Klik op  in de kolom Bediening om de apparaatstatus te bekijken, inclusief camera's, opnamestatus, signaalstatus, hardwarestatus, enz.
Apparaatinformatie bewerken	Klik op  in de kolom Werking om de apparaatinformatie te bewerken, zoals IP-adres, gebruikersnaam en wachtwoord.
Controleer online gebruiker	Klik op  in de Operation kolom om de online gebruikers te controleren die toegang hebben tot het apparaat, zoals gebruikersnaam, gebruikerstype, IP-adres van de gebruiker en aanmeldtijd.
Vernieuw	Klik op  in de kolom Werking om de meest recente apparaatinformatie te krijgen.
Apparaat verwijderen	Selecteer een of meerdere apparaten en klik op Verwijderen om de geselecteerde apparaten van de client te verwijderen.

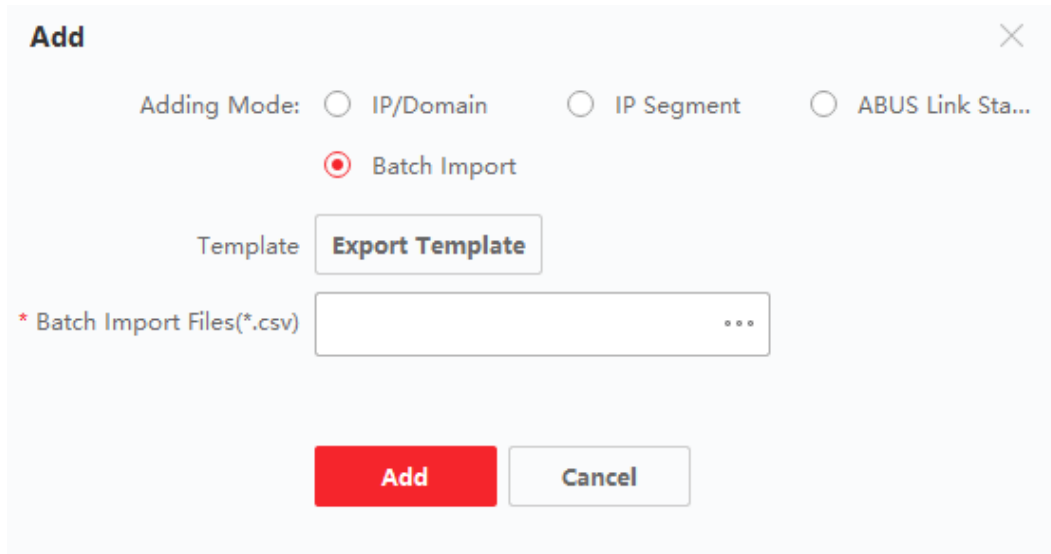
3.2.4 Apparaten importeren in een batch

Je kunt meerdere apparaten in een batch aan de client toevoegen door de apparaatparameters in een vooraf gedefinieerd CSV-bestand in te voeren.

Stappen

1. Ga naar de module Apparaatbeheer.
2. Klik op het tabblad **Apparaat** boven in het rechterpaneel.

- Klik op **Toevoegen** om het venster Toevoegen te openen en selecteer vervolgens **Batch importeren** als invoegmodus.



Afbeelding 3-7 Apparaten toevoegen in een batch

- Klik op **Sjabloon exporteren** en sla de vooraf gedefinieerde sjabloon (CSV-bestand) op uw pc op.
- Open het geëxporteerde sjabloonbestand en voer de vereiste informatie van de apparaten die moeten worden toegevoegd in de overeenkomstige kolom in.

Opmerking

Raadpleeg de introducties in de sjabloon voor een gedetailleerde beschrijving van de verplichte velden.

Modus toevoegen

Voer **0** of **1** of **2** in.

Adres

Bewerk het adres van het apparaat.

Haven

Voer het poortnummer van het apparaat in. Het standaard poortnummer is **8000**.

Gebruikersnaam

Voer de gebruikersnaam van het apparaat in. Standaard is de gebruikersnaam **admin**.

Wachtwoord

Voer het wachtwoord van het apparaat in.

Let op

De wachtwoordsterkte van het apparaat kan automatisch worden gecontroleerd. We raden u ten zeerste aan het wachtwoord van uw eigen keuze te wijzigen (met minimaal 8 tekens, waaronder ten minste drie soorten uit de volgende categorieën: hoofdletters, kleine letters, cijfers en speciale tekens) om de beveiliging van uw product te verbeteren. En we raden u aan uw wachtwoord regelmatig te wijzigen, vooral in het hoogbeveiligde systeem kan een maandelijkse of wekelijkse wijziging van het wachtwoord uw product beter beschermen. De juiste configuratie van alle wachtwoorden en andere beveiligingsinstellingen is de verantwoordelijkheid van de installateur en/of eindgebruiker.

Offline apparaat toevoegen

Voer **1** in om een offline apparaat toe te voegen.

Nadat het offline apparaat aan de client is toegevoegd, zal de netwerkstatus van het apparaat worden weergegeven als "Offline"; wanneer het apparaat online komt, zal de netwerkstatus van het apparaat veranderen in "Online" en zal de client het automatisch verbinden. Voer **0** in om het toevoegen van een offline apparaat uit te schakelen.

Importeren naar groep


Voer **1** in om een groep te maken met de naam van het apparaat. Alle kanalen van het apparaat worden standaard geïmporteerd in de corresponderende groep. Voer **0** in om deze functie uit te schakelen.

Kanaalnummer



Als u **Offline apparaat toevoegen** inschakelt, voert u het kanaalnummer van het apparaat in. Als u **Offline apparaat toevoegen** uitschakelt, is dit veld niet vereist.

Alarmingang Nummer


Als u **Offline apparaat toevoegen** inschakelt, voert u het alarmingangnummer van het apparaat in. Als u **Offline apparaat toevoegen** uitschakelt, is dit veld niet vereist.

6. Klik op  en selecteer het sjabloonbestand.
7. Klik op **Toevoegen** om de apparaten te importeren.
8. Optioneel: Voer de volgende bewerking(en) uit.


Configuratie op afstand

Klik op de pagina met de apparatenlijst op  in de kolom Bediening om een apparaat op afstand te configureren. De  staat in de meest rechtse kolom van de pagina Apparaat. Raadpleeg de gebruikershandleiding van het apparaat voor meer informatie.

Apparaatstatus


Klik op  in de kolom Bediening om de apparaatstatus te bekijken, inclusief camera's, opnamestatus, signaalstatus, hardwarestatus, enz.

Apparaatinformatie bewerken

Klik op  in de kolom Werking om de apparaatinformatie te bewerken, zoals IP-adres, gebruikersnaam en wachtwoord.

Controleer online

Klik op  in de Operation kolom om de online gebruikers te

gebruiker	controleren die toegang hebben tot het apparaat, zoals gebruikersnaam, gebruikerstype, IP-adres van de gebruiker en aanmeldtijd.
Vernieuw	Klik op  in de kolom Werking om de meest recente apparaatinformatie te krijgen.
Apparaat verwijderen	Selecteer een of meerdere apparaten en klik op Verwijderen om de geselecteerde apparaten van de client te verwijderen.


3.3 Wachtwoord van apparaat herstellen/herstellen

Als je het wachtwoord van de gedetecteerde online apparaten bent vergeten, kun je het standaardwachtwoord van het apparaat herstellen of het wachtwoord van het apparaat opnieuw instellen via de client.

3.3.1 Wachtwoord voor apparaat opnieuw instellen

Als je het wachtwoord van de gedetecteerde online apparaten bent vergeten, kun je het wachtwoord van het apparaat opnieuw instellen via de client.

Stappen

1. Open de pagina Apparaatbeheer.
2. Klik op het tabblad **Apparaat** boven in het rechterpaneel.
3. Klik op **Online apparaat** om het gedeelte Online apparaat weer te geven.
Alle online apparaten die hetzelfde subnet delen, worden in de lijst weergegeven.
4. Selecteer het apparaat in de lijst en klik op  in de kolom Werking.
5. Reset het wachtwoord van het apparaat.
 - Klik op **Export** om het apparaatbestand op je pc op te slaan en stuur het bestand vervolgens naar onze technische ondersteuning.

Opmerking

Neem voor de volgende handelingen voor het resetten van het wachtwoord contact op met onze technische ondersteuning.

- Klik op **Generate** om het QR Code venster te openen en klik op **Download** om de QR code op te slaan op je PC. Je kunt ook een foto maken van de QR code om deze op je telefoon op te slaan. Stuur de foto naar onze technische ondersteuning.
-

Opmerking

Neem voor de volgende handelingen voor het resetten van het wachtwoord contact op met onze technische ondersteuning.

- Selecteer de Veilige modus volgens de werkelijke behoeften.

 **Opmerking**

Neem voor de volgende handelingen voor het resetten van het wachtwoord contact op met onze technische ondersteuning.


 **Let op**

De wachtwoordsterkte van het apparaat kan automatisch worden gecontroleerd. We raden u ten zeerste aan het wachtwoord van uw eigen keuze te wijzigen (met minimaal 8 tekens, waaronder ten minste drie soorten uit de volgende categorieën: hoofdletters, kleine letters, cijfers en speciale tekens) om de beveiliging van uw product te verbeteren. En we raden u aan uw wachtwoord regelmatig te wijzigen, vooral in het hoogbeveiligde systeem kan een maandelijkse of wekelijkse wijziging van het wachtwoord uw product beter beschermen. De juiste configuratie van alle wachtwoorden en andere beveiligingsinstellingen is de verantwoordelijkheid van de installateur en/of eindgebruiker.

3.3.2 Het standaardwachtwoord van het apparaat herstellen

Als je het wachtwoord van de gedetecteerde online apparaten bent vergeten, kun je hun standaardwachtwoord herstellen via de client.

Stappen

1. Open de pagina Apparaatbeheer.
2. Klik op het tabblad **Apparaat** boven in het rechterpaneel.
3. Klik op **Online apparaat** om het gedeelte Online apparaat onder aan de pagina weer te geven. Alle online apparaten die hetzelfde subnet delen, worden in de lijst weergegeven.
4. Selecteer een apparaat en klik op  in de kolom Werking om het venster Wachtwoord opnieuw instellen te openen.
5. Herstel het wachtwoord van het apparaat.
 - Voer de beveiligingscode in en herstel het standaardwachtwoord van het geselecteerde apparaat.

 **Opmerking**

Neem voor het verkrijgen van de beveiligingscode contact op met onze technische ondersteuning.

- Klik op **Export** om het apparaatbestand op je pc op te slaan en naar onze technische ondersteuning te sturen.
-

 **Opmerking**

Neem voor de volgende handelingen voor het resetten van het wachtwoord contact op met onze technische ondersteuning.

Wat nu te doen

Het standaardwachtwoord (12345) voor de beheerdersaccount is alleen bedoeld om de eerste keer mee in te loggen. U moet dit standaardwachtwoord wijzigen om u beter te beschermen tegen veiligheidsrisico's, zoals onbevoegde toegang door anderen tot het product, waardoor het product niet goed meer kan functioneren en/of andere ongewenste gevolgen kan hebben.



Let op

De wachtwoordsterkte van het apparaat kan automatisch worden gecontroleerd. We raden u ten zeerste aan het wachtwoord van uw eigen keuze te wijzigen (met minimaal 8 tekens, waaronder ten minste drie soorten uit de volgende categorieën: hoofdletters, kleine letters, cijfers en speciale tekens) om de beveiliging van uw product te verbeteren. En we raden u aan uw wachtwoord regelmatig te wijzigen, vooral in het hoogbeveiligde systeem kan een maandelijks of wekelijkse wijziging van het wachtwoord uw product beter beschermen.

De juiste configuratie van alle wachtwoorden en andere beveiligingsinstellingen is de verantwoordelijkheid van de installateur en/of eindgebruiker.

3.4 Firmwareversie van apparaat upgraden

Als er een nieuwe firmwareversie beschikbaar is voor het toegevoegde apparaat, kun je de firmwareversie upgraden via de client.



Opmerking

- Het apparaat moet deze functie ondersteunen.
 - U kunt de upgrademodus configureren in Systeemconfiguratie. Zie [Algemene parameters instellen](#) voor meer informatie.
-

Ga naar de module Apparaatbeheer en klik op het tabblad **Apparaat** om de apparatenlijst weer te geven.

Voer de volgende handelingen uit volgens de verschillende upgrademodi.

uitschakelen

Op het paneel Device for Management, als er een nieuwe firmwareversie beschikbaar is, verandert de status in de kolom Firmware Upgrade van het apparaat in **Upgradeable**.

Selecteer het apparaat dat geüpgraded kan worden en klik op **Upgrade** om het upgraden van de apparaatfirmware te starten.



Opmerking

De voortgang van de upgrade wordt weergegeven. Wanneer de upgrade voltooid is, verandert de status in de kolom Firmware upgrade van het apparaat in **Upgraded**.

Prompt Me If Downloaden en Upgraden

Als er een nieuwe firmwareversie beschikbaar is, verschijnt er een promptvenster. Klik op **Upgrade All** om het downloaden en upgraden te starten.

Downloaden en vraag me om een upgrade

Er verschijnt een dialoogvenster waarin je kunt selecteren of je wilt upgraden na het downloaden van het pakket met de nieuwe versie. Klik op **Upgrade All** om het upgraden van de apparaatfirmware te starten.

Opmerking

Nadat je op **Upgrade All hebt** geklikt, verschijnt er een prompt waarmee je de details kunt bekijken. Als u niet op de pagina Apparaatbeheer bent, klikt u op **Details weergeven** om naar de pagina Apparaatbeheer te gaan; als u op de pagina Apparaatbeheer bent, sluit u de prompt.

Upgradestatus

Op de pagina Apparaatbeheer wordt de volgende upgrade-status weergegeven in de kolom Firmware-upgrade.


Geen versie beschikbaar

Geen nieuwe firmwareversie beschikbaar.

Upgradebaar

Er is een nieuwe firmwareversie beschikbaar.

Opmerking

Beweeg de cursor op  om de huidige versie, de laatste versie en de upgrade-inhoud van de firmwareversie te bekijken.

Wachten

Het apparaat wacht op een upgrade.

Downloaden

De client downloadt het pakket met de nieuwe firmwareversie.

Upgraden

De firmware van het apparaat wordt geüpgraded.

Opgewaardeerd

Beweeg de cursor over **Upgraded** om de versie na het upgraden weer te geven.

Upgraden mislukt









Wanneer de upgrade mislukt, verschijnt er een prompt om de details te bekijken. Als u niet op de pagina Apparaatbeheer bent, klikt u op **Details weergeven** om naar de pagina Apparaatbeheer te gaan; als u op de pagina Apparaatbeheer bent, sluit u de prompt. Beweeg de

cursor over **Upgraden mislukt** om de foutdetails weer te geven en klik op **Opnieuw upgraden** om het opnieuw te proberen.

3.5 Toegevoegde apparaten beheren

Nadat u apparaten hebt toegevoegd aan de apparatenlijst, kunt u de toegevoegde apparaten beheren, waaronder apparaatparameters bewerken, externe configuratie, apparaatstatus bekijken, enz.

Tabel 3-1 Toegevoegde apparaten beheren

Apparaat bewerken	Klik op  om apparaatinformatie te bewerken, zoals apparaatnaam, adres, gebruikersnaam, wachtwoord, enz.
Apparaat verwijderen	Vink een of meer apparaten aan en klik op Verwijderen om de geselecteerde apparaten te verwijderen.
Configuratie op afstand	Klik op de pagina met de apparatenlijst op  in de kolom Bediening om een apparaat op afstand te configureren. De  staat in de meest rechtse kolom van de pagina Apparaat. Raadpleeg de gebruikershandleiding van het apparaat voor meer informatie.
Apparaatstatus weergeven	<p>Klik op  om de apparaatstatus te bekijken, inclusief camera's, opnamestatus, signaalstatus, hardwarestatus, enz.</p> <hr/> <p> Opmerking Voor verschillende apparaten ziet u verschillende informatie over de apparaatstatus.</p> <hr/>
Online gebruiker bekijken	Klik op  om de details te bekijken van online gebruikers die toegang hebben tot het apparaat, inclusief gebruikersnaam, gebruikerstype, IP-adres en aanmeldtijd.
Apparaatinformatie verversen	Klik op  om te verversen en de nieuwste apparaatinformatie te krijgen.
QR-code genereren	<p>Vink één of meer apparaten aan en klik op QR Code om een QR code te genereren van de toegevoegde apparaten. Je kunt apparaten toevoegen aan de Mobile Client door de QR-code te scannen.</p> <hr/> <p> Opmerking Apparaten toegevoegd door ISUP of ABUS Link Station kunnen geen QR code genereren.</p> <hr/>

Apparaat upgraden	Bekijk de apparaatstatus in de kolom Firmware-upgrade, vink een of meer apparaten aan die geüpgraded kunnen worden en klik op Apparaatfirmware upgraden om de geselecteerde apparaten te upgraden. Raadpleeg <u>Firmwareversie van apparaat upgraden</u> voor meer informatie.
Gebeurtenissen van apparaat ophalen	Vink één apparaat aan en klik op Haal gebeurtenissen op van apparaat om gebeurtenissen te synchroniseren. Raadpleeg <u>Haal gebeurtenissen op van apparaat</u> voor meer informatie.

3.6 Groepsmanagement

De client biedt groepen om de toegevoegde bronnen in verschillende groepen te beheren. Je kunt de resources groeperen in verschillende groepen op basis van de locaties van de resources.

Voorbeeld

Op de 1e verdieping zijn er bijvoorbeeld 64 camera's, 16 deuren, 64 alarmingangen en 16 alarmuitgangen. U kunt deze bronnen in één groep indelen (met de naam 1e verdieping) voor eenvoudig beheer. U kunt het livebeeld krijgen, de videobestanden afspelen, de deurstatus controleren en enkele andere bewerkingen van de apparaten uitvoeren nadat u de bronnen per groep hebt beheerd.

3.6.1 Groepsmiddelen

De client biedt twee methoden om een groep toe te voegen: een groep aanpassen of een groep maken op apparaatnaam. Na het aanpassen van een groep moet je handmatig bronnen importeren in deze groep. Na het maken van een groep op apparaatnaam worden de bronnen van het apparaat automatisch geïmporteerd in de groep. U kunt een methode kiezen om uw bronnen te groeperen op basis van uw werkelijke behoeften.

Stappen

1. Klik in het gebied Onderhoud en beheer op **Apparaatbeheer** → **Groep** om de pagina Groepsbeheer te openen.
2. Voeg een groep toe.
 - **Een groep aanpassen:** Klik op **Groep toevoegen** en maak een naam voor de nieuwe groep.
 - **Maak een groep aan op apparaatnaam:** Klik op **Create Group by Device Name** en selecteer een toegevoegd apparaat om een nieuwe groep aan te maken met de naam van het geselecteerde apparaat. Na het aanmaken van een groep op apparaatnaam worden de bronnen (zoals codeerkanalen, alarmingangen, alarmingangen en toegangspunten) van het apparaat automatisch geïmporteerd in de groep.

 **Opmerking**

- Er kunnen maximaal 256 groepen worden toegevoegd.
 - Je kunt meerdere groepen selecteren door de Shift- of Ctrl-toets op het toetsenbord ingedrukt te houden.
-


3. Nadat je een groep hebt toegevoegd, moet je bronnen importeren in de groep.

 **Opmerking**

Een bron kan aan verschillende groepen worden toegevoegd.

- 1) Selecteer het type bronnen dat geïmporteerd moet worden en klik op **Importeren**.
 - 2) Selecteer de bronnen die moeten worden geïmporteerd en klik op **Importeren** om alle geselecteerde bronnen in deze groep te importeren.
4. Optioneel: Voer na het toevoegen van een groep indien nodig een van de volgende bewerkingen uit.

**Bronnenlijst
uitbreiden of
inklappen**

Klik op  om de bronnenlijst in de groep uit te vouwen of in te klappen.

Zoeken

Voer het trefwoord in en klik op  om doelbronnen te zoeken.

**Hulpbron uit groep
verwijderen**

Selecteer resource(s) en klik op **Verwijderen** om de geselecteerde resource(s) uit de groep te verwijderen.

Bronnaam bijwerken

Je kunt alle namen van bronnen in een groep of in een kanaal bijwerken.

- Selecteer een groep en klik op **Resourcenaam bijwerken** om alle resourcenaamen in de geselecteerde groep bij te werken.
- Selecteer een kanaal in een groep en werk alle bronnamen in dit kanaal bij. Klik bijvoorbeeld op **Coderingskanalen** → **Cameranaam bijwerken** om alle cameranamen in coderingskanalen bij te werken.

 **Opmerking**

Deze functie moet worden ondersteund door het apparaat.

3.6.2 Bronparameters bewerken


Na het importeren van de bronnen naar de groep, kun je de bronparameters bewerken. Voor het coderingskanaal kunt u de kanaalnaam, het streamtype, het protocoltype, enz. bewerken. Voor toegangspunt kunt u de naam van het toegangspunt bewerken. Voor de alarmingang kunt u de

naam van de alarmingang bewerken. Hier nemen we het coderingskanaal als voorbeeld.

Voordat u begint

Importeer de bronnen om te groeperen.

Stappen

1. Ga naar de module Apparaatbeheer.
2. Klik op **Apparaatbeheer** → **Groep** om de pagina Groepsbeheer te openen.
Alle toegevoegde groepen worden links weergegeven.
3. Selecteer een groep in de groepslijst en klik op **Coderingskanaal**.
De in de groep geïmporteerde codeerkanalen worden weergegeven.
4. Klik op  in de kolom **Bewerking** om het venster Hulpbron bewerken te openen.
5. Bewerk de camera-informatie, inclusief de cameranaam, het streamtype, enz.

Videostream

Selecteer het gewenste streamtype voor liveweergave van de camera.

Opmerking

Je moet liveweergave opnieuw starten om effect te krijgen.

Type afspeelstroom

Selecteer het gewenste streamtype voor het afspelen van de camera.

Opmerking

- Dit veld wordt weergegeven als het apparaat dual-stream ondersteunt.
 - Je moet liveweergave opnieuw starten om effect te krijgen.
-

Type rotatie

Selecteer naar wens het rotatietype voor de liveweergave of het afspelen van de camera.

Protocoltype

Selecteer het transmissieprotocol voor de camera.

Opmerking

Je moet liveweergave opnieuw starten om effect te krijgen.

Streaming Protocol

Selecteer het protocol als RTSP of privé voor het verkrijgen van stream bij live weergave.

Opmerking

Je moet liveweergave opnieuw starten om effect te krijgen.

Kopiëren naar...

Kopieer de geconfigureerde parameters naar andere camera('s).

Vernieuw

Een nieuwe foto maken voor de live-weergave van de camera.

6. Klik op **OK** om de nieuwe instellingen op te slaan.

Hoofdstuk 4 ABUS Link Station

De clientsoftware ondersteunt ook het registreren van een ABUS Link Station account, het inloggen op uw ABUS Link Station account en het beheren van de apparaten die de ABUS Link Station service ondersteunen.

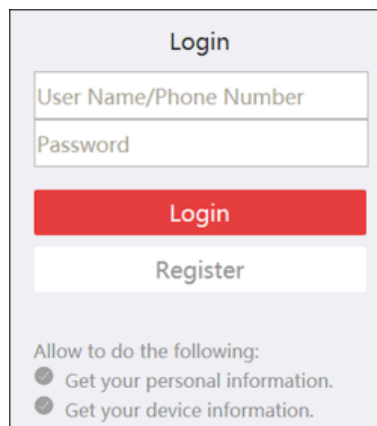
4.1 Een ABUS Link Station Account registreren

De client ondersteunt het registreren van een ABUS Link Station account om apparaten te beheren die de ABUS Link Station service ondersteunen.

Stappen

1. Ga naar de inlogpagina van ABUS Link Station.
 - Klik op **Aanmelden in** de rechterbovenhoek van de client.
 1. Klik op **Apparaatbeheer** → **Apparaat** om de pagina Apparaatbeheer te openen.
 2. Klik op **Toevoegen** om het paneel Apparaat toevoegen te openen.
 3. Selecteer **ABUS Link Station** als toevoegmodus.
 4. Klik op **Aanmelden**.

Het venster Aanmelden verschijnt.



Afbeelding 4-1 Aanmeldingsvenster

2. Klik op **Registreren** om het venster Account registreren te openen.
3. Voer de vereiste informatie in, zoals gebruikersnaam, wachtwoord, wachtwoord bevestigen en telefoonnummer/e-mailadres.

 **Let op**

De wachtwoordsterkte van het apparaat kan automatisch worden gecontroleerd. We raden u ten eerste aan het wachtwoord van uw eigen keuze te wijzigen (met minimaal 8 tekens, waaronder ten minste drie soorten uit de volgende categorieën: hoofdletters, kleine letters, cijfers en speciale tekens) om de beveiliging van uw product te verbeteren. En we raden u aan uw wachtwoord regelmatig te wijzigen, vooral in het hoogbeveiligde systeem kan een maandelijkse of wekelijkse wijziging van het wachtwoord uw product beter beschermen. De juiste configuratie van alle wachtwoorden en andere beveiligingsinstellingen is de verantwoordelijkheid van de installateur en/of eindgebruiker.

4. Klik op **Bericht verzenden** om een verificatiecode te ontvangen.
Het systeem stuurt een verificatiecode naar je telefoon of e-mail.
5. Voer de ontvangen verificatiecode in het tekstveld **Verificatiecode in**.
6. Vink aan dat **ik de Servicevoorwaarden Privacybeleid heb gelezen en ermee akkoord ga**.
7. Klik op **Registreren** om de registratie te voltooien.

4.2 Aanmelden bij ABUS Link Station Account

U kunt inloggen op een ABUS Link Station-account via de client om apparaten te bedienen die worden beheerd door een ABUS Link Station-account.

Voordat u begint

Registreer een ABUS Link Station account.

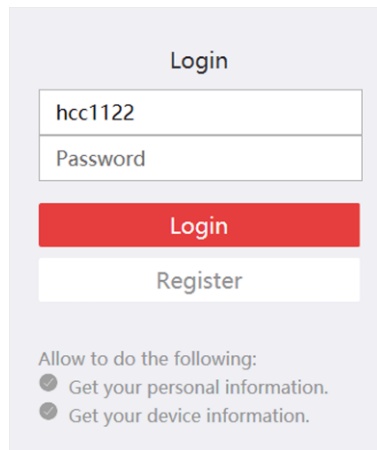
 **Opmerking**

Raadpleeg [een ABUS Link Station Account registreren](#) voor meer informatie.

Stappen

1. Ga naar de inlogpagina van ABUS Link Station.
 - Klik op **Aanmelden in** de rechterbovenhoek van de client.
 1. Klik op **Apparaatbeheer** → **Apparaat** om de pagina Apparaatbeheer te openen.
 2. Klik op **Toevoegen** om het paneel Apparaat toevoegen te openen.
 3. Selecteer **ABUS Link Station** als toevoegmodus.
 4. Klik op **Aanmelden**.

Het venster Aanmelden verschijnt.



Afbeelding 4-2 Aanmeldingspagina van ABUS Link Station

2. Voer de gebruikersnaam en het wachtwoord in.
3. Klik op **Log in** om in te loggen op je account.
Inloggen verandert in **Ingelogd**.
4. Optioneel: Klik op **Ingelogd** → **Uitloggen** om uit te loggen uit je account.

Opmerking

- Apparaten die zijn toegevoegd door ABUS Link Station worden verborgen nadat de ABUS Link Station-service is afgemeld.
 - Alarmgerelateerde beelden die zijn opgeslagen in ABUS Link Station blijven 2 uur geldig.
-












Hoofdstuk 5 Liveweergave

Je kunt de live video van de toegevoegde netwerkcamera's en video-encoders bekijken op de pagina Hoofdweergave. En sommige basisbewerkingen worden ondersteund, zoals het vastleggen van beelden, handmatige opname, verdeling van vensters, PTZ-besturing, automatisch schakelen in liveweergave, enz.

5.1 Werkbalk Liveweergave




Met de werkbalk voor liveweergave kun je het liveweergavevenster handiger en sneller bedienen en beheren. Je kunt bijvoorbeeld foto's maken, geluid opnemen, het volume aanpassen en het venster splitsen met één klik op de gereedschappen op de werkbalk.

Tabel 5-1 Beschrijvingen van de werkbalk

Pictogram	Functie Naam	Functiebeschrijving en werking
	Weergave opslaan	Sla de weergave op die je nu maakt, wat handig is om snel de gewenste camera's te bekijken. Klik op  om het venster voor het opslaan van weergaven te openen. Selecteer Create View (Weergave maken) of Current View (Huidige weergave) en geef de weergave een naam.
	Liveweergave stoppen	Stop alle livecamera's.
	Dempen/annuler en Dempen	Klik op  om de volumebalk te laten verschijnen, klik op  om het dempen te annuleren en u kunt het volume aanpassen. Klik op  om de volumebalk op te roepen, klik nogmaals op  om de livecamera's in te stellen als gedempt.
	Venster divisie	Selecteer de verschillende vensterdelingsmodi voor liveweergave. Klik op  om één vensterdelingsmodus te selecteren (bijv. 9-vensterdeling). Je kunt ook op Toevoegen klikken om een vensterdelingsmodus aan te passen.
	Volledig scherm	Geef de live-weergave op het volledige scherm weer. Druk op Esc om de modus volledig scherm te verlaten.
	Configuratie	Ga naar de instellingsmodus voor liveweergaveparameters, configureer voor liveweergave

Pictogram	Functie Naam	Functiebeschrijving en werking
		en afspelen, beeld, bestanden en werkbalk.


Tabel 5-2 Beschrijving van pictogrammen in het venster Liveweergave

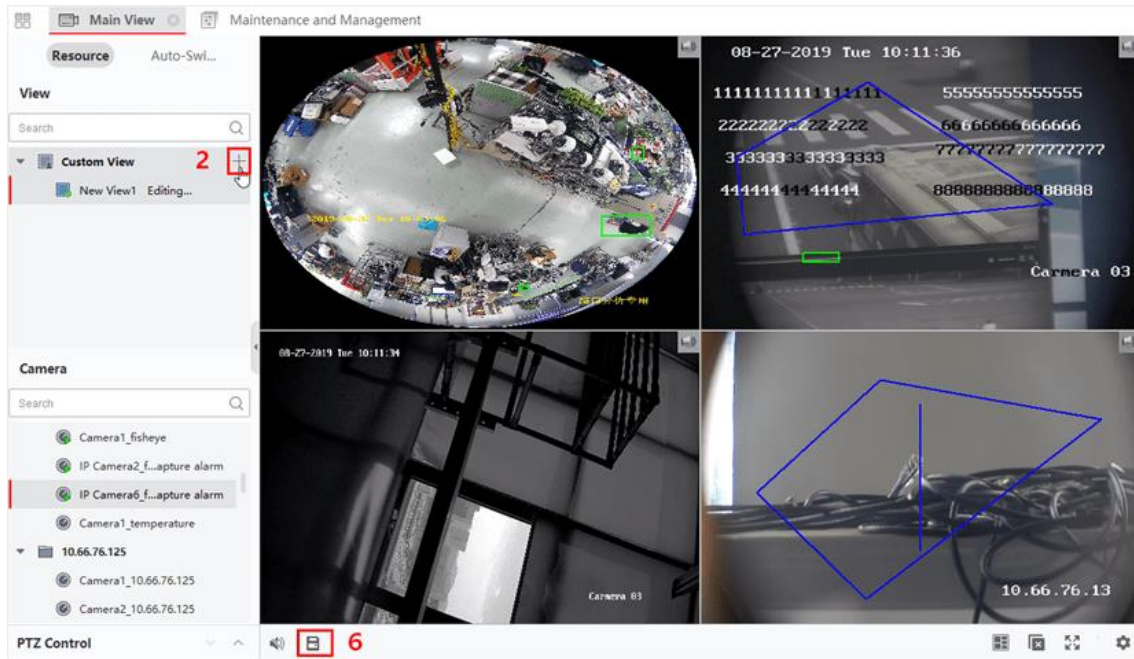
Pictogram	Functie Naam	Functiebeschrijving en bediening
	Vang	Leg de foto's handmatig vast voor het liveweergavevenster.
	Opname starten/stoppen	Klik de eerste keer om de opname te starten en klik nogmaals om de opname te stoppen en de opnamebestanden automatisch op te slaan op het pad dat je hebt ingesteld.
	Overschakelen naar onmiddellijk afspelen	Op de huidige tijd kunt u selecteren om de video af te spelen in voorgaande 30 s, 1 min, 3 min, 5 min, 8 min, 10 min.

5.2 Aangepaste weergave toevoegen



Een weergave is een vensterindeling met camera's geconfigureerd voor elk venster; in de weergavemodus kun je de vensterindeling en de correspondentie tussen camera's en vensters opslaan als favoriet om later snel toegang te krijgen tot de gerelateerde camera's. U kunt bijvoorbeeld camera 1, camera 2 en camera 3 in uw kantoor koppelen om vensters weer te geven en deze opslaan als een weergave met de naam kantoor.

Stappen

1. Ga naar de pagina Hoofdweergave.
2. Klik op het tabblad **Hulpbronnen**.
3. Beweeg de cursor naar de Aangepaste weergave in het resourcepaneel en klik op  om een nieuwe weergave te maken.
4. Voer een naam in voor de weergave.





Figuur 5-1 Aangepaste weergave toevoegen

5. Optioneel: Klik op  in de live weergave werkbalk om de vensterdelingsmodus in te stellen voor de nieuwe weergave.
6. Start liveweergave voor gespecificeerde camera in gespecificeerd venster volgens actuele behoeften.
7. Klik op  om de huidige weergave op te slaan of op te slaan als een nieuwe weergave.

Opmerking

Je kunt maximaal 16 aangepaste weergaven toevoegen aan de client.

8. Optioneel: Voer de volgende bewerkingen uit na het toevoegen van de aangepaste weergave.

Bewerk weergavenaam	Beweeg de cursor over de nieuwe weergave en klik op  om de weergavenaam te bewerken.
Weergave verwijderen	Beweeg de cursor over de nieuwe weergave en klik op  om de weergave te verwijderen.

Wat nu te doen





Klik nogmaals op  om de aangepaste vensterindeling te selecteren.

5.3 Liveweergave starten

Je kunt liveweergave starten nadat je apparaat(en) aan de client hebt toegevoegd, zodat je het bewaakte gebied goed kunt leren kennen. Je kunt de liveweergave van één camera of van alle camera's in een groep starten. Je kunt de liveweergave ook starten in de aangepaste

weergavemodus.

Klik op **Hoofdweergave** → **Hulpbron** om de pagina Hoofdweergave te openen. Selecteer in de linker resource lijst resource(s) en start de live view op de volgende manieren.

Beschikbare manieren	Beschrijving	Operatie
Liveweergave starten voor één camera	Start de liveweergave van slechts één camera in een groep.	<ul style="list-style-type: none"> • Selecteer een camera en sleep deze naar het venster. • Dubbelklik op de camera in een groep. • Beweeg de cursor over de cameranaam en klik op  .
Liveweergave voor cameragroep starten	Start de live-weergave van alle camera's in één groep synchroon.	<ul style="list-style-type: none"> • Selecteer een groep en sleep deze naar het venster. • Dubbelklik op de groep. • Beweeg de cursor over de groepsnaam en klik op  , of klik op  → Alle camera's in groep weergeven.
Liveweergave starten in aangepaste weergavemodus	Start de live weergave van de camera's in de aangepaste weergave.	<ul style="list-style-type: none"> • Selecteer een aangepaste weergave en sleep deze naar het venster. • Dubbelklik op de aangepaste weergave. <hr/> <p> Opmerking Pas een weergave aan die informatie bevat zoals vensterindeling, camera en correspondentie tussen camera's en vensters. Zie <u>Aangepaste weergave toevoegen</u> voor meer informatie.</p> <hr/>

 **Opmerking**

Als het apparaat streamcodering ondersteunt en de stream van zijn liveweergave is gecodeerd, moet je een streamsleutel invoeren voor dubbele verificatie.

Figuur 5-2 Liveweergave starten

Tijdens liveweergave kun je de bitrate, framerate en resolutie-informatie op het beeld bekijken.

5.4 Automatisch schakelen in Liveweergave

Je kunt de live-weergave van camera's weergeven of de aangepaste weergaven om de beurt, wat "auto-switch" wordt genoemd. Als je een groot aantal camera's live wilt weergeven, kun je de geselecteerde camera's automatisch schakelen, wat betekent dat de client automatisch schakelt tussen de liveweergaven van de camera's in het weergavevenster. Je kunt ook meerdere weergaven automatisch schakelen.


Bij automatisch schakelen in liveweergave zijn drie modi beschikbaar:

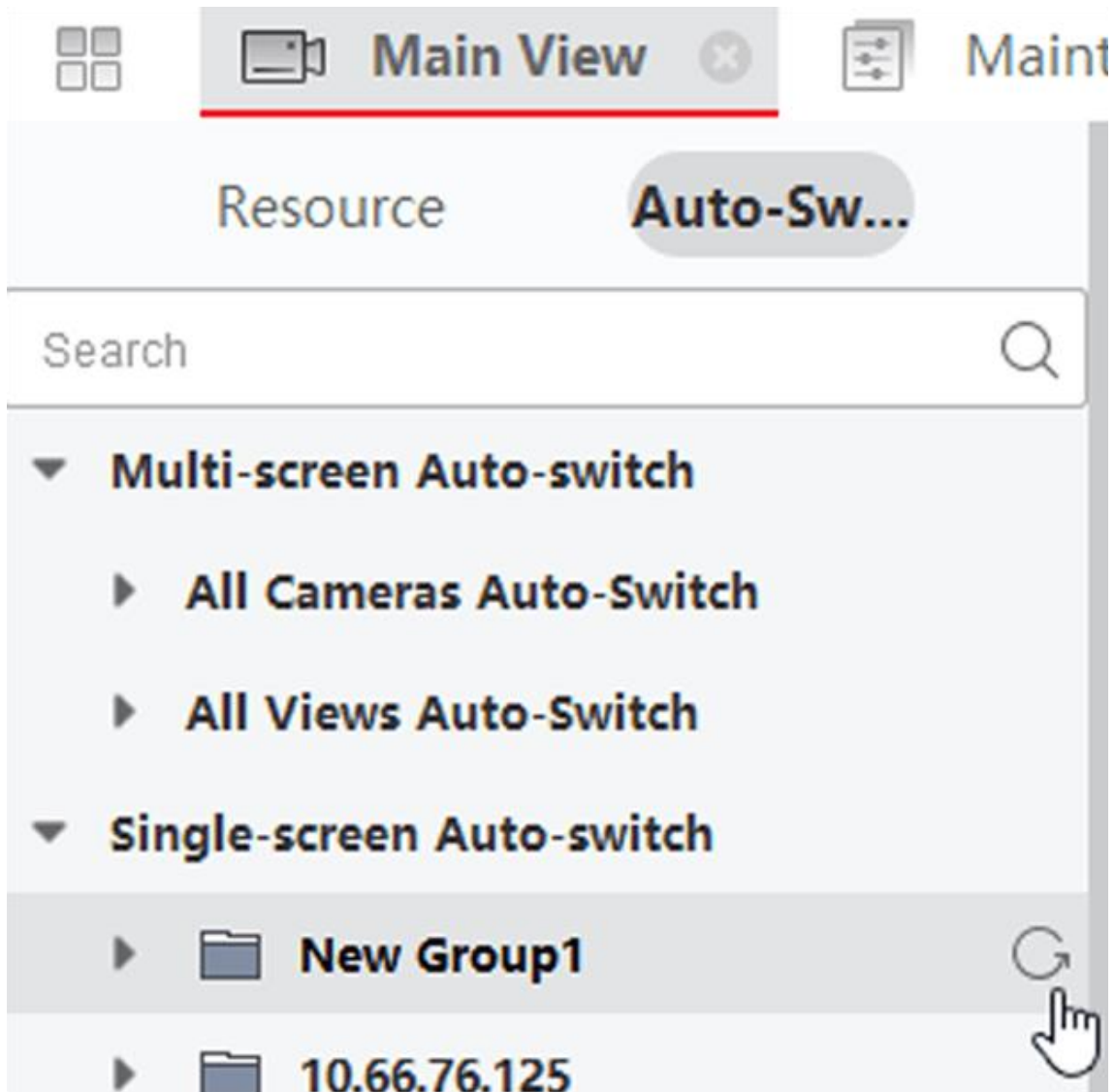
- Automatisch schakelen tussen alle camera's in standaardweergave
- Automatisch schakelen tussen camera's in een groep
- Automatisch schakelen tussen aangepaste weergaven

5.4.1 Automatisch schakelen tussen camera's in een groep

De videostream van de camera's van dezelfde groep kan automatisch schakelen in een geselecteerd weergavevenster. Als je bijvoorbeeld automatisch schakelen van een groep met 5 camera's start, wordt de liveweergave van de 5 camera's om de beurt weergegeven met een interval dat kan worden geconfigureerd. Je kunt ook overschakelen naar afspelen en andere bewerkingen uitvoeren in het weergavevenster.

Stappen

1. Ga naar de pagina Hoofdweergave.
2. Klik op **Auto-Switch** → **Single Window Auto-Switch** in het linkerpaneel om de groepen weer te geven.
3. Selecteer een weergavevenster in het rechterpaneel.
4. Beweeg de cursor over een groepsnaam en klik op  .



Afbeelding 5-3 Automatisch schakelen van camera's in een groep starten

De camera's in de geselecteerde groep beginnen automatisch te schakelen in het weergavevenster.

Opmerking

De audio is standaard uitgeschakeld nadat de automatische omschakeling is gestart.

5. Optioneel: Voer de volgende bewerkingen uit.

Operatie	Beschrijving
Automatisch schakelen pauze/hervatten	Klik op of om automatisch schakelen te pauzeren/hervatten.
Ga naar	Klik op of om camera's van de vorige/volgende groep weer te


vorige/volgende pagina geven.

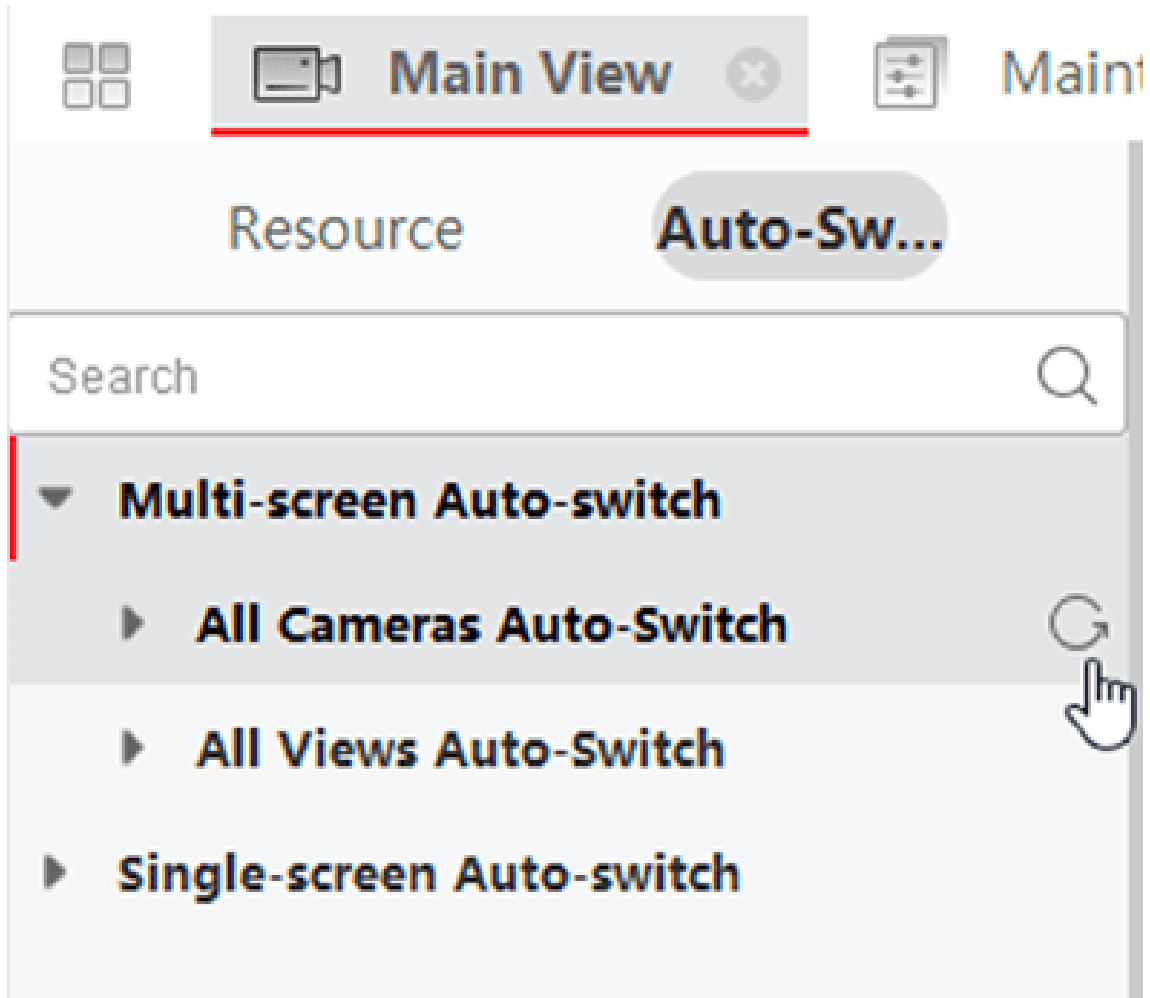
Stilstandtijd instellen Klik na het stoppen van de huidige auto-switch op « of » om de dwell-tijd van de auto-switch te verlagen/verhogen, of klik op **20s** onderaan de pagina om de dwell-tijd van de auto-switch te wijzigen. Je kunt ook op **Aangepaste intervaltijd** klikken om de intervaltijd naar wens in te stellen. Als je bijvoorbeeld een interval van 10 seconden instelt, wordt het beeld van elke groep 10 seconden weergegeven en wordt er vervolgens naar de volgende groep geschakeld.

5.4.2 Alle camera's automatisch schakelen

De video van alle camera's in de cameralijst kan automatisch schakelen in een zelfaanpassende modus. Als je automatisch schakelen van alle camera's start, kan de live-weergave van alle camera's snel worden weergegeven, wat een effectieve manier is voor live-weergave. De automatische omschakeling wordt uitgevoerd met een interval dat kan worden geconfigureerd. U kunt ook overschakelen naar afspelen en andere bewerkingen uitvoeren in het auto-switch venster.

Stappen

1. Ga naar de pagina Hoofdweergave.
2. Klik op **Auto-Switch** → **Multi-Window Auto-Switch** in het linkerpaneel.
3. Beweeg de cursor over **Auto-Switch All Cameras** en klik vervolgens op  .



Afbeelding 5-4 Auto-Switch van alle camera's starten

Alle camera's in de cameralist beginnen automatisch te schakelen in een zelfaanpassende modus.

4. Optioneel: Voer de volgende bewerkingen uit.

Operatie	Beschrijving
Automatisch schakelen pauze/hervatten	Klik op of ↺ om automatisch schakelen te pauzeren/hervatten.
Ga naar vorige/volgende pagina	Klik op < of > om camera's op de vorige/volgende pagina weer te geven.
Stilstandtijd instellen	Klik na het stoppen van de huidige auto-switch op << of >> om de dwell-tijd van de auto-switch te verlagen/verhogen, of klik op 20s onderaan de pagina om de dwell-tijd van de auto-switch te wijzigen. Je kunt ook op Aangepaste intervaltijd klikken om de intervaltijd naar

wens in te stellen. Als je bijvoorbeeld een interval van 10 seconden instelt, wordt het beeld van elke camera 10 seconden weergegeven en wordt daarna naar de volgende camera geschakeld.


5.4.3 Automatisch schakelen tussen aangepaste weergaven

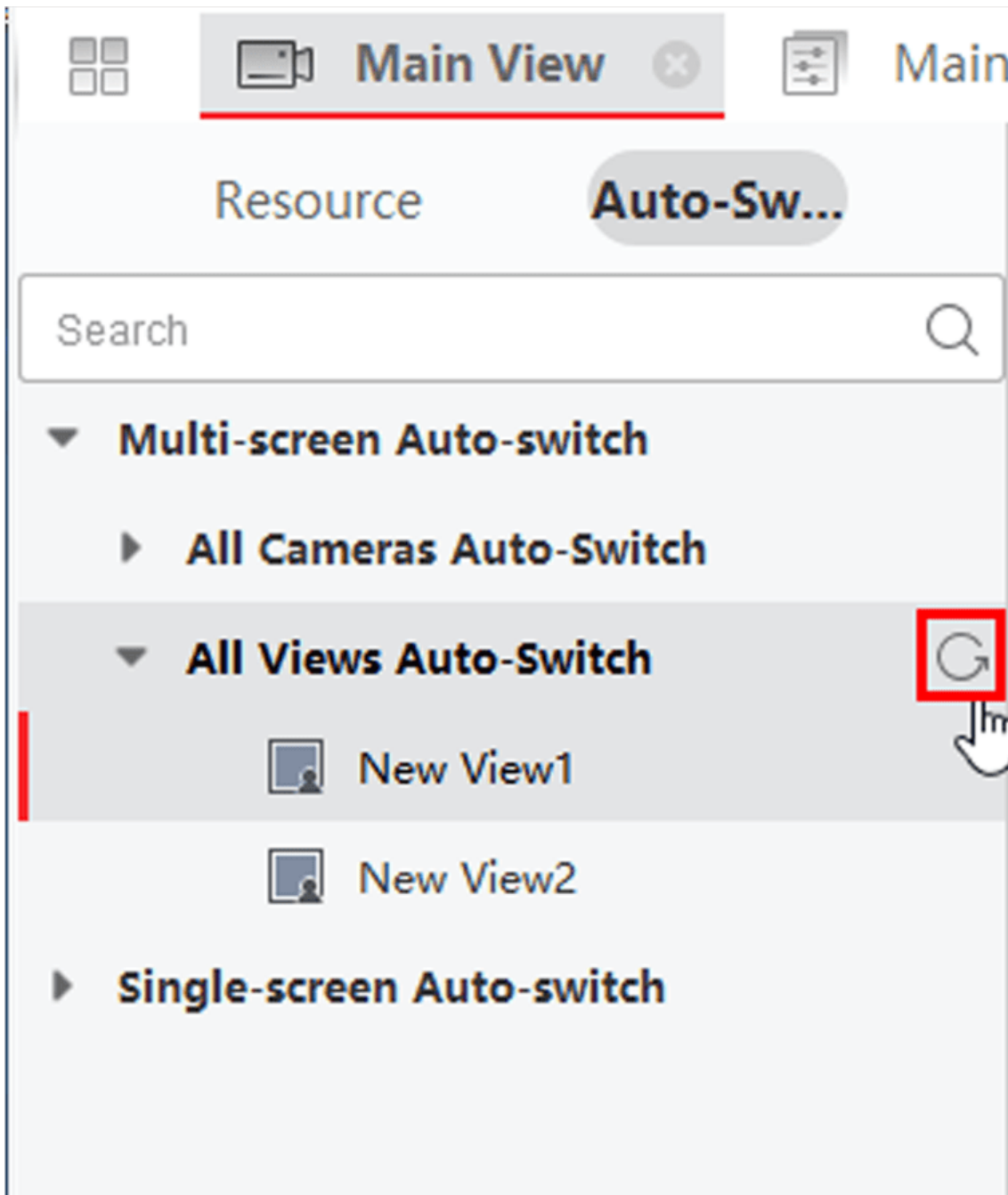
Een weergave is een vensterindeling met bronkanalen (bijv. camera's) die aan elk venster zijn gekoppeld. In de weergavemodus kun je de vensterindeling en de correspondentie tussen camera's en vensters opslaan als favoriet, zodat je deze kanalen later snel kunt openen. Als je een weergave opslaat die alle camera's op een verdieping bevat, sla je een aangepaste weergave op en kun je met één klik achtereenvolgens de liveweergave van alle camera's op de verdieping bekijken. Op deze manier hoeft je deze camera's niet elke keer dat je inlogt op te zoeken in de cameralijst. De auto-switch werkt met een interval dat handmatig kan worden ingesteld.

Voordat u begint

Voeg de aangepaste weergaven toe. Zie [Aangepaste weergave toevoegen](#) voor meer informatie.

Stappen

1. Ga naar de pagina Hoofdweergave.
2. Klik op **Resource** → **Multi-Window Auto-Switch** in het linkerpaneel.
3. Beweeg de cursor over **Auto-Switch All Views** en klik op  .



Afbeelding 5-5 Automatisch schakelen tussen aangepaste weergaven

Alle aangepaste weergaven beginnen automatisch te schakelen.

4. Optioneel: Voer de volgende bewerkingen uit.

Operatie	Beschrijving
Automatisch schakelen pauze/hervatten	Klik op of ↺ om automatisch schakelen te pauzeren/hervatten.

Ga naar vorige/volgende pagina

Klik op < of > om de vorige/volgende weergave weer te geven.

Stilstandtijd instellen

Klik na het stoppen van de huidige auto-switch op << of >> om de dwell-tijd van de auto-switch te verlagen/verhogen, of klik op **20s** onderaan de pagina om de dwell-tijd van de auto-switch te wijzigen. Je kunt ook op **Aangepaste intervaltijd** klikken om de intervaltijd naar wens in te stellen. Als je het interval bijvoorbeeld instelt op 10 seconden, wordt het beeld van elke weergave 10 seconden weergegeven en wordt er vervolgens overgeschakeld naar de volgende weergave.

5.5 PTZ-besturing

De software biedt PTZ-besturing voor camera's met pan/tilt/zoom-functionaliteit. Tijdens de PTZ-besturing kun je voorinstellingen, patrouilles en patronen instellen en je kunt ook een nieuw venster openen voor het besturen van de PTZ.



Let op

- Sommige functies moeten worden ondersteund door het apparaat.
-

5.5.1 PTZ-bedieningspaneel

De software biedt PTZ-bediening via het bedieningspaneel, zoals detectie, snelheid, inzoomen, uitzoomen, enz. Je kunt ook een nieuw venster openen om de PTZ te bedienen.







Opmerking





ABUS Link Station ondersteunt alleen PTZ-bewegingen in de richtingen omhoog, omlaag, links en rechts.





Ga naar de module **Main View** en selecteer **PTZ Control** om het PTZ-bedieningspaneel te openen. De volgende pictogrammen zijn beschikbaar op het PTZ-bedieningspaneel.

Tabel 5-3 Pictogrammen op het PTZ-bedieningspaneel

Pictogram	Naam	Beschrijving
	Richtingsknoppen	Klik of houd de linkermuisknop ingedrukt om de PTZ te draaien. Klik om de PTZ horizontaal en continu rond te draaien; klik nogmaals om te stoppen met draaien.



Pictogram	Naam	Beschrijving
	Snelheidsregeling	Versleep de schuifregelaar om de PTZ-bewegingssnelheid aan te passen.
	In-/uitzoomen	Zoom in om het beeld van dichtbij te bekijken voor details; zoom uit om een panoramisch beeld te bekijken.
	Focus +/-	Klik op Focus + om het brandpunt naar voren te verplaatsen en klik op Focus - om het brandpunt naar achteren te verplaatsen.
	Iris +/-	Wordt gebruikt om de helderheid van het beeld aan te passen. Hoe groter de iris, hoe meer licht er binnenkomt en hoe helderder het beeld zal zijn.
	3D-positionering	Klik met de linkermuisknop op de gewenste positie in het videobeeld en sleep een rechthoek in de rechterbenedenrichting, waarna het koepelsysteem de positie naar het midden verplaatst en het rechthoekgebied laat inzoomen. Sleep met de linkermuisknop een rechthoek in de linkerbovenrichting om de positie naar het midden te verplaatsen en het rechthoekgebied uit te zoomen.
	Hulpfocus	Klik om automatisch scherp te stellen.
	Lens initialisatie	Initialiseer de lens en stel opnieuw scherp voor een helder beeld.
	Licht	Klik om licht te vullen. <hr/>  Opmerking Deze functie moet worden ondersteund door het apparaat. <hr/>
	Ruitenwisser	Gebruik de wisser om het stof op de cameralens te verwijderen.
	Handmatig volgen	Voor speed dome met auto-tracking functie, schakel de auto-tracking in (via rechtsklik menu) en klik op het pictogram om handmatig het doel te volgen door te klikken






Pictogram	Naam	Beschrijving
		op de video.
	Menu	Voor analoge speed dome, klik op het pictogram om het lokale menu weer te geven. Raadpleeg de gebruikershandleiding van de speed dome voor meer informatie over de werking van het menu.
	Patrouille met één druk op de knop	Voor de speed dome met one-touch patroolfunctie, klikt u op het pictogram en de speed dome begint na een periode van inactiviteit (parkeertijd) te patrouilleren vanaf de vooraf ingestelde voorkeursinstellingen nr. 1 tot voorkeursinstelling nr. 32 in volgorde. Raadpleeg de gebruikershandleiding van de speed dome voor het instellen van de parkeertijd.
	Parkeren met één druk op de knop	Voor de speed dome met one-touch parkeerfunctie, klik op het pictogram en de speed dome slaat de huidige weergave op in voorinstelling nr. 32. Het apparaat begint automatisch te parkeren op voorkeuzenr. 32 na een periode van inactiviteit (parkeertijd). Raadpleeg de gebruikershandleiding van de speed dome voor het instellen van de parkeertijd.
	Handmatige lensontdooiing inschakelen	Schakel deze functie in om de prestaties van de camera te garanderen door deze te verwarmen. <hr/>  Opmerking We raden u aan deze functie in te schakelen wanneer de omgevingstemperatuur onder 0 °C ligt, anders kan de hoge temperatuur de werking van de camera beïnvloeden. <hr/>
	Handmatige PT-ontdooiing inschakelen	Schakel deze functie in om de prestaties van de camera te garanderen door het ijs weg te vegen dat op de PTZ-camera is gekleefd.

Pictogram	Naam	Beschrijving
	Handmatig gezichten vastleggen	Klik op deze knop en houd de linkermuisknop ingedrukt om een gezicht in de afbeelding te selecteren en vast te leggen. De afbeelding wordt geüpload naar de server om te worden bekeken.
	FOV synchroniseren	Voor thermische camera's klikt u op het pictogram om het gezichtsveld van het optische kanaal te synchroniseren met dat van het thermische kanaal.
	Regionale blootstelling	Klik voor speed domes op het pictogram en teken een rechthoek op de afbeelding om het belichtingseffect in dit gebied te optimaliseren.
	Regionale focus	Klik voor speed domes op het pictogram en teken een rechthoek op de afbeelding om het scherpstellingseffect in dit gebied te optimaliseren.
	Bewapenen en traceren	Voor camera's die bewapenen en volgen ondersteunen, klik op het pictogram en selecteer het doel (persoon of voertuig) in de live-weergave om dit doel te bewapenen en volgen.

5.5.2 Preset, Patrol en Patroon instellen

PTZ-bediening ondersteunt het instellen en oproepen van een preset, patrouille en patroon. Klik op de startpagina op **Hoofdweergave** → **PTZ-bediening** om het PTZ-bedieningspaneel weer te geven.

Taak	Definitie	Operatie
Vooraf ingesteld	Een preset koppelt de belangrijkste regio's aan mobiele PTZ-positie en status. Mensen die toezicht houden gebruiken het om snel sleutelregio's te vinden. Door het verzenden van een vooraf ingesteld commando registreert de mobiele PTZ de	Hoe instellen: selecteer een voorinstelling in de voorkeuzelijst → draai de camera naar een gewenste positie → klik op  .
		Hoe te bellen: klik op  .

Taak	Definitie	Operatie
	positie en status van zoom, focus en iris. Wanneer het vooraf ingestelde commando wordt uitgevoerd, rolt de mobiele PTZ snel naar de ingestelde positie en wordt de ingestelde status hervat.	
Patroon	Door het opnamepatroon kunnen het bewegingspad en de verblijftijd in een bepaalde positie nauwkeurig worden opgenomen. Bij het oproepen van het patroon beweegt de mobiele PTZ volledig volgens het geregistreerde pad.	Hoe in te stellen: klik op  om het opnemen van een patroon te starten → klik op de richtingsknoppen om het patroon vorm te geven → klik op  .
		Hoe te bellen: klik op  .
Patrouille	Patrouille is de functie waarmee gebruikers een scantrack specificeren met een groep gedefinieerde presets. De patrouille tussen twee presets wordt uitgevoerd met de ingestelde snelheid en tijd.	Hoe instellen: klik op  → selecteer voorinstellingen en stel snelheid en tijd in → klik op OK .
		Hoe te bellen: klik op  .

 **Opmerking**

Je moet op voorhand minstens twee presets instellen.

5.6 Vensterindeling aanpassen


De clientsoftware biedt meerdere soorten voorgedefinieerde vensterverdelingen. Je kunt de vensterindeling ook naar wens aanpassen.

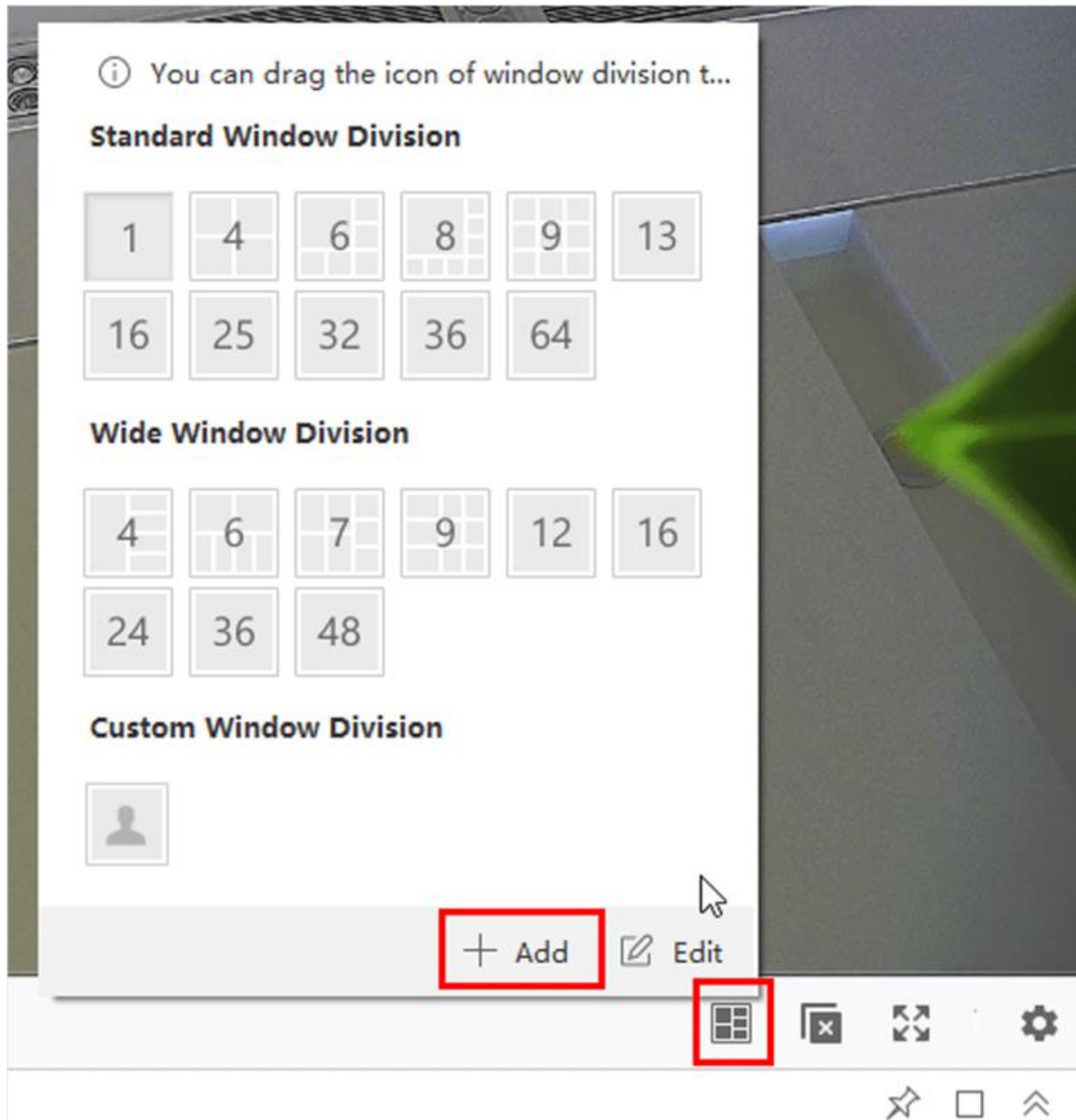
Stappen

 **Opmerking**

Er kunnen maximaal 5 vensterverdelingen worden aangepast.

1. Open de pagina Hoofdweergave of Afspelen op afstand.

2. Klik op  op de werkbalk voor liveweergave of afspelen om het vensterverdelingspaneel te openen.



Afbeelding 5-6 Aangepaste vensterindeling toevoegen

3. Klik op **Toevoegen** om het dialoogvenster Aangepaste vensterindeling toevoegen te openen.
4. Voer de vensternummers van zowel de horizontale als verticale dimensie in het veld Dimensie in en druk vervolgens op **Enter** op je toetsenbord.

 **Opmerking**

Voor afspelen op afstand kunnen maximaal 16 vensters tegelijk worden afgespeeld, dus de aangepaste vensterindeling met meer dan 16 vensters is ongeldig.

5. Optioneel: Sleep je muis om de aangrenzende vensters te selecteren en klik op **Gezamenlijk** om ze samen te voegen als een heel venster.

Add Custom Window Division

Mouse cursor icon

Name

Dimension X

Window Division Joint Restore

Afbeelding 5-7 Venster Verdeling Aangepast venster toevoegen

6. Optioneel: Selecteer het voegvenster en klik op **Herstellen** om de voeg te annuleren.
7. Klik op **Opslaan**.
8. Optioneel: Klik of sleep een verdelingsmodus naar het weergavevenster om de modus toe te passen voor weergave.
9. Optioneel: Bewerk een aangepaste vensterdelingsmodus.
- 1) Klik op op de liveweergave- of afspelerwerkbalk om het vensterverdelingspaneel te openen.

- 2) Klik op **Bewerken** om de divisie Aangepast venster toevoegen te openen.
- 3) Selecteer een aangepaste verdeelmodus en voer bewerkingen uit zoals hernoemen, dimensie instellen, vensters verbinden/ontvoegen.

5.7 Handmatig opnemen en vastleggen

Tijdens liveweergave kunt u video's opnemen en foto's handmatig vastleggen en vervolgens de opgenomen videobestanden en vastgelegde foto's op de lokale pc bekijken.






5.7.1 Video handmatig opnemen

Met de handmatige opnamefunctie kun je de live video op de hoofdweergavepagina handmatig opnemen en kun je de videobestanden opslaan op de lokale pc.

Stappen

Opmerking

Handmatig opnemen wordt niet ondersteund door ABUS Link Station tijdens live weergave.

1. Open de pagina Hoofdweergave.
2. Start de liveweergave.
3. Voer een van de volgende handelingen uit om de handmatige opname te starten.
 - Verplaats de cursor naar het weergavevenster in liveweergave om de werkbalk weer te geven en klik op  op de werkbalk.
 - Klik met de rechtermuisknop op het weergavevenster en klik op **Opname starten** in het rechtermuisknopmenu.Het pictogram  verandert in . In de rechterbovenhoek van het weergavevenster verschijnt een indicator .
4. Klik op  om de handmatige opname te stoppen.

Het opgenomen videobestand wordt automatisch opgeslagen op de lokale pc en er verschijnt een klein venster met informatie over het opslagpad in de rechterbenedenhoek van het bureaublad.

Opmerking

Het opslagpad van de opgenomen videobestanden kan worden ingesteld op de pagina Systeemconfiguratie. Zie **Bestand opslaan pad instellen** voor meer informatie.


5.7.2 Lokale video's bekijken

U kunt de opgenomen videobestanden bekijken die op uw lokale pc zijn opgeslagen.

Voordat u begint

Neem de live video op.

Stappen

1. Klik op  → **Bestand** → **Videobestand openen** in de rechterbovenhoek om de pagina Videobestanden te openen.
2. Selecteer de camera om de opgenomen videobestanden te zoeken in de lijst Cameragroep.
3. Geef linksonder de starttijd en eindtijd op voor het zoeken.
4. Klik op **Zoeken**.
De videobestanden die zijn opgenomen tussen de starttijd en eindtijd worden in miniatuurformaat weergegeven op de pagina.
5. Optioneel: Voer na het zoeken de volgende bewerking(en) uit.

Videobestand verwijderen

Selecteer het videobestand en klik op **Verwijderen** om het videobestand te verwijderen.

Verstuur e-mail

Selecteer het videobestand en klik op **E-mail** om een e-mail te versturen met het geselecteerde videobestand als bijlage.

Opmerking

Om een e-mailmelding te versturen, moeten de e-mailinstellingen geconfigureerd worden voordat u verder gaat. Raadpleeg [**E-mailparameters instellen**](#) voor meer informatie.

Lokale video opslaan

Selecteer het videobestand en klik op **Opslaan als** om een nieuwe kopie van het videobestand op te slaan.

Afspelen


Dubbeltklik op het videobestand om het lokaal afspelen te starten.

5.7.3 Foto's vastleggen

U kunt opnamen maken tijdens de live-weergave.

Voer deze taak uit als u opnamen moet maken tijdens de liveweergave.

Stappen

1. Open de pagina Hoofdweergave en start de liveweergave van een camera.
2. Voer een van de volgende handelingen uit om foto's te maken.
 - Verplaats de cursor naar het weergavevenster in liveweergave om de werkbalk weer te geven en klik op  op de werkbalk.

- Klik met de rechtermuisknop op het weergavevenster en klik op **Capture** in het rechtermuisknopmenu.

De vastgelegde foto wordt automatisch opgeslagen op de lokale pc en er verschijnt een klein venster met het afbeeldingsvoorbeeld en informatie over het opslagpad in de rechterbenedenhoek van het bureaublad.

Opmerking

Het opslagpad van de vastgelegde beelden kan worden ingesteld op de pagina Systeemconfiguratie. Raadpleeg **Bestand opslaan pad instellen** voor meer informatie.


5.7.4 Vastgelegde afbeeldingen weergeven

De beelden die worden vastgelegd in de live-weergave worden opgeslagen op de pc waarop de software draait. U kunt de gemaakte foto's indien nodig bekijken.

Voordat u begint

Foto's maken in de live-weergave.

Stappen

1. Klik op  → **Bestand** → **Vastgelegde foto openen** in de rechterbovenhoek om de pagina Vastgelegde foto te openen.
2. Selecteer de camera die u wilt doorzoeken in de lijst met cameragroepen.
3. Geef linksonder de starttijd en eindtijd op voor het zoeken.
4. Klik op **Zoeken**.
De foto's die zijn gemaakt tussen de starttijd en eindtijd worden in miniatuurformaat weergegeven op de pagina.
5. Optioneel: Voer na het zoeken de volgende bewerking(en) uit.

Afbeelding vergroten Dubbelklik op de miniatuurafbeelding om deze te vergroten en beter te bekijken.

Afbeelding afdrukken Selecteer de vastgelegde afbeelding en klik op **Afdrukken** om de geselecteerde afbeelding af te drukken.

Afbeelding verwijderen Selecteer de vastgelegde foto en klik op **Verwijderen** om de geselecteerde foto te verwijderen.

Verstuur e-mail Selecteer de vastgelegde afbeelding en klik op **E-mail** om een e-mail te versturen met de geselecteerde afbeelding als bijlage.

Afbeelding opslaan Selecteer de vastgelegde afbeelding en klik op **Opslaan als** om een nieuwe kopie van de geselecteerde afbeelding op te slaan.



5.8 Onmiddellijk afspelen

Direct afspelen toont een stukje van de video dat opmerkelijk is, of dat op het eerste gezicht onduidelijk is. Je kunt de videobestanden dus direct afspelen op de pagina Hoofdweergave en indien nodig direct een beoordeling krijgen.

Voordat u begint


Neem de videobestanden op en sla ze op de opslagapparaten op, zoals de SD/SDHC-kaarten en HDD's op de DVR's, NVR's, netwerkkamera's, etc., of op de opslagservers.


Stappen

1. Open de pagina Hoofdweergave en start de liveweergave.
2. Voer een van de volgende handelingen uit om de lijst met voorlooptijden voor onmiddellijk afspelen weer te geven.
 - Verplaats de cursor naar het weergavevenster om de werkbalk weer te geven en klik op  .
 - Klik met de rechtermuisknop op het weergavevenster en selecteer **Schakel naar directe weergave** in het rechtermuisknopmenu.
 - Verplaats de cursor naar het knooppunt Standaardweergave of Aangepaste weergave in het paneel Weergave en klik op  .Een lijst met voorspeelduur van 30s, 1 min, 3 min, 5 min, 8 min en 10 min wordt weergegeven.
3. Selecteer een periode uit de lijst om het afspelen te starten.

Voorbeeld

Als u 3 min. selecteert en de huidige tijd van de live-weergave is 09:30:00, dan start de onmiddellijke weergave vanaf 09:27:00 uur.

Tijdens het direct afspelen verschijnt er een indicator  in de rechterbovenhoek van het weergavevenster.

4. Optioneel: Klik nogmaals op  om het direct afspelen te stoppen en terug te gaan voor de live weergave.

5.9 Liveweergave voor Fisheye-camera

Voor fisheye-camera's kun je de live-weergave starten in fisheye-modus, presets en patrouilles instellen en PTZ-besturing uitvoeren.

5.9.1 Liveweergave in visooqmodus uitvoeren


Tijdens live weergave van fisheye-camera's wordt het hele groothoekervormde beeld weergegeven. Maar het kan moeilijk zijn om sommige details te zien. Om dit probleem op te lossen, kun je de live video's afspelen in de fisheye-uitbreidingsmodus. Fisheye-uitbreiding kan beelden in verschillende modi uitbreiden: 180° panorama, 360° panorama, PTZ, halve bol, enz. Zo

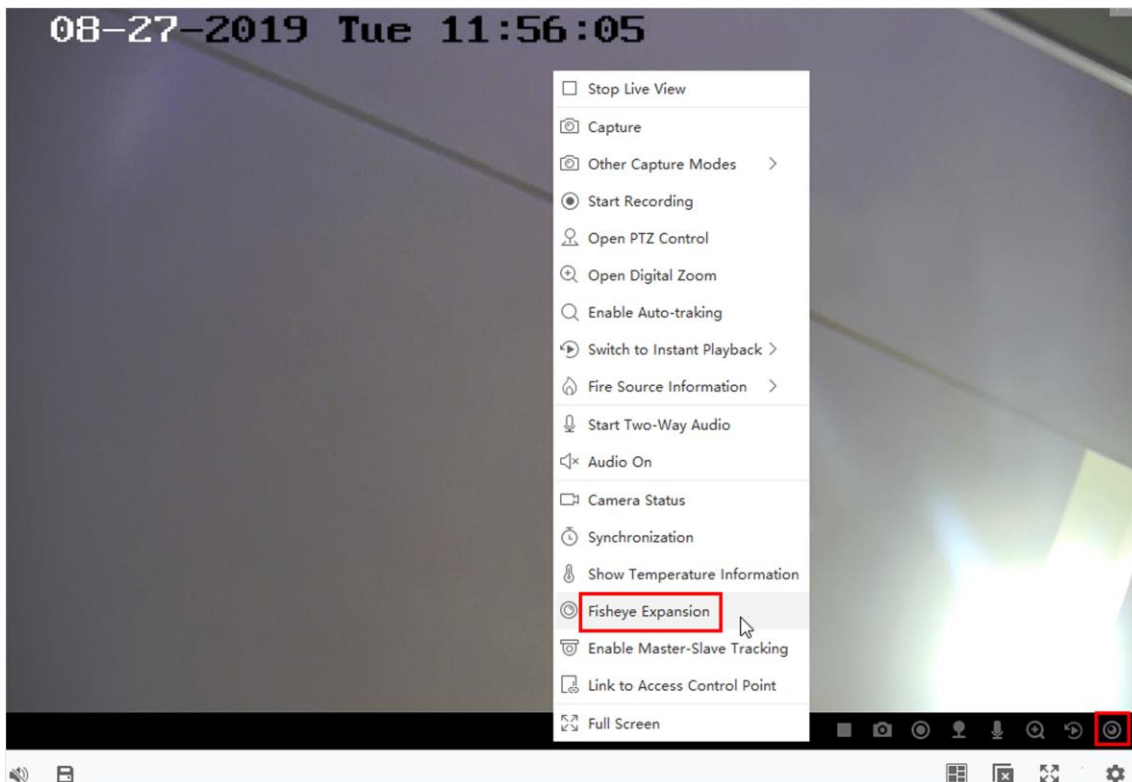
kun je het beeld duidelijk bekijken.

Voordat u begint

Zorg ervoor dat je Microsoft DirectX component geïnstalleerd is.



Stappen


1. Open de pagina Hoofdweergave en start de liveweergave van de fisheye-camera.
2. Activeer de modus Fisheye-uitbreiding.
 - Klik met de rechtermuisknop op de video en selecteer **Fisheye Expansion**.
 - Klik op  in de werkbalk. Zie [Pictogrammen op werkbalk instellen voor](#) meer informatie over het instellen van de werkbalk.



Afbeelding 5-8 Liveweergave in visenoogmodus

–

 gaat naar .

3. Klik op  in de linkerbenedenhoek van het weergavevenster om het selectiepaneel Montagetypen & Uitbreidingsmodus te openen.
4. Selecteer het montagetypen van de fisheye-camera op basis van de werkelijke montagepositie.
5. Selecteer naar wens de uitbreidingsmodus voor liveweergave.

Fisheye

In de Fisheye-weergavemodus wordt het volledige groothoekbeeld van de camera weergegeven. Deze weergavemodus wordt Fisheye genoemd omdat het het zicht van het bolle oog van een vis benadert. De lens produceert kromlijnige beelden van een groot gebied, terwijl het perspectief en de hoeken van objecten in het beeld worden vervormd.

Panorama

In de modus Panoramaweergave wordt het vervormde fisheye-beeld getransformeerd naar een normaal perspectiefbeeld door middel van een aantal kalibratiemethoden.

PTZ

De PTZ-weergave is de close-up weergave van een bepaald gebied in de Fisheye-weergave of Panoramaweergave en ondersteunt de elektronische PTZ-functie, ook wel e-PTZ genoemd.

Opmerking

Elke PTZ-weergave is gemarkeerd op de Fisheye-weergave en Panoramaweergave met een specifiek navigatievak. Je kunt het navigatievak slepen op de Fisheye-weergave of Panoramaweergave om de PTZ-weergave aan te passen, of sleep de PTZ-weergave om de weergave aan te passen aan de gewenste hoek.

Halve bol

In de halve bol-modus kun je de afbeelding slepen en roteren, gecentreerd op de diameter, om de weergave aan te passen aan de gewenste hoek.

AR halve bol

De AR halve bol modus overlapt beelden ver weg en dichtbij, zodat je een dimensionaal beeld in een brede hoek kunt bekijken.

Cilinder

In de cilindermodus wordt de afbeelding gevormd tot een cilinderpagina.

6. Optioneel: Voer de volgende handeling(en) uit na het starten van liveweergave in de fisheye-modus.

Vang	Klik met de rechtermuisknop op het venster en selecteer Vastleggen om de foto vast te leggen in het liveweergaveproces.
Volledig scherm openen	Klik met de rechtermuisknop op een afspeelvenster en schakel het geselecteerde venster over naar volledig scherm.

5.9.2 PTZ-besturing in visseenoogmodus




In de fisheye-modus kunt u de PTZ bedienen om het PTZ-venster aan te passen.

Opmerking

Het PTZ-paneel verschilt per apparaat.

De volgende functies zijn beschikbaar op het PTZ-bedieningspaneel.





- Selecteer een PTZ-venster en klik op de richtingsknoppen om de kijkhoek aan te passen. Of sleep het Nr.-label in het fisheye- of panoramavenster om de kijkhoek van het PTZ-venster te wijzigen.

- Selecteer een PTZ-venster, klik op  om auto-scan te starten (de camera draait in horizontale richting) en klik er nogmaals op om auto-scan te stoppen.
- Versleep de schuifregelaar op  om de snelheid voor PTZ-bewegingen aan te passen.
- Klik op  of scroll met het muiswiel om in of uit te zoomen op het geselecteerde PTZ-venster.

5.9.3 Een preset en patrouille instellen

PTZ ondersteunt het configureren en oproepen van een preset en patrouille.

Ga naar de pagina **Hoofdweergave** en selecteer **Fisheye-uitbreiding** nadat je met de rechtermuisknop op een camera hebt geklikt.

Taak	Definitie	Operatie
Vooraf ingesteld	Een preset koppelt de belangrijkste regio's aan mobiele PTZ-positie en status. Mensen die toezicht houden gebruiken het om snel sleutelregio's te vinden. Door het verzenden van een vooraf ingesteld commando registreert de mobiele PTZ de positie en status van zoom, focus en iris. Wanneer het vooraf ingestelde commando wordt uitgevoerd, rolt de mobiele PTZ snel naar de ingestelde positie en wordt de ingestelde status hervat.	<p>Hoe instellen: selecteer een voorinstelling in de voorkeuzelijst → draai de camera naar een gewenste positie → klik op  .</p> <p>Hoe te bellen: klik op  .</p>
Patrouille	Patrouille is de functie waarmee gebruikers een scantrack specificeren met een groep gedefinieerde presets. De patrouille tussen twee presets wordt uitgevoerd met de ingestelde snelheid en tijd.	<p>Hoe instellen: klik op  → selecteer voorinstellingen en stel snelheid en tijd in → klik op OK.</p> <p>Hoe te bellen: klik op  .</p>

5.11 Liveweergave voor thermische camera

Voor thermische camera's kun je de informatie over de vuurbron en de temperatuur bekijken tijdens live weergave. Je kunt de temperatuur ook handmatig meten om temperatuurinformatie in het livebeeld te krijgen.

5.11.1 Vuurbroninformatie bekijken tijdens Live weergave

Tijdens de live-weergave kunt u de gedetecteerde informatie over de vuurbron bekijken.

Voordat u begint

Configureer de alarmregels voor het thermische apparaat, zie de gebruikershandleiding van het apparaat voor meer informatie.

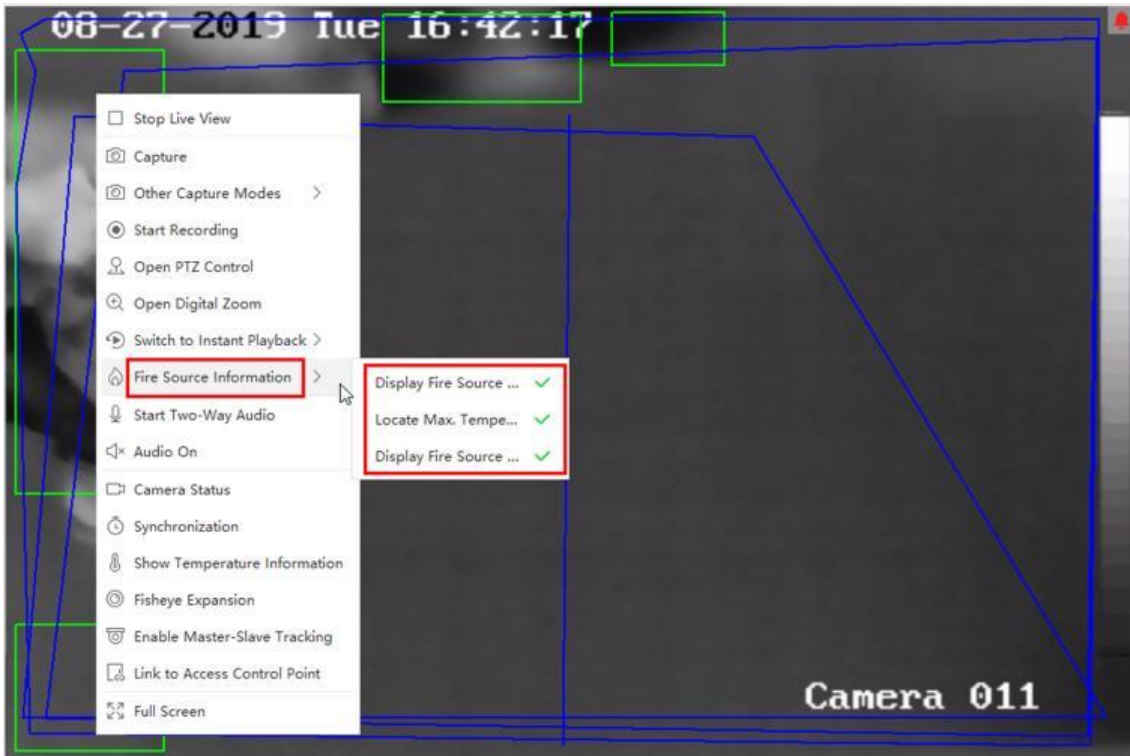
Stappen

1. Ga naar de pagina Hoofdweergave en start de liveweergave van een thermische camera.

Opmerking

Raadpleeg [Liveweergave starten](#) voor het starten van liveweergave.

2. Klik met de rechtermuisknop op het livebeeld en selecteer **Bestandsbroninformatie** in het rechtermuisknopmenu om de lijst met informatietypes weer te geven.



Figuur 5-9 Vuurbroninformatie weergeven

3. Selecteer een informatietype in de lijst om de informatie weer te geven.

Vuurbronregio weergeven

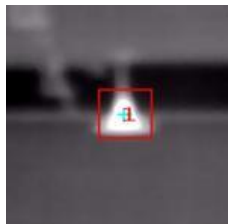
Het gebied waarin de temperatuur hoger is dan de geconfigureerde alarmdrempel.

Zoek Max. Temperatuur

Markeer het gebied waar de temperatuur het hoogst is in het vuurbrongebied. Dit is groen gemarkeerd.

Weergave Brandbron Doel

De afstand tussen het apparaat en de vuurbron.



Afbeelding 5-10 Informatie over de vuurbron in het livebeeld

5.11.2 Temperatuurinformatie op Live View-beeld tonen

U kunt de real-time temperatuurinformatie van de monitoringscène tonen of verbergen wanneer

u de live video bekijkt.

Voordat u begint

- Schakel het VCA-brontype van het apparaat in als **Temperatuurmeting + Detectie van abnormale gebeurtenissen**.
- Schakel de temperatuurmeetfunctie van het apparaat in en stel de temperatuurmeetregels in, zie de handleiding van het apparaat voor meer informatie.

Voer deze taak uit als u de temperatuurinformatie op het livebeeld wilt weergeven.

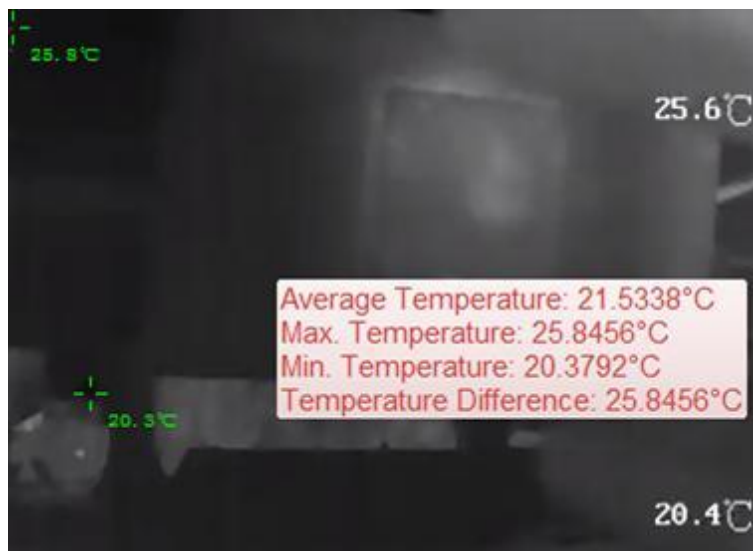
Stappen

1. Ga naar de pagina Hoofdweergave en start de liveweergave van een thermische camera.

Opmerking

Raadpleeg **Liveweergave starten** voor het starten van liveweergave.

2. Stel de scène in op het gebied dat is geconfigureerd met de temperatuurmeetregel.
3. Klik met de rechtermuisknop op het livebeeld en selecteer **Temperatuurinformatie weergeven** in het rechtermuisknopmenu.
De temperatuur wordt weergegeven op het livebeeld.
4. Klik op de afbeelding om de gedetailleerde temperatuurinformatie te bekijken.



Figuur 5-11 Temperatuurinformatie op het Live beeld

5. Optioneel: Klik met de rechtermuisknop op het livebeeld en selecteer **Temperatuurinformatie verbergen** om de temperatuurinformatie te verbergen.

5.11.3 Temperatuur handmatig meten

Tijdens de live-weergave van de thermische camera kun je overal op het live-weergavebeeld klikken om de temperatuur van verschillende punten weer te geven, zodat je de brandhaard snel

kunt lokaliseren.

Stappen

Opmerking

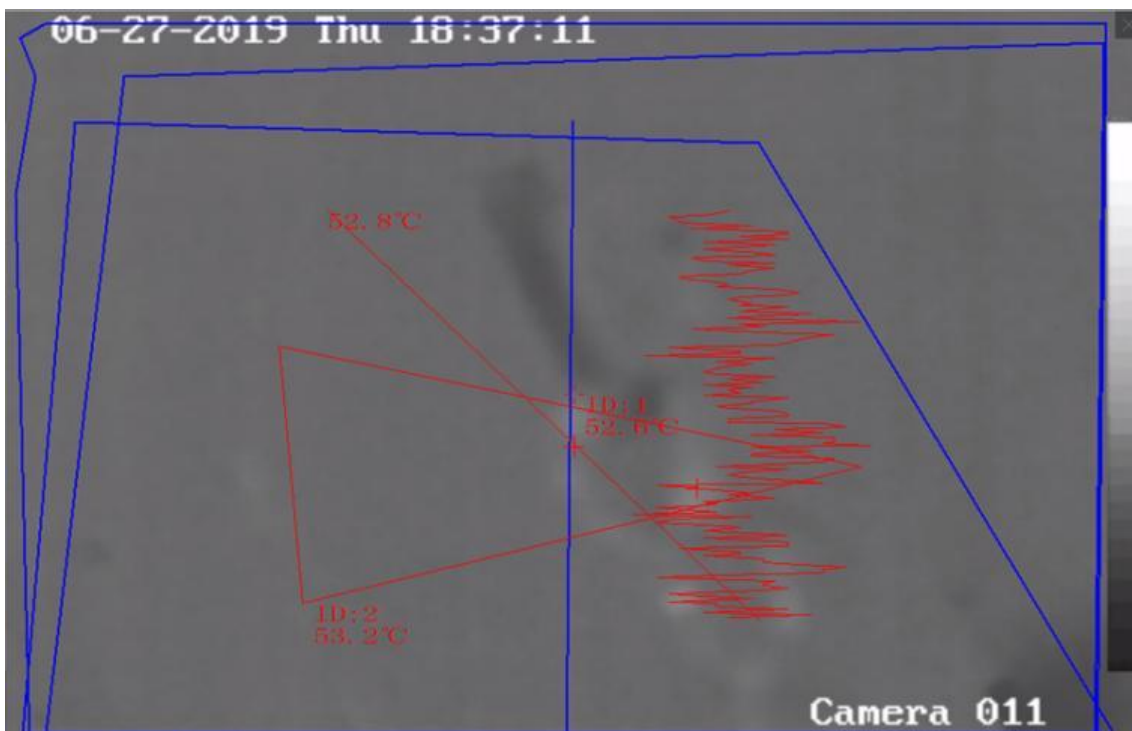
- De gemeten temperatuur wordt gedurende 5 seconden op het beeldscherm weergegeven.
 - Slechts de temperatuur van één punt kan worden weergegeven.
 - Wanneer meerdere clients de live video van één camera ontvangen, zal als één client meetpunten toevoegt of verwijdert, de live weergave van andere clients ook beïnvloed worden. De meetpunten worden gewist als alle gebruikers stoppen met het live bekijken van de camera.
-

1. Ga naar de pagina Hoofdweergave en start de liveweergave van een thermische camera.
-

Opmerking

Raadpleeg **Liveweergave starten** voor het starten van liveweergave.

2. Klik met de rechtermuisknop op het livebeeld en selecteer **Temperatuurinformatie weergeven**.
3. Klik op het livebeeld om de temperatuur van deze positie weer te geven.
De temperatuur van de aangeklikte punten wordt weergegeven op de afbeelding.



Afbeelding 5-12 Temperatuur op punten handmatig meten

4. Optioneel: Klik met de rechtermuisknop op het livebeeld en selecteer **Temperatuurinformatie verbergen** in het menu.

5.11.4 Vuurbrondetectiescherm gebied weergeven

Het detectieafschermingsgebied voor brandbronnen is een vooraf gedefinieerd gebied dat kan worden afgeschermd van detectie bij brandbronnen. Tijdens liveweergave kunt u het gebied op het beeld weergeven.

Klik met de rechtermuisknop op een livebeeld en selecteer **Schermgebied weergeven**. Het schildgebied wordt weergegeven op het warmtebeeld van de camera.

Opmerking

- Deze functie moet worden ondersteund door het apparaat.
 - Zorg ervoor dat je de functie Fire Source Detection Shield hebt ingeschakeld en geconfigureerd voor het apparaat. Raadpleeg de gebruikershandleiding van het apparaat voor meer informatie.
-



Figuur 5-13 Vuurbronschildgebied

5.13 Meer functies

Er worden nog enkele functies ondersteund in de live-weergave, waaronder hulpschermpreview, digitale zoom, kanaal-nul, tweewegaudio, camerastatus en synchronisatie.

Voorbeeld hulpschermbewaking

Geef de live video weer op verschillende hulpschermen voor een handige preview van meerdere bewakingsscènes.



Opmerking

Tot 3 hulpschermen worden ondersteund.

Digitale zoom

Sleep de muis om een rechthoek te tekenen in de richting rechtsonder/linksboven om in of uit te zoomen op het getekende gebied. Of gebruik het muiswiel om in digitale zoommodus in of uit te zoomen.

Kanaal-nul

Houd voor het kanaal-nul van het apparaat de Ctrl-toets ingedrukt en dubbelklik om het specifieke kanaal weer te geven. Houd de Ctrl-toets ingedrukt en dubbelklik nogmaals om te herstellen.

Audio in twee richtingen

Dankzij de bidirectionele audiofunctie kun je met de camera praten. Je kunt niet alleen de live video maar ook de real-time audio van de camera ontvangen. Als het apparaat meerdere tweerichtingsaudiokanalen heeft, kun je een kanaal selecteren om tweerichtingsaudio te starten.



Opmerking

- De tweewegaudio kan slechts voor één camera tegelijk worden gebruikt.
 - ABUS Link Station-apparaat ondersteunt het selecteren van een kanaal tijdens tweewegaudio niet.
-

Camerastatus

De camerastatus, zoals opnamestatus, signaalstatus, verbindingsnummer enz. kan worden gedetecteerd en weergegeven ter controle. De statusinformatie wordt elke 10 seconden vernieuwd.

Synchronisatie



De synchronisatiefunctie biedt een manier om de klok van het apparaat te synchroniseren met de pc waarop de clientsoftware draait.

Streamtype instellen

Automatisch wisselen van streamtype

De camera selecteert het streamtype aan de hand van de grootte van het weergavevenster. Als

het venstergedeelte kleiner is dan 9, is het streamtype hoofdstream, anders substream.
Er zijn drie manieren om het streamtype in te stellen:

- Beweeg de cursor in de bronnenlijst over de naam van een camera en klik op  → **Stream** om een streamtype te selecteren, of klik op **Automatisch streamtype wijzigen**. Je kunt deze handeling ook uitvoeren voor een apparaatgroep om het streamtype in te stellen voor alle apparaten in deze groep.
- Klik op  in de live weergave werkbalk en selecteer een streamtype. Zie [Pictogrammen op werkbalk instellen voor](#) meer informatie over het bewerken van de werkbalk.
- Klik met de rechtermuisknop op een liveweergavevenster en klik op **Stream** om een streamtype voor de camera te selecteren.



Opmerking

Deze functie moet worden ondersteund door het apparaat.

Client vergrendelen in de modus Volledig scherm

Druk op **Ctrl** en **L** op je toetsenbord om de client te vergrendelen nadat je naar de volledige schermmodus bent gegaan. Na het vergrendelen van de client kun je de client niet meer bedienen, ook niet de andere vensters in de huidige vensterindelingsmodus. Klik op **Ontgrendelen** bovenaan en voer het inlogwachtwoord voor de client in en klik op **Ontgrendelen** om de client te ontgrendelen.

Hoofdstuk 6 Weergave op afstand

Het apparaat neemt de video op volgens het opnameschema. U kunt de videobestanden bekijken die zijn opgeslagen op de opslagserver en het lokale apparaat, om het proces van het voorval te herstellen voor een postmortale analyse en een verder oordeel te vellen. Het opslaan van de gewaardeerde videobeelden kan basismateriaal leveren voor videoanalyse en videobewijs. De client ondersteunt meerdere afspeelmodi, zoals: VCA afspelen, gebeurtenis afspelen, enz.

Opmerking

Er zijn twee afspeelmodi: direct afspelen in de hoofdweergavemodule (raadpleeg [*Direct afspelen*](#) voor meer informatie) en videobestanden zoeken en afspelen in de Remote Playback-module. In dit hoofdstuk introduceren we alleen het afspelen in de Remote Playback module.

6.2 Externe opslagconfiguratie

De videobestanden en gemaakte foto's kunnen worden opgeslagen op de HDD's, Net HDD's of SD/SDHC-kaarten op het lokale apparaat of op de aangesloten opslagserver.

Opmerking

Deze functie moet worden ondersteund door het apparaat.

6.2.1 Foto en video opslaan op DVR, NVR of netwerkcamera

Sommige lokale apparaten, waaronder de DVR's, NVR's en netwerkcamera's, bieden opslagapparaten zoals HDD's, Net HDD's en SD/SDHC-kaarten voor video- en beeldbestanden. U kunt een opnameschema of opnameschema instellen voor de kanalen van de lokale apparaten.

Voordat u begint

Zorg ervoor dat de nieuw geïnstalleerde opslagapparaten geformatteerd zijn. Raadpleeg De [HDD van de opslagserver formatteren](#) voor meer informatie.

Voer deze taak uit als u de afbeeldings- en videobestanden moet opslaan op het codeerapparaat zoals een DVR, NVR of netwerkcamera.

Stappen

Opmerking

De afbeeldingen die via het vastlegschaema zijn vastgelegd, worden opgeslagen op het lokale apparaat en kunnen worden doorzocht op de configuratiepagina op afstand van het apparaat.

1. Ga naar de module Opslagschema.

2. Selecteer de camera in de lijst Cameragroep.
3. Zet de schakelaar **Opnameschema** of **Opnameschema** op AAN in het veld **Opslag op codeerapparaat om** lokaal opnemen of vastleggen in te schakelen.
4. Selecteer de sjabloon voor opname of vastleggen in de vervolgkeuzelijst.

Sjabloon voor de hele dag

De hele dag door opnemen.

Weekdag Sjabloon

Werkuren continue opname van 8:00 AM tot 20:00 PM.

Evenement Sjabloon

De hele dag door gebeurtenisgestuurd opnemen.

Sjabloon 01 tot 08

Vaste sjablonen voor specifieke planningen. Je kunt de sjablonen bewerken als dat nodig is.

Aangepast

Pas een sjabloon naar wens aan.

Opmerking

Als u de sjabloon wilt bewerken of aanpassen, raadpleeg dan [Opnameschema sjabloon configureren](#) of [Opnameschema sjabloon configureren](#).

5. Klik op **Geavanceerd** van Opnameschema om de geavanceerde opnameparameters in te stellen.

Opmerking

De weergegeven items variëren afhankelijk van het apparaat.

Vooraf opnemen

Normaal gebruikt voor de gebeurtenisgetriggerde opname, wanneer je wilt opnemen voordat de gebeurtenis plaatsvindt.

Na opname

Nadat het evenement is afgelopen, kan de video ook gedurende een bepaalde tijd worden opgenomen.

Videobestanden bewaren voor

De tijd voor het bewaren van de videobestanden op het opslagapparaat, zodra deze wordt overschreden, worden de bestanden verwijderd. De bestanden worden permanent opgeslagen als de waarde is ingesteld op 0.

Overbodige opname

Sla de videobestanden niet alleen op de R/W HDD op, maar ook op de redundante HDD.

Audio opnemen

Neem de videobestanden op met audio of niet.

Videostream

Selecteer het streamtype voor de opname.

Opmerking

Voor specifieke apparaten kun je **Dual-Stream** selecteren om zowel de hoofdstream als de substream van de camera op te nemen. In deze modus kunt u tijdens het afspelen op afstand het streamtype wijzigen. Raadpleeg **Normaal afspelen** voor het wisselen van stream tijdens het afspelen.

6. Klik op **Geavanceerd** van Vastlegschema om de geavanceerde vastlegparameters in te stellen.

Resolutie

Selecteer de resolutie voor de continu of event-opnamen.

Beeldkwaliteit

Stel de kwaliteit in voor foto's die continu of tijdens een gebeurtenis worden gemaakt.

Interval

Selecteer het interval dat verwijst naar de tijdsperiode tussen twee vastlegacties.

Vastgelegd beeldnummer

Stel het beeldnummer in voor het vastleggen van gebeurtenissen.

7. Optioneel: Klik op **Kopiëren naar...** om de instellingen van het opnameschema te kopiëren naar andere kanalen.
8. Klik op **Opslaan** om de instellingen op te slaan.

6.2.3 Afbeelding en extra informatie opslaan op lokale pc

Je kunt de foto's en de extra informatie, zoals de warmtekaart, gegevens over het tellen van mensen en verkeersgegevens, opslaan op de lokale pc.

Voer deze taak uit als u foto's en extra informatie op de lokale pc wilt opslaan.

Stappen

1. Ga naar de module **Opslagschema**.
2. Selecteer de camera in de lijst Cameragroep.

Opmerking

Deze functie moet worden ondersteund door het apparaat.

3. Selecteer opslaginhoud.

Afbeeldingen opslaan

Sla de alarmfoto's van de camera op wanneer zich een gebeurtenis voordoet. U kunt klikken

op **Systeemconfiguratie** → **Bestand** om het pad voor het opslaan van afbeeldingen te wijzigen.

Extra informatie Opslag

Sla de aanvullende informatie (bijv. hittekaart, gegevens over het tellen van mensen, etc.) op een lokale pc op.

4. Klik op **Opslaan** om de instellingen op te slaan.

6.2.4 Opnameschema sjabloon configureren


Je kunt de opnamesjabloon bewerken of een opnamesjabloon aanpassen.

Stappen

1. Ga naar de module Opslagschema.

2. Open het venster met sjablooninstellingen.


Selecteer **Sjabloon 01** tot **Sjabloon 08** in de vervolgkeuzelijst en klik op **Bewerken**. Selecteer **Aangepast** in de vervolgkeuzelijst.

3. Sleep op de tijdlijn om de tijdsperioden voor de geselecteerde sjabloon in te stellen wanneer de cursor verandert in  .


Doorlopend

Normaal en continu opnemen. De tijdbalk van het schema is gemarkeerd met  .

Evenement opnemen

De opname wordt geactiveerd door een gebeurtenis. De tijdbalk van de planning is gemarkeerd met  .

Opdracht

De opname wordt geactiveerd door een opdracht. De tijdbalk van de planning is gemarkeerd met  .




Opmerking


Voor elke dag kunnen maximaal 8 tijdsperioden worden ingesteld in het opnameschema.

4. Optioneel: Na het instellen van de tijdsperioden kun je een of meer van de volgende dingen doen:

Verplaats




Sleep een periode om deze te verplaatsen wanneer de cursors naar  gaan.

Verlengen of verkorten

Selecteer een tijdsperiode en verleng of verkort deze wanneer de cursor verandert in  .

Nauwkeurige tijd instellen

Klik op een tijdsperiode om de precieze begin- en eindtijd van de periode in te stellen.

Verwijder	Selecteer de geconfigureerde planningstijdperiode en klik op  om deze te verwijderen.
Alles verwijderen	Klik op  om alle geconfigureerde perioden te verwijderen.
Kopiëren naar	Selecteer een datum en klik op  om de periode-instellingen van de datum te kopiëren naar de andere datums.

5. Optioneel: Voor sjabloon 01 tot 08 kunt u de naam van de sjabloon naar wens bewerken.
6. Klik op **OK** om de instellingen op te slaan.


Opmerking

Als je **Aangepast** selecteert om een sjabloon aan te passen, kun je klikken op **Opslaan als sjabloon**, waarna de aangepaste sjabloon kan worden opgeslagen als sjabloon 01 t/m 08.

6.2.5 Vastlegschemasjabloon configureren

U kunt de vastlegschemasjabloon bewerken of een vastlegschemasjabloon aanpassen.


Stappen

1. Ga naar de module Opslagschema.
2. Open het venster met sjablooninstellingen.
Selecteer **Sjabloon 01** tot **Sjabloon 08** in de vervolgkeuzelijst en klik op **Bewerken**. Selecteer **Aangepast** in de vervolgkeuzelijst.
3. Sleep op de tijdlijn om tijdsperioden in te stellen voor de geselecteerde sjabloon wanneer de cursor verandert in  .





Continu vastleggen


Normale en continue opname. De tijdbalk van de planning is gemarkeerd met  .

Gebeurtenis vastleggen

Het vastleggen wordt geactiveerd door een gebeurtenis. De tijdbalk van de planning is gemarkeerd met  .

4. Optioneel: Na het instellen van de tijdsperiode kun je een of meer van de volgende dingen doen

Verplaats	Wanneer de cursor verandert in  , kunt u de periode die u zojuist hebt bewerkt verplaatsen. U kunt ook het weergegeven tijdpunt bewerken om de juiste tijdsperiode in te stellen.
Verlengen of verkorten	Wanneer de cursor op  staat, kunt u de geselecteerde tijdsperiode verlengen of verkorten.
Verwijder	Selecteer een periode en klik op  om deze te verwijderen.
Alles verwijderen	Klik op  om alle geconfigureerde perioden te verwijderen.

Kopiëren naar Selecteer een datum en klik op  om de periode-instellingen van de datum te kopiëren naar de andere datums.

5. Optioneel: Voor sjabloon 01 tot 08 kunt u de naam van de sjabloon naar wens bewerken.
6. Klik op **OK** om de instellingen op te slaan.

 **Opmerking**

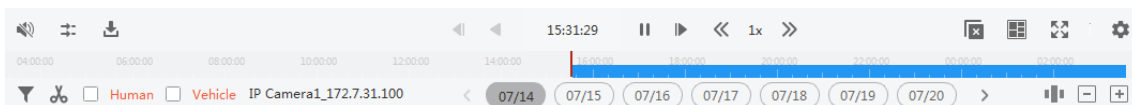
Als je **Aangepast** selecteert om een sjabloon aan te passen, kun je klikken op **Opslaan als sjabloon**, waarna de aangepaste sjabloon kan worden opgeslagen als sjabloon 01 t/m 08.

6.3 Werkbalk voor afspelen

Wanneer u video afspeelt op de Remote Playback-module, kunt u de hulpmiddelen in de werkbalk gebruiken om verschillende functies uit te voeren.







 **Opmerking**












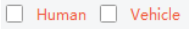
De tools in de verschillende afspelmodes kunnen verschillen. In dit deel maak je kennis met de tools in de module Camera afspelen.




Figuur 6-2 Werkbalk voor afspelen

Tabel 6-1 Werkbalk voor afspelen

Pictogram	Naam pictogram	Beschrijvingen
	Achteruit afspelen	Speel de videobestanden omgekeerd af.
	Pauzeren/afspelen	Het videobestand pauzeren/afspelen.
	Alles sluiten	Sluit alle spelende videobestanden.
	Enkel frame (Achteruit)	Speel de videobestanden frame voor frame achteruit af.
	Enkel frame	Speel de videobestanden frame per frame af.
	Langzaam vooruit/Snel vooruit	Stel de afspeelsnelheid in en speel de videobestanden langzaam of snel af volgens deze snelheid.


Pictogram	Naam pictogram	Beschrijvingen
	Volume	Klik op dit pictogram om de audio te openen/sluiten en het volume aan te passen.
	Clip	Stel de begin- en eindtijd in voor het knippen en download het geknipte videobestand naar de lokale schijf.
	Downloaden voor meerdere camera's	Stel de starttijd en eindtijd in voor meerdere camera's en download de videobestanden van meerdere camera's tegelijkertijd.
	Venster divisie	Stel de vensterverdeling in.
	Volledig scherm	Speel videobestand(en) af op volledig scherm. Druk op ESC om af te sluiten.
	Asynchroon afspelen/Synchroon afspelen	<p>Schakel over naar de asynchrone/synchrone afspeelmodus.</p> <hr/> <p> Opmerking Raadpleeg <i>Synchroon afspelen</i> voor meer informatie.</p> <hr/>
	Instellingen	Ga naar de module Instellingen videoparameters en configureer de parameters voor liveweergave en afspelen, beeld, bestanden en werkbalk.
	Filter	Filter de videobestanden op opnametype.
	Nauwkeurige positionering	Stel de juiste tijd in voor het afspelen van videobestand(en).
	Videodatum	<p>De datum van het videobestand dat momenteel wordt afgespeeld. U kunt snel schakelen om de videobestanden op een andere datum af te spelen.</p> <p>Als je bijvoorbeeld de datum instelt op 07/30, wordt de video automatisch weergegeven vanaf 00:00 op 30 juli (als er op dat moment video is).</p>
	Filter Mens- of voertuigerelateerde video	Vink Mens of Voertuig aan om de video's te filteren waarbij een menselijk lichaam of voertuig is gedetecteerd. De video met een menselijk lichaam of voertuig wordt oranje gemarkeerd op de tijdbalk en je kunt de video snel vinden op de tijdbalk.

Pictogram	Naam pictogram	Beschrijvingen
		 Opmerking Deze functie moet worden ondersteund door het apparaat, anders is de Human of Vehicle grijs en kan deze niet worden gecontroleerd.

6.4 Normaal afspelen

Je kunt videobestanden zoeken op camera of groep voor normaal afspelen en gevonden videobestanden downloaden naar de lokale pc. Je kunt ook een tag toevoegen om belangrijk videomateriaal te markeren, enzovoort.

Je kunt met de rechtermuisknop op het afspeelvenster klikken om de gewenste bewerkingen te selecteren in het snelmenu. Sommige worden als volgt opgesomd:

Naam	Beschrijving
Temperatuurinformatie tonen/verbergen	Temperatuurinformatie tonen/verbergen <hr/>  Opmerking De overlay met temperatuurinformatie wordt alleen ondersteund door thermische camera's.
Labelcontrole	Voeg standaard (de standaard tagnaam is TAG) of aangepaste tag (de tagnaam is aangepast) toe aan het videobestand om het belangrijke videopunt te markeren. U kunt de tag ook bewerken of gemakkelijk naar de tagpositie gaan.
Andere opnamemodi	<ul style="list-style-type: none"> ● Vastgelegde foto afdrukken: Een foto vastleggen en afdrukken. ● E-mail verzenden: Leg het huidige beeld vast en stuur vervolgens een e-mailmelding naar een of meer ontvangers. De vastgelegde afbeelding kan als bijlage worden toegevoegd. ● Aangepast vastleggen: De huidige foto vastleggen. U kunt de naam bewerken en vervolgens opslaan.


Opmerking

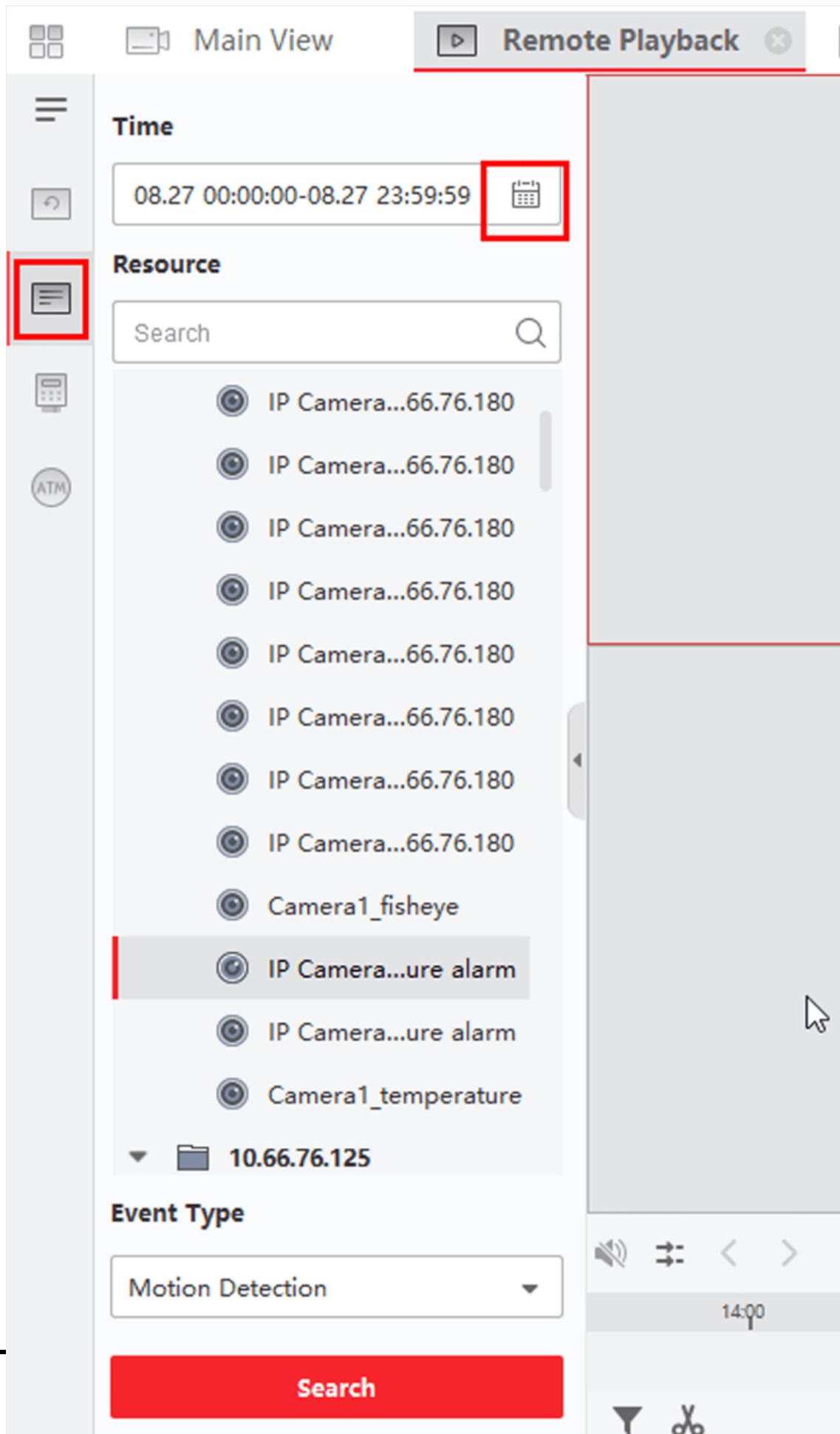
- Het ABUS Link Station-apparaat ondersteunt alleen normaal afspelen en ondersteunt ook niet de functies voor achteruit afspelen, langzaam vooruitspoelen of snel vooruitspoelen en tag toevoegen.
 - Voor NVR's die aan de client zijn toegevoegd met een andere gebruikersnaam (behalve admin), geldt dat als **dubbele verificatie** is ingeschakeld op deze NVR, u bij het afspelen van video's op de client de gebruikersnaam en het wachtwoord moet invoeren die zijn ingesteld voor dubbele verificatie. Raadpleeg de gebruikershandleiding van de NVR voor meer informatie over dubbele verificatie.
-

6.4.1 Videobeelden zoeken


Je kunt de videobeelden doorzoeken op datum en je kunt ook een trefwoord invoeren om de overeenkomende resultaten te filteren voor normaal afspelen.

Stappen



1. Ga naar de Remote Playback-module.
2. Klik op  aan de linkerkant om de pagina Camera afspelen te openen.



Figuur 6-3 Videobestanden zoeken

3. Optioneel: Klik op  om de begindatum en einddatum van de zoekperiode in te stellen.

Opmerking

In de kalender wordt de datum waarop videobeelden zijn opgenomen volgens schema gemarkeerd met  en wordt de datum waarop videobeelden zijn opgenomen op basis van een gebeurtenis gemarkeerd met .

4. Start het afspelen van camera('s) om de videobeelden van de geselecteerde camera('s) te zoeken. U kunt een van de volgende handelingen uitvoeren om het afspelen te starten.

Opmerking

Er kunnen maximaal 16 camera's tegelijkertijd worden doorzocht.

- Sleep de camera of groep naar een weergavevenster.
- Selecteer een weergavevenster en dubbelklik op de camera of groep om het afspelen in het geselecteerde venster te starten.
- Dubbelklik achtereenvolgens op de camera's om automatisch het weergavevenster te selecteren en het afspelen in de vensters te starten.

6.4.2 Video afspelen

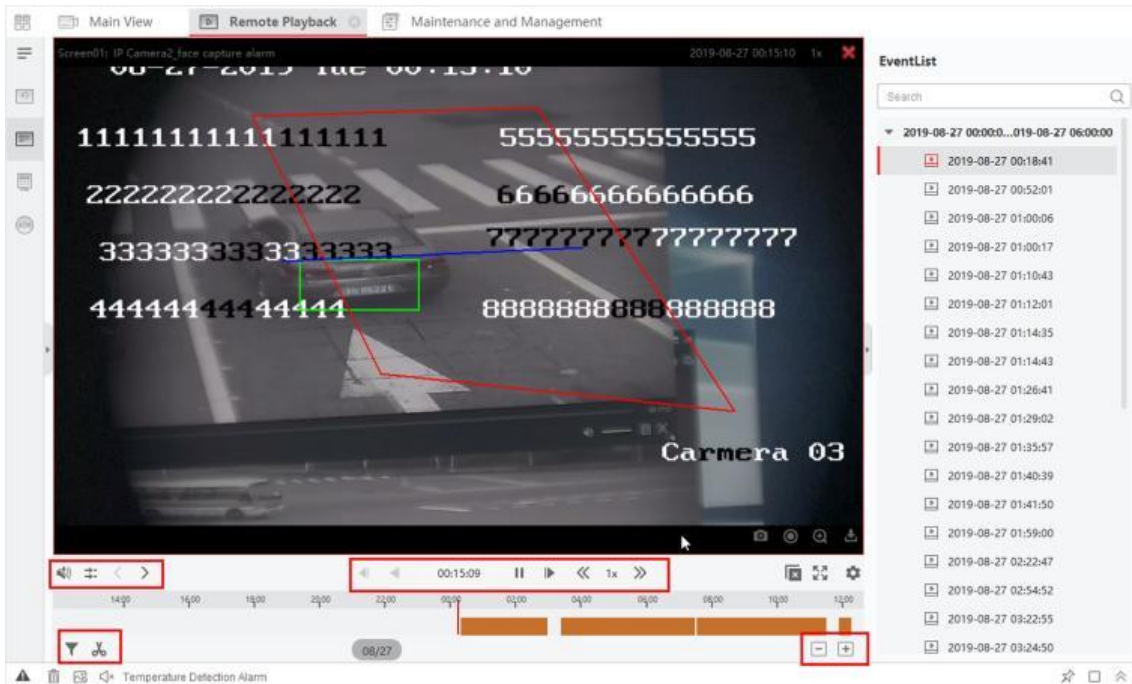
Na het zoeken van de videobeelden voor normaal afspelen, kun je de video afspelen via de tijdslijn.

Stappen

1. Ga naar de Remote Playback-module.
2. Doorzoek de videobeelden.
3. Video afspelen via tijdslijn.


Je kunt op **Stream** → **Hoofdstroom / Substream klikken** om het streamtype te wisselen voor afspelen volgens je eigenlijke behoefte.

De videobeelden worden automatisch afgespeeld. Je kunt op de tijdlijn klikken om het gewenste videosegment van de opgegeven tijd te positioneren voor normaal afspelen.






Figuur 6-4 Videobeelden afspelen


Opmerking

- De tijdlijn geeft de tijdsduur van de videobeelden aan en de videobeelden van verschillende types hebben een kleurcode. Tijdens het afspelen kun je de bitrate, framesnelheid en resolutie-informatie op het beeld bekijken.
- Je kunt het muiswiel gebruiken of klikken op  om de tijdlijn balk te vergroten of te verkleinen.

4. Optioneel: Voer de volgende bewerkingen uit op de werkbalk om het afspelen te regelen.


Enkel frame (Achteruit) Klik op  of scroll met het muiswielje omlaag om de videobeelden frame voor frame (omgekeerd) af te spelen.

Audiobediening Klik op  of  om het geluid uit/aan te zetten. U kunt ook het volume aanpassen bij het inschakelen.

Downloaden voor meerdere camera's Klik op  om videobeelden van meerdere camera's tegelijk te downloaden.

Opmerking

Raadpleeg ***Download voor meerdere camera's*** voor meer informatie.

Videobestanden downloaden op Klik op  om de videobeelden van de camera op datum en tijd te downloaden en op te slaan op de lokale pc. De voortgang van het

datum	downloaden wordt rechtsboven op de pagina weergegeven en u kunt het downloaden handmatig onderbreken.
Nauwkeurige positionering	Klik op 09:25:46 om het nauwkeurige tijdstip in te stellen waarop het videobestand moet worden afgespeeld.
Naar de afbeelding van een miniatuur springen	Klik op  in de rechterbenedenhoek om de miniatuurfunctie in te schakelen en plaats de cursor op de tijdlijn om de miniatuur van het punt te tonen. Klik op de miniatuur om naar de afbeelding ervan te springen.

 **Opmerking**

Deze functie moet worden ondersteund door apparaten.

6.5 Alarm ingang afspelen

Wanneer de alarmingang wordt geactiveerd en de gekoppelde video kan worden gezocht voor het afspelen van de alarmingang. Deze functie vereist ondersteuning van het aangesloten apparaat. Raadpleeg ***Normale weergave*** voor de beschrijving van de afspelerbalk voor de wekkingang en het rechtsklikmenu van het weergavevenster.


 **Opmerking**

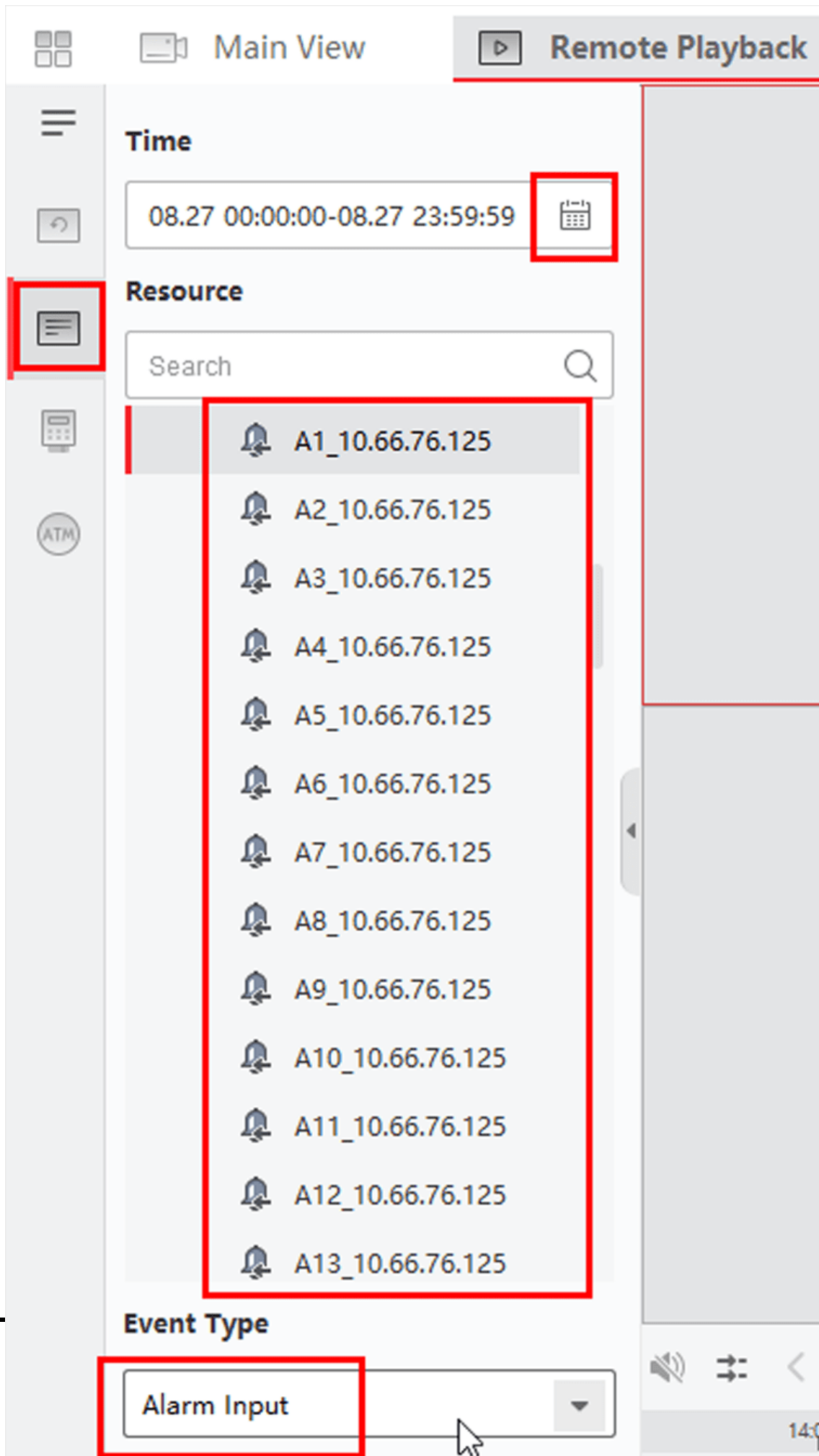
Sommige pictogrammen zijn mogelijk niet beschikbaar voor het afspelen van wekkingangen.

6.5.1 Videobeelden zoeken


U kunt de videobeelden zoeken op datum en u kunt ook een trefwoord invoeren om de overeenkomende resultaten te filteren voor het afspelen van alarminvoer.

Stappen

1. Ga naar de Remote Playback-module.
2. Klik op  aan de linkerkant om de pagina Gebeurtenissen afspelen te openen.



Figuur 6-5 Videobestanden zoeken

3. Selecteer links een alarmingangskanaal.
4. Optioneel: Klik op  om de begindatum en einddatum van de zoekperiode in te stellen.
5. Selecteer **Alarmingang** uit de vervolgkeuzelijst als gebeurtenistype.
6. Klik op **Zoeken** om het zoeken te starten.


De overeenkomende videobeelden van de geselecteerde alarmingang worden in chronologische volgorde op de rechterpagina weergegeven. En standaard wordt de eerste video automatisch afgespeeld.

7. Optioneel: Voer een trefwoord in het veld **Zoeken in** om de resultaten te filteren.

6.5.2 Videobeelden afspelen

Na het zoeken van de videobeelden voor het afspelen van de alarmingang, kunt u de video afspelen via de bestandslijst of tijdlijn.

Stappen


1. Ga naar de Remote Playback-module.
2. Klik op  aan de linkerkant om de pagina Gebeurtenissen afspelen te openen.
3. Zoek de videobeelden van de alarmingang.

Opmerking

Zie [Videobeelden zoeken](#) voor meer informatie over het zoeken van videobeelden van de alarmingang.

4. Video afspelen via bestandslijst of tijdlijn.
 - Dubbelklik op de videobeelden om de video af te spelen in het weergavevenster.
 - Klik op de tijdlijn om het gewenste videosegment van de opgegeven tijd te positioneren voor het afspelen van de alarmingang.

Opmerking

- De tijdlijn geeft de tijdsduur van de videobeelden aan en de videobeelden van verschillende typen hebben een kleurcode.
 - Je kunt het muiswiel gebruiken of klikken op  om de tijdsbalk omhoog of omlaag te schalen.
-

6.6 Gebeurtenissen afspelen

De opgenomen videobestanden die zijn geactiveerd door een gebeurtenis, zoals bewegingsdetectie, VCA-detectie of abnormale gebeurtenisdetectie, kunnen worden doorzocht voor het afspelen van gebeurtenissen. Deze functie vereist ondersteuning van het aangesloten apparaat.

Raadpleeg [Normale weergave](#) voor een beschrijving van de werkbalk voor het afspelen van

gebeurtenissen en het rechtsklikmenu van het weergavevenster.



Opmerking

Sommige pictogrammen zijn mogelijk niet beschikbaar voor het afspelen van gebeurtenissen.



6.6.1 Videobeelden/foto zoeken

Je kunt video's/foto's van evenementen zoeken op datum en eventtype.

Stappen

1. Ga naar de Remote Playback-module.
 2. Klik op  aan de linkerkant om de pagina Gebeurtenissen afspelen te openen.
 3. Klik op  om de begin- en einddatum van het zoeken in te stellen.
-

Opmerking

In de kalender wordt de datum waarop videobeelden zijn opgenomen volgens schema gemarkeerd met , en de datum waarop videobeelden zijn opgenomen op basis van een gebeurtenis wordt gemarkeerd met  .

4. Selecteer **Video** of **Afbeelding** als de inhoud waarnaar u wilt zoeken.
5. Selecteer een camera uit de bronnenlijst.
6. Selecteer een gebeurtenistype in de vervolgkeuzelijst **gebeurtenistype**.
7. Klik op **Zoeken**.
 - Als je **Video** selecteert als de gezochte inhoud, worden de overeenkomende videobeelden in chronologische volgorde op de rechterpagina weergegeven. En standaard wordt het eerste videobestand automatisch afgespeeld.
 - Als u **Afbeelding** selecteert als de gezochte inhoud, worden de overeenkomende afbeeldingen automatisch weergegeven op de rechterpagina.

6.6.2 Videobeelden/afbeelding bekijken


Wanneer de camera gebeurtenissen detecteert (zoals lijnoverschrijding, bewegingsdetectie en detectie van abnormale gebeurtenissen) of het buitenstation een videogesprek voert, zal het de gekoppelde camera activeren om videobeelden op te nemen of foto's vast te leggen. U kunt de videobeelden of foto's zoeken en de video's afspelen via de bestandslijst of tijdlijn en de foto's op hun beurt bekijken.

Stappen



Opmerking

Voor het buitenstation ondersteunt alleen de DS-KV8123-M de volgende bewerkingen.

1. Ga naar de Remote Playback-module.
-

2. Klik op  aan de linkerkant om de pagina Gebeurtenissen afspelen te openen.
3. De opgenomen videobeelden of foto's zoeken op basis van de gebeurtenis.
4. Videobeelden of foto's bekijken.
 - Dubbelklik op de videobeelden om de video af te spelen in het weergavevenster.
 - Gezochte foto's worden automatisch afgespeeld.

Opmerking

- De tijdlijn geeft de tijdsduur voor de videobestanden aan en de videobestanden van verschillende types hebben een kleurcode.
- Je kunt het muiswiel gebruiken of klikken op   om de tijdsbalk omhoog of omlaag te schalen.

-
5. Optioneel: Voer de volgende bewerkingen uit als dat nodig is.

Speelbeelden van bepaalde tijd	Klik op de tijdlijn om een videosegment van het opgegeven tijdstip weer te geven voor het afspelen van een gebeurtenis.
Toon beelden met mens en/of voertuig	Vink onder de tijdlijn Mens en/of Voertuig aan om beelden weer te geven die mensen of voertuigen bevatten.
Schakelaar Foto's	Klik op  of  om naar de vorige of volgende afbeelding te gaan.
Beeldweergave-interval instellen	Klik op  om het interval van de beeldweergave in te stellen.
Afbeeldingen op volledig scherm weergeven	Klik op  om foto's op het volledige scherm weer te geven.
Afbeeldingen weergeven in lijstmodus	Klik op  om foto's in lijstmodus weer te geven. Klik op  om over te schakelen naar de miniatuurmodus.
Foto's downloaden	Klik op  en controleer afbeeldingen en klik op Downloaden om de geselecteerde afbeeldingen naar je pc te downloaden.
Video's downloaden	Klik op  , selecteer meerdere videobestanden en klik op Downloaden om videobestanden naar je pc te downloaden.

6.9 VCA afspelen

Voor de gezochte videobestanden kun je VCA-regels instellen om de videobeelden te vinden die een VCA-gebeurtenis vertonen, zoals bewegingsdetectie, detectie van lijnoverschrijding en

inbraakdetectie. Deze functie helpt bij het zoeken naar de video die u mogelijk meer zorgen baart en markeert deze met een rode kleur.


Voordat u begint

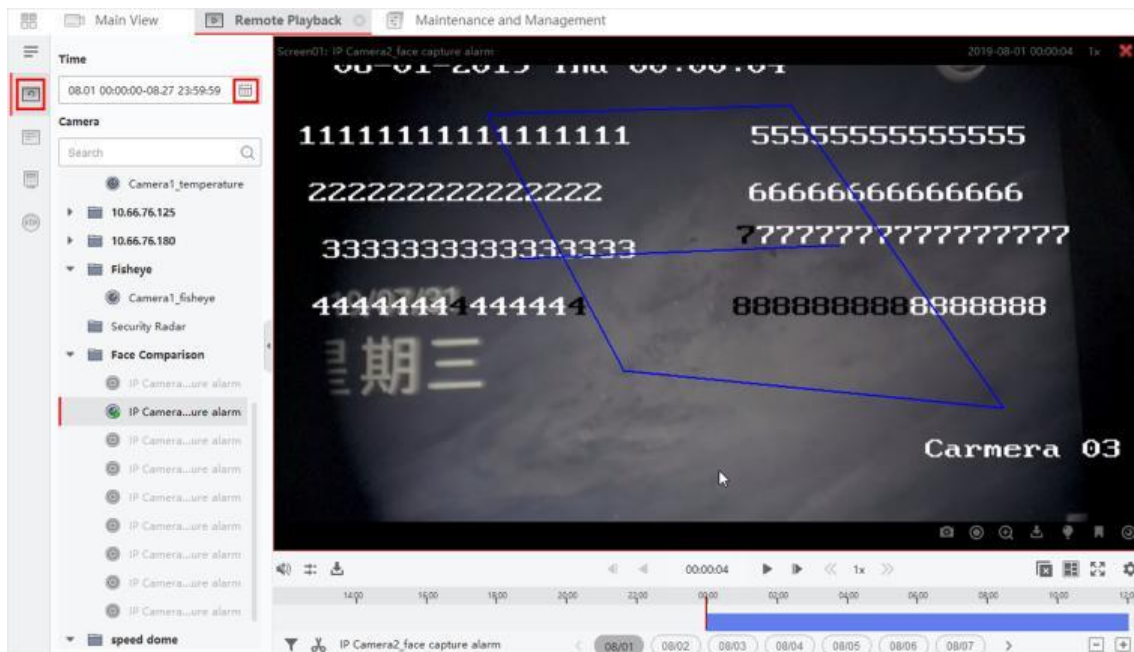
Zorg ervoor dat het apparaat met VCA-functie geïnstalleerd is.

Stappen


Opmerking

VCA afspelen wordt alleen ondersteund in een enkel venster, synchroon en asynchroon afspelen worden niet ondersteund.

1. Ga naar de Remote Playback-module.
2. Klik op  aan de linkerkant om de pagina Camera afspelen te openen.
3. Selecteer de camera en start de videoweergave van de camera.



Figuur 6-9 VCA afspelen

4. Ga naar het menu VCA zoeken.
 - Klik met de rechtermuisknop op het afspeelvenster om het snelmenu op te roepen en klik vervolgens op **VCA Search**.
 - Klik op  in de rechterbenedenhoek van het afspeelvenster.
5. Schakel het VCA-type in, teken het detectiegebied en stel de gevoeligheid in.

Bewegingsdetectie

Wanneer het zicht op de video verandert (zoals een persoon passeert, de lens wordt bewogen), worden de videobeelden gemarkeerd als rode kleur op de tijdlijn, die wordt gebruikt voor de automatische alarmscène of geen bewakingscène.

Lijnovergangdetectie

Je kunt een virtuele lijn op de video tekenen en de videobeelden worden als rode kleur op de tijdlijn gemarkeerd wanneer de client in twee richtingen mensen, voertuigen en andere bewegende objecten detecteert die de virtuele lijn overschrijden.

Inbraakdetectie


Je kunt een virtueel gebied op de video tekenen en de videobeelden zullen als rode kleur op de tijdlijn worden gemarkeerd wanneer er mensen, voertuigen en andere bewegende objecten in het vooraf gedefinieerde gebied binnendringen.

VCA-instellingen

Stel de gevoeligheid in en filter de gezochte videobestanden door de doeltkens in te stellen. De videobeelden worden met een rode kleur gemarkeerd op de tijdlijn wanneer een persoon (waarvan de kenmerken overeenkomen met de ingestelde kenmerken) in de video voorkomt.

Opmerking

Hoe hoger de gevoeligheid, hoe nauwkeuriger de gematchte persoon is.

6. Optioneel: Klik op  om de begindatum en einddatum van de zoekperiode in te stellen.

7. Start het afspelen van de VCA.

De VCA-gebeurtenissen in het gedefinieerde gebied worden rood gemarkeerd op de tijdlijn.

Opmerking

- Standaard is de afspeelsnelheid van de betreffende video 1X, en de afspeelsnelheid van de onbezorgde video 8X.
 - U kunt instellen om de onbezorgde video over te slaan tijdens VCA-weergave in Systeemconfiguratie en de onbezorgde video wordt niet afgespeeld tijdens VCA-weergave. Raadpleeg [Liveweergave- en afspeelparameters instellen](#) voor meer informatie.
 - Als u het afspelen van VCA wilt uitschakelen, klikt u met de rechtermuisknop op het venster VCA afspelen en klikt u op **VCA zoeken** om het afspelen van VCA uit te schakelen.
-

6.10 Synchrono afspelen


Standaard speelt de client de videobestanden van meerdere camera's af in de asynchrone afspeelmodus: de afspeeltijd van verschillende videobestanden kan verschillen. Bij synchrono afspelen kunnen de videobestanden synchrono worden afgespeeld.

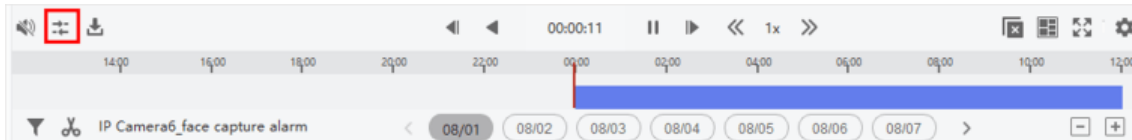
Stappen

Opmerking

- Videobestanden van maximaal 16 camera's kunnen tegelijkertijd worden afgespeeld.
 - Synchrono en asynchrone afspelen worden niet ondersteund in de ATM-videoweergavemodus en de VCA-afspeelmodus.
 - Gebeurtenisvideoweergave en POS-videoweergave ondersteunen alleen synchrono afspelen.
-


Om meerdere camera's te koppelen, gaat u naar **Onderhoud en beheer** → **Gebeurtenisbeheer** en schakelt u de gekoppelde camera in op basis van het eventtype.

1. Ga naar de Remote Playback-module.
2. Start de weergave van ten minste twee camera's.
3. Klik op  in de werkbalk om synchroon afspelen in te schakelen.



Figuur 6-10 Synchroon afspelen uitschakelen

De camera onder weergave start synchroon afspelen.

4. Klik op  om synchroon afspelen uit te schakelen.

6.11 De videoweergave van de Fisheye-camera

Bij het afspelen van de video van de fisheye-camera kan het beeld vervormd zijn. Om de details beter waar te nemen, kun je de fisheye-uitbreidingsfunctie inschakelen om het beeld te corrigeren als een onvervormd beeld. De client ondersteunt meerdere fisheye-uitbreidingsmodi, zoals: panorama, halve bol, PTZ, fisheye+PTZ-modus.

Voordat u begint

Zorg ervoor dat je Microsoft DirectX component geïnstalleerd is.

Stappen


Opmerking

Raadpleeg **Normale weergave** voor andere afspeelinstructies. Sommige pictogrammen zijn mogelijk niet beschikbaar voor fisheye-weergave.

1. Ga naar de Remote Playback-module.
2. Selecteer een fisheye camera om het afspelen te starten.



Opmerking

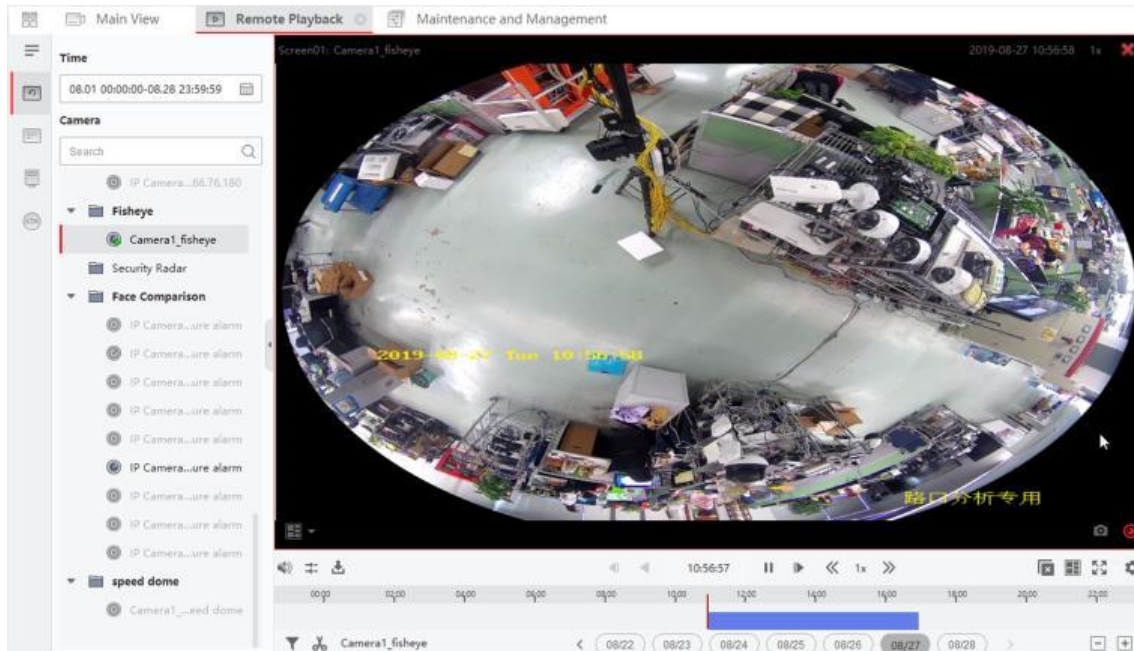
Raadpleeg **Normale weergave** voor gedetailleerde configuratie over afspelen en afspelbesturing.

3. Activeer de modus Fisheye-uitbreiding.
 - Klik met de rechtermuisknop op het weergavevenster en selecteer **Fisheye Expansion**.
 - Klik op  in de werkbalk. Zie **Pictogrammen op werkbalk instellen voor** meer informatie over het instellen van de werkbalk.
-


Opmerking

Het montage-type in de weergave van de fisheye-uitbreiding wordt ingesteld volgens het montage-type in liveweergave. Raadpleeg [Liveweergave uitvoeren in fisheye-modus](#) voor meer informatie

 gaat naar  .



Figuur 6-11 De videoweergave van de Fisheye-camera

4. Klik op  in de linkerbenedenhoek van het weergavegebied om de gewenste uitbreidingsmodus voor afspelen te selecteren.

Fisheye

In de Fisheye-weergavemodus wordt het volledige groothoekbeeld van de camera weergegeven. Deze weergavemodus wordt **Fisheye** genoemd omdat het het zicht van het bolle oog van een vis benadert. De lens produceert kromlijnige beelden van een groot gebied, terwijl het perspectief en de hoeken van objecten in het beeld worden vervormd.

Panorama / Dubbel-180° Panorama / 360° Panorama

In de modus Panoramaweergave wordt het vervormde fisheye-beeld getransformeerd naar een normaal perspectiefbeeld door middel van een aantal kalibratiemethoden.

PTZ

De PTZ-weergave is de close-up weergave van een bepaald gebied in de Fisheye-weergave of Panoramaweergave en ondersteunt de elektronische PTZ-functie, ook wel e-PTZ genoemd.

 **Opmerking**

Elke PTZ-weergave is gemarkeerd op de Fisheye-weergave en Panoramaweergave met een specifiek navigatievak. Je kunt het navigatievak slepen op de Fisheye-weergave of Panoramaweergave om de PTZ-weergave aan te passen, of sleep de PTZ-weergave om de weergave aan te passen aan de gewenste hoek.

Halve bol

In de halve bol-modus kun je de afbeelding slepen en roteren, gecentreerd op de diameter, om de weergave aan te passen aan de gewenste hoek.

AR halve bol

De AR halve bol modus overlapt beelden veraf en dichtbij, zodat je een dimensionaal beeld in een brede hoek kunt bekijken.

Cilinder

In de cilindermodus wordt het beeld gevormd tot een cilinderpagina en kun je het beeld naar elke gewenste richting slepen om overal in het detectiegebied te kijken.

5. Optioneel: Klik met de rechtermuisknop op een spelend venster in de Fisheye-weergavemodus en je kunt het geselecteerde venster overschakelen naar de schermvullende modus.

 **Opmerking**

Je kunt met de rechtermuisknop op het venster klikken en **Volledig scherm afsluiten** selecteren om de modus Volledig scherm af te sluiten.

6.13 Videobeelden downloaden

Tijdens het afspelen kunt u de videobestanden van één camera of meerdere camera's downloaden naar de lokale pc.

6.13.1 Videobeelden downloaden op datum

Tijdens het afspelen kun je de videobeelden van de camera downloaden en opslaan op de lokale pc.

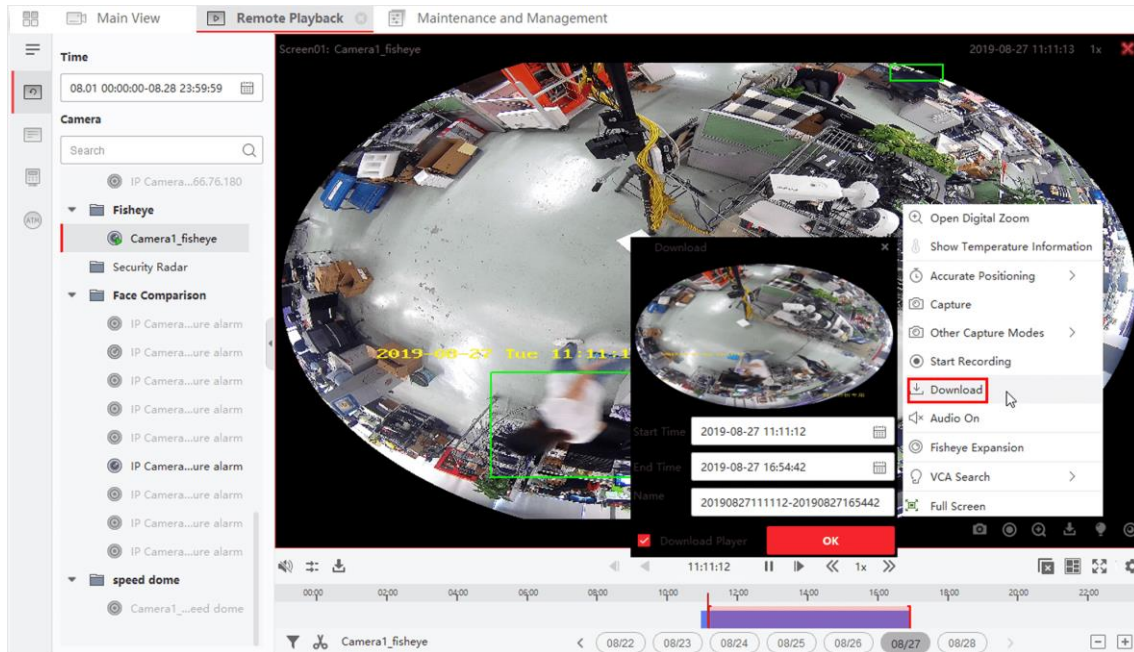
Stappen

1. Open de Remote Playback-pagina en selecteer een camera om het afspelen te starten.

 **Opmerking**

Raadpleeg **Afspelen op afstand** voor meer informatie over het starten van het afspelen.

2. Klik met de rechtermuisknop op de afbeelding en klik op **Downloaden**.



Figuur 6-12 Videobeelden downloaden op datum

3. Stel de begin- en eindtijd van de te downloaden videobeelden in.
4. Voer een naam in voor de videobeelden.
5. Klik op **OK** om het downloaden van de videobeelden naar de lokale pc te starten.

6.13.2 Downloaden voor meerdere camera's


Tijdens het afspelen van meerdere camera's kunt u de videobestanden van meerdere camera's tegelijkertijd downloaden op datum.

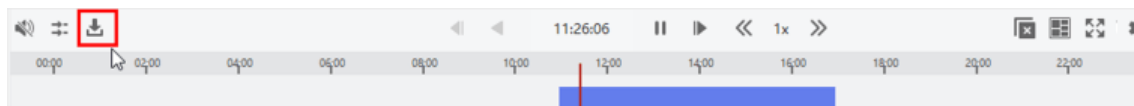
Stappen

1. Open de Remote Playback pagina en selecteer meerdere camera's om het afspelen te starten.

Opmerking

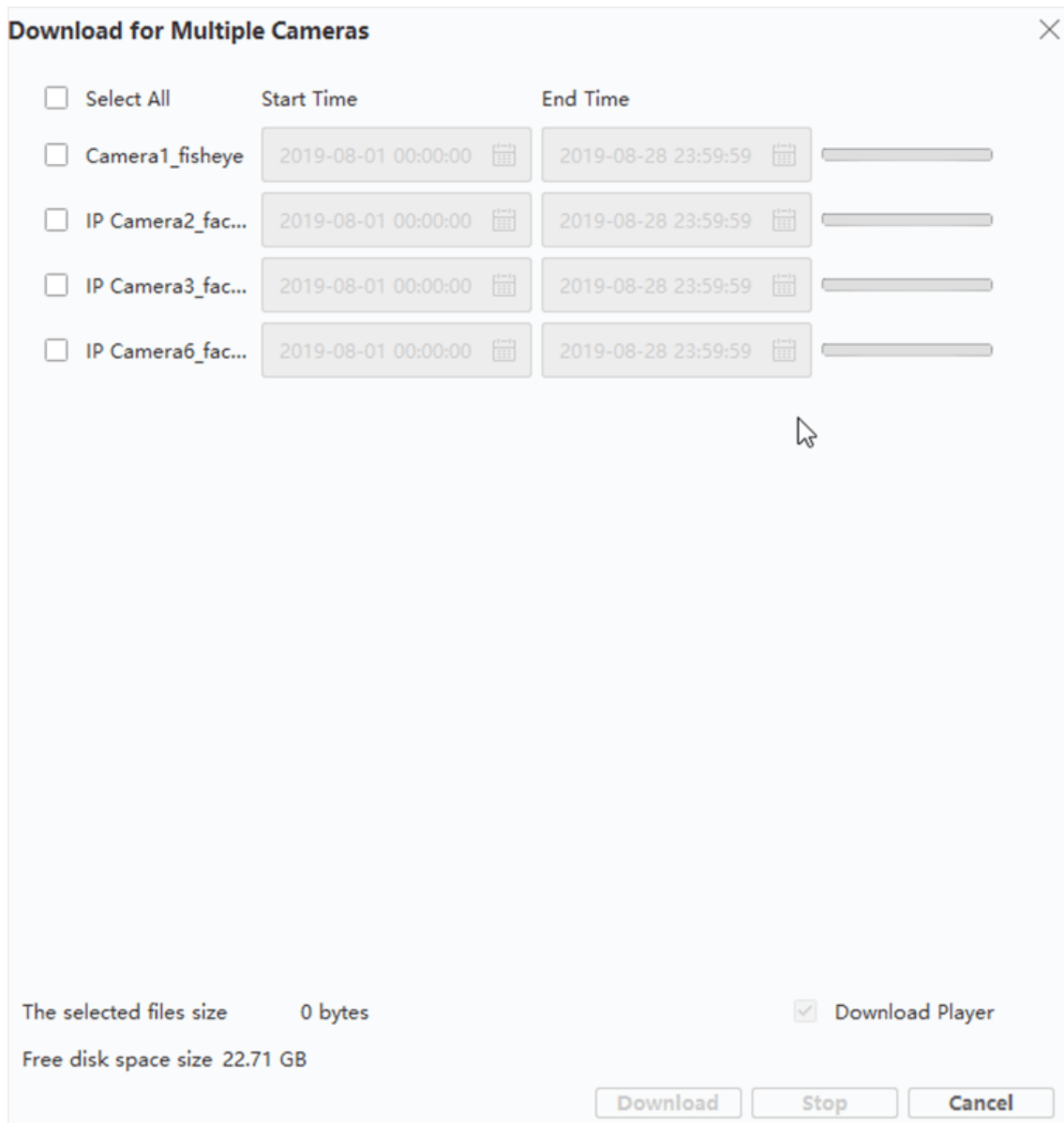
Raadpleeg **Afspelen op afstand** voor meer informatie over het starten van het afspelen.

2. Klik op  om het venster Download voor meerdere camera's te openen.



Afbeelding 6-13 Gereedschapsbalk

- Alle camera's die worden afgespeeld, worden weergegeven.
3. Selecteer de camera's waarvoor je videobestanden wilt downloaden.
 4. Stel de starttijd en eindtijd van de videoduur in voor elke camera.



Afbeelding 6-14 Camera's selecteren

5. Optioneel: Vink **Download Player** aan om de speler te downloaden.
6. Klik op **Download om te** beginnen met het downloaden van de videobestanden van de geconfigureerde duur (lengtes) naar de lokale pc.
De voortgangsbalk toont het downloadproces van de videobestanden van elke camera.
7. Optioneel: Klik op **Stop** om het downloaden handmatig te stoppen.

 **Opmerking**

Er kunnen videobestanden van maximaal 16 camera's tegelijk worden gedownload.

Hoofdstuk 7 Gebeurtenisconfiguratie

Gebeurtenissen worden gebruikt om beveiligingspersoneel op de hoogte te stellen van een bepaalde situatie, waardoor de situatie direct kan worden afgehandeld. Gebeurtenissen kunnen een reeks koppelingsacties triggeren (bijv. geluidssignaal en verzenden van e-mail) voor kennisgeving en afhandeling van gebeurtenissen. Je kunt de gebeurtenis inschakelen en koppelingsactie(s) instellen voor de bronnen die aan de client zijn toegevoegd. Als de geselecteerde gebeurtenissen plaatsvinden, ontvangt de client gebeurtenismeldingen in real-time en kun je de details controleren en de gebeurtenissen dienovereenkomstig afhandelen.

Video-evenement

De videogebeurtenissen verwijzen naar de speciale gebeurtenissen die worden geactiveerd door de video-uitzondering, de uitzondering van het bewakingsgebied, de alarmingang, de uitzondering van het codeerapparaat, enz. Raadpleeg [**Gebeurtenis configureren voor camera**](#), [**Gebeurtenis configureren voor alarmingang**](#) en [**Gebeurtenis configureren voor codeerapparaat**](#) voor meer informatie.

Gebeurtenis Toegangscontrole

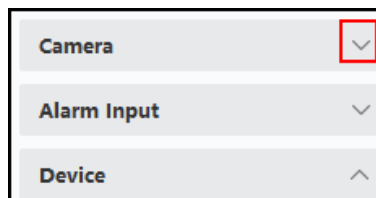
De toegangscontrolegebeurtenissen verwijzen naar de speciale gebeurtenissen die worden geactiveerd op de toegangscontroleapparaten, deuren, kaartlezers, liften, video-intercomapparaten, enz. Raadpleeg voor meer informatie [**Clientacties configureren voor toegangsgebeurtenis**](#) en [**Video-intercomgebeurtenis configureren**](#).

7.1 Gebeurtenis voor camera configureren

De gebeurtenis voor de camera verwijst naar de video-uitzondering of de gebeurtenissen die worden gedetecteerd in het bewakingsgebied van de camera, zoals bewegingsdetectie, videoverlies, lijnoverschrijding, enzovoort. Je kunt een gebeurtenis voor de camera's in de client inschakelen. Wanneer de gebeurtenis op de camera wordt geactiveerd, kan de client de gebeurtenis ontvangen en opnemen om te controleren en een reeks koppelingsacties activeren (bijv. e-mail verzenden) voor kennisgeving.

Stappen

1. Klik op **Gebeurtenisconfiguratie** → **Videogebeurtenis** → **Camera**.



Afbeelding 7-1 Camerabron weergeven

2. Ontvouw de groep en selecteer een camera als gebeurtenisbron.

 **Opmerking**

Zorg ervoor dat de bron online is.

Alle gebeurtenistypes die door de geselecteerde camera worden ondersteund, worden weergegeven.

<input type="checkbox"/>	Event Type	Priority	Trigger Client Action	Linked Camera	Enable
<input type="checkbox"/>	Audio Input Exception...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_10.6.113.250	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Face Detection Alarm	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_10.6.113.250	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Intrusion Detection Al...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_10.6.113.250	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Line Crossing Detectio...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_10.6.113.250	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Motion Detection Alar...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_10.6.113.250	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Region Entrance Dete...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_10.6.113.250	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Region Exiting Detecti...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_10.6.113.250	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Video Loss Alarm	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_10.6.113.250	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Video Tampering Det...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_10.6.113.250	<input checked="" type="checkbox"/>

Figuur 7-2 Gebeurtenissen voor camera configureren


- Optioneel: Voer trefwoorden in het veld **Filter in** om de gewenste gebeurtenis snel te vinden.
- Optioneel: Zet de schakelaar in de kolom Inschakelen aan om het gebeurtenistype in te schakelen, of klik op **Alles inschakelen om** alle gebeurtenistypen van deze camera in te schakelen.

 **Opmerking**

Na het inschakelen kan de gebeurtenis worden ontvangen door de client en de koppelingsactie(s) activeren. Je kunt ook een gebeurtenistype of alle gebeurtenistypen uitschakelen.

- Optioneel: Selecteer de gebeurtenis(sen) en voer vervolgens de volgende bewerkingen uit.
 - Prioriteit bewerken** Klik op **Prioriteit bewerken** om de prioriteit van de gebeurtenis(sen) in te stellen.
Prioriteit staat voor de mate van nood van de gebeurtenis.
 - Gebeurteniskoppeling bewerken** Klik op **Gebeurteniskoppeling bewerken** om de koppelingsactie(s) van de gebeurtenis(sen) in te stellen.

Hoorbare waarschuwing

Activeer de hoorbare waarschuwing van de klant wanneer de gebeurtenis wordt geactiveerd. Je kunt het audiobestand in de vervolgkeuzelijst selecteren of op **Toevoegen klikken** om een nieuw audiobestand (in WAV-indeling) toe te voegen.
Je kunt op  klikken om een auditie te maken van het geselecteerde audiobestand.

Verstuur e-mail


Stuur een e-mailmelding van de alarminformatie naar een of meer ontvangers.

Raadpleeg [E-mailparameters instellen](#) voor meer informatie over het instellen van e-mailparameters.

Pop-upvenster

Pop-upvenster om de gebeurtenisgerelateerde informatie (inclusief gebeurtenisdetails, live video van de broncamera, vastgelegde beelden van de gekoppelde camera) weer te geven op de client wanneer de gebeurtenis wordt geactiveerd. Je kunt ook opmerkingen invoeren over hoe de gebeurtenis moet worden afgehandeld.

Weergeven op kaart

Wanneer de gebeurtenisbron wordt toegevoegd als hotspot op de kaart, wordt de hotspot weergegeven met  die opzij knippert wanneer de gebeurtenis wordt geactiveerd, waardoor beveiligingspersoneel de locatie van de gebeurtenis kan zien.

Je kunt ook op de hotspot klikken om de details van de gebeurtenis en de live video van de gekoppelde camera te bekijken.

Gekoppelde camera

Koppel de geselecteerde camera om foto's te maken of video's op te nemen wanneer de gebeurtenis wordt geactiveerd.

Wat nu te doen

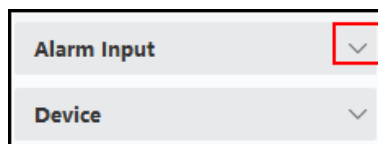
Je moet het apparaat waartoe de camera behoort inschakelen, anders kan de client de geconfigureerde gebeurtenissen niet ontvangen. Zie [Gebeurtenissen van apparaten ontvangen inschakelen](#) voor meer informatie.

7.2 Gebeurtenis voor alarmingang configureren

De gebeurtenis voor alarmingang verwijst naar de gebeurtenis die wordt geactiveerd door alarmingang. Je kunt een gebeurtenis inschakelen voor de alarmingangen in de client. Wanneer de alarmingang wordt geactiveerd, kan de client de gebeurtenis ontvangen en vastleggen ter controle en een reeks koppelingsacties activeren (bijv. e-mail verzenden) voor kennisgeving.

Stappen

1. Klik op **Gebeurtenisconfiguratie** → **Videogebeurtenis** → **Alarmingang**.



Afbeelding 7-3 Alarmingangsbron weergeven

2. Ontvouw de groep en selecteer een alarmingang als gebeurtenisbron.

Opmerking

Zorg ervoor dat de bron online is.

Alle gebeurtenistypes die door de geselecteerde alarmingang worden ondersteund, worden weergegeven.

3. Optioneel: Voer trefwoorden in het veld **Filter in** om de gewenste gebeurtenis snel te vinden.
 4. Optioneel: Zet de schakelaar in de kolom **Inschakelen** aan om het gebeurtenistype in te schakelen, of klik op **Alles inschakelen om** alle gebeurtenistypen van deze alarmingang in te schakelen.
-

Opmerking

Na het inschakelen kan de gebeurtenis worden ontvangen door de client en de koppelingsactie(s) activeren. Je kunt ook een gebeurtenistype of alle gebeurtenistypes uitschakelen.

5. Optioneel: Selecteer de gebeurtenis(sen) en voer vervolgens de volgende bewerkingen uit.

Prioriteit bewerken Klik op **Prioriteit bewerken** om de prioriteit van de gebeurtenis(sen) in te stellen.
Prioriteit staat voor de mate van nood van de gebeurtenis.

Gebeurteniskoppeling bewerken Klik op **Gebeurteniskoppeling bewerken** om de koppelingsactie(s) van de gebeurtenis(sen) in te stellen.

Hoorbare waarschuwing

Activeer de hoorbare waarschuwing van de klant wanneer de gebeurtenis wordt geactiveerd. Je kunt het audiobestand in de vervolgkeuzelijst selecteren of op **Toevoegen klikken** om een nieuw audiobestand (in WAV-indeling) toe te voegen.

Je kunt op  klikken om een auditie te maken van het geselecteerde audiobestand.

Verstuur e-mail


Stuur een e-mailmelding van de alarminformatie naar een of meer ontvangers.

Raadpleeg [**E-mailparameters instellen**](#) voor meer informatie over het instellen van e-mailparameters.

Pop-upvenster

Pop-upvenster om de gebeurtenisgerelateerde informatie (inclusief gebeurtenisdetails, live video van de broncamera, vastgelegde beelden van de gekoppelde camera) weer te geven op de client wanneer de gebeurtenis wordt geactiveerd. Je kunt ook opmerkingen invoeren over hoe de gebeurtenis moet worden afgehandeld.

Weergeven op kaart

Wanneer de gebeurtenisbron wordt toegevoegd als hotspot op de kaart, wordt de hotspot weergegeven met  die opzij knippert wanneer de gebeurtenis wordt geactiveerd, waardoor beveiligingspersoneel de locatie van de gebeurtenis kan zien.

Je kunt ook op de hotspot klikken om de details van de gebeurtenis en de live video van de gekoppelde camera te bekijken.

Gekoppelde camera

Koppel de geselecteerde camera om foto's te maken of video's op te nemen wanneer de gebeurtenis wordt geactiveerd.

Wat nu te doen

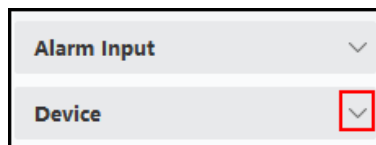
Je moet het apparaat waartoe de alarmingang behoort bewapenen, anders kan de client de geconfigureerde gebeurtenissen niet ontvangen. Zie [**Gebeurtenissen van apparaten ontvangen inschakelen**](#) voor meer informatie.

7.3 Gebeurtenis voor codeerapparaat configureren

De gebeurtenis voor het codeerapparaat verwijst naar de uitzondering van het codeerapparaat, zoals apparaat offline. Je kunt een event inschakelen voor de codeerapparaten die in de client zijn toegevoegd. Wanneer de gebeurtenis op het apparaat wordt geactiveerd, kan de client de gebeurtenis ontvangen en opnemen om te controleren en een reeks koppelingsacties activeren (bijv. e-mail verzenden) voor kennisgeving.

Stappen

1. Klik op **Gebeurtenisconfiguratie** → **Videogebeurtenis** → **Apparaat**.



Afbeelding 7-4 Apparaatbron weergeven

2. Selecteer een apparaat als gebeurtenisbron.

Opmerking

Zorg ervoor dat de bron online is.

Alle gebeurtenistypes die door het geselecteerde apparaat worden ondersteund, worden weergegeven.

3. Optioneel: Voer trefwoorden in het veld **Filter in** om de gewenste gebeurtenis snel te vinden.
4. Optioneel: Zet de schakelaar in de kolom **Inschakelen** aan om het gebeurtenistype in te schakelen, of klik op **Alles inschakelen** om alle gebeurtenistypen van dit apparaat in te schakelen.

Opmerking

Nadat de gebeurtenis is ingeschakeld, kan deze worden ontvangen door de client en de koppelingsactie(s) activeren. Je kunt ook een gebeurtenistype of alle gebeurtenistypes uitschakelen.

5. Optioneel: Selecteer de gebeurtenis(sen) en voer vervolgens de volgende bewerkingen uit.

Prioriteit bewerken Klik op **Prioriteit bewerken** om de prioriteit van de gebeurtenis(sen) in te stellen.

Prioriteit staat voor de mate van nood van de gebeurtenis.

Gebeurteniskoppeling bewerken Klik op **Gebeurteniskoppeling bewerken** om de koppelingsactie(s) van de gebeurtenis(sen) in te stellen.

Hoorbare waarschuwing

Activeer de hoorbare waarschuwing van de klant wanneer de gebeurtenis wordt geactiveerd. Je kunt het audiobestand in de vervolgkeuzelijst selecteren of op **Toevoegen klikken** om een nieuw audiobestand (in WAV-indeling) toe te voegen.

Je kunt op  klikken om een auditie te maken van het geselecteerde audiobestand.

Verstuur e-mail

Stuur een e-mailmelding van de alarminformatie naar een of meer ontvangers.

Raadpleeg **E-mailparameters instellen** voor meer informatie over het instellen van e-mailparameters.

Klik op **Kopiëren om** de gebeurtenisinstellingen van dit apparaat te kopiëren naar andere apparaten.

Opmerking

Je kunt de gebeurtenisinstellingen alleen kopiëren naar de bron(nen) van hetzelfde type.

Wat nu te doen

Je moet dit apparaat bewapenen, anders kan de client de geconfigureerde gebeurtenissen niet ontvangen. Zie **Gebeurtenissen van apparaten ontvangen inschakelen** voor meer informatie.

Hoofdstuk 8 Evenemententerrein


De gebeurtenisinformatie (bijvoorbeeld apparaat offline) die door de client is ontvangen, wordt weergegeven. In het Event Center kun je de gedetailleerde informatie van de real-time en historische events controleren, de video van de event bekijken, de events afhandelen, enzovoort. Voordat de client de gebeurtenisinformatie van het apparaat kan ontvangen, moet je eerst de gebeurtenissen van de bron inschakelen en het apparaat bewapenen. Raadpleeg **Gebeurtenisconfiguratie** en **Gebeurtenis ontvangen van apparaten inschakelen** voor meer informatie.

Voordat je de pop-upalarminformatie kunt bekijken, moet je het pop-upbeeld van de gebeurtenis activeren in het gebeurteniscentrum. Raadpleeg **Pop-up gebeurtenisinformatie weergeven** voor meer informatie.

8.1 Gebeurtenissen van apparaten ontvangen inschakelen

Voordat de clientsoftware gebeurtenismeldingen van het apparaat kan ontvangen, moet je het apparaat eerst activeren.

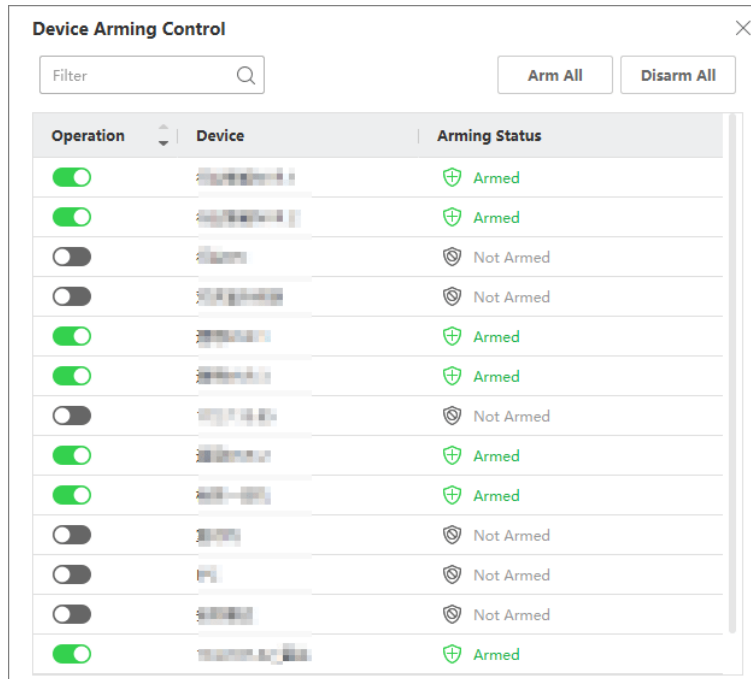
Stappen

1. Klik op  → **Tool** → **Device Arming Control** om de pagina Device Arming Control te openen. Alle toegevoegde apparaten verschijnen op deze pagina.
2. Optioneel: Als er te veel apparaten zijn, voer dan de sleutelwoorden in bij Filter filed om de gewenste apparaten te filteren.

Opmerking

Voor de gefilterde apparaten kunt u klikken op **Alles inschakelen** of **Alles uitschakelen** om de ontvangst van gebeurtenissen voor deze apparaten in te schakelen.

3. Schakel in de kolom Automatisch bewapenen de schakelaar in om automatisch bewapenen in te schakelen.



Afbeelding 8-1 Arm Apparaat

Nadat de apparaten zijn ingeschakeld, worden ze ingeschakeld. En meldingen over de gebeurtenissen die door het (de) ingeschakelde apparaat(en) worden geactiveerd, worden automatisch en in real-time naar de clientsoftware verzonden.

8.2 Realtime gebeurtenissen weergeven

De realtime gebeurtenisinformatie die de client van de aangesloten bronnen ontvangt, wordt weergegeven. U kunt de real-time gebeurtenisinformatie controleren, inclusief de bron van de gebeurtenis, tijd van de gebeurtenis, prioriteit, enz.

Voordat u begint

Schakel het ontvangen van gebeurtenissen van apparaten in voordat de client gebeurtenissen van het apparaat kan ontvangen, zie **Gebeurtenissen van apparaten ontvangen inschakelen** voor meer informatie.

Stappen

1. Klik op **Gebeurteniscentrum** → **Real-timegebeurtenis** om de pagina met real-timegebeurtenissen te openen en je kunt de door de client ontvangen real-timegebeurtenissen bekijken.

Evenement Tijd

Voor codeerapparaten is gebeurtenistijd de tijd van de client wanneer deze het event ontvangt. Voor andere apparaattypes is de gebeurtenistijd de tijd waarop de gebeurtenis wordt geactiveerd.

Prioriteit

Prioriteit staat voor de mate van nood van de gebeurtenis.

2. Filter de gebeurtenissen.

Filter op apparaatype en (of) prioriteit Selecteer apparaatype(s) en (of) prioriteiten om gebeurtenissen te filteren.

Filter op trefwoorden Voer de trefwoorden in om de gebeurtenissen te filteren.

3. Optioneel: Klik met de rechtermuisknop op de tabelkop van de gebeurtenissenlijst om de gebeurtenisgerelateerde items aan te passen die moeten worden weergegeven in de gebeurtenissenlijst.
4. Selecteer een gebeurtenis in de gebeurtenissenlijst om de details van de gebeurtenis te bekijken.

 **Opmerking**

Wanneer **Foto's opslaan in structuurdataformaat** is ingeschakeld, worden er geen foto's weergegeven in Gebeurtenisdetails in Gebeurteniscentrum. Raadpleeg **Algemene parameters instellen** voor meer informatie over **Foto's opslaan in structuurdataformaat**.

 **Opmerking**

- De details van de gebeurtenis omvatten de vastgelegde foto('s), video (opgenomen video die door de gebeurtenis werd geactiveerd of liveweergave van het apparaat) en andere beschrijvingen van de gebeurtenis.
 - Om de opgenomen video te bekijken die door de gebeurtenis is geactiveerd, moet je camera('s) koppelen aan het apparaat in de gebeurtenisconfiguratie. Raadpleeg **Gebeurtenisconfiguratie** voor meer informatie.
 - Om de vastgelegde foto('s) te bekijken, moet u de opslag van foto's configureren in Opslagschema.
-

5. Optioneel: Voer indien nodig de volgende bewerkingen uit.

Afhandeling afzonderlijke gebeurtenis Klik op **Hanteren** om de verwerkingssuggestie in te voeren en klik vervolgens op **OK**.

 **Opmerking**

Nadat een gebeurtenis is **afgehandeld**, wordt de knop **Opmerking toevoegen**. Klik op **Opmerking toevoegen** om meer opmerkingen voor deze afgehandelde gebeurtenis toe te voegen.

Gebeurtenissen in Selecteer gebeurtenissen die verwerkt moeten worden en klik dan op

een batch verwerken	Verwerken in batch. Voer de verwerkingssuggestie in en klik op OK .
Audio alarm in-/uitschakelen	Klik op Audio aan/uit om de audio van de gebeurtenis in/uit te schakelen.
Selecteer automatisch de laatste gebeurtenis	Vink Automatisch laatste gebeurtenis selecteren aan om automatisch de laatste gebeurtenis te selecteren en de details van de gebeurtenisinformatie worden weergegeven.
Duidelijke gebeurtenissen	Klik op Wissen om alle gebeurtenissen in de gebeurtenissenlijst te wissen.
Verstuur e-mail	Selecteer een evenement en klik op Verzend e-mail , waarna de informatie over dit evenement per e-mail wordt verzonden.

 **Opmerking**

U moet eerst de e-mailparameters configureren, zie [E-mailparameters instellen](#) voor meer informatie.

Video automatisch afspelen	Vink Automatisch video afspelen aan om automatisch video af te spelen bij het weergeven van evenementgegevens.
Video of afbeelding vergroten	<ul style="list-style-type: none">• Dubbelklik op de videoafbeelding om de video in een groter venster te bekijken.• Plaats de cursor op de afbeelding en klik op  om de afbeelding in een groter venster te bekijken.
Captured Picture downloaden	Beweeg de cursor over de vastgelegde foto en klik op het downloadpictogram in de rechterbenedenhoek van de foto om deze te downloaden naar de lokale pc.
Gebeurtenis gestuurde video downloaden	Beweeg de cursor over de opgenomen video, klik op  om de video te downloaden (30s voordat de gebeurtenis plaatsvindt) die door de gebeurtenis is geactiveerd.

8.3 Historische gebeurtenissen zoeken

Je kunt historische gebeurtenissen zoeken en weergeven door zoekvoorwaarden in te stellen zoals tijd, apparaattype en prioriteit in de client. De gezochte gebeurtenissen kun je verwerken en

exporteren.

Voordat u begint

Schakel het ontvangen van gebeurtenissen van apparaten in voordat de client gebeurtenisinformatie van het apparaat kan ontvangen, zie [Gebeurtenissen van apparaten ontvangen inschakelen](#) voor meer informatie.

Stappen

1. Klik op **Evenementcentrum** → **Evenement zoeken** om de zoekpagina voor evenementen te openen.
2. Stel de filtervoorwaarden in om alleen de gewenste gebeurtenissen weer te geven.

Tijd

De tijd waarop het evenement begint.

Zoeken op

Apparaat

Zoek de gebeurtenissen op apparaat of op de bronkanalen van het apparaat. Als je zoekt op apparaat, moet je het volgende instellen:

- **Subnode opnemen:** Doorzoek de gebeurtenissen van het apparaat en alle resourcekanalen.
- **Type apparaat:** Selecteer het apparaat waarvan je gebeurtenissen wilt zoeken.

Groep

Zoek de gebeurtenissen op resourcekanalen in de groep.

Opmerking

- Voor video-intercomapparaat moet je zoekbereik selecteren: Alles en Logboek vergrendelen.
 - Voor toegangscontroleapparaten kunt u op **Toon meer** klikken om meer voorwaarden in te stellen: status, gebeurtenistype, kaartlezertype, persoonsnaam, kaartnummer en organisatie.
-

Prioriteit

De prioriteit bestaat uit laag, medium, hoog en ongecategoriseerd, wat de mate van nood van de gebeurtenis aangeeft.

Type evenement

Selecteer een of meer gebeurtenistypen in de vervolgkeuzelijst.

Opmerking

Je kunt een sleutelwoord invoeren (ondersteunt fuzzy search) in het zoekvak om het (de) doelevanttype(s) te zoeken.

Status

De afhandelingsstatus van de gebeurtenis.

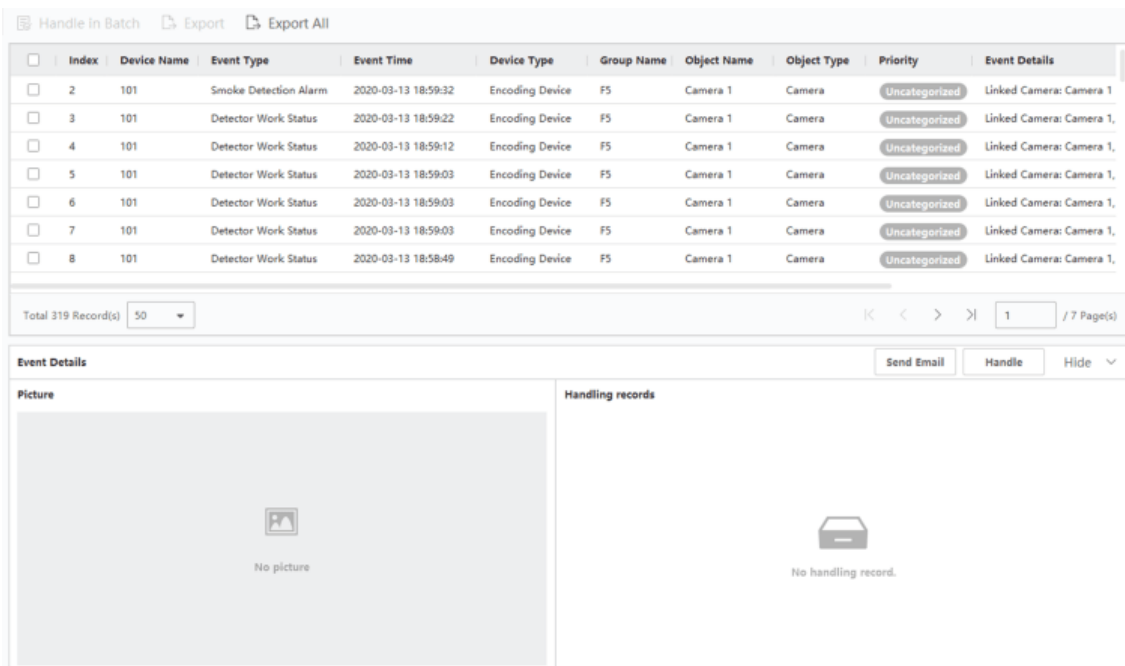
Zoeken op trefwoord

Voer een sleutelwoord in (ondersteunt fuzzy search) om snel de gewenste historische gebeurtenis(sen) te zoeken. Je kunt bijvoorbeeld de naam van een persoon invoeren om de gebeurtenissen met betrekking tot deze persoon te zoeken.

3. Klik op **Zoeken** om de gebeurtenissen te zoeken volgens de voorwaarden die u hebt ingesteld.

Opmerking

Als **Afbeelding opslaan in structuurdataformaat** is ingeschakeld, worden er geen afbeeldingen weergegeven in het veld Gebeurtenisdetails in Gebeurteniscentrum. Raadpleeg **Algemene parameters instellen** voor meer informatie over **Afbeeldingen opslaan in structuurgegevensformaat**.



The screenshot displays the 'Event Details' section of the ABUS CMS interface. At the top, there are buttons for 'Handle in Batch', 'Export', and 'Export All'. Below this is a table with the following columns: Index, Device Name, Event Type, Event Time, Device Type, Group Name, Object Name, Object Type, Priority, and Event Details. The table contains eight rows of data, all with 'Camera 1' as the object name and 'Unategorized' as the priority. Below the table, there is a pagination control showing 'Total 319 Record(s)' and '50' records per page, with a page number of '1' out of '7 Page(s)'. The 'Event Details' section is divided into two panels: 'Picture' and 'Handling records'. Both panels show a placeholder icon and the text 'No picture' and 'No handling record.' respectively. There are also buttons for 'Send Email', 'Handle', and a 'Hide' dropdown menu.

Index	Device Name	Event Type	Event Time	Device Type	Group Name	Object Name	Object Type	Priority	Event Details
2	101	Smoke Detection Alarm	2020-03-13 18:59:32	Encoding Device	F5	Camera 1	Camera	Unategorized	Linked Camera: Camera 1
3	101	Detector Work Status	2020-03-13 18:59:22	Encoding Device	F5	Camera 1	Camera	Unategorized	Linked Camera: Camera 1,
4	101	Detector Work Status	2020-03-13 18:59:12	Encoding Device	F5	Camera 1	Camera	Unategorized	Linked Camera: Camera 1,
5	101	Detector Work Status	2020-03-13 18:59:03	Encoding Device	F5	Camera 1	Camera	Unategorized	Linked Camera: Camera 1,
6	101	Detector Work Status	2020-03-13 18:59:03	Encoding Device	F5	Camera 1	Camera	Unategorized	Linked Camera: Camera 1,
7	101	Detector Work Status	2020-03-13 18:59:03	Encoding Device	F5	Camera 1	Camera	Unategorized	Linked Camera: Camera 1,
8	101	Detector Work Status	2020-03-13 18:58:49	Encoding Device	F5	Camera 1	Camera	Unategorized	Linked Camera: Camera 1,

Figuur 8-2 Historische gebeurtenissen zoeken

4. Optioneel: Klik met de rechtermuisknop op de tabelkop van de gebeurtenissenlijst om de gebeurtenisgerelateerde items aan te passen die in de gebeurtenissenlijst moeten worden weergegeven.
5. Selecteer een gebeurtenis in de gebeurtenissenlijst om de details van de gebeurtenis te bekijken.

Opmerking

- De details van de gebeurtenis omvatten de vastgelegde foto('s), video (opgenomen video die door de gebeurtenis werd geactiveerd of liveweergave van het apparaat) en andere beschrijvingen van de gebeurtenis.
 - Om de opgenomen video te bekijken die door de gebeurtenis is geactiveerd, moet je camera('s) koppelen aan het apparaat in de gebeurtenisconfiguratie. Raadpleeg **Gebeurtenisconfiguratie** voor meer informatie.
 - Om de vastgelegde foto('s) te bekijken, moet u de opslag van foto's configureren in Opslagschema.
-

6. Optioneel: Voer een van de volgende bewerkingen uit.

Afhandeling afzonderlijke gebeurtenis

Afhandeling afzonderlijke gebeurtenis: Selecteer één gebeurtenis die moet worden afgehandeld en klik vervolgens op **Afhandelen** op de pagina met informatie over de gebeurtenis en voer de afhandelingssuggestie in.

Opmerking

Nadat een gebeurtenis is afgehandeld, verandert de knop **Afhandelen** in **Opmerking toevoegen**. Klik op **Opmerking toevoegen** om meer opmerkingen voor deze afgehandelde gebeurtenis toe te voegen.

Batchgebeurtenissen afhandelen

Verwerk gebeurtenissen in een batch: Selecteer de gebeurtenissen die moeten worden afgehandeld en klik vervolgens op **Handle in Batch** en voer de afhandelingssuggestie in.


Opmerking

Nadat een gebeurtenis is afgehandeld, verandert de knop **Afhandelen** in **Opmerking toevoegen**. Klik op **Opmerking toevoegen** om meer opmerkingen voor deze afgehandelde gebeurtenis toe te voegen.

Video automatisch afspelen

Vink **Automatisch video afspelen** aan om automatisch video af te spelen bij het weergeven van evenementgegevens.

Video of afbeelding vergroten

- Dubbelklik op de videoafbeelding om de video in een groter venster te bekijken.
- Plaats de cursor op de afbeelding en klik op  om de afbeelding in een groter venster te bekijken.


Verstuur e-mail

Selecteer een evenement en klik op **Verzend e-mail**, waarna de

informatie over dit evenement per e-mail wordt verzonden.

 **Opmerking**

U moet eerst de e-mailparameters configureren, zie [E-mailparameters instellen](#) voor meer informatie.

Gebeurtenisinformatie exporteren	Klik op Exporteren om het gebeurtenissenlogboek of de gebeurtenissenfoto's te exporteren naar de lokale pc in een CSV/Excel-bestand. Je kunt het opslagpad handmatig instellen.
Captured Picture downloaden	Beweeg de cursor over de vastgelegde afbeelding en klik op het downloadpictogram in de rechterbenedenhoek van de afbeelding om deze te downloaden naar de lokale pc.
Gebeurtenis gestuurde video downloaden	Beweeg de cursor over de opgenomen video, klik op  om de video te downloaden (30s voordat de gebeurtenis plaatsvindt) die door de gebeurtenis is geactiveerd.

8.4 Gebeurtenissen van apparaat ophalen

Voor sommige scenario's (bijv. de client kan niet opstarten, het toegangscontroleapparaat is ingeschakeld door een andere client, enz.) zijn de gebeurtenissen die door de client worden ontvangen en op het toegangscontroleapparaat worden geactiveerd niet consistent. U kunt op afstand gebeurtenissen van het apparaat ophalen om de gebeurtenissen van het apparaat te synchroniseren met het Event Center van de client.

Klik op **Apparaatbeheer** → **Apparaat** → **Apparaat**, selecteer toegangscontroleapparaat (-apparaten) en klik op **Gebeurtenissen van apparaat ophalen**.

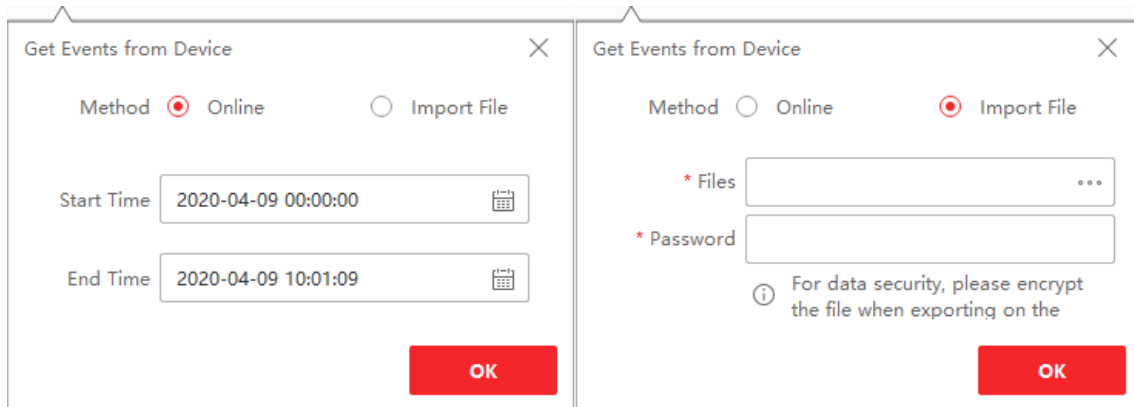
Synchroniseer de gebeurtenissen op twee manieren:

- **Online:** Wanneer het apparaat online is en met de client kan communiceren in realtime, kunt u **Online** selecteren en de begin- en eindtijd instellen om de gebeurtenissen tijdens deze periode op te halen.
- **Bestand importeren:** Als het netwerk niet goed is of als het apparaat niet realtime kan communiceren met de client, kun je het gebeurtenisbestand eerst exporteren vanaf het geselecteerde apparaat en dit geëxporteerde bestand later importeren op de client door **Bestand importeren** te selecteren en het wachtwoord van het gecodeerde bestand in te voeren.

 **Opmerking**

- Voor de veiligheid van de gegevens moet je het bestand coderen wanneer je het exporteert naar het apparaat. Ondertussen moet het geselecteerde toegangscontroleapparaat het apparaat zijn waarvan je het bestand hebt geëxporteerd.

- o De functie moet worden ondersteund door het apparaat.
-



Figuur 8-3 Gebeurtenissen van apparaat ophalen

Opmerking

Als je alleen de gebeurtenissen met betrekking tot aanwezigheid wilt ophalen, kun je ook naar **Tijdregistratie** → **Aanwezigheidsstatistieken** → **Aanwezigheidsbestanden** gaan, klik op **Gebeurtenissen van apparaat ophalen** en selecteer **Online** of **Bestand importeren** om de gebeurtenissen op te halen.

8.5 Pop-up gebeurtenisinformatie weergeven

Als je gebeurtenismelding hebt ingeschakeld en Gebeurtenis geactiveerd pop-upafbeelding als koppelingsactie hebt ingesteld, verschijnt er een venster wanneer de gebeurtenis plaatsvindt met informatie over de gebeurtenis, gerelateerde afbeeldingen en gerelateerde video's.

Ga naar **Gebeurteniscentrum** → **Real-Time Gebeurtenis** en klik vervolgens op **Pop-upbeeld Alarm Triggered Inschakelen** om de functie in te schakelen.

Je kunt de videobeelden van de gebeurtenis bekijken (van 30 seconden voor de gebeurtenis tot het einde van de gebeurtenis), de foto die is gemaakt toen de gebeurtenis plaatsvond en de details van de gebeurtenis, zoals de bron van de gebeurtenis, de gekoppelde camera, het type gebeurtenis, enz.

Opmerking

- Als het venster niet gesloten is, moet je op **Volgende** klikken om de nieuwe gebeurtenisinformatie te bekijken als er een nieuwe gebeurtenis is getriggerd.
 - Als je de gebeurtenisinformatie niet hebt gewist, kun je op **Vorige** klikken om de vorige gebeurtenisinformatie te bekijken.
 - Wanneer **Afbeeldingen opslaan in structuurgegevensformaat** is ingeschakeld, worden afbeeldingen niet weergegeven in de gebeurtenisinformatie. Zie **Algemene parameters instellen** voor meer informatie.
-

Je kunt **Gebeurtenis automatisch bijwerken** aanvinken om het venster automatisch te laten overschakelen naar de meest recente gebeurtenisinformatie wanneer een nieuwe gebeurtenis wordt geactiveerd.

Hoofdstuk 9 Kaartbeheer

De E-map functie geeft een visueel overzicht van de locaties en distributies van de geïnstalleerde camera's en alarminvoerapparaten. Je kunt de camera's live op de kaart zien en je krijgt een melding op de kaart wanneer er een alarm afgaat.

Een e-map is een statische afbeelding (het hoeven geen geografische kaarten te zijn, hoewel ze dat vaak wel zijn. Afhankelijk van de behoeften van uw organisatie kunnen foto's en andere soorten beeldbestanden ook worden gebruikt als e-maps) die u een visueel overzicht geeft van de locaties en distributies van de hot spots (middelen (bijv. camera's, alarmingangen) die op de kaart zijn geplaatst, worden hot spots genoemd). Je kunt de fysieke locaties van de camera's en alarmingangen zien en in welke richting de camera's wijzen. Met de functie van hot spots kunnen e-maps worden georganiseerd in hiërarchieën om te navigeren van grote perspectieven naar gedetailleerde perspectieven, bijvoorbeeld van vloerniveau naar ruimteniveau.

9.1 Kaart toevoegen

Je moet een kaart toevoegen als bovenliggende kaart voor de hotspots en hotregio's.

Stappen

Opmerking

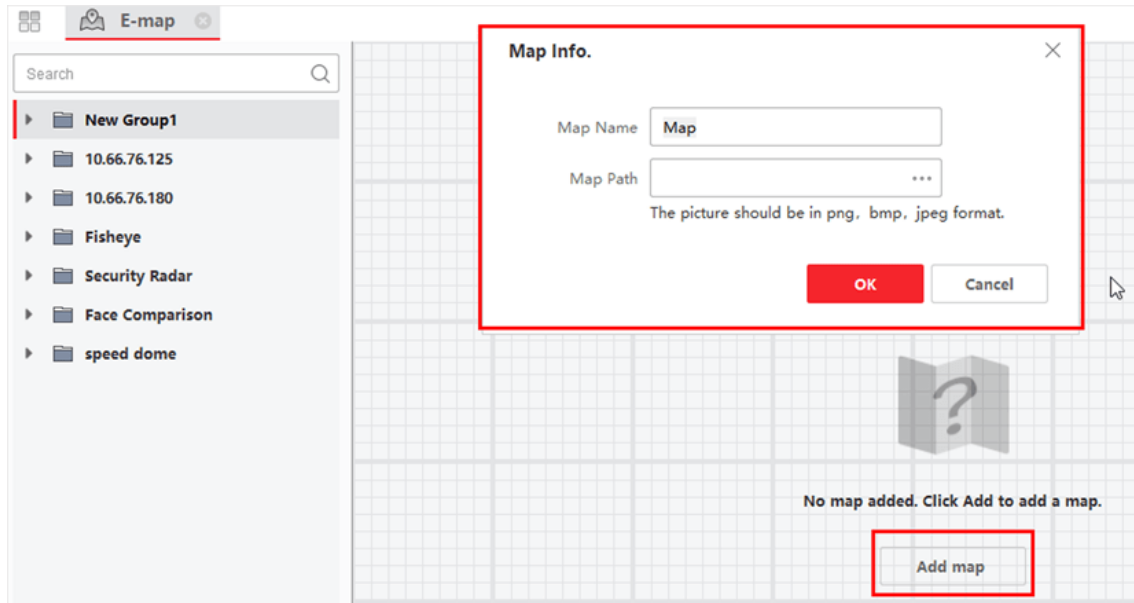
Er kan maar één kaart worden toegevoegd aan één groep.

1. Open de E-map pagina.
 2. Selecteer een groep waarvoor je een kaart wilt toevoegen.
-

Opmerking

Raadpleeg [Groepsbeheer](#) voor meer informatie over het instellen van de groep.

3. Klik op **Kaart toevoegen** om het venster voor het toevoegen van kaarten te openen.



Figuur 9-1 Kaart toevoegen

4. Voer een beschrijvende naam in voor de toegevoegde kaart.
5. Selecteer een kaartbeeld van het lokale pad.

Opmerking

Het afbeeldingsformaat van de kaart kan alleen PNG, JPEG of BMP zijn.

6. Klik op **OK**.
7. Optioneel: Voer de volgende taken uit na het toevoegen van de kaart.

In-/uitzoomen	Gebruik het muiswiel of klik op + of - om in of uit te zoomen op de kaart.
Kaart aanpassen	Sleep het gele venster in de rechterbenedenhoek of gebruik de richtingstoetsen en de zoombalk om het kaartgebied aan te passen voor weergave.

9.2 Kaartschaal bewerken


De schaal van een kaart is de verhouding tussen een afstand op de kaart en de overeenkomstige afstand op de grond. De client kan de afstand van twee locaties op de kaart berekenen aan de hand van de afstand op de grond. Een nauwkeurige kaartschaal is essentieel voor het bepalen van het bereik van de radar.

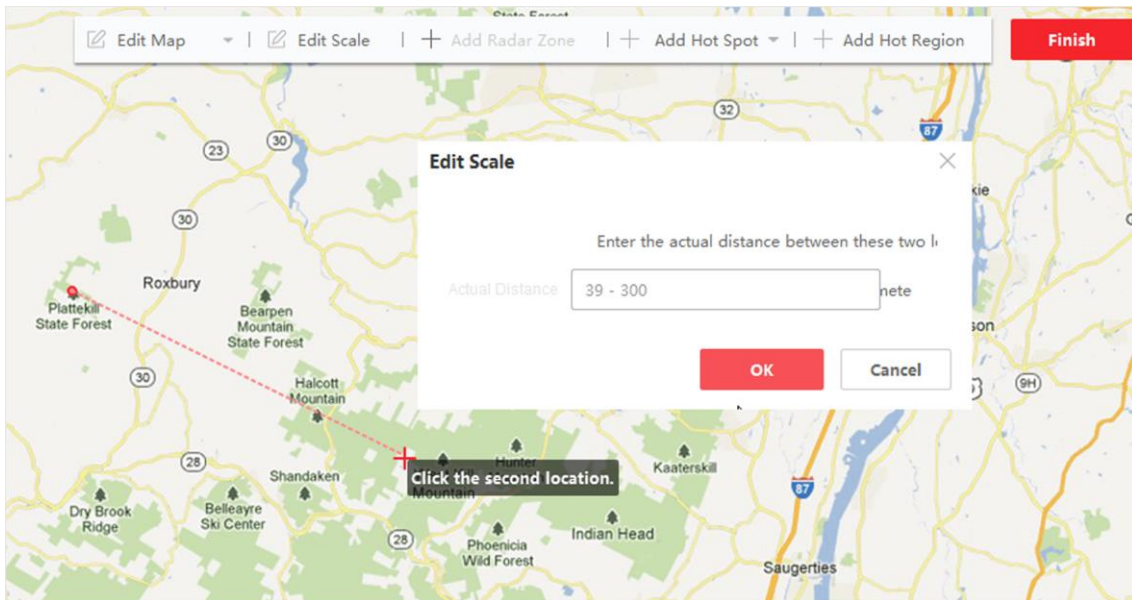
Voordat u begint

Zorg ervoor dat je een kaart hebt toegevoegd. Zie [Kaart toevoegen](#) voor meer informatie.

Voer deze taak uit als je een beveiligingsradar aan de kaart moet toevoegen.

Stappen

1. Ga naar de E-mapmodule.
2. Klik op **Bewerken** op de E-map werkbalk om de kaartbewerkingsmodus te openen.
3. Klik op **Kaartkalibratie** → **Schaal bewerken** om twee locaties op de kaart te selecteren.
De cursor verandert in  als je hem op de kaart houdt.



Figuur 9-2 Kaartschaal bewerken

4. Klik op de kaart om twee locaties te selecteren.
Het venster Edit Scale verschijnt.
5. Voer de grondafstand tussen de twee locaties in en klik op **OK**.
De client berekent de schaal van de kaart automatisch.

9.3 Kalibratie van lengtegraad en breedtegraad

Nadat u de lengtegraad en breedtegraad van twee punten op de E-kaart hebt gekalibreerd, kunt u de radar in de groep naar de E-kaart slepen. De radar zal automatisch naar de juiste positie op de E-kaart bewegen volgens het resultaat van de lengte- en breedtegraadkalibratie.

Voordat u begint

1. Zorg ervoor dat u radar hebt toegevoegd op de Client. Raadpleeg [**Enkele of meerdere online apparaten toevoegen**](#) voor meer informatie.
2. Zorg ervoor dat u de lengte- en breedteparameters van de radar met de webbrowser hebt ingesteld.

Stappen

1. Ga naar de E-mapmodule.
2. Klik op **Bewerken** op de E-map werkbalk om de kaartbewerkingsmodus te openen.

3. Klik op **Kaartkalibratie** → **Lengtegraad-Latitudekalibratie**.
4. Klik op **Kalibratiepunt toevoegen**.
5. Klik op een punt op de kaart, voer de lengtegraad en breedtegraad van het punt in het pop-upvenster in en klik op **Opslaan**.
6. Klik op **Kalibratiepunt toevoegen** en herhaal de vorige stap om het tweede kalibratiepunt toe te voegen.
7. Sleep de radar in de linkermiddelengroep naar de kaart.
De radar beweegt automatisch naar de juiste positie op de kaart op basis van de lengte- en breedtegraad van twee kalibratiepunten.

9.4 Hot Spot beheren

De apparaten die aan de kaart worden toegevoegd, worden hotspots genoemd. De hotspots tonen de locaties van de apparaten en je kunt via de hotspots ook de live weergave of alarminformatie van de bewakingsscenario's krijgen.

9.4.1 Camera toevoegen als hotspot

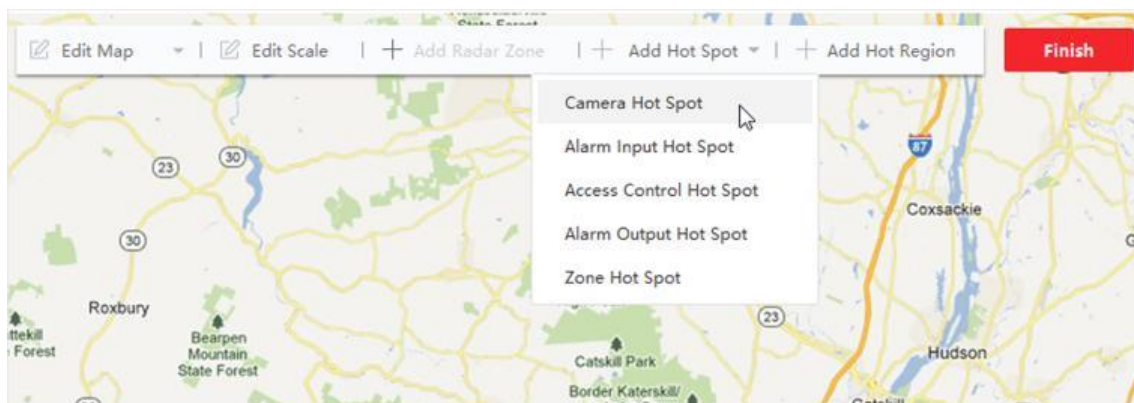
Je kunt camera's aan de kaart toevoegen als hotspot.

Voordat u begint

Zorg ervoor dat je een e-map en een camera hebt toegevoegd aan de client. Zie [Kaart toevoegen](#) en [Apparaatbeheer](#) voor meer informatie.

Stappen

1. Ga naar de E-map pagina.
2. Klik op **Bewerken** in de rechterbovenhoek om de kaartbewerkingsmodus te openen.
3. Klik op **Hot Spot toevoegen** → **Camera Hot Spot** om het venster Hot Spot toevoegen te openen.



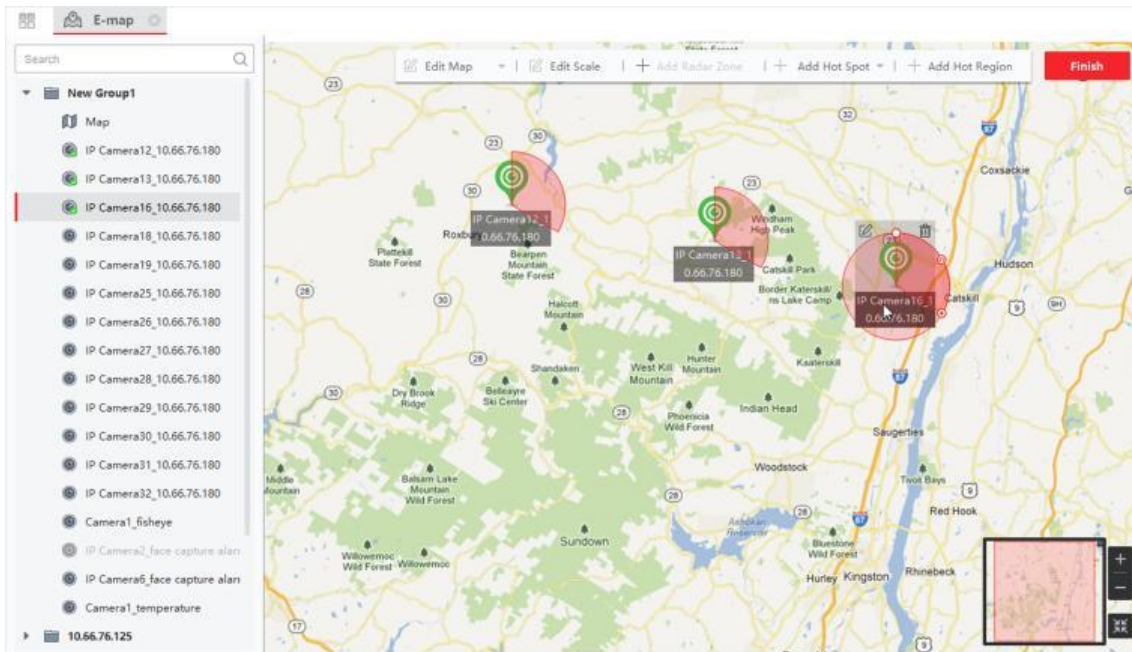
Afbeelding 9-3 Hot Spot toevoegen

4. Selecteer de camera's die aan de kaart moeten worden toegevoegd.
5. Optioneel: Bewerk de naam van de hotspot, selecteer de kleur van de naam en selecteer het hotspotpictogram.



6. Klik op **OK** om de instellingen op te slaan.

Opmerking

Je kunt de camerapictogrammen ook rechtstreeks van de groepslijst naar de kaart slepen om de hotspots toe te voegen.



Afbeelding 9-4 Camera hotspot toegevoegd


De camerapictogrammen worden op de kaart toegevoegd als hotspots en de pictogrammen van de toegevoegde camera's in de groepslijst veranderen van  naar . De sector geeft het gezichtsveld van de camera aan.

7. Voer de volgende handeling(en) uit.

De hotspot verplaatsen

Sleep de hotspot om hem naar een bepaalde positie te verplaatsen.

De FOV-hoek wijzigen

Versleep  en draai om het gezichtsveld van de camera te veranderen.

De FOV-grootte wijzigen

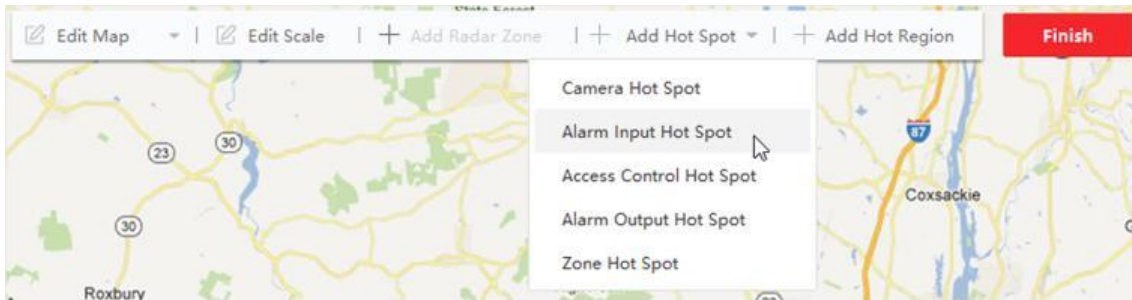
Versleep  om de FOV-grootte te wijzigen.

9.4.2 Alarmingang toevoegen als hotspot

Je kunt de alarmingangen toevoegen aan de kaart als hotspots.

Stappen

1. Ga naar de E-mapmodule.
2. Klik op **Bewerken** in de rechterbovenhoek om de kaartbewerkingsmodus te openen.
3. Klik op **Hot Spot toevoegen** → **Hot Spot voor alarmingang** om het venster Hot Spot toevoegen te openen.

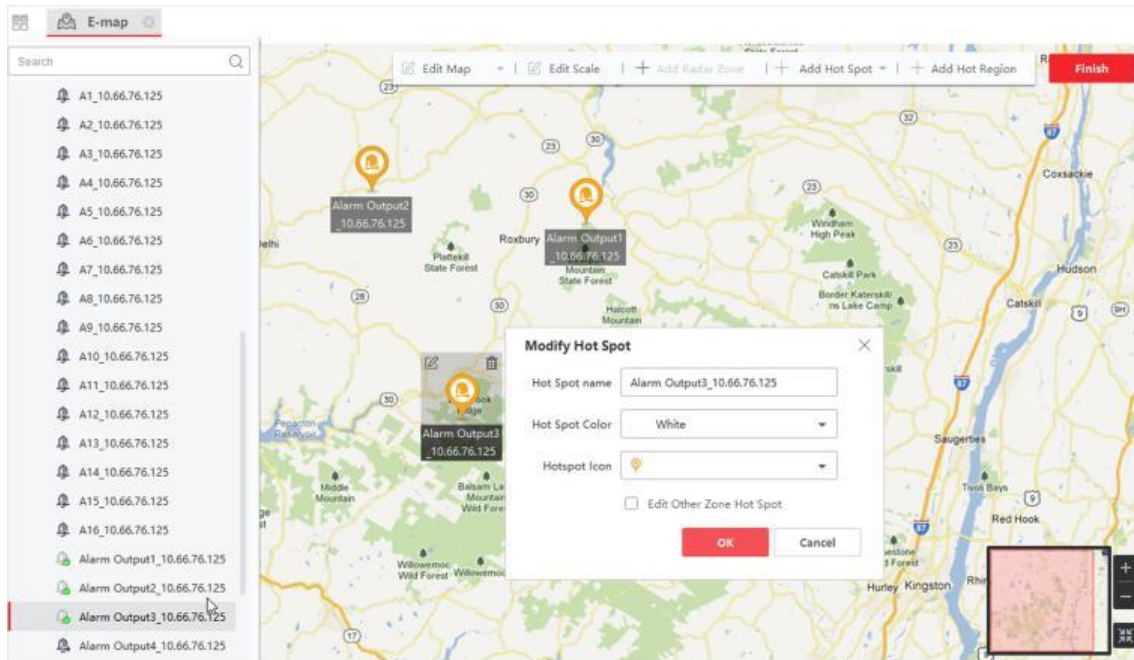


Afbeelding 9-5 Alarmingang toevoegen als hotspot



4. Selecteer de alarmingangen die moeten worden toegevoegd aan de kaart.
5. Optioneel: Bewerk de hotspotnaam, selecteer de naamkleur en selecteer het hotspotpictogram door te dubbelklikken op het overeenkomstige veld.
6. Klik op **OK**.

Opmerking

Je kunt de pictogrammen van de alarmingang ook rechtstreeks van de groepslijst naar de kaart slepen om de hotspot toe te voegen.



Afbeelding 9-6 Alarmingang Hot Spot toegevoegd

De pictogrammen van de alarmingangen worden toegevoegd aan de kaart als hotspots en de pictogrammen van de toegevoegde alarmingangen in de groepslijst veranderen van  naar  .

7. Optioneel: Sleep de hotspot om hem naar een bepaalde positie te verplaatsen.

9.4.3 Alarmuitgang toevoegen als Hot Spot

Je kunt alarmuitgangen toevoegen aan de kaart als hotspot voor beheer. Daarna kun je ze op een snelle manier in- of uitschakelen. Als je een alarmuitgang op de kaart inschakelt, zullen de beveiligingscontroleapparaten (bijv. sirenes, bellen) die erop zijn aangesloten om aandacht vragen.

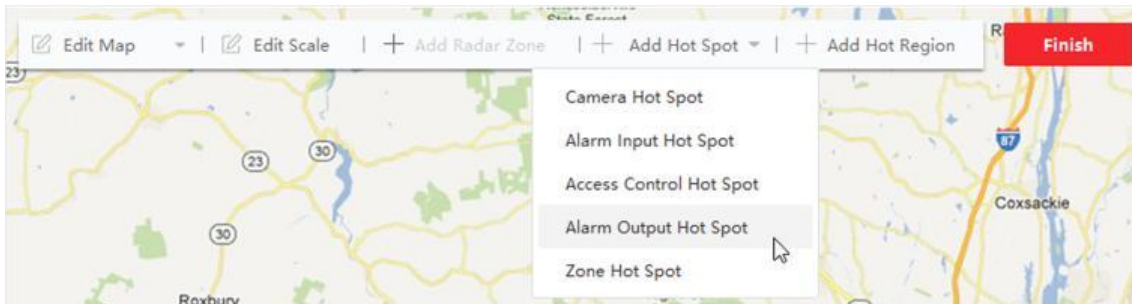
Voordat u begint

Zorg ervoor dat je een e-map en alarmuitgang hebt toegevoegd aan de client. Zie [Kaart toevoegen](#) en [Apparaatbeheer](#) voor meer informatie.

Stappen

1. Ga naar de E-mapmodule.
2. Klik op **Bewerken** op de E-map werkbalk om de kaartbewerkingsmodus te openen.

3. Klik op **Hot Spot toevoegen** → **Hot Spot alarmuitgang** om het paneel Hot Spot toevoegen te openen.

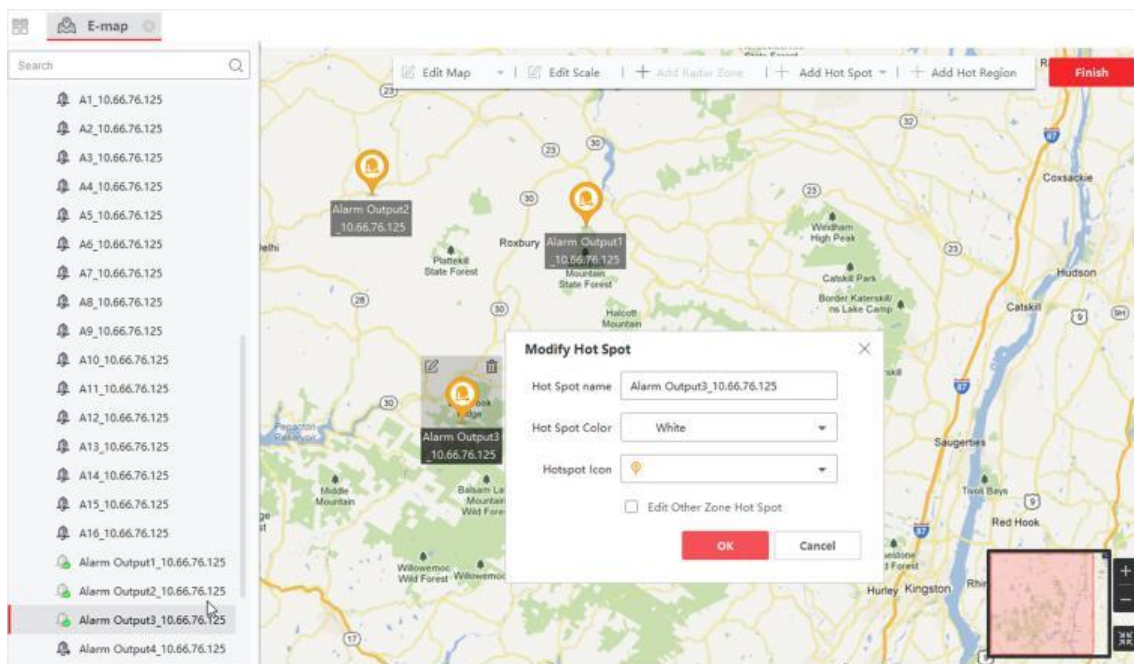


Afbeelding 9-7 Alarmuitgang toevoegen als hotspot



4. Selecteer de alarmuitgang die moet worden toegevoegd aan de kaart.
5. Optioneel: Bewerk de naam van de hotspot, selecteer de kleur van de naam en selecteer het hotspotpictogram.
6. Klik op **OK**.

Opmerking

Je kunt ook een pictogram van een alarmuitgang uit de lijst met alarmuitgangen naar de kaart slepen om de hotspot toe te voegen.



Afbeelding 9-8 Hotspot voor toegevoegde alarmuitgang

De alarmuitgang wordt als hotspot aan de kaart toegevoegd en het pictogram ervan in de groepslijst verandert van  in  .

7. Optioneel: Sleep de alarmuitgang om deze naar een bepaalde positie te verplaatsen.

9.4.4 Zone toevoegen als hotspot

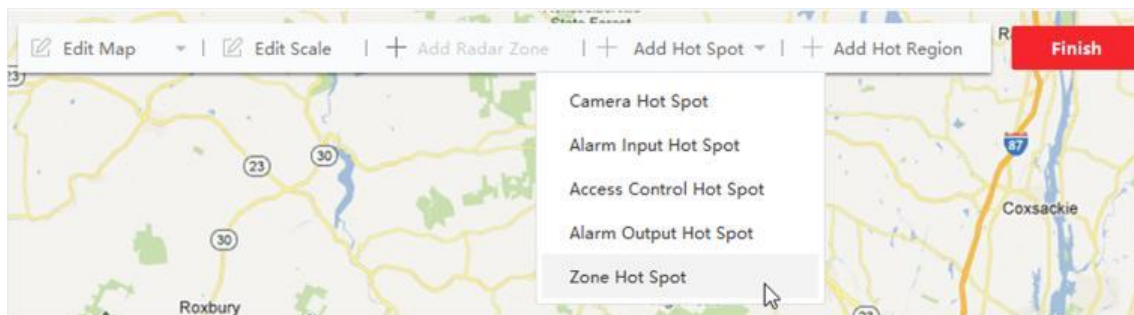
Je kunt zones toevoegen aan de kaart zodat je de zone snel kunt lokaliseren wanneer er een alarm afgaat.

Voordat u begint

Zorg ervoor dat je een kaart en zone hebt toegevoegd aan de client. Zie [Kaart toevoegen](#) en [Apparaat toevoegen](#) voor meer informatie.

Stappen

1. Ga naar de E-mapmodule.
2. Klik op **Bewerken** op de E-map werkbalk om de kaartbewerkingsmodus te openen.
3. Klik op **Hot Spot toevoegen** → **Zone hotspot** om het paneel Hot Spot toevoegen te openen.

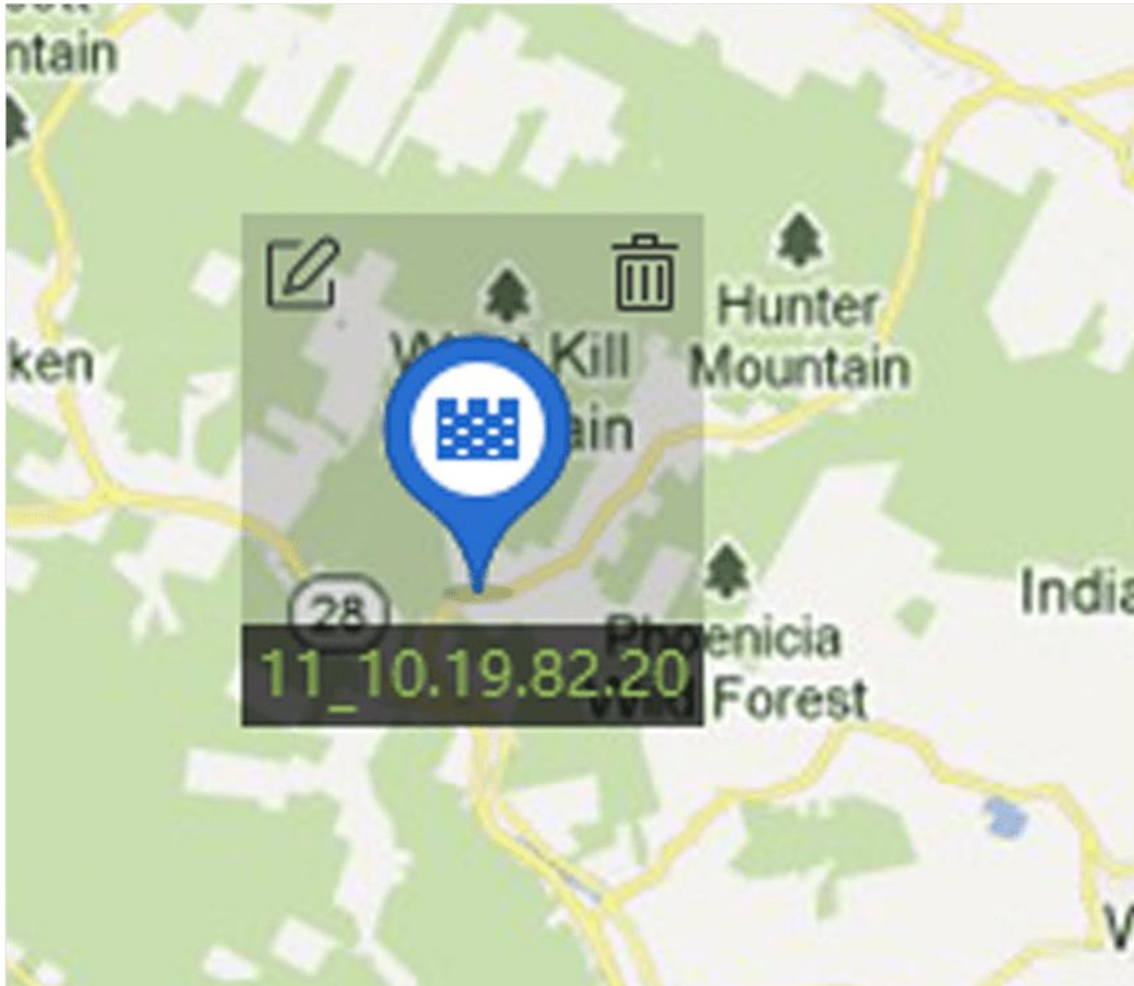


Afbeelding 9-9 Zone toevoegen als hotspot



4. Selecteer de zone(s) die u wilt toevoegen aan de kaart.
5. Optioneel: Bewerk de naam van de hotspot, selecteer de kleur van de naam en selecteer het hotspotpictogram.
6. Klik op **OK**.

 **Opmerking**

Je kunt ook de pictogrammen van de alarmuitgang uit de lijst met alarmuitgangen naar de kaart slepen om de hotspot toe te voegen.



Afbeelding 9-10 Zone op de kaart

De zone wordt als hotspot toegevoegd aan de kaart en het pictogram ervan in de groepslijst verandert van  in  .

7. Optioneel: Sleep de hotspot van de zone om deze naar een bepaalde positie te verplaatsen. Als er alarmen afgaan, wordt het nummer van de nieuwste alarmen weergegeven op het pictogram van de zone. Je kunt op het nummer klikken om de details van het alarm te bekijken.

 **Opmerking**

Er kunnen niet meer dan 10 nieuwste alarmen worden weergegeven.

8. Optioneel: Klik op **Alarm wissen** om de alarmen van de zones op de huidige kaart als gelezen te markeren.

9.4.5 Toegangspunt toevoegen als hotspot

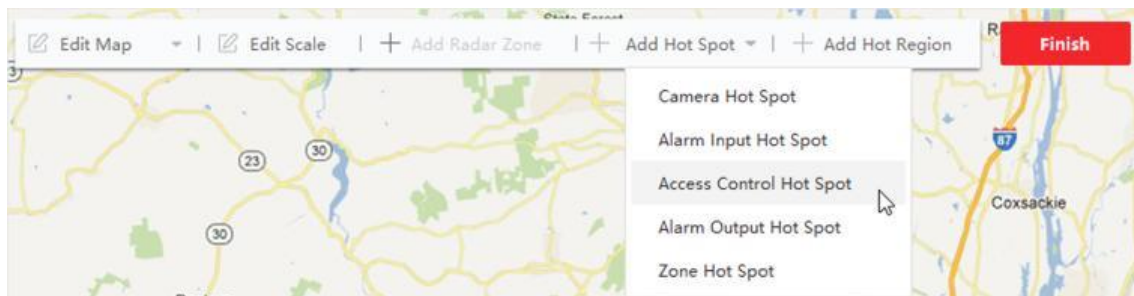
Je kunt toegangspunten aan de kaart toevoegen als hotspots, zodat je de hotspots kunt vinden en hun status en alarmnummers kunt bekijken.

Voordat u begint

Zorg ervoor dat je een kaart en een toegangspunt hebt toegevoegd aan de client. Zie [Kaart toevoegen](#) en [Apparaat toevoegen](#) voor meer informatie.

Stappen

1. Ga naar de E-mapmodule.
2. Klik op **Bewerken** op de E-map werkbalk om de kaartbewerkingsmodus te openen.
3. Klik op **Hot Spot toevoegen** → **Hot Spot toegangspunt om** het venster Hot Spot toevoegen te openen.

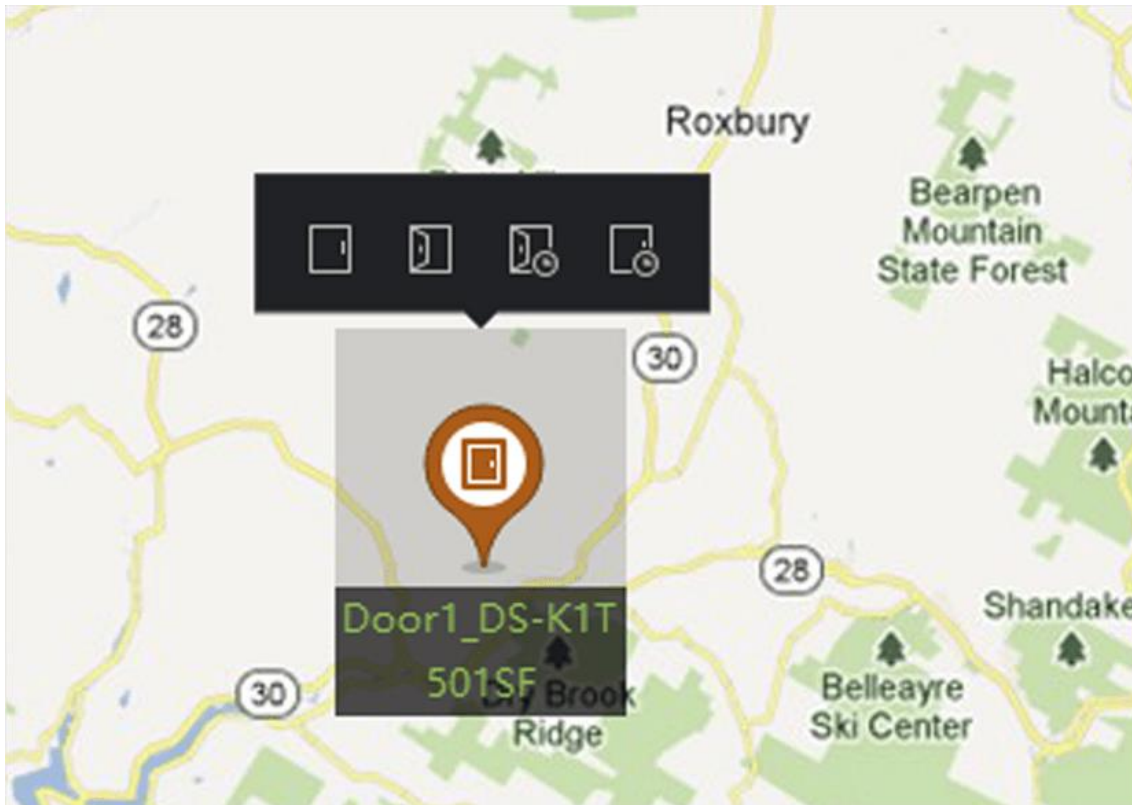


Afbeelding 9-11 Toegangspunt toevoegen als hotspot



4. Selecteer het toegangspunt (de toegangspunten) dat (die) moet(en) worden toegevoegd aan de kaart.
5. Optioneel: Bewerk de naam van de hotspot, selecteer de kleur van de naam en selecteer het hotspotpictogram.
6. Klik op **OK**.

 **Opmerking**

Je kunt ook een pictogram van een toegangspunt uit de lijst met toegangspunten naar de kaart slepen.



Afbeelding 9-12 Toegangspunt op de kaart

Het toegangspunt wordt toegevoegd aan de kaart als hotspot en het pictogram ervan in de groepslijst verandert van  naar  .

7. Optioneel: Sleep de hotspot van het toegangspunt om het naar een bepaalde positie te verplaatsen.

Wanneer er alarmen afgaan, wordt het nummer van de nieuwste alarmen weergegeven op het hotspotpictogram. Je kunt op het nummer klikken om de details van het alarm te bekijken.

 **Opmerking**

Er kunnen niet meer dan 10 nieuwste alarmen worden weergegeven.

Hoofdstuk 10 Statistieken

10.1.1 Rapport over het tellen van personen per codeerapparaat

Rapport over het tellen van personen per codeerapparaat toont gegevens over het tellen van personen die zijn verzameld door codeerapparaten. Je kunt de gegevens over het tellen van personen in verschillende dimensies doorzoeken.

Voordat u begint

Voeg een codeerapparaat met een functie voor het tellen van personen toe aan de software en configureer het overeenkomstige gebied en de regel voor het tellen van personen correct. Raadpleeg [Apparaat toevoegen](#) voor meer informatie over het toevoegen van een apparaat voor het tellen van personen.

Stappen

1. Klik op **Rapport** → **Volkstelling** om de pagina Volkstelling te openen.
2. Selecteer **Codeerapparaat** als **Apparaattype**.
3. Selecteer dagelijks rapport, wekelijks rapport, maandelijks rapport of jaarlijks rapport als rapporttype.

Dagelijks verslag

Dagelijks rapport toont gegevens op dagelijkse basis. Het systeem berekent het aantal mensen in elk uur van een dag.

Wekelijks rapport, maandelijks rapport en jaarlijks rapport

In vergelijking met dagrapporten kunnen wekrapporten, maandrapporten en jaarrapporten minder tijdrovend zijn, omdat ze niet elke dag hoeven te worden ingediend. Het systeem berekent het aantal mensen in elke dag van een week, in elke dag van een maand, in elke maand van een jaar.

Aangepast rapport

Gebruikers kunnen de dagen in het rapport aanpassen om het aantal mensen op elke dag of maand van het aangepaste tijdsinterval te analyseren.



Opmerking

Je kunt niet meer dan 31 dagen op de kalender selecteren.

4. Selecteer het type statistiektijd en klik op  om de tijd in te stellen.

Een periode

Genereer de statistieken in één tijdsperiode.

Meerdere perioden

Genereer de statistieken in twee tijdsperiodes, die je kunnen helpen om de mensenstroom en het aantal mensen in twee tijdsperiodes te vergelijken.

Als u bijvoorbeeld het rapporttype instelt als maandrapport en maart en april instelt als statistiektijd, worden de resultaten van het tellen van mensen in maart en april weergegeven in dezelfde grafiek met verschillende kleuren en kunt u de gegevens op verschillende dagen van elke maand vergelijken.

5. Selecteer **Statistiektype**.

Weergave per apparaat

Het rapport per apparaat weergeven.

Als je bijvoorbeeld één NVR selecteert (met 4 personen die camera's tellen), zal het rapport het totale aantal personen weergeven, gesommeerd door de 4 personen die camera's tellen.

Weergave per camera

Het rapport per camera weergeven.

Als je bijvoorbeeld één NVR selecteert (met 4 mensen die camera's tellen), zal het rapport de statistieken van elke camera respectievelijk weergeven, namelijk de statistieken in 4/8 kleuren (elke één of twee kleuren vertegenwoordigen één camera).

Weergave door groepering Statistieken

Geef het rapport weer door statistieken te groeperen.

Als je bijvoorbeeld één apparaatgroep selecteert (de groep wordt aangemaakt op de Client), zal het rapport het totale aantal personen weergeven, opgeteld bij het totale aantal personen dat camera's telt in de groep.

Opmerking

- Raadpleeg **Groepsbronnen** voor meer informatie over apparaatgroepen.
 - Deze functie moet worden ondersteund door het apparaat.
-

6. Selecteer de filtermodus.

Kanaal

Teldata van mensen weergeven die verzameld zijn door kanalen van een codeerapparaat.

Regio

Geef het aantal mensen in geselecteerde gebieden van een camera weer.

Opmerking

U moet vooraf regio's configureren voor de camera. Raadpleeg de gebruikershandleiding van het apparaat voor meer informatie.

7. Selecteer camera('s) of regio('s) in de lijst **Camera**.

8. Stel de weer te geven inhoud in.

Richting

Bereken het aantal mensen in verschillende richtingen, zoals binnenkomen, weggaan of binnenkomen en weggaan.

Ga naar

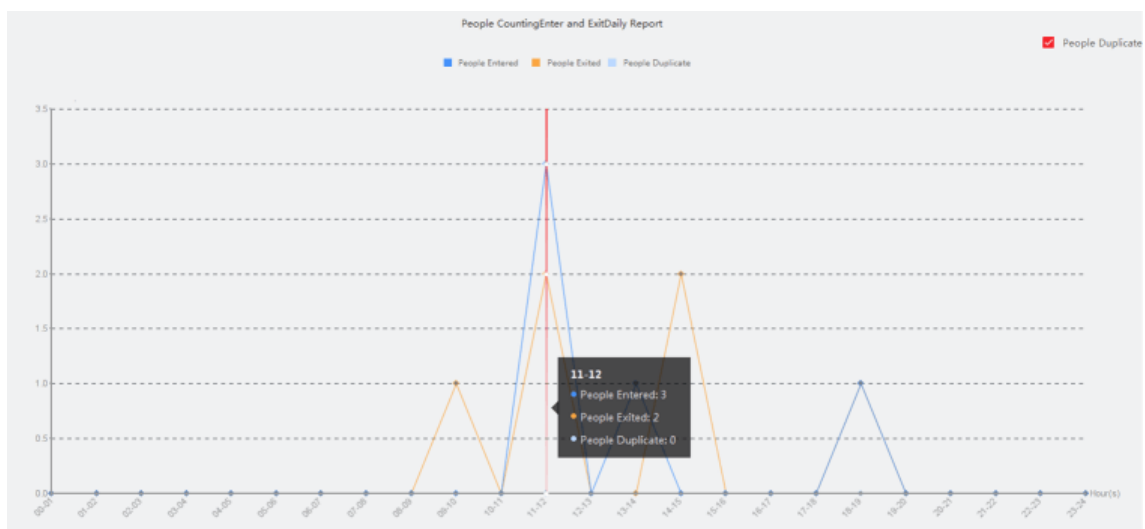
De ingevoerde mensen worden geteld.

Ga naar

De mensen die weggaan worden geteld.

In- en uitgaan

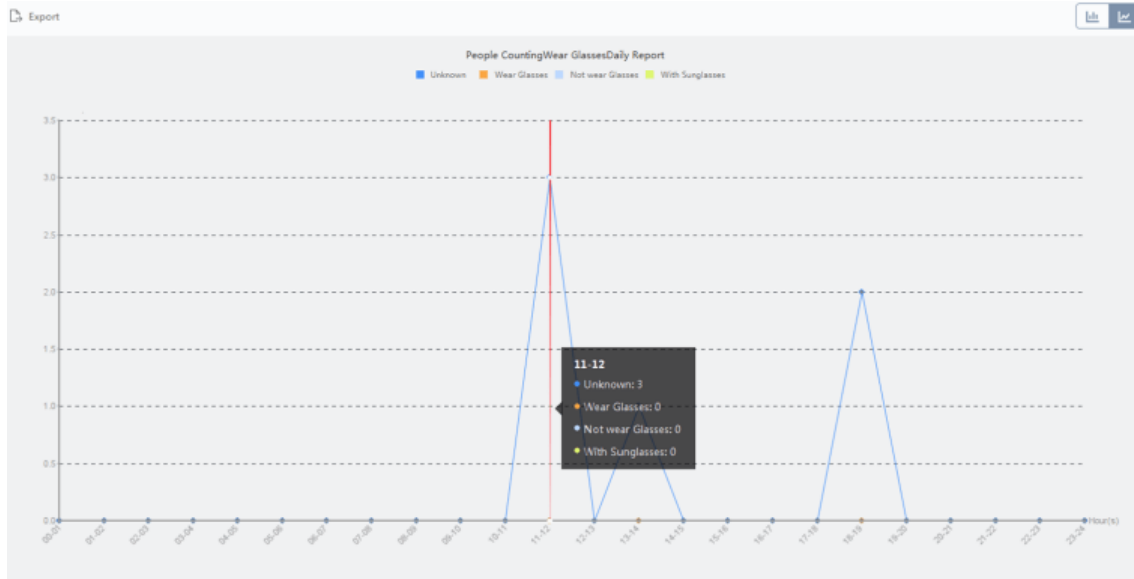
Zowel in- als uitgaande personen worden geteld.



Figuur 10-1 Telling van personen per richting

Gezichtskenmerken

Genereer het rapport op basis van het gezichtskenmerk.



Figuur 10-2 Mensen tellen op gezichtskenmerken

9. Optioneel: Vink **Alleen kinderen** aan om een rapport van herkende kinderen te genereren.

Opmerking

- De client telt gedetecteerde personen die kleiner zijn dan een vooraf gedefinieerde lengte die kan worden geconfigureerd op de externe configuratiepagina van het apparaat. Raadpleeg de gebruikershandleiding van het apparaat voor meer informatie over het configureren van de hoogtedrempel.
- Deze functie moet worden ondersteund door het apparaat.

10. Klik op **Zoeken** om de statistieken van het aantal personen en gedetailleerde gegevens voor elk uur, elke dag of elke maand te bekijken.

Standaard worden de statistieken weergegeven in histogramvorm.

11. Optioneel: Voor het rapport per richting kun je **Mensen dupliceren** aanvinken in de rechterbovenhoek van de rapportpagina om het aantal dubbele personen weer te geven.

Opmerking

Het aantal dubbele personen wordt berekend door het apparaat. Als hetzelfde gezicht meer dan eens wordt herkend, wordt hij/zij berekend als een dubbel persoon.


Als een caissière bijvoorbeeld meer dan één keer de supermarkt binnenkomt of verlaat, wordt hij/zij berekend als een dubbel persoon. Op deze manier kan de supermarkt het werkelijke aantal winkelende mensen achterhalen.

12. Optioneel: Voer de volgende bewerkingen uit na het zoeken.

Overschakelen naar lijndiagram Klik op om over te schakelen naar lijngrafiek.

 **Opmerking**

Standaard worden de statistieken weergegeven in een staafdiagram.

Overschakelen naar staafdiagram Klik op  om over te schakelen naar staafdiagram.

Opslaan op lokale pc Klik op **Exporteren** om de gedetailleerde gegevens van het tellen van personen op te slaan op je pc.

10.2 Rapport over het tellen van personen op kruispunten bekijken

Kruispuntanalyse wordt gebruikt om de doorstroming en het aantal mensen in een kruispuntachtige omgeving te controleren. De pijlen in de afbeelding verwijzen naar verschillende richtingen. Door één richting (bijv. A) als ingang te selecteren, worden de andere richtingen standaard ingesteld als uitgangen, zodat er meerdere paden worden gegenereerd (bijv. van A naar A, van A naar B, van A naar C en van A naar D). Je kunt het aantal mensen bekijken die elk pad zijn gepasseerd, wat de winkelier kan helpen om de mensenstroom in verschillende deuren te analyseren. Het statistische resultaat kan worden weergegeven in een dagelijks, wekelijks, maandelijks en jaarlijks rapport.

Voordat u begint

Zorg ervoor dat een fisheye-camera die de functie voor kruispuntanalyse ondersteunt correct is geconfigureerd en wordt toegevoegd aan de software. Raadpleeg **Apparaat toevoegen** voor meer informatie over het toevoegen van het apparaat.

Stappen

 **Opmerking**

Er kunnen maximaal 10 kruispunten worden geanalyseerd.

1. Klik op **Rapport** → **Kruispuntanalyse** om de module voor kruispuntanalyse te openen.
2. Selecteer dagelijks rapport, wekelijks rapport, maandelijks rapport of jaarlijks rapport als rapporttype.

Dagelijks verslag

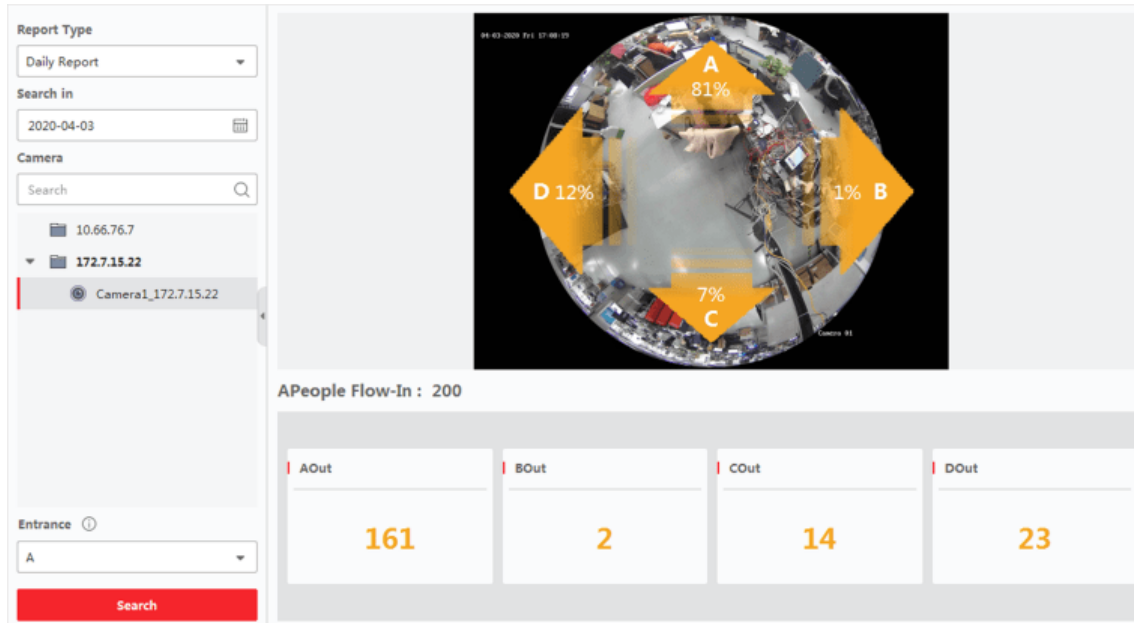
Dagrapport toont gegevens op dagelijkse basis. Het systeem berekent het aantal mensen in het intersectierapport in elk uur van een dag.

Wekelijks rapport, maandelijks rapport en jaarlijks rapport

In vergelijking met een dagelijks rapport, kunnen weekrapporten, maandrapporten en

jaarrapporten minder tijdrovend zijn, omdat ze niet elke dag hoeven te worden ingediend. Het systeem berekent het aantal personen in het intersectierapport op elke dag van een week, op elke dag van een maand, in elke maand van een jaar.

3. Stel de starttijd voor het rapport in.
4. Selecteer de camera voor het genereren van het rapport.
5. Selecteer één richting als ingang in de vervolgkeuzelijst in het vak **Flow in**.
6. Klik op **Zoeken** voor het resultaat van de statistieken.



Figuur 10-4 Resultaten

Het mensennummer voor elk pad wordt rechts weergegeven.

10.4 Hittekaartrapport

Hittekaart is een grafische weergave van gegevens die worden weergegeven door kleuren en de gegevens van de hittekaart kunnen worden weergegeven in een lijndiagram. Je kunt de hittekaartfunctie van de camera gebruiken om de bezoektijden en verblijftijd van klanten in een ingesteld gebied te analyseren, wat de winkelhouder kan helpen om het geïnteresseerde gebied van de klanten te analyseren en de goederen te rangschikken.

Voordat u begint

Voeg een netwerkcamera met heatmap toe aan de software en configureer het bijbehorende gebied op de juiste manier. De toegevoegde camera moet geconfigureerd zijn met de heatmap-regel. Zie [Apparaat toevoegen](#) voor meer informatie over het toevoegen van een netwerkcamera met heatmap.

Stappen

1. Klik op **Rapport** → **Hittekaart** om de pagina Hittekaart te openen.

2. Selecteer **Dagelijks** rapport/Wekelijks rapport/Maandelijks rapport/ **Jaarlijks** rapport/Aangepast **rapport** als het rapporttype.

Dagelijks verslag

Dagelijks rapport toont gegevens op dagelijkse basis. Het systeem berekent de gegevens van de hittekaart in elk uur van een dag.

Wekelijks rapport, maandelijks rapport en jaarlijks rapport

In vergelijking met dagrapporten kunnen wekrapporten, maandrapporten en jaarrapporten minder tijdrovend zijn, omdat ze niet elke dag hoeven te worden ingediend. Het systeem berekent de gegevens van de warmtekaart voor elke dag van een week, voor elke dag van een maand en voor elke maand van een jaar.

Aangepast rapport

Je kunt de dagen in het rapport aanpassen om de verblijftijd of druktestrend op elke dag of maand van het aangepaste tijdsinterval te analyseren.

Opmerking

De tijdsperiode in het aangepaste rapport mag niet langer zijn dan 31 dagen.

3. Selecteer **Op verblijfstijd** of **Op menigte-trend** als statistiektype.

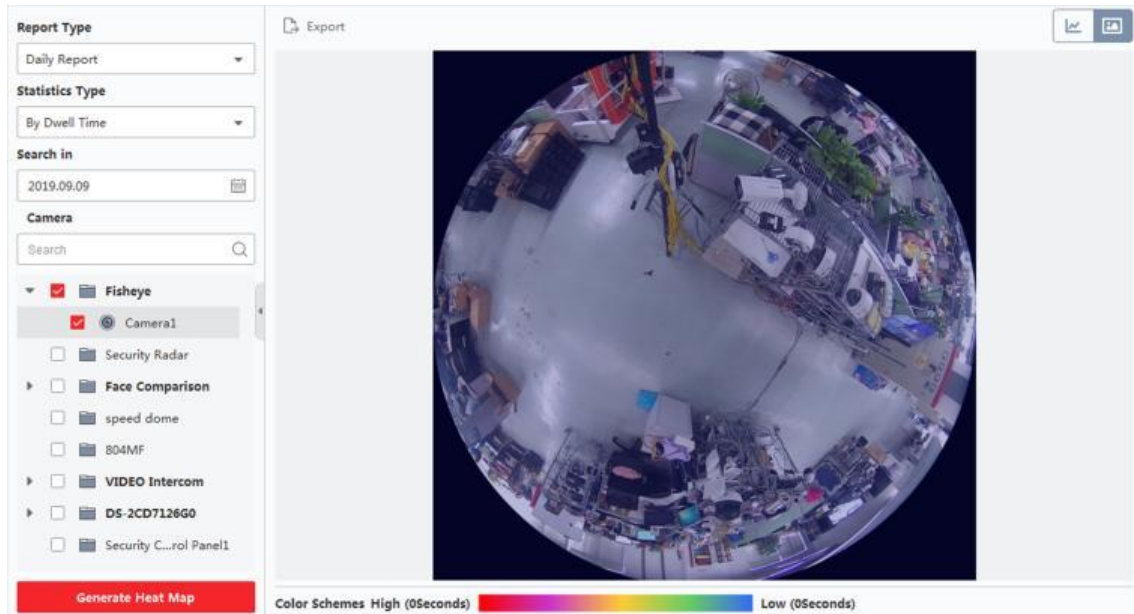
Door Dwell Time

Het systeem berekent de waarde van de hittekaart (de ordinaatwaarde in de lijngrafiek of de kleur in afbeeldingen) op basis van de verblijftijd van de mensen.

Door Crowd Trend

Het systeem berekent de waarde van de hittekaart (de ordinaatwaarde in de lijngrafiek of de kleur in afbeeldingen) op basis van het aantal gedetecteerde personen.

4. Stel de zoekperiode in.
5. Selecteer een warmtekaartcamera in de cameralijst.
6. Klik op **Warmtekaart genereren** om de warmtekaart van de camera weer te geven.




Afbeelding 10-9 Resultaten

7. Optioneel: Na het genereren van het hittekaartrapport kun je de volgende bewerkingen uitvoeren.

Weergave in lijndiagram

Klik op  om de statistieken weer te geven in een lijngrafiek.

Weergave in de modus Beeld

Klik op  om de statistieken in beeldmodus weer te geven. Het rode kleurblok (255, 0, 0) geeft het meest welkome gebied aan en het blauwe kleurblok (0, 0, 255) geeft het minder populaire gebied aan.

Statistieken opslaan

Klik op **Exporteren** om de gedetailleerde gegevens van de hittekaart op te slaan op je pc.

10.7 Temperatuurkaart

Een temperatuurkaart toont het temperatuurverloop van een regio gedurende een bepaalde dag. Als je regio's voor temperatuurbewaking hebt geconfigureerd, kun je een temperatuurkaart van specifieke regio's genereren om een overzicht van de temperatuurtrend van elke regio te bekijken.

Voordat u begint

- Zorg ervoor dat je regio's hebt getekend voor de temperatuurkaart op de configuratiepagina van het apparaat. Raadpleeg de gebruikershandleiding van het apparaat voor meer informatie.
- Zorg ervoor dat je minstens één apparaat voor de temperatuurkaart hebt toegevoegd aan de client. Zie **Apparaat toevoegen** voor meer informatie.

Stappen

Opmerking

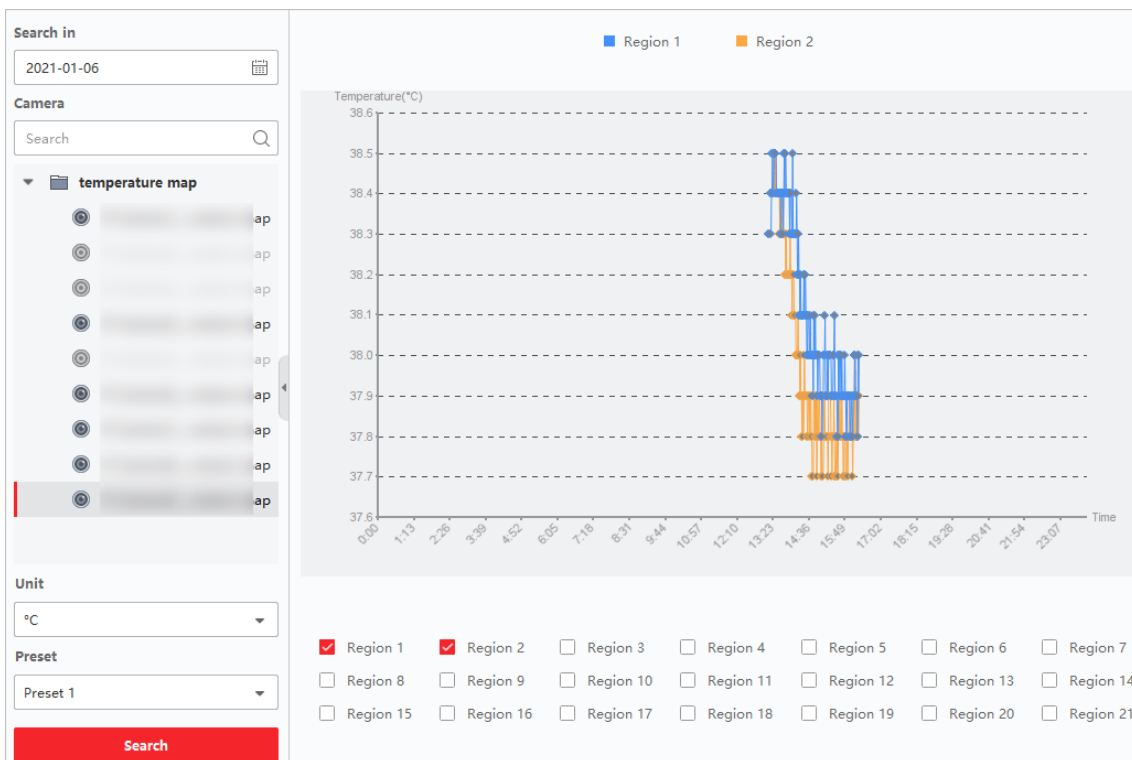
Deze functie moet worden ondersteund door het apparaat.

1. Klik op **Rapport** → **Temperatuurkaart**.
2. Selecteer een datum in de kalender.
3. Selecteer een camera in de lijst Camera.

Opmerking

U kunt een trefwoord invoeren in het zoekveld om een camera te zoeken.

4. Selecteer een eenheid.
5. Selecteer een preset.



Afbeelding 10-12 Temperatuurkaart

6. Selecteer in het rechterpaneel regio('s) voor het genereren van het rapport.

Opmerking

Er kunnen niet meer dan 8 regio's worden gecontroleerd.

7. Klik op **Zoeken**.
De temperatuurkaart wordt weergegeven in een lijngrafiek waarbij elke lijn een regio voorstelt.

8. Optioneel: Selecteer een andere eenheid om de temperatuurkaart in een andere eenheid weer te geven.

Hoofdstuk 11 Gegevens ophalen

In de Data Retrieval-module kunt u zoeken naar opnames op basis van auto's en menselijke objecten. Het apparaat moet de functie "Auto" of "Mens" ondersteunen.


11.1 Ophalen van voertuigen

Voor apparaten die het terugvinden van voertuigen ondersteunen, kunt u de gerelateerde foto's en video's van voertuigen zoeken door de zoekvoorwaarden in te stellen, zoals het kenteken en de tijd van opname.

Voordat u begint

Voeg het apparaat dat het ophalen van voertuigen ondersteunt toe aan de client en configureer de bijbehorende instellingen. Zie [Apparaat toevoegen](#) voor meer informatie over het toevoegen van het apparaat.

Stappen

1. Klik op **Gegevens ophalen** → **Voertuig ophalen om naar** de pagina Voertuig ophalen te gaan.
2. Klik op  om de begin- en eindtijd voor het zoeken in te stellen.
3. Selecteer het zoektype.

Voertuig

Zoek en toon de vastgelegde voertuigfoto's door het kenteken van het voertuig in te voeren.

Detectie van gemengd verkeer

Zoek en toon de foto's van het specifieke voertuig met betrekking tot verkeersdetectie door het kenteken van het voertuig in te voeren.



Opmerking

De camera moet verkeersherkenning ondersteunen.

4. Selecteer een apparaat in de lijst met camera's.
-

6. Optioneel: Voer het kenteken in (ondersteuning voor fuzzy search) om te zoeken.
7. Optioneel: Stel het maximum aantal weer te geven zoekresultaten in.
8. Klik op **Zoeken om te** beginnen met zoeken.
De gemaakte foto's die voldoen aan de zoekvoorwaarden worden weergegeven op het rechterpaneel. Er kunnen maximaal 30 foto's op één pagina worden weergegeven.
9. Optioneel: Voer indien nodig de volgende bewerkingen uit.

Afbeelding exporteren


- U kunt een of meer gezochte afbeeldingen exporteren.
1. Klik op **Afbeelding exporteren**.

2. Vink een of meer foto's aan of **selecteer Alles selecteren** op de pagina hieronder.
3. Klik op **Exporteren** om de geselecteerde foto('s) te exporteren naar de lokale pc.

Details bekijken

Klik op een foto om de opnamegegevens te bekijken, zoals de tijd van opname en de naam van de camera.





Opmerking

Je kunt op  klikken om een vergrote afbeelding te bekijken.


Gerelateerde video afspelen

Klik op **Afspelen** om het bijbehorende videobestand (5s voor en 5s na de opname) af te spelen in het weergavevenster.

Opmerking

- Je kunt op  klikken om de video in een groter venster te bekijken.
 - U kunt op  klikken om de afspeelsnelheid aan te passen, op  klikken om het videobestand frame per frame af te spelen en op  klikken om audio in te schakelen.
-

Enkel record exporteren

Op de vergrote afbeeldingspagina klikt u op  en vervolgens op **Afbeelding exporteren**, **Videobestand exporteren** of **Details exporteren** om de afbeelding, het videobestand en de opnamegegevens van één opname naar de lokale pc te exporteren.

Hoofdstuk 14 Persoonsbeheer

Je kunt persoonsinformatie aan het systeem toevoegen voor verdere bewerkingen zoals toegangscontrole, video-intercom, tijdregistratie, enz. Je kunt de toegevoegde personen beheren, zoals het uitgeven van kaarten aan hen in een batch, het importeren en exporteren van persoonsinformatie in een batch, enz.

Belangrijke opmerking: Voor gedetailleerde configuratie, bijv. voor ABUS intercomsystemen of ABUS Face Access modules, dient u de bijbehorende handleiding van het betreffende product te

lezen.

14.1 Organisatie toevoegen

Je kunt een organisatie toevoegen en informatie over personen importeren in de organisatie voor een effectief beheer van personen. Je kunt ook een ondergeschikte organisatie toevoegen voor de toegevoegde organisatie.


Stappen


1. Module **Persoon** invoeren.
2. Selecteer een bovenliggende organisatie in de linkerkolom en klik op **Toevoegen** in de linkerbovenhoek om een organisatie toe te voegen.
3. Maak een naam voor de toegevoegde organisatie.

Opmerking

Er kunnen maximaal 10 niveaus van organisaties worden toegevoegd.

4. Optioneel: Voer de volgende bewerking(en) uit.

Organisatie bewerken Beweeg de muis over een toegevoegde organisatie en klik op  om de naam te bewerken.

Organisatie verwijderen Beweeg de muis over een toegevoegde organisatie en klik op  om deze te verwijderen.

Opmerking

- De organisaties op een lager niveau worden ook verwijderd als je een organisatie verwijdert.
 - Zorg ervoor dat er geen persoon is toegevoegd onder de organisatie, anders kan de organisatie niet worden verwijderd.
-

Toon personen in suborganisatie Vink **Toon personen in suborganisatie** aan en selecteer een organisatie om personen in de suborganisaties te tonen.

14.2 Persoon toevoegen

Je kunt personen één voor één toevoegen aan de clientsoftware. De persoonsinformatie bevat basisinformatie, gedetailleerde informatie, profielen, informatie over toegangscontrole,

referenties, aangepaste informatie, enz.

14.2.1 Basisinformatie configureren

Je kunt één voor één personen aan de client toevoegen en de basisinformatie van de persoon configureren, zoals naam, e-mail, telefoonnummer, enz.

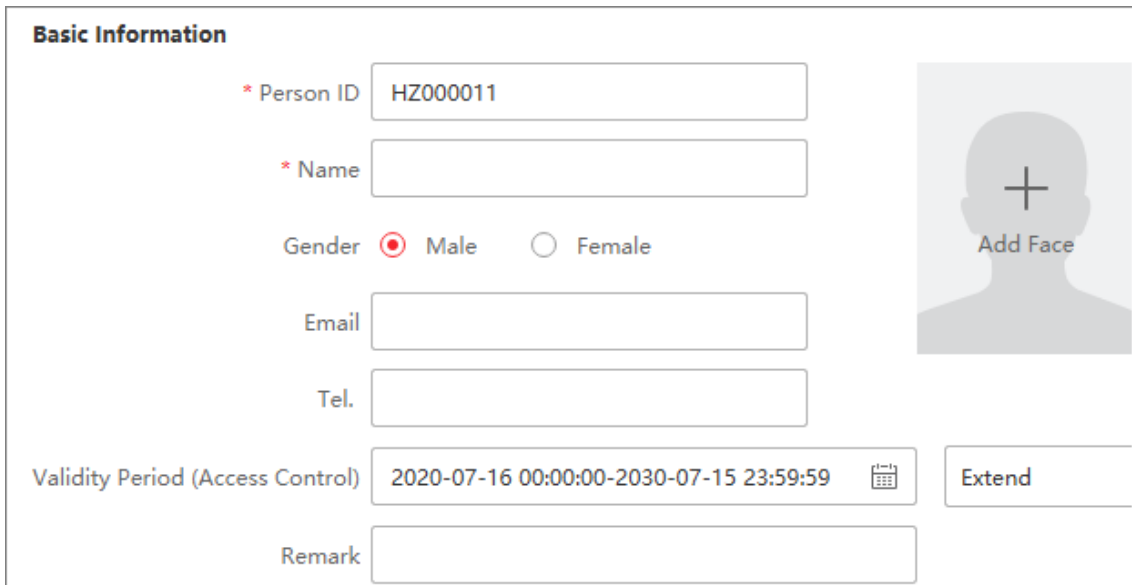
Stappen

1. Module **Persoon** invoeren.

Opmerking

De eerste keer dat je naar de module **Persoon** gaat, verschijnt er een venster waarin je de regels kunt instellen voor het genereren van persoon-ID's (ondersteund door letters en cijfers) bij het toevoegen van personen. Als er geen persoon-ID's zijn bij het ophalen van persoonsinformatie van het apparaat, worden de persoon-ID's volgens de regel gegenereerd.

2. Selecteer een organisatie in de organisatielijst om de persoon toe te voegen.
3. Klik op **Toevoegen** om het venster Persoon toevoegen te openen.
De persoon-ID wordt automatisch aangemaakt.
4. Voer de basisinformatie in, waaronder de naam van de persoon, het telefoonnummer, het e-mailadres, de geldigheidsperiode, enz.



Basic Information


* Person ID

* Name

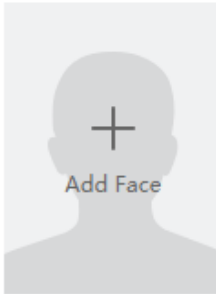
Gender Male Female

Email

Tel.

Validity Period (Access Control) 

Remark

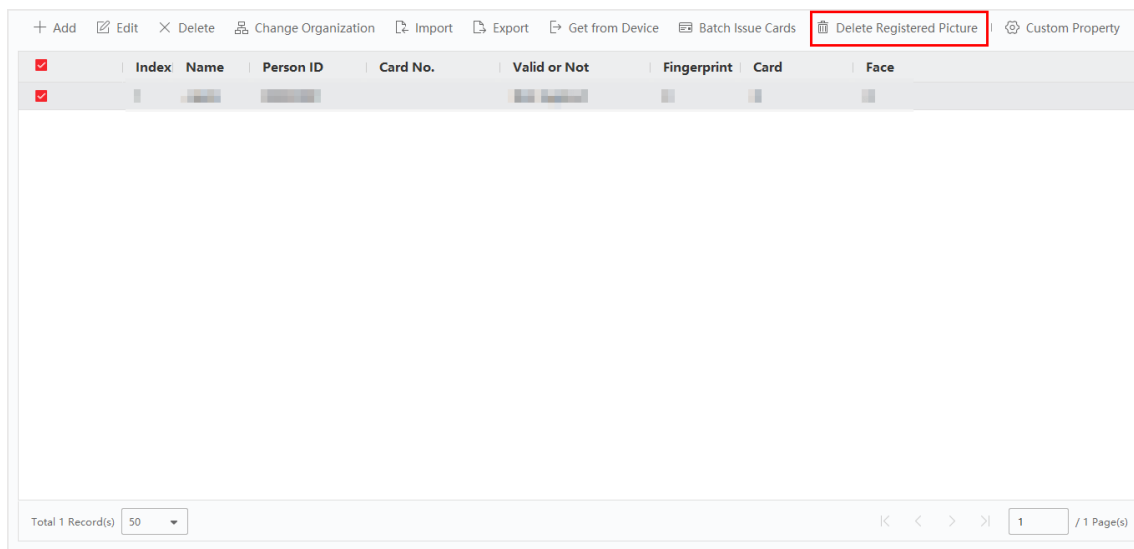


Figuur 14-1 Basisinformatie configureren

Opmerking

Als de geldigheidsperiode is verlopen, zijn de referenties en toegangscontrole-instellingen van de persoon ongeldig en heeft de persoon geen autorisatie meer voor toegang tot de deuren. Je kunt op **Verlengen** klikken om de geldigheidsperiode van de persoon te verlengen met 1 maand, 3 maanden, 6 maanden of 1 jaar.

5. Bevestig om de persoon toe te voegen.
 - Klik op **Toevoegen** om de persoon toe te voegen en sluit het venster Persoon toevoegen.
 - Klik op **Toevoegen en Nieuw** om de persoon toe te voegen en ga verder om andere personen toe te voegen.
6. Geregistreerd gezichtsbeeld verwijderen



Afbeelding 14-2 Geregistreerde afbeelding verwijderen

Opmerking

Als **Afbeeldingen opslaan in structuurgegevensformaat** is ingeschakeld, wordt de knop **Geregistreerde afbeelding verwijderen** toegevoegd aan de pagina **Persoon**. Over het algemeen wordt de geregistreerde gezichtsfoto automatisch verwijderd zodra de informatie van de persoon op het apparaat is toegepast. Door op de persoon te dubbelklikken, verschijnt het venster **Persoon bewerken** en kun je controleren of de geregistreerde gezichtsfoto is verwijderd. Zo niet, dan kun je deze persoon selecteren en op **Verwijder geregistreerde foto** klikken om de foto handmatig te verwijderen.

14.2.2 Een kaart uitgeven aan één persoon

Als je een persoon toevoegt, kun je hem/haar een kaart geven als toegangsbewijs voor de deur(en). Voordat je een persoon een kaart geeft, moet je de kaartuitgiftmodus instellen om het

kaartnummer te krijgen. Behalve het handmatig invoeren van het kaartnummer, biedt de client ook twee andere modi voor het lezen van het kaartnummer: lokaal (via het kaartregistratiestation) of op afstand (via de kaartlezer van het toegangscontroleapparaat).

Opmerking

Eén persoon kan maximaal vijf kaarten krijgen.

Kaart uitgeven door kaartnummer in te voeren


Als er geen apparaat (kaartregistratiestation/kaartlezer) beschikbaar is om het kaartnummer te lezen, kunt u een kaart uitgeven door het kaartnummer handmatig in te voeren.

Stappen

1. Module **Persoon** invoeren.
 2. Selecteer een organisatie in de organisatielijst om de persoon toe te voegen en klik op **Toevoegen** om het paneel Persoon toevoegen te openen.
-

Opmerking

Voer eerst de basisinformatie van de persoon in. Raadpleeg **Basisinformatie configureren** voor meer informatie over het configureren van de basisinformatie van de persoon.

3. Klik in het gebied **Credential** → **Card** op  .
4. Voer het kaartnummer handmatig in op de pagina Toevoegen.
5. Klik op **Toevoegen**.
De kaart wordt aan de persoon verstrekt.

Een kaart uitgeven in lokale modus


Als er een kaartregistratiestation beschikbaar is, kun je een kaart uitgeven via de lokale modus. Om het kaartnummer te lezen, moet je het kaartregistratiestation verbinden met de pc waarop de client draait via de USB-interface of COM, en de kaart op het kaartregistratiestation plaatsen.

Stappen

1. Module **Persoon** invoeren.
 2. Selecteer een organisatie in de organisatielijst om de persoon toe te voegen en klik op **Toevoegen** om het paneel Persoon toevoegen te openen.
-

Opmerking

Voer eerst de basisinformatie van de persoon in. Raadpleeg **Basisinformatie configureren** voor meer informatie over het configureren van de basisinformatie van de persoon.

3. Klik in het gebied **Credential** → **Card** op  .
 4. Klik op **Instellingen** om de instellingenpagina te openen.
-

5. Selecteer **Lokaal** als de kaartuitgiftemodus.
6. Stel andere gerelateerde parameters in.

Kaart registratiestation

Selecteer een model van het kaartregistratiestation in de vervolgkeuzelijst. U kunt het kaartregistratiestation aansluiten op de pc en de basisinformatie over de toegevoegde persoon overdragen tussen de twee apparaten via USB.

Kaarttype

Selecteer het kaarttype als EM-kaart of Mifare-kaart op basis van het actuele kaarttype.

Zoemend

Zoemgeluid in- of uitschakelen wanneer het kaartnummer met succes is gelezen.

Kaartnr. Type

Selecteer het type kaartnummer volgens de werkelijke behoeften.

M1-kaartcodering

Als de kaart een M1-kaart is, dan kun je de M1-kaartcoderingsfunctie inschakelen en de te coderen kaartsector selecteren.

7. Klik op **OK om** de bewerking te bevestigen.
8. Plaats de kaart op het kaartregistratiestation en klik op **Lezen** om het kaartnummer te krijgen. Het kaartnummer wordt automatisch weergegeven in het veld Kaartnummer.
9. Klik op **Toevoegen**.
De kaart wordt aan de persoon verstrekt.

Een kaart uitgeven met de modus Op afstand


Behalve een kaart uitgeven via de lokale modus, kun je de kaart ook op de kaartlezer van het toegevoegde toegangscontroleapparaat vegen om het kaartnummer te krijgen. Dit is van toepassing als de klant en de personen die de kaarten moeten uitgeven zich niet op dezelfde locatie bevinden. Je kunt bijvoorbeeld kaarten uitgeven voor werknemers in een filiaal op afstand via de client.

Stappen

1. Module **Persoon** invoeren.
2. Selecteer een organisatie in de organisatielijst om de persoon toe te voegen en klik op **Toevoegen** om het paneel Persoon toevoegen te openen.

Opmerking

Voer eerst de basisinformatie van de persoon in. Raadpleeg **[Basisinformatie configureren](#)** voor meer informatie over het configureren van de basisinformatie van de persoon.

3. Klik in het gebied **Credential** → **Card** op  .
4. Klik op **Instellingen** om de instellingenpagina te openen.

5. Selecteer **Kaartlezer** als de kaartuitgiftemodus.
6. Selecteer een toegangscontroleapparaat dat is toegevoegd in de client.
7. Selecteer een toegevoegd toegangscontroleapparaat of het registratiestation in de vervolgkeuzelijst.

Opmerking

- Als je toegangscontroleapparaat selecteert, controleer dan of je de apparaten hebt ingeschakeld.
 - Als je het registratiestation selecteert, moet je op **Aanmelden** klikken om de gerelateerde parameters van het apparaat in te stellen, zoals IP-adres, poortnummer, gebruikersnaam en wachtwoord. Controleer ook RF-kaarttype(s) als dat nodig is.
-

8. Klik op **OK om** de bewerking te bevestigen.
9. Plaats de kaart op de kaartlezer en klik op **Lezen** om het kaartnummer te krijgen. Het kaartnummer wordt automatisch weergegeven in het veld Kaartnummer.
10. Klik op **Toevoegen**. De kaart wordt aan de persoon verstrekt.

14.2.3 Een gezichtsfoto uploaden vanaf de lokale pc

Wanneer je een persoon toevoegt, kun je een gezichtsfoto die op je lokale pc is opgeslagen uploaden naar de client als het profiel van de persoon.

Stappen

1. Module **Persoon** invoeren.
2. Selecteer een organisatie in de organisatielijst om de persoon toe te voegen en klik op **Toevoegen**.

Opmerking

Voer eerst de basisinformatie van de persoon in. Raadpleeg **Basisinformatie configureren** voor meer informatie over het configureren van de basisinformatie van de persoon.

3. Klik op **Gezicht toevoegen** in het paneel Basisinformatie.
4. Selecteer **Uploaden**.
5. Selecteer een afbeelding op de pc waarop de client draait.

Opmerking

De foto moet het JPG- of JPEG-formaat hebben en kleiner zijn dan 200 KB.

6. Optioneel: Schakel **Verify by Device** in om te controleren of het gezichtsherkenningapparaat dat in de client wordt beheerd het gezicht op de foto kan herkennen.

 **Opmerking**

Deze functie wordt verborgen of getoond afhankelijk van de capaciteit van het apparaat.

7. Bevestig om de persoon toe te voegen.

- Klik op **Toevoegen** om de persoon toe te voegen en sluit het venster Persoon toevoegen.
- Klik op **Toevoegen en Nieuw** om de persoon toe te voegen en ga verder om andere personen toe te voegen .

14.2.4 Een foto maken via de client

Wanneer u een persoon toevoegt, kunt u een foto van een persoon maken met de geïntegreerde camera van de client, een USB-camera of een registratiestation en deze foto instellen als het profiel van de persoon.

Voordat u begint

Zorg ervoor dat de pc waarop de client draait aan een van de volgende voorwaarden voldoet:

- De klant heeft een camera.
- U hebt een USB-camera aangesloten op de pc.
- U hebt het registratiestation via de USB-interface aangesloten op de PC.

Stappen

1. Module **Persoon** invoeren.
2. Selecteer een organisatie in de organisatielijst om de persoon toe te voegen en klik op **Toevoegen** om het venster Persoon toevoegen te openen.

 **Opmerking**



Voer eerst de basisinformatie van de persoon in. Raadpleeg ***Basisinformatie configureren*** voor meer informatie.

3. Klik op **Gezicht toevoegen** in het gedeelte Basisinformatie.
4. Selecteer **Foto maken** om het venster Foto maken te openen.
5. Klik op ▼ om de geïntegreerde camera of het registratiestation te selecteren in de vervolgkeuzelijst.
6. Optioneel: Schakel **Verify by Device** in om te controleren of de vastgelegde gezichtsfoto kan voldoen aan de uploadvereisten.

 **Opmerking**

Deze functie wordt verborgen of getoond afhankelijk van de capaciteit van het apparaat.

7. Maak een foto.

- 1) Kijk met je gezicht naar de camera en zorg dat je gezicht in het midden van het opvangvenster staat.
- 2) Klik op  om een gezichtsfoto te maken.
- 3) Optioneel: Klik op  om opnieuw vast te leggen.
- 4) Klik op **OK** om de vastgelegde foto op te slaan.

Afbeelding 14-3 Een foto maken via de client

8. Bevestig om de persoon toe te voegen.
 - Klik op **Toevoegen** om de persoon toe te voegen en sluit het venster Persoon toevoegen.
 - Klik op **Toevoegen en Nieuw** om de persoon toe te voegen en ga verder om andere personen toe te voegen.

14.2.5 Gezicht verzamelen via toegangscontroleapparaat

Bij het toevoegen van personen kun je het gezicht van de persoon ophalen via het toegangscontroleapparaat dat aan de client is toegevoegd en dat gezichtsherkenningsondersteunt.

Stappen

1. Module **Persoon** invoeren.
2. Selecteer een organisatie in de organisatielijst om de persoon toe te voegen en klik op **Toevoegen**.

Opmerking

Voer eerst de basisinformatie van de persoon in. Raadpleeg **Basisinformatie configureren** voor meer informatie over het configureren van de basisinformatie van de persoon.

3. Klik op **Gezicht toevoegen** in het paneel Basisinformatie.
4. Selecteer **Collectie op afstand**.
5. Selecteer een toegevoegd toegangscontroleapparaat of het registratiestation in de vervolgkeuzelijst.

Opmerking

Als je het registratiestation selecteert, moet je op **Aanmelden** klikken om de gerelateerde parameters van het apparaat in te stellen, waaronder IP-adres, poortnummer, gebruikersnaam en wachtwoord. Je kunt ook **Face Anti-Spoofing** aanvinken en het liveness-niveau selecteren als Laag, Medium of Hoog.

Gezicht Anti-Spoofing

Als je deze functie aanvinkt, kan het apparaat detecteren of het gezicht dat moet worden


verzameld authentiek is.

6. Optioneel: Klik op **Kaartlezer**, selecteer de kaartlezer-ID en klik op **OK**.
-

Opmerking

Deze functie moet worden ondersteund door het apparaat.

7. Gezicht verzamelen.

- 1) Ga met je gezicht naar de camera van het geselecteerde toegangscontroleapparaat en zorg ervoor dat je gezicht zich in het midden van het verzamelenvenster bevindt.
- 2) Klik op  om een foto te maken.
- 3) Klik op **OK** om de gemaakte foto op te slaan.

8. Bevestig om de persoon toe te voegen.

- Klik op **Toevoegen** om de persoon toe te voegen en sluit het venster Persoon toevoegen.
- Klik op **Toevoegen en Nieuw** om de persoon toe te voegen en ga verder om andere personen toe te voegen.

14.2.10 Informatie over toegangscontrole configureren

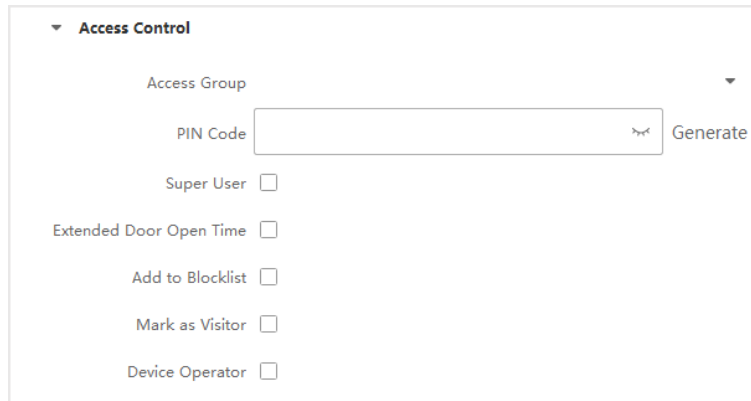
Bij het toevoegen van een persoon kun je haar/zijn toegangscontrole-informatie instellen, zoals het binden van een toegangsgroep aan de persoon, het configureren van een pincode, het instellen van de persoon als bezoeker, persoon op de blokkadellijst of supergebruiker, enz.

Stappen

1. Module **Persoon** invoeren.
 2. Selecteer een organisatie in de organisatielijst om de persoon toe te voegen en klik op **Toevoegen**.
 3. Klik in het gebied **Toegangsbeheer** op ▼ om de toegangsgroep(en) voor de persoon te selecteren.
-

Opmerking

Raadpleeg [Toegangsgroep instellen om toegangsrechten toe te wijzen aan personen](#) voor meer informatie.



▼ Access Control

Access Group ▼

PIN Code Generate

Super User

Extended Door Open Time

Add to Blocklist

Mark as Visitor

Device Operator

Figuur 14-4 Informatie over toegangscontrole configureren

4. Stel een unieke PIN-code in voor de persoon die kan worden gebruikt voor toegangsverificatie.
- Voer handmatig een pincode van 4 tot 8 cijfers in.

 **Opmerking**

PIN-codes van personen kunnen niet worden herhaald.

- Klik op **Genereren** om willekeurig een PIN-code van 6 cijfers te genereren.
-

 **Opmerking**

Als er herhaalde PIN-codes zijn, verschijnt er een prompt op de client. De beheerder kan een nieuwe PIN-code genereren om de herhaalde PIN-code te vervangen en de betreffende personen op de hoogte stellen.

5. Controleer de bedieningsrechten van de persoon.

Supergebruiker

Als de persoon is ingesteld als supergebruiker, dan heeft hij/zij toegang tot alle deuren/vloeren en is hij/zij vrijgesteld van de resterende gesloten beperkingen, alle anti-passback regels en de autorisatie van de eerste persoon.

Verlengde deur openingstijd

Gebruik deze functie voor personen met beperkte mobiliteit. Bij het betreden van de deur zal de persoon meer tijd hebben dan anderen om door deuren te gaan.

Raadpleeg **Parameters configureren voor deur/lift** voor meer informatie over het instellen van de duur dat de deur open is.

Toevoegen aan blokkijst

Voeg de persoon toe aan de blokkadellijst en wanneer de persoon toegang probeert te krijgen tot deuren/vloeren, wordt er een gebeurtenis geactiveerd en naar de klant gestuurd om het beveiligingspersoneel op de hoogte te stellen.

Markeren als bezoeker

Als de persoon een bezoeker is, moet je zijn/haar geldige bezoektijden instellen.

 **Opmerking**

De geldige tijden voor bezoek liggen tussen 1 en 100. Je kunt ook **Geen limiet** aanvinken, dan zijn er geen gelimiteerde tijden voor de bezoeker om deuren/vloeren te betreden.

Apparaat Exploitant

De persoon met de rol van apparaatoperator is gemachtigd om de toegangscontroleapparaten te bedienen.

 **Opmerking**

De functies Supergebruiker, Verlengde deuropenertijd, Toevoegen aan blokkadellijst en Markeren als bezoeker kunnen niet tegelijkertijd worden ingeschakeld. Als een persoon bijvoorbeeld is ingesteld als supergebruiker, kun je voor haar/hem geen verlengde deuropeningstijd inschakelen, haar/hem toevoegen aan de blokkadellijst of haar/hem instellen als bezoeker.

6. Bevestig om de persoon toe te voegen.
 - Klik op **Toevoegen** om de persoon toe te voegen en sluit het venster Persoon toevoegen.
 - Klik op **Toevoegen en Nieuw** om de persoon toe te voegen en ga verder om andere personen toe te voegen.

14.2.11 Persoonsgegevens aanpassen

Je kunt de persoonskenmerken die niet vooraf gedefinieerd zijn in de client aanpassen aan je eigen behoeften, bijvoorbeeld geboorteplaats. Na het aanpassen kun je bij het toevoegen van een persoon de aangepaste informatie invoeren om de persoonsinformatie compleet te maken.

Stappen

1. Module **Persoon** invoeren.
 2. Stel de velden met aangepaste informatie in.
 - 1) Klik op **Aangepast eigendom**.
 - 2) Klik op **Toevoegen** om een nieuwe eigenschap toe te voegen.
 - 3) Voer de naam van de eigenschap in.
 - 4) Klik op **OK**.
 3. Stel de aangepaste informatie in bij het toevoegen van een persoon.
 - 1) Selecteer een organisatie in de organisatielijst om de persoon toe te voegen en klik op **Toevoegen**.
-

 **Opmerking**

Voer eerst de basisinformatie van de persoon in. Raadpleeg ***Basisinformatie configureren*** voor meer informatie over het configureren van de basisinformatie van de persoon.

- 2) Voer in het deelvenster **Aangepaste informatie** de persoonsinformatie in.
-

- 3) Klik op **Toevoegen** om de persoon toe te voegen en het venster Persoon toevoegen te sluiten, of klik op **Toevoegen en Nieuw** om de persoon toe te voegen en door te gaan met het toevoegen van andere personen.

14.2.12 Informatie over de bewoner configureren

Als de persoon inwonend is, moet u voor video-intercomdoeleinden het kamernummer voor haar/hem instellen en een binnenpost binden. Na het binden kunt u deze persoon oproepen door het binnenstation te bellen en video-intercom met haar/hem uit te voeren.

Stappen

1. Module **Persoon** invoeren.
2. Selecteer een organisatie in de organisatielijst om de persoon toe te voegen en klik op **Toevoegen**.

Opmerking

Voer eerst de basisinformatie van de persoon in. Raadpleeg **Basisinformatie configureren** voor meer informatie over het configureren van de basisinformatie van de persoon.

3. Selecteer in het paneel **Bewonersinformatie** het binnenstation om het aan de persoon te binden.

Opmerking

Als je **Analoog binnenstation** selecteert, wordt het veld **Deurstation** weergegeven en moet je het deurstation selecteren dat communiceert met het analoge binnenstation.

4. Voer het verdieplingsnummer en het kamernummer van de persoon in.
5. Bevestig om de persoon toe te voegen.
 - Klik op **Toevoegen** om de persoon toe te voegen en sluit het venster Persoon toevoegen.
 - Klik op **Toevoegen en Nieuw** om de persoon toe te voegen en ga verder om andere personen toe te voegen.

14.2.13 Extra informatie configureren

Wanneer u een persoon toevoegt, kunt u de extra informatie voor de persoon configureren, zoals het identiteitstype van de persoon, het identificatienummer, het land, enzovoort, afhankelijk van de werkelijke behoeften.

Stappen

1. Module **Persoon** invoeren.
2. Selecteer een organisatie in de organisatielijst om de persoon toe te voegen en klik op **Toevoegen**.

 **Opmerking**

Voer eerst de basisinformatie van de persoon in. Raadpleeg ***Basisinformatie configureren*** voor meer informatie over het configureren van de basisinformatie van de persoon.

3. In het paneel **Extra informatie** voert u de extra informatie van de persoon in, waaronder het ID-type van de persoon, het ID-nummer, de functietitel enzovoort, afhankelijk van de huidige behoeften.
4. Bevestig om de persoon toe te voegen.
 - Klik op **Toevoegen** om de persoon toe te voegen en sluit het venster Persoon toevoegen.
 - Klik op **Toevoegen en Nieuw** om de persoon toe te voegen en ga verder om andere personen toe te voegen.

14.3 Informatie over persoonsidentificatie importeren en exporteren

Je kunt de informatie en foto's van meerdere personen in een batch importeren in de clientsoftware. Ondertussen kun je ook de gegevens en foto's van personen exporteren en op je pc opslaan.

14.3.1 Persoonlijke invoergegevens

Je kunt de informatie van meerdere personen invoeren in een vooraf gedefinieerd sjabloon (CSV/Excel-bestand) om de informatie in een batch naar de klant te importeren.

Stappen

1. Ga naar de module Persoon.
2. Selecteer een toegevoegde organisatie in de lijst of klik op **Toevoegen** in de linkerbovenhoek om een organisatie toe te voegen en deze vervolgens te selecteren.
3. Klik op **Importeren** om het paneel Importeren te openen.
4. Selecteer **Persoonsgegevens** als importeermodus.
5. Klik op **Sjabloon voor importeren van persoon downloaden** om de sjabloon te downloaden.
6. Voer de persoonsinformatie in de gedownloade sjabloon in.

 **Opmerking**

- Als de persoon meerdere kaarten heeft, scheidt u het kaartnummer met een puntkomma.
 - Items met een sterretje zijn verplicht.
 - Standaard is de Inhuurdatum de huidige datum.
-

7. Klik op **...** om het CSV/Excel-bestand met persoonsgegevens van de lokale pc te selecteren.
8. Klik op **Importeren** om het importeren te starten.

 **Opmerking**

- Als een persoonsnummer al bestaat in de database van de klant, verwijder dan de bestaande informatie voordat u importeert.
 - Je kunt informatie van niet meer dan 2.000 personen importeren.
-


14.3.2 Afbeeldingen van personen importeren

Na het importeren van gezichtsfoto's voor de toegevoegde personen in de client, kunnen de personen op de foto's worden geïdentificeerd door een toegevoegde terminal voor gezichtsherkenning. Je kunt de foto's van personen één voor één importeren of meerdere foto's tegelijk, afhankelijk van je behoefte.

Voordat u begint

Zorg ervoor dat je vooraf informatie hebt geïmporteerd aan de klant.

Stappen

1. Ga naar de module Persoon.
 2. Selecteer een toegevoegde organisatie in de lijst of klik op **Toevoegen** in de linkerbovenhoek om een organisatie toe te voegen en deze vervolgens te selecteren.
 3. Klik op **Importeren** om het paneel Importeren te openen en vink **Face** aan.
 4. Optioneel: Schakel **Verify by Device** in om te controleren of het gezichtsherkenningsapparaat dat in de client wordt beheerd, het gezicht op de foto kan herkennen.
 5. Klik op  om een bestand met gezichtsfoto's te selecteren.
-

 **Opmerking**

- De (map met) gezichtsfoto's moet in ZIP-formaat zijn.
 - Elk afbeeldingsbestand moet in JPG-formaat zijn en mag niet groter zijn dan 200 KB.
 - Elk afbeeldingsbestand moet de naam "Persoon ID_Naam" hebben. De persoon-ID moet dezelfde zijn als die van de geïmporteerde persoonsinformatie.
-

6. Klik op **Importeren** om het importeren te starten.
De voortgang en het resultaat van het importeren worden weergegeven.

14.3.3 Persoonsgegevens exporteren

Je kunt de gegevens van de toegevoegde personen exporteren naar een lokale pc als CSV/Excel-bestand.

Voordat u begint

- Controleer of je personen hebt toegevoegd aan een organisatie.
 - Zorg ervoor dat je de functie **Persoonsgegevens exporteren** hebt ingeschakeld om de knop **Exporteren** weer te geven. Zie [***Algemene parameters instellen***](#) voor meer informatie.
-

Stappen

1. Ga naar de module Persoon.
2. Optioneel: Selecteer een organisatie in de lijst.

Opmerking

Als je geen organisatie selecteert, worden alle gegevens van personen geëxporteerd.

3. Klik op **Exporteren**.
4. Voer ter verificatie de supergebruikersnaam en het wachtwoord in.
Het paneel Exporteren wordt weergegeven.
5. Vink **Person Information** aan als te exporteren inhoud.
6. Vink de gewenste items aan om te exporteren.
7. Klik op **Exporteren** om het geëxporteerde bestand in CSV/Excel op te slaan op je pc.

14.3.4 Afbeeldingen van personen exporteren

Je kunt gezichtsfoto's van de toegevoegde personen exporteren en op je pc opslaan.

Voordat u begint

- Zorg ervoor dat je personen en hun gezichtsfoto's hebt toegevoegd aan een organisatie.
- Zorg ervoor dat je de functie **Persoongegevens exporteren** hebt ingeschakeld om de knop **Exporteren** weer te geven. Zie [Algemene parameters instellen](#) voor meer informatie.

Stappen

1. Ga naar de module Persoon.
2. Optioneel: Selecteer een organisatie in de lijst.

Opmerking

De gezichtsfoto's van alle personen worden geëxporteerd als je geen organisatie selecteert.

3. Klik op **Exporteren** in de bovenste menubalk.
4. Voer ter verificatie de supergebruikersnaam en het wachtwoord in.
Het paneel Exporteren wordt weergegeven.
5. Vink **Face** aan als te exporteren inhoud.
6. Klik op **Exporteren** en stel een coderingsleutel in om het geëxporteerde bestand te versleutelen.

Opmerking

- Het geëxporteerde bestand is in ZIP-formaat.
 - De geëxporteerde gezichtsfoto krijgt de naam "Persoon ID_Naam_0" ("0" staat voor een gezicht met het volledige gezicht).
-

14.4 Persoonsgegevens ophalen uit toegangscontroleapparaat

Als het toegangscontroleapparaat geconfigureerd is met persoonsinformatie (inclusief persoonsgegevens, vingerafdruk en afgegeven kaartinformatie), kun je de persoonsinformatie ophalen uit het toegevoegde apparaat en importeren in de client voor verdere bewerkingen.

Stappen

Opmerking

- Als de naam van de persoon die op het apparaat is opgeslagen leeg is, wordt de naam van de persoon gevuld met het afgegeven kaartnummer na het importeren naar de client.
 - Personen zijn standaard **Mannelijk**.
 - Als het kaartnummer of de persoon-ID (werknemers-ID) die op het apparaat is opgeslagen al bestaat in de database van de client, wordt de persoon met dit kaartnummer of deze persoon-ID niet geïmporteerd naar de client.
-

1. Module **Persoon** invoeren.
 2. Selecteer een organisatie om de personen te importeren.
 3. Klik op **Verkrijgen van apparaat**.
 4. Selecteer een toegevoegd toegangscontroleapparaat of het registratiestation in de vervolgkeuzelijst.
-

Opmerking

Als je het aanmeldstation selecteert, moet je op **Aanmelden** klikken en het IP-adres, poortnummer, gebruikersnaam en wachtwoord van het apparaat invoeren.

5. Selecteer de **Ontvangstmodus**.
-

Opmerking

De verkrijgmodus verschilt per apparaat. Het toegangscontroletoestel ondersteunt het verkrijgen van de persoonsinformatie per werknemers-ID. Er kunnen maximaal 5 werknemers-ID's per keer worden opgegeven.

6. Klik op **Importeren** om het importeren van de persoonsinformatie naar de client te starten.
-

Opmerking

Er kunnen maximaal 2.000 personen en 5.000 kaarten worden geïmporteerd.

De persoonsinformatie, inclusief persoonsgegevens, vingerafdrukgegevens van de persoon (indien geconfigureerd) en de gekoppelde kaarten (indien geconfigureerd), worden geïmporteerd naar de geselecteerde organisatie.

14.5 Personen verhuizen naar een andere organisatie

Je kunt de toegevoegde personen naar een andere organisatie verplaatsen als dat nodig is.

Voordat u begint

- Zorg ervoor dat je minstens twee organisaties hebt toegevoegd.
- Zorg ervoor dat je persoonlijke informatie hebt geïmporteerd.

Stappen

1. Module **Persoon** invoeren.
2. Selecteer een organisatie in het linkerpaneel.
De personen onder de organisatie worden weergegeven in het rechterpaneel.
3. Selecteer de persoon die u wilt verplaatsen.
4. Klik op **Organisatie wijzigen**.
5. Selecteer de organisatie waarnaar u personen wilt verplaatsen.
6. Klik op **OK**.

14.6 Kaarten afgeven aan personen in batch

De client biedt een handige manier om kaarten uit te geven aan meerdere personen in een batch.

Stappen


1. Module **Persoon** invoeren.
2. Klik op **Kaarten batchgewijs uitgeven**.
Alle toegevoegde personen zonder uitgegeven kaart worden weergegeven in het rechterpaneel.
3. Optioneel: Voer sleutelwoorden (naam of persoon-ID) in het invoervak in om de persoon/personen te filteren die kaarten moeten uitgeven.
4. Optioneel: Klik op **Instellingen** om de kaartuitgifteparameters in te stellen. Raadpleeg [Een kaart uitgeven aan één persoon](#) voor meer informatie.
5. Klik op **Initialiseren** om het kaartregistratiestation of de kaartlezer te initialiseren en klaar te maken voor de uitgifte van kaarten.
6. Klik op de kolom **Kaartnummer** en voer het kaartnummer in.
 - Plaats de kaart op het kaartregistratiestation.
 - Veeg de kaart door de kaartlezer.
 - Voer het kaartnummer handmatig in en druk op de Enter-toets.De persoon (personen) op de lijst krijgt (krijgen) een kaart (kaarten).

14,7 Rapport Verlies

Als de persoon zijn/haar kaart kwijt is, kun je het verlies van de kaart melden zodat de bijbehorende toegangsautorisatie van de kaart inactief wordt.

Stappen

1. Module **Persoon** invoeren.

2. Selecteer de persoon voor wie je kaartverlies wilt melden en klik op **Bewerken** om het venster Persoon bewerken te openen.
3. Klik in het paneel **Credential** → **Kaart** op  op de toegevoegde kaart om deze kaart in te stellen als verloren kaart.
Na melding van kaartverlies wordt de toegangsbevoegdheid van deze kaart ongeldig en inactief. Een andere persoon die deze kaart krijgt, kan geen toegang krijgen tot de deuren door met deze verloren kaart te swipen.
4. Optioneel: Als de verloren kaart wordt gevonden, kun je op  klikken om het verlies te annuleren.
Na annulering van kaartverlies blijft de toegangsbevoegdheid van de persoon geldig en actief.
5. Als de verloren kaart is toegevoegd aan een toegangsgroep en de toegangsgroep al is toegepast op het apparaat, verschijnt er na het melden van kaartverlies of het annuleren van kaartverlies een venster met de melding dat je de wijzigingen moet toepassen op het apparaat. Na het toepassen op het apparaat kunnen deze wijzigingen van kracht worden op het apparaat.

14.8 Hulpbronstatistieken bekijken

Na het toepassen van personen en toegangscontrolegegevens (inclusief gezichten, kaarten en vingerafdrukken) op het apparaat, kun je de resourcestatistieken op de client en op het apparaat bekijken om te zien of de resources met succes zijn toegepast.

U hebt personen en referenties toegepast op het apparaat. Raadpleeg [Toegangsgroep instellen om toegangsrechten aan personen toe te wijzen](#) voor meer informatie.

Klik op **Personeelsbeheer** → **Hulpbronstatistieken** om het venster Hulpbronstatistieken te openen.

Afbeelding 14-5 Overzicht op client

Selecteer in **Overzicht op apparaat** een apparaat in de vervolgkeuzelijst en klik op **Telling** om apparaatbronnen te bekijken, inclusief personen, gezichten, kaarten en vingerafdrukken. Door de bronnen op de client en die op het apparaat te vergelijken, kunt u weten of de bronnen op de client zijn toegepast op het apparaat.

Afbeelding 14-6 Clientbronnen toegepast op apparaat

Opmerking

Deze functie moet worden ondersteund door het apparaat. Als het apparaat gezicht of vingerafdruk niet ondersteunt, verschijnt er een prompt in de rechterbenedenhoek van het bureaublad van de pc.

Hoofdstuk 15 Toegangscontrole

De module Toegangscontrole kan worden gebruikt voor toegangscontroleapparaten en video-intercomapparaten. Het biedt meerdere functies, waaronder configuratie van toegangsgroepen, video-intercom en andere geavanceerde functies.

Opmerking

De gebruiker met rechten voor de toegangscontrolemodule kan de toegangscontrolemodule openen en de toegangscontrole-instellingen configureren. Raadpleeg [***Gebruiker toevoegen***](#) voor het instellen van de gebruikersrechten voor de module Toegangsbeheer.

15.2 Schema en sjabloon configureren

Je kunt de sjabloon configureren inclusief vakantie- en wekschema. Na het instellen van de sjabloon kun je de geconfigureerde sjabloon overnemen voor toegangsgroepen bij het instellen van de toegangsgroepen, zodat de toegangsgroep van kracht wordt in de tijdsduur van de sjabloon.

Opmerking

Raadpleeg [***Toegangsgroep instellen om toegangsrechten aan personen toe te wijzen***](#) voor instellingen van toegangsgroepen.

15.2.1 Vakantie toevoegen

Je kunt vakantiedagen aanmaken en de dagen in de vakantie instellen, inclusief begindatum, einddatum en duur van de vakantie op één dag.

Stappen

Opmerking

Je kunt tot 64 vakantiedagen toevoegen aan het softwaresysteem.

1. Klik op **Toegangsbeheer** → **Rooster** → **Vakantie** om naar de Vakantie-pagina te gaan.
2. Klik op **Toevoegen** in het linkerpaneel.
3. Verzin een naam voor de feestdag.
4. Optioneel: Voer de beschrijvingen of enkele meldingen van deze vakantie in het vak Opmerking in.
5. Voeg een vakantieperiode toe aan de vakantielijst en configureer de vakantieperiode.






Opmerking

Er kunnen maximaal 16 vakantieperiodes aan één vakantie worden toegevoegd.

- 1) Klik op **Toevoegen** in het veld Vakantielijst.
 - 2) Sleep de cursor om de tijdsduur te tekenen, wat betekent dat in die tijdsduur de geconfigureerde toegangsgroep geactiveerd is.
-

Opmerking

Je kunt tot 8 tijdsduren instellen voor één vakantieperiode.

- 3) Optioneel: Voer de volgende bewerkingen uit om de tijdsduur te bewerken.
 - Beweeg de cursor naar de tijdsduur en sleep de tijdsduur op de tijdlijn balk naar de gewenste positie wanneer de cursor verandert in .
 - Klik op de tijdsduur en bewerk direct de begin-/eindtijd in het dialoogvenster dat verschijnt.
 - Beweeg de cursor naar het begin of het einde van de tijdsduur en sleep om de tijdsduur te verlengen of te verkorten wanneer de cursor verandert in .
 - 4) Optioneel: Selecteer de tijdsduur of tijdsduren die moeten worden verwijderd en klik vervolgens op  in de kolom **Bewerking** om de geselecteerde tijdsduur of tijdsduren te verwijderen.
 - 5) Optioneel: Klik op  in de kolom **Bewerking** om alle tijdsduren in de tijdbalk te wissen.
 - 6) Optioneel: Klik op  in de kolom **Werking** om deze toegevoegde vakantieperiode te verwijderen uit de vakantielijst.
6. Klik op **Opslaan**.

15.2.2 Sjabloon toevoegen

Sjabloon bevat weekschema en vakantie. U kunt een weekschema instellen en de tijdsduur van de toegangsmachtiging toewijzen aan verschillende personen of groepen. U kunt ook de toegevoegde vakantie(s) voor de sjabloon selecteren.

Stappen

Opmerking

Je kunt tot 255 sjablonen toevoegen in het softwaresysteem.

1. Klik op **Toegangsbeheer** → **Schema** → **Sjabloon** om de pagina Sjabloon te openen.
-

Opmerking

Er zijn twee standaardsjablonen: All-Day Authorized (Alle dagen toegestaan) en All-Day Denied (Alle dagen geweigerd), en deze kunnen niet bewerkt of verwijderd worden.

Gehele dag toegestaan

De toegangsautorisatie is geldig op elke dag van de week en heeft geen feestdagen.



Hele dag geweigerd

De toegangsautorisatie is ongeldig op elke dag van de week en heeft geen vakantie.

2. Klik op **Toevoegen** in het linkerpaneel om een nieuwe sjabloon te maken.
 3. Maak een naam voor de sjabloon.
 4. Voer de beschrijvingen of een melding van deze sjabloon in het vak Opmerking in.
 5. Bewerk het weekschema om het toe te passen op de sjabloon.
 - 1) Klik op het tabblad **Weekschema** in het onderste paneel.
 - 2) Selecteer een dag van de week en teken tijdsduur(en) op de tijdlijn balk.
-

Opmerking

Er kunnen maximaal 8 tijdsduren worden ingesteld voor elke dag in het weekschema.

- 3) Optioneel: Voer de volgende bewerkingen uit om de tijdsduur te bewerken.
 - Beweeg de cursor naar de tijdsduur en sleep de tijdsduur op de tijdlijn balk naar de gewenste positie wanneer de cursor verandert in .
 - Klik op de tijdsduur en bewerk direct de begin-/eindtijd in het dialoogvenster dat verschijnt.
 - Beweeg de cursor naar het begin of het einde van de tijdsduur en sleep om de tijdsduur te verlengen of te verkorten wanneer de cursor verandert in .
 - 4) Herhaal de twee bovenstaande stappen om meer tijdsduren te tekenen op de andere dagen van de week.
 6. Voeg een vakantie toe om deze toe te passen op de sjabloon.
-


Opmerking

Er kunnen maximaal 4 feestdagen worden toegevoegd aan één sjabloon.

- 1) Klik op het tabblad **Vakantie**.
 - 2) Selecteer een vakantie in de linkerlijst en deze wordt toegevoegd aan de geselecteerde lijst in het rechterpaneel.
 - 3) Optioneel: Klik op **Toevoegen** om een nieuwe vakantie toe te voegen.
-

Opmerking

Raadpleeg **Vakantie toevoegen** voor meer informatie over het toevoegen van een vakantie.

- 4) Optioneel: Selecteer een geselecteerde vakantie in de rechter lijst en klik op  om de geselecteerde vakantie te verwijderen, of klik op **Wissen** om alle geselecteerde vakanties in de rechter lijst te wissen.
 7. Klik op **Opslaan** om de instellingen op te slaan en het toevoegen van de sjabloon te voltooien.
-

15.3 Toegangsgroep instellen om toegangsrechten aan personen toe te wijzen

Nadat je de persoon hebt toegevoegd en de referenties van de persoon hebt geconfigureerd, kun je de toegangsgroepen maken om te definiëren welke persoon of personen toegang krijgen tot welke deur of deuren en vervolgens de toegangsgroep toepassen op het toegangscontroleapparaat om in werking te treden.

Voordat u begint

- Persoon toevoegen aan de klant.
- Voeg het toegangscontroleapparaat toe aan de client en groep toegangspunten. Raadpleeg **Groepsbeheer** voor meer informatie.
- Sjabloon toevoegen.

Stappen

Wanneer de instellingen van de toegangsgroepen gewijzigd zijn, moet u de toegangsgroepen opnieuw toepassen op de apparaten om van kracht te worden. De wijzigingen aan de toegangsgroep omvatten wijzigingen aan de sjabloon, de instellingen van de toegangsgroep, de instellingen van de toegangsgroep van de persoon en de gerelateerde details van de persoon (inclusief kaartnummer, vingerafdruk, gezichtsfoto, koppeling tussen kaartnummer en vingerafdruk, koppeling tussen kaartnummer en vingerafdruk, kaartwachtwoord, geldigheidsperiode van de kaart, enz.)

1. Klik op **Toegangsbeheer** → **Autorisatie** → **Toegangsgroep** om de interface Toegangsgroep te openen.
2. Klik op **Toevoegen** om het venster Toevoegen te openen.
3. Maak in het tekstveld **Naam** een naam aan voor de toegangsgroep zoals je wilt.
4. Selecteer een sjabloon voor de toegangsgroep.

Opmerking

Je moet de sjabloon configureren voordat je de toegangsgroepinstellingen configureert. Raadpleeg **Schema en sjabloon configureren** voor meer informatie.

5. Selecteer in de linker lijst van het veld Persoon selecteren de persoon (personen) waaraan u toegangsrechten wilt toekennen.
6. Selecteer in de linker lijst van het veld Toegangspunt selecteren deur(en), deurstation(s) of verdieping(en) waartoe de geselecteerde personen toegang moeten hebben.
7. Klik op **Opslaan**.
Je kunt de geselecteerde persoon (personen) en het (de) geselecteerde toegangspunt(en) bekijken aan de rechterkant van de interface.

Name	Person ID	Organization
Jane	2	New Organization
Mike	1	New Organization

Access Point	Group Name
Door1_Access control host	Access control host
Door2_Access control host	Access control host

Afbeelding 15-2 De geselecteerde persoon/personen en toegangspunt(en) weergeven

8. Nadat je de toegangsgroepen hebt toegevoegd, moet je ze toepassen op het toegangscontroleapparaat om van kracht te worden.
 - 1) Selecteer de toegangsgroep(en) die je wilt toepassen op het toegangscontroleapparaat.
 - 2) Klik op **Alles toepassen op Apparaten** om alle geselecteerde toegangsgroep(en) toe te passen op het toegangscontroletoestel of deurstation.
 - 3) Klik op **Alles toepassen op apparaten** of **Wijzigingen toepassen op apparaten**.

Alles toepassen op apparaten

Deze handeling wist alle bestaande toegangsgroepen van de geselecteerde apparaten en past vervolgens de nieuwe toegangsgroep toe op het apparaat.

Wijzigingen toepassen op apparaten

Deze handeling wist de bestaande toegangsgroepen van de geselecteerde apparaten niet en past alleen het gewijzigde deel van de geselecteerde toegangsgroep(en) toe op het apparaat/de apparaten.

- 4) Bekijk de status van het toepassen in de kolom Status of klik op **Status toepassen** om alle toegepaste toegangsgroepen te bekijken.

Opmerking

Je kunt **Alleen mislukkingen weergeven** aanvinken om de toepassingsresultaten te filteren.

De geselecteerde personen in de toegepaste toegangsgroepen hebben de autorisatie om de geselecteerde deuren/deurstations te betreden/verlaten met hun gekoppelde kaart(en) of vingerafdrukken.

9. Optioneel: Klik op  om de toegangsgroep indien nodig te bewerken.

 **Opmerking**

Als je de toegangsgegevens van de personen of andere gerelateerde informatie wijzigt, zie je de prompt **Toegangsgroep die moet worden toegepast** in de rechterhoek van de client. U kunt op de prompt klikken om de gewijzigde gegevens toe te passen op het apparaat. U kunt **Nu toepassen** of **Later toepassen** selecteren.

15.4 Toegangsgroep zoeken

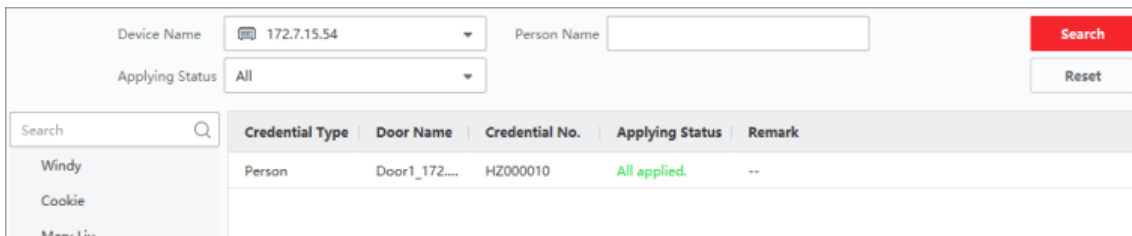
Na het instellen van de toegangsgroep en het toewijzen van de toegangsbevoegdheid aan personen, kun je de toegangsgroep zoeken waartoe de persoon behoort en andere gerelateerde informatie bekijken, zoals het toegangsnummer, het toegangsbewijstype, de aanvraagstatus, enz.

 **Opmerking**

Zorg ervoor dat u een toegangsgroep hebt ingesteld om toegangsautorisatie toe te wijzen aan bepaalde personen en dat u deze hebt toegepast. Raadpleeg [Toegangsgroep instellen om toegangsmachtiging toe te wijzen aan personen](#) voor meer informatie.

Klik op **Toegangsbeheer** → **Autorisatie** → **Zoeken**. Selecteer een apparaatnaam en stel de zoekvoorwaarde in (inclusief persoonsnaam en aanvraagstatus, optioneel) en klik vervolgens op **Zoeken**.

Je kunt de toegangsgroep bekijken waartoe de gezochte persoon behoort en andere informatie, zoals het type toegangsbewijs, deurnaam, toegangsbewijsnummer, aanvraagstatus, opmerking, enz.




Credential Type	Door Name	Credential No.	Applying Status	Remark
Person	Door1_172...	HZ000010	All applied.	--

Figuur 15-3 Zoektoegangsgroep

15.5 Geavanceerde functies configureren

U kunt de geavanceerde functies van toegangscontrole configureren om te voldoen aan enkele speciale vereisten in verschillende scènes, zoals multi-factor authenticatie, anti-passback, enz.

Opmerking

- Voor de kaartgerelateerde functies (het type toegangscontrolekaart/multifactorauthenticatie) worden alleen de kaart(en) met toegepaste toegangsgroep weergegeven bij het toevoegen van kaarten.
 - De geavanceerde functies moeten worden ondersteund door het apparaat.
 - Beweeg de cursor over de geavanceerde functie en klik vervolgens op  om de weer te geven geavanceerde functie(s) aan te passen.
-

15.5.1 Apparaatparameters configureren

Na het toevoegen van het toegangscontroleapparaat kun je de parameters configureren van het toegangscontroleapparaat (toegangscontroller), de toegangscontrolepunten (deur of vloer), de alarmingangen, de alarmuitgangen, de kaartlezers en de baancontroller.

Parameters configureren voor toegangscontroleapparaat

Nadat u het toegangscontroleapparaat hebt toegevoegd, kunt u de parameters configureren, waaronder het overlappen van gebruikersinformatie op de foto, het uploaden van foto's na het vastleggen, het opslaan van vastgelegde foto's, enz.


Voordat u begint

Apparaat voor toegangscontrole toevoegen aan de client.

Stappen

1. Klik op **Toegangsbeheer** → **Geavanceerde functie** → **Apparaatparameter**.

Opmerking

Als u de Device Parameter niet kunt vinden in de lijst Geavanceerde functie, plaatst u de cursor op de Geavanceerde functie en klikt u vervolgens op  om de weer te geven Device Parameter te selecteren.

2. Selecteer een toegangsapparaat om de parameters ervan op de rechterpagina weer te geven.
3. Zet de schakelaar op ON om de overeenkomstige functies in te schakelen.

Opmerking

- De weergegeven parameters kunnen verschillen voor verschillende toegangscontroleapparaten.
 - Sommige van de volgende parameters staan niet op de pagina Basisinformatie. Klik op **Meer** om de parameters te bewerken.
-

RS-485 Comm. Redundantie

Je moet deze functie inschakelen als je de RS-485 kaartlezer redundant bedraadt naar de toegangscontrole.

Gezicht gedetecteerd weergeven

Gezichtsfoto weergeven bij verificatie.

Kaartnummer weergeven

De kaartinformatie weergeven bij het verifiëren.

Persoonsgegevens weergeven

Geef de persoonsinformatie weer bij het verifiëren.

Info over persoon op foto weergeven

Geef de persoonsinformatie op de vastgelegde foto weer.

Stemboodschap

Als je deze functie inschakelt, wordt de gesproken prompt ingeschakeld op het apparaat. U kunt de gesproken instructies horen wanneer u het apparaat bedient.

Foto uploaden. Na gekoppelde opname

Upload de foto's die door de gekoppelde camera zijn gemaakt automatisch naar het systeem.

Foto opslaan. Na gekoppelde opname

Als u deze functie inschakelt, kunt u de foto die door de gekoppelde camera is gemaakt, opslaan op het apparaat.

Druk op om het kaartnummer in te voeren

Als u deze functie inschakelt, kunt u het kaartnummer invoeren door op de toets te drukken.

Wi-Fi-sonde

Als je deze functie inschakelt, kan het apparaat het MAC-adres van de omringende communicatieapparaten peilen en het MAC-adres uploaden naar het systeem. Als het MAC-adres overeenkomt met het gespecificeerde MAC-adres, kan het systeem bepaalde koppelingsacties activeren.

3G/4G

Als u deze functie inschakelt, kan het apparaat communiceren in een 3G/4G-netwerk.

NFC Anti-Cloning

Als u deze functie inschakelt, kunt u de gekloonde kaart niet gebruiken voor authenticatie en de beveiliging verder verbeteren.

4. Klik op **OK**.
5. Optioneel: Klik op **Kopiëren naar en** selecteer vervolgens het (de) toegangscontroleapparaat (-apparaten) om de parameters op de pagina te kopiëren naar het (de) geselecteerde apparaat (apparaten).


Parameters configureren voor deur/lift

Nadat je het toegangscontroleapparaat hebt toegevoegd, kun je de parameters van het toegangspunt (deur of vloer) configureren.

Voordat u begint

Apparaat voor toegangscontrole toevoegen aan de client.

Stappen

1. Klik op **Toegangsbeheer** → **Geavanceerde functie** → **Apparaatparameter**.
2. Selecteer een toegangscontroleapparaat in het linkerpaneel en klik dan op  om de deuren of verdiepingen van het geselecteerde apparaat weer te geven.
3. Selecteer een deur of vloer om de parameters ervan op de rechterpagina weer te geven.
4. Bewerk de deur- of vloerparameters.

Opmerking

- De weergegeven parameters kunnen verschillen voor verschillende toegangscontroleapparaten.
 - Sommige van de volgende parameters staan niet op de pagina Basisinformatie. Klik op **Meer** om de parameters te bewerken.
-

Naam

Bewerk de naam van de kaartlezer naar wens.

Deurcontact

Je kunt de deursensor instellen op gesloten blijven of open blijven. Meestal is dit gesloten blijven.

Type knop afsluiten

Je kunt de afsluitknop instellen als gesloten blijven of open blijven. Meestal is dit open blijven.

Tijd deur op slot

Na het vegen van de normale kaart en de relaisactie begint de timer voor het vergrendelen

van de deur te werken.

Verlengde Open Looptijd

Het deurcontact kan met de juiste vertraging worden ingeschakeld nadat de persoon met uitgebreide toegangsbehoeften zijn/haar kaart heeft gebruikt.

Time-out alarm deur open

Het alarm kan worden geactiveerd als de deur niet is gesloten in een geconfigureerde tijdsperiode. Als dit is ingesteld op 0, wordt er geen alarm geactiveerd.

Deur vergrendelen bij gesloten deur

De deur kan worden vergrendeld zodra deze is gesloten, zelfs als de **Deur Vergrendeld Tijd** niet is bereikt.

Code dwang

De deur kan worden geopend door de code in te voeren wanneer er sprake is van dwang. Tegelijkertijd kan de klant de noodsituatie melden.

Super wachtwoord

De specifieke persoon kan de deur openen door het superwachtwoord in te voeren.

Code Ontslag

Maak een ontslagcode waarmee de zoemer van de kaartlezer kan worden gestopt (door de ontslagcode in te voeren op het toetsenbord).



Opmerking

- De dwangcode, supercode en ontslagcode moeten verschillend zijn.
- De dwangcode, het superwachtwoord en de ontslagcode moeten verschillen van het authenticatiewachtwoord.
- De lengte van de dwangcode, het superwachtwoord en de ontslagcode is afhankelijk van het apparaat en moet meestal 4 tot 8 cijfers bevatten.

5. Klik op **OK**.

6. Optioneel: Klik op **Kopiëren naar** en selecteer vervolgens de deur/vloer(en) om de parameters op de pagina te kopiëren naar de geselecteerde deur/vloer(en).



Opmerking

De instellingen voor de statusduur van de deur of verdieping worden ook gekopieerd naar de geselecteerde deur/verdieping(en).

Parameters voor kaartlezer configureren


Nadat je het toegangscontroleapparaat hebt toegevoegd, kun je de parameters van de kaartlezer

configureren.

Voordat u begint

Apparaat voor toegangscontrole toevoegen aan de client.

Stappen

1. Klik op **Toegangsbeheer** → **Geavanceerde functie** → **Apparaatparameter**.
2. Klik in de apparatenlijst aan de linkerkant op  om de deur uit te vouwen, selecteer een kaartlezer en je kunt de parameters van de kaartlezer aan de rechterkant bewerken.
3. Bewerk de basisparameters van de kaartlezer op de pagina Basisgegevens.

Opmerking

- De weergegeven parameters kunnen verschillen voor verschillende toegangscontroleapparaten. Hieronder volgt een deel van de parameters. Raadpleeg de gebruikershandleiding van het apparaat voor meer informatie.
 - Sommige van de volgende parameters staan niet op de pagina Basisinformatie. Klik op **Meer** om de parameters te bewerken.
-

Naam

Bewerk de naam van de kaartlezer naar wens.

OK LED Polariteit/fout LED Polariteit/zoemer Polariteit

Stel de OK LED Polariteit/Error LED Polariteit/Buzzer LED Polariteit van de hoofdkaart in volgens de parameters van de kaartlezer. Over het algemeen worden de standaardinstellingen gebruikt.

Minimaal interval tussen kaartwissels

Als het interval tussen het wisselen van dezelfde kaart kleiner is dan de ingestelde waarde, is het wisselen van de kaart ongeldig. Je kunt dit instellen van 0 tot 255.

Max. Interval bij invoeren PWD

Wanneer u het wachtwoord invoert op de kaartlezer en het interval tussen het indrukken van twee cijfers groter is dan de ingestelde waarde, worden de cijfers die u eerder hebt ingedrukt automatisch gewist.

Alarm van Max. Mislukte pogingen

Inschakelen om een alarm te melden wanneer de kaartleespogingen de ingestelde waarde bereiken.

Max. Tijden van kaartstoring

Stel de max. faalpogingen in voor het lezen van de kaart.

Detectie van sabotage

Schakel de anti-tamperdetectie voor de kaartlezer in.

Communiceer met Regelaar Elke

Als de toegangscontrole langer dan de ingestelde tijd geen verbinding kan maken met de kaartlezer, zal de kaartlezer automatisch offline gaan.

Zoemende tijd

Stel de zoemtijd van de kaartlezer in. De beschikbare tijd loopt van 0 tot 5.999s. 0 staat voor continu zoemen.

Kaartlezer Type/Kaartlezer Beschrijving

Krijg kaartlezer type en beschrijving. Ze zijn alleen-lezen.

Vingerafdrukherkenningsniveau

Selecteer het vingerafdrukherkenningsniveau in de vervolgkeuzelijst.

Standaard Authenticatiemodus kaartlezer

De standaard verificatiemodus voor kaartlezers weergeven.

Vingerafdrukcapaciteit

Bekijk het maximum aantal beschikbare vingerafdrukken.

Bestaand vingerafdruknummer

Het aantal bestaande vingerafdrukken op het apparaat weergeven.

Score

Het apparaat zal het vastgelegde beeld een score geven op basis van de yawhoek, pitchhoek en pupilafstand. Als de score lager is dan de geconfigureerde waarde, zal de gezichtsherkenning mislukken.

Time-outwaarde gezichtsherkenning

Als de herkenningstijd langer is dan de geconfigureerde tijd, zal het apparaat je eraan herinneren.

Interval gezichtsherkenning

Het tijdsinterval tussen twee ononderbroken gezichtsherkenningen bij authenticatie. Standaard is dit 2s.

Gezicht 1:1 matchingsdrempel

Stel de overeenstemmingsdrempel in bij authenticatie via de 1:1 overeenstemmingsmodus. Hoe groter de waarde, hoe kleiner het percentage fout-acceptatie en hoe groter het percentage fout-afwijzing bij authenticatie.

1:N Beveiligingsniveau

Stel het overeenstemmingsbeveiligingsniveau in bij verificatie via de 1:N overeenstemmingsmodus. Hoe groter de waarde, hoe kleiner het percentage valse aanvaardingen en hoe groter het percentage valse weigeringen bij verificatie.

Live gezichtsdetectie

De functie voor het herkennen van levende gezichten in- of uitschakelen. Als de functie is

ingeschakeld, kan het apparaat herkennen of de persoon in leven is of niet.

Live gezichtsdetectie Beveiligingsniveau

Na het inschakelen van de functie Live gezichtsdetectie, kunt u het overeenkomende beveiligingsniveau instellen bij het uitvoeren van live gezichtsverificatie.

Max. Mislukte pogingen voor gezichtsaut.

Stel het maximum aantal mislukte pogingen voor live gezichtsdetectie in. Het systeem zal het gezicht van de gebruiker voor 5 minuten vergrendelen als de live gezichtsdetectie voor meer dan de geconfigureerde pogingen mislukt. Dezelfde gebruiker kan zich niet binnen 5 minuten authenticeren via het nepgezicht. Binnen de 5 minuten kan de gebruiker zich twee keer continu authenticeren via het echte gezicht om te ontgrendelen.

Authenticatie slot mislukt Gezicht

Na het inschakelen van de functie Live gezichtsdetectie zal het systeem het gezicht van de gebruiker 5 minuten lang vergrendelen als de live gezichtsdetectie meer dan de geconfigureerde pogingen mislukt. Dezelfde gebruiker kan zich niet binnen 5 minuten authenticeren via het nepgezicht. Binnen de 5 minuten kan de gebruiker zich twee keer continu authenticeren via het echte gezicht om te ontgrendelen.

Toepassingsmodus

U kunt binnen- of andere toepassingsmodi selecteren op basis van de werkelijke omgeving.

4. Klik op **OK**.

5. Optioneel: Klik op **Kopiëren naar en** selecteer vervolgens de kaartlezer(s) om de parameters op de pagina te kopiëren naar de geselecteerde kaartlezer(s).

Parameters voor alarmingang configureren

Nadat je het toegangscontroleapparaat hebt toegevoegd, kun je de parameters voor de alarmingangen configureren.


Voordat u begint

Voeg het toegangscontroleapparaat toe aan de client en zorg ervoor dat het apparaat alarminvoer ondersteunt.

Stappen

Opmerking

Als de alarmingang ingeschakeld is, kun je de parameters niet wijzigen. Schakel hem eerst uit.

1. Klik op **Toegangsbeheer** → **Geavanceerde functie** → **Apparaatparameter** .
2. Klik in de apparatenlijst aan de linkerkant op  om de deur uit te vouwen, selecteer een alarmingang en je kunt de parameters van de alarmingang aan de rechterkant bewerken.
3. Stel de parameters voor de alarmingang in.

Naam

Bewerk de naam van de alarmingang naar wens.

Type detector

Het detectortype van de alarmingang.

Type zone

Stel het zonetype in voor de alarmingang.

Gevoeligheid

Alleen wanneer de duur van het signaal dat door de detector wordt gedetecteerd de ingestelde tijd bereikt, wordt de alarmingang geactiveerd. Bijvoorbeeld, je hebt de gevoeligheid ingesteld op 10ms, alleen wanneer de duur van het door de detector gedetecteerde signaal 10ms bereikt, wordt deze alarmingang geactiveerd.

Trigger Alarm Uitgang

Selecteer de alarmuitgang(en) die moet(en) worden geactiveerd.

4. Klik op **OK**.
5. Optioneel: Klik op de schakelaar in de rechterbovenhoek om de alarmingang in of uit te schakelen.


Parameters voor alarmuitgang configureren

Na het toevoegen van het toegangscontroleapparaat kun je, als het apparaat is gekoppeld aan alarmuitgangen, de parameters configureren.

Voordat u begint

Voeg het toegangscontroleapparaat toe aan de client en zorg ervoor dat het apparaat alarmuitvoer ondersteunt.

Stappen

1. Klik op **Toegangscontrole** → **Geavanceerde functie** → **Apparaatparameter om de configuratiepagina voor de toegangscontroleparameters te openen**.
2. Klik in de apparatenlijst aan de linkerkant op  om de deur uit te vouwen, selecteer een alarmingang en je kunt de parameters van de alarmingang aan de rechterkant bewerken.
3. Stel de parameters voor de alarmuitgang in.

Naam

Bewerk de naam van de kaartlezer naar wens.

Alarm Uitgang Actieve Tijd

Hoe lang de alarmuitgang duurt na activering.

4. Klik op **OK**.
5. Optioneel: Zet de schakelaar rechtsboven op **ON** om de alarmuitgang te activeren.

Parameters voor rijstrookcontroller configureren

Nadat je de rijstrookcontroller aan de client hebt toegevoegd, kun je de parameters voor het

passeren van de rijstrook configureren.

Voordat u begint

Apparaat voor toegangscontrole toevoegen aan de client.

Stappen

1. Klik op **Toegangsbeheer** → **Geavanceerde functie** → **Apparaatparameter** om de pagina Parameterinstellingen te openen.
2. Selecteer een baancontroller in de apparatenlijst aan de linkerkant en bewerk de parameters van de baancontroller aan de rechterkant.
3. Bewerk de parameters.

Passerende modus

Selecteer de controller die de barrièrestatus van het apparaat regelt.

- Als u **Volgens de DIP-instellingen van de rijstrookcontroller** selecteert, volgt het apparaat de DIP-instellingen van de rijstrookcontroller om de slagboom te besturen. De instellingen in de software zijn dan ongeldig.
- Als u **Volgens de instellingen van de hoofdcontroller** selecteert, volgt het apparaat de instellingen van de software om de slagboom te besturen. De DIP-instellingen van de rijstrookcontroller zijn dan ongeldig.

Authenticatie met vrije doorgang

Als je deze functie inschakelt en de barrièremodus van zowel de ingang als de uitgang op Open blijven staat, moeten de voetgangers zich elke keer dat ze de rijstrook passeren legitimeren. Anders gaat er een alarm af.

Snelheid openen/sluiten barrière

Stel de openings- en sluitsnelheid van de slagboom in. U kunt kiezen uit 1 tot 10. Hoe groter de waarde, hoe sneller de snelheid.

Opmerking

De aanbevolen waarde is 6.

Hoorbare prompt duur

Instellen hoe lang het geluid duurt dat wordt afgespeeld wanneer een alarm afgaat .

Opmerking

0 verwijst naar het alarmgeluid dat wordt afgespeeld tot het alarm wordt beëindigd.

Temperatuureenheid

Selecteer de temperatuureenheid die wordt weergegeven in de apparaatstatus.

4. Klik op **OK**.

15.5.2 Resterende vergrendeld/ontgrendeld configureren

Je kunt de status van de deur instellen als ontgrendeld of vergrendeld en de liftbesturing instellen als vrij en gecontroleerd. Je kunt bijvoorbeeld instellen dat de deur vergrendeld blijft in de vakantie en dat de deur ontgrendeld blijft in de opgegeven periode van de werkdag.

Voordat u begint

Voeg de toegangscontroleapparaten toe aan het systeem.

Stappen

1. Klik op **Toegangsbeheer** → **Geavanceerde functie** → **Vergrendeld/ontgrendeld blijven** om naar de pagina Vergrendeld/ontgrendeld blijven te gaan.
2. Selecteer de deur- of liftcontroller die geconfigureerd moet worden op het linkerpaneel.
3. Om de status van de deur- of liftbesturing tijdens de werkdag in te stellen, klik je op **Weekschema** en voer je de volgende handelingen uit.

- 1) Klik voor de deur op **Blijven ontgrendeld**, **Blijven vergrendeld**, **Inductieve modus** of **Barrièrevrije modus**.



Opmerking

- **Inductieve modus:** Het openen en sluiten van de deur wordt geactiveerd door infrarood inductie van het menselijk lichaam.
 - **Barrièrevrije modus:** Wanneer een groot aantal mensen de deur moet passeren, blijft de deur open (zonder frequente authenticatie) als de persoon- en ID-vergelijking slaagt. Alleen als de persoon- en ID-vergelijking mislukt, wordt de deur gesloten.
 - Inductieve modus en barrièrevrije modus moeten worden ondersteund door het apparaat.
-

- 2) Klik voor de liftbesturing op **Vrij** of **Bestuurd**.
- 3) Sleep de cursor om de tijdsduur te tekenen, wat betekent dat in die tijdsduur de geconfigureerde toegangsgroep geactiveerd is.

Opmerking

Er kunnen maximaal 8 tijdsduren worden ingesteld voor elke dag in het weekschema.

- 4) Optioneel: Voer de volgende bewerkingen uit om de tijdsduur te bewerken.
 - Beweeg de cursor naar de tijdsduur en sleep de tijdsduur op de tijdlijn balk naar de gewenste positie wanneer de cursor verandert in  .
 - Klik op de tijdsduur en bewerk direct de begin-/eindtijd in het dialoogvenster dat verschijnt.
 - Beweeg de cursor naar het begin of het einde van de tijdsduur en sleep om de tijdsduur te verlengen of te verkorten wanneer de cursor verandert in  .

- 5) Klik op **Opslaan**.






Verwante operaties

Kopiëren naar hele week	Selecteer een tijdsduur op de tijdbalk en klik op Kopiëren naar hele week om alle tijdsduurinstellingen op deze tijdbalk naar andere weekdays te kopiëren.
Geselecteerd verwijderen	Selecteer een duur op de tijdbalk en klik op Geselecteerde verwijderen om deze duur te verwijderen.
Duidelijk	Klik op Wissen om alle duurinstellingen in het weekschema te wissen.

4. Om de deurstatus tijdens de vakantie in te stellen, klik je op **Vakantie** en voer je de volgende handelingen uit.
- 1) Klik op **Blijven ontgrendeld, Blijven vergrendeld, Inductieve modus** of **Barrièrevrije modus**.
 - 2) Klik op **Toevoegen**.
 - 3) Voer de begindatum en einddatum in.
 - 4) Sleep de cursor om de tijdsduur te tekenen, wat betekent dat in die tijdsduur de geconfigureerde toegangsgroep geactiveerd is.

 **Opmerking**

Je kunt tot 8 tijdsduren instellen voor één vakantieperiode.

- 5) Voer de volgende bewerkingen uit om de tijdsduur te bewerken.
 - Beweeg de cursor naar de tijdsduur en sleep de tijdsduur op de tijdlijn balk naar de gewenste positie wanneer de cursor verandert in .
 - Klik op de tijdsduur en bewerk direct de begin-/eindtijd in het dialoogvenster dat verschijnt.
 - Beweeg de cursor naar het begin of het einde van de tijdsduur en sleep om de tijdsduur te verlengen of te verkorten wanneer de cursor verandert in .
 - 6) Optioneel: Selecteer de tijdsduur of tijdsduren die moeten worden verwijderd en klik vervolgens op  in de kolom **Bewerking** om de geselecteerde tijdsduur of tijdsduren te verwijderen.
 - 7) Optioneel: Klik op  in de kolom **Bewerking** om alle tijdsduur(en) in de tijdbalk te wissen.
 - 8) Optioneel: Klik op  in de kolom **Werking** om deze toegevoegde vakantieperiode te verwijderen uit de vakantielijst.
 - 9) Klik op **Opslaan**.
5. Optioneel: Klik op **Kopiëren om** de deurstatusinstellingen van deze deur te kopiëren naar andere deur(en).

15.5.3 Multi-Factor Authenticatie configureren

Je kunt de personen per groep beheren en de authenticatie instellen voor meerdere personen van één toegangscontrolepunt (deur).

Voordat u begint

Stel een toegangsgroep in en pas de toegangsgroep toe op het toegangscontroleapparaat.

Raadpleeg **Toegangsgroep instellen om toegangsautorisatie toe te wijzen aan personen** voor meer informatie.

Voer deze taak uit als je verificaties wilt instellen voor meerdere kaarten van één toegangscontrolepunt (deur).

Stappen

1. Klik op **Toegangsbeheer** → **Geavanceerde functie** → **Multi-Factor Auth**.
2. Selecteer een toegangscontroleapparaat in de apparatenlijst in het linkerpaneel.
3. Voeg een persoon/kaartgroep toe voor het toegangscontroleapparaat.
 - 1) Klik op **Toevoegen** in het rechterpaneel.
 - 2) Maak naar wens een naam aan voor de groep.
 - 3) Geef de begin- en eindtijd op van de effectieve periode voor de persoon/kaartgroep.
 - 4) Selecteer leden en kaart(en) in de lijst Beschikbaar en de geselecteerde leden en kaart(en) worden toegevoegd aan de lijst Geselecteerd.

Opmerking

Zorg ervoor dat je de persoon een kaart geeft.

Zorg ervoor dat je de toegangsgroep hebt ingesteld en de toegangsgroep met succes hebt toegepast op het toegangscontroleapparaat.

- 5) Klik op **Opslaan**.
 - 6) Optioneel: Selecteer de persoon/kaartgroep(en) en klik op **Verwijderen** om deze te verwijderen.
 - 7) Optioneel: Selecteer de persoon/kaartgroep(en) en klik vervolgens op **Toepassen** om de toegangsgroep die niet eerder is toegepast opnieuw toe te passen op het toegangscontroleapparaat.
4. Selecteer een toegangscontrolepunt (deur) van het geselecteerde apparaat op het linkerpaneel.
 5. Voer het maximale interval in bij het invoeren van het wachtwoord.
 6. Voeg een authenticatiegroep toe voor het geselecteerde toegangscontrolepunt.
 - 1) Klik op **Toevoegen** in het paneel Authenticatiegroepen.
 - 2) Selecteer een geconfigureerde sjabloon als authenticatiesjabloon in de vervolgkeuzelijst.

Opmerking

Raadpleeg **Schema en sjabloon configureren** voor het instellen van de sjabloon.

- 3) Selecteer het verificatietype als **Lokale verificatie**, **Lokale verificatie en deur op afstand openen** of **Lokale verificatie en superwachtwoord** uit de vervolgkeuzelijst.

Lokale verificatie

Authenticatie door het toegangscontroleapparaat.

Lokale verificatie en deur op afstand openen

Authenticatie door het toegangscontroleapparaat en door de klant. Als de persoon met de kaart op het apparaat veegt, verschijnt er een venster. Je kunt de deur ontgrendelen via de

client.

Afbeelding 15-4 Deur op afstand openen

Opmerking

Je kunt **Offline Authenticatie** aanvinken om de superwachtwoordverificatie in te schakelen wanneer de verbinding tussen het toegangscontroleapparaat en de client verbroken is.

Lokale verificatie en superwachtwoord

Authenticatie door het toegangscontroleapparaat en door het superwachtwoord.

- 4) Selecteer de toegevoegde persoon/kaartgroep in de linkerlijst hieronder en deze wordt toegevoegd aan de lijst Geselecteerd rechts als verificatiegroep.
 - 5) Klik op de toegevoegde authenticatiegroep in de rechter lijst om de authenticatietijden in te stellen in de kolom Auth Times.
-

Opmerking

- De authenticatietijden moeten groter zijn dan 0 en kleiner dan de toegevoegde hoeveelheid personeel in de personeelsgroep.
 - De maximale waarde van verificatietijden is 16.
-

- 6) Klik op **Opslaan**.
-

Opmerking

- Voor elk toegangscontrolepunt (deur) kunnen tot vier authenticatiegroepen worden toegevoegd.
 - Voor de authenticatiegroep waarvan het authenticatietype **Lokale Authenticatie is**, kunnen maximaal 8 personen-/kaartgroepen aan de authenticatiegroep worden toegevoegd.
 - Voor de authenticatiegroep waarvan het authenticatietype **Lokale Authenticatie en Superwachtwoord** of **Lokale Authenticatie en Deur Op Afstand Openen** is, kunnen tot 7 personen-/kaartgroepen worden toegevoegd aan de authenticatiegroep.
-

7. Klik op **Opslaan**.

15.5.4 Aangepaste Wiegand-regel configureren

Gebaseerd op de kennis van het uploaden van regels voor de derde partij Wiegand, kun je meerdere aangepaste Wiegand regels instellen om te communiceren tussen het apparaat en de derde partij kaartlezers.

Voordat u begint

Sluit de kaartlezers van derden aan op het apparaat.

Stappen

Opmerking

- Standaard schakelt het apparaat de aangepaste wiegand functie uit. Als het apparaat de aangepaste Wiegand functie inschakelt, zullen alle wiegand interfaces in het apparaat het aangepaste wiegand protocol gebruiken.
 - Er kunnen maximaal 5 aangepaste Wiegands worden ingesteld.
 - Zie Aangepaste Wiegand [regelbeschrijvingen](#) voor meer informatie over de aangepaste Wiegand.
-

1. Klik op **Toegangsbeheer** → **Geavanceerde functie** → **Aangepaste Wiegand** om de pagina Aangepaste Wiegand te openen.
 2. Selecteer links een aangepaste Wiegand.
 3. Maak een Wiegand-naam aan.
-

Opmerking

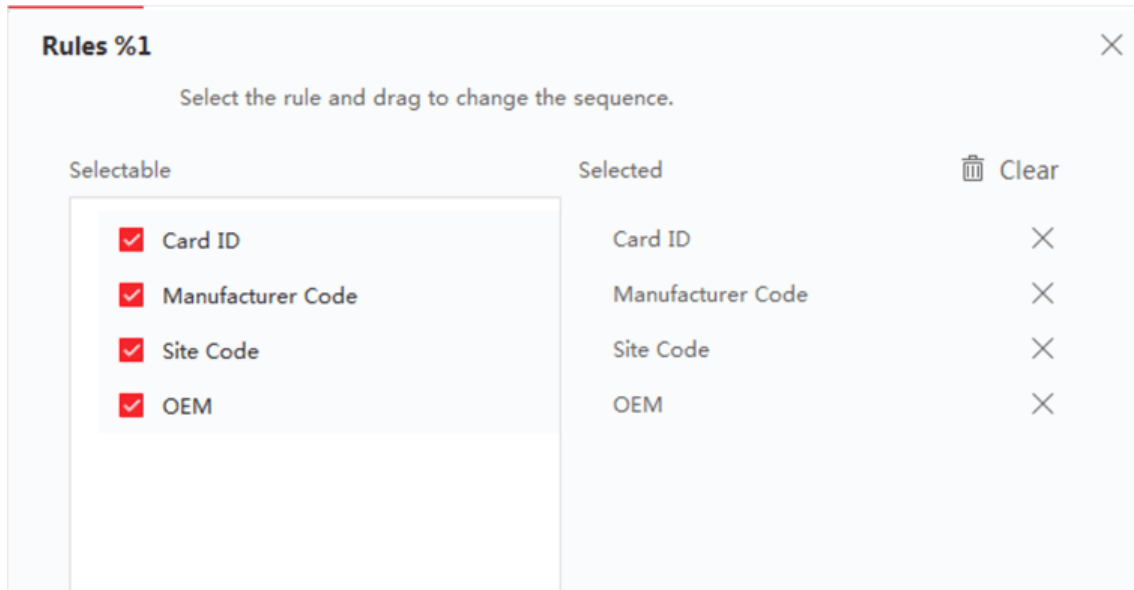
Er zijn maximaal 32 tekens toegestaan in de aangepaste Wiegand-naam.

4. Klik op **Select Device (Apparaat selecteren)** om het toegangscontroleapparaat te selecteren voor het instellen van de aangepaste wiegand.
 5. Stel de pariteitsmodus in volgens de eigenschap van de kaartlezer van derden.
-

Opmerking

- De totale lengte mag maximaal 80 bits bedragen.
 - De oneven pariteitsbeginbit, de oneven pariteitslengte, de even pariteitsbeginbit en de even pariteitslengte variëren van 1 tot 80 bit.
 - De startbit van de kaart-ID, de fabrikantcode, de sitecode en de OEM moet tussen 1 en 80 bit liggen.
-

6. Stel de uitgangstransformatieregel in.
 - 1) Klik op **Regel instellen** om het venster Regels voor uitvoertransformatie instellen te openen.



Figuur 15-5 Uitvoer transformatieregel instellen

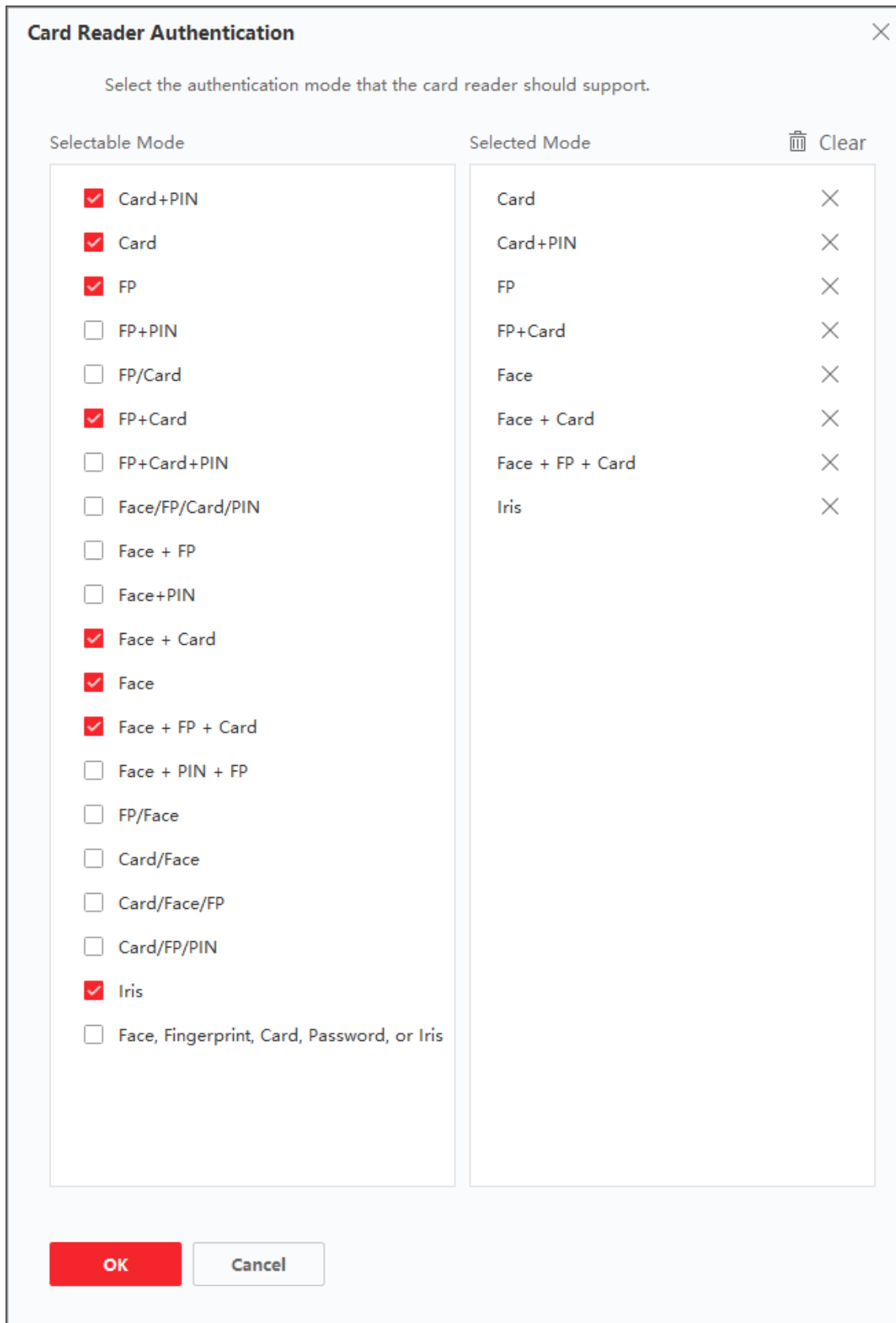
- 2) Selecteer regels in de linker lijst.
De geselecteerde regels worden toegevoegd aan de rechter lijst.
- 3) Optioneel: Versleep de regels om de regelvolgorde te wijzigen.
- 4) Klik op **OK**.
- 5) Stel op het tabblad Aangepaste Wiegand de startbit, lengte en het decimale cijfer van de regel in.
7. Klik op **Opslaan**.

15.5.5 Kaartlezerauthenticatiemodus en -schema configureren

Je kunt de passeerregels voor de kaartlezer van het toegangscontrolesysteem instellen volgens je eigen behoeften.

Stappen

1. Klik op **Toegangsbeheer** → **Geavanceerde functie** → **Authenticatie om** de configuratiepagina voor de authenticatiemodus te openen.
2. Selecteer links een kaartlezer om te configureren.
3. Stel de verificatiemodus van de kaartlezer in.
 - 1) Klik op **Configuratie**.

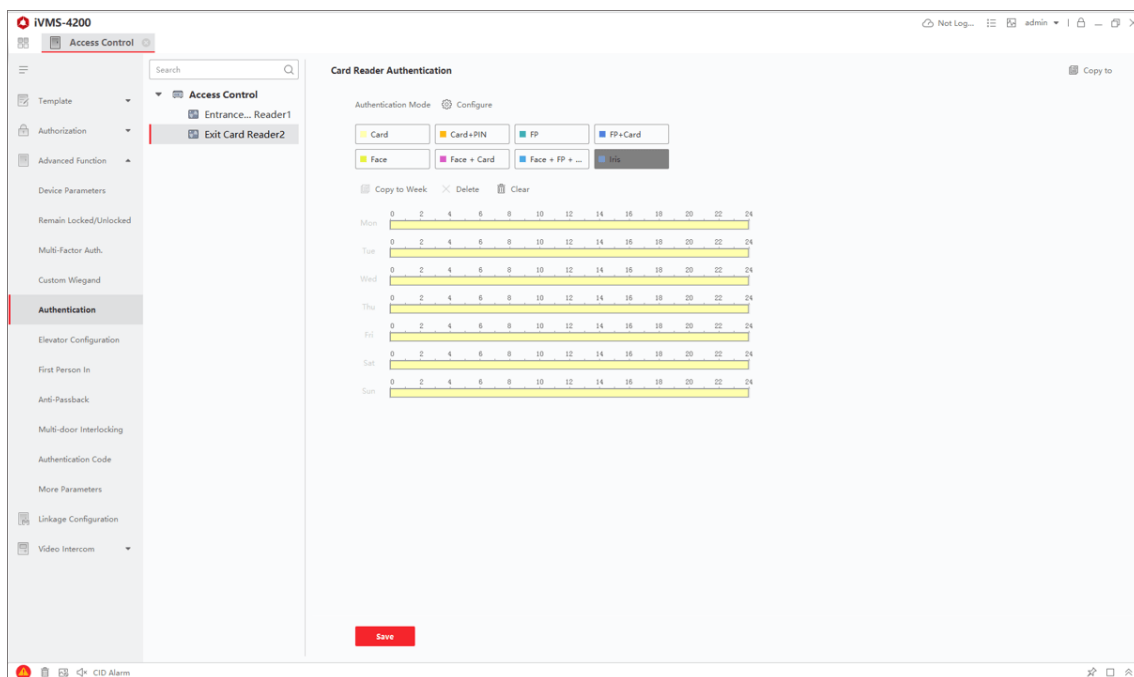


Figuur 15-6 Authenticatiemodus kaartlezer selecteren

Opmerking

PIN verwijst naar de PIN-code die is ingesteld om de deur te openen. Raadpleeg [Informatie over toegangscontrole configureren](#).

- 2) Vink de modi aan in de lijst Beschikbare modi en ze worden toegevoegd aan de lijst met geselecteerde modi.
- 3) Klik op **OK**.
Na het selecteren van de modi worden de geselecteerde modi weergegeven als pictogrammen met verschillende kleuren.
4. Klik op het pictogram om een kaartlezerauthenticatiemodus te selecteren en sleep de cursor om een kleurenbalk op het schema te tekenen, wat betekent dat in die periode de kaartlezerauthenticatie geldig is.
5. Herhaal de bovenstaande stap om andere tijdsperioden in te stellen.



Figuur 15-7 Authenticatiemodi instellen voor kaartlezers

6. Optioneel: Selecteer een geconfigureerde dag en klik op **Kopiëren naar week** om dezelfde instellingen naar de hele week te kopiëren.
7. Optioneel: Klik op **Kopiëren om** de instellingen naar andere kaartlezers te kopiëren.
8. Klik op **Opslaan**.

15.5.6 De modus persoonsauthenticatie configureren

Je kunt de regels voor het doorgeven van personen aan het gespecificeerde toegangscontroleapparaat instellen op basis van je werkelijke behoeften.

Voordat u begint

- Voeg het toegangscontroleapparaat toe aan de client en zorg ervoor dat het toegangscontroleapparaat de functie voor persoonsverificatie ondersteunt.
- Voeg persoon toe en wijs toegangsrechten toe aan ontworpen persoon. Raadpleeg **Persoonsbeheer** en **Toegangsgroep instellen om toegangsrechten aan personen toe** te wijzen voor meer informatie.

Stappen

1. Klik op **Toegangsbeheer** → **Geavanceerde functie** → **Authenticatie**.
2. Selecteer een toegangscontroleapparaat (dat de functie van persoonsauthenticatie ondersteunt) op het linkerpaneel om de pagina Modus persoonsauthenticatie te openen.
3. Klik op **Toevoegen** om het venster Toevoegen te openen.
4. Selecteer de persoon (personen) die geconfigureerd moet(en) worden in het linkerpaneel. De geselecteerde persoon/personen wordt/worden toegevoegd aan het rechterpaneel.
5. Selecteer de verificatiemodus in de vervolgkeuzelijst **Authenticatiemodus**.
6. Klik op **OK**.

Figuur 15-8 Authenticatiemodi voor personen instellen

7. Optioneel: Selecteer persoon (personen) op de pagina Persoonauthenticatiemodus en klik vervolgens op **Toepassen** om de persoonauthenticatiemodus toe te passen op het apparaat.

Opmerking

De persoonsverificatie heeft een hogere prioriteit dan andere verificatiemodi. Wanneer de persoonauthenticatiemodus op het toegangscontroleapparaat is geconfigureerd, moet de persoon zich op dit apparaat authenticeren via de persoonauthenticatiemodus.

15.5.8 Eerste persoon in configureren

Je kunt meerdere eerste personen instellen voor één toegangscontrolepunt. Nadat de eerste persoon is geautoriseerd, kunnen meerdere personen toegang krijgen tot de deur of andere authenticatieacties uitvoeren.

Voordat u begint

- Voeg het toegangscontroleapparaat toe aan de client en zorg ervoor dat het apparaat de eerste persoon in-functie ondersteunt.
- Voeg persoon toe en wijs toegangsrechten toe aan ontworpen persoon. Raadpleeg **Persoonsbeheer** en **Toegangsgroep instellen om toegangsrechten aan personen toe** te wijzen

voor meer informatie.

Stappen

1. Klik op **Toegangsbeheer** → **Geavanceerde functie** → **Eerste persoon binnen om de pagina** Eerste persoon binnen te openen.
2. Selecteer een toegangscontroleapparaat in de lijst aan de linkerkant.
3. Selecteer de huidige modus als **Inschakelen Resterende Open na Eerste Persoon, Uitschakelen Resterende Open na Eerste Persoon** of **Autorisatie door Eerste Persoon** in de vervolgkeuzelijst voor elk toegangscontrolepunt van het geselecteerde apparaat.

Open blijven na eerste persoon inschakelen

De deur blijft open gedurende de geconfigureerde tijdsduur nadat de eerste persoon geautoriseerd is tot de duur van open blijven eindigt. Als je deze modus selecteert, moet je de opeenvolgende authenticatietijden en het interval van opeenvolgende authenticatie instellen.

Opmerking

De duur van open blijven moet tussen 0 en 1440 minuten liggen. Standaard is de duur van open blijven 10 minuten.

Blijven openstaan na eerste persoon uitschakelen

Schakel de functie van de eerste persoon die binnenkomt uit, namelijk normale authenticatie.

Machtiging door eerste persoon

Alle authenticaties (behalve de authenticaties van superkaart, superwachtwoord, duresskaart en duresscode) zijn alleen toegestaan na autorisatie door de eerste persoon.

Opmerking

Je kunt je opnieuw authenticeren door de eerste persoon om de eerste persoonsmodus uit te schakelen.

4. Klik op **Toevoegen** in het paneel Eerste persoonslijst.
5. Selecteer persoon (personen) in de linker lijst en de persoon (personen) wordt (worden) toegevoegd aan de geselecteerde personen als de eerste persoon (personen) van de deuren. De toegevoegde eerste persoon (personen) wordt (worden) weergegeven in de lijst Eerste persoon
6. Optioneel: Selecteer een eerste persoon uit de lijst en klik op **Verwijderen** om de persoon uit de lijst met eerste personen te verwijderen.
7. Klik op **Opslaan**.

15.5.9 Anti-Passback configureren

De anti-passbackfunctie is ontworpen om misbruik of frauduleus gebruik van toegangsgegevens te minimaliseren, zoals het teruggeven van een kaart aan een onbevoegd persoon of toegang via de

achterklep. De anti-passback functie stelt een specifieke volgorde in waarin de toegangsgegevens moeten worden gebruikt om toegang te verlenen. Je kunt de volgorde instellen op basis van het werkelijke pad via de client en als de persoon de credentials in de verkeerde volgorde gebruikt, kun je ook de antipaswoordrecords resetten.


Voordat u begint

Voeg het toegangscontroleapparaat toe aan de client en schakel de anti-terugloofunctie van het toegangscontroleapparaat in.

Stappen

Opmerking

Zowel de anti-pass back als de multi-door interlocking functie kunnen tegelijkertijd geconfigureerd worden voor een toegangscontrole apparaat. Raadpleeg **Multi-door interlocking configureren** voor de configuratie van de multi-door interlocking.

1. Klik op **Toegangsbeheer** → **Geavanceerde functie** → **Anti-Passback** om de pagina Anti-Passback-instellingen te openen.
 2. Selecteer een toegangscontroleapparaat in het linkerpaneel.
 3. Selecteer een kaartlezer als begin van het pad in het veld **Eerste kaartlezer**.
 4. Klik op  van de geselecteerde eerste kaartlezer in de kolom **Kaartlezer erna** om het dialoogvenster Kaartlezer selecteren te openen.
 5. Selecteer de volgende kaartlezers voor de eerste kaartlezer.
-

Opmerking

Er kunnen maximaal vier kaartlezers worden toegevoegd als kaartlezers voor één kaartlezer.

6. Klik op **OK** in het dialoogvenster om de selecties op te slaan.
7. Klik op **Opslaan** op de pagina Anti-Passback Instellingen om de instellingen op te slaan en in werking te laten treden.

Voorbeeld

Kaartschrijfpad instellen: Als u Reader In_01 als begin selecteert en Reader In_02, Reader Out_04 als de gekoppelde kaartlezers. Dan kun je alleen door het toegangspunt door de kaart te swipen in de volgorde Reader In_01, Reader In_02 en Reader Out_04.

8. Klik op **Reset Anti-Passback** en selecteer de persoon/personen om de gerelateerde anti-passback records over de persoon/personen op het apparaat te verwijderen.
-

Opmerking

Deze functie moet worden ondersteund door het apparaat.

15.5.10 Multideurvergrendeling configureren

Je kunt de multideurvergrendeling instellen tussen meerdere deuren van hetzelfde toegangscontroleapparaat. Om een van de deuren te openen, moeten de andere deuren gesloten blijven. Dat betekent dat in de interlocking gecombineerde deurgroep maximaal één deur tegelijkertijd geopend kan worden.

Voordat u begint

Voeg het toegangscontroleapparaat toe aan de client en controleer of het apparaat de functie voor vergrendeling van meerdere deuren ondersteunt.

Stappen

Opmerking

- De Multi-door Interlocking-functie wordt alleen ondersteund door het toegangscontroleapparaat dat meer dan één toegangscontrolepunt (deur) heeft.
 - Zowel de anti-passbackfunctie als de functie voor het vergrendelen van meerdere deuren kan tegelijkertijd worden geconfigureerd voor een toegangscontroleapparaat. Raadpleeg **Anti-Passback configureren** voor de configuratie van de anti-passbackfunctie.
-

1. Klik op **Toegangscontrole** → **Geavanceerde functie** → **Multideurvergrendeling**.
 2. Selecteer een toegangscontroleapparaat in het linkerpaneel.
 3. Klik op **Add (Toevoegen)** in het paneel Multi-door Interlocking List (Lijst meerdere deuren) om Add Access Control Point (Toegangscontrolepunt toevoegen) te openen.
 4. Selecteer minstens twee toegangscontrolepunten (deuren) uit de lijst.
-

Opmerking

Er kunnen maximaal vier deuren worden toegevoegd in een combinatie van meerdere deuren.

5. Klik op **OK** om het/de geselecteerde toegangscontrolepunt(en) toe te voegen voor vergrendeling.
De geconfigureerde combinatie van vergrendelingen voor meerdere deuren wordt weergegeven op het paneel Lijst van vergrendelingen voor meerdere deuren.
6. Optioneel: Selecteer een toegevoegde combinatie van vergrendelingen voor meerdere deuren uit de lijst en klik op **Verwijderen** om de combinatie te verwijderen.
7. Klik op **Toepassen** om de instellingen toe te passen op het toegangscontroleapparaat.

15.5.11 Authenticatiecode configureren

Je kunt de verificatiecode instellen op de client. Daarna kun je de deur openen door de verificatiecode in te voeren als je de kaart bent vergeten.

Voordat u begint

Voeg het toegangscontroleapparaat toe aan de client en zorg ervoor dat het apparaat de

authenticatiecode ondersteunt als authenticatiemodus.

Stappen

1. Klik op **Toegangsbeheer** → **Geavanceerde functie** → **Authenticatiecode** om de configuratiepagina voor de authenticatiecode te openen.
2. Selecteer een toegangscontroleapparaat in de lijst van het Controller List-paneel. Alle toegepaste kaarten en personen worden weergegeven op het deelvenster Kaartlijst.

Opmerking

Raadpleeg **Toegangsgroep instellen om toegangsrechten toe te wijzen aan personen** voor het instellen en toepassen van de rechten op het apparaat.

3. Klik op het veld van elke kaart in de kolom Verificatiecode om de verificatiecode in te voeren.

Opmerking

De authenticatiecode moet 4 tot 8 cijfers bevatten.

4. Klik op **Opslaan** in de rechterbovenhoek van de pagina Authenticatiecode om de instellingen op te slaan.
De authenticatiecodefunctie van de kaart wordt automatisch ingeschakeld.

Wat nu te doen

Je moet de kaartlezerauthenticatiemodus van het toegangscontroleapparaat instellen als **Kaart/Authenticatiecode**. Raadpleeg **Kaartlezerauthenticatiemodus en -schema configureren** voor meer informatie.

15.6.3 Parameters voor apparaatopname instellen

Je kunt de vastlegparameters van het toegangscontroleapparaat configureren, inclusief handmatige vastlegging en vastlegging op basis van gebeurtenissen.

Opmerking

- De capture-functie moet worden ondersteund door het apparaat.
 - Voordat u de vastlegparameters instelt, moet u eerst de beeldopslag instellen om te bepalen waar de foto's die door een gebeurtenis worden geactiveerd, worden opgeslagen. Raadpleeg **Beeldopslag instellen** voor meer informatie.
-

Parameters voor getriggerde opname instellen

Wanneer zich een gebeurtenis voordoet, kan de camera van het toegangscontroleapparaat worden geactiveerd om foto('s) te maken om vast te leggen wat er gebeurt wanneer de gebeurtenis plaatsvindt. Je kunt de gemaakte foto's bekijken wanneer je de details van de gebeurtenis in Gebeurteniscentrum controleert. Daarvoor moet je de parameters voor de opname

instellen, zoals het aantal foto's dat per keer wordt vastgelegd.

Voordat u begint

Voordat u de vastlegparameters instelt, moet u eerst de beeldopslag instellen om te bepalen waar de vastgelegde beelden worden opgeslagen. Raadpleeg [Beeldopslag instellen](#) voor meer informatie.

Stappen

Opmerking

Deze functie moet worden ondersteund door het apparaat

1. Ga naar de module Toegangscontrole.
2. Ga in de navigatiebalk links naar **Geavanceerde functie** → **Meer parameters** → **Vastleggen**.
3. Selecteer een toegangscontroleapparaat in de apparatenlijst en selecteer **Gekoppeld vastleggen**.
4. Stel het beeldformaat en de beeldkwaliteit in.
5. Stel de opnametijden in zodra de camera wordt geactiveerd. Dit bepaalt hoeveel foto's er per keer worden vastgelegd.
6. Als het aantal vastleggingen meer dan 1 is, stel dan het interval voor elke vastlegging in.
7. Klik op **Opslaan**.

Handmatige vastlegparameters instellen

In de module Status Monitoring kun je handmatig een beeld vastleggen van de camera van het toegangscontroletoestel door op een knop te klikken. Daarvoor moet je de parameters voor de opname instellen, zoals de beeldkwaliteit.

Voordat u begint

Voordat u de vastlegparameters instelt, moet u eerst het opslagpad instellen om te bepalen waar de vastgelegde beelden worden opgeslagen. Raadpleeg [Bestandsopslagpad instellen](#) voor meer informatie.

Stappen

Opmerking

Deze functie moet worden ondersteund door het apparaat

1. Ga naar de module Toegangscontrole.
2. Ga in de navigatiebalk links naar **Geavanceerde functie** → **Meer parameters** → **Vastleggen**.
3. Selecteer een toegangscontroleapparaat in de apparatenlijst en selecteer **Handmatig vastleggen**.
4. Selecteer de resolutie van de vastgelegde beelden in de vervolgkeuzelijst.
5. Selecteer de beeldkwaliteit als **Hoog**, **Medium** of **Laag**. Hoe hoger de beeldkwaliteit, hoe groter het beeld.

6. Klik op **Opslaan**.

15.6.4 Parameters instellen voor gezichtsherkenningsterminal

Voor de gezichtsherkenningsterminal kunt u de parameters instellen, waaronder de database met gezichtsfoto's, QR-codeverificatie, enz.

Stappen

Opmerking

Deze functie moet worden ondersteund door het apparaat.

1. Ga naar de module Toegangscontrole.
 2. Ga in de navigatiebalk links naar **Geavanceerde functie** → **Meer parameters**.
 3. Selecteer een toegangscontroleapparaat in de apparatenlijst en klik op **Gezichtsherkenningsterminal**.
 4. Stel de parameters in.
-

Opmerking

Deze weergegeven parameters variëren naargelang de verschillende apparaatmodellen.

COM

Selecteer een COM-poort voor configuratie. COM1 verwijst naar de RS-485 interface en COM2 verwijst naar de RS-232 interface.

Database met gezichtsfoto's

kies Deep Learning als database voor gezichtsfoto's.

Authenticeren met QR Code

Indien ingeschakeld, kan de camera van het apparaat de QR-code scannen om te verifiëren. Standaard is de functie uitgeschakeld.

Authenticatie blokkijst

Als dit is ingeschakeld, vergelijkt het apparaat de persoon die toegang wil krijgen met de personen in de blokkadellijst.

Als er een overeenkomst is (de persoon staat op de blokkadellijst), wordt de toegang geweigerd en uploadt het apparaat een alarm naar de client.

Als deze niet overeenkomt (de persoon staat niet in de blokkadellijst), wordt de toegang verleend.

Authenticatie gezichtsfoto opslaan

Als deze optie is ingeschakeld, wordt de gezichtsfoto die tijdens de verificatie is gemaakt, opgeslagen op het apparaat.

MCU-versie

Bekijk de MCU-versie van het apparaat.

5. Klik op **Opslaan**.

15.6.5 M1-kaartcodering inschakelen

M1-kaartcodering kan het beveiligingsniveau van authenticatie verbeteren.

Stappen

Opmerking

De functie moet worden ondersteund door het toegangscontroleapparaat en de kaartlezer.

1. Ga naar de module Toegangscontrole.
2. Ga in de navigatiebalk links naar **Geavanceerde functie** → **Meer parameters**.
3. Selecteer een toegangscontroleapparaat in de apparatenlijst en klik op **M1-kaartcodering** om de pagina M1-kaartcodering te openen.
4. Zet de schakelaar op aan om de coderingsfunctie van de M1-kaart in te schakelen.
5. Stel de sector-ID in.

De sector-ID gaat van 1 tot 100.

6. Klik op **Opslaan** om de instellingen op te slaan.

15.6.6 RS-485 parameters instellen

Je kunt de RS-485-parameters van het toegangscontroletoestel instellen, waaronder de baudsnelheid, de gegevensbit, de stopbit, het pariteitstype, het flowcontroletype, de communicatiemodus, de werkmodus en de verbindingmodus.

Voordat u begint

Voeg het toegangscontroleapparaat toe aan de client en zorg ervoor dat het apparaat de RS-485 interface ondersteunt.

Stappen

1. Ga naar de module Toegangscontrole.
2. Ga in de navigatiebalk links naar **Geavanceerde functie** → **Meer parameters**.
3. Selecteer een toegangscontroleapparaat in de apparatenlijst en klik op **RS-485** om de pagina RS-485 Instellingen te openen.
4. Selecteer het seriële poortnummer in de vervolgkeuzelijst om de RS-485-parameters in te stellen.
5. Stel de baudrate, de gegevensbit, de stopbit, het pariteitstype, de communicatiemodus, de werkmodus en de verbindingmodus in de vervolgkeuzelijst in.

 **Opmerking**

Wanneer de verbindingsmodus **Toegangscontroleapparaat verbinden** is, kunt u **Kaartnummer** of **Persoon ID** selecteren als het uitvoertype.

6. Klik op **Opslaan**.

- De geconfigureerde parameters worden automatisch toegepast op het apparaat.
- Wanneer je de werkmodus of verbindingsmodus wijzigt, zal het apparaat automatisch herstarten.

15.6.7 Wiegand-parameters instellen

Je kunt het Wiegand-kanaal en de communicatiemodus van het toegangscontroleapparaat instellen. Na het instellen van de Wiegand parameters kan het apparaat verbinding maken met een Wiegand kaartlezer via Wiegand communicatie.

Voordat u begint

Voeg het toegangscontroleapparaat toe aan de client en zorg ervoor dat het apparaat Wiegand ondersteunt.

Stappen

1. Ga naar de module Toegangscontrole.
2. Ga in de navigatiebalk links naar **Geavanceerde functie** → **Meer parameters**.
3. Selecteer een toegangscontroleapparaat in de apparatenlijst en klik op **Wiegand** om de pagina met Wiegand-instellingen te openen.
4. Zet de schakelaar op on om de Wiegand-functie voor het apparaat in te schakelen.
5. Selecteer het Wiegand kanaalnr. en de communicatiemodus in de vervolkeuzelijst.

 **Opmerking**

Als je **Communicatierichting** instelt als **Verzenden**, moet je de **Wiegand-modus** instellen als **Wiegand 26** of **Wiegand 34**.

6. Klik op **Opslaan**.

- De geconfigureerde parameters worden automatisch toegepast op het apparaat.
- Na het wijzigen van de communicatierichting zal het apparaat automatisch herstarten.

15.7. Koppelingsacties voor toegangscontrole configureren

Je kunt verschillende verbindingsacties configureren voor de gebeurtenis die wordt gedetecteerd door het toegangscontroleapparaat. Daarna worden de koppelingsacties geactiveerd zodra de gebeurtenis plaatsvindt. Dit mechanisme wordt gebruikt om het beveiligingspersoneel op de hoogte te stellen van de gebeurtenis of om automatische toegangscontrole in realtime te

activeren.

Twee soorten koppelingsacties worden ondersteund:

- **Acties op de client:** Wanneer de gebeurtenis wordt gedetecteerd, worden de acties op de client geactiveerd, zoals de client die een hoorbare waarschuwing geeft...
- **Acties van het apparaat:** Wanneer de gebeurtenis wordt gedetecteerd, zal het de acties van een specifiek apparaat activeren, zoals het zoemen van een kaartlezer en het openen/sluiten van een deur, ...

15.7.1 Klantacties voor toegangsgebeurtenis configureren

Zelfs als je ver weg bent van een toegangspunt, kun je toch weten wat er gebeurt en hoe dringend de gebeurtenis is via de client door clientacties te configureren voor de toegangsgebeurtenis. Clientacties verwijzen hier naar de acties die automatisch door de client zelf worden uitgevoerd, zoals het geven van een geluidssignaal en het versturen van een e-mail. Zodra een gebeurtenis wordt geactiveerd, zal de client het beveiligingspersoneel hiervan op de hoogte stellen, zodat hij/zij de gebeurtenis op tijd kan afhandelen.

Voordat u begint

Apparaat voor toegangscontrole toevoegen aan de client.

Stappen

1. Klik op **Gebeurtenisconfiguratie** → **Gebeurtenis toegangscontrole**.
De toegevoegde toegangscontroleapparaten worden weergegeven in de apparatenlijst.
2. Selecteer een bron (inclusief apparaat, alarmingang, deur/lift en kaartlezer) in de apparatenlijst.
De gebeurtenistypen die de geselecteerde bron ondersteunt, worden weergegeven.
3. Selecteer de gebeurtenis(sen) en klik op **Prioriteit bewerken** om de prioriteit voor de gebeurtenis(sen) te bepalen, die kan worden gebruikt om gebeurtenissen in het gebeurteniscentrum te filteren.
4. Stel de koppelingsacties van de gebeurtenis in.
 - 1) Selecteer de gebeurtenis(sen) en klik op **Koppeling bewerken** om de clientacties in te stellen wanneer de gebeurtenis(sen) worden geactiveerd.

Hoorbare waarschuwing

De clientsoftware geeft een hoorbare waarschuwing wanneer de gebeurtenis wordt geactiveerd. Je kunt een alarmgeluid selecteren voor de hoorbare waarschuwing.

Opmerking

Raadpleeg **Alarmgeluid instellen** voor meer informatie over het instellen van het alarmgeluid.

Verstuur e-mail

Stuur een e-mailmelding over de gebeurtenis naar een of meer ontvangers.

Raadpleeg **E-mailparameters instellen** voor meer informatie over het instellen van e-mailparameters.

Pop-upvenster

Pop-upvenster om de gebeurtenisinformatie (inclusief gebeurtenisdetails, videobeelden van de gebeurtenis, foto's van de gebeurtenis) weer te geven op de softwareclient wanneer de gebeurtenis wordt geactiveerd.

Weergeven op kaart

Wanneer de gebeurtenisbron wordt toegevoegd als een hotspot op de kaart, wordt de hotspot weergegeven met een rood nummer (geeft het aantal gebeurtenissen aan en het maximumaantal is 10) opzij wanneer de gebeurtenis wordt geactiveerd, wat het beveiligingspersoneel helpt om de locatie van de gebeurtenis te zien.

Je kunt ook op de hotspot klikken om de details van de gebeurtenis en de live video van de gekoppelde camera te bekijken.

Gekoppelde camera

Koppel de geselecteerde camera om een foto te maken wanneer de toegangsevent wordt geactiveerd.

Selecteer de camera in de vervolgkeuzelijst.

2) Klik op **OK**.

- Schakel de gebeurtenis in zodat wanneer de gebeurtenis wordt gedetecteerd, de gebeurtenis naar de client wordt verzonden en de koppelingsacties worden geactiveerd.
- Optioneel: Klik op **Kopiëren om** de gebeurtenisinstellingen te kopiëren naar een ander toegangscontroleapparaat, alarmingang, deur/lift of kaartlezer.

15.7.2 Apparaatacties voor toegangsgebeurtenis configureren

Je kunt de koppelingsacties van het toegangscontroleapparaat instellen voor de getriggerde gebeurtenis van het toegangscontroleapparaat. Daarna kan een getriggerde gebeurtenis de alarmuitgang, zoemer op de toegangscontroller en andere acties activeren.

Stappen

Opmerking

De koppelingsacties moeten worden ondersteund door het apparaat.

- Klik op **Toegangsbeheer** → **Koppelingsconfiguratie**.
- Selecteer het toegangscontroleapparaat in de lijst aan de linkerkant.
- Klik op **Toevoegen** om een nieuwe koppeling toe te voegen.
- Selecteer **Event Linkage** als gebeurtenisbron.
- Selecteer het gebeurtenistype en de gedetailleerde gebeurtenis om de koppeling in te stellen.
- Stel in het gebied Linkage Target het eigenschapsdoel in om deze actie in te schakelen.

Zoemer op controller

De akoestische waarschuwing van de toegangscontrole wordt geactiveerd.

Vang

Er wordt een gebeurtenisafbeelding gemaakt wanneer de geselecteerde gebeurtenis plaatsvindt.

Opname

Er wordt een gebeurtenisafbeelding gemaakt wanneer de geselecteerde gebeurtenis plaatsvindt.

Opmerking

Het apparaat moet opname ondersteunen.

Zoemer op Lezer

De hoorbare waarschuwing van de kaartlezer wordt geactiveerd.

Alarm Uitgang

De alarmuitgang wordt geactiveerd voor notificatie wanneer de geselecteerde gebeurtenis plaatsvindt.

Alarm ingang

De alarmingang in- of uitschakelen.

Opmerking

Het apparaat moet de alarmingang ondersteunen.

Toegangspunt

De deurstatus open, dicht, open blijven of dicht blijven wordt geactiveerd.

Opmerking

De doeldeur en de brondeur kunnen niet dezelfde zijn.

Audio afspelen

De audio-aanvraag wordt geactiveerd. En de geselecteerde audio-index gerelateerde audio-inhoud zal worden afgespeeld volgens de geconfigureerde afspeelmodus.

7. Klik op **Opslaan**.

8. Optioneel: Na het toevoegen van de apparaatkoppeling kun je een of meer van de volgende dingen doen:

Koppelingsinstellingen bewerken Selecteer de geconfigureerde koppelingsinstellingen in de apparatenlijst en u kunt de gebeurtenisbronparameters bewerken, inclusief gebeurtenisbron en koppelingsdoel.

Koppelingsinstellingen verwijderen Selecteer de geconfigureerde koppelingsinstellingen in de apparatenlijst en klik op **Verwijderen** om het te verwijderen.

15.7.3 Apparaatacties voor kaartzwemmen configureren

Je schakelt de koppelingsacties van een toegangscontroleapparaat in (zoals het uitschakelen van een zone en het activeren van een audioboodschap) voor het vegen van een specifieke kaart. Op deze manier kun je het gedrag en de verblijfplaats van de kaarthouder controleren.

Stappen

Opmerking

Het apparaat moet dit ondersteunen.

1. Klik op **Toegangsbeheer** → **Koppelingsconfiguratie**.
2. Selecteer het toegangscontroleapparaat in de lijst aan de linkerkant.
3. Klik op **Toevoegen** om een nieuwe koppeling toe te voegen.
4. Selecteer **Card Linkage** als gebeurtenisbron.
5. Voer het kaartnummer in of selecteer de kaart in de vervolgkeuzelijst.
6. Selecteer de kaartlezer waar de kaart naartoe veegt.
7. Stel in het gebied Linkage Target het eigenschapsdoel in om deze actie in te schakelen.

Zoemer op controller

De akoestische waarschuwing van de toegangscontrole wordt geactiveerd.

Zoemer op Lezer

De hoorbare waarschuwing van de kaartlezer wordt geactiveerd.

Vang

Er wordt een gebeurtenisafbeelding gemaakt wanneer de geselecteerde gebeurtenis plaatsvindt.

Opname

Er wordt een gebeurtenisafbeelding gemaakt wanneer de geselecteerde gebeurtenis plaatsvindt.

Opmerking

Het apparaat moet opname ondersteunen.

Alarm Uitgang

De alarmuitgang wordt geactiveerd voor notificatie.

Alarm ingang

De alarmingang in- of uitschakelen.

 **Opmerking**

Het apparaat moet de alarmingang ondersteunen.

Toegangspunt

De deurstatus open, dicht, open blijven of gesloten blijven wordt geactiveerd.

Audio afspelen

De audio-aanvraag wordt geactiveerd. En de geselecteerde audio-index gerelateerde audio-inhoud zal worden afgespeeld volgens de geconfigureerde afspeelmodus.

8. Klik op **Opslaan**.

Wanneer de kaart (geconfigureerd in stap 5) over de kaartlezer (geconfigureerd in stap 6) veegt, kunnen de gekoppelde acties (geconfigureerd in stap 7) worden geactiveerd.

9. Optioneel: Na het toevoegen van de apparaatkoppeling kun je een of meer van de volgende dingen doen:

Koppelingsinstellingen verwijderen Selecteer de geconfigureerde koppelingsinstellingen in de apparatenlijst en klik op **Verwijderen** om het te verwijderen.

Koppelingsinstellingen bewerken Selecteer de geconfigureerde koppelingsinstellingen in de apparatenlijst en u kunt de gebeurtenisbronparameters bewerken, inclusief gebeurtenisbron en koppelingsdoel.

15.7.4 Apparaatacties voor persoon-ID configureren

U kunt de koppelingsacties van de toegangscontrole instellen voor de gespecificeerde persoon-ID. Wanneer het toegangscontroleapparaat de gespecificeerde persoon-ID detecteert, kan het de alarmuitgang, zoemer op kaartlezer en andere acties activeren om speciale bewaking op de gespecificeerde persoon uit te voeren.

Stappen

 **Opmerking**

Het apparaat moet dit ondersteunen.

1. Klik op **Toegangsbeheer** → **Koppelingsconfiguratie**.
2. Selecteer het toegangscontroleapparaat in de lijst aan de linkerkant.
3. Klik op **Toevoegen** om een nieuwe koppeling toe te voegen.
4. Selecteer **Person Linkage** als gebeurtenisbron.
5. Voer het personeelsnummer in of selecteer de persoon in de vervolgkeuzelijst.
6. Selecteer de kaartlezer waar de kaart naartoe veegt.
7. Stel in het gebied Linkage Target het eigenschapsdoel in om deze actie in te schakelen.

Zoemer op controller

De akoestische waarschuwing van de toegangscontrole wordt geactiveerd.

Zoemer op Lezer

De hoorbare waarschuwing van de kaartlezer wordt geactiveerd.

Vang

Er wordt een gebeurtenisafbeelding gemaakt wanneer de geselecteerde gebeurtenis plaatsvindt.

Opname

Er wordt een gebeurtenisafbeelding gemaakt wanneer de geselecteerde gebeurtenis plaatsvindt.

Opmerking

Het apparaat moet opname ondersteunen.

Alarm Uitgang

De alarmuitgang wordt geactiveerd voor notificatie.

Alarm ingang

De alarmingang in- of uitschakelen.

Opmerking

Het apparaat moet de zonefunctie ondersteunen.

Toegangspunt

De deurstatus open, dicht, open blijven of gesloten blijven wordt geactiveerd.

Audio afspelen

De audio-aanvraag wordt geactiveerd. En de geselecteerde audio-index gerelateerde audio-inhoud zal worden afgespeeld volgens de geconfigureerde afspeelmodus.

8. Klik op **Opslaan**.

9. Optioneel: Na het toevoegen van de apparaatkoppeling kun je een of meer van de volgende dingen doen:

Koppelingsinstellinge n verwijderen Selecteer de geconfigureerde koppelingsinstellingen in de apparatenlijst en klik op **Verwijderen** om het te verwijderen.

Koppelingsinstellinge n bewerken Selecteer de geconfigureerde koppelingsinstellingen in de lijst met apparaten en u kunt de gebeurtenisbronparameters bewerken, inclusief gebeurtenisbron en koppelingsdoel.

15.8.1 Status besturingsdeur

Je kunt de status van de deur(en) bepalen, waaronder deur ontgrendelen, deur vergrendelen, deur ontgrendeld blijven, deur vergrendeld blijven, alles ontgrendeld blijven, enz.

Voordat u begint

- Voeg persoon toe en wijs toegangsrechten toe aan de ontworpen persoon, en de persoon zal toegangsrechten hebben voor de toegangspunten (deuren). Raadpleeg [Persoonsbeheer](#) en [Toegangsgroep instellen om toegangsautorisatie aan personen toe te wijzen](#) voor meer informatie.
- Zorg ervoor dat de gebruiker toestemming heeft voor de toegangspunten (deuren). Raadpleeg [Gebruiker toevoegen](#) voor meer informatie.

Stappen

1. Klik op **Monitoring** om naar de statusmonitoringpagina te gaan.
2. Selecteer een groep toegangspunten in de rechterbovenhoek.

Opmerking

Raadpleeg [Groepsbeheer](#) voor het beheren van de groep toegangspunten.

De deuren in de geselecteerde toegangscontrolegroep worden weergegeven.

3. Klik op een deurpictogram om een deur te selecteren of druk op **Ctrl** en selecteer meerdere deuren.

Opmerking

Voor **Alles ontgrendeld** en **Alles vergrendeld blijven**, negeer deze stap.

4. Klik op de volgende knoppen om de deur te bedienen.

Ontgrendel

Als de deur vergrendeld is, ontgrendel je hem en gaat hij eenmalig open. Na de openingsperiode wordt de deur automatisch gesloten en weer vergrendeld.

Slot

Als de deur ontgrendeld is, vergrendel je hem en wordt hij gesloten. De persoon die de toegangsrechten heeft, kan de deur openen met referenties.

Blijf ontgrendeld

De deur wordt ontgrendeld (ongeacht of deze gesloten of open is). Alle personen hebben toegang tot de deur zonder dat er referenties nodig zijn.

Vergrendeld blijven

De deur wordt gesloten en vergrendeld. Niemand heeft toegang tot de deur, zelfs niet als hij/zij de geautoriseerde toegangsgegevens heeft, behalve de supergebruikers.

Blijven allemaal ontgrendeld

Alle deuren in de groep worden ontgrendeld (ongeacht of ze gesloten of open zijn). Alle personen hebben toegang tot de deuren zonder dat er referenties nodig zijn.

Blijven allemaal vergrendeld

Alle deuren in de groep worden gesloten en vergrendeld. Niemand heeft toegang tot de deuren, zelfs niet als hij/zij de geautoriseerde credentials heeft, behalve de supergebruikers.

Vang

Maak een foto handmatig.



Opmerking

De knop **Capture** is beschikbaar als het apparaat de capture-functie ondersteunt. Het beeld wordt opgeslagen op de pc waarop de client draait. Raadpleeg Het pad [voor bestandsopslag instellen](#) voor het instellen van het opslagpad.

Resultaat

Het pictogram van de deuren verandert in realtime volgens de bewerking als de bewerking is geslaagd.

15.8.3 Real-time toegangsrecords controleren

De realtime toegangsgegevens kunnen worden weergegeven in de client, waaronder gegevens over kaartswaaien, gezichtsherkenning, informatie over de temperatuur van het huidoppervlak, enz. Je kunt ook de persoonsinformatie bekijken en de foto bekijken die tijdens de toegang is gemaakt.

Voordat u begint

Je hebt persoon (personen) en toegangscontroleapparaat (-apparaten) toegevoegd aan de client. Raadpleeg [Persoonsbeheer](#) en [Apparaat toevoegen](#) voor meer informatie.

Stappen

1. Klik op **Monitoring** om de monitoringmodule te openen.

Real-time toegangsrecords worden onderaan de pagina weergegeven. Je kunt de details van de records bekijken, zoals kaartnummer, naam van de persoon, tijd van de gebeurtenis, locatie van de deur, temperatuur, authenticatietype enz.

Figuur 15-12 Real-time toegangsrecords



Opmerking

Je kunt met de rechtermuisknop op de kolomnaam van de tabel met toegangsgebeurtenissen klikken om de kolom te tonen of te verbergen, afhankelijk van de werkelijke behoeften.

2. Optioneel: Selecteer een toegangspuntgroep uit de vervolgkeuzelijst in de rechterbovenhoek om de realtime toegangsrecords van de geselecteerde groep weer te geven.
 3. Optioneel: Controleer het gebeurtenistype en de status van de gebeurtenis.
De gedetecteerde gebeurtenissen van gecontroleerd type en status worden weergegeven in de onderstaande lijst.
 4. Optioneel: Vink **Toon laatste gebeurtenis** aan om de laatste toegangsregistratie te bekijken.
De recordlijst wordt omgekeerd chronologisch weergegeven.
 5. Optioneel: Vink **Enable Abnormal Temperature Prompt (Abnormale temperatuurmelding inschakelen)** aan om de melding voor abnormale huidoppervlaktetemperatuur in te schakelen.
-


Opmerking

Wanneer deze optie is ingeschakeld, verschijnt er bij informatie over abnormale temperaturen een venster Abnormale temperatuur wanneer u de bewakingsmodule opent, waarin de foto van de persoon, de temperatuur van het huidoppervlak, het kaartnummer, de naam van de persoon, enz. worden weergegeven.


6. Optioneel: Klik op een gebeurtenis om persoonsfoto's te bekijken (inclusief vastgelegde foto en profiel).
-

Opmerking

In het **gekoppelde** veld **Afbeelding vastleggen kunt** u dubbelklikken op de vastgelegde afbeelding om een vergrote afbeelding te bekijken.

7. Optioneel: Klik op  om monitoringdetails te bekijken (inclusief gedetailleerde informatie over de persoon en de vastgelegde foto).
-


Opmerking

In het pop-upvenster kun je op  klikken om de monitoringdetails op het volledige scherm te bekijken.

Hoofdstuk 19 Logboek zoeken

Er zijn twee soorten logboeken: operationeel logboek en systeemlogboek. De operation logs verwijzen naar de normale bewerkingen die de gebruiker uitvoerde op de client, zoals het toevoegen van een apparaat, het resetten van het wachtwoord, het starten van de live-weergave, enzovoort; en de systeemlogs registreren de systeem informatie, zoals aanmelden, afmelden, vergrendelen en ontgrendelen, enzovoort. Je kunt de logbestanden doorzoeken en de loggegevens bekijken, inclusief tijd, gebruiker, enz.

Stappen

1. Ga naar de logboekzoekmodule.
2. Klik op  om de begin- en eindtijd op te geven.

Opmerking

Je kunt de logboeken binnen een maand doorzoeken.

3. Selecteer een gebruiker om de logbestanden te doorzoeken die worden gegenereerd wanneer deze gebruiker op de client werkt.
4. Selecteer **Operation Log** of **System Log** als logtype.
5. Klik op **Zoeken**.
De logbestanden tussen de starttijd en eindtijd worden weergegeven in de lijst. Je kunt de werkingstijd, het type en andere informatie van de logs controleren.
6. Optioneel: Voer de volgende bewerkingen uit als er te veel logbestanden zijn.

Filer Klik op  op elke tabelkop en selecteer om de logboeken te filteren.

Sorteer Klik op de tabelkop om de logs te sorteren op tijd of lettervolgorde.

Hoofdstuk 20 Gebruikersbeheer

Om het systeem beter te beveiligen, moet de beheerder verschillende accounts aanmaken voor verschillende gebruikers en verschillende rechten toekennen aan de gebruiker. Om te voorkomen dat verschillende mensen dezelfde gebruikersaccount delen, raden we aan om de gebruikersaccounts regelmatig te beheren.

20.1 Gebruiker toevoegen

De supergebruiker en beheerder kunnen nieuwe gebruikers toevoegen en indien nodig verschillende rechten toekennen aan verschillende gebruikers.

Voer deze taak uit om een gebruikersaccount toe te voegen.

Stappen

Opmerking

De gebruikersaccount die je hebt geregistreerd om in te loggen in de software is ingesteld als supergebruiker.

1. Ga naar de module Gebruikersbeheer.
2. Klik op **Gebruiker toevoegen** om het gebruikersinformatiegebied weer te geven.
3. Selecteer het gebruikerstype in de vervolgkeuzelijst.

Beheerder

De beheerdersaccount heeft standaard alle rechten en kan de wachtwoorden en rechten van alle operators en zijn eigen account wijzigen.

Exploitant

De operatoraccount heeft standaard geen rechten en je kunt de rechten handmatig toewijzen. Een operator kan alleen de wachtwoorden wijzigen van zijn eigen account en de accounts die door hem zijn toegevoegd.

4. Voer naar wens de gebruikersnaam, het wachtwoord en het bevestigingswachtwoord in.

 **Let op**

De wachtwoordsterkte van het apparaat kan automatisch worden gecontroleerd. We raden u ten eerste aan het wachtwoord van uw eigen keuze te wijzigen (met minimaal 8 tekens, waaronder ten minste drie soorten uit de volgende categorieën: hoofdletters, kleine letters, cijfers en speciale tekens) om de beveiliging van uw product te verbeteren. En we raden u aan uw wachtwoord regelmatig te wijzigen, vooral in het hoogbeveiligde systeem kan een maandelijkse of wekelijkse wijziging van het wachtwoord uw product beter beschermen. De juiste configuratie van alle wachtwoorden en andere beveiligingsinstellingen is de verantwoordelijkheid van de installateur en/of eindgebruiker.

5. Schakel de selectievakjes in om de machtigingen toe te wijzen aan de aangemaakte gebruiker.
 6. Optioneel: Klik op **Standaardwaarde** om de standaardmachtigingen van deze gebruiker te herstellen.
 7. Klik op **Opslaan**.
-

 **Opmerking**

Er kunnen maximaal 50 gebruikersaccounts worden toegevoegd voor de clientsoftware.

Nadat de gebruikersaccount met succes is aangemaakt, wordt de gebruikersaccount toegevoegd aan de gebruikerslijst op de pagina Accountbeheer.

8. Optioneel: Voer de volgende handelingen uit nadat de gebruikersaccount is aangemaakt.

Gebruiker bewerken Klik op een gebruiker in de lijst om de gebruikersinformatie te bewerken.

 **Opmerking**

Alleen het wachtwoord van de supergebruiker kan worden gewijzigd.

Gebruiker verwijderen Selecteer de gebruiker in de lijst en klik op **Gebruiker verwijderen**.

 **Opmerking**

Je kunt de supergebruiker niet verwijderen.

20.2 Het wachtwoord van de gebruiker wijzigen

De beheerder kan het wachtwoord van normale gebruikers wijzigen zonder het oude wachtwoord in te voeren, terwijl de beheerder het oude wachtwoord moet invoeren wanneer hij het

wachtwoord van zichzelf wijzigt.

Voordat u begint

Gebruiker toevoegen aan de softwareclient.

Stappen

1. Ga naar de module Gebruikersbeheer.
2. Selecteer de gebruiker van wie het wachtwoord moet worden gewijzigd en klik op **Wijzigen**.
3. Optioneel: Voer het oude wachtwoord in.

Opmerking

Als je het wachtwoord van de beheerder wijzigt, moet je eerst het oude wachtwoord invoeren.

4. Voer het nieuwe wachtwoord in en bevestig het wachtwoord.
5. Klik op **OK**.

Hoofdstuk 21 Systeemconfiguratie

21.1 Algemene parameters instellen

U kunt de veelgebruikte parameters configureren, waaronder de tijd dat het logboek is verlopen, netwerkprestaties, enz.

Stappen

1. Ga naar de module Systeemconfiguratie.
2. Klik op het tabblad **Algemeen** om de pagina Algemene instellingen te openen.
3. Configureer de algemene parameters.

Datumformaat / Tijdformaat

De weergavestijl van datum en tijd op gerelateerde pagina's.

Bewaarperiode logboek

De tijd voor het bewaren van de logbestanden. Eenmaal overschreden, worden de bestanden verwijderd.

Maximale modus

Selecteer **Maximaliseren** of **Volledig scherm** als de maximale modus. De modus **Maximaliseren** kan het scherm maximaliseren en de taakbalk weergeven. De modus **Volledig scherm** kan de client op het volledige scherm weergeven.

Netwerkprestaties

Stel de netwerkomstandigheden in op **Normaal**, **Beter** of **Beste**.

Afbeeldingen opslaan in structuurgegevensformaat

- Nadat **Afbeelding opslaan in structuurgegevensformaat** is ingeschakeld, is de module **Geregistreerde afbeelding bij persoon verwijderen** beschikbaar. Als de informatie van een persoon met succes is toegepast op het/de apparaat/apparaten, wordt de foto van de persoon automatisch verwijderd en wordt er geen foto weergegeven in Basisinformatie. De kolom **Gezicht** in de module **Persoon** toont het nummer van de toegevoegde gezichtsfoto('s).
- Als **Foto's opslaan in structuurgegevensindeling** is ingeschakeld, worden er geen foto's weergegeven in het veld Gebeurtenisdetails in Evenementcentrum.

Toetsenbord en joystick inschakelen

Schakel het toetsenbord of de joystick in. Na het inschakelen kunt u de sneltoetsen voor het toetsenbord en de joystick instellen.

Opmerking

Raadpleeg [Toetsenbord- en joysticksnelkoppelingen instellen](#) voor meer informatie.

Informatie persoon exporteren

Als je dit inschakelt, wordt de knop **Exporteren** voor het exporteren van persoonsinformatie weergegeven op de pagina Persoonsbeheer. Let op de beveiliging van de persoonsinformatie.

Bewaarperiode gebeurtenissen

De bewaarperiode voor de gebeurtenisinformatie. Wanneer de bewaarperiode verstrijkt, wordt het gebeurtenisrecord automatisch verwijderd.

Automatische tijdsynchronisatie

Automatisch de tijd van de toegevoegde apparaten synchroniseren met de tijd van de pc waarop de client draait op een opgegeven tijdstip.

Apparaat automatisch upgraden

Stel de upgrademodus in nadat de nieuwe versie van het apparaat is gedetecteerd.

uitschakelen

Na het inschakelen zal de client het firmwarepakket niet downloaden en upgraden, zelfs als de client een nieuwe versie van de client detecteert.

Prompt Me If Downloaden en Upgraden

Nadat de client een nieuwe versie van het apparaat heeft gedetecteerd, zal hij de gebruiker vragen of hij het firmwarepakket wil downloaden en upgraden.

Downloaden en vraag me om een upgrade

Nadat de client de nieuwe versie van het apparaat heeft gedetecteerd, wordt het firmwarepakket automatisch gedownload en wordt de gebruiker gevraagd of hij de upgrade wil uitvoeren.

Automatisch downloaden en vragen

Nadat de client de nieuwe versie van de apparaten heeft gedetecteerd, wordt het firmwarepakket gedownload en wordt de nieuwe versie automatisch geüpgraded.

Je moet een schema instellen in het veld **Upgrade Time**, waarin de client de nieuwe versie automatisch upgradet.

Land/regio

Selecteer de regio van de server voor ABUS Link Station. U kunt de regio selecteren waartoe u behoort of de dichtstbijzijnde regio in de buurt.

4. Klik op **Opslaan**.

21.2 Liveweergave- en weergaveparameters instellen

U kunt de parameters voor liveweergave en afspelen instellen, waaronder het beeldformaat, de

duur van de voor-weergave, enz.

Stappen

1. Ga naar de module Systeemconfiguratie.
2. Klik op het tabblad **Liveweergave en Afspelen**.
3. Configureer de parameters voor liveweergave en afspelen.

Afbeeldingsformaat

Selecteer **JPEG** of **BMP** als het afbeeldingsformaat voor het opslaan van foto's.

Opmerking

Als de schakelaar **Temperatuur weergeven bij vastgelegde beelden** is ingesteld op ON, wordt JPEG standaard geselecteerd als het afbeeldingsformaat en kan dit niet worden gewijzigd.

Video-indeling

Selecteer **MP4/AVI** als het formaat van opgenomen video's.

Gedownloade videobestanden samenvoegen

Stel de maximale grootte van het samengevoegde videobestand in voor het downloaden van het videobestand op datum.

Zoek videobestanden opgeslagen in

Zoek de videobestanden die opgeslagen zijn op het lokale apparaat, op de opslagserver of zowel op de opslagserver als op het lokale apparaat om ze af te spelen.

Voorspelen voor

Stel de voorlooptijd in voor het afspelen van gebeurtenissen. Standaard is dit 30s.

Prioriteit geven aan het afspelen van videobestanden op de opslagserver

Speel bij voorkeur de videobestanden af die op de opslagserver zijn opgenomen. Speel anders de videobestanden af die zijn opgenomen op het lokale apparaat.

Laatste Live weergave hervatten na herstart

Hervat de laatste live-weergavestatus nadat je opnieuw inlogt op de client.

Achtergrondvideo's loskoppelen in enkele Live-weergave

In de modus voor verdelen in meerdere vensters dubbelklikt u op een live video om deze weer te geven in de modus voor verdelen in 1 venster, waarna de andere live video's worden gestopt om de bronnen te sparen.

Wiel inschakelen voor zoomen

Gebruik het muiswiel om in de PTZ-modus in of uit te zoomen op de video, of om in de digitale zoommodus in of uit te zoomen op de video. Op deze manier kun je direct in- of uitzoomen (of herstellen) op de live video door met de muis te scrollen.

Onbezorgde video overslaan tijdens afspelen VCA

Sla de onbezorgde video over tijdens VCA-weergave en de onbezorgde video wordt niet

afgespeeld tijdens VCA-weergave.

4. Klik op **Opslaan**.

21.3 Beeldparameters instellen

De beeldparameters van de client kunnen worden geconfigureerd, zoals weergaveschaal, afspeelprestaties, enz.

Stappen

1. Open de pagina Systeemconfiguratie.
2. Klik op het tabblad **Beeld** om de interface Beeldinstellingen te openen.
3. Configureer de beeldparameters.

Schaal bekijken

De weergaveschaal van de video in liveweergave of afspelen. Deze kan worden ingesteld als **Volledig scherm, 4:3, 16:9** of **Oorspronkelijke resolutie**.



Opmerking

U kunt de weergaveschaal ook instellen in de module Liveweergave. Raadpleeg [Liveweergave](#) voor meer informatie.

Spelen

De afspeelprestatie van de live video. Het kan worden ingesteld als **Kortste vertraging**, **Evenwichtig** of **Vloeiend**.

Je kunt ook **Custom (Aangepast)** selecteren en de framerate configureren volgens je eigen behoeften.

Hardwaredecodering Aanbevolen

Selecteer **D3D9** of **D3D11** om hardware decodering in te schakelen voor live weergave en afspelen. Hardwaredecodering kan zorgen voor betere decoderingsprestaties en lager CPU-gebruik bij het afspelen van HD-video tijdens liveweergave of afspelen.

Markering inschakelen

Markeer de gedetecteerde objecten met groene rechthoeken in liveweergave en afspelen.

Transactiegegevens weergeven

Geef de transactie-informatie weer op het livebeeld.

VCA-regel

Geef de VCA-regel weer in de live weergave.

Frame-extractie inschakelen voor afspelen op hoge snelheid

Bij het afspelen van de video op hoge snelheid (8x snelheid en hoger), kunt u deze functie uitschakelen om het beeld van het afspelen vloeiender te maken om de details te bekijken.

Het patroon van het doelwit weergeven

Nadat dit is ingeschakeld, kunt u het bewegingsspoor van de persoon in kwestie bekijken in het weergavevenster.

Overlay-regels op vastgelegd beeld

Stel voor het thermische apparaat in om de temperatuurinformatie en informatie over de vuurbron weer te geven op de vastgelegde beelden.

Opmerking

Nadat deze functie is ingeschakeld, wordt het afbeeldingsformaat dat is geconfigureerd in **Systeemconfiguratie** → **Liveweergave en -weergave** gewijzigd in JPEG en kan het niet worden bewerkt.

Ruisonderdrukking

Ruisonderdruktingsmodus, die kan worden ingesteld als **Disable**, **Self-adaptive** of **Enable**.

4. Klik op **Opslaan**.

21.4 Beeldopslag instellen

De foto's die worden gemaakt door de gebeurtenissen op de apparaten, kunnen worden opgeslagen op de pc waarop de ABUS CMS Service draait. U kunt de opslaglocatie van de beelden hier handmatig instellen.

Stappen



1. Ga naar de module Systeemconfiguratie.
2. Klik op **Gebeurtenisbeeldopslag**.
3. Zet de schakelaar **Afbeeldingen opslaan in server** op Aan.
Alle schijven van de pc waarop de ABUS CMS service draait worden weergegeven.
4. Selecteer de schijf om de foto's op te slaan.
5. Klik op **Opslaan**.

21.5 Alarmgeluid instellen

Wanneer de gebeurtenis wordt geactiveerd, kan de client een hoorbare waarschuwing geven om het beveiligingspersoneel te waarschuwen. Je kunt het geluid van de hoorbare waarschuwing in dit onderdeel instellen.

Stappen

1. Open de pagina Systeemconfiguratie.
2. Klik op het tabblad **Alarmgeluid** om de instellingenpagina voor het alarmgeluid te openen.
3. Optioneel: Klik op **...** en selecteer de audiobestanden van het lokale pad voor verschillende gebeurtenissen.
4. Optioneel: Aangepast alarmgeluid toevoegen.
 - 1) Klik op **Toevoegen** om een aangepast alarmgeluid toe te voegen.

- 2) Dubbelklik op het veld **Type** om de naam van het alarmgeluid naar wens aan te passen.
- 3) Klik op **...** en selecteer de audiobestanden van het lokale pad voor verschillende alarmen.
5. Optioneel: Klik op  voor een test van het audiobestand.
6. Optioneel: Klik op  in de kolom **Bewerking** om het aangepaste geluid te verwijderen.
7. Klik op **Opslaan**.

 **Opmerking**

Het formaat van het audiobestand kan alleen WAV zijn.

21.6 Parameters voor toegangscontrole en video-intercom instellen

U kunt de parameters voor toegangscontrole en video-intercom configureren volgens uw eigen behoeften.

Stappen

1. Open de pagina **Systeemconfiguratie**.
2. Klik op het tabblad **Toegangsbeheer & video-intercom**.
3. Voer de vereiste informatie in.

Beltoon

Klik en selecteer het audiobestand op het lokale pad voor de beltoon van het binnenstation. Optioneel kun je klikken voor een test van het audiobestand.

Max. Duur ring

Geef de seconden op die het belsignaal maximaal mag duren. De maximale belduur kan worden ingesteld tussen 15s en 60s.

Max. Spreekduur met binnenstation

Geef aan hoe lang het gesprek met het binnenstation maximaal mag duren. De maximale gespreksduur tussen het binnenstation en de client kan worden ingesteld tussen 120s en 600s.

Max. Spreekduur met deurintercom

Geef aan hoe lang het gesprek met het deurstation maximaal mag duren. De maximale gespreksduur tussen het deurstation en de client kan worden ingesteld van 90s tot 120s.

Max. Spreekduur met toegangscontrole


Geef de seconden op die het gesprek met het toegangscontroleapparaat maximaal mag duren. De maximale gespreksduur tussen het toegangscontroleapparaat en de client kan ingesteld worden tussen 90s en 120s.

4. Klik op **Opslaan**.

21.7 Pad voor bestandsopslag instellen

De videobeelden (handmatig opgenomen tijdens liveweergave en geclipt tijdens afspelen) en gemaakte foto's worden opgeslagen op de lokale pc. Het opslagpad van deze bestanden kan worden ingesteld.

Stappen

1. Open de pagina Systeemconfiguratie.
2. Klik op het tabblad **Bestand** om naar de pagina Instellingen bestandspad te gaan.
3. Klik op  en selecteer een lokaal pad voor de bestanden.
4. Klik op **Opslaan**.

21.8 Pictogrammen op werkbalk instellen

De pictogrammen en de volgorde op de werkbalk in de live-weergave en het afspeelvenster kunnen worden aangepast. U kunt instellen welke pictogrammen worden weergegeven en de pictogramvolgorde instellen.



Voer de volgende taak uit als u de pictogrammen op de werkbalk wilt instellen.

Stappen




1. Ga naar de module Systeemconfiguratie.
2. Klik op het tabblad **Werkbalk** om naar de pagina Werkbalkinstellingen te gaan.
3. Zet de schakelaar **Enable Screen Toolbar Display** op ON om de weergave van de werkbalk in de live-weergave en het afspeelvenster in te schakelen.
4. Klik op het gewenste pictogram om het weer te geven op de werkbalk.
5. Optioneel: Sleep het pictogram om de pictogramvolgorde bij weergave op de werkbalk in te stellen.

Tabel 21-1 Pictogrammen op de werkbalk Liveweergave

	Liveweergave stoppen	Stop de liveweergave in het weergavevenster.
	Vang	Leg het beeld vast in het liveweergaveproces. Het gemaakte beeld wordt opgeslagen op de PC.
	Opnemen	Start de handmatige opname. Het videobestand wordt opgeslagen op de pc.
	PTZ-besturing	Start de PTZ-modus voor speed dome. Klik en sleep in de weergave om de PTZ-bediening uit te voeren.
	Tweewegaudio	Start de tweewegaudio met het apparaat in liveweergave.
	Digitale zoom	Schakel de digitale zoomfunctie in. Klik nogmaals om de functie uit te schakelen.

	Direct afspeelen	Schakel over naar de modus voor onmiddellijk afspeelen.
	Configuratie op afstand	Open de externe configuratiepagina van de camera in liveweergave.

Tabel 21-2 Pictogrammen op de afspelerbalk

	Vang	Leg het beeld vast in het liveweergaveproces. Het gemaakte beeld wordt opgeslagen op de PC.
	Opnemen	Start de handmatige opname. Het videobestand wordt opgeslagen op de pc.
	Digitale zoom	Schakel de digitale zoomfunctie in. Klik nogmaals om de functie uit te schakelen.
	Downloaden	Download de videobestanden van de camera en de videobestanden worden opgeslagen op de PC.
	VCA afspeelen	Stel de VCA-regels in. Raadpleeg <u>VCA-weergave</u> voor meer informatie.
	Labelcontrole	Voeg standaard of aangepaste tags toe aan de videobestanden om het belangrijke videopunt te markeren. Je kunt de tag ook bewerken.

6. Klik op **Opslaan**.

21.9 Toetsenbord en joystick snelkoppelingen instellen

Het toetsenbord kan worden aangesloten op de client en worden gebruikt om de PTZ-camera's te bedienen. Je kunt sneltoetsen instellen voor het toetsenbord en de joystick om snel en gemakkelijk toegang te krijgen tot veelgebruikte acties.

Voer deze taak uit wanneer u sneltoetsen voor het toetsenbord en de joystick moet instellen.

Stappen

Opmerking

Deze configuratiepagina wordt weergegeven na het inschakelen van het toetsenbord en de joystick in Algemene instellingen. Raadpleeg **Algemene parameters instellen** voor meer informatie.

1. Ga naar de module **Systeemconfiguratie**.
2. Klik op **Toetsenbord en joystick** om het gebied Toetsenbord- en joystickinstellingen weer te geven.

3. Selecteer de COM-poort uit de vervolgkeuzelijst voor het toetsenbord als het toetsenbord is aangesloten op de pc waarop de client is geïnstalleerd.

Opmerking

Je kunt de Device Manager van de pc openen om de COM-poort te controleren waarop het toetsenbord is aangesloten.

4. Sneltoetsen voor toetsenbord en joystick instellen.
 - 1) Selecteer een bepaalde functienaam in de kolom Functie.
 - 2) Dubbelklik op het itemveld onder de kolom PC-toetsenbord, USB-joystick of USB-toetsenbord.
 - 3) Selecteer de samengestelde toetsbediening of het nummer in de vervolgkeuzelijst om deze in te stellen als snelkoppeling voor de functie van het toetsenbord of de USB-joystick.
5. Klik op **Opslaan**.

Voorbeeld

Voor de **Focus (+)** functie, als u **Home, 1** en **F1** instelt als de snelkoppelingen van het PC-toetsenbord, de USB-joystick en het USB-toetsenbord, kunt u op de Home-toets op het PC-toetsenbord drukken, de joystick in de 1 richting sturen of op de F1-toets op het USB-toetsenbord drukken om in te zoomen.

21.10 E-mailparameters instellen

Als een gebeurtenis wordt getriggerd en je kunt **E-mail verzenden** instellen als koppelingsactie voor deze gebeurtenis, dan stuurt de client een e-mail naar de ontvangers ter kennisgeving. Je moet de e-mailinstellingen instellen en de ontvangers in dit gedeelte opgeven.

Stappen

1. Ga naar de module Systeemconfiguratie.
2. Klik op het tabblad **Email** om de interface Email Settings te openen.
3. Voer de vereiste informatie in.

SMTP-server

Het IP-adres van de SMTP-server of de hostnaam (bijv. smtp.263xmail.com)

Type codering

Je kunt het keuzerondje aanvinken om **Niet-gecodeerd**, **SSL** of **STARTTLS** te selecteren.

Haven

Voer de communicatiepoort in die wordt gebruikt voor SMTP. De poort is standaard 25.

Adres afzender

Het e-mailadres van de afzender.

Beveiligingscertificaat (optioneel)

Als uw e-mailserver verificatie vereist, schakelt u dit selectievakje in om verificatie te

gebruiken om in te loggen op de server en de gebruikersnaam en het wachtwoord van uw e-mailaccount in te voeren.

Gebruikersnaam

Voer de gebruikersnaam van het e-mailadres van de afzender in als **Serververificatie** is aangevinkt.

Wachtwoord

Voer het wachtwoord van het e-mailadres van de afzender in als **Serverauthenticatie** is aangevinkt.

Ontvanger 1 tot 3

Voer het e-mailadres van de ontvanger in. Er kunnen maximaal 3 ontvangers worden ingesteld.

4. Optioneel: Klik op **Send Test Email (Test-e-mail verzenden)** om een e-mail te verzenden naar de ontvanger voor de test.
5. Klik op **Opslaan**.

21.11 Beveiligingsauthenticatie beheren

Voor de beveiliging van gegevens moet het beveiligingscertificaat van clients en toegevoegde servers hetzelfde zijn. Je kunt instellen of het verificatiecertificaat al dan niet vereist is bij het inschakelen van transmissiecodering met behulp van het TLS-protocol (Transport Layer Security).

Voordat je een server toevoegt aan de client, moet je het service certificaat van de client exporteren en importeren naar de server. Als meerdere clients dezelfde server gebruiken, moet je de beveiligingscertificaten van de clients en de server aan elkaar aanpassen.

21.11.1 Certificaat exporteren vanuit Servicebeheer

Je kunt het beveiligingscertificaat van de huidige clientservice exporteren en het geëxporteerde certificaatbestand importeren naar andere clients.

Stappen

1. Ga naar Servicebeheer.
2. Klik op **Exporteren** om het certificaatbestand op de lokale pc op te slaan.

Opmerking

Het certificaatbestand is in XML-formaat.

Wat nu te doen

Na het exporteren van het certificaat kun je het certificaat kopiëren naar de pc waarop de client is geïnstalleerd en importeren naar andere clients.

21.11.2 Certificaat importeren naar klant

Als er meerdere clients toegang hebben tot dezelfde steam media server, moet je hetzelfde certificaat importeren naar de clients en de server.

Voordat u begint

Zorg ervoor dat je het beveiligingscertificaat van een van de clientservices hebt geëxporteerd.

Opmerking

Raadpleeg [Certificaat exporteren vanuit Servicebeheer](#) voor meer informatie.

Stappen

1. Kopieer het certificaatbestand van de andere client naar de lokale pc.
 2. Ga naar de module **Systeemconfiguratie**.
 3. Klik op het tabblad **Beveiligingsauthenticatie om** de interface voor het instellen van de beveiligingsauthenticatie te openen.
 4. Klik op **Importeren**.
 5. Selecteer het certificaatbestand van uw lokale pc en klik op **Openen**.
-

Opmerking

Start de client opnieuw op om dit te activeren.

21.11.3 Certificaatverificatie voor transmissie-encryptie

Op de pagina Beveiligingsverificatie kunt u instellen of verificatie van het apparaatcertificaat al dan niet vereist is voor transmissiecodering.

Klik op **Systeemconfiguratie** → **Beveiligingsauthenticatie om** de interface voor beveiligingsauthenticatie te openen. Selecteer Certificaat verifiëren als **Ja** of **Nee**.

Ja


Je moet het apparaatcertificaat in de ontworpen map zetten als je transmissiecodering inschakelt bij het toevoegen van apparaten. Het apparaat zal worden toegevoegd met transmissiecodering en het certificaat zal worden geverifieerd, wat het beveiligingsniveau verbetert.

Geen

Het apparaatcertificaat is niet vereist als u transmissiecodering inschakelt bij het toevoegen van apparaten. Het apparaat wordt toegevoegd met transmissiecodering.

Hoofdstuk 22 Bediening en onderhoud

Je kunt onderhoudsbewerkingen uitvoeren in het menu voor een soepel en handig gebruik van de client.

Klik in de rechterbovenhoek van de client op  → **Bestand** → **Systeem** → **Gereedschap** en voer de volgende handelingen uit.

Logbestand openen

Je kunt een logbestand openen dat is opgeslagen op je lokale pc of logbestanden van de client.

Configuratiebestand importeren/exporteren

Indien nodig kun je configuratiebestanden importeren van de lokale pc naar de client en vice versa.

Auto back-up

Selecteer dag en tijd om een back-up te maken van configuratiebestanden en gegevens in de database, of om de geback-upte gegevens te herstellen.

Uitzending

Vink een of meer apparaten aan om de broadcastfunctie van de apparaten in te schakelen.

Batchwisserregeling

De wisser in batch in- of uitschakelen.

1 VS 1 Gezichtsvergelijking

Selecteer twee gezichtsfoto's van de lokale pc om te vergelijken. De gelijkenis tussen de twee

foto's wordt getoond.

Opmerking

Deze functie kan worden gebruikt voor identiteitsverificatie en moet worden ondersteund door het DeepinMind apparaat.

Batch tijd synchroniseren

Synchroniseer de tijd van geselecteerde apparaten met de tijd op je pc.

Berichtenwachtrij

Na het configureren van de e-mailkoppeling worden de getriggerde gebeurtenis(sen) hier weergegeven. Selecteer een gebeurtenis en annuleer het verzenden van een e-mail naar de ontvanger.

A. Aangepaste Wiegand-regelbeschrijvingen

Neem Wiegand 44 als voorbeeld, de instelwaarden op het tabblad Custom Wiegand zijn als volgt:

Aangepaste Wiegand-naam	Wiegand 44				
Totale lengte	44				
Transformatieregel (Decimaal cijfer)	byFormatRule[4]=[1][4][0][0]				
Pariteitsmodus	XOR Pariteit				
Oneven pariteit startbit		Lengte			
Even pariteit startbit		Lengte			
XOR pariteit startbit	0	Lengte per groep	4	Totale lengte	40
Beginbit kaart-ID	0	Lengte	32	Decimaal cijfer	10
Site Code Start Bit		Lengte		Decimaal cijfer	
OEM Startbit		Lengte		Decimaal cijfer	
Code fabrikant Start bit	32	Lengte	8	Decimaal cijfer	3

Wiegand-gegevens

Wiegand-gegevens = geldige gegevens + pariteitsgegevens

Totale lengte

Wiegand datalengte.

Transportregel

4 bytes. Geef de combinaties van geldige gegevens weer. Het voorbeeld toont de combinatie van kaart-ID en fabrikantcode. De geldige gegevens kunnen een enkele regel of een combinatie van meerdere regels zijn.

Pariteitsmodus

Geldige pariteit voor Wiegand-gegevens. Je kunt oneven pariteit of even pariteit selecteren.

Oneven pariteit startbit en lengte

Als je Oneven pariteit selecteert, zijn deze items beschikbaar. Als de startbit voor oneven pariteit 1 is en de lengte is 12, dan start het systeem de berekening van oneven pariteit vanaf bit 1. Het berekent dan 12 bits. Er worden 12 bits berekend. Het resultaat staat in bit 0. (Bit 0 is het eerste bit).

Even pariteit startbit en lengte

Als je Even Parity selecteert, zijn deze items beschikbaar. Als de even parity startbit 12 is en de lengte 12, dan start het systeem de even parity berekening vanaf bit 12. Het berekent dan 12 bits. Er worden 12 bits berekend. Het resultaat staat in het laatste bit.

XOR pariteit startbit, lengte per groep en totale lengte

Als je XOR Parity selecteert, zijn deze items beschikbaar. Volgens de bovenstaande tabel is het startbit 0, de lengte per groep is 4 en de totale lengte is 40. Dit betekent dat het systeem vanaf bit 0 rekt, elke 4 bits berekent en in totaal 40 bits berekent (10 groepen in totaal). Dit betekent dat het systeem rekt vanaf bit 0, elke 4 bits berekent en in totaal 40 bits berekent (10 groepen in totaal). Het resultaat zal in de laatste 4 bits zitten. (De lengte van het resultaat is hetzelfde als de lengte per groep).

Beginbit, lengte en decimaal cijfer van kaart-ID

Als je de transformatieregel gebruikt, zijn deze items beschikbaar. Volgens de bovenstaande tabel is de startbit van de kaart-ID 0, de lengte 32 en het decimale cijfer 10. Dit betekent dat er vanaf bit 0 32 bits zijn voor de kaart-ID. Dit betekent dat er vanaf bit 0 32 bits zijn voor de kaart-ID. (De lengte wordt hier per bit berekend.) En de lengte van het decimale cijfer is 10 bits.

Site Code Start Bit, Lengte en Decimaal Cijfer

Als je de transformatieregel gebruikt, zijn deze items beschikbaar. Voor gedetailleerde informatie, zie de uitleg van de kaart-ID.

OEM startbit, lengte en decimaal cijfer

Als je de transformatieregel gebruikt, zijn deze items beschikbaar. Voor gedetailleerde informatie, zie de uitleg van de kaart-ID.

Startbit, lengte en decimaal cijfer van de fabrikantcode

Als je de transformatieregel gebruikt, zijn deze items beschikbaar. Volgens de tabel hierboven is de startbit van de fabrikantcode 32, de lengte 8 en het decimale cijfer 3. Dit betekent dat er vanaf bit 32 8 bits fabrikantcode zijn. (De lengte wordt hier per bit berekend.) En de decimale lengte is 3.

D. Foutcode

Cod e	Fout Naam	Beschrijving
ABUS CMS		
317	Geen video's.	Dit wordt gevraagd als de gebruiker geen toestemming heeft om af te spelen.
HCNetSDK.dll		
1	Ongeldige gebruikersnaam of ongeldig wachtwoord.	
2	Geen toestemming.	De gebruiker in het apparaat heeft niet genoeg rechten.
4	Ongeldig kanaalnummer.	Dit wordt gevraagd in de live-weergave van schermbediening op afstand.
5	Er kunnen geen apparaten meer worden aangesloten.	
7	Verbinding met het apparaat mislukt.	
23	Niet ondersteund.	
29	Operatie mislukt.	
43	Geen buffer.	Dit wordt gevraagd wanneer een apparaat wordt toegevoegd en de apparaatpoort bezet is door een webserver.
55	Ongeldig IP-adres.	
56	Ongeldig MAC-adres.	
91	Het kanaal ondersteunt de bewerking niet.	Als het niet lukt om de substream te krijgen, wordt dit gevraagd.
96	Het apparaat is niet geregistreerd bij de DDNS.	
153	De gebruiker is vergrendeld.	
250	Het apparaat is niet geactiveerd.	
404	Channel No. fout of het apparaat ondersteunt de substream niet.	Dit wordt gevraagd als het niet lukt om de substream te krijgen of als de substream niet bestaat.

Cod e	Fout Naam	Beschrijving
424	De gegevens voor RTSP SETUP zijn niet ontvangen.	Dit wordt gevraagd bij het toevoegen van de liveweergave voor de software DVS via een extern netwerk.
800	Er kan geen bandbreedte meer worden gebruikt.	
Playctrl.dll		
2		De stream is geen video- en audiostream.
6		Het afspeelvenster wordt zwart bij het aannemen van H.265 in het 64-bits besturingssysteem.



Security Tech Germany

Brugervejledning V1.0 ABUS CMS Software

Indhold

Kapitel 3 Enhedsstyring	1
3.1 Aktivér enheder	1
3.2 Tilføj enhed	2
3.2.1 Tilføj en eller flere online-enheder	3
3.2.2 Tilføj enhed efter IP-adresse eller domænenavn	6
3.2.3 Tilføj enheder efter IP-segment	9
3.2.4 Importer enheder i en batch	12
3.3 Gendan/genindstil enhedens adgangskode	15
3.3.1 Nulstil enhedens adgangskode	15
3.3.2 Gendan enhedens standardadgangskode	16
3.4 Opgradering af enhedens firmwareversion	17
3.5 Administrer tilføjede enheder	18
3.6 Gruppeledelse	20
3.6.1 Gruppens ressourcer	20
3.6.2 Rediger ressourceparametre	21
Kapitel 4 ABUS Link Station	23
4.1 Registrer en ABUS Link Station-konto	23
4.2 Log ind på ABUS Link Station-konto	24
Kapitel 5 Livevisning	26
5.1 Live View-værktøjslinje	26
5.2 Tilføj brugerdefineret visning	27
5.3 Start Live View	28
5.4 Automatisk skift i Live View	30
5.4.1 Automatisk skift af kameraer i en gruppe	30
5.4.2 Automatisk omskiftning af alle kameraer	32
5.4.3 Automatisk skift af brugerdefinerede visninger	34
5.5 PTZ-styring	36
5.5.1 PTZ-kontrolpanel	36
5.5.2 Indstil forudindstilling, patrulje og mønster	39

5.6 Tilpas inddeling af vinduer	40
5.7 Manuel optagelse og indfangning	43
5.7.1 Optag video manuelt	43
5.7.2 Se lokale videoer	43
5.7.3 Optagelse af billeder	44
5.7.4 Vis optagede billeder	44
5.8 Øjeblikkelig afspilning	45
5.9 Livevisning til fiskeøjekameraer	46
5.9.1 Udfør Live View i Fisheye-tilstand	46
5.9.2 PTZ-styring i Fisheye-tilstand	48
5.9.3 Indstil en forudindstilling og patrulje	48
5.11 Livevisning til termisk kamera	49
5.11.1 Vis information om brandkilde under livevisning	49
5.11.2 Vis temperaturoplysninger på Live View-billedet	51
5.11.3 Manuel måling af temperatur	52
5.11.4 Vis skærmområde til detektering af brandkilder	53
5.13 Flere funktioner	54
Kapitel 6 Fjernafspilning	56
6.2 Konfiguration af fjernlager	56
6.2.1 Gem billede og video på DVR, NVR eller netværkskamera	56
6.2.3 Gem billede og yderligere oplysninger på lokal pc	58
6.2.4 Konfigurer skabelonen til optagelsesplanen	59
6.2.5 Konfigurer skabelonen til optagelsesplanen	60
6.3 Værktøjslinje til afspilning	61
6.4 Normal afspilning	62
6.4.1 Søg i videooptagelser	63
6.4.2 Afspil videooptagelser	65
6.5 Afspilning af alarmindgang	67
6.5.1 Søg i videooptagelser	67
6.5.2 Afspil videooptagelser	69
6.6 Afspilning af begivenheder	69

6.6.1 Søg i videooptagelser/billeder.....	70
6.6.2 Se videooptagelser/billeder.....	70
6.9 Afspilning af VCA.....	71
6.10 Synkron afspilning.....	73
6.11 Fisheye-kameraets videoafspilning.....	74
6.13 Download videooptagelser.....	76
6.13.1 Download videooptagelser efter dato.....	76
6.13.2 Download til flere kameraer.....	77
Kapitel 7 Hændelseskonfiguration.....	79
7.1 Konfigurer hændelse for kamera.....	79
7.2 Konfigurer hændelse for alarmindgang.....	81
7.3 Konfigurer hændelse for kodningsenhed.....	83
Kapitel 8 Eventcenter.....	85
8.1 Aktivér modtagelse af hændelser fra enheder.....	85
8.2 Visning af realtidshændelser.....	86
8.3 Søg i historiske begivenheder.....	88
8.4 Hent hændelser fra enheden.....	91
8.5 Vis information om pop op-begivenhed.....	92
Kapitel 9 Kortstyring.....	94
9.1 Tilføj kort.....	94
9.2 Rediger kortets skala.....	95
9.3 Kalibrering af længde- og breddegrader.....	96
9.4 Administrer Hot Spot.....	97
9.4.1 Tilføj kamera som hotspot.....	97
9.4.2 Tilføj alarmindgang som hotspot.....	98
9.4.3 Tilføj alarmudgang som hotspot.....	100
9.4.4 Tilføj zone som hotspot.....	101
9.4.5 Tilføj adgangspunkt som hotspot.....	103
Kapitel 10 Statistik.....	105
10.1.1 Rapport om optælling af personer efter kodningsenhed.....	105
10.2 Vis rapport om optælling af personer i vejkryds.....	109

10.4 Rapport om varmekort	110
10.7 Temperaturkort	112
Kapitel 11 Datahentning.....	114
11.1 Hentning af køretøj	114
Kapitel 14 Personaleledelse.....	115
14.1 Tilføj organisation	115
14.2 Tilføj enkeltperson	116
14.2.1 Konfigurer grundlæggende oplysninger	116
14.2.2 Udsted et kort til én person	118
14.2.3 Upload et ansigtsfoto fra lokal pc.....	121
14.2.4 Tag et billede via klienten	121
14.2.5 Indsaml ansigt via adgangskontrolenhed.....	122
14.2.10 Konfigurer oplysninger om adgangskontrol.....	123
14.2.11 Tilpas personoplysninger	125
14.2.12 Konfigurer beboeroplysninger	126
14.2.13 Konfigurer yderligere oplysninger	126
14.3 Import og eksport af personidentifikationsoplysninger	127
14.3.1 Oplysninger om importperson.....	127
14.3.2 Import af personbilleder	127
14.3.3 Oplysninger om eksportperson	128
14.3.4 Eksport af personbilleder	129
14.4 Hent personoplysninger fra adgangskontrolenheden	129
14.5 Flyt personer til en anden organisation	130
14.6 Udsted kort til personer i en batch.....	131
14.7 Tab af rapportkort	131
14.8 Vis ressourcestatistik	132
Kapitel 15 Adgangskontrol.....	133
15.2 Konfigurer tidsplan og skabelon	133
15.2.1 Tilføj ferie	133
15.2.2 Tilføj skabelon	134
15.3 Indstil adgangsgruppe for at tildele adgangsauctorisation til personer.....	135

15.4 Søg adgangsgruppe	138
15.5 Konfigurer avancerede funktioner	138
15.5.1 Konfigurer enhedens parametre	139
15.5.2 Konfigurer resterende ulåst/låst	147
15.5.3 Konfigurer multifaktorgodkendelse	149
15.5.4 Konfigurer brugerdefineret Wiegand-regel	151
15.5.5 Konfigurer kortlæserens godkendelsestilstand og tidsplan	152
15.5.6 Konfigurer person-godkendelsestilstand	154
15.5.8 Konfigurer første person i	155
15.5.9 Konfigurer anti-passback	156
15.5.10 Konfigurer låsning af flere døre	157
15.5.11 Konfigurer autentificeringskode	158
15.6.3 Indstilling af parametre for enhedsoptagelse	159
15.6.4 Indstil parametre for ansigtsgenkendelsesterminal	160
15.6.5 Aktivering af M1-kortkryptering	161
15.6.6 Indstil RS-485-parametre	162
15.6.7 Indstil Wiegand-parametre	162
15.7 Konfigurer linkage-handlinger til adgangskontrol	163
15.7.1 Konfigurer klienthandlinger for adgangshændelse	163
15.7.2 Konfigurer enhedens handlinger for adgangshændelse	164
15.7.3 Konfigurer enhedens handlinger for kortgennemføring	166
15.7.4 Konfigurer enhedens handlinger for person-id'et	167
15.8.1 Status for kontroldør	169
15.8.3 Tjek adgangsregistreringer i realtid	170
Kapitel 19 Logsøgning	172
Kapitel 20 Brugeradministration	173
20.1 Tilføj bruger	173
20.2 Skift brugerens adgangskode	174
Kapitel 21 Systemkonfiguration	175
21.1 Indstil generelle parametre	175
21.2 Indstilling af Live View- og afspilningsparametre	176

21.3 Indstil billedparametre.....	178
21.4 Indstil billedopbevaring	179
21.5 Indstil alarmlyd	179
21.6 Indstil parametre for adgangskontrol og videointercom	180
21.7 Indstil sti til lagring af filer	180
21.8 Indstil ikoner, der vises på værktøjslinjen.....	180
21.9 Indstil genveje til tastatur og joystick	182
21.10 Indstil e-mail-parametre	182
21.11 Administrer sikkerhedsgodkendelse	183
21.11.1 Eksportcertifikat fra Service Management	184
21.11.2 Importer certifikat til klient	184
21.11.3 Certifikatverifikation for transmissionskryptering	185
Kapitel 22 Drift og vedligeholdelse	186
A. Beskrivelser af brugerdefinerede Wiegand-regler	188
D. Fejlkode.....	190

Kapitel 3 Enhedsstyring

3.1 Aktivér enheder

For de inaktive enheder skal du oprette en adgangskode for at aktivere dem, før de kan føjes til softwaren og fungere korrekt.

Før du går i gang

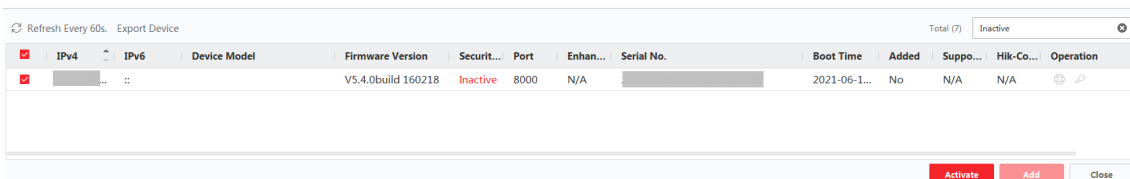
Sørg for, at den enhed, der skal aktiveres, er forbundet til netværket og på samme subnet som den pc, hvor klienten kører.

Trin

Bemærk

Denne funktion skal understøttes af enheden.

1. Gå ind på siden Device Management.
2. Klik på **Enhed** øverst i højre panel.
3. Klik på **Online Device** for at få vist listen over online-enheder nederst på siden.
De søgte online-enheder vises på listen.
4. Tjek enhedens status (vist i kolonnen **Sikkerhedsniveau**), og vælg en inaktiv enhed.



IPv4	IPv6	Device Model	Firmware Version	Securit...	Port	Enhanc...	Serial No.	Boot Time	Added	Suppo...	Hik-Co...	Operation
...	::		V5.4.0build 160218	Inactive	8000	N/A		2021-06-1...	No	N/A	N/A	

Buttons: Activate, Add, Close

Figur 3-1 Online inaktive enheder

5. Klik på **Aktivér** for at åbne aktiveringsdialogen.
6. Opret en adgangskode i adgangskodefeltet, og bekræft adgangskoden.

Forsigtig

Styrken af enhedens adgangskode kan kontrolleres automatisk. Vi anbefaler på det kraftigste, at du ændrer den adgangskode, du selv vælger (med mindst 8 tegn, herunder mindst tre slags af følgende kategorier: store bogstaver, små bogstaver, tal og specialtegn) for at øge sikkerheden for dit produkt. Og vi anbefaler, at du ændrer din adgangskode regelmæssigt, især i højsikkerhedssystemet, hvor en månedlig eller ugentlig ændring af adgangskoden kan beskytte dit produkt bedre.

Korrekt konfiguration af alle adgangskoder og andre sikkerhedsindstillinger er installatørens og/eller slutbrugers ansvar.


Bemærk

For NVR-enheden skal du oprette en adgangskode i feltet **Standardadgangskode for netværkskameraer** og bekræfte adgangskoden for at aktivere netværkskameraer, der er tilsluttet NVR'en.

7. Valgfrit: Aktivér ABUS Link Station-tjenesten, når du aktiverer enheden, hvis enheden understøtter det.
 - 1) Markér **Enable Cloud P2P** for at åbne dialogboksen Note.
 - 2) Opret en verifikationskode, og bekræft verifikationskoden.
 - 3) Klik på **Terms of Service** og **Privacy Policy** for at læse kravene.
 - 4) Klik på **OK** for at aktivere ABUS Link Station-tjenesten.
 8. Klik på **OK** for at aktivere enheden.
-

Bemærk

Hvis enheden understøtter nulstilling af adgangskoden via den reservede e-mail, sikkerhedsspørgsmål eller GUID, kan du konfigurere dem efter aktivering af enheden.

9. Valgfrit: Klik på  i kolonnen Operation for at redigere netværksoplysningerne (herunder IP-adresse, portnummer, gateway osv.) for online-enheden.

3.2 Tilføj enhed

Klienten tilbyder forskellige måder at tilføje enheder på, herunder IP/domæne, IP-segment, ABUS Link Station. Klienten understøtter også import af flere enheder i en batch, når der skal tilføjes en

stor mængde enheder.

3.2.1 Tilføj en eller flere online-enheder

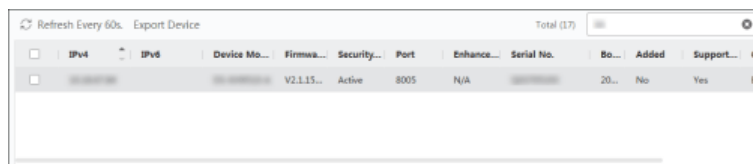
Klienten kan registrere online-enheder, som er på samme netværk som den pc, der kører klienten. Du kan vælge en registreret onlineenhed, der vises på listen over onlineenheder, og tilføje den til klienten. For registrerede online-enheder, der deler samme brugernavn og adgangskode, kan du tilføje dem til klienten i en batch.

Før du går i gang

- Den eller de enheder, der skal tilføjes, er på samme netværk som den pc, der kører klienten.
- Den eller de enheder, der skal tilføjes, er blevet aktiveret.

Trin

1. Klik på **Enhedsstyring** → **Enhed** → **Enhed**.
2. Klik på **Online Device** for at vise online-enhedsområdet.
De søgte online-enheder vises på listen.



	IPV4	IPV6	Device Mo...	Firma...	Security...	Port	Enhance...	Serial No.	Bo...	Added	Support...
<input type="checkbox"/>			V2.1.15...	Active	8005	N/A	Serial No.	20...	No	Yes	Er

Figur 3-2 Online-enhed

3. I området **Online Device** skal du markere en eller flere online-enheder og klikke på **Add for** at åbne vinduet til tilføjelse af enheder.

The 'Add' dialog box contains the following fields and options:

- Name:
- IP Address:
- Transmission Encryptio...:
- Port:
- User Name:
- Password:
- Synchronize Time:
- Import to Group:

Set the device name as the group name and add all the channels connected to the device to the group.

Add

Figur 3-3 Tilføj en enkelt online-enhed

The 'Add' dialog box contains the following fields and options:

- User Name:
- Password:
- Synchronize Time:
- Import to Group:

Set the device name as the group name and add all the channels connected to the device to the group.

Add

Figur 3-4 Tilføj flere online-enheder

4. Indtast de nødvendige oplysninger.

Navn

Indtast et beskrivende navn til enheden.

IP-adresse

Indtast enhedens IP-adresse. Enhedens IP-adresse indhentes automatisk i denne tilføjeelsestilstand.

Havn

Du kan tilpasse portnummeret. Enhedens portnummer hentes automatisk i denne tilføjeelsestilstand.

Bemærk

For nogle enhedstyper kan du indtaste **80** som portnummer. Denne funktion skal understøttes af enheden.

Brugernavn

Som standard er brugernavnet **admin** for TVVR/HDCC/NVR og **installer** for IPC'er.

Adgangskode

Indtast enhedens adgangskode.

Forsigtig

Styrken af enhedens adgangskode kan kontrolleres automatisk. Vi anbefaler på det kraftigste, at du ændrer adgangskoden efter eget valg (med mindst 8 tegn, herunder mindst tre slags af følgende kategorier: store bogstaver, små bogstaver, tal og specialtegn) for at øge sikkerheden for dit produkt. Og vi anbefaler, at du ændrer din adgangskode regelmæssigt, især i højsikkerhedssystemet, hvor en månedlig eller ugentlig ændring af adgangskoden kan beskytte dit produkt bedre.

Korrekt konfiguration af alle adgangskoder og andre sikkerhedsindstillinger er installatørens og/eller slutbrugerens ansvar.

5. Det er valgfrit: Markér **Transmission Encryption (TLS)** for at aktivere transmissionskryptering ved hjælp af TLS-protokollen (Transport Layer Security) af sikkerhedshensyn.

Bemærk

- Denne funktion skal understøttes af enheden.
 - Hvis du har aktiveret Certificate Verification, skal du klikke på **Open Certificate Directory** for at åbne standardmappen og kopiere certifikatfilen, der er eksporteret fra enheden, til denne standardmappe for at styrke sikkerheden. Se [Certifikatbekræftelse for transmissionskryptering](#) for detaljer om aktivering af certifikatbekræftelse.
 - Du kan logge ind på enheden for at hente certifikatfilen via en webbrowser.
-

6. Markér **Synkroniser tid** for at synkronisere enhedens tid med den pc, der kører klienten, efter at enheden er tilføjet til klienten.
7. Valgfrit: Marker **Import to Group** for at oprette en gruppe efter enhedens navn og importere alle enhedens kanaler til denne gruppe.

Eksempel

For en kodningsenhed vil dens kodningskanaler og alarmindgange/udgange blive importeret til

denne gruppe.

For adgangskontrolenheder importeres deres adgangspunkter, alarmindgange/udgange og kodningskanaler (hvis de findes) til denne gruppe.

8. Klik på **Tilføj**.

9. Valgfrit: Klik på **Eksporter enhed**, vælg lagringssti og enhedstype, og klik på **OK** for at eksportere enhedsoplysningerne til din pc.



Bemærk

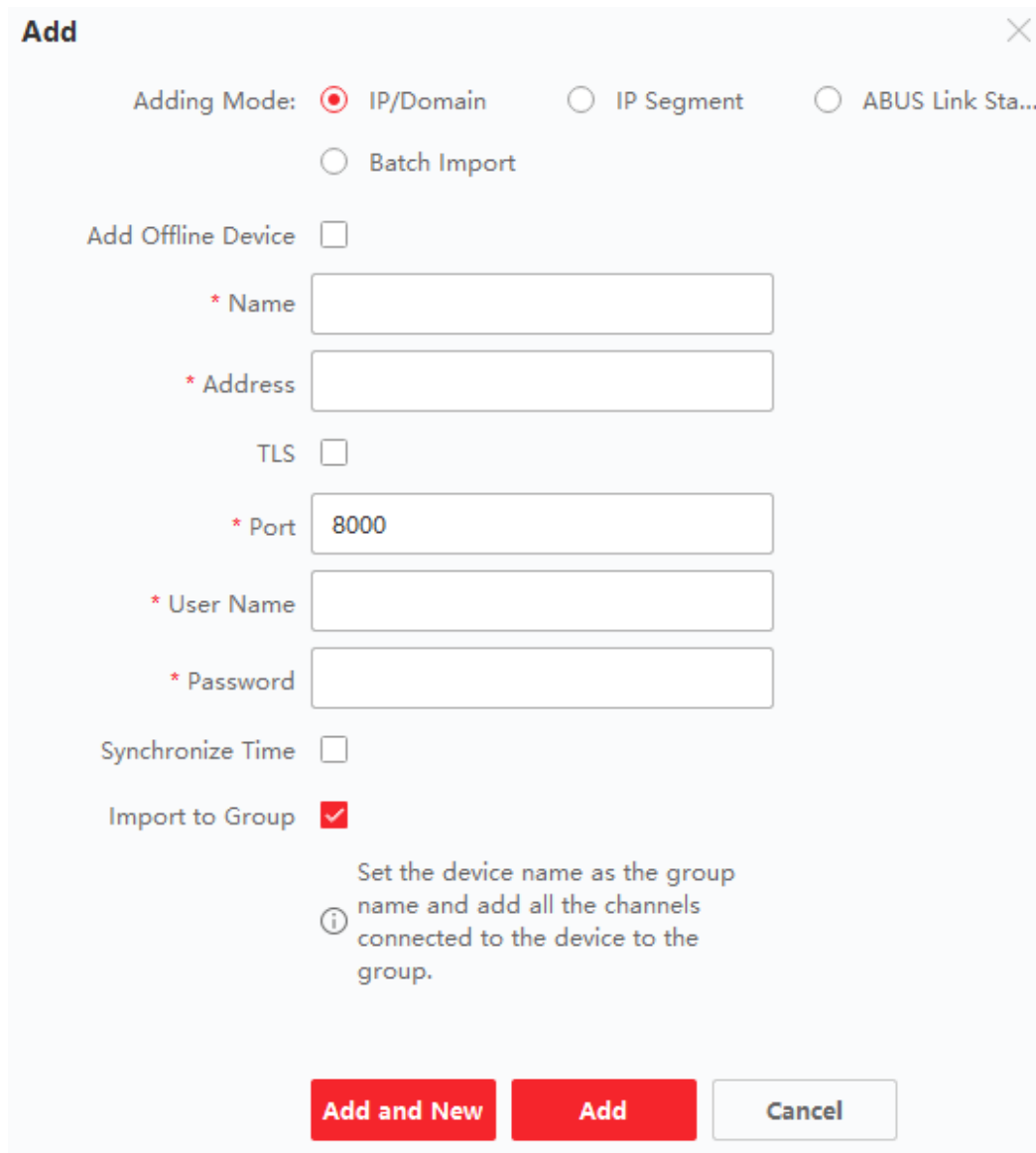
I øjeblikket understøtter platformen kun eksport af oplysninger om videointercom-enheder, herunder dørstationer, indendørs stationer og hovedstationer.

3.2.2 Tilføj enhed efter IP-adresse eller domænenavn

Hvis du kender IP-adressen eller domænenavnet på den enhed, der skal tilføjes, kan du tilføje enheder til klienten ved at angive IP-adressen (eller domænenavnet), brugernavnet, adgangskoden osv.

Trin

1. Gå ind i Device Management-modulet.
2. Klik på fanen **Enhed** øverst i højre panel.
De tilføjede enheder vises i højre panel.



Add

Adding Mode: IP/Domain IP Segment ABUS Link Sta...

Batch Import

Add Offline Device

* Name

* Address

TLS

* Port

* User Name

* Password

Synchronize Time

Import to Group

Set the device name as the group name and add all the channels connected to the device to the group.

Add and New **Add** Cancel

Figur 3-5 Tilføj enhed efter IP-adresse eller domænenavn

3. Klik på **Add** for at åbne vinduet Add, og vælg derefter **IP/Domain** som tilføjelestilstand.
4. Indtast de nødvendige oplysninger.

Navn

Opret et beskrivende navn til enheden. Du kan f.eks. bruge et kaldenavn, der kan vise enhedens placering eller funktion.

Adresse

Enhedens IP-adresse eller domænenavn.

Havn

De enheder, der skal tilføjes, har samme portnummer. Standardværdien er **8000**.

Bemærk

For nogle enhedstyper kan du indtaste **80** som portnummer. Denne funktion skal understøttes af enheden.

Brugernavn

Indtast enhedens brugernavn. Som standard er brugernavnet **admin**.

Adgangskode

Indtast enhedens adgangskode.

Forsigtig

Styrken af enhedens adgangskode kan kontrolleres automatisk. Vi anbefaler på det kraftigste, at du ændrer adgangskoden efter eget valg (med mindst 8 tegn, herunder mindst tre slags af følgende kategorier: store bogstaver, små bogstaver, tal og specialtegn) for at øge sikkerheden for dit produkt. Og vi anbefaler, at du ændrer din adgangskode regelmæssigt, især i højsikkerhedssystemet, hvor en månedlig eller ugentlig ændring af adgangskoden kan beskytte dit produkt bedre.

Korrekt konfiguration af alle adgangskoder og andre sikkerhedsindstillinger er installatørens og/eller slutbrugerens ansvar.

5. Det er valgfrit: Tilføj offline-enhederne.

- 1) Markér **Tilføj offline-enhed**.
 - 2) Indtast de nødvendige oplysninger, herunder enhedens kanalnummer og alarmindgangsnummer.
-

Bemærk

Når du har tilføjet offline-enheden til klienten, vises enhedens netværksstatus som "Offline"; Når enheden kommer online, skifter enhedens netværksstatus til "Online", og klienten forbinder den automatisk.

6. Det er valgfrit: Markér **Transmission Encryption (TLS)** for at aktivere transmissionskryptering ved hjælp af TLS-protokollen (Transport Layer Security) af sikkerhedshensyn.

Bemærk

- Denne funktion skal understøttes af enheden.
 - Hvis du har aktiveret Certificate Verification, skal du klikke på **Open Certificate Directory** for at åbne standardmappen og kopiere certifikatfilen, der er eksporteret fra enheden, til denne standardmappe for at styrke sikkerheden. Se **Certificate Verification for Transmission Encryption** for detaljer om aktivering af certifikatverifikation.
 - Du kan logge ind på enheden for at hente certifikatfilen via en webbrowser.
-

7. Markér **Synkroniser tid** for at synkronisere enhedens tid med den pc, der kører klienten, efter at enheden er tilføjet til klienten.

8. Valgfrit: Marker **Import to Group** for at oprette en gruppe efter enhedens navn og importere alle enhedens kanaler til denne gruppe.

Eksempel







For en kodningsenhed vil dens kodningskanaler og alarmindgange/udgange blive importeret til denne gruppe.

For adgangskontrolenheder vil adgangspunkter, alarmindgange/-udgange og kodningskanaler (hvis de findes) blive importeret til denne gruppe.

9. Afslut tilføjjelsen af enheden.

- Klik på **Tilføj** for at tilføje enheden og vende tilbage til siden med enhedslisten.
- Klik på **Tilføj og Ny** for at gemme indstillingerne og fortsætte med at tilføje andre enheder.

10. Valgfrit: Udfør følgende handling(er).

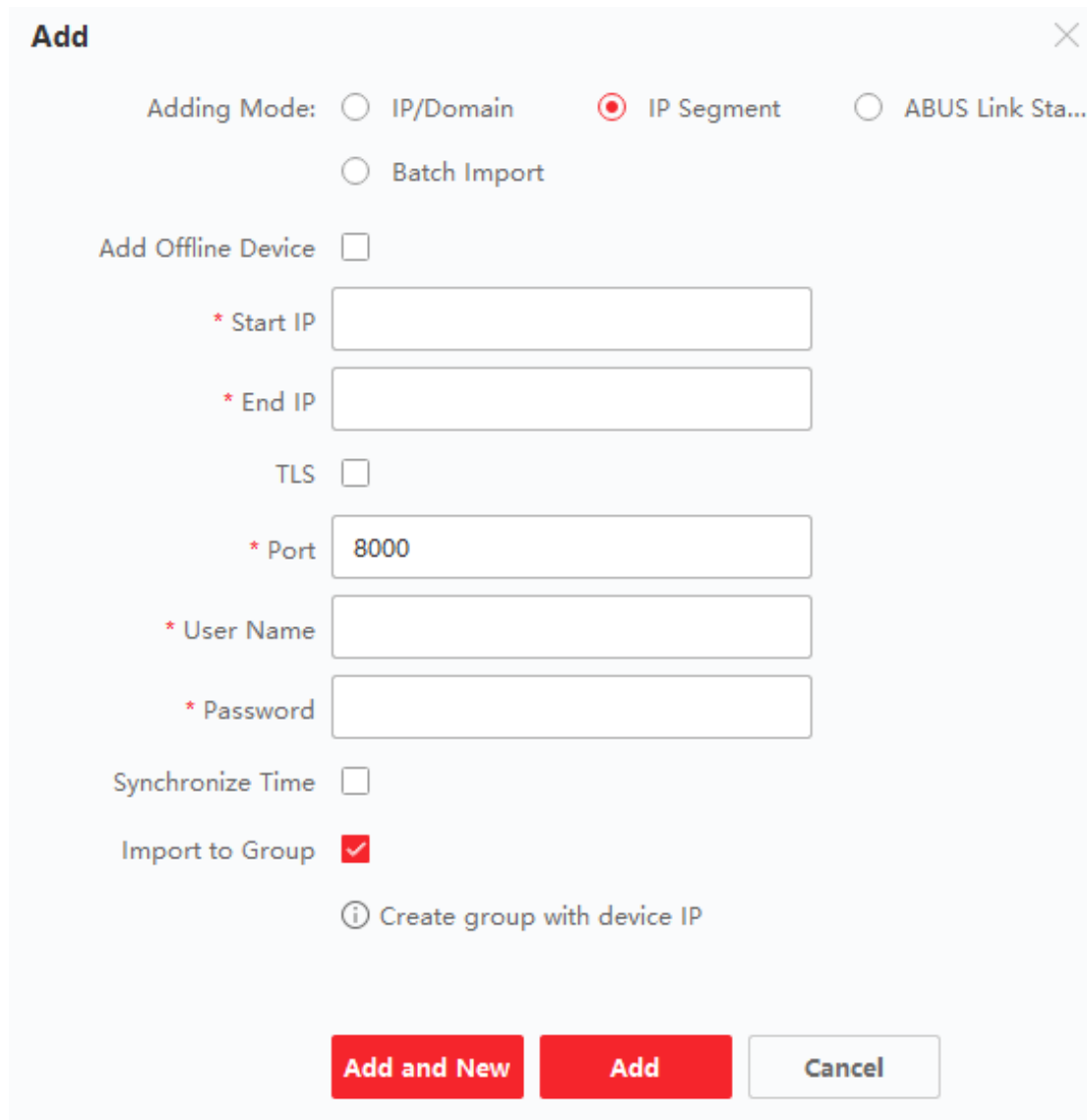
Fjernkonfiguration	På enhedslistesiden skal du klikke på  i kolonnen Operation for at udføre fjernkonfiguration af en enhed.  er i kolonnen længst til højre på enhedssiden. For detaljer henvises til enhedens brugervejledning.
Enhedsstatus	Klik på  i kolonnen Operation for at se enhedens status, herunder kameraer, optagestatus, signalstatus, hardwarestatus osv.
Rediger oplysninger om enheden	Klik på  i kolonnen Operation for at redigere enhedens oplysninger, såsom IP-adresse, brugernavn og adgangskode.
Tjek online bruger	Klik på  i kolonnen Operation for at tjekke de onlinebrugere, der har adgang til enheden, såsom brugernavn, brugertype, brugerens IP-adresse og login-tid.
Opfrisk	Klik på  i kolonnen Operation for at få de seneste oplysninger om enheden.
Slet enhed	Vælg en eller flere enheder, og klik på Slet for at slette de(n) valgte enhed(er) fra klienten.

3.2.3 Tilføj enheder efter IP-segment

Hvis enhederne har samme portnummer, brugernavn og adgangskode, og deres IP-adresser ligger i samme IP-segment, kan du tilføje dem til klienten ved at angive start-IP-adresse og slut-IP-adresse, portnummer, brugernavn, adgangskode osv. for enhederne.

Trin

1. Klik på **Device** Management på panelet Maintenance and Management i højre side af klienten.
2. Klik på fanen **Enhed** øverst i venstre panel.
De tilføjede enheder vises i højre panel.
3. Klik på **Tilføj** for at åbne vinduet Tilføj.



Add ×

Adding Mode: IP/Domain IP Segment ABUS Link Sta...

Batch Import

Add Offline Device

* Start IP

* End IP

TLS

* Port

* User Name

* Password

Synchronize Time

Import to Group

ⓘ Create group with device IP

Add and New **Add** Cancel

Figur 3-6 Tilføj enhed efter IP-segment

4. Vælg **IP-segment** som tilføje tilstand.
5. Indtast de nødvendige oplysninger.

Start IP

Indtast en start-IP-adresse.

Slut IP

Indtast en slut-IP-adresse i det samme netværkssegment som start-IP'en.

Havn

Indtast enhedens portnummer. Standardværdien er **8000**.

Bemærk

For nogle enhedstyper kan du indtaste **80** som portnummer. Denne funktion skal understøttes af enheden.

Brugernavn

Som standard er brugernavnet **admin**.

Adgangskode

Indtast enhedens adgangskode.

Forsigtig

Styrken af enhedens adgangskode kan kontrolleres automatisk. Vi anbefaler på det kraftigste, at du ændrer adgangskoden efter eget valg (med mindst 8 tegn, herunder mindst tre slags af følgende kategorier: store bogstaver, små bogstaver, tal og specialtegn) for at øge sikkerheden for dit produkt. Og vi anbefaler, at du ændrer din adgangskode regelmæssigt, især i højsikkerhedssystemet, hvor en månedlig eller ugentlig ændring af adgangskoden kan beskytte dit produkt bedre.

Korrekt konfiguration af alle adgangskoder og andre sikkerhedsindstillinger er installatørens og/eller slutbrugerens ansvar.

6. Det er valgfrit: Tilføj offline-enhederne.

- 1) Markér **Tilføj offline-enhed**.
 - 2) Indtast de nødvendige oplysninger, herunder enhedens kanalnummer og alarmindgangsnummer.
-

Bemærk

Når du har tilføjet offline-enheden til klienten, vises enhedens netværksstatus som "Offline"; Når enheden kommer online, skifter enhedens netværksstatus til "Online", og klienten forbinder den automatisk.

7. Det er valgfrit: Markér **Transmission Encryption (TLS)** for at aktivere transmissionskryptering ved hjælp af TLS-protokollen (Transport Layer Security) af sikkerhedshensyn.

Bemærk

- Denne funktion skal understøttes af enheden.
 - Hvis du har aktiveret certifikatverificering, skal du klikke på **Åbn certifikatmappe** for at åbne standardmappen og kopiere certifikatfilen, der er eksporteret fra enheden, til denne standardmappe for at styrke sikkerheden. Se **Certificate Verification for Transmission Encryption** for detaljer om aktivering af certifikatverifikation.
 - Du kan logge ind på enheden for at hente certifikatfilen via en webbrowser.
-







8. Markér **Synkroniser tid** for at synkronisere enhedens tid med den pc, der kører klienten, efter at enheden er tilføjet til klienten.

9. Valgfrit: Marker **Import to Group** for at oprette en gruppe efter enhedens navn og importere alle enhedens kanaler til gruppen.

10. Afslut tilføjelsen af enheden.

- Klik på **Tilføj** for at tilføje enheden og vende tilbage til siden med enhedslisten.
- Klik på **Tilføj og Ny** for at gemme indstillingerne og fortsætte med at tilføje andre enheder.

11. Valgfrit: Udfør følgende handling(er).

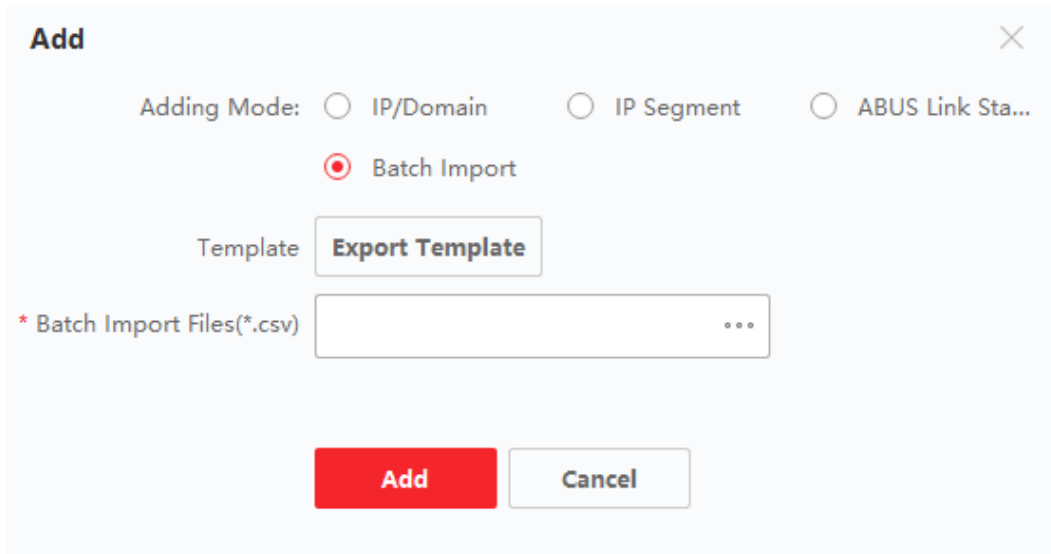
Fjernkonfiguration	På enhedslistesiden skal du klikke på  i kolonnen Operation for at udføre fjernkonfiguration af en enhed.  er i kolonnen længst til højre på enhedssiden. For detaljer henvises til enhedens brugervejledning.
Enhedsstatus	Klik på  i kolonnen Operation for at se enhedens status, herunder kameraer, optagestatus, signalstatus, hardwarestatus osv.
Rediger oplysninger om enheden	Klik på  i kolonnen Operation for at redigere enhedens oplysninger, såsom IP-adresse, brugernavn og adgangskode.
Tjek online bruger	Klik på  i kolonnen Operation for at tjekke de onlinebrugere, der har adgang til enheden, såsom brugernavn, brugertype, brugerens IP-adresse og login-tid.
Opfrisk	Klik på  i kolonnen Operation for at få de seneste oplysninger om enheden.
Slet enhed	Vælg en eller flere enheder, og klik på Slet for at slette de(n) valgte enhed(er) fra klienten.

3.2.4 Importer enheder i en batch

Du kan tilføje flere enheder til klienten i en batch ved at indtaste enhedsparametrene i en foruddefineret CSV-fil.

Trin

1. Gå ind i Device Management-modulet.
2. Klik på fanen **Enhed** øverst i højre panel.
3. Klik på **Add** for at åbne vinduet Add, og vælg derefter **Batch Import** som tilføjelsestilstand.



Figur 3-7 Tilføj enheder i en batch

4. Klik på **Eksporter skabelon**, og gem derefter den foruddefinerede skabelon (CSV-fil) på din pc.
5. Åbn den eksporterede skabelonfil, og indtast de nødvendige oplysninger om de enheder, der skal tilføjes, i den tilsvarende kolonne.

Bemærk

For en detaljeret beskrivelse af de påkrævede felter henvises til introduktionerne i skabelonen.

Tilføjelse af tilstand

Indtast **0** eller **1** eller **2**.

Adresse

Rediger enhedens adresse.

Havn

Indtast enhedens portnummer. Standardportnummeret er **8000**.

Brugernavn

Indtast enhedens brugernavn. Som standard er brugernavnet **admin**.

Adgangskode

Indtast enhedens adgangskode.

Forsigtig

Styrken af enhedens adgangskode kan kontrolleres automatisk. Vi anbefaler på det kraftigste, at du ændrer adgangskoden efter eget valg (med mindst 8 tegn, herunder mindst tre slags af følgende kategorier: store bogstaver, små bogstaver, tal og specialtegn) for at øge sikkerheden for dit produkt. Og vi anbefaler, at du ændrer din adgangskode regelmæssigt, især i højsikkerhedssystemet, hvor en månedlig eller ugentlig ændring af adgangskoden kan beskytte dit produkt bedre.

Korrekt konfiguration af alle adgangskoder og andre sikkerhedsindstillinger er installatørens og/eller slutbrugerens ansvar.

Tilføj offline-enhed

Indtast **1** for at aktivere tilføjelse af en offline-enhed.

Når du har tilføjet offline-enheden til klienten, vises enhedens netværksstatus som "Offline"; Når enheden kommer online, skifter enhedens netværksstatus til "Online", og klienten forbinder den automatisk. Indtast **0** for at deaktivere tilføjelse af en offline-enhed.

Import til gruppe


Indtast **1** for at oprette en gruppe med enhedens navn. Alle enhedens kanaler vil som standard blive importeret til den tilsvarende gruppe. Indtast **0** for at deaktivere denne funktion.






Kanalnummer


Hvis du aktiverer **Tilføj offline-enhed**, skal du indtaste enhedens kanalnummer. Hvis du deaktiverer **Tilføj offline-enhed**, er dette felt ikke påkrævet.

Nummer på alarmindgang

Hvis du aktiverer **Tilføj offline-enhed**, skal du indtaste enhedens alarmindgangsnummer. Hvis du deaktiverer **Tilføj offline-enhed**, er dette felt ikke påkrævet.

6. Klik på  , og vælg skabelonfilen.
7. Klik på **Tilføj** for at importere enhederne.
8. Valgfrit: Udfør følgende handling(er).

Fjernkonfiguration	På enhedslistesiden skal du klikke på  i kolonnen Operation for at udføre fjernkonfiguration af en enhed.  er i kolonnen længst til højre på enhedssiden. For detaljer henvises til enhedens brugervejledning.
Enhedsstatus	Klik på  i kolonnen Operation for at se enhedens status, herunder kameraer, optagestatus, signalstatus, hardwarestatus osv.
Rediger oplysninger om enheden	Klik på  i kolonnen Operation for at redigere enhedens oplysninger, såsom IP-adresse, brugernavn og adgangskode.
Tjek online bruger	Klik på  i kolonnen Operation for at tjekke de onlinebrugere, der har adgang til enheden, såsom brugernavn, brugertype, brugerens IP-

	adresse og login-tid.
Opdatering	Klik på  i kolonnen Operation for at få de seneste oplysninger om enheden.
Slet enhed	Vælg en eller flere enheder, og klik på Slet for at slette de(n) valgte enhed(er) fra klienten.


3.3 Gendan/genindstil enhedens adgangskode

Hvis du har glemt adgangskoden til de registrerede online-enheder, kan du gendanne enhedens standardadgangskode eller nulstille enhedens adgangskode via klienten.

3.3.1 Nulstil enhedens adgangskode

Hvis du har glemt adgangskoden til de registrerede online-enheder, kan du nulstille enhedens adgangskode via klienten.

Trin

1. Gå ind på siden Device Management.
2. Klik på fanen **Enhed** øverst i højre panel.
3. Klik på **Online Device** for at vise online-enhedsområdet.
Alle online-enheder, der deler det samme subnet, vises på listen.
4. Vælg enheden fra listen, og klik på  i kolonnen Operation.
5. Nulstil enhedens adgangskode.
 - Klik på **Export** for at gemme enhedsfilen på din pc, og send derefter filen til vores tekniske support.

Bemærk

Kontakt vores tekniske support for at få hjælp til at nulstille adgangskoden.

- Klik på **Generate** for at åbne QR-kodevinduet, og klik på **Download** for at gemme QR-koden på din pc. Du kan også tage et billede af QR-koden for at gemme den på din telefon. Send billedet til vores tekniske support.

Bemærk

Kontakt vores tekniske support for at få hjælp til at nulstille adgangskoden.

- Vælg fejlsikret tilstand efter de faktiske behov.

Bemærk

Kontakt vores tekniske support for at få hjælp til at nulstille adgangskoden.

Forsigtig


Styrken af enhedens adgangskode kan kontrolleres automatisk. Vi anbefaler på det kraftigste, at du ændrer adgangskoden efter eget valg (med mindst 8 tegn, herunder mindst tre slags af følgende kategorier: store bogstaver, små bogstaver, tal og specialtegn) for at øge sikkerheden for dit produkt. Og vi anbefaler, at du ændrer din adgangskode regelmæssigt, især i højsikkerhedssystemet, hvor en månedlig eller ugentlig ændring af adgangskoden kan beskytte dit produkt bedre.

Korrekt konfiguration af alle adgangskoder og andre sikkerhedsindstillinger er installatørens og/eller slutbrugers ansvar.

3.3.2 Gendan enhedens standardadgangskode

Hvis du glemmer adgangskoden til de registrerede online-enheder, kan du gendanne deres standardadgangskode via klienten.

Trin

1. Gå ind på siden Device Management.
2. Klik på fanen **Enhed** øverst i højre panel.
3. Klik på **Online Device** for at vise online-enhedsområdet nederst på siden.
Alle online-enheder, der deler det samme subnet, vises på listen.
4. Vælg en enhed, og klik på  i kolonnen Operation for at åbne vinduet Reset Password.
5. Gendan enhedens adgangskode.
 - Indtast sikkerhedskoden, og derefter kan du gendanne standardadgangskoden for den valgte enhed.

Bemærk

Kontakt vores tekniske support for at få sikkerhedskoden.

- Klik på **Export** for at gemme enhedsfilen på din pc og sende filen til vores tekniske support.
-

Bemærk

Kontakt vores tekniske support for at få hjælp til at nulstille adgangskoden.

Hvad du skal gøre nu

Standardadgangskoden (12345) til administratorkontoen er kun til førstegangslogin. Du skal ændre denne standardadgangskode for bedre at beskytte mod sikkerhedsrisici, såsom andres uautoriserede adgang til produktet, der kan forhindre produktet i at fungere korrekt og/eller føre til andre uønskede konsekvenser.



Forsigtig

Styrken af enhedens adgangskode kan kontrolleres automatisk. Vi anbefaler på det kraftigste, at du ændrer den adgangskode, du selv vælger (med mindst 8 tegn, herunder mindst tre slags af følgende kategorier: store bogstaver, små bogstaver, tal og specialtegn) for at øge sikkerheden for dit produkt. Og vi anbefaler, at du ændrer din adgangskode regelmæssigt, især i højsikkerhedssystemet, hvor en månedlig eller ugentlig ændring af adgangskoden kan beskytte dit produkt bedre.

Korrekt konfiguration af alle adgangskoder og andre sikkerhedsindstillinger er installatørens og/eller slutbrugerens ansvar.

3.4 Opgradering af enhedens firmwareversion

Når der er en ny firmwareversion tilgængelig for den tilføjede enhed, kan du opgradere dens firmwareversion via klienten.



Bemærk

- Enheden skal understøtte denne funktion.
 - Du kan konfigurere opgraderingstilstand i Systemkonfiguration. Se [***Indstil generelle parametre***](#) for detaljer.
-

Gå ind i Device Management-modulet, og klik derefter på fanen **Device** for at få vist enhedslisten. Udfør følgende handlinger i henhold til de forskellige opgraderingstilstande.

Deaktiver

Hvis der er en ny firmwareversion tilgængelig på Device for Management-panelet, vil status i kolonnen Firmware Upgrade for enheden skifte til **Upgradeable**.

Vælg den enhed, der kan opgraderes, og klik på **Upgrade** for at starte opgraderingen af enhedens firmware.



Bemærk

Status for opgraderingen vises. Når opgraderingen er færdig, skifter status i kolonnen Firmwareopgradering på enheden til **Opgraderet**.

Spørg mig, hvis du downloader og opgraderer

Hvis der er en ny firmwareversion tilgængelig, vises et promptvindue. Klik på **Upgrade All** for at begynde at downloade og opgradere.

Download og spørg mig, hvis du opgraderer

Der vises en dialogboks, hvor du kan vælge, om du vil opgradere, når du har downloadet pakken med den nye version. Klik på **Upgrade All** for at starte opgraderingen af enhedens firmware.

Bemærk

Når du har klikket på **Upgrade All**, dukker der en prompt op, hvor du kan se detaljer. Hvis du ikke er på siden Enhedsstyring, skal du klikke på **Vis detaljer** for at hoppe til siden Enhedsstyring; hvis du er på siden Enhedsstyring, skal du lukke prompten.

Status for opgradering

På enhedens administrationsside vil følgende opgraderingsstatus blive vist i kolonnen Firmware Upgrade.


Ingen tilgængelig version

Ingen ny firmwareversion tilgængelig.

Kan opgraderes

En ny firmwareversion er tilgængelig.

Bemærk

Flyt markøren på  for at se den aktuelle version, seneste version og opgraderingsindhold for firmwareversionen.

Venter

Enheden venter på opgradering.

Downloading

Klienten er ved at downloade pakken med den nye firmwareversion.

Opgradering

Opgraderingen af enhedens firmware er i gang.

Opgraderet

Hold markøren over **Opgraderet** for at vise versionen efter opgraderingen.

Opgradering mislykkedes









Når opgraderingen mislykkes, dukker der en prompt op for at se detaljer. Hvis du ikke er på siden Enhedsstyring, skal du klikke på **Vis detaljer** for at hoppe til siden Enhedsstyring; hvis du er på siden Enhedsstyring, skal du lukke prompten. Hold markøren over **Opgradering mislykkedes** for at vise fejloplysningerne, og klik på Opgrader **igen** for at prøve igen.

3.5 Administrer tilføjede enheder

Når du har tilføjet enheder til enhedslisten, kan du administrere de tilføjede enheder, herunder

redigering af enhedsparametre, fjernkonfiguration, visning af enhedsstatus osv.

Tabel 3-1 Administrer tilføjede enheder

Rediger enhed	Klik på  for at redigere enhedsoplysninger, herunder enhedsnavn, adresse, brugernavn, adgangskode osv.
Slet enhed	Marker en eller flere enheder, og klik på Slet for at slette de valgte enheder.
Fjernkonfiguration	På enhedslistesiden skal du klikke på  i kolonnen Operation for at udføre fjernkonfiguration af en enhed.  er i kolonnen længst til højre på enhedssiden. For detaljer henvises til enhedens brugervejledning.
Se enhedens status	Klik på  for at se enhedens status, herunder kameraer, optagestatus, signalstatus, hardwarestatus osv. <hr/>  Bemærk For forskellige enheder vil du se forskellige oplysninger om enhedens status. <hr/>
Se online bruger	Klik på  for at se oplysninger om onlinebrugere, der har adgang til enheden, herunder brugernavn, brugertype, IP-adresse og login-tid.
Opdater enhedsoplysninger	Klik på  for at opdatere og få de nyeste oplysninger om enheden.
Generer QR-kode	Marker en eller flere enheder, og klik på QR-kode for at generere en QR-kode for den/de tilføjede enhed(er). Du kan tilføje enhed(er) til mobil klienten ved at scanne QR-koden. <hr/>  Bemærk Enheder tilføjet af ISUP eller ABUS Link Station kan ikke generere en QR-kode. <hr/>
Opgrader enhed	Se enhedsstatus i kolonnen Firmwareopgradering, marker en eller flere enheder, der kan opgraderes, og klik på Opgrader enhedsfirmware for at opgradere de valgte enheder. For detaljer, se <u>Opgrader enhedsfirmwareversion</u> .
Hent hændelser fra enheden	Markér én enhed, og klik på Hent hændelser fra enhed for at synkronisere hændelser. For detaljer, se Hent hændelser <u>fra enhed</u> .

3.6 Gruppelidelse

Klienten tilbyder grupper til at administrere de tilføjede ressourcer i forskellige grupper. Du kan gruppere ressourcerne i forskellige grupper i henhold til ressourcernes placering.

Eksempel

På 1. sal er der f.eks. monteret 64 kameraer, 16 døre, 64 alarmindgange og 16 alarmudgange. Du kan organisere disse ressourcer i én gruppe (kaldet 1. sal) for at gøre administrationen nemmere. Du kan få livevisning, afspille videofiler, styre dørstatus og udføre andre funktioner på enhederne, når du har administreret ressourcerne i grupper.

3.6.1 Gruppens ressourcer

Klienten tilbyder to metoder til at tilføje en gruppe: tilpasning af en gruppe eller oprettelse af en gruppe efter enhedsnavn. Når du har tilpasset en gruppe, skal du importere ressourcer til denne gruppe manuelt. Når du har oprettet en gruppe efter enhedens navn, bliver enhedens ressourcer automatisk importeret til gruppen. Du kan vælge en metode til at gruppere dine ressourcer efter de faktiske behov.

Trin

1. Klik på **Enhedsstyring** → **Gruppe** i området Vedligeholdelse og styring for at åbne siden til gruppestyring.
2. Tilføj en gruppe.
 - **Tilpas en gruppe:** Klik på **Tilføj gruppe**, og opret et navn til den nye gruppe.
 - **Opret en gruppe efter enhedsnavn:** Klik på **Create Group by Device Name**, og vælg en tilføjet enhed for at oprette en ny gruppe med navnet på den valgte enhed. Når du har oprettet en gruppe med enhedens navn, importeres enhedens ressourcer (såsom kodningskanaler, alarmindgange, alarmudgange og adgangspunkter) automatisk til gruppen.

Bemærk



- Der kan tilføjes op til 256 grupper.
 - Du kan vælge flere grupper ved at holde Shift- eller Ctrl-tasten nede på tastaturet.
-

3. Når du har tilføjet en gruppe, skal du importere ressourcer til gruppen.

Bemærk

En ressource kan tilføjes til forskellige grupper.

- 1) Vælg den type ressourcer, der skal importeres, og klik på **Import**.
 - 2) Vælg de ressourcer, der skal importeres, og klik på **Import** for at importere alle de valgte ressourcer til denne gruppe.
 4. Valgfrit: Når du har tilføjet en gruppe, skal du udføre en af følgende handlinger, hvis det er nødvendigt.
-

Udvid eller fold ressourcelisten	Klik på  for at udvide eller folde ressourcelisten i gruppen.
Søg efter ressourcer	Indtast søgeordet, og klik på  for at søge efter målressourcer.
Fjern ressource fra gruppe	Vælg ressource(r), og klik på Slet for at fjerne de(n) valgte ressource(r) fra gruppen.
Opdater ressourcenavn	Du kan opdatere alle ressourcenavne i en gruppe eller i en kanal. <ul style="list-style-type: none">• Vælg en gruppe, og klik på Opdater ressourcenavn for at opdatere alle ressourcenavne i den valgte gruppe.• Vælg en kanal i en gruppe, og opdater alle ressourcenavne i denne kanal. Klik f.eks. på Kodningskanaler → Opdater kameranavn for at opdatere alle kameranavne i kodningskanaler.

Bemærk

Denne funktion skal understøttes af enheden.


3.6.2 Rediger ressourceparametre

Når du har importeret ressourcerne til gruppen, kan du redigere ressourceparametrene. For kodningskanalen kan du redigere kanalnavnet, stream-typen, protokol-typen osv. For access point kan du redigere navnet på access point. For alarmindgang kan du redigere navnet på alarmindgangen. Her tager vi kodningskanalen som et eksempel.

Før du går i gang

Importer ressourcerne til gruppen.

Trin

1. Gå ind i Device Management-modulet.
2. Klik på **Enhedsstyring** → **Gruppe** for at åbne siden til gruppestyring.
Alle de tilføjede grupper vises til venstre.
3. Vælg en gruppe på gruppelisten, og klik på **Encoding Channel**.
De kodningskanaler, der er importeret til gruppen, vises.
4. Klik på  i kolonnen Operation for at åbne vinduet Edit Resource.
5. Rediger kameraoplysningerne, herunder kameraets navn, stream-typen osv.

Videostream

Vælg den ønskede stream-type til livevisning af kameraet.

Bemærk

Du skal starte live view igen, før det træder i kraft.

Type af afspilningsstrøm

Vælg den ønskede stream-type til afspilning af kameraet.

Bemærk

- Dette felt vises, hvis enheden understøtter dual-stream.
 - Du skal starte live view igen, før det træder i kraft.
-

Rotationstype

Vælg den ønskede rotationstype for livevisning eller afspilning af kameraet.

Protokoltype

Vælg transmissionsprotokol for kameraet.

Bemærk

Du skal starte live view igen, før det træder i kraft.

Streaming-protokol

Vælg protokollen som RTSP eller privat for at få stream, når du ser live.

Bemærk

Du skal starte live view igen, før det træder i kraft.

Kopier til...

Kopier de konfigurerede parametre til andre kameraer.

Opdatering

Hent et nyt billede til kameraets livevisning.

6. Klik på **OK** for at gemme de nye indstillinger.

Kapitel 4 ABUS Link Station

Klientsoftwaren understøtter også registrering af en ABUS Link Station-konto, login på din ABUS Link Station-konto og administration af de enheder, der understøtter ABUS Link Station-tjenesten.

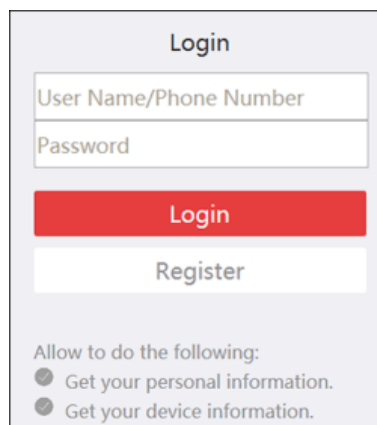
4.1 Registrer en ABUS Link Station-konto

Klienten understøtter registrering af en ABUS Link Station-konto til styring af enheder, der understøtter ABUS Link Station-tjenesten.

Trin

1. Gå ind på login-siden for ABUS Link Station.
 - Klik på **Log ind** i øverste højre hjørne af klienten.
 1. Klik på **Enhedsstyring** → **Enhed** for at åbne siden Enhedsstyring.
 2. Klik på **Tilføj** for at åbne panelet Tilføj enhed.
 3. Vælg **ABUS Link Station** som tilføjelsestilstand.
 4. Klik på **Login**.

Login-vinduet dukker op.



Figur 4-1 Login-vindue

2. Klik på **Register** for at åbne vinduet Register Account.
3. Indtast de nødvendige oplysninger, herunder brugernavn, adgangskode, bekræft adgangskode og telefonnummer/e-mailadresse.

Forsigtig

Styrken af enhedens adgangskode kan kontrolleres automatisk. Vi anbefaler på det kraftigste, at du ændrer den adgangskode, du selv vælger (med mindst 8 tegn, herunder mindst tre slags af følgende kategorier: store bogstaver, små bogstaver, tal og specialtegn) for at øge sikkerheden for dit produkt. Og vi anbefaler, at du ændrer din adgangskode regelmæssigt, især i højsikkerhedssystemet, hvor en månedlig eller ugentlig ændring af adgangskoden kan beskytte dit produkt bedre.

Korrekt konfiguration af alle adgangskoder og andre sikkerhedsindstillinger er installatørens og/eller slutbrugerens ansvar.

4. Klik på **Send besked** for at få en bekræftelseskode.
Systemet sender en bekræftelseskode til din telefon eller e-mail.
5. Indtast den modtagne verifikationskode i tekstfeltet **Verification Code**.
6. Tjek **Jeg har læst og accepteret Servicevilkår Privatlivspolitik**.
7. Klik på **Register** for at afslutte registreringen.

4.2 Log ind på ABUS Link Station-konto

Du kan logge ind på ABUS Link Station-kontoen via klienten, så du kan betjene enheder, der administreres af ABUS Link Station-kontoen.

Før du går i gang

Registrer en ABUS Link Station-konto.

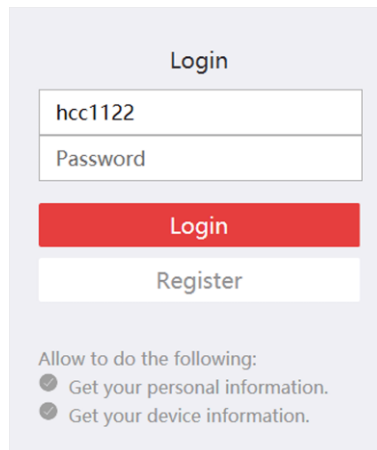
Bemærk

For detaljer, se [**Registrer en ABUS Link Station-konto**](#).

Trin

1. Gå ind på login-siden for ABUS Link Station.
 - Klik på **Log ind** i øverste højre hjørne af klienten.
 1. Klik på **Enhedsstyring** → **Enhed** for at åbne siden Enhedsstyring.
 2. Klik på **Tilføj** for at åbne panelet Tilføj enhed.
 3. Vælg **ABUS Link Station** som tilføjelsestilstand.
 4. Klik på **Login**.

Login-vinduet dukker op.



Login

hcc1122

Password

Login

Register

Allow to do the following:

- Get your personal information.
- Get your device information.

Figur 4-2 Login-side for ABUS Link Station

2. Indtast brugernavn og adgangskode.
3. Klik på **Log ind** for at logge ind på din konto.
Log ind bliver til **Logget ind**.
4. Valgfrit: Klik på **Logget ind** → **Log ud** for at logge ud af din konto.

 **Bemærk**

- Enheder, der tilføjes af ABUS Link Station, skjules, når du logger ud af ABUS Link Station-tjenesten.
 - Alarmrelaterede billeder gemt i ABUS Link Station vil være gyldige i 2 timer.
-













Kapitel 5 Livevisning

Du kan se live-video fra de tilføjede netværkskameraer og videokodere på Main View-siden. Og nogle grundlæggende funktioner understøttes, herunder billedoptagelse, manuel optagelse, vinduesopdeling, PTZ-kontrol, Auto-Switch i livevisning osv.




5.1 Live View-værktøjslinje

Live-view-værktøjslinjen kan hjælpe dig med at betjene og administrere live-view-vinduet mere bekvemt og hurtigt. For eksempel kan du tage billeder, optage lyd, justere lydstyrken og dele vinduet med et enkelt klik på værktøjerne på værktøjslinjen.

Tabel 5-1 Beskrivelser af værktøjslinjen

Ikon	Funktionsnavn	Funktionsbeskrivelse og betjening
	Gem visning	Gem den visning, du opretter i øjeblikket, hvilket er praktisk til hurtig visning af de ønskede kameraer. Klik på  for at åbne vinduet til lagring af visning. Vælg Create View eller Current View , og giv visningen et navn.
	Stop Live View	Stop alle live view-kameraerne.
	Mute/Annuller Mute	Klik på  for at åbne lydstyrkebjælken, klik på  for at annullere mute, og du kan justere lydstyrken. Klik på  for at åbne lydstyrkebjælken, klik på  igen for at indstille live-view-kameraerne som lydløse.
	Vinduesafdelinger	Vælg de forskellige vinduesinddelinger til livevisning. Klik på  for at vælge en vinduesopdelingstilstand (f.eks. 9 vinduesopdelinger). Du kan også klikke på Tilføj for at tilpasse en vinduesopdelingstilstand.
	Fuld skærm	Vis livevisningen i fuld skærm. Tryk på Esc-tasten for at forlade fuldskræmstilstand.
	Konfiguration	Gå ind i tilstanden for indstilling af livevisningsparametre, konfigurer livevisning og afspilning, billede, filer og værktøjslinje.


Tabel 5-2 Beskrivelse af ikoner i Live View-vinduet

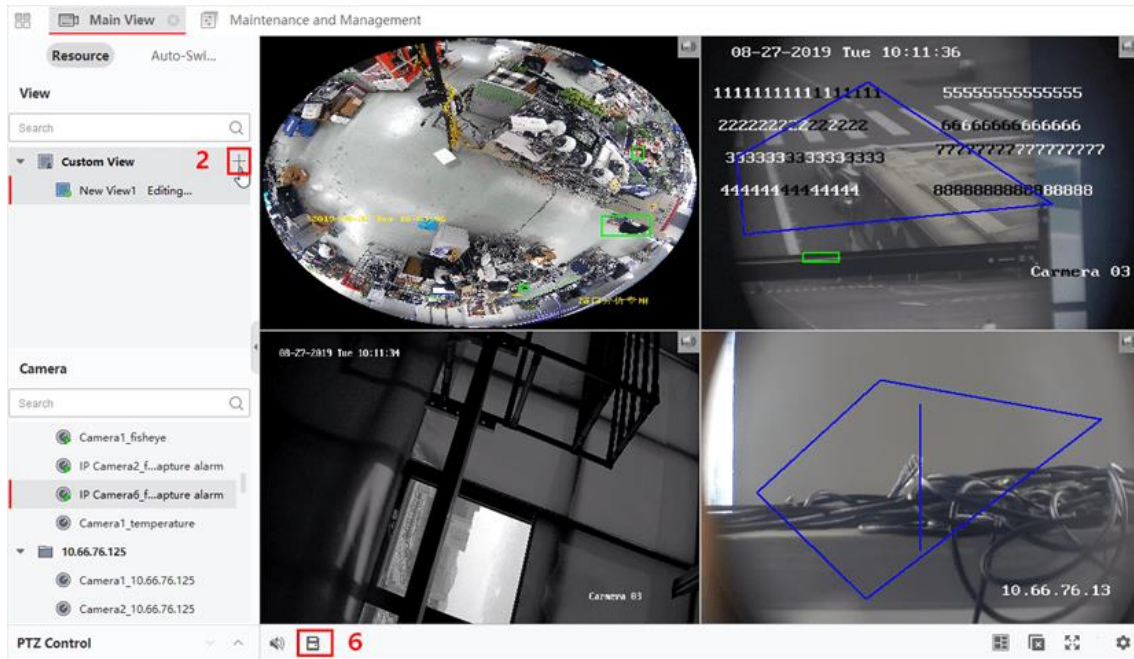
Ikon	Funktionsnavn	Funktionsbeskrivelse og betjening
	Indfangning	Tag billederne manuelt til live view-vinduet.
	Start optagelse/stop optagelse	Klik første gang for at starte optagelsen, og klik igen for at stoppe optagelsen, og gem automatisk optagelsesfilerne på den sti, du har angivet.
	Skift til øjeblikkelig afspilning	På det aktuelle tidspunkt kan du vælge at afspille videoen i de foregående 30 s, 1 min, 3 min, 5 min, 8 min, 10 min.

5.2 Tilføj brugerdefineret visning



En visning er en vinduesinddeling med kameraer konfigureret til hvert vindue; Visningstilstand giver dig mulighed for at gemme vinduesinddelingen og korrespondancen mellem kameraer og vinduer som favorit for hurtigt at få adgang til de relaterede kameraer senere. Du kan f.eks. forbinde kamera 1, kamera 2 og kamera 3 på dit kontor for at vise vinduer og gemme dem som en visning, der hedder kontor.

Trin

1. Gå ind på siden Hovedvisning.
2. Klik på fanen **Ressource**.
3. Flyt markøren til Custom View i ressourcepanelet, og klik på  for at oprette en ny visning.
4. Indtast et navn til visningen.




Figur 5-1 Tilføj brugerdefineret visning


5. Valgfrit: Klik på  i live view-værktøjslinjen for at indstille vinduesopdelingstilstand for den nye visning.
6. Start livevisning for det angivne kamera i det angivne vindue i henhold til de aktuelle behov.
7. Klik på  for at gemme den aktuelle visning eller gemme den som en ny visning.

Bemærk


Det er tilladt at tilføje op til 16 brugerdefinerede visninger til klienten.

8. Valgfrit: Udfør følgende handlinger, når du har tilføjet den brugerdefinerede visning.

Rediger visningsnavn Flyt markøren over den nye visning, og klik på  for at redigere visningsnavnet.

Slet visning Flyt markøren over den nye visning, og klik på  for at slette visningen.

Hvad du skal gøre nu





Klik på  igen for at vælge den brugerdefinerede vinduesinddeling.

5.3 Start Live View

Du kan starte livevisning, når du har tilføjet enhed(er) til klienten, så du kan lære det overvågede område godt at kende. Du kan starte livevisning af ét kamera eller alle kameraer i en gruppe. Du kan også starte livevisningen i brugerdefineret visningstilstand.

Klik på **Hovedvisning** → **Ressource** for at komme til siden Hovedvisning. Vælg ressource(r) på den

venstre ressourceliste, og start livevisning på følgende måder.

Tilgængelige måder	Beskrivelse	Betjening
Start Live View for ét kamera	Start livevisning af kun ét kamera i en gruppe.	<ul style="list-style-type: none"> • Vælg et kamera, og træk det til vinduet. • Dobbeltklik på kameraet i en gruppe. • Flyt markøren over kameraets navn, og klik på  .
Start Live View for kameragruppe	Start livevisning af alle kameraer i en gruppe synkront.	<ul style="list-style-type: none"> • Vælg en gruppe, og træk den til vinduet. • Dobbeltklik på gruppen. • Flyt markøren over gruppenavnet, og klik på  , eller klik på  → Vis alle kameraer i gruppen.
Start Live View i brugerdefineret visningstilstand	Start livevisningen af kameraerne i den brugerdefinerede visning.	<ul style="list-style-type: none"> • Vælg en brugerdefineret visning, og træk den til vinduet. • Dobbeltklik på den brugerdefinerede visning. <hr/> <p> Bemærk</p> <p>Tilpas en visning, der indeholder oplysninger som vinduesinddeling, kamera og korrespondance mellem kameraer og vinduer. Se <i>Tilføj brugerdefineret visning</i> for detaljer.</p> <hr/>

 **Bemærk**

Hvis enheden understøtter streamkryptering, og streamingen af dens livevisning er krypteret, skal du indtaste en streamnøgle til dobbeltbekræftelse.

Figur 5-2 Start Live View

Under livevisning kan du se oplysninger om bitrate, frame rate og opløsning på billedet.

5.4 Automatisk skift i Live View

Du kan vise livevisning af kameraer eller vise de brugerdefinerede visninger efter tur, hvilket kaldes "auto-switch". Hvis du vil udføre livevisning af et stort antal kameraer, kan du auto-switch de valgte kameraer, hvilket betyder, at klienten automatisk skifter livevisning af kameraerne i visningsvinduet. Du kan også automatisk skifte mellem flere visninger.

Når der skiftes automatisk i live view, er der tre tilstande til rådighed:

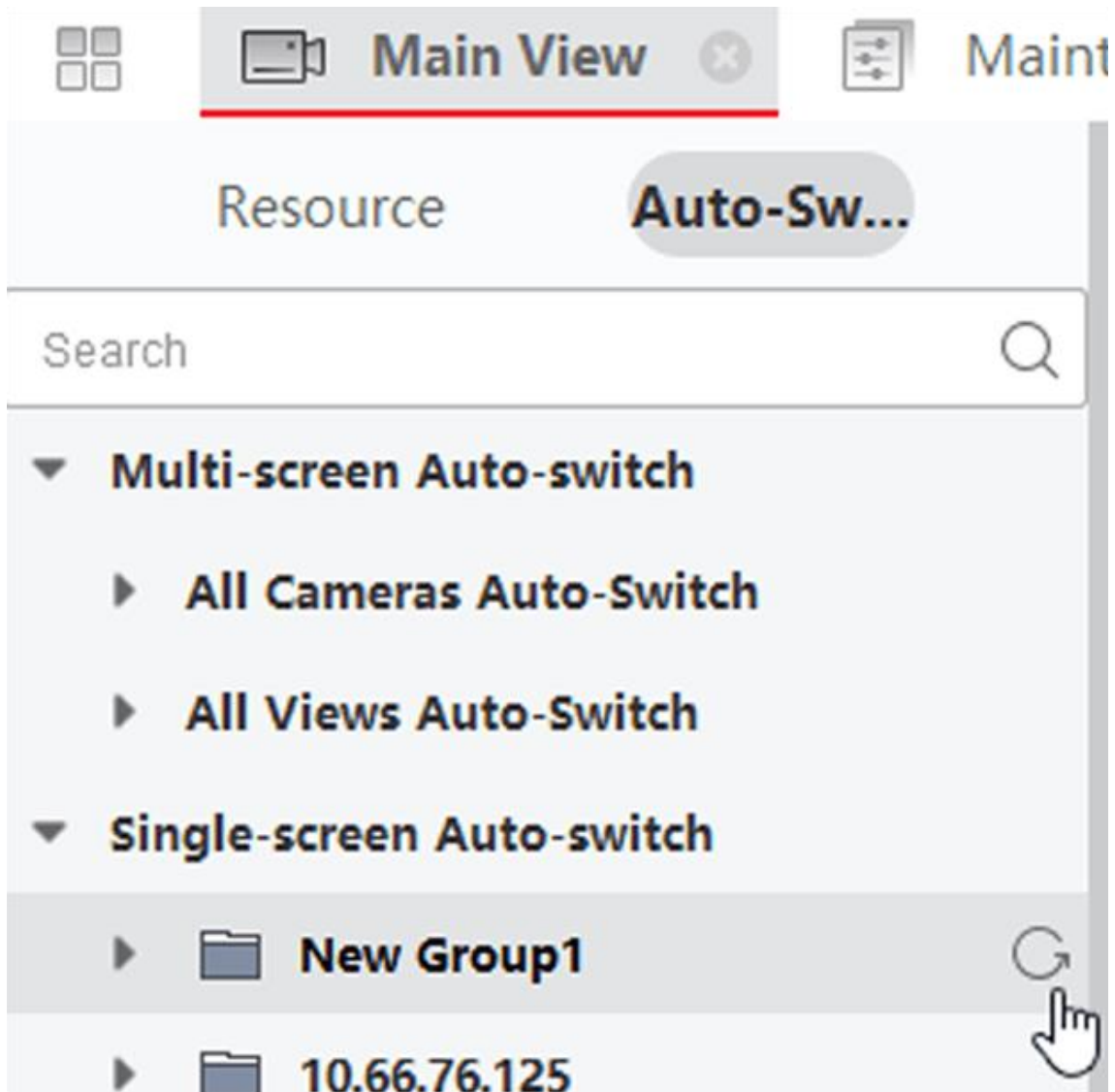
- Skift automatisk mellem alle kameraer i standardvisning
- Automatisk skift af kameraer i en gruppe
- Automatisk skift af brugerdefinerede visninger

5.4.1 Automatisk skift af kameraer i en gruppe

Videostrømmen fra kameraerne i den samme gruppe kan skifte automatisk i et valgt visningsvindue. Hvis du f.eks. starter automatisk skift af en gruppe, der indeholder 5 kameraer, vil livevisningen af de 5 kameraer blive vist på skift med et interval, der kan konfigureres. Du kan også skifte til afspilning og udføre andre handlinger i visningsvinduet.

Trin

1. Gå ind på siden Hovedvisning.
2. Klik på **Auto-Switch** → **Single Window Auto-Switch** i venstre panel for at vise grupperne.
3. Vælg et visningsvindue i højre panel.
4. Hold markøren over et gruppenavn, og klik på  .



Figur 5-3 Start automatisk skift af kameraer i en gruppe

Kameraerne i den valgte gruppe starter automatisk skift i visningsvinduet.



Bemærk

Lyden er som standard slået fra, når auto-switch starter.

5. Valgfrit: Udfør følgende handlinger.

Betjening	Beskrivelse
Pause/Fortsæt Auto-Switch	Klik på eller ↻ for at sætte automatisk skift på pause/genoptage det.
Gå til forrige/næste side	Klik på < eller > for at få vist kameraerne i den forrige/næste gruppe.

Indstil dvæletid

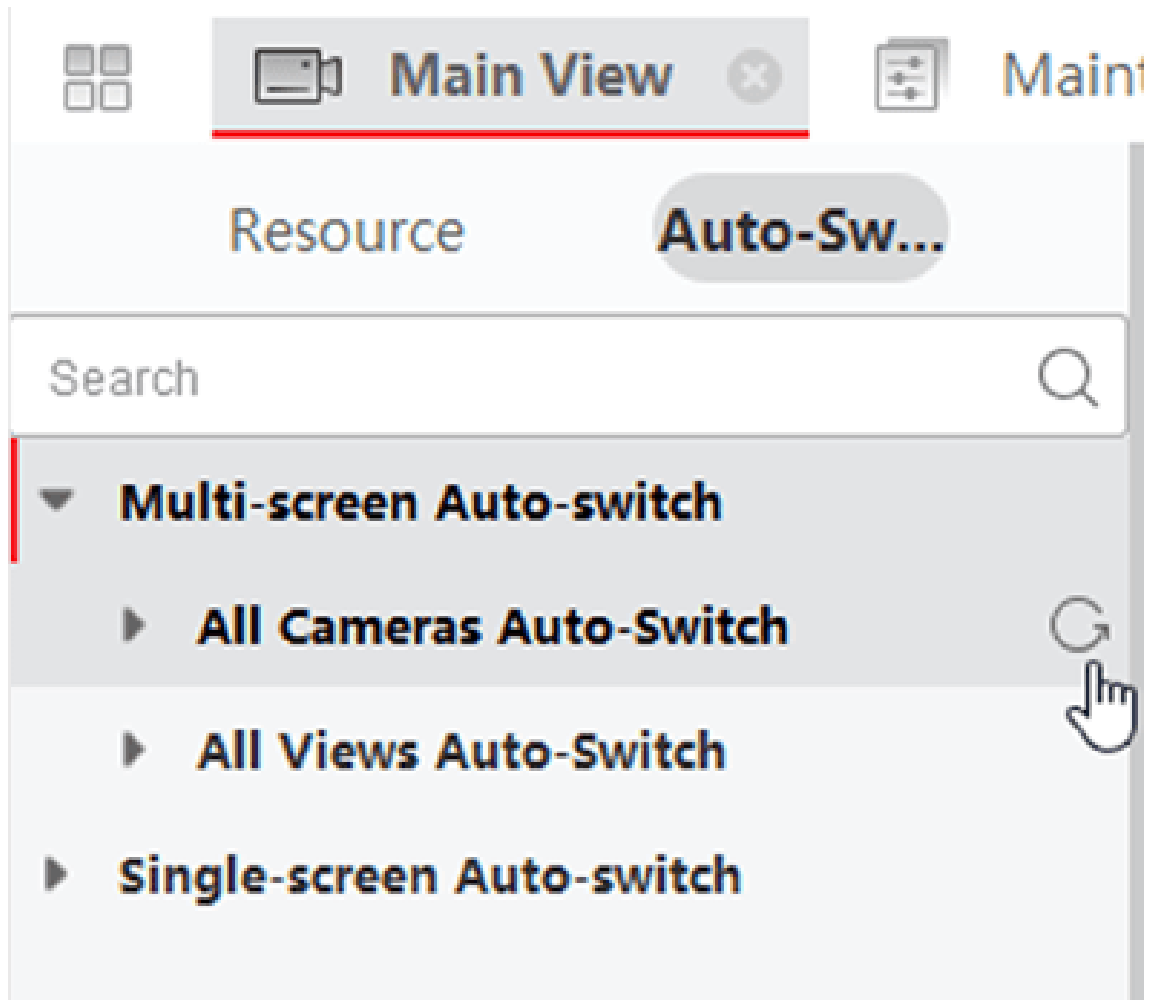
Når du har stoppet den aktuelle auto-switch, skal du klikke på « eller  for at mindske/øge auto-switchens dvæletid, eller klikke på **20s** nederst på siden for at ændre auto-switchens dvæletid. Du kan også klikke på **Custom Dwell Time** for at indstille dvæletiden efter dit behov. Hvis du f.eks. indstiller intervallet til 10 sekunder, vil billedet af hver gruppe blive vist i 10 sekunder og derefter skifte til næste gruppe.

5.4.2 Automatisk omskiftning af alle kameraer

Videoen fra alle kameraerne på kameralisten kan skifte automatisk i en selvtilpassende tilstand. Hvis du starter automatisk skift af alle kameraer, kan livevisningen af alle kameraer vises hurtigt, hvilket er en effektiv måde til livevisning. Auto-switch udføres med et interval, som kan konfigureres. Du kan også skifte til afspilning og udføre andre handlinger i vinduet for automatisk skift.

Trin

1. Gå ind på siden Hovedvisning.
2. Klik på **Auto-Switch** → **Multi-Window Auto-Switch** i venstre panel.
3. Hold markøren over **Auto-Switch All Cameras**, og klik derefter på  .



Figur 5-4 Start automatisk omskiftning af alle kameraer

Alle kameraer på kameralisten begynder at skifte automatisk i en selvtilpassende tilstand.

4. Valgfrit: Udfør følgende handlinger.

Betjening	Beskrivelse
Pause/Fortsæt Auto-Switch	Klik på eller for at sætte automatisk skift på pause/genoptage det.
Gå til forrige/næste side	Klik på eller for at få vist kameraer på forrige/næste side.
Indstil dvæletid	Når du har stoppet den aktuelle auto-switch, skal du klikke på eller for at mindske/øge auto-switchens dvæletid, eller klikke på 20s nederst på siden for at ændre auto-switchens dvæletid. Du kan også klikke på Custom Dwell Time for at indstille dvæletiden efter dit behov. Hvis du f.eks. indstiller intervallet til 10 sekunder, vil billedet af hvert kamera blive vist i 10 sekunder og derefter skifte til næste kamera.


5.4.3 Automatisk skift af brugerdefinerede visninger

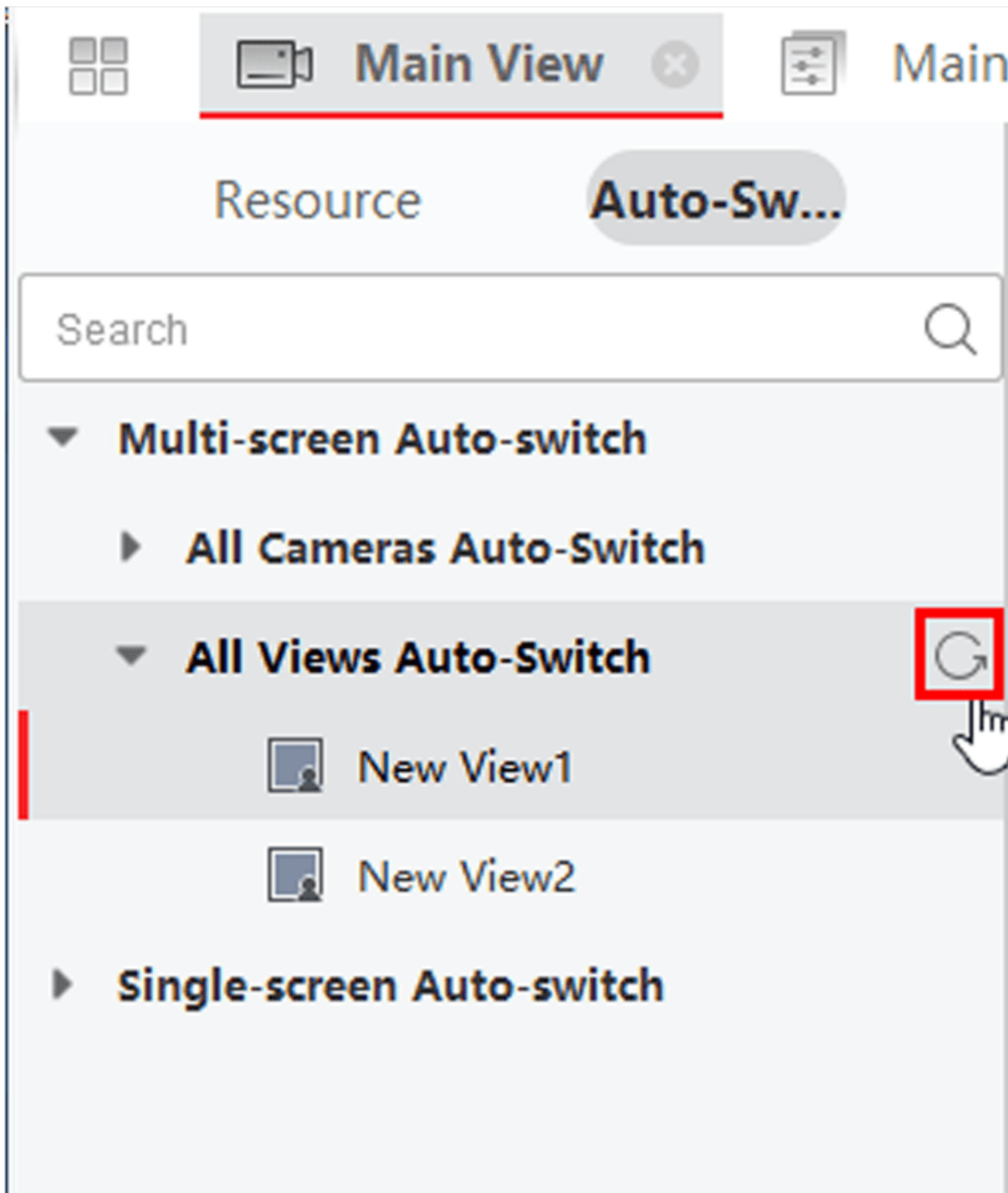
En visning er en vinduesinddeling med ressourcekanaler (f.eks. kameraer) knyttet til hvert vindue. Med visningsfunktionen kan du gemme vinduesinddelingen og korrespondancen mellem kameraer og vinduer som favorit, så du hurtigt kan få adgang til disse kanaler senere. Hvis du gemmer en visning, der indeholder alle kameraer på en etage, gemmer du en brugerdefineret visning, og du kan se livevisningen af alle kameraerne på etagen efter tur med et enkelt klik. På den måde behøver du ikke at søge efter disse kameraer i kameralisten, hver gang du logger på. Auto-switch fungerer med et interval, som kan konfigureres manuelt.

Før du går i gang

Tilføj de brugerdefinerede visninger. Se [Tilføj brugerdefineret visning](#) for detaljer.

Trin

1. Gå ind på siden Hovedvisning.
2. Klik på **Resource** → **Multi-Window Auto-Switch** i venstre panel.
3. Hold markøren over **Auto-Switch All Views**, og klik på  .



Figur 5-5 Automatisk skift af en brugerdefineret visning



Alle brugerdefinerede visninger begynder at skifte automatisk.

4. Valgfrit: Udfør følgende handlinger.

Betjening	Beskrivelse
Pause/Fortsæt Auto-Switch	Klik på eller ↻ for at sætte automatisk skift på pause/genoptage det.
Gå til forrige/næste	Klik på < eller > for at få vist den forrige/næste visning.

side

Indstil dvæletid

Når du har stoppet den aktuelle auto-switch, skal du klikke på « eller  for at mindske/øge auto-switchens dvæletid, eller klikke på **20s** nederst på siden for at ændre auto-switchens dvæletid. Du kan også klikke på **Custom Dwell Time** for at indstille dvæletiden efter dit behov. Hvis du f.eks. indstiller intervallet til 10 sekunder, vil billedet af hver visning blive vist i 10 sekunder og derefter skifte til næste visning.

5.5 PTZ-styring

Softwaren giver PTZ-kontrol til kameraer med panorering/tiltning/zoom-funktionalitet. Under PTZ-styringen kan du indstille forudindstilling, patrulje og mønster, og du kan også åbne et nyt vindue til styring af PTZ.



Forsigtig

- Nogle funktioner bør understøttes af enheden.

5.5.1 PTZ-kontrolpanel

Softwaren giver PTZ-kontrolfunktioner via kontrolpanelet, såsom detektion, hastighed, zoom ind, zoom ud osv. Du kan også åbne et nyt vindue til styring af PTZ.
















Bemærk








ABUS Link Station-enheden understøtter kun PTZ-bevægelser i retningerne op, ned, venstre og højre.

Gå ind i hovedvisningsmodulet, og vælg **PTZ Control** for at åbne PTZ-kontrolpanelet. Følgende ikoner er tilgængelige på PTZ-kontrolpanelet.

Tabel 5-3 Ikoner på PTZ-kontrolpanelet

Ikon	Navn	Beskrivelse
	Retningsknapper	Klik eller hold venstre museknap nede for at dreje PTZ'en rundt. Klik for at dreje PTZ'en horisontalt og kontinuerligt; klik igen for at stoppe drejningen.
	Hastighedskontrol	Træk i skyderen for at justere PTZ'ens bevægelseshastighed.

Ikon	Navn	Beskrivelse
	Zoom ind/ud	Zoom ind for at se detaljer i nærbilledet, zoom ud for at se et panoramabillede.
	Fokus +/-	Klik på Focus + for at flytte fokuspunktet fremad, og klik på Focus - for at flytte fokuspunktet bagud.
	Iris +/-	Bruges til at justere billedets luminans. Jo større iris er, jo mere lys kommer der ind, og jo lysere bliver billedet.
	3D-positionering	Brug venstre musetast til at klikke på den ønskede position i videobilledet og træk et rektangelområde i nederste højre retning, så vil kuppelsystemet flytte positionen til midten og lade rektangelområdet zoome ind. Brug venstre musetast til at trække et rektangelområde i øverste venstre retning for at flytte positionen til midten og lade rektangelområdet zoome ud.
	Hjælpefokus	Klik for at fokusere automatisk.
	Initialisering af linse	Initialiser linsen, og fokusér igen for at få et klart billede.
	Lys	Klik for at fylde lys. <hr/>  Bemærk Denne funktion skal understøttes af enheden. <hr/>
	Visker	Brug viskeren til at fjerne støv fra katedralinsen.
	Manuel spring	For speed dome med auto-tracking-funktion skal du aktivere auto-tracking (via højrekliksmenuen) for den og klikke på ikonet for manuelt at spore målet ved at klikke på videoen.
	Menu	For analog speed dome skal du klikke på ikonet for at få vist den lokale menu. For detaljeret betjening af menuen henvises til



Ikon	Navn	Beskrivelse
		speeddomens brugervejledning.
	Patrulje med ét tryk	For speed dome med one-touch patruljefunktion, klik på ikonet, og speed dome starter patrulje fra den foruddefinerede forudindstilling nr. 1 til forudindstilling nr. 32 i rækkefølge efter en periode med inaktivitet (parkeringstid). For indstilling af parkeringstid henvises til speeddomens brugervejledning.
	Park med ét tryk	For speed dome med one-touch park-funktion, klik på ikonet, og speed domen gemmer den aktuelle visning på forudindstilling nr. 32. Enheden begynder automatisk at parkere ved forudindstilling nr. 32 efter en periode med inaktivitet (parkeringstid). For indstilling af parkeringstid henvises til speeddomens brugervejledning.
	Aktivér manuel opvarmning til afisning af linsen	Aktivér denne funktion for at sikre kameraets ydeevne ved opvarmning. <hr/> Bemærk Vi foreslår, at du aktiverer denne funktion, når omgivelsestemperaturen er under 0 °C, da den høje temperatur ellers kan påvirke kameraets funktion. <hr/>
	Aktiver manuel PT-afisning	Aktiver denne funktion for at sikre kameraets ydeevne ved at tørre den is af, der sidder fast på PTZ-kameraet.
	Manuel ansigtsoptagelse	Klik på denne knap, og hold venstre museknap nede for at vælge et ansigt i billedet og tage et billede af det. Billedet bliver uploadet til serveren, så du kan se det.
	Synkroniser FOV	For termiske kameraer skal du klikke på ikonet for at synkronisere den optiske kanals synsfelt med den termiske kanals.
	Regional eksponering	For speed domes skal du klikke på ikonet og

Ikon	Navn	Beskrivelse
		tegne et rektangel på billedet for at optimere eksponeringseffekten i dette område.
	Regionalt fokus	For speed domes skal du klikke på ikonet og tegne et rektangel på billedet for at optimere fokuseffekten i dette område.
	Armering og sporing	For kameraer, der understøtter armering og sporing, skal du klikke på ikonet og vælge målet (person eller køretøj) i livevisningen for at aktivere og spore dette mål.

5.5.2 Indstil forudindstilling, patrulje og mønster

PTZ-kontrol understøtter indstilling og opkald af en forudindstilling, patrulje og mønster. Klik på **Hovedvisning** → **PTZ-kontrol** på startsideen for at vise PTZ-kontrolpanelet.

Opgave	Definition	Betjening
Forudindstillet	En forudindstilling forbinder de vigtigste områder med mobil PTZ-position og -status. Overvågningspersonalet bruger den til hurtigt at positionere sig til nøgleområderne. Ved at sende en forudindstillet kommando registrerer den mobile PTZ positionen og status for zoom, fokus og iris. Når den forudindstillede kommando for opkald udføres, ruller den mobile PTZ hurtigt til den indstillede position og genoptager den indstillede status.	Sådan gør du: Vælg en forudindstilling fra listen over forudindstillinger → Drej kameraet til den ønskede position → Klik på .
		Sådan ringer du: klik på .
Mønster	Med et optagelsesmønster kan bevægelsesbanen og opholdstiden i en bestemt position registreres præcist. Med et opkaldsmønster	Sådan indstilles: Klik på for at begynde at optage et mønster → klik på retningsknapperne for at forme mønsteret → klik på .
		Sådan ringer du: klik på .

Opgave	Definition	Betjening
	begynder den mobile PTZ at bevæge sig helt i overensstemmelse med den registrerede bane.	
Patrolje	Patrol er en funktion, hvor brugeren angiver et scanningsspor med en gruppe af definerede forudindstillinger. Patroljen mellem to forudindstillinger udføres med den indstillede hastighed og tid.	Sådan indstilles: klik på  → vælg forudindstillinger, og indstil hastighed og tid → klik på OK .
		Sådan ringer du: Klik på  .

 **Bemærk**

Du bør indstille mindst to forudindstillinger på forhånd.


5.6 Tilpas inddeling af vinduer

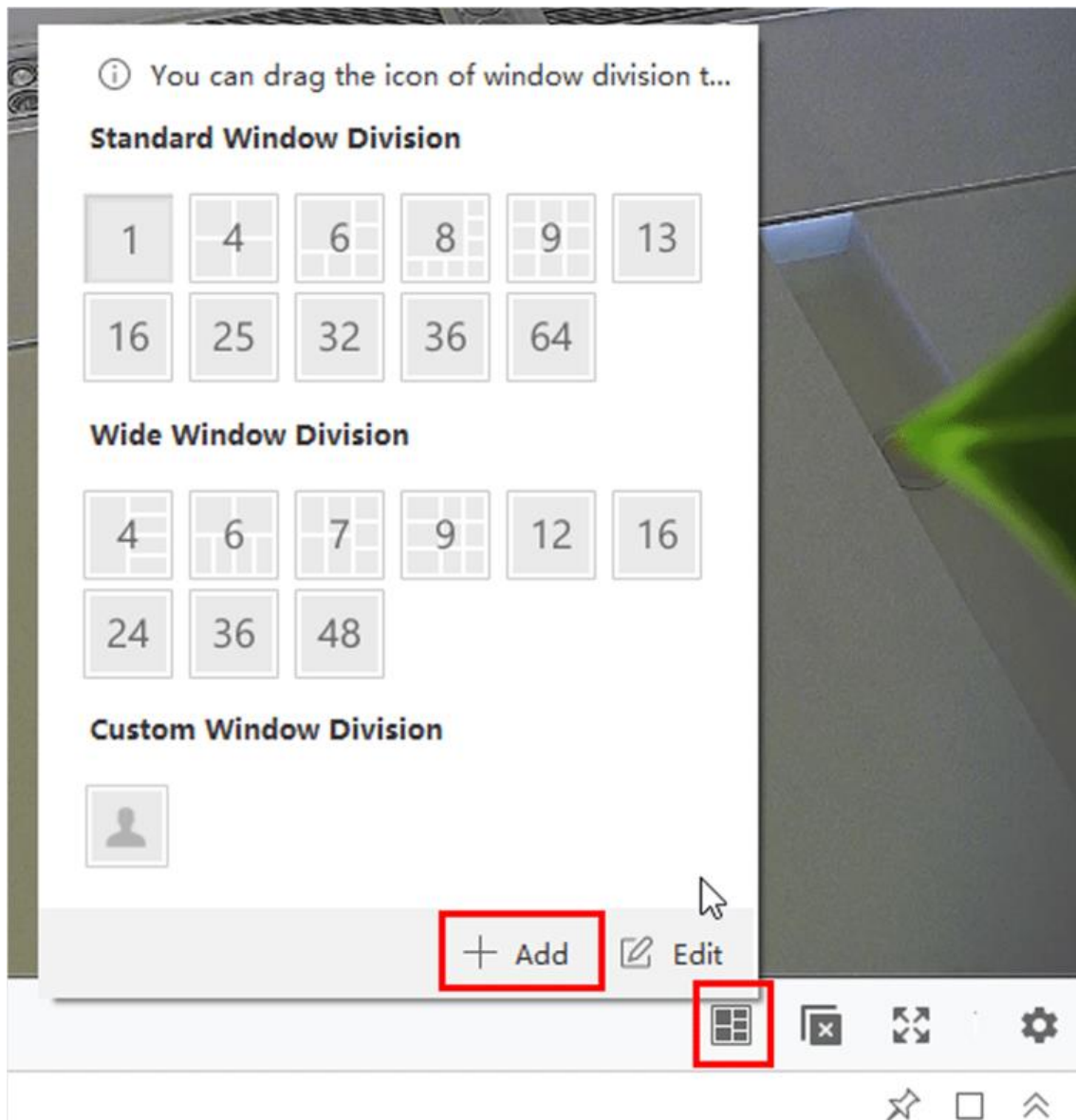
Klientsoftwaren indeholder flere slags foruddefinerede vinduesinddelinger. Du kan også tilpasse vinduesinddelingen efter ønske.

Trin

 **Bemærk**

Op til 5 vinduesinddelinger kan tilpasses.

1. Åbn siden Hovedvisning eller Fjernafspilning.
2. Klik på  på værktøjslinjen for livevisning eller afspilning for at åbne panelet til opdeling af vinduer.



Figur 5-6 Tilføj brugerdefineret vinduesinddeling

3. Klik på **Tilføj** for at åbne dialogen Tilføj brugerdefineret vinduesinddeling.
4. Indtast vinduesnumrene i både vandret og lodret dimension i feltet Dimension, og tryk derefter på **Enter** på dit tastatur.

Bemærk

Ved fjernafspilning kan der afspilles op til 16 vinduer på samme tid, så den brugerdefinerede vinduesinddeling med mere end 16 vinduer er ugyldig.

5. Det er valgfrit: Træk musen for at vælge de tilstødende vinduer, og klik på **Joint** for at samle dem som et helt vindue.

Add Custom Window Division

Name

Dimension X

Window Division Joint Restore

Figur 5-7 Tilføj brugerdefineret vindue Opdelingsvindue

6. Det er valgfrit: Vælg joint-vinduet, og klik på **Restore** for at annullere joint'en.
7. Klik på **Gem**.
8. Valgfrit: Klik eller træk en opdelingstilstand til visningsvinduet for at anvende tilstanden til visning.
9. Valgfrit: Rediger en tilpasset vinduesopdelingstilstand.
 - 1) Klik på på værktøjslinjen for livevisning eller afspilning for at åbne panelet til opdeling af vinduer.
 - 2) Klik på **Edit** for at åbne Add Custom Window Division.
 - 3) Vælg en tilpasset opdelingstilstand, og udfør operationer, herunder omdøbning, indstilling af dimension, sammenføjning/ikke sammenføjning af vinduer.

5.7 Manuel optagelse og indfangning

Under livevisning kan du optage videoer og tage billeder manuelt og derefter se de optagede videofiler og optagne billeder på den lokale pc.




5.7.1 Optag video manuelt

Manuel optagefunktion gør det muligt at optage livevideoen på Main View-siden manuelt, og du kan gemme videofilerne på den lokale pc.

Trin

Bemærk

Manuel optagelse understøttes ikke af ABUS Link Station-enheden under livevisning.

1. Åbn siden Hovedvisning.
 2. Start live-visningen.
 3. Udfør en af følgende handlinger for at starte manuel optagelse.
 - Flyt markøren til displayvinduet i live view for at vise værktøjslinjen, og klik på  på værktøjslinjen.
 - Højreklik på displayvinduet, og klik på **Start optagelse** i højrekliksmenuen. Ikonet  bliver til . En indikator  vises i øverste højre hjørne af displayvinduet.
 4. Klik på  for at stoppe den manuelle optagelse.
Den optagede videofil gemmes automatisk på den lokale pc, og et lille vindue med oplysninger om lagringsstien vises i nederste højre hjørne af skrivebordet.
-

Bemærk

Gemместien for de optagede videofiler kan indstilles på siden Systemkonfiguration. Se [Indstil sti til lagring af filer](#) for detaljer.


5.7.2 Se lokale videoer

Du kan se de optagede videofiler, der er gemt på din lokale pc.

Før du går i gang

Optag live-videoen.

Trin

1. Klik på  → **Filer** → **Åbn videofil** i øverste højre hjørne for at åbne siden Videofiler.
2. Vælg det kamera, der skal søge i de optagede videofiler, fra listen Kameragruppe.
3. Angiv start- og sluttidspunkt for søgningen i nederste venstre hjørne.
4. Klik på **Søg**.
De videofiler, der er optaget mellem start- og sluttidspunktet, vises i miniatureformat på siden.

5. Valgfrit: Udfør følgende handling(er) efter søgningen.

- | | |
|----------------------|--|
| Slet videofil | Vælg videofilen, og klik på Slet for at slette videofilen. |
| Send e-mail | Vælg videofilen, og klik på Email for at sende en e-mailnotifikation med den valgte videofil vedhæftet. |

 **Bemærk**

Hvis du vil sende en e-mailnotifikation, skal e-mailindstillingerne konfigureres, før du fortsætter. For detaljer, se Indstil [e-mail-parametre](#).


- | | |
|------------------------|---|
| Gem lokal video | Vælg videofilen, og klik på Gem som for at gemme en ny kopi af videofilen. |
| Afspilning | Dobbeltklik på videofilen for at starte den lokale afspilning. |

5.7.3 Optagelse af billeder

Du kan tage billeder under livevisningen.

Udfør denne opgave, når du har brug for at tage billeder under live view.

Trin

1. Åbn Main View-siden, og start livevisningen af et kamera.
2. Udfør en af følgende handlinger for at tage billeder.
 - Flyt markøren til displayvinduet i live view for at vise værktøjslinjen, og klik på  på værktøjslinjen.
 - Højreklik på displayvinduet, og klik på **Capture** i højrekliksmenuen.Det optagne billede gemmes automatisk på den lokale pc, og et lille vindue med billedeksemplet og oplysninger om gemmestien vises i nederste højre hjørne af skrivebordet.

 **Bemærk**

Lagringsstien for de optagne billeder kan indstilles på siden Systemkonfiguration. For detaljer, se [Indstil sti til lagring af filer](#).


5.7.4 Vis optagede billeder

De billeder, der tages i live view, gemmes på den pc, hvor softwaren kører. Du kan se de optagne billeder, hvis du har brug for det.

Før du går i gang

Tag billeder i live-visningen.

Trin

1. Klik på  → **File** → **Open Captured Picture** i øverste højre hjørne for at åbne siden Captured Picture.
2. Vælg det kamera, der skal søge i de optagne billeder, fra kameragrupperlisten.
3. Angiv start- og sluttidspunkt for søgningen i nederste venstre hjørne.
4. Klik på **Søg**.
De billeder, der er taget mellem start- og sluttidspunktet, vises i miniatureformat på siden.
5. Valgfrit: Udfør følgende handling(er) efter søgningen.

Forstør billede	Dobbelklik på miniaturebilledet for at forstørre det, så du bedre kan se det.
Udskriv billede	Vælg det optagne billede, og klik på Print for at udskrive det valgte billede.
Slet billede	Vælg det optagne billede, og klik på Delete for at slette det valgte billede.
Send e-mail	Vælg det optagne billede, og klik på Email for at sende en e-mailnotifikation med det valgte billede vedhæftet.
Gem billede	Vælg det optagne billede, og klik på Gem som for at gemme en ny kopi af det valgte billede.



5.8 Øjeblikkelig afspilning

Øjeblikkelig afspilning viser et stykke af videoen, som er bemærkelsesværdigt, eller som er uklart ved første øjekast. Så du kan afspille videofilerne med det samme på Main View-siden og få en øjeblikkelig gennemgang, hvis det er nødvendigt.

Før du går i gang

Optag videofilerne, og gem dem på lagerenhederne, f.eks. SD/SDHC-kort og HDD'er på DVR'er, NVR'er, netværkskameraer osv. eller på lagringsserverne.

Trin

1. Åbn Main View-siden, og start livevisningen.
2. Udfør en af følgende handlinger for at vise listen over varigheder for øjeblikkelig afspilning.
 - Flyt markøren til displayvinduet for at vise værktøjslinjen, og klik på .
 - Højreklik på displayvinduet, og vælg **Skift til øjeblikkelig afspilning** i højreklikmenuen.
 - Flyt markøren til noden for standardvisning eller brugerdefineret visning i panelet Vis, og klik på .

Der vises en liste med preplay-varigheder på 30s, 1 min, 3 min, 5 min, 8 min og 10 min.
3. Vælg en tidsperiode fra den viste liste for at starte den øjeblikkelige afspilning.

Eksempel

Hvis du vælger 3 min, og det aktuelle tidspunkt for livevisningen er 09:30:00, starter den øjeblikkelige afspilning fra 09:27:00.

Under øjeblikkelig afspilning vises en indikator  i øverste højre hjørne af displayvinduet.

4. Valgfrit: Klik på  igen for at stoppe den øjeblikkelige afspilning og gå tilbage til livevisningen.

5.9 Livevisning til fiskeøjekameraer

For fisheye-kameraer kan du starte livevisningen i fisheye-tilstand, indstille forudindstillinger og patruljer og udføre PTZ-styring.


5.9.1 Udfør Live View i Fisheye-tilstand

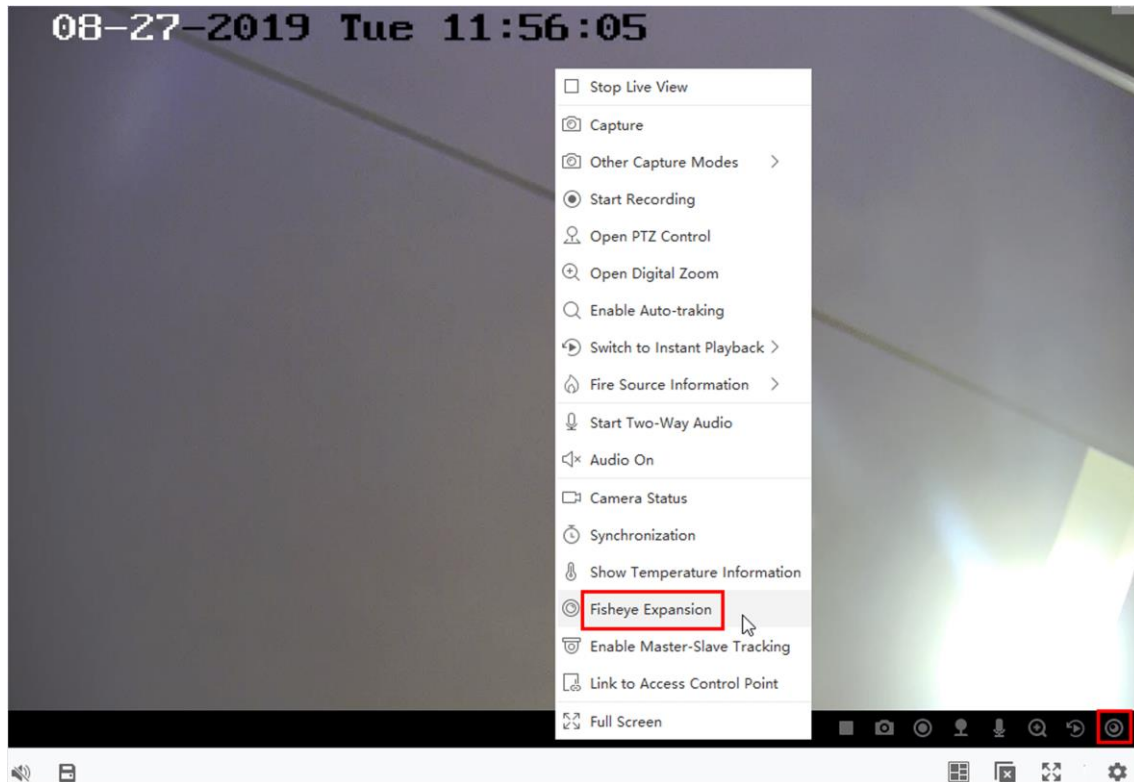
Under livevisning af fiskeøjekameraer vises hele det forvrængede vidvinkelbillede. Men du kan have svært ved at se nogle detaljer. For at løse dette problem kan du afspille livevideoerne i fisheye-udvidelsestilstand. Fisheye-udvidelse kan udvide billeder i forskellige tilstande: 180° panorama, 360° panorama, PTZ, halv kugle osv. Så du kan se billedet tydeligt.

Før du går i gang

Sørg for, at du har installeret Microsoft DirectX-komponenten.

Trin

1. Åbn siden Main View, og start livevisningen af fiskeøjekameraet.
2. Gå ind i Fisheye Expansion-tilstand.
 - Højreklik på videoen, og vælg **Fisheye Expansion**.
 - Klik på  i værktøjslinjen. Se [Indstil ikoner vist på værktøjslinjen](#) for detaljer om indstilling af værktøjslinjen.



Figur 5-8 Livevisning i fisheye-tilstand

—
☉ henvender sig til ☉ .

3. Klik på ☉ i nederste venstre hjørne af visningsvinduet for at åbne panelet Mounting Type & Expanding Mode Selection.
4. Vælg monteringsstype for fisheye-kameraet i henhold til dets faktiske monteringsposition.
5. Vælg den ønskede udvidelsestilstand for livevisning.

Fisheye

I visningsfunktionen Fisheye vises hele kameraets vidvinkelvisning. Denne visningstilstand kaldes Fisheye, fordi den minder om synet af en fisks konvekse øje. Linsen producerer krumme billeder af et stort område, mens den forvrænger perspektivet og vinklerne på objekterne i billedet.

Panorama

I panoramavisningstilstanden omdannes det forvrængede fiskeøjebillede til et normalt perspektivbillede ved hjælp af nogle kalibreringsmetoder.

PTZ

PTZ-visningen er et nærbillede af et defineret område i Fisheye-visningen eller Panoramavisningen, og den understøtter den elektroniske PTZ-funktion, som også kaldes e-PTZ.

Bemærk

Hver PTZ-visning er markeret på Fisheye-visningen og Panorama-visningen med en specifik navigationsboks. Du kan trække i navigationsboksen på Fisheye-visningen eller Panorama-visningen for at justere PTZ-visningen, eller trække i PTZ-visningen for at justere visningen til den ønskede vinkel.

Halv kugle

I halvkugle-tilstanden kan du trække i billedet og rotere det centreret om diameteren for at justere visningen til den ønskede vinkel.

AR halvkugle

AR half sphere-tilstand overlapper billeder langt væk og tæt på, så du kan se et dimensionelt billede i en vid vinkel.

Cylinder

I cylindertilstand formes billedet til en cylinderside.

6. Valgfrit: Udfør følgende handling(er) efter start af livevisning i fisheye-tilstand.

Indfangning	Højreklik på vinduet, og vælg Capture for at optage billedet i live view-processen.
Gå til fuld skærm	Højreklik på et vindue, der afspilles, og skift det valgte vindue til fuldskræmstilstand.





5.9.2 PTZ-styring i Fisheye-tilstand

I fisheye-tilstand kan du styre PTZ'en for at justere PTZ-vinduet.

Bemærk

PTZ-panelet varierer afhængigt af de forskellige enheder.





Følgende funktioner er tilgængelige på PTZ-kontrolpanelet.

- Vælg et PTZ-vindue, og klik på retningsknapperne for at justere synsvinklen. Eller træk i nr. mærket i fiskeøje- eller panoramavinduet for at ændre PTZ-vinduets synsvinkel.
- Vælg et PTZ-vindue, klik på  for at starte automatisk scanning (kameraet roterer i vandret retning), og klik på det igen for at stoppe automatisk scanning.
- Træk i skyderen på  for at justere hastigheden for PTZ-bevægelser.
- Klik på  , eller rul med musehjulet for at zoome ind eller ud på det valgte PTZ-vindue.

5.9.3 Indstil en forudindstilling og patrulje

PTZ understøtter konfiguration og opkald af en forudindstilling og patrulje.

Gå ind på **Main View**-siden, og vælg **Fisheye Expansion** efter at have højreklikket på et kamera.

Opgave	Definition	Betjening
Forudindstillet	En forudindstilling forbinder de vigtigste områder med mobil PTZ-position og -status. Overvågningspersonalet bruger den til hurtigt at positionere sig til nøgleområderne. Ved at sende en forudindstillet kommando registrerer den mobile PTZ positionen og status for zoom, fokus og iris. Når den forudindstillede kommando for opkald udføres, ruller den mobile PTZ hurtigt til den indstillede position og genoptager den indstillede status.	Sådan indstilles: Vælg en forudindstilling fra listen over forudindstillinger → Drej kameraet til den ønskede position → Klik på  .
		Sådan ringer du: Klik på  .
Patrolje	Patrol er en funktion, hvor brugeren angiver et scanningsspor med en gruppe af definerede forudindstillinger. Patroljen mellem to forudindstillinger udføres med den indstillede hastighed og tid.	Sådan indstilles: klik på  → vælg forudindstillinger, og indstil hastighed og tid → klik på OK .
		Sådan ringer du: Klik på  .

5.11 Livevisning til termisk kamera

Med et termisk kamera kan du se oplysninger om brandkilden og temperaturen under livevisning. Du kan også måle temperaturen manuelt for at få temperaturoplysninger i live view-billedet.

5.11.1 Vis information om brandkilde under livevisning

Under livevisningen kan du se oplysninger om den registrerede brandkilde.

Før du går i gang

Konfigurer alarmreglerne for den termiske enhed, se enhedens brugervejledning for detaljer.

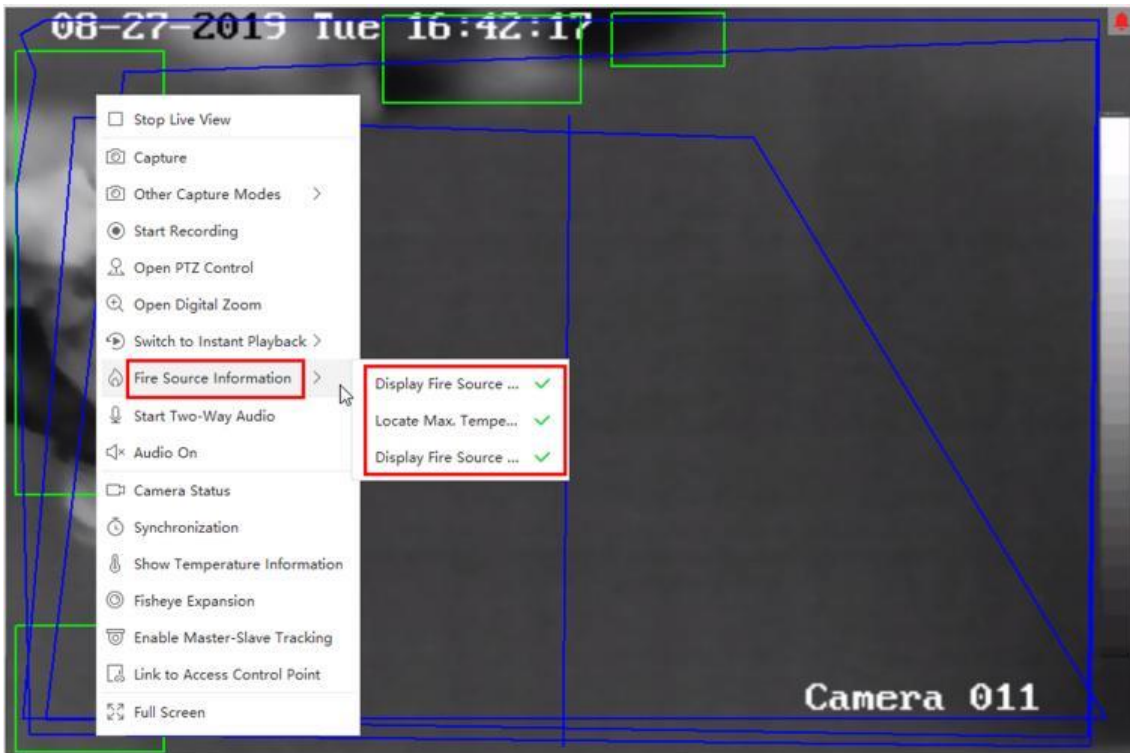
Trin

1. Gå ind på Main View-siden, og start livevisningen af et termisk kamera.

 **Bemærk**

Se **Start** live-visning for at starte **live-visning**.

2. Højreklik på live view-billedet, og vælg **File Source Information** i højrekliksmenuen for at få vist listen over informationstyper.



Figur 5-9 Vis information om brandkilde

3. Vælg en informationstype på listen for at få vist informationen.

Visning af brandkilderegion

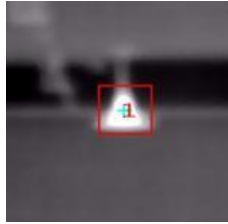
Det område, hvor temperaturen er højere end den konfigurerede alarmtærskel.

Find maks. Temperaturområde

Marker det område, hvor temperaturen er højest i brandkilderegionen. Det er markeret med grønt.

Visning af brandkilde Mål

Afstanden mellem enheden og brandkilden.



Figur 5-10 Information om brandkilde på live view-billede

5.11.2 Vis temperaturoplysninger på Live View-billedet

Du kan vise eller skjule temperaturoplysningerne i realtid for overvågningsscenen, når du ser livevideoen.

Før du går i gang

- Skift enhedens VCA-kildetype til **Temperaturmåling + Registrering af unormal hændelse**.
- Aktivér enhedens temperaturmålingsfunktion, og indstil temperaturmålingsreglerne, se enhedens brugervejledning for detaljer.

Udfør denne opgave, når du har brug for at vise temperaturoplysninger på live view-billedet.

Trin

1. Gå ind på Main View-siden, og start livevisningen af et termisk kamera.

Bemærk

Se **Start** live-visning for at starte **live-visning**.

2. Juster scenen til det område, der er konfigureret med temperaturmålereglen.
3. Højreklik på live view-billedet, og vælg **Vis temperaturinformation** i højreklikmenuen. Temperaturen vises på live view-billedet.
4. Klik på billedet for at se de detaljerede temperaturoplysninger.



Figur 5-11 Temperaturoplysninger på Live View-billedet

5. Valgfrit: Højreklik på live view-billedet, og vælg **Skjul temperaturoplysninger** for at skjule temperaturoplysningerne.

5.11.3 Manuel måling af temperatur

Under livevisningen på det termiske kamera kan du klikke hvor som helst på livevisningsbilledet for at få vist temperaturen på forskellige punkter, så du hurtigt kan lokalisere brandkilden.

Trin

Bemærk

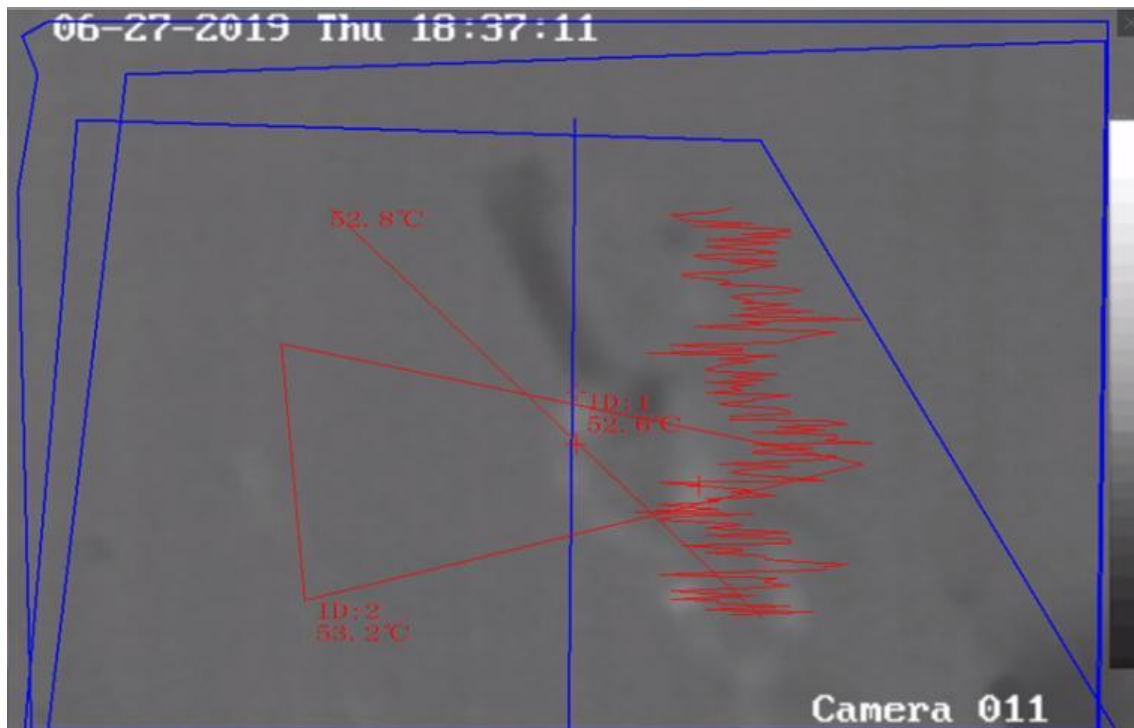
- Den målte temperatur vises på billedet i 5 sekunder.
- Kun ét punkts temperatur kan vises.
- Når flere klienter modtager livevideo fra et kamera, vil andre klienters livevisning også blive påvirket, hvis en klient tilføjer eller sletter målepunkterne. Målepunkterne ryddes, hvis alle brugere stopper livevisningen af kameraet.

-
1. Gå ind på Main View-siden, og start livevisningen af et termisk kamera.

Bemærk

Se **Start** live-visning for at starte **live-visning**.

2. Højreklik på live view-billedet, og vælg **Vis temperaturinformation**.
3. Klik på live view-billedet for at vise temperaturen i denne position.
Temperaturen på de klickede punkter vises på billedet.



Figur 5-12 Manuel måling af temperatur på punkter

4. Valgfrit: Højreklik på live view-billedet, og vælg **Hide Temperature Information** i menuen.

5.11.4 Vis skærmområde til detektering af brandkilder

Afskærmningsområde for detektering af brandkilde er et foruddefineret område, der kan afskærmes fra at blive detekteret i detektering af brandkilde. Under livevisning kan du vise området på billedet.

Højreklik på et live view-billede, og vælg **Display Shield Area**. Skjoldområdet vil blive vist på kameraets termiske billede.

Bemærk

- Denne funktion skal understøttes af enheden.
- Sørg for, at du har aktiveret og konfigureret funktionen Fire Source Detection Shield for enheden. Se enhedens brugervejledning for detaljer.



Figur 5-13 Område med brandkildeafskærmning

5.13 Flere funktioner

Der er nogle flere funktioner, der understøttes i livevisningen, herunder forhåndsvisning af hjælpeskærm, digital zoom, kanal-nul, tovejslyd, kamerastatus og synkronisering.

Forhåndsvisning af hjælpeskærm

Vis livevideoen på forskellige ekstraskærme, så du nemt kan få vist flere overvågningsscener.

Bemærk

Der understøttes op til 3 ekstra skærme.

Digital zoom

Træk musen for at tegne et rektangelområde i nederste højre/øverste venstre retning for at zoome ind eller ud på det tegnede område. Eller brug musehjulet til at zoome ind eller ud i visningen i digital zoom-tilstand.

Channel-Zero

For enhedens kanal-nul skal du holde Ctrl-tasten nede og dobbeltklikke for at få vist den specifikke kanal. Hold **Ctrl-tasten nede**, og dobbeltklik igen for at gendanne.

To-vejs lyd

Tovejs lydfunktion gør det muligt at tale med kameraet. Du kan ikke kun få live video, men også lyd i realtid fra kameraet. Hvis enheden har flere tovejs lydkanaler, kan du vælge en kanal for at starte tovejs lyd.

Bemærk

- Tovejslyden kan kun bruges til ét kamera ad gangen.
 - ABUS Link Station-enheden understøtter ikke valg af kanal under tovejs-lyd.
-

Kameraets status

Kameraets status, såsom optagestatus, signalstatus, forbindelsesnummer osv., kan registreres og vises til kontrol. Statusoplysningerne opdateres hvert 10. sekund.



Synkronisering

Synkroniseringsfunktionen gør det muligt at synkronisere enhedens ur med den pc, der kører klientsoftwaren.

Indstil strømtype

Automatisk ændring af strømtype

Kameraet vælger stream-type i henhold til størrelsen på displayvinduet. Når vinduets inddelingstal er mindre end 9, vil stream-typen være main stream, ellers sub stream. Der er tre måder at indstille strømtyper på:

- Hold markøren på et kameras navn i ressourcelisten, og klik på  → **Stream** for at vælge en streamtype, eller klik på **Auto-Change Stream Type**. Eller du kan udføre denne handling for en enhedsgruppe for at indstille streamtype for alle enheder i denne gruppe.
 - Klik på  i værktøjslinjen for livevisning, og vælg en stream-type. Se [Indstil ikoner vist på værktøjslinjen](#) for detaljer om redigering af værktøjslinjen.
 - Højreklik på et live view-vindue, og klik på **Stream** for at vælge en streamtype til kameraet.
-

Bemærk

Denne funktion skal understøttes af enheden.

Lås klienten i fuldskræmstilstand

Tryk på **Ctrl** og **L** på tastaturet for at låse klienten, når du er gået i fuldskræmstilstand. Når du har låst klienten, vil du ikke kunne betjene klienten, inklusive de andre vinduer i den aktuelle vinduesopdelingstilstand. Klik på **Lås op** i toppen, indtast login-adgangskoden til klienten, og klik på **Lås op** for at låse klienten op.

Kapitel 6 Fjernafspilning

Enheden optager videoen i henhold til optagelsesplanen. Du kan se de videofiler, der er gemt på lagringsserveren og den lokale enhed, for at gendanne hændelsesprocessen til postmortem-analyse og foretage den videre vurdering. Lagring af de værdsatte videooptagelser kan give grundlæggende materialer til videoanalyse og videobevis. Klienten understøtter flere afspilningstilstande, f.eks: VCA-afspilning, begivenhedsafspilning osv.

Bemærk

Der er to afspilningstilstande: den ene er øjeblikkelig afspilning i hovedvisningsmodulet (se **Øjeblikkelig** afspilning for detaljer), den anden er søgning efter videofiler og afspilning af videofiler i Remote Playback-modulet. I dette kapitel introducerer vi kun afspilning i Remote Playback-modulet.

6.2 Konfiguration af fjernlager

Videofilerne og de optagne billeder kan gemmes på harddiske, netharddiske eller SD/SDHC-kort på den lokale enhed eller på den tilsluttede lagringsserver.

Bemærk

Denne funktion skal understøttes af enheden.

6.2.1 Gem billede og video på DVR, NVR eller netværkskamera

Nogle lokale enheder, herunder DVR'er, NVR'er og netværkskameraer, har lagringsenheder som HDD'er, Net HDD'er og SD/SDHC-kort til video- og billedfiler. Du kan indstille en optagelsesplan eller capture schedule for kanalerne på de lokale enheder.

Før du går i gang

Sørg for, at de nyinstallerede lagerenheder er formateret. Se **Format Storage Server's HDD** for detaljer.

Udfør denne opgave, når du skal gemme billed- og videofiler på en kodningsenhed som DVR, NVR eller netværkskamera.

Trin

Bemærk

De billeder, der optages via optagelsesplanen, gemmes på den lokale enhed og kan søges frem på enhedens fjernkonfigurationsside.

1. Gå ind i modulet Storage Schedule.
2. Vælg kameraet på listen Kameragruppe.
3. Sæt kontakten **Recording Schedule** eller **Capture Schedule** til ON i **Storage on Encoding Device**-området for at aktivere lokal optagelse eller capture på enheden.
4. Vælg skabelonen til optagelses- eller capture-planen fra rullelisten.

Skabelon til hele dagen

Kontinuerlig optagelse hele dagen.

Ugedagsskabelon

Kontinuerlig optagelse i arbejdstiden fra kl. 8.00 til 20.00.

Begivenhedsskabelon

Hændelsesudløst optagelse hele dagen.

Skabelon 01 til 08

Faste skabeloner til specifikke skemaer. Du kan redigere skabelonerne efter behov.

Brugerdefineret

Tilpas en skabelon, som du vil.

Bemærk

Hvis du har brug for at redigere eller tilpasse skabelonen, se [Konfigurer skabelon til optagelsesplan](#) eller [Konfigurer skabelon til optagelsesplan](#).

5. Klik på **Advanced** of Recording Schedule for at indstille de avancerede optagelsesparametre.

Bemærk

De viste elementer varierer afhængigt af enhederne.

Forudindspilning

Bruges normalt til begivenhedsudløst optagelse, når du vil optage, før begivenheden sker.

Efter optagelse

Når begivenheden er slut, kan videoen også optages i et bestemt tidsrum.

Opbevar videofiler til

Den tid, videofilerne skal opbevares på lagerenheden, og når den overskrides, slettes filerne. Filerne gemmes permanent, hvis værdien er sat til 0.

Redundant optagelse

Gem videofilerne ikke kun på R/W-harddisken, men også på den redundante harddisk.

Optag lyd

Optag videofilerne med lyd eller ej.

Videostream

Vælg stream-typen for optagelsen.

Bemærk

For bestemte typer enheder kan du vælge **Dual-Stream** til optagelse af både kameraets hovedstrøm og understrøm. I denne tilstand kan du skifte streamtype under fjernafspilning. Se **Normal afspilning** for skift af stream under afspilning.

- Klik på **Advanced** of Capture Schedule for at indstille de avancerede parametre for optagelsen.

Opløsning

Vælg opløsningen for de kontinuerlige eller begivenhedsoptagede billeder.

Billedkvalitet

Indstil kvaliteten for de kontinuerlige eller begivenhedsoptagede billeder.

Interval

Vælg det interval, der refererer til tidsperioden mellem to optagelseshandlinger.

Optaget billede nummer

Indstil billednummeret til begivenhedsoptagelse.

- Det er valgfrit: Klik på **Kopier til...** for at kopiere indstillingerne for optagelsesplanen til andre kanaler.
- Klik på **Gem** for at gemme indstillingerne.

6.2.3 Gem billede og yderligere oplysninger på lokal pc

Du kan gemme billederne og de yderligere oplysninger, såsom varmekortet, data om antal personer og vejtrafikdata, på den lokale pc.

Udfør denne opgave, når du har brug for at gemme billeder og yderligere oplysninger på den lokale pc.

Trin

- Gå ind i modulet **Storage Schedule**.
- Vælg kameraet på listen Kameragruppe.

Bemærk

Denne funktion skal understøttes af enheden.

- Vælg lagringsindhold.

Opbevaring af billeder

Gem alarmbillederne fra kameraet, når der opstår en hændelse. Du kan klikke på **Systemkonfiguration** → **Filer** for at ændre stien til lagring af billeder.

Yderligere oplysninger Opbevaring

Gem de ekstra oplysninger (f.eks. varmekort, data om optælling af personer osv.) på den lokale pc.

4. Klik på **Gem** for at gemme indstillingerne.

6.2.4 Konfigurer skabelonen til optagelsesplanen


Du kan redigere skabelonen til optagelsesplanen eller tilpasse en skabelon til optagelsesplanen.

Trin

1. Gå ind i modulet Storage Schedule.

2. Åbn vinduet med skabelonindstillinger.

Vælg **Template 01** to **Template 08** fra rullelisten, og klik på **Edit**. Select **Custom** fra rullelisten.

3. Træk på tidslinjen for at indstille tidsperioderne for den valgte skabelon, når markøren skifter til  .


Kontinuerlig

Normal og kontinuerlig optagelse. Tidslinjen for tidsplanen er markeret med  .

Optagelse af begivenheder

Optagelsen udløses af en begivenhed. Tidslinjen for tidsplanen er markeret med  .

Kommando


Optagelsen udløses af en kommando. Tidsplanen er markeret med  .

Bemærk


Der kan indstilles op til 8 tidsperioder for hver dag i optagelsesplanen.


4. Valgfrit: Når du har indstillet tidsperioderne, kan du gøre et eller flere af følgende:


Flyt dig Træk i en tidsperiode for at flytte den, når markøren skifter til  .

Forlæng eller forkort Vælg en tidsperiode, og forlæng eller forkort den, når markøren skifter til  .

Indstil nøjagtig tid Klik på en tidsperiode for at indstille det nøjagtige start- og sluttidspunkt for perioden.

Slet Vælg den konfigurerede tidsplanperiode, og klik på  for at slette den.

Slet alle Klik på  for at slette alle de konfigurerede tidsperioder.

Kopier til Vælg en dato, og klik på  for at kopiere datoens tidsperiodeindstillinger til de andre datoer.

5. Valgfrit: For skabelon 01 til 08 kan du redigere skabelonnavnet, som du vil.

6. Klik på **OK** for at gemme indstillingerne.


 **Bemærk**

Hvis du vælger **Brugerdefineret** for at tilpasse en skabelon, kan du klikke på **Gem som skemaskabelon**, og så kan den tilpassede skabelon gemmes som skabelon 01 til 08.

6.2.5 Konfigurer skabelonen til optagelsesplanen

Du kan redigere skabelonen til optagelsesplanen eller tilpasse en skabelon til optagelsesplanen.

Trin

1. Gå ind i modulet Storage Schedule.
2. Åbn vinduet med skabelonindstillinger.
Vælg **Template 01** to **Template 08** fra rullelisten, og klik på **Edit.Select Custom** fra rullelisten.
3. Træk på tidslinjen for at indstille tidsperioder for den valgte skabelon, når markøren skifter til  .






Kontinuerlig indfangning

Normal og kontinuerlig optagelse. Tidsplanen er markeret med  .

Optagelse af begivenheder

Optagelsen udløses af en begivenhed. Tidslinjen for tidsplanen er markeret med  .

4. Valgfrit: Når du har indstillet tidsperioden, kan du gøre et eller flere af følgende

- | | |
|------------------------------|---|
| Flyt dig | Når markøren skifter til  , kan du flytte den tidsperiode, du lige har redigeret. Du kan også redigere det viste tidspunkt for at indstille den nøjagtige tidsperiode. |
| Forlæng eller forkort | Når markøren skifter til  , kan du forlænge eller forkorte den valgte tidsperiode. |
| Slet | Vælg en tidsperiode, og klik på  for at slette den. |
| Slet alle | Klik på  for at slette alle de konfigurerede tidsperioder. |
| Kopier til | Vælg en dato, og klik på  for at kopiere datoens indstillinger for tidsperiode til de andre datoer. |

5. Valgfrit: For skabelon 01 til 08 kan du redigere skabelonnavnet, som du vil.
6. Klik på **OK** for at gemme indstillingerne.

 **Bemærk**

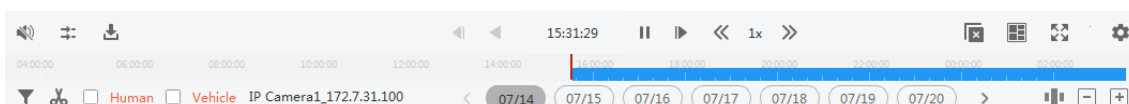
Hvis du vælger **Brugerdefineret** for at tilpasse en skabelon, kan du klikke på **Gem som skemaskabelon**, og så kan den tilpassede skabelon gemmes som skabelon 01 til 08.

6.3 Værktøjslinje til afspilning

Når du afspiller video på Remote Playback-modulet, kan du bruge værktøjerne i værktøjslinjen til at udføre forskellige funktioner.













Bemærk






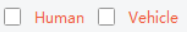

Værktøjerne i de forskellige afspilningstilstande kan være forskellige. I dette afsnit introduceres værktøjerne i kameraafspilningsmodulet.



Figur 6-2 Værktøjslinje til afspilning


Tablet 6-1 Værktøjslinje til afspilning

Ikon	Navn på ikon	Beskrivelser
	Omvendt afspilning	Afspil videofilen(erne) baglæns.
	Pause/afspil	Sæt videofilen(erne) på pause/afspil.
	Luk alle	Luk alle videofiler, der afspilles.
	Enkelt ramme (omvendt)	Afspil videofilen(erne) frame for frame baglæns.
	Enkelt ramme	Afspil videofil(er) billede for billede.
	Langsomt fremad/hurtigt fremad	Indstil afspilningshastigheden, og afspil videofilen(erne) langsomt eller hurtigt i henhold til hastigheden.
	Volumen	Klik på dette ikon for at åbne/lukke for lyden og justere lydstyrken.
	Klip	Indstil start- og sluttidspunktet for klipningen, og download den klippede videofil til den lokale disk.
	Download til flere kameraer	Indstil start- og sluttidspunkt for flere kameraer, og download videofiler fra flere kameraer samtidigt.
	Vinduesafdelingen	Indstil vinduesinddelingen.
	Fuld skærm	Afspil videofil(er) i fuld skærm. Tryk på ESC for at afslutte.
	Asynkron	Skift til asynkron/synkron afspilningstilstand.

Ikon	Navn på ikon	Beskrivelser
	afspilning/Synkron afspilning	 Bemærk Se <i>Synkron afspilning</i> for flere oplysninger.
	Indstillinger	Gå ind i modulet Video Parameters Settings, og konfigurer parametrene for livevisning og afspilning, billede, filer og værktøjslinje.
	Filter	Filtrer videofilerne efter optagelsestype.
	Nøjagtig positionering	Indstil det nøjagtige tidspunkt for afspilning af videofil(er).
	Video Dato	Datoen for den eller de videofiler, der afspilles i øjeblikket. Du kan hurtigt skifte til afspilning af videofilen(e) på en anden dato. Hvis du f.eks. skifter datoen til 30.07., vises videoen automatisk fra kl. 00.00 den 30. juli (hvis der er video på dette tidspunkt).
	Filtrer menneske- eller køretøjsrelateret video	Tjek Menneske eller Køretøj for at filtrere videoen med detekteret menneske eller detekteret køretøj. Den menneske- eller køretøjsrelaterede video vil blive markeret med orange på tidslinjen, og du kan hurtigt finde videoen på tidslinjen.  Bemærk Denne funktion skal understøttes af enheden, ellers er mennesket eller køretøjet gråt og kan ikke kontrolleres.

6.4 Normal afspilning

Du kan søge videofiler efter kamera eller gruppe til normal afspilning og downloade fundne videofiler til lokal pc. Du kan også tilføje et tag for at markere vigtige videooptagelser og så videre. Du kan højreklikke på afspilningsvinduet for at vælge de ønskede handlinger fra genvejsmenuen. Nogle af dem er listet som følger:

Navn	Beskrivelse
Vis/skjul temperaturoplysninger	<p>Vis/skjul temperaturoplysninger</p> <hr/> <p> Bemærk</p> <p>Overlejringen med temperaturoplysninger understøttes kun af termiske kameraer.</p> <hr/>
Tag-kontrol	<p>Tilføj standardtag (standardtagnavnet er TAG) eller brugerdefineret tag (tagnavnet er tilpasset) til videofilen for at markere det vigtige videopunkt. Du kan også redigere tagget eller nemt gå til tagpositionen.</p>
Andre optagelsestilstande	<ul style="list-style-type: none"> ● Udskriv taget billede: Tag et billede, og udskriv det. ● Send e-mail: Optag det aktuelle billede, og send derefter en e-mail til en eller flere modtagere. Det optagne billede kan vedhæftes. ● Brugerdefineret optagelse: Optag det aktuelle billede. Du kan redigere dets navn og derefter gemme det.


 **Bemærk**

- ABUS Link Station-enheden understøtter kun normal afspilning, og den understøtter heller ikke funktionerne baglæns afspilning, langsom fremføring eller hurtig fremføring og tilføjelse af tag.
- For NVR, som er tilføjet til klienten med enhedens andet brugernavn (undtagen admin), hvis **dobbeltbekræftelse** er aktiveret på denne NVR, skal du indtaste det brugernavn og den adgangskode, der er oprettet til dobbeltbekræftelse, når du afspiller videoer på klienten. For detaljer om dobbeltbekræftelse henvises til NVR'ens brugervejledning.

6.4.1 Søg i videooptagelser

Du kan søge i videooptagelserne efter dato, og du kan også indtaste nøgleord for at filtrere de matchede resultater til normal afspilning.

Trin

1. Gå ind i Remote Playback-modulet.
2. Klik på  til venstre for at åbne siden Camera Playback.

The screenshot displays the 'Remote Playback' window in the ABUS CMS software. The interface is divided into several sections:



- Time:** A search field containing the date and time range '08.27 00:00:00-08.27 23:59:59'. A calendar icon to the right of the field is highlighted with a red box.
- Resource:** A search field labeled 'Search' with a magnifying glass icon. Below it is a list of camera resources, each with a camera icon and a name. The list includes several 'IP Camera...66.76.180' entries, 'Camera1_fisheye', 'IP Camera...ure alarm' (highlighted with a red bar), and 'Camera1_temperature'. A folder icon and the IP address '10.66.76.125' are visible at the bottom of the list.
- Event Type:** A dropdown menu currently set to 'Motion Detection'.
- Search:** A prominent red button labeled 'Search' at the bottom of the filter section.
- Playback Area:** A large grey area on the right side of the window, currently blank, with a mouse cursor visible. Below this area is a playback control bar with icons for mute, full screen, and navigation, and a time display showing '14:00'.

Red boxes highlight the calendar icon in the Time field and the list icon in the sidebar.

Figur 6-3 Søg i videofiler

3. Valgfrit: Klik på  for at angive startdato og slutdato for søgeperioden.

 **Bemærk**

I kalenderen vil den dato, hvor videooptagelserne er optaget efter en tidsplan, blive markeret med , og den dato, hvor videooptagelserne er optaget efter en begivenhed, vil blive markeret med .

4. Start afspilning af kamera (er) for at søge i videooptagelserne fra det/de valgte kamera (er). Du kan gøre et af følgende for at starte afspilningen.

 **Bemærk**

Der kan søges på op til 16 kameraer samtidigt.

- Træk kameraet eller gruppen til et visningsvindue.
- Vælg et visningsvindue, og dobbeltklik på kameraet eller gruppen for at starte afspilningen i det valgte vindue.
- Dobbeltklik på kameraerne efter tur for at vælge visningsvinduet automatisk og starte afspilningen i vinduerne.

6.4.2 Afspil videooptagelser

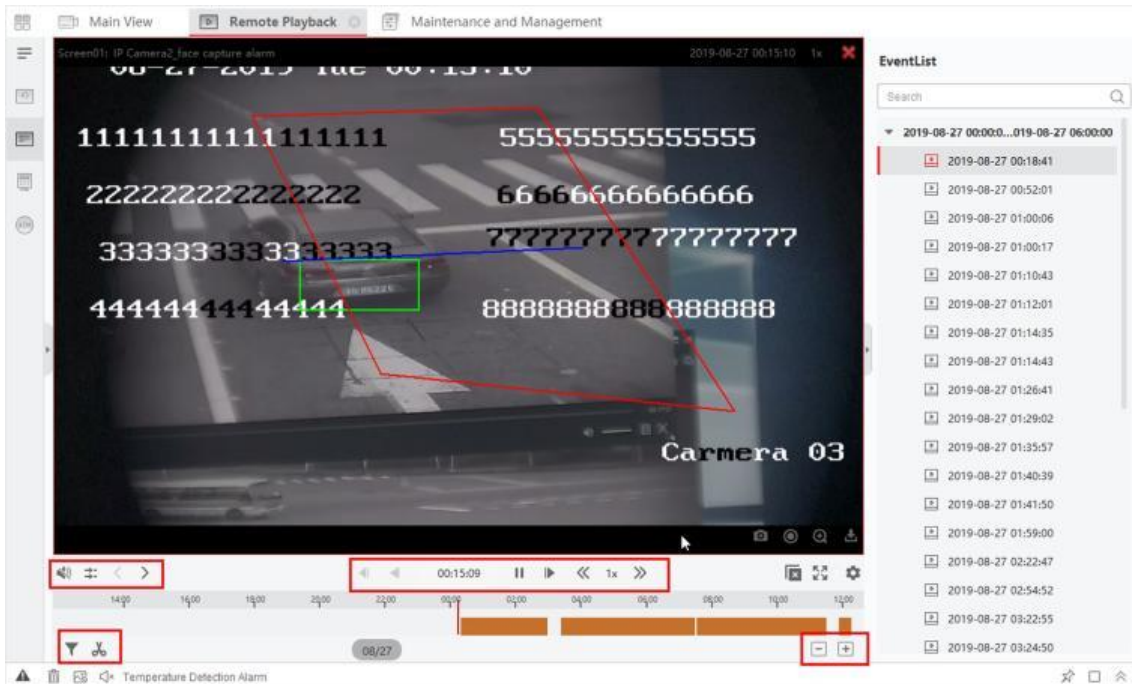
Når du har søgt efter videooptagelser til normal afspilning, kan du afspille videoen via tidslinjen.

Trin

1. Gå ind i Remote Playback-modulet.
2. Søg i videooptagelserne.
3. Afspil video via tidslinje.


Du kan klikke på **Stream** → **Main Stream / Sub Stream** for at skifte streamtype til afspilning efter dit aktuelle behov.

Videooptagelserne afspilles automatisk. Du kan klikke på tidslinjen for at placere det ønskede videosegment på det angivne tidspunkt til normal afspilning.




Figur 6-4 Afspil videooptagelser

Bemærk



- Tidslinjen angiver varigheden af videooptagelserne, og videooptagelser af forskellige typer er farvekodede. Under afspilning kan du se oplysninger om bitrate, frame rate og opløsning på billedet.
- Du kan bruge musehjulet eller klikke på  for at op- eller nedskalere tidslinjebjælken.

4. Valgfrit: Udfør følgende handlinger på værktøjslinjen for at styre afspilningen.


Enkelt ramme (omvendt)

Klik på  eller rul ned med musehjulet for at afspille videooptagelserne billede for billede (baglæns).

Lydkontrol

Klik på  eller  for at tænde/slukke for lyden. Du kan også justere lydstyrken, når du tænder.


Download til flere kameraer

Klik på  for at downloade videooptagelser fra flere kameraer på samme tid.

Bemærk

For flere detaljer, se [***Download til flere kameraer.***](#)

Download videofiler efter dato


Klik på  for at downloade kameraets videooptagelser efter dato og klokkeslæt og gemme dem på den lokale pc. Status for downloading vises i øverste højre hjørne af siden, og du kan manuelt sætte

downloadingen på pause.

Nøjagtig positionering

Klik på **09:25:46** for at indstille det nøjagtige tidspunkt for afspilning af videofilen.

Spring til billedet af et miniaturebillede

Klik på  i nederste højre hjørne for at aktivere miniaturefunktionen, og placer markøren på tidslinjen for at vise miniaturebilledet af punktet. Klik på miniaturebilledet for at hoppe til billedet af det.

Bemærk

Denne funktion skal understøttes af enhederne.

6.5 Afspilning af alarmindgang

Når alarmindgangen udløses, og den tilknyttede video kan søges efter afspilning af alarmindgang. Denne funktion kræver understøttelse af den tilsluttede enhed.

Se **Normal** afspilning for en beskrivelse af værktøjslinjen til afspilning af alarmindgang og højrekliksmenuen i visningsvinduet.


Bemærk

Nogle ikoner er muligvis ikke tilgængelige for afspilning af alarmindgang.

6.5.1 Søg i videooptagelser

Du kan søge i videooptagelserne efter dato, og du kan også indtaste nøgleord for at filtrere de matchede resultater til afspilning af alarminput.


Trin

1. Gå ind i Remote Playback-modulet.
2. Klik på  til venstre for at åbne siden Event Playback.

The screenshot displays the 'Remote Playback' view of the ABUS CMS software. The interface is divided into several sections:

- Header:** 'Main View' and 'Remote Playback' tabs are visible at the top.
- Time Filter:** A date and time range is set to '08.27 00:00:00-08.27 23:59:59'. A calendar icon to the right of the input field is highlighted with a red box.
- Resource Filter:** A search bar is present above a list of resources. A red box highlights the entire list of resources.
- Resource List:** The list contains 13 items, each with a bell icon and a text label: A1_10.66.76.125, A2_10.66.76.125, A3_10.66.76.125, A4_10.66.76.125, A5_10.66.76.125, A6_10.66.76.125, A7_10.66.76.125, A8_10.66.76.125, A9_10.66.76.125, A10_10.66.76.125, A11_10.66.76.125, A12_10.66.76.125, and A13_10.66.76.125.
- Event Type Filter:** A dropdown menu is located at the bottom, currently showing 'Alarm Input'. This dropdown is highlighted with a red box.


Figur 6-5 Søg i videofiler

3. Vælg en alarmindgangskanal til venstre.
4. Valgfrit: Klik på  for at angive startdato og slutdato for søgeperioden.
5. Vælg **Alarm Input** fra rullelisten som hændelsestype.
6. Klik på **Søg** for at starte søgningen.
De matchede videooptagelser af den valgte alarmindgang vises på højre side i kronologisk rækkefølge. Og som standard afspilles den første video automatisk.
7. Valgfrit: Indtast søgeord i feltet **Søg** for at filtrere resultaterne.

6.5.2 Afspil videooptagelser

Når du har søgt efter videooptagelser til afspilning af alarmindgang, kan du afspille videoen via filliste eller tidslinje.

Trin


1. Gå ind i Remote Playback-modulet.
2. Klik på  til venstre for at åbne siden Event Playback.
3. Søg i videooptagelserne af alarmindgangen.

Bemærk

Se [Søg i videooptagelser](#) for detaljer om søgning i videooptagelser af alarmindgangen.

4. Afspil video via filliste eller tidslinje.
 - Dobbeltklik på videooptagelserne for at afspille videoen i afspilningsvinduet.
 - Klik på tidslinjen for at placere det ønskede videosegment i det angivne tidsrum til afspilning af alarmindgang.

Bemærk

- Tidslinjen angiver varigheden af videooptagelserne, og videooptagelser af forskellige typer er farvekodede.
 - Du kan bruge musehjulet eller klikke på  for at skalere tidslinjebjælken op eller ned.
-

6.6 Afspilning af begivenheder

De optagede videofiler, der udløses af en hændelse, som f.eks. bevægelsesdetektering, VCA-detektering eller detektering af unormale hændelser, kan søges efter til afspilning af hændelser. Denne funktion kræver understøttelse af den tilsluttede enhed.

Se [**Normal**](#) afspilning for en beskrivelse af værktøjslinjen til afspilning af begivenheder og højrekliksmenuen i visningsvinduet.



Bemærk

Nogle ikoner er muligvis ikke tilgængelige til afspilning af begivenheder.



6.6.1 Søg i videooptagelser/billeder

Du kan søge i eventvideoer/billeder efter dato og eventtype.

Trin

1. Gå ind i Remote Playback-modulet.
2. Klik på  til venstre for at åbne siden Event Playback.
3. Klik på  for at indstille start- og slutdatoen for søgningen.

Bemærk

I kalenderen vil den dato, hvor videooptagelserne er optaget efter en tidsplan, blive markeret med , og den dato, hvor videooptagelserne er optaget efter en begivenhed, vil blive markeret med .

4. Vælg **Video** eller **Picture** som det indhold, du vil søge efter.
5. Vælg et kamera fra ressourcelisten.
6. Vælg en hændelsestype fra rullelisten **Hændelsestype**.
7. Klik på **Søg**.
 - Hvis du vælger **Video** som det søgte indhold, vil de matchede videooptagelser blive vist på højre side i kronologisk rækkefølge. Og som standard afspilles den første videofil automatisk.
 - Hvis du vælger **Picture** som det søgte indhold, vil de matchede billeder automatisk blive vist på højre side.


6.6.2 Se videooptagelser/billeder

Når kameraet registrerer hændelser (såsom krydsning af linjer, bevægelsesregistrering og registrering af unormale hændelser), eller den udendørs station udfører videosamtale, vil det udløse det forbundne kameras optagelse af video eller tage billeder. Du kan søge i videooptagelserne eller billederne og afspille videoerne via fillisten eller tidslinjen og se billederne efter tur.

Trin

Bemærk


For den udendørs station er det kun DS-KV8123-M, der understøtter følgende funktioner.

1. Gå ind i Remote Playback-modulet.
 2. Klik på  til venstre for at åbne siden Event Playback.
 3. Søg i videooptagelser eller billeder optaget/fanget baseret på begivenhed.
-









4. Se videooptagelser eller billeder.

- Dobbeltklik på videooptagelserne for at afspille videoen i afspilningsvinduet.
- De søgte billeder afspilles automatisk.

Bemærk

- Tidslinjen angiver videofilernes varighed, og videofiler af forskellige typer er farvekodede.
 - Du kan bruge musehjulet eller klikke på  for at op- eller nedskalere tidslinjebjælken.
-

5. Det er valgfrit: Udfør følgende handlinger, hvis du har brug for det.

Afspil optagelser fra en bestemt tid	Klik på tidslinjen for at vise et videosegment af det angivne tidspunkt til afspilning af begivenheden.
Vis optagelser med menneske og/eller køretøj	Under tidslinjen skal du markere Menneske og/eller Køretøj for at få vist optagelser, der indeholder mennesker eller køretøjer.
Skift billeder	Klik på  eller  for at gå til forrige eller næste billede.
Indstil interval for billedvisning	Klik på  for at indstille intervallet for billedvisning.
Vis billeder i fuld skærm	Klik på  for at vise billeder i fuldskræmstilstand.
Vis billeder i listetilstand	Klik på  for at vise billeder i listetilstand. Klik på  for at skifte til miniature-tilstand.
Download billeder	Klik på  og tjek billederne, og klik på Download for at downloade de valgte billeder til din pc.
Download videoer	Klik på  , vælg flere videofiler, og klik på Download for at downloade videofiler til din pc.

6.9 Afspilning af VCA

For de søgte videofiler kan du indstille en VCA-regel til at finde de videooptagelser, hvor der opstår en VCA-hændelse, f.eks. bevægelsesdetektering, linjekrydsningsdetektering og indtrængningsdetektering. Denne funktion hjælper med at finde den video, som du måske er mere bekymret for, og markere den med rød farve.


Før du går i gang

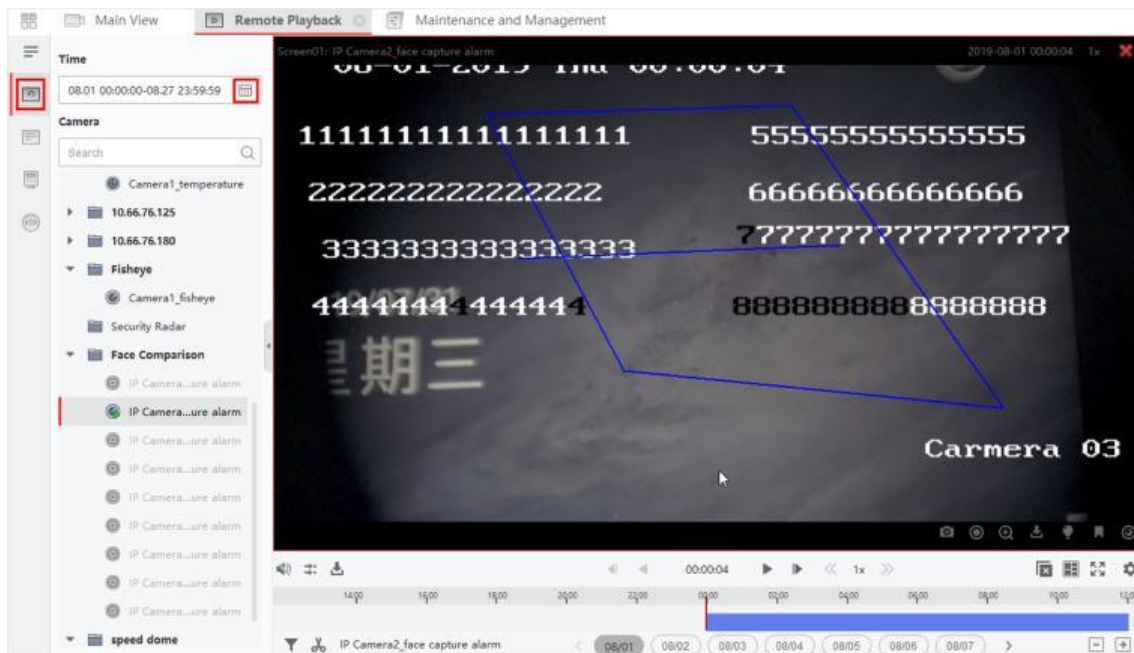
Sørg for, at enheden med VCA-funktion er installeret.

Trin


Bemærk

VCA-afspilning understøttes kun i et enkelt vindue, synkron og asynkron afspilning understøttes ikke.

1. Gå ind i Remote Playback-modulet.
2. Klik på  til venstre for at åbne siden Camera Playback.
3. Vælg kameraet, og start kameraets videoafspilning.



Figur 6-9 VCA-afspilning

4. Gå ind i menuen VCA Search.
 - Højreklik på afspilningsvinduet for at åbne genvejsmenuen, og klik derefter på **VCA Search**.
 - Klik på  i nederste højre hjørne af afspilningsvinduet.
5. Aktivér VCA-typen, tegn detekteringsområdet, og indstil følsomheden.

Registrering af bevægelse

Når visningen af videoen ændres (f.eks. hvis en person passerer, eller linsen flyttes), markeres videooptagelserne med rød farve på tidslinjen, som bruges til den automatiske alarmscene eller scenen uden vagt.

Detektion af jernbaneoverskæringer

Du kan tegne en virtuel linje på videoen, og videooptagelserne vil blive markeret med rød farve på tidslinjen, når klienten bidirektionalt registrerer personer, køretøjer og andre bevægelige objekter, der krydser den virtuelle linje.

Registrering af indtrængen

Du kan tegne en virtuel region på videoen, og videooptagelserne vil blive markeret med rød

farve på tidslinjen, når der er mennesker, køretøjer og andre bevægelige objekter, der trænger ind i den foruddefinerede region.

VCA-indstillinger

Indstil følsomheden, og filtrer de søgte videofiler ved at indstille måltegnene. Videooptagelserne vil blive markeret med rød farve på tidslinjen, når en person (hvis attributter matcher de indstillede attributter) optræder i videoen.

Bemærk

Jo højere følsomhed, jo mere præcis er den matchede person.

6. Valgfrit: Klik på  for at angive startdato og slutdato for søgeperioden.

7. Start afspilning af VCA.

De VCA-hændelser, der sker i det definerede område, bliver markeret med rødt på tidslinjen.

Bemærk

- Som standard vil afspilningshastigheden for den berørte video være 1X, og afspilningshastigheden for den uberørte video vil være 8X.
 - Du kan indstille til at springe den uberørte video over under VCA-afspilning i Systemkonfiguration, og den uberørte video vil ikke blive afspillet under VCA-afspilning. Se **Indstil livevisning og afspilningsparametre** for detaljer.
 - Hvis du har brug for at deaktivere VCA-afspilning, skal du højreklikke på VCA-afspilningsvinduet og klikke på VCA **Search** for at deaktivere VCA-afspilning.
-


6.10 Synkron afspilning

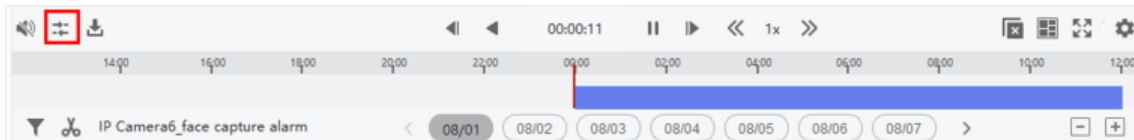
Som standard afspiller klienten videofiler fra flere kameraer i asynkron afspilningstilstand: Afspilningstiden for forskellige videofiler kan være forskellig. I synkron afspilning kan videofilerne afspilles synkroniseret.

Trin

Bemærk

- Videofiler fra op til 16 kameraer kan afspilles samtidigt.
 - Synkron og asynkron afspilning understøttes ikke i ATM-videoafspilning og VCA-afspilningstilstand.
 - Videoafspilning af begivenheder og POS-videoafspilning understøtter kun synkron afspilning. For at forbinde flere kameraer skal du gå ind i **Maintenance and Management** → **Event Management** og aktivere det forbundne kamera i henhold til begivenhedstypen.
-

1. Gå ind i Remote Playback-modulet.
2. Start afspilning af mindst to kameraer.
3. Klik på  i værktøjslinjen for at aktivere den synkrone afspilning.



Figur 6-10 Deaktiver synkron afspilning

Kameraet under afspilning vil starte synkron afspilning.

4. Klik på  for at deaktivere den synkron afspilning.

6.11 Fisheye-kameraets videoafspilning

Når du afspiller fisheye-kameraets video, kan der være forvrængning i billedet. Hvis du vil se detaljerne bedre, kan du aktivere fisheye-udvidelsesfunktionen for at korrigere visningen til en uforvrænget visning. Klienten understøtter flere fisheye-udvidelsestilstande, såsom: panorama, halv kugle, PTZ, fisheye+PTZ-tilstand.

Før du går i gang

Sørg for, at du har installeret Microsoft DirectX-komponenten.

Trin


Bemærk

Se **Normal** afspilning for andre instruktioner til **afspilningskontrol**. Nogle ikoner er muligvis ikke tilgængelige ved fiskeøjefafspilning.

1. Gå ind i Remote Playback-modulet.
2. Vælg et fisheye-kamera for at starte afspilningen.

Bemærk

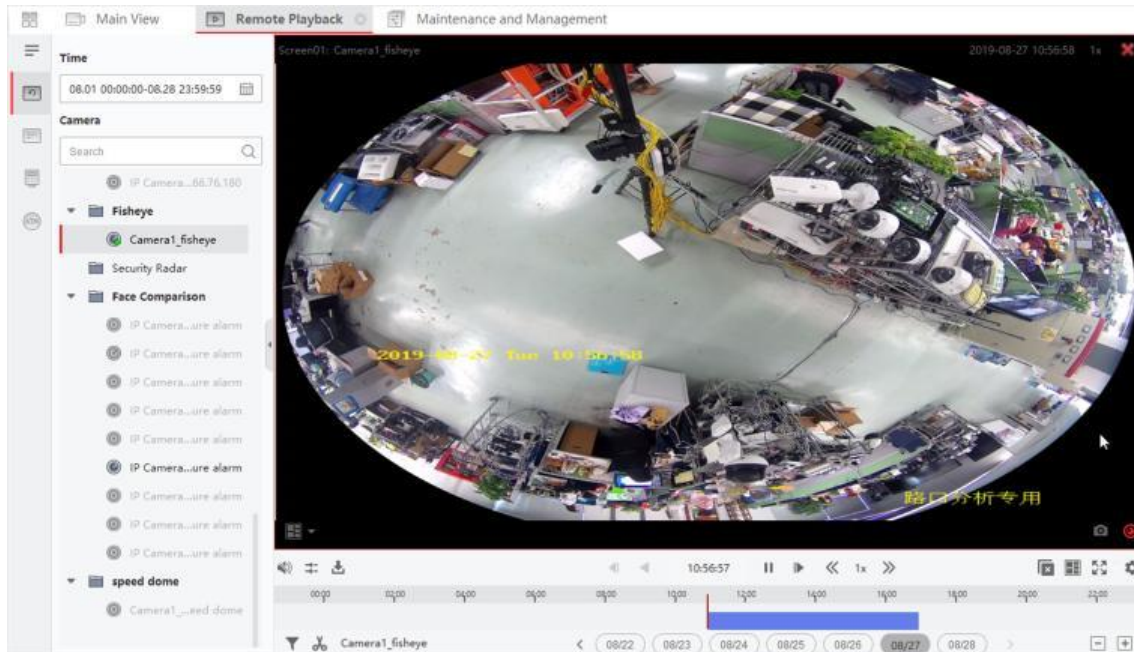
For detaljeret konfiguration af afspilning og afspilningskontrol henvises til **Normal afspilning**.

3. Gå ind i Fisheye Expansion-tilstand.
 - Højreklik på displayvinduet, og vælg **Fisheye Expansion**.
 - Klik på  i værktøjslinjen. Se **Indstil ikoner vist på værktøjslinjen** for detaljer om indstilling af værktøjslinjen.


Bemærk

Moneringstypen i afspilning af fisheye-udvidelse indstilles i henhold til moneringstypen i live view. For detaljer, se **Udfør Live View i Fisheye-tilstand**

 henvender sig til  .



Figur 6-11 Fisheye-kameraets videoafspilning

4. Klik på  i nederste venstre hjørne af displayområdet for at vælge en udvidelsestilstand til afspilning, som du ønsker.

Fisheye

I visningsfunktionen Fisheye vises hele kameraets vidvinkelvisning. Denne visningstilstand kaldes **Fisheye**, fordi den ligner synet af en fisks konvekse øje. Linsen producerer krumme billeder af et stort område, mens den forvrænger perspektivet og vinklerne på objekterne i billedet.

Panorama / Dobbelt-180° Panorama / 360° Panorama

I Panorama-visningstilstanden omdannes det forvrængede fiskeøjebillede til et normalt perspektivbillede ved hjælp af nogle kalibreringsmetoder.

PTZ

PTZ-visningen er et nærbillede af et defineret område i Fisheye-visningen eller Panorama-visningen, og den understøtter den elektroniske PTZ-funktion, som også kaldes e-PTZ.

Bemærk

Hver PTZ-visning er markeret på Fisheye-visningen og Panorama-visningen med en specifik navigationsboks. Du kan trække i navigationsboksen på Fisheye-visningen eller Panorama-visningen for at justere PTZ-visningen, eller trække i PTZ-visningen for at justere visningen til den ønskede vinkel.

Halv kugle

I halvkugle-tilstanden kan du trække i billedet og rotere det centreret om diameteren for at justere visningen til den ønskede vinkel.

AR halvkugle

AR half sphere-tilstand overlapper billeder langt væk og tæt på, så du kan se et dimensionelt billede i en vid vinkel.

Cylinder

I cylindertilstand formes billedet til en cylinderside, og du kan trække billedet fleksibelt i alle retninger for at se hele detekteringsområdet.

5. Valgfrit: Højreklik på et afspilningsvindue i Fisheye-visningstilstand, og du kan skifte det valgte vindue til fuldskærmstilstand.



Bemærk

Du kan højreklikke på vinduet og vælge **Quit Full Screen** for at afslutte fuldskærmstilstanden.

6.13 Download videooptagelser

Under afspilning kan du downloade videofiler fra et eller flere kameraer til den lokale pc.

6.13.1 Download videooptagelser efter dato

Under afspilning kan du downloade kameraets videooptagelser og gemme dem på den lokale pc.

Trin

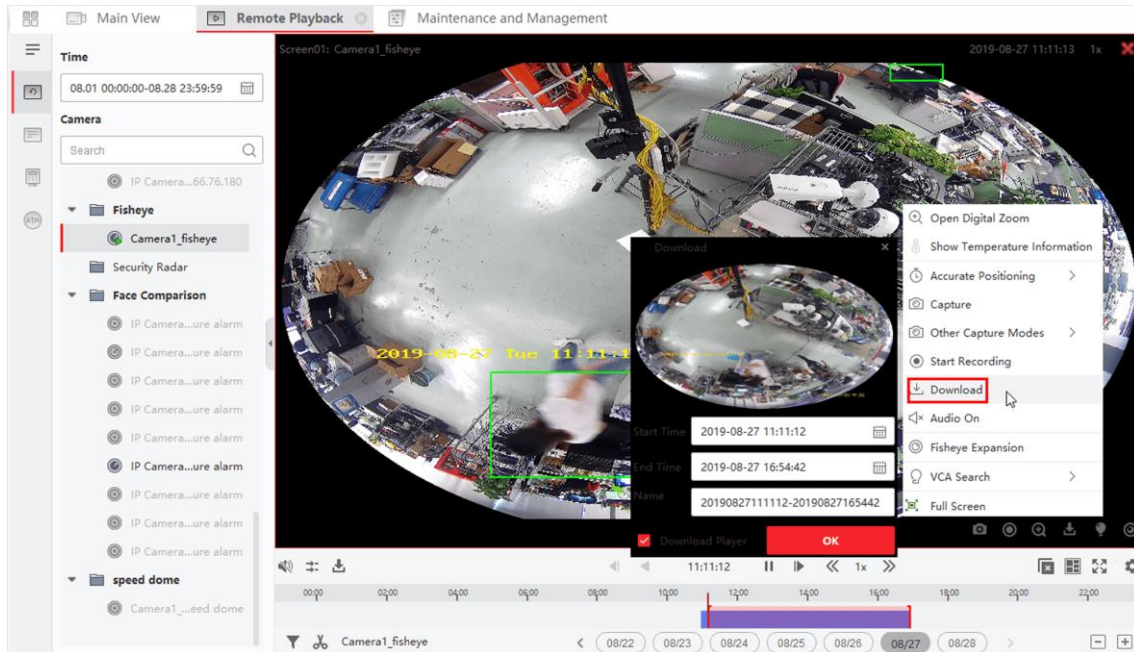
1. Gå ind på Remote Playback-siden, og vælg et kamera for at starte afspilningen.



Bemærk

For detaljer om start af afspilning, se [***Remote Playback***](#).

2. Højreklik på billedet, og klik på **Download**.



Figur 6-12 Download videooptagelser efter dato

3. Indstil start- og sluttidspunktet for de videooptagelser, der skal downloades.
4. Indtast et navn til videooptagelserne.
5. Klik på **OK** for at begynde at downloade videooptagelserne til den lokale pc.

6.13.2 Download til flere kameraer

Under afspilning af flere kameraer kan du downloade videofilerne fra flere kameraer efter dato samtidigt.

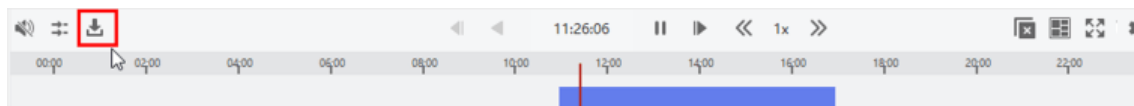
Trin

1. Gå ind på Remote Playback-siden, og vælg flere kameraer for at starte afspilningen.

Bemærk

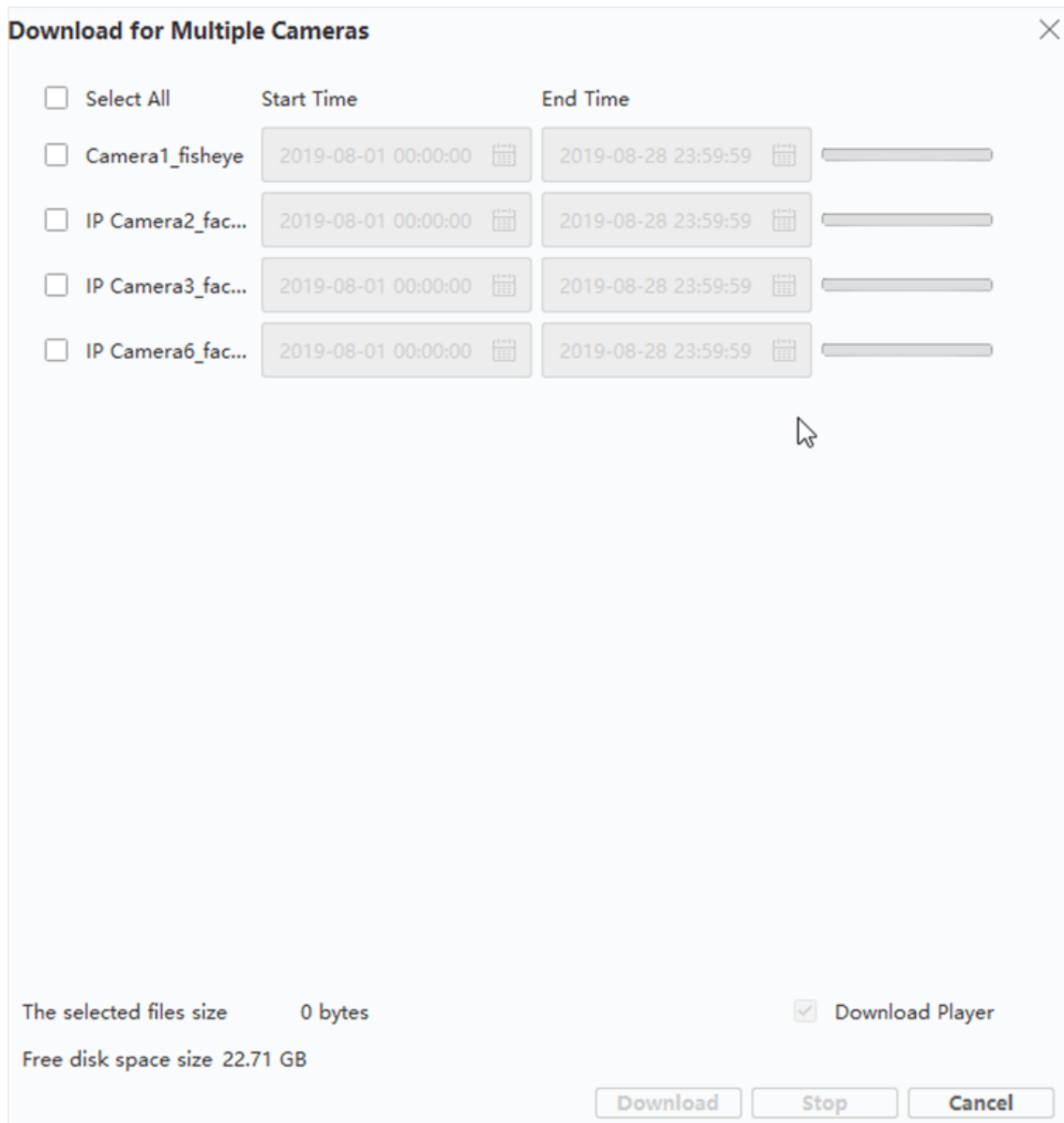
For detaljer om start af afspilning, se [Remote Playback](#).

2. Klik på  for at åbne vinduet Download for Multiple Cameras.



Figur 6-13 Værktøjslinje

- Alle kameraer i afspilning vises.
3. Vælg de kameraer, du vil downloade videofiler til.
4. Indstil start- og sluttidspunktet for videoens varighed for hvert kamera.



Figur 6-14 Vælg kameraer

5. Valgfrit: Markér **Download Player** for at downloade afspilleren.
6. Klik på **Download** for at begynde at downloade videofilerne af den/de konfigurerede varighed(er) til den lokale pc.
Fremdriftslinjen viser downloadprocessen for hvert kameras videofiler.
7. Det er valgfrit: Klik på **Stop** for at stoppe downloadingen manuelt.

 **Bemærk**

Op til 16 kameraers videofiler kan downloades samtidigt.

Kapitel 7 Hændelseskonfiguration

Event bruges til at underrette sikkerhedspersonalet om en bestemt situation, hvilket hjælper med at håndtere situationen hurtigt. Hændelsen kan udløse en række koblingshandlinger (f.eks. lydadvarel og afsendelse af e-mail) til notifikation og hændeshåndtering. Du kan aktivere hændelsen og indstille linkage action(s) for de ressourcer, der er tilføjet til klienten. Hvis de valgte hændelser sker, vil klienten modtage hændelsesnotifikationer i realtid, og du kan tjekke detaljerne og håndtere hændelserne i overensstemmelse hermed.

Video-begivenhed

Videohændelserne henviser til de særlige hændelser, der udløses af videoundtagelser, undtagelser i overvågningsområdet, alarmindgange, undtagelser i kodningsenheden osv. For flere detaljer, se [Konfigurer hændelse for kamera](#), Konfigurer hændelse [for alarmindgang](#) og [Konfigurer hændelse for kodningsenhed](#).

Begivenhed for adgangskontrol

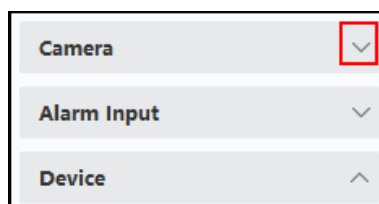
Adgangskontrolhændelser henviser til de særlige hændelser, der udløses ved adgangskontrolenheder, døre, kortlæsere, elevatorer, videointercom-enheder osv. For flere detaljer, se [Konfigurer klienthandlinger for adgangshændelse](#) og [Konfigurer videointercomhændelse](#).

7.1 Konfigurer hændelse for kamera

Hændelsen for kameraet henviser til videoundtagelsen eller de hændelser, der registreres i kameraets overvågningsområde, såsom bevægelsesdetektering, videotab, linjekrydsning og så videre. Du kan aktivere en begivenhed for kameraerne i klienten. Når hændelsen udløses på kameraet, kan klienten modtage og optage hændelsen til kontrol og udløse en række linkhandlinger (f.eks. sende e-mail) til notifikation.

Trin

1. Klik på **Hændelseskonfiguration** → **Videohændelse** → **Kamera**.



Figur 7-1 Visning af kameraressource

2. Fold gruppen ud, og vælg et kamera som begivenhedskilde.

Bemærk

Sørg for, at ressourcen er online.

Alle de hændelsestyper, der understøttes af det valgte kamera, vises.

<input type="checkbox"/>	Event Type	Priority	Trigger Client Action	Linked Camera	Enable
<input type="checkbox"/>	Audio Input Exception...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_10.6.113.250	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Face Detection Alarm	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_10.6.113.250	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Intrusion Detection Al...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_10.6.113.250	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Line Crossing Detectio...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_10.6.113.250	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Motion Detection Alar...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_10.6.113.250	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Region Entrance Dete...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_10.6.113.250	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Region Exiting Detecti...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_10.6.113.250	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Video Loss Alarm	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_10.6.113.250	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Video Tampering Det...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_10.6.113.250	<input checked="" type="checkbox"/>

Figur 7-2 Konfigurer hændelser for kamera

- Valgfrit: Indtast nøgleord i feltet **Filter** for hurtigt at finde den ønskede begivenhed.
- Valgfrit: Tænd for kontakten i kolonnen Aktiver for at aktivere hændelsestypen, eller klik på **Aktiver alle for** at aktivere alle hændelsestyper for dette kamera.

Bemærk


Når den er aktiveret, kan hændelsen modtages af klienten og udløse forbindelseshandling(er). Du kan også deaktivere en hændelsestype eller deaktivere alle hændelsestyper.

- Valgfrit: Vælg begivenhed(er), og udfør derefter følgende handlinger.

Rediger prioritet Klik på **Edit Priority** for at indstille **prioriteten** for begivenheden/begivenhederne.
 Prioritet repræsenterer hændelsens grad af nødsituation.

Rediger sammenkædning af begivenheder Klik på **Edit Event Linkage** for at angive linkage action(s) for event(s).

Hørbar advarsel

Udløs klientens akustiske advarsel, når hændelsen udløses.
 Du kan vælge lydfilen på rullelisten eller klikke på **Tilføj** for at tilføje en ny lydfil (i WAV-format).
 Du kan klikke på  for at lave en audition af den valgte lydfil.

Send e-mail


Send en e-mail med alarmoplysninger til en eller flere modtagere.

For detaljer om indstilling af e-mail-parametre, se [Indstil e-mail-parametre](#).

Pop op-vindue

Popup-vindue til visning af hændelsesrelaterede oplysninger (herunder hændelsesdetaljer, livevideo af kildekameraet, optagne billeder af det forbundne kamera) på klienten, når hændelsen udløses. Du kan også indtaste bemærkninger om, hvordan hændelsen skal håndteres.

Visning på kort

Når begivenhedskilden tilføjes som et hot spot på kortet, vil hot spottet blive vist med , der blinker til side, når begivenheden udløses, hvilket hjælper sikkerhedspersonalet med at se, hvor begivenheden finder sted.

Du kan også klikke på hotspottet for at se detaljerne om begivenheden og livevideoen fra det tilknyttede kamera.

Forbundet kamera

Forbind det valgte kamera for at tage billeder eller optage video, når hændelsen udløses.

Hvad du skal gøre nu

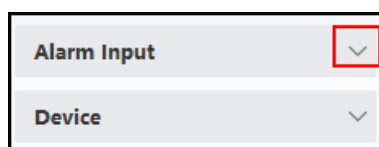
Du skal aktivere den enhed, som kameraet hører til, ellers kan klienten ikke modtage de konfigurerede hændelser. For detaljer, se [Aktiver modtagelse af hændelser fra enheder](#).

7.2 Konfigurer hændelse for alarmindgang

Hændelsen for alarmindgangen henviser til den hændelse, der udløses af alarmindgangen. Du kan aktivere en hændelse for alarmindgangene i klienten. Når alarmindgangen udløses, kan klienten modtage og registrere hændelsen til kontrol og udløse en række sammenkædningshandlinger (f.eks. sende e-mail) til notifikation.

Trin

1. Klik på **Hændelseskonfiguration** → **Videohændelse** → **Alarmindgang**.



Figur 7-3 Visning af alarmindgangsressource

2. Fold gruppen ud, og vælg en alarmindgang som hændelseskilde.

Bemærk

Sørg for, at ressourcen er online.

Alle de hændelsestyper, der understøttes af den valgte alarmindgang, vises.

3. Valgfrit: Indtast nøgleord i feltet **Filter** for hurtigt at finde den ønskede begivenhed.

4. Valgfrit: Tænd for kontakten i Enable-kolonnen for at aktivere hændelsestypen, eller klik på **Enable All** for at aktivere alle hændelsestyper for denne alarmindgang.

Bemærk

Når den er aktiveret, kan hændelsen modtages af klienten og udløse forbindelseshandling(er). Du kan også deaktivere en hændelsestype eller deaktivere alle hændelsestyper.

5. Valgfrit: Vælg begivenhed(er), og udfør derefter følgende handlinger.

Rediger prioritet

Klik på **Edit Priority** for at indstille **prioriteten** for begivenheden/begivenhederne. Prioritet repræsenterer hændelsens grad af nødsituation.


Rediger sammenkædning af begivenheder

Klik på **Edit Event Linkage** for at angive linkage action(s) for event(s).

Hørbar advarsel

Udløs klientens akustiske advarsel, når hændelsen udløses.

Du kan vælge lydfilen på rullelisten eller klikke på **Tilføj** for at tilføje en ny lydfil (i WAV-format).

Du kan klikke på  for at lave en audition af den valgte lydfil.

Send e-mail


Send en e-mail med alarmoplysninger til en eller flere modtagere.

For detaljer om indstilling af e-mail-parametre, se [Indstil e-mail-parametre](#).

Pop op-vindue

Popup-vindue til visning af hændelsesrelaterede oplysninger (herunder hændelsesdetaljer, livevideo af kildekameraet, optagne billeder af det forbundne kamera) på klienten, når hændelsen udløses. Du kan også indtaste bemærkninger om, hvordan hændelsen skal håndteres.

Visning på kort

Når begivenhedskilden tilføjes som et hot spot på kortet, vil hot spottet blive vist med , der blinker til side, når begivenheden udløses, hvilket hjælper sikkerhedspersonalet med at se, hvor begivenheden finder sted.

Du kan også klikke på hotspottet for at se detaljerne om begivenheden og livevideoen fra det tilknyttede kamera.

Forbundet kamera

Forbind det valgte kamera for at tage billeder eller optage video, når hændelsen udløses.

Hvad du skal gøre nu

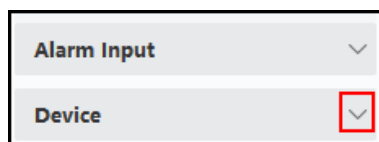
Du skal aktivere den enhed, som alarmindgangen hører til, ellers kan klienten ikke modtage de konfigurerede hændelser. For detaljer, se [Aktiver modtagelse af hændelser fra enheder](#).

7.3 Konfigurer hændelse for kodningsenhed

Hændelsen for en kodningsenhed refererer til en kodningsenheds undtagelse, såsom at enheden er offline. Du kan aktivere en begivenhed for de kodningsenheder, der er tilføjet i klienten. Når hændelsen udløses på enheden, kan klienten modtage og registrere hændelsen til kontrol og udløse en række linkhandlinger (f.eks. sende e-mail) til notifikation.

Trin

1. Klik på **Hændelseskonfiguration** → **Videohændelse** → **Enhed**.



Figur 7-4 Ressource for skærmenhed

2. Vælg en enhed som hændeskilde.

Bemærk

Sørg for, at ressourcen er online.

Alle de hændelsestyper, der understøttes af den valgte enhed, vises.

3. Valgfrit: Indtast nøgleord i feltet **Filter** for hurtigt at finde den ønskede begivenhed.
4. Valgfrit: Tænd for kontakten i kolonnen Aktiver for at aktivere hændelsestypen, eller klik på **Aktiver alle for** at aktivere alle hændelsestyper på denne enhed.

Bemærk

Når den er aktiveret, kan hændelsen modtages af klienten og udløse forbindelseshandling(er). Du kan også deaktivere en hændelsestype eller deaktivere alle hændelsestyper.

5. Valgfrit: Vælg begivenhed(er), og udfør derefter følgende handlinger.

Rediger prioritet

Klik på **Edit Priority** for at indstille **prioriteten** for begivenheden/begivenhederne. Prioritet repræsenterer hændelsens grad af nødsituation.


Rediger sammenkædning af begivenheder

Klik på **Edit Event Linkage** for at angive linkage action(s) for event(s).

Hørbar advarsel

Udløs klientens akustiske advarsel, når hændelsen udløses.

Du kan vælge lydfilen på rullelisten eller klikke på **Tilføj** for at tilføje en ny lydfil (i WAV-format).

Du kan klikke på  for at lave en audition af den valgte lydfil.

Send e-mail

Send en e-mail med alarmoplysninger til en eller flere modtagere.
For detaljer om indstilling af e-mail-parametre, se [**Indstil e-mail-parametre**](#).

Klik på **Copy for** at kopiere hændelsesindstillingerne for denne enhed til andre enheder.

 **Bemærk**

Du kan kun kopiere hændelsesindstillingerne til ressourcer af samme type.

Hvad du skal gøre nu

Du skal armere denne enhed, ellers kan klienten ikke modtage de konfigurerede hændelser. For detaljer, se [**Aktiver modtagelse af hændelser fra enheder**](#).

Kapitel 8 Eventcenter

De hændelsesoplysninger (f.eks. enhed offline), som klienten har modtaget, vises. I Event Center kan du se detaljerede oplysninger om realtidshændelser og historiske hændelser, se den hændelsesrelaterede video, håndtere hændelserne og så videre.


Før klienten kan modtage hændelsesoplysninger fra enheden, skal du først aktivere ressourcens hændelser og aktivere enheden. Se [***Event Configuration***](#) og [***Enable Receiving Event from Devices***](#) for detaljer.

Før du kan se pop-up-alarmoplysningerne, skal du aktivere hændelsesudløst pop-up-billede i hændelsescentret. For detaljer, se [***Vis pop op-hændelsesinformation***](#).

8.1 Aktivér modtagelse af hændelser fra enheder

Før klientsoftwaren kan modtage hændelsesmeddelelser fra enheden, skal du først tilkoble enheden.

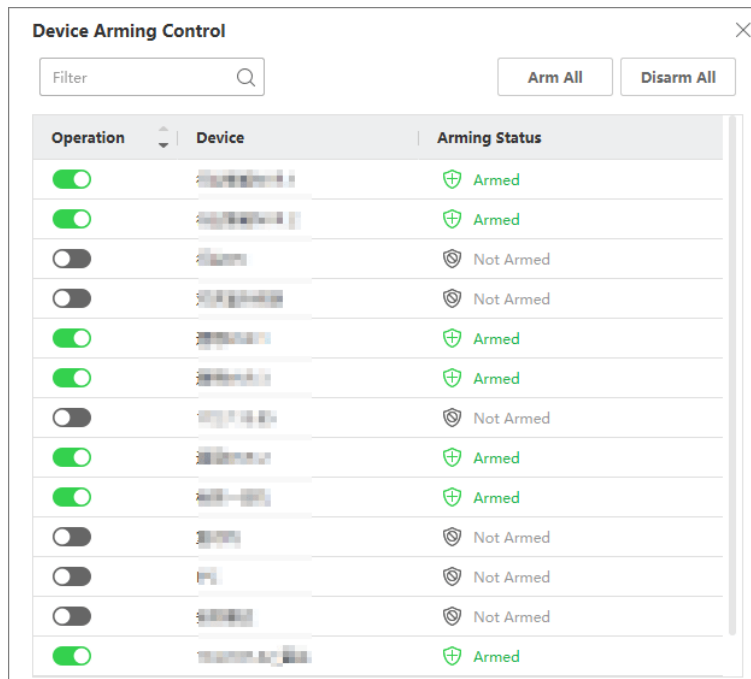
Trin

1. Klik på  → **Tool** → **Device Arming Control** for at åbne siden Device Arming Control.
Alle tilføjede enheder vises på denne side.
2. Valgfrit: Hvis der er for mange enheder, skal du indtaste nøgleordene i Filter filed for at filtrere den eller de enheder, du ønsker.

Bemærk

For de filtrerede enheder kan du klikke på **Armér alle** eller **Dearmér alle for** at aktivere modtagelse af hændelser for disse enheder.

3. I kolonnen Auto-Arming skal du tænde for kontakten for at aktivere automatisk armering.



Figur 8-1 Arm-enhed

Når den er tændt, vil enheden/enhederne blive armeret. Og meddelelser om de hændelser, der udløses af den eller de aktiverede enheder, sendes automatisk til klientsoftwaren i realtid.

8.2 Visning af realtidshændelser

De realtidshændelsesoplysninger, som klienten modtager fra de tilsluttede ressourcer, vises. Du kan tjekke realtidshændelsesoplysningerne, herunder hændelseskilde, hændelsestidspunkt, prioritet osv.

Før du går i gang

Aktivér modtagelse af hændelser fra enheder, før klienten kan modtage hændelser fra enheden, se **Aktivér modtagelse af hændelser fra enheder** for detaljer.

Trin

1. Klik på **Event Center** → **Real-time Event** for at åbne siden med realtidshændelser, og du kan se de realtidshændelser, som klienten har modtaget.

Tidspunkt for begivenhed

For kodningsenheder er hændelsestidspunktet det tidspunkt, hvor klienten modtager hændelsen. For andre enhedstyper er hændelsestidspunktet det tidspunkt, hvor hændelsen udløses.

Prioritet

Prioritet repræsenterer hændelsens grad af nødsituation.

2. Filtrer begivenhederne.

Filtrer efter enhedstype og (eller) prioritet Vælg enhedstype(r) og (eller) prioriteter for at filtrere hændelser.

Filtrer efter nøgleord Indtast nøgleordene for at filtrere begivenhederne.

3. Valgfrit: Højreklik på tabeloverskriften på hændelseslisten for at tilpasse de hændelsesrelaterede elementer, der skal vises på hændelseslisten.
4. Vælg en begivenhed i begivenhedslisten for at se detaljerne om begivenheden.

Bemærk

Når **Gem billeder i strukturdataformat** er aktiveret, vises der ingen billeder i Begivenhedsdetaljer i Event Center. For detaljer om **Gem billeder i strukturdataformat**, se Indstil [*generelle parametre*](#).

Bemærk

- Hændelsesdetaljerne omfatter de(t) optagne billede(r), video (optaget video udløst af hændelsen eller livevisning af enheden) og andre beskrivelser af hændelsen.
 - For at se den optagede video, der udløses af hændelsen, skal du linke kamera(er) med enheden i hændelseskonfigurationen. For detaljer, se [*Hændelseskonfiguration*](#).
 - Hvis du vil se de optagne billeder, skal du konfigurere lagring af billeder i lagringsplanen.
-

5. Valgfrit: Udfør følgende handlinger, hvis det er nødvendigt.

Håndter en enkelt begivenhed Klik på **Håndter** for at indtaste behandlingsforslaget, og klik derefter på **OK**.




Bemærk

Når en begivenhed er håndteret, bliver knappen **Håndter til Tilføj bemærkning**. Klik på **Tilføj bemærkning** for at tilføje flere bemærkninger til den håndterede begivenhed.

Håndter begivenheder i en batch Vælg de hændelser, der skal behandles, og klik derefter på **Håndter i batch**. Indtast behandlingsforslaget, og klik derefter på **OK**.

Aktivere/deaktivere alarmlyd Klik på **Audio On/Mute** for at aktivere/deaktivere lyden til begivenheden.

Vælg den seneste begivenhed automatisk Markér **Auto-Select Latest Event** for at vælge den seneste begivenhed automatisk, og detaljerne om begivenheden vises.

Klare begivenheder	Klik på Ryd for at rydde alle hændelser i hændelseslisten.
Send e-mail	Vælg en begivenhed, og klik derefter på Send e-mail , så sendes oplysningerne om denne begivenhed via e-mail.
<hr/>	
 Bemærk	
Du bør konfigurere e-mail-parametrene først, se <u>Indstil e-mail-parametre</u> for detaljer.	
<hr/>	
Automatisk afspilning af video	Markér Auto-Play Video for automatisk at afspille video, når der vises detaljer om begivenheden.
Forstør video eller billede	<ul style="list-style-type: none">• Dobbeltklik på videobilledet for at se videoen i et større vindue.• Placer markøren på billedet, og klik på  for at se billedet i et større vindue.
Download et indfanget billede	Hold markøren over det optagne billede, og klik på download-ikonet i nederste højre hjørne af billedet for at downloade det til den lokale pc.
Download video om begivenhedsudløsnings	Hold markøren over den optagede video, klik på  for at downloade videoen (30 sekunder før hændelsen sker) udløst af hændelsen.

8.3 Søg i historiske begivenheder

Du kan søge og se historiske hændelser ved at indstille søgebetingelser som tid, enhedstype og prioritet i klienten. For de søgte hændelser kan du håndtere og eksportere dem.

Før du går i gang

Aktivér modtagelse af hændelser fra enheder, før klienten kan modtage hændelsesoplysninger fra enheden, se [Aktivér modtagelse af hændelser fra enheder](#) for detaljer.

Trin

1. Klik på **Event Center** → **Event Search** for at åbne siden til søgning efter events.
2. Indstil filterbetingelserne til kun at vise de ønskede begivenheder.

Tid

Det tidspunkt, hvor begivenheden starter.

Søg efter

Enhed

Søg i begivenhederne efter enhed eller enhedens ressourcekanaler. Hvis der søges efter enhed, skal du indstille følgende:

- **Inkluder underknode:** Søg i enhedens hændelser og alle ressourcekanaler.
- **Enhedstype:** Vælg den enhed, som du vil søge hændelser fra.

Gruppe

Søg i begivenhederne efter ressourcekanaler i gruppen.

Bemærk

- For videointercom-enheder skal du vælge søgeområde: Alle og Låsning af log.
 - For adgangskontrolenheder kan du klikke på **Vis mere** for at angive flere betingelser: status, hændelsestype, kortlæsertype, personnavn, kortnummer og organisation.
-

Prioritet

Prioriteten inkluderer lav, medium, høj og ukategoriseret, hvilket indikerer hændelsens beredskabsgrad.

Begivenhedstype

Vælg en eller flere begivenhedstyper, der skal søges efter, fra rullelisten.

Bemærk

Du kan indtaste et nøgleord (understøtter fuzzy search) i søgefeltet for at søge i målhændelsestype(r).

Status

Status for håndtering af hændelsen.

Søg efter nøgleord

Indtast et nøgleord (understøtter fuzzy search) for hurtigt at søge efter den eller de ønskede historiske begivenheder. Du kan f.eks. indtaste en persons navn for at søge i de begivenheder, der er relateret til denne person.

3. Klik på **Søg** for at søge i begivenhederne efter de betingelser, du har angivet.

Bemærk

Når **Gem billeder i strukturdataformat** er aktiveret, vises der ingen billeder i feltet Begivenhedsdetaljer i Event Center. For detaljer om **Gem billeder i strukturdataformat**, se Indstil ***generelle parametre***.

Index	Device Name	Event Type	Event Time	Device Type	Group Name	Object Name	Object Type	Priority	Event Details
2	101	Smoke Detection Alarm	2020-03-13 18:59:32	Encoding Device	F5	Camera 1	Camera	Uncategorized	Linked Camera: Camera 1
3	101	Detector Work Status	2020-03-13 18:59:22	Encoding Device	F5	Camera 1	Camera	Uncategorized	Linked Camera: Camera 1,
4	101	Detector Work Status	2020-03-13 18:59:12	Encoding Device	F5	Camera 1	Camera	Uncategorized	Linked Camera: Camera 1,
5	101	Detector Work Status	2020-03-13 18:59:03	Encoding Device	F5	Camera 1	Camera	Uncategorized	Linked Camera: Camera 1,
6	101	Detector Work Status	2020-03-13 18:59:03	Encoding Device	F5	Camera 1	Camera	Uncategorized	Linked Camera: Camera 1,
7	101	Detector Work Status	2020-03-13 18:59:03	Encoding Device	F5	Camera 1	Camera	Uncategorized	Linked Camera: Camera 1,
8	101	Detector Work Status	2020-03-13 18:58:49	Encoding Device	F5	Camera 1	Camera	Uncategorized	Linked Camera: Camera 1,

Total 319 Record(s) 50 / 7 Page(s)

Event Details: Send Email, Handle, Hide

Picture: No picture

Handling records: No handling record.

Figur 8-2 Søg i historiske begivenheder

- Valgfrit: Højreklik på tabeloverskriften på hændelseslisten for at tilpasse de hændelsesrelaterede elementer, der skal vises på hændelseslisten.
- Vælg en begivenhed i begivenhedslisten for at se detaljerne om begivenheden.

Bemærk

- Hændelsesdetaljerne omfatter de(t) optagne billede(r), video (optaget video udløst af hændelsen eller livevisning af enheden) og andre beskrivelser af hændelsen.
- For at se den optagede video, der udløses af hændelsen, skal du linke kamera(er) med enheden i hændelseskonfigurationen. For detaljer, se ***Hændelseskonfiguration***.
- Hvis du vil se de optagne billeder, skal du konfigurere lagring af billeder i lagringsplanen.

- Valgfrit: Udfør en af følgende handlinger.

Håndter en enkelt begivenhed

Håndter en enkelt begivenhed: Vælg en begivenhed, der skal håndteres, og klik derefter på **Håndter** på siden med oplysninger om begivenheden, og indtast forslaget til håndtering.

Bemærk

Når en begivenhed er håndteret, bliver knappen **Håndter til Tilføj bemærkning**. Klik på **Tilføj bemærkning** for at tilføje flere bemærkninger til den håndterede begivenhed.

Batch-håndtering af begivenheder

Håndter hændelser i en batch: Vælg de hændelser, der skal håndteres, og klik derefter på **Håndter i batch**, og indtast forslaget til

håndtering.


Bemærk

Når en begivenhed er håndteret, bliver knappen **Håndter til Tilføj bemærkning**. Klik på **Tilføj bemærkning** for at tilføje flere bemærkninger til den håndterede begivenhed.

Automatisk afspilning af video

Markér **Auto-Play Video** for automatisk at afspille video, når der vises detaljer om begivenheden.

Forstør video eller billede

- Dobbeltklik på videobilledet for at se videoen i et større vindue.
- Placer markøren på billedet, og klik på  for at se billedet i et større vindue.

Send e-mail

Vælg en begivenhed, og klik derefter på **Send e-mail**, så sendes oplysningerne om denne begivenhed via e-mail.

Bemærk

Du bør konfigurere e-mail-parametrene først, se [Indstil e-mail-parametre](#) for detaljer.


Eksporter oplysninger om begivenheden

Klik på **Export** for at eksportere hændelsesloggen eller hændelsesbillederne til den lokale pc i en CSV/Excel-fil. Du kan indstille lagringsstien manuelt.

Download et indfanget billede

Hold markøren over det optagne billede, og klik på download-ikonet i nederste højre hjørne af billedet for at downloade det til den lokale pc.

Download video om begivenhedsudløsnin

Hold markøren over den optagede video, klik på  for at downloade videoen (30 sekunder før hændelsen sker) udløst af hændelsen.

g

8.4 Hent hændelser fra enheden

I nogle scenarier (f.eks. hvis klienten ikke kan starte op, adgangskontrolenheden er blevet armeret af en anden klient osv.) er de hændelser, der modtages af klienten og udløses på adgangskontrolenheden, ikke konsistente. Du kan hente hændelser fra enheden eksternt for at

synkronisere hændelserne fra enheden til klientens hændelsescenter.

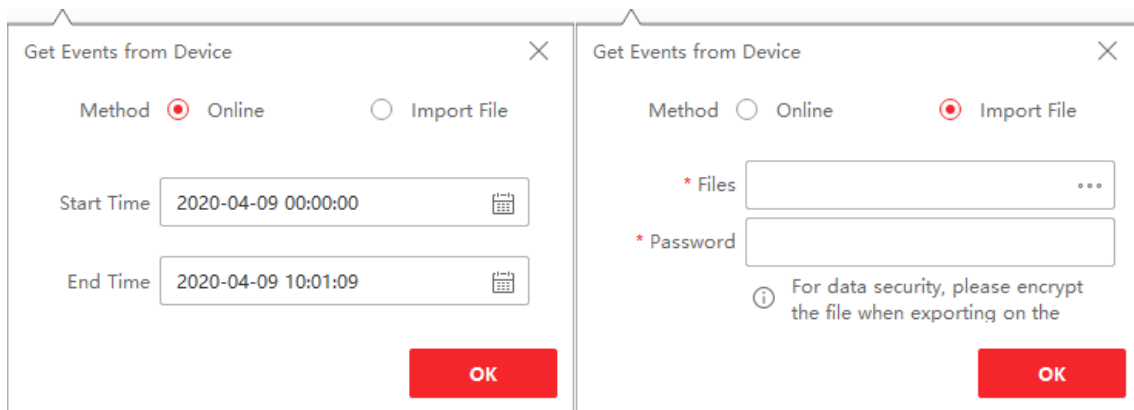
Klik på **Enhedsstyring** → **Enhed** → **Enhed**, vælg adgangskontrolenhed(er), og klik på **Hent hændelser fra enhed**.

Synkroniser begivenhederne på to måder:

- **Online**: Når enheden er online og kan kommunikere med klienten i realtid, kan du vælge **Online og** indstille starttidspunkt og sluttidspunkt for at få hændelserne i denne periode.
- **Importer fil**: Hvis netværket ikke er godt, eller enheden ikke kan kommunikere med klienten i realtid, kan du eksportere hændelsesfilen fra den valgte enhed først og importere denne eksporterede fil på klienten senere ved at vælge **Importer fil** og indtaste adgangskoden til den krypterede **fil**.

Bemærk

- Af hensyn til datasikkerheden bør du kryptere filen, når du eksporterer den til enheden. I mellemtiden skal den valgte adgangskontrolenhed være den, du eksporterede filen fra.
 - Funktionen skal være understøttet af enheden.
-



Figur 8-3 Hent hændelser fra enheden

Bemærk

Hvis du kun ønsker at hente de begivenheder, der er relateret til fremmøde, kan du også gå ind i **Time & Attendance** → **Attendance Statistics** → **Attendance Records**, klikke på **Get Events from Device** og vælge **Online** eller **Import File** for at hente begivenhederne.

8.5 Vis information om pop op-begivenhed

Hvis du har aktiveret hændelsesnotifikation og indstillet Event Triggered Pop-up Image som linkhandling, vil et vindue poppe op, når hændelsen sker, og vise hændelsesinformation, relaterede billeder og relaterede videoer.

Gå til **Event Center** → **Real-Time Event**, og klik derefter på **Enable Alarm Triggered Pop-up Image** for at aktivere funktionen.

Du kan se de hændelsesrelaterede videooptagelser (fra 30 sekunder før hændelsen til slutningen af hændelsen), det billede, der blev taget, da hændelsen fandt sted, samt hændelsesoplysninger som f.eks. hændelseskilde, tilknyttet kamera, hændelsestype osv.

Bemærk

- Når vinduet ikke er lukket, skal du klikke på **Næste** for at se de nye hændelsesoplysninger, hvis der udløses en ny hændelse.
 - Hvis du ikke har ryddet begivenhedsoplysningerne, kan du klikke på **Forrige for** at se de tidligere begivenhedsoplysninger.
 - Når **Gem billeder i strukturdataformat** er aktiveret, vises der ikke billeder i hændelsesoplysningerne. Se ***Indstil generelle parametre*** for flere detaljer.
-

Du kan markere **Auto-Update Event** for at aktivere vinduet til automatisk at skifte til de seneste hændelsesoplysninger, når en ny hændelse udløses.

Kapitel 9 Kortstyring

E-map-funktionen giver et visuelt overblik over placeringen og fordelingen af de installerede kameraer og alarmindgangsenheder. Du kan få livevisning af kameraerne på kortet, og du får en besked fra kortet, når alarmen udløses.

E-map er et statisk billede (det behøver ikke at være geografiske kort, selvom de ofte er det). Afhængigt af din organisations behov kan fotos og andre former for billedfiler også bruges som e-maps), som giver dig et visuelt overblik over placeringen og fordelingen af hot spots (ressourcer (f.eks. kamera, alarmindgang), der er placeret på kortet, kaldes hot spots). Du kan se de fysiske placeringer af kameraerne og alarmindgangene, og i hvilken retning kameraerne peger. Med funktionen hot region kan e-maps organiseres i hierarkier, så man kan navigere fra store perspektiver til detaljerede perspektiver, f.eks. fra gulvniveau til rumniveau.

9.1 Tilføj kort

Du skal tilføje et kort som det overordnede kort for hot spots og hot regions.

Trin

 **Bemærk**

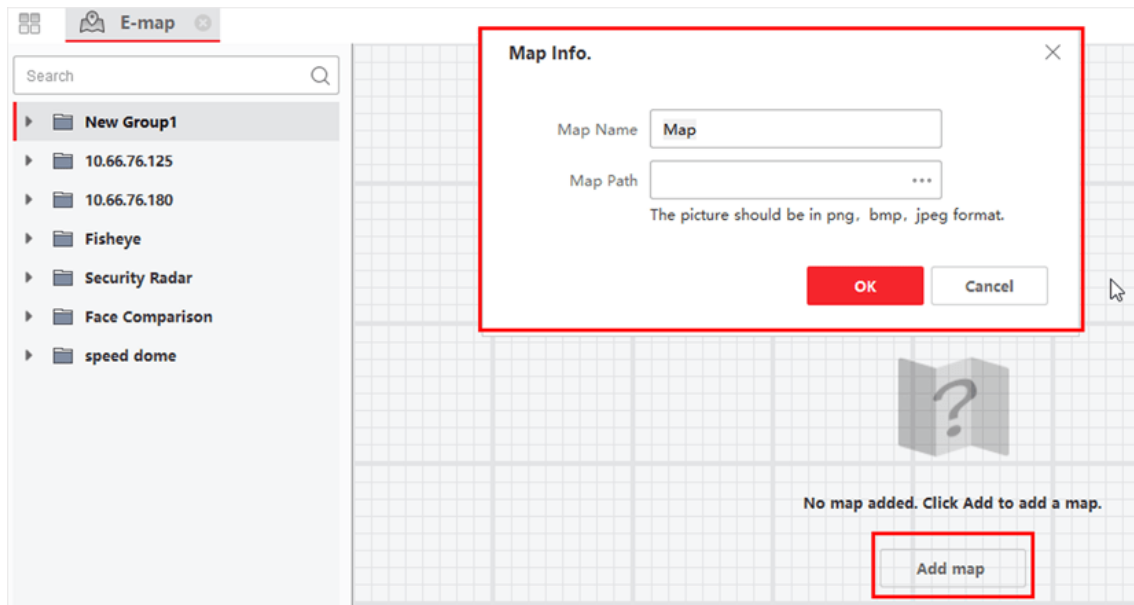
Der kan kun tilføjes ét kort til en gruppe.

1. Åbn siden E-map.
2. Vælg en gruppe, som du vil tilføje et kort til.

 **Bemærk**

For detaljer om indstilling af gruppen, se [Gruppestyring](#).

3. Klik på **Add Map** for at åbne vinduet til tilføjelse af kort.



Figur 9-1 Tilføj kort

4. Indtast et beskrivende navn på det tilføjede kort.
5. Vælg et kortbillede fra den lokale sti.

Bemærk

Kortets billedformat kan kun være PNG, JPEG eller BMP.

6. Klik på **OK**.
7. Det er valgfrit: Udfør følgende opgaver, når du har tilføjet kortet.

Zoom ind/ud Brug musehjulet, eller klik på + eller - for at zoome ind eller ud på kortet.

Juster kortområdet Træk i det gule vindue i nederste højre hjørne, eller brug retningsknapperne og zoomlinjen til at justere kortområdet, så du kan se det.

9.2 Rediger kortets skala


Et korts målestok er forholdet mellem en afstand på kortet og den tilsvarende afstand på jorden. Klienten kan beregne afstanden mellem to steder på kortet i forhold til afstanden på jorden. En nøjagtig kortskala er afgørende for at definere radarens overvågningsområde.

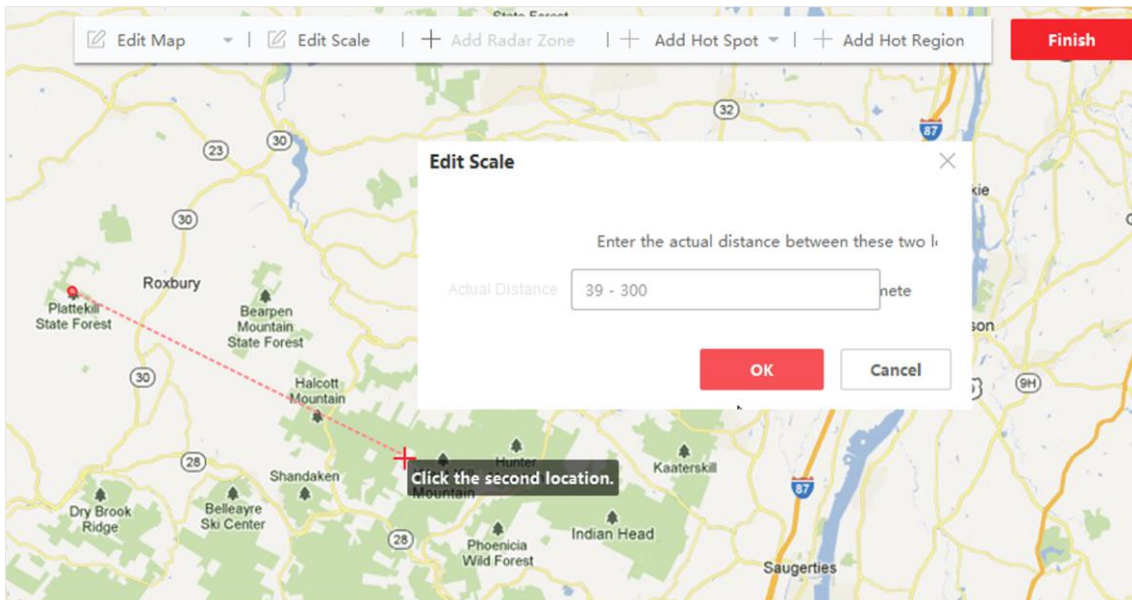
Før du går i gang

Sørg for, at du har tilføjet et kort. Se [Tilføj kort](#) for detaljer.

Udfør denne opgave, hvis du har brug for at tilføje en sikkerhedsradar til kortet.

Trin

1. Gå ind i E-map-modulet.
2. Klik på **Rediger** på E-maps værktøjslinje for at åbne kortredigeringsstilstanden.
3. Klik på **Kortkalibrering** → **Rediger skala** for at vælge to steder på kortet.
Markøren bliver til , hvis du holder den hen over kortet.



Figur 9-2 Rediger kortets skala

4. Klik på kortet for at vælge to steder.
Vinduet Rediger skala dukker op.
5. Indtast jordafstanden mellem de to steder, og klik derefter på **OK**.
Klienten beregner automatisk kortets skala.

9.3 Kalibrering af længde- og breddegrader

Når du har kalibreret længde- og breddegraden for to punkter på E-kortet, kan du trække radaren i gruppen til E-kortet. Radaren flyttes automatisk til den korrekte position på E-kortet i henhold til resultatet af længde- og breddegradskalibreringen.

Før du går i gang

1. Sørg for, at du har tilføjet radar på klienten. Se [***Tilføj en enkelt eller flere online-enheder***](#) for detaljer.
2. Sørg for, at du har indstillet radarens længde- og breddegradsparametre via webbrowseren.

Trin

1. Gå ind i E-map-modulet.
2. Klik på **Rediger** på E-maps værktøjslinje for at åbne kortredigeringsstilstanden.
3. Klik på **Map Calibration** → **LongitudeLatitude Calibration**.

4. Klik på **Tilføj kalibreringspunkt**.
5. Klik på et punkt på kortet, indtast længde- og breddegrad for punktet i pop op-vinduet, og klik derefter på **Gem**.
6. Klik på **Add Calibration Point**, og gentag det foregående trin for at tilføje det andet kalibreringspunkt.
7. Træk radaren i den venstre ressourcegruppe over på kortet.
Radaren flytter sig automatisk til den korrekte position på kortet i henhold til længde- og breddegraden for to kalibreringspunkter.

9.4 Administrer Hot Spot

De enheder, der tilføjes på kortet, kaldes hot spots. Hot spots viser enhedernes placering, og du kan også få livevisning eller alarmoplysninger om overvågningsscenerierne via hot spots.

9.4.1 Tilføj kamera som hotspot

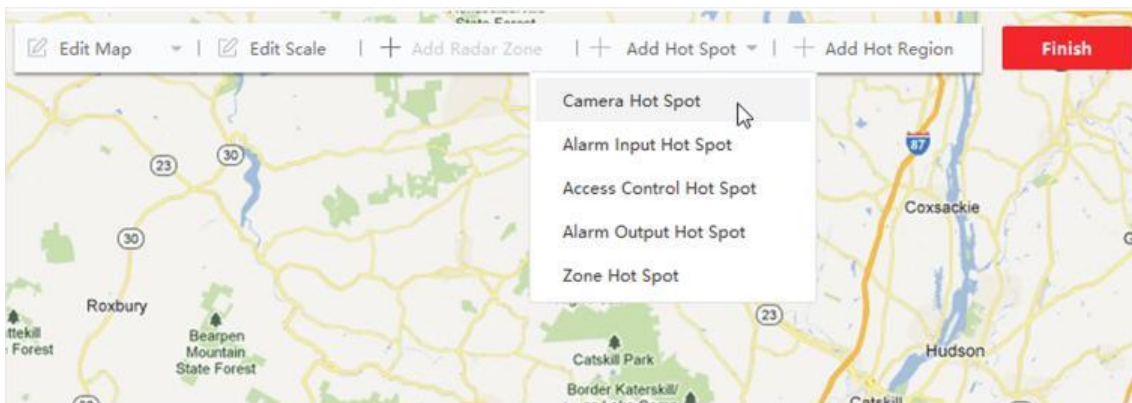
Du kan tilføje kameraer til kortet som hot spots.

Før du går i gang

Sørg for, at du har tilføjet et e-map og et kamera til klienten. Se [Tilføj kort](#) og [Enhedsstyring](#) for detaljer.

Trin

1. Gå ind på E-map-siden.
2. Klik på **Rediger** i øverste højre hjørne for at åbne kortredigeringsstilstanden.
3. Klik på **Tilføj hotspot** → **Kamera-hotspot** for at åbne vinduet Tilføj hotspot.

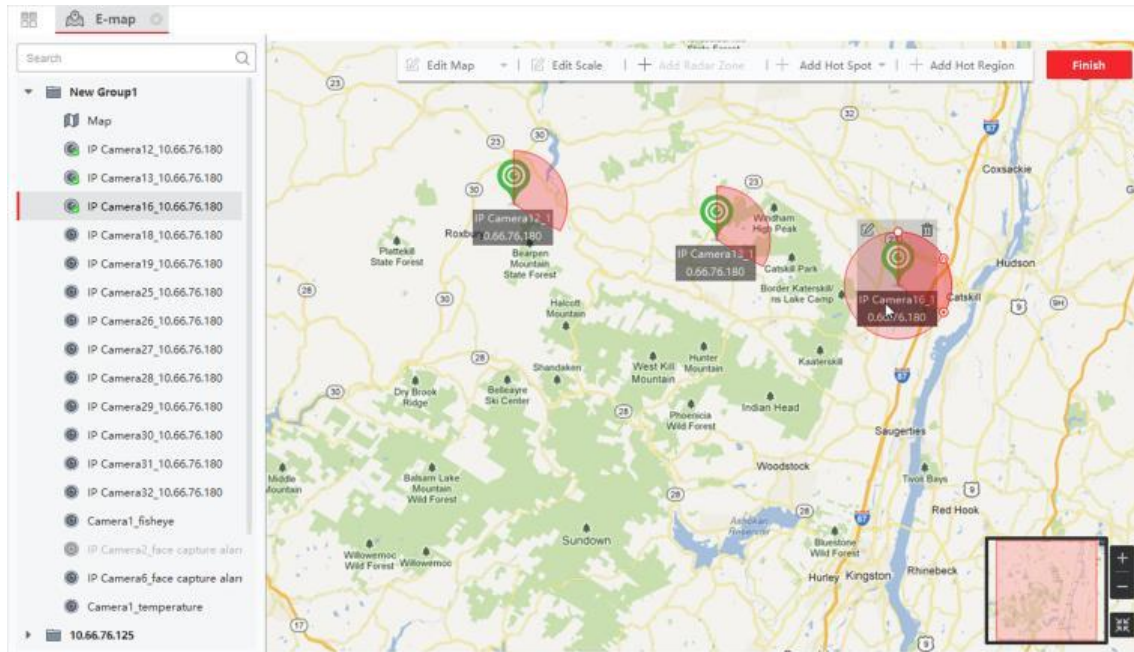


Figur 9-3 Tilføj hotspot



4. Vælg de kameraer, der skal føjes til kortet.
5. Valgfrit: Rediger hotspot-navnet, vælg navnefarve, og vælg hotspot-ikonet.
6. Klik på **OK** for at gemme indstillingerne.

Bemærk



Du kan også trække kameraikonerne fra gruppelisten direkte til kortet for at tilføje hot spots.



Figur 9-4 Tilføjet kamera-hotspot

Kameraikonerne tilføjes på kortet som hot spots, og ikonerne for de tilføjede kameraer i gruppelisten ændres fra  til . Sektoren angiver kameraets synsfelt.

7. Udfør følgende handling(er).

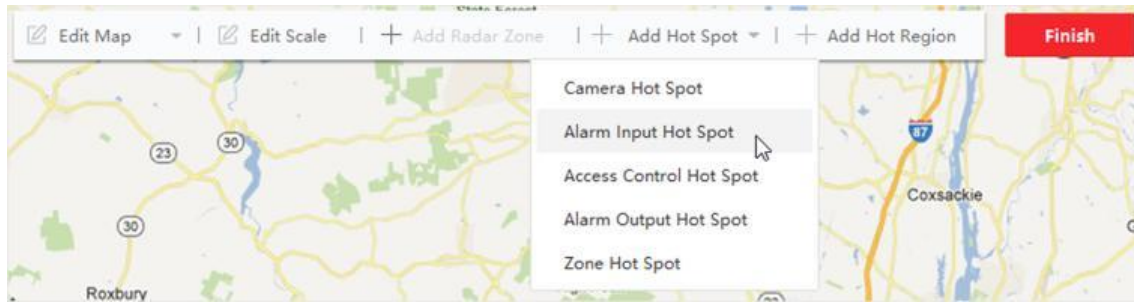
- Flyt Hot Spot** Træk i hotspottet for at flytte det til en bestemt position.
- Skift FOV-vinkel** Træk i /  og drej for at ændre kameraets synsfelt.
- Skift FOV-størrelse** Træk i  for at ændre FOV-størrelsen.

9.4.2 Tilføj alarmindgang som hotspot

Du kan tilføje alarmindgangene til kortet som hot spots.

Trin

1. Gå ind i E-map-modulet.
2. Klik på **Rediger** i øverste højre hjørne for at åbne kortredigeringsstilstanden.
3. Klik på **Add Hot Spot** → **Alarm Input Hot Spot** for at åbne vinduet Add Hot Spot.

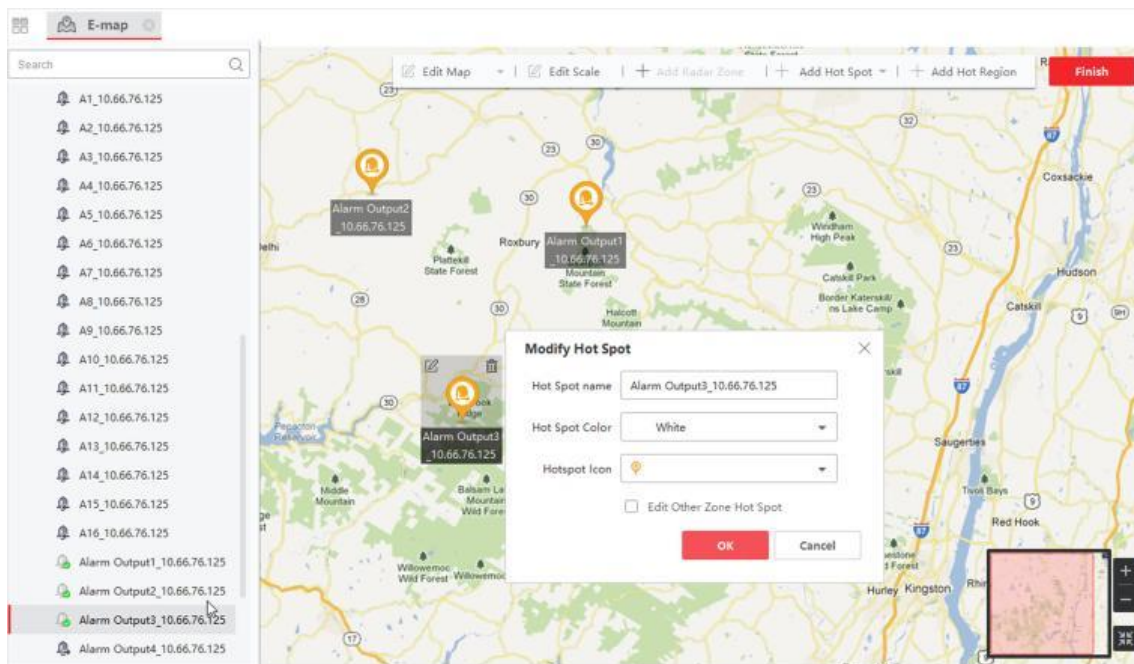


Figur 9-5 Tilføj alarmindgang som hotspot



4. Vælg de alarmindgange, der skal føjes til kortet.
5. Valgfrit: Rediger hotspot-navnet, vælg navnefarven og vælg hotspot-ikonet ved at dobbeltklikke på det tilsvarende felt.
6. Klik på **OK**.

Bemærk

Du kan også trække alarmindgangsikonerne fra gruppelisten direkte til kortet for at tilføje hotspotet.



Figur 9-6 Tilføjet hotspot for alarmindgang

Ikonerne for alarmindgangene tilføjes på kortet som hot spots, og ikonerne for de tilføjede alarmindgange i gruppelisten ændres fra  til .

7. Valgfrit: Træk i hotspottet for at flytte det til en bestemt position.

9.4.3 Tilføj alarmudgang som hotspot

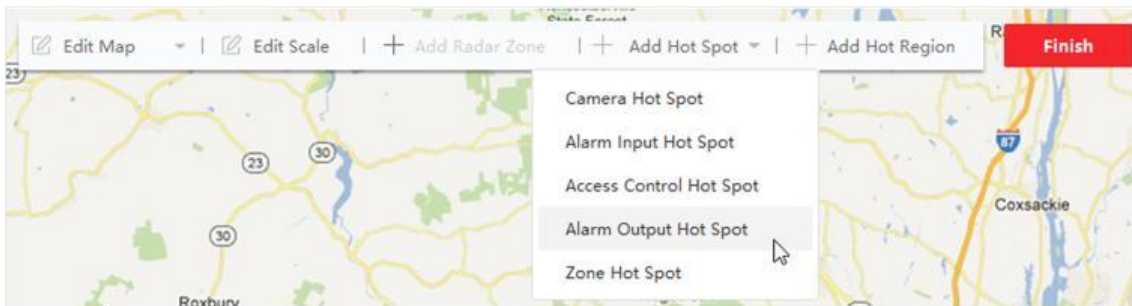
Du kan tilføje alarmudgange til kortet som hot spots til styring. Derefter kan du aktivere eller deaktivere dem på en hurtig måde. Hvis du aktiverer en alarmudgang på kortet, vil de sikkerhedskontrolenheder (f.eks. sirener, klokker), der er forbundet med den, alarmere for opmærksomhed.

Før du går i gang

Sørg for, at du har tilføjet et e-map og en alarmudgang til klienten. Se [Tilføj kort](#) og [Enhedsstyring](#) for detaljer.

Trin

1. Gå ind i E-map-modulet.
2. Klik på **Rediger** på E-maps værktøjslinje for at åbne kortredigeringsstilstanden.
3. Klik på **Tilføj hotspot** → Hotspot for **alarmudgang** for at åbne panelet Tilføj hotspot.

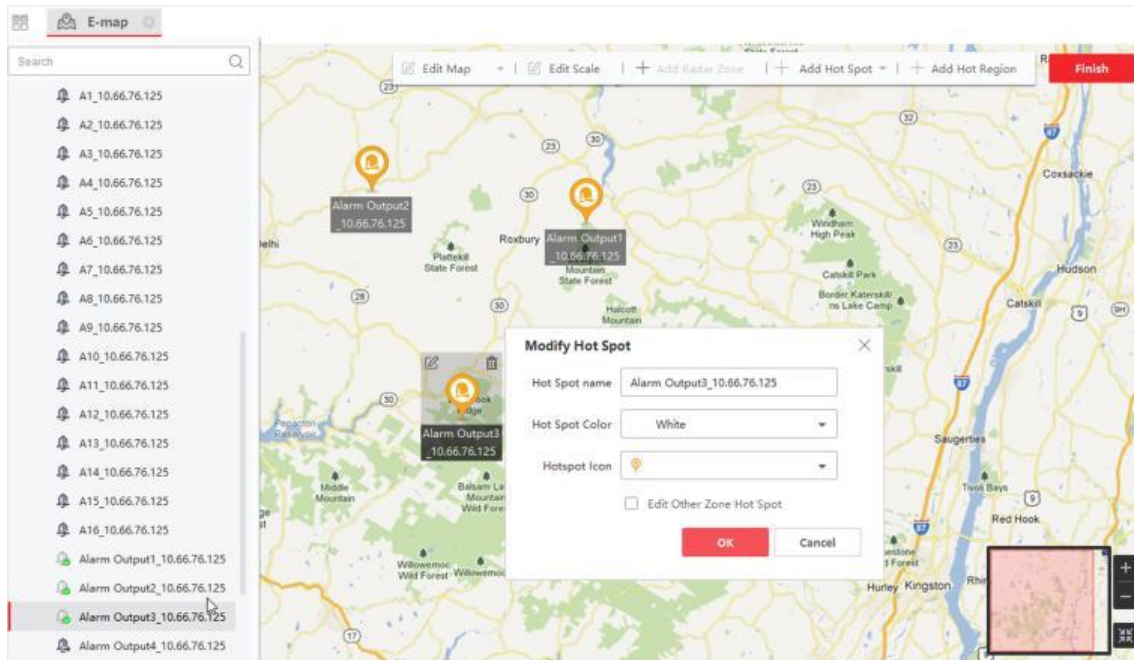


Figur 9-7 Tilføj alarmudgang som hotspot



4. Vælg den alarmudgang, der skal føjes til kortet.
5. Valgfrit: Rediger hotspot-navnet, vælg navnefarven, og vælg hotspot-ikonet.
6. Klik på **OK**.

Bemærk

Du kan også trække et alarmudgangsikon fra alarmudgangslisten til kortet for at tilføje hotspotet.



Figur 9-8 Tilføjet hotspot for alarmudgang

Alarmudgangen tilføjes på kortet som et hotspot, og dens ikon på gruppe listen ændres fra  til .

7. Valgfrit: Træk i alarmudgangen for at flytte den til en bestemt position.

9.4.4 Tilføj zone som hotspot

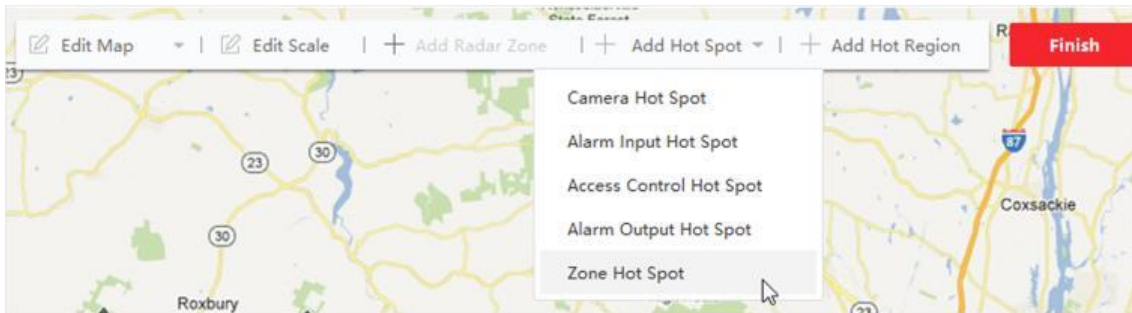
Du kan tilføje zoner til kortet, så du hurtigt kan finde zonen, når en alarm udløses.

Før du går i gang

Sørg for, at du har tilføjet et kort og en zone til klienten. Se [Tilføj kort](#) og [Tilføj enhed](#) for detaljer.

Trin

1. Gå ind i E-map-modulet.
2. Klik på **Rediger** på E-maps værktøjslinje for at åbne kortredigerings tilstanden.
3. Klik på **Add Hot Spot** → **Zone Hot Spot** for at åbne panelet Add Hot Spot.

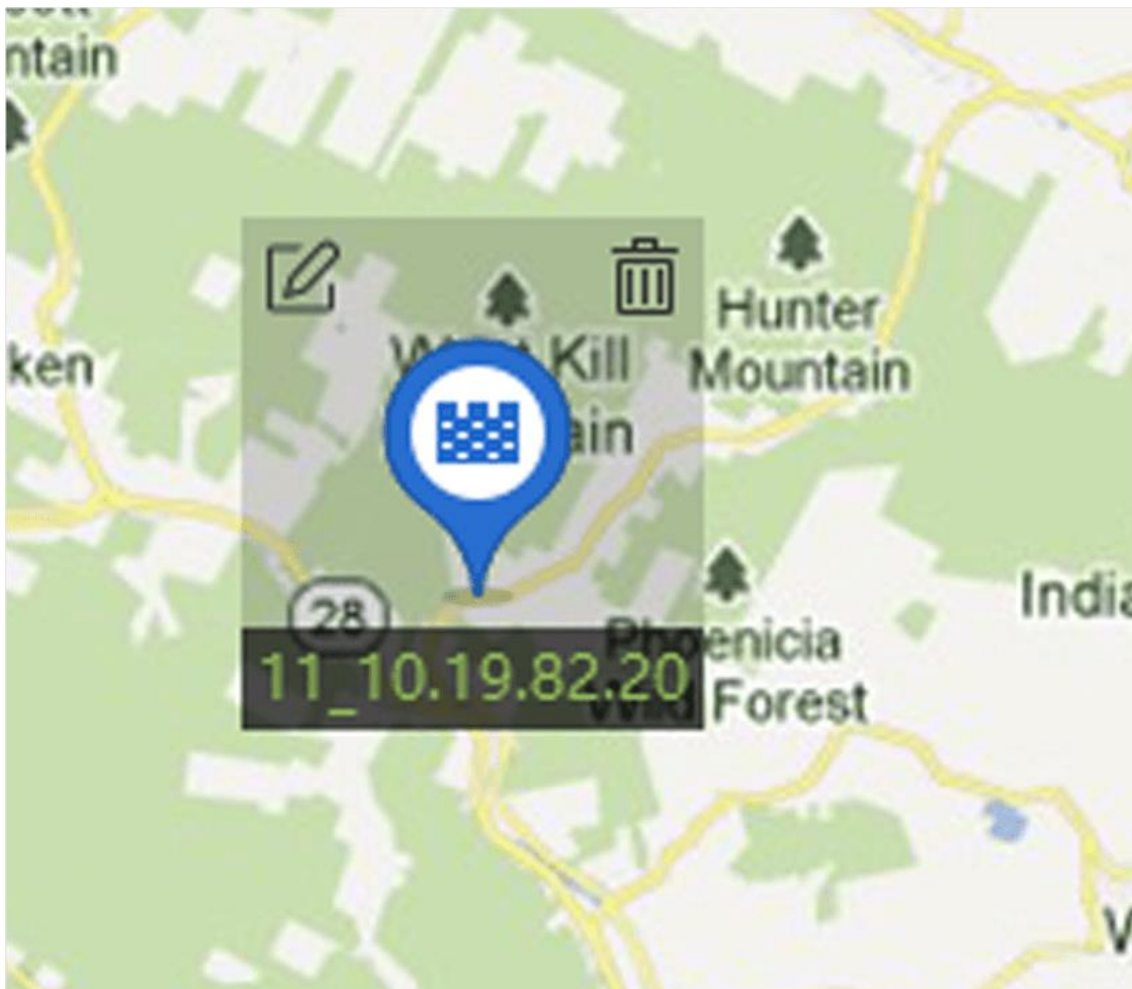


Figur 9-9 Tilføj zone som hotspot



4. Vælg den eller de zoner, der skal føjes til kortet.
5. Valgfrit: Rediger hotspot-navnet, vælg navnefarven, og vælg hotspot-ikonet.
6. Klik på **OK**.

Bemærk

Du kan også trække alarmudgangsikonerne fra alarmudgangslisten til kortet for at tilføje hotspotet.



Figur 9-10 Zone på kortet

Zonen tilføjes på kortet som et hot spot, og dens ikon på gruppelisten ændres fra  til  .

7. Valgfrit: Træk i zonen hot spot for at flytte den til en bestemt position.

Når der udløses alarmer, vises nummeret på de nyeste alarmer på zonen ikon. Du kan klikke på nummeret for at se detaljerne om alarmerne.

Bemærk

Der kan ikke vises mere end de 10 nyeste alarmer.

8. Valgfrit: Klik på **Clear Alarms** for at markere alarmerne for zonerne på det aktuelle kort som aflæste.

9.4.5 Tilføj adgangspunkt som hotspot

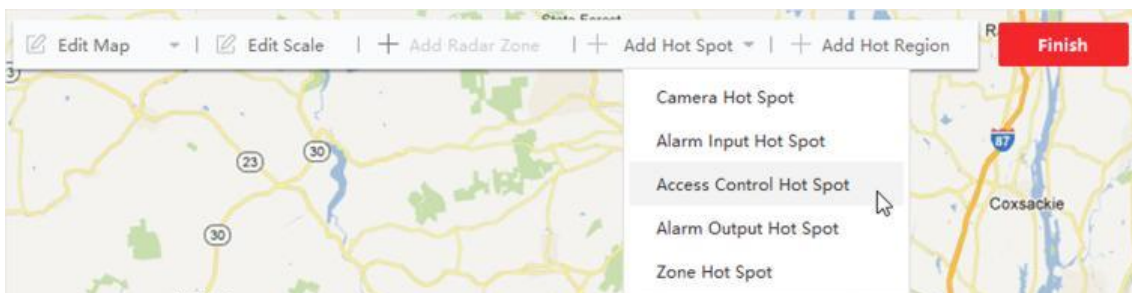
Du kan tilføje adgangspunkter til kortet som hot spots, så du kan finde hot spots og se deres status og alarmnumre.

Før du går i gang

Sørg for, at du har tilføjet et kort og et adgangspunkt til klienten. Se [Tilføj kort](#) og [Tilføj enhed](#) for detaljer.

Trin

1. Gå ind i E-map-modulet.
2. Klik på **Rediger** på E-maps værktøjslinje for at åbne kortredigeringsstilstanden.
3. Klik på **Add Hot Spot** → **Access Point Hot Spot** for at åbne vinduet Add Hot Spot.

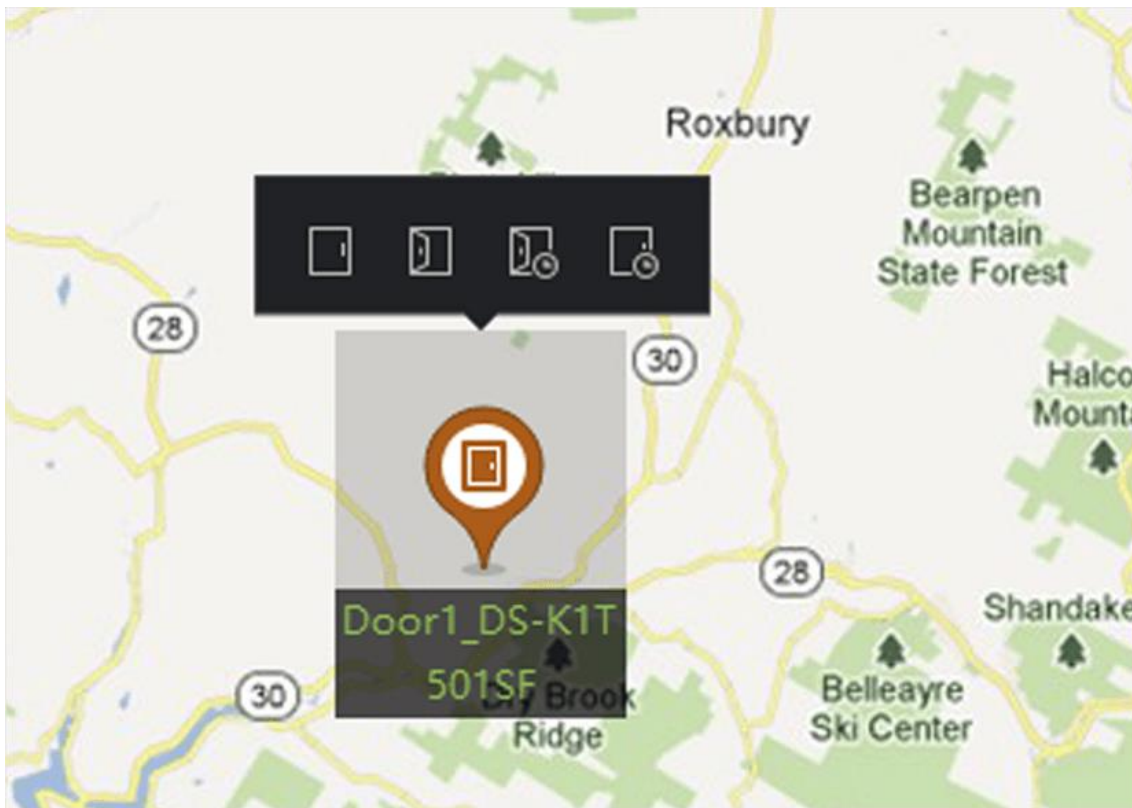


Figur 9-11 Tilføj adgangspunkt som hotspot



4. Vælg de(t) adgangspunkt(er), der skal føjes til kortet.
5. Valgfrit: Rediger hotspot-navnet, vælg navnefarven, og vælg hotspot-ikonet.
6. Klik på **OK**.

 **Bemærk**

Du kan også trække et access point-ikon fra access point-listen til kortet.



Figur 9-12 Adgangspunkt på kortet

Adgangspunktet føjes til kortet som et hotspot, og dets ikon på gruppelisten ændres fra  til .

7. Valgfrit: Træk i adgangspunktets hotspot for at flytte det til en bestemt position. Når der udløses alarmer, vises nummeret på de nyeste alarmer på hotspot-ikonet. Du kan klikke på nummeret for at se detaljerne om alarmen.

 **Bemærk**

Der kan ikke vises mere end de 10 nyeste alarmer.

Kapitel 10 Statistik

10.1.1 Rapport om optælling af personer efter kodningsenhed

Rapport om optælling af personer ved hjælp af kodningsenhed viser data om optælling af personer indsamlet af kodningsenheder. Du kan søge i persontællingsdataene i forskellige dimensioner.

Før du går i gang

Tilføj en kodningsenhed med personoptællingsfunktion til softwaren, og konfigurer det tilsvarende område og personoptællingsreglen korrekt. Se [Tilføj enhed](#) for detaljer om tilføjelse af personoptællingsenhed.

Trin

1. Klik på **Rapport** → **Optælling af personer** for at åbne siden Optælling af personer.
2. Vælg **Kodningsenhed** som **Enhedstype**.
3. Vælg daglig rapport, ugentlig rapport, månedlig rapport eller årlig rapport som rapporttype.

Daglig rapport

Daglig rapport viser data på daglig basis. Systemet beregner antallet af personer i hver time på en dag.

Ugentlig rapport, månedlig rapport og årlig rapport


Sammenlignet med den daglige rapport kan den ugentlige rapport, den månedlige rapport og den årlige rapport være mindre tidskrævende, da de ikke skal indsendes hver dag. Systemet beregner antallet af personer for hver dag i en uge, for hver dag i en måned og for hver måned i et år.

Brugerdefineret rapport

Brugere kan tilpasse dagene i rapporten for at analysere antallet af personer på hver dag eller måned i det tilpassede tidsinterval.

Bemærk

Du kan ikke vælge mere end 31 dage i kalenderen.

4. Vælg statistikkens tidstype, og klik på  for at indstille tiden.

En periode

Generer statistikken i én tidsperiode.

Flere perioder

Generer statistikken i to tidsperioder, som kan hjælpe dig med at sammenligne personflow og antal i to tidsperioder.

Hvis du f.eks. indstiller rapporttypen som månedsrapport og indstiller marts og april som statistiktidspunkt, vil resultaterne af optællingen af personer i marts og april blive vist i det samme diagram med forskellige farver, og du kan sammenligne dataene på forskellige dage i hver måned.

5. Vælg **Statistiktype**.

Visning efter enhed

Vis rapporten efter enhed.

Hvis du f.eks. vælger én NVR (med 4 personer, der tæller kameraer), vil rapporten vise det samlede antal personer summeret af de 4 personer, der tæller kameraer.

Visning med kamera

Vis rapporten efter kamera.

Hvis du f.eks. vælger en NVR (med 4 personer, der tæller kameraer), vil rapporten vise hvert kameras statistik, dvs. vise statistikken i 4/8 farver (hver af de to farver repræsenterer et kamera).

Visning efter grupperingsstatistik

Vis rapporten ved at gruppere statistikker.

Hvis du f.eks. vælger en enhedsgruppe (gruppen oprettes på klienten), viser rapporten det samlede antal personer summeret af det samlede antal personer, der tæller kameraer i gruppen.



Bemærk

- For detaljer om enhedsgrupper, se [Grupperessourcer](#).
 - Denne funktion skal understøttes af enheden.
-

6. Vælg filtreringstilstand.

Kanal

Vis data for optælling af personer indsamlet af kanaler i en kodningsenhed.

Region

Vis antallet af personer i udvalgte områder af et kamera.



Bemærk

Du skal konfigurere regioner for kameraet på forhånd. Se enhedens brugervejledning for detaljer.

7. Vælg kamera(er) eller region(er) fra kameralisten.

8. Indstil det indhold, der skal vises.

Retning

Beregn antallet af personer i forskellige retninger, f.eks. ind, ud eller ind og ud.

Indtast

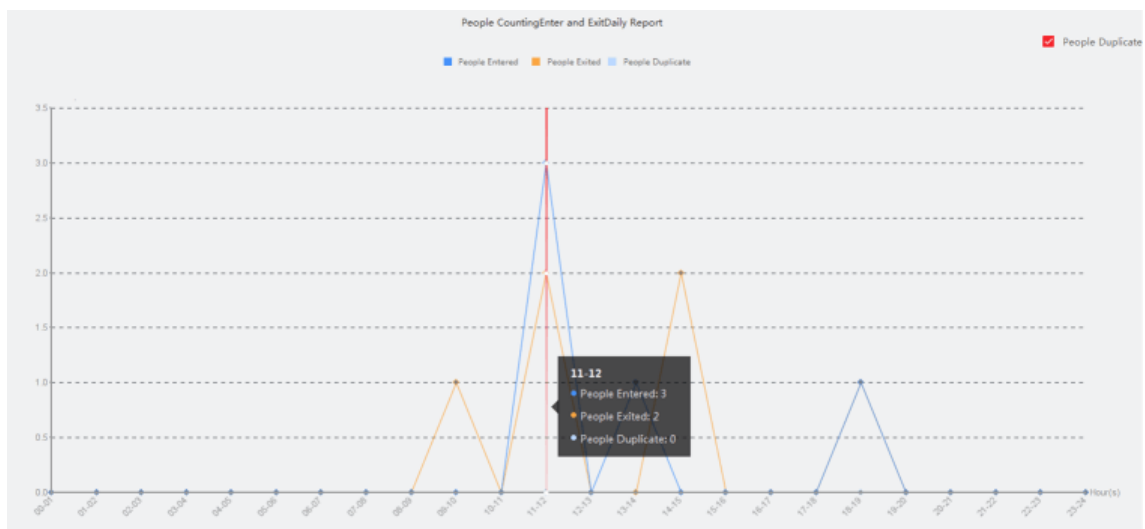
De tilmeldte personer vil blive talt op.

Udgang

De mennesker, der går ud, vil blive talt.

Gå ind og ud

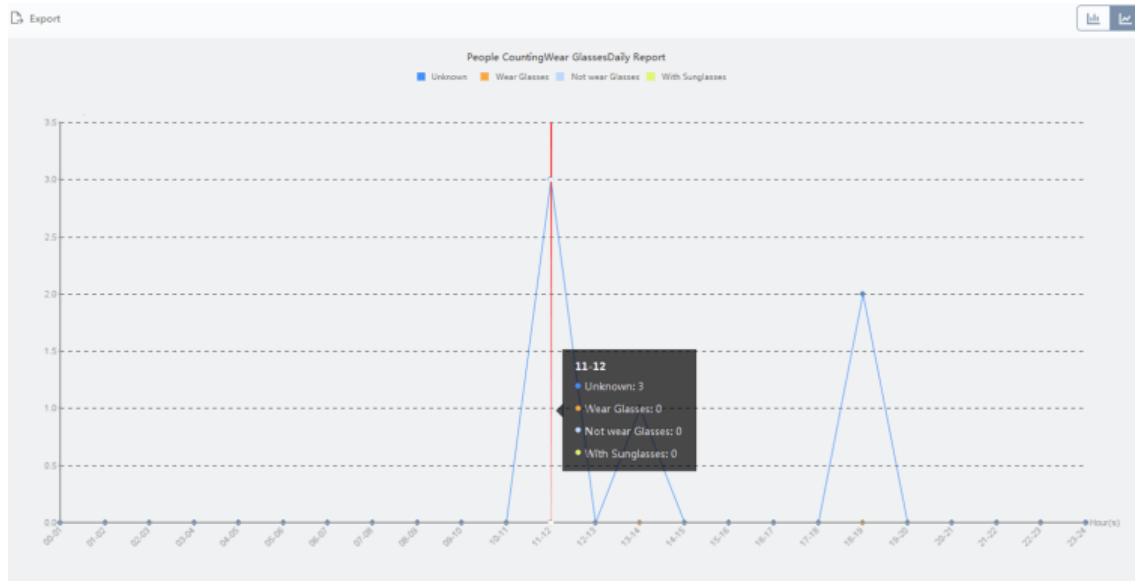
Både personer, der går ind og ud, tælles med.



Figur 10-1 Optælling af personer efter retning

Ansigtstræk

Generer rapporten baseret på ansigtstræk.



Figur 10-2 Optælling af personer ud fra ansigtstræk

9. Valgfrit: Markér **Kun børn** for at generere en rapport over anerkendte børn.

Bemærk

- Klienten tæller registrerede personer, der er lavere end en foruddefineret højde, som kan konfigureres på enhedens fjernkonfigurationsside. Se enhedens brugervejledning for detaljer om konfiguration af højdetærsklen.
- Denne funktion skal understøttes af enheden.

10. Klik på **Søg** for at få statistikker over antal personer og detaljerede data for hver time, dag eller måned.

Som standard vises statistikkerne i histogramform.

11. Valgfrit: For rapporten efter retning kan du markere **Personer duplikeret** i øverste højre hjørne af rapportensiden for at få vist antallet af dupliserede personer.

Bemærk

Antallet af dupliserede personer beregnes af enheden. Hvis det samme ansigt genkendes mere end én gang, vil han/hun blive beregnet som dobbeltperson.

Hvis en kassemedarbejder f.eks. går ind eller ud af supermarkedet mere end én gang, vil han/hun blive regnet som en dobbeltperson. På den måde kan supermarkedet få det faktiske antal personer, der handler.

12. Valgfrit: Udfør følgende handlinger efter søgning.

Skift til linjediagram Klik på  for at skifte til linjediagram.

Bemærk

Som standard vises statistikkerne i et søjlediagram.

Skift til søjlediagram Klik på  for at skifte til søjlediagram.

Gem på lokal pc Klik på **Eksporter** for at gemme de detaljerede data om optælling af personer på din pc.

10.2 Vis rapport om optælling af personer i vejkryds

Analyse af vejkryds bruges til at overvåge trafikstrømmen og antallet af mennesker i et vejkrydslignende område. Pilene på billedet henviser til forskellige retninger. Ved at vælge en retning (f.eks. A) som indgang, vil de andre retninger blive indstillet som udgange som standard, så der genereres flere stier (f.eks. A til A, A til B, A til C og A til D). Du kan se antallet af personer, der har passeret hver vej, hvilket kan hjælpe butiksindehaveren med at analysere personflowet i forskellige døre. Statistikresultatet kan vises i en daglig, ugentlig, månedlig og årlig rapport.

Før du går i gang

Sørg for, at et fisheye-kamera, der understøtter funktionen til analyse af kryds, er konfigureret korrekt og er tilføjet til softwaren. Se [Tilføj enhed](#) for detaljer om tilføjelse af enheden.

Trin

Bemærk

Der kan analyseres op til 10 kryds.

1. Klik på **Rapport** → **Krydsanalyse** for at åbne modulet til krydsanalyse.
2. Vælg daglig rapport, ugentlig rapport, månedlig rapport eller årlig rapport som rapporttype.

Daglig rapport

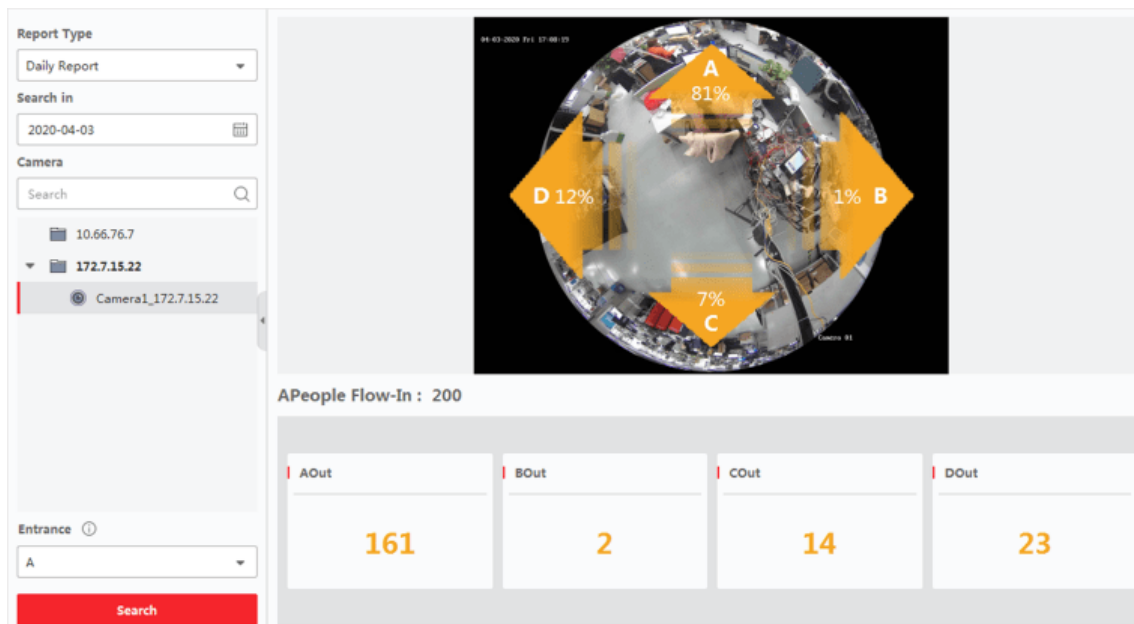
Daglig rapport viser data på daglig basis. Systemet beregner antallet af personer i krydsningsrapporten i hver time på en dag.

Ugentlig rapport, månedlig rapport og årlig rapport

Sammenlignet med den daglige rapport kan den ugentlige rapport, den månedlige rapport og den årlige rapport være mindre tidskrævende, da de ikke skal indsendes hver dag. Systemet beregner antallet af personer i krydsrapporten for hver dag i en uge, for hver dag i en måned og for hver måned i et år.

3. Indstil starttidspunktet for rapporten.
4. Vælg det kamera, der skal generere rapporten.
5. Vælg en retning som indgang fra rullelisten i **Flow in** filed.

6. Klik på **Søg** for at få statistikresultatet.



Figur 10-4 Resultater

Personnummeret for hver sti vises til højre.

10.4 Rapport om varmekort

Varmekort er en grafisk repræsentation af data repræsenteret ved farver, og varmekortdataene kan vises i linjediagram. Du kan bruge kameraets varmekortfunktion til at analysere kundernes besøgstider og opholdstid i et konfigureret område, hvilket kan hjælpe butiksindehaveren med at analysere kundernes interesseområde og arrangere varer.

Før du går i gang

Tilføj et heat map-netværkskamera til softwaren, og konfigurer det tilsvarende område korrekt. Det tilføjede kamera skal være konfigureret med heat map-regel. Se **Tilføj enhed** for detaljer om tilføjelse af heat map-netværkskamera.

Trin

1. Klik på **Rapport** → **Heat Map** for at åbne heat map-siden.
2. Vælg **Daglig** rapport/Ugevis rapport/Månedsvist rapport/Årsvis rapport/Brugertilpasset **rapport** som rapporttype.

Daglig rapport

Daglig rapport viser data på daglig basis. Systemet beregner data for varmekort i hver time på en dag.

Ugentlig rapport, månedlig rapport og årlig rapport

Sammenlignet med daglige rapporter kan ugentlige rapporter, månedsrapporter og

årsrapporter være mindre tidskrævende, da de ikke skal indsendes hver dag. Systemet beregner varmekortets data for hver dag i en uge, for hver dag i en måned og for hver måned i et år.

Brugerdefineret rapport

Du kan tilpasse dagene i rapporten for at analysere opholdstiden eller crowd-tendensen på hver dag eller måned i det tilpassede tidsinterval.

Bemærk

Tidsperioden i den brugerdefinerede rapport bør ikke være mere end 31 dage.

3. Vælg **By Dwell Time** eller **By Crowd Trend** som statistiktype.

Af Dwell Time

Systemet beregner heat map-værdien (ordinatværdien i linjediagrammet eller farven i billederne) i henhold til folks opholdstid.

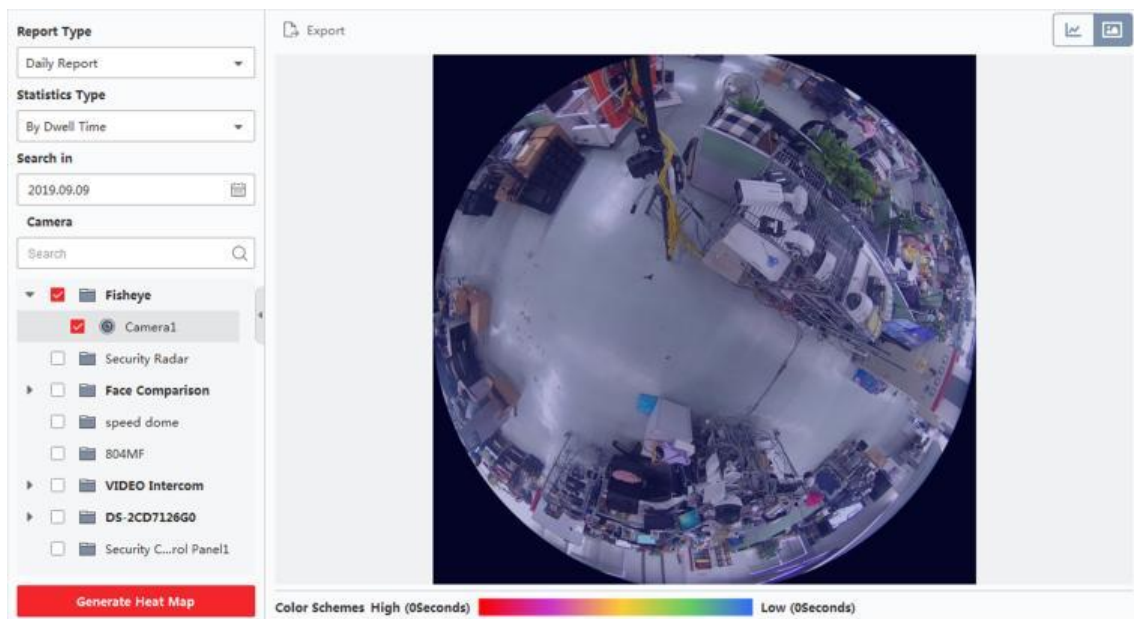
Af Crowd Trend

Systemet beregner varmekortværdien (ordinatværdien i linjediagrammet eller farven i billeder) i henhold til antallet af registrerede personer.

4. Indstil tidsperioden for søgning.

5. Vælg et varmekortkamera på kameralisten.


6. Klik på **Generate Heat Map** for at få vist kameraets varmekort.




Figur 10-9 Resultater

7. Valgfrit: Når du har genereret heat map-rapporten, kan du udføre følgende handlinger.

Visning i linjediagram

Klik på  for at få vist statistikken i et linjediagram.

Visning i billedtilstand	Klik på  for at få vist statistikkerne i billedtilstand. Den røde farveblok (255, 0, 0) angiver det mest velkomne område, og den blå farveblok (0, 0, 255) angiver det mindre populære område.
Gem statistikdata	Klik på Eksporter for at gemme de detaljerede data fra varmekortet på din pc.

10.7 Temperaturkort

Et temperaturkort viser temperaturudviklingen i en region i løbet af en bestemt dag. Hvis du har konfigureret temperaturovervågningsregioner, kan du generere temperaturkort over specifikke regioner for at se oversigten over hver regions temperaturtrend.

Før du går i gang

- Sørg for, at du har tegnet regioner til temperaturkort på enhedens konfigurationsside. Se enhedens brugervejledning for detaljer.
- Sørg for, at du har tilføjet mindst én enhed for temperaturkort til klienten. Se [Tilføj enhed](#) for detaljer.

Trin

Bemærk

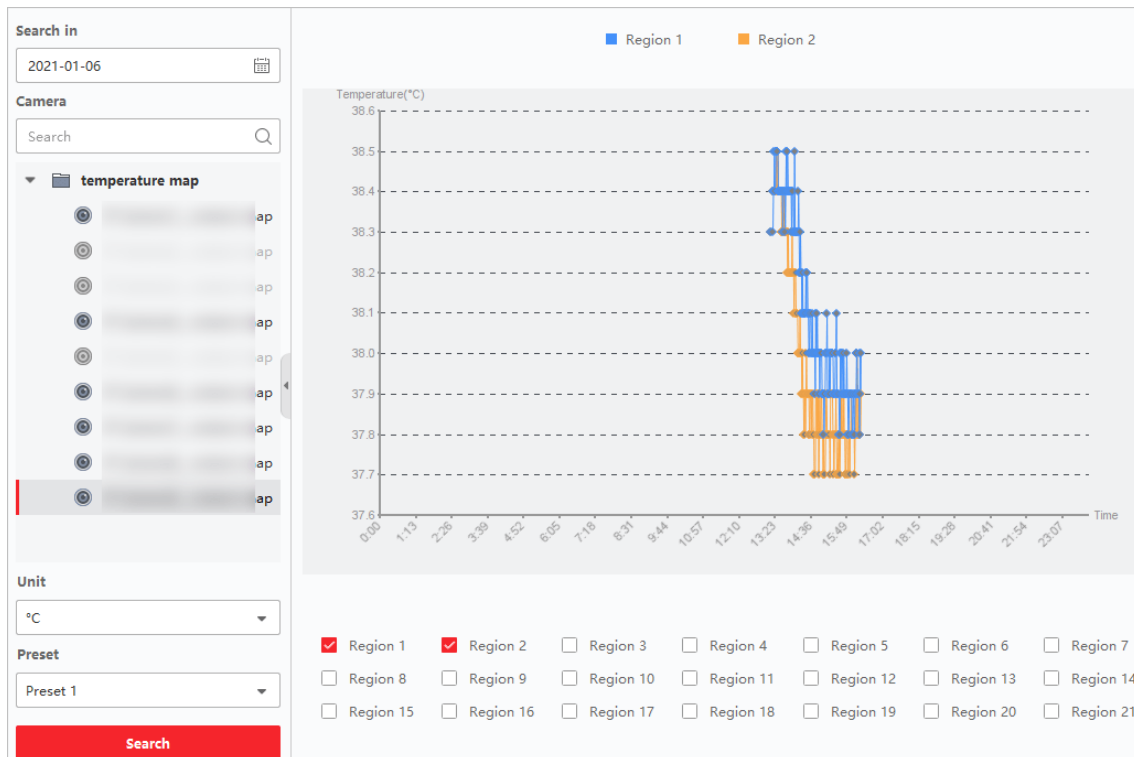
Denne funktion skal understøttes af enheden.

1. Klik på **Rapport** → **Temperaturkort**.
 2. Vælg en dato fra kalenderen.
 3. Vælg et kamera på kameranlisten.
-

Bemærk

Du kan indtaste et søgeord i søgefeltet for at søge efter et kamera.

4. Vælg en enhed.
5. Vælg en forudindstilling.



Figur 10-12 Temperaturkort

6. I højre panel skal du markere region(er) for generering af rapporten.

Bemærk

Der kan ikke kontrolleres mere end 8 regioner.

7. Klik på **Søg**.

Temperaturkortet vil blive vist i et linjediagram, hvor hver linje repræsenterer en region.

8. Valgfrit: Vælg en anden enhed for at få vist temperaturkortet i en anden enhed.

Kapitel 11 Datahentning

I Data Retrieval-modulet kan du søge efter bil- og menneskeobjektbaserede optagelser. Enheden skal understøtte funktionen "Bil" eller "Menneske".


11.1 Hentning af køretøj

På enheder, der understøtter køretøjshentning, kan du søge i de relaterede køretøjsbilleder og -videoer ved at indstille søgebetinger som nummerplade og optagelsestidspunkt.

Før du går i gang

Tilføj den enhed, der understøtter køretøjshentning, til klienten, og konfigurér de tilhørende indstillinger korrekt. Se [Tilføj enhed](#) for detaljer om tilføjelse af enheden.

Trin

1. Klik på **Data Retrieval** → **Vehicle Retrieval** for at komme til siden for køretøjshentning.
2. Klik på  for at indstille start- og sluttidspunktet for søgningen.
3. Vælg søgetype.

Køretøj

Søg og vis de optagne køretøjsbilleder ved at indtaste køretøjets nummerplade.

Registrering af blandet trafik

Søg og få vist billeder af et bestemt køretøj i forbindelse med detektering af blandet trafik ved at indtaste køretøjets nummerplade.

Bemærk

Kameraet skal understøtte detektering af blandet trafik.

4. Vælg en enhed fra kameralisten.
-

6. Valgfrit: Indtast nummerpladen (understøtter fuzzy search) til søgning.
7. Valgfrit: Indstil det maksimale antal søgeresultater, der skal vises.
8. Klik på **Søg** for at starte søgningen.
De optagne billeder, der opfylder søgebetingerne, vises på højre panel. Der kan vises op til 30 billeder på én side.
9. Valgfrit: Udfør følgende handlinger, hvis det er nødvendigt.

Eksportbillede

Du kan eksportere et eller flere søgte billeder.


1. Klik på **Eksporter billede**.
2. Marker et eller flere billeder, eller marker **Vælg alle** på siden nedenfor.

3. Klik på **Export** for at eksportere de valgte billeder til den lokale pc.

Se detaljer om optagelser

Klik på et billede for at se dets optagelsesdetaljer, såsom optagelsestidspunkt og kameranavn.





Bemærk

Du kan klikke på  for at se et forstørret billede.


Afspil relateret video

Klik på **Playback** for at afspille billedets tilhørende videofil (5 sek. før og 5 sek. efter optagelsen) i visningsvinduet.

Bemærk

- Du kan klikke på  for at se videoen i et større vindue.
 - Du kan klikke på  for at justere afspilningshastigheden, klikke på  for at afspille videofilen billede for billede, og klikke på  for at aktivere lyd.
-

Eksporter en enkelt post

Klik på  på siden med det forstørrede billede, og klik derefter på Eksporter **billede**, Eksporter **videofil** eller Eksporter **detaljer** for at eksportere billedet, videofilen og optagelsesdetaljerne for en enkelt optagelse til den lokale pc.

Kapitel 14 Personaleledelse

Du kan tilføje personoplysninger til systemet for yderligere funktioner som adgangskontrol, videointercom, tid og fremmøde osv. Du kan administrere de tilføjede personer, f.eks. udstede kort til dem i en batch, importere og eksportere personoplysninger i en batch osv.

Vigtig bemærkning: For detaljeret konfiguration af f.eks. ABUS Intercom-systemer eller ABUS Face Access-moduler, læs den tilhørende manual til det passende produkt.

14.1 Tilføj organisation

Du kan tilføje en organisation og importere personoplysninger til organisationen for effektiv

administration af personerne. Du kan også tilføje en underordnet organisation til den tilføjede.


Trin


1. Gå ind i Person-modulet.
2. Vælg en overordnet organisation i venstre kolonne, og klik på **Tilføj i** øverste venstre hjørne for at tilføje en organisation.
3. Opret et navn til den tilføjede organisation.

Bemærk

Der kan tilføjes op til 10 niveauer af organisationer.

4. Valgfrit: Udfør følgende handling(er).

Rediger organisation Hold musen over en tilføjet organisation, og klik på  for at redigere dens navn.

Slet organisation Hold musen over en tilføjet organisation, og klik på  for at slette den.

Bemærk

- Organisationer på lavere niveauer vil også blive slettet, hvis du sletter en organisation.
 - Sørg for, at der ikke er tilføjet nogen person under organisationen, ellers kan organisationen ikke slettes.
-

Vis personer i underorganisationen Markér **Vis personer i underorganisation**, og vælg en organisation for at vise personer i dens underorganisationer.

14.2 Tilføj enkeltperson

Du kan tilføje personer til klientsoftwaren én efter én. Personoplysningerne indeholder grundlæggende oplysninger, detaljerede oplysninger, profiler, oplysninger om adgangskontrol, legitimationsoplysninger, brugerdefinerede oplysninger osv.

14.2.1 Konfigurer grundlæggende oplysninger

Du kan tilføje personer til klienten én efter én og konfigurere personens grundlæggende oplysninger som navn, e-mail, telefonnummer osv.

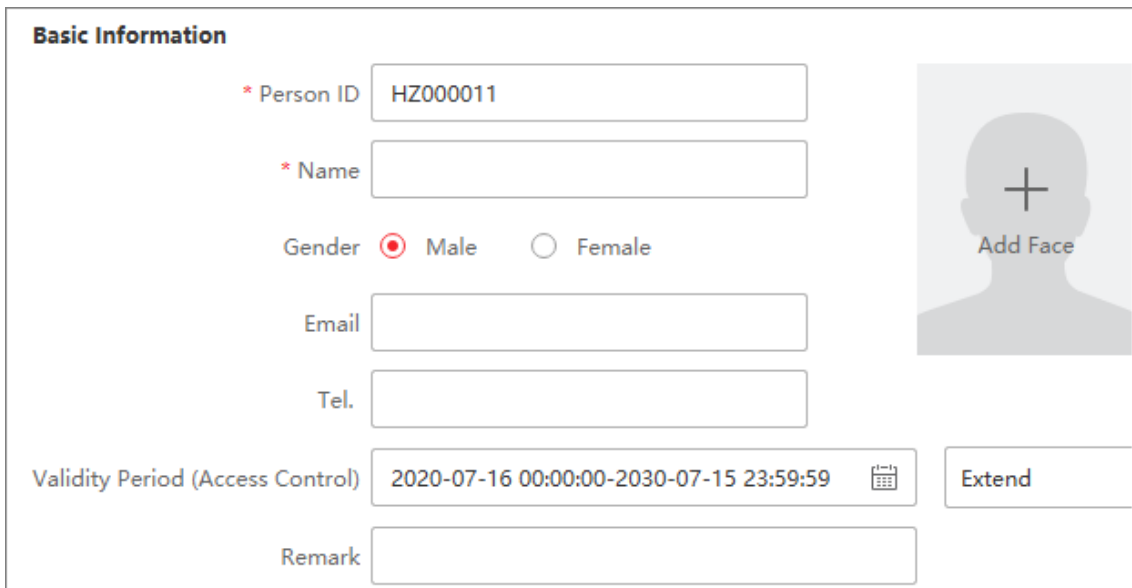
Trin

1. Gå ind i Person-modulet.

Bemærk

Første gang du åbner Person-modulet, dukker der et vindue op, hvor du kan indstille reglerne for generering af person-ID (bogstaver og tal understøttes), når du tilføjer en person. Hvis der ikke er nogen person-id'er, når der hentes personoplysninger fra enheden, vil person-id'erne blive genereret i henhold til reglen.

2. Vælg en organisation på organisationslisten for at tilføje personen.
3. Klik på **Tilføj** for at åbne vinduet Tilføj person.
Person-ID'et vil blive genereret automatisk.
4. Indtast de grundlæggende oplysninger, herunder personnavn, telefonnummer, e-mailadresse, gyldighedsperiode osv.



Basic Information

* Person ID

* Name

Gender Male Female

Email

Tel.

Validity Period (Access Control)

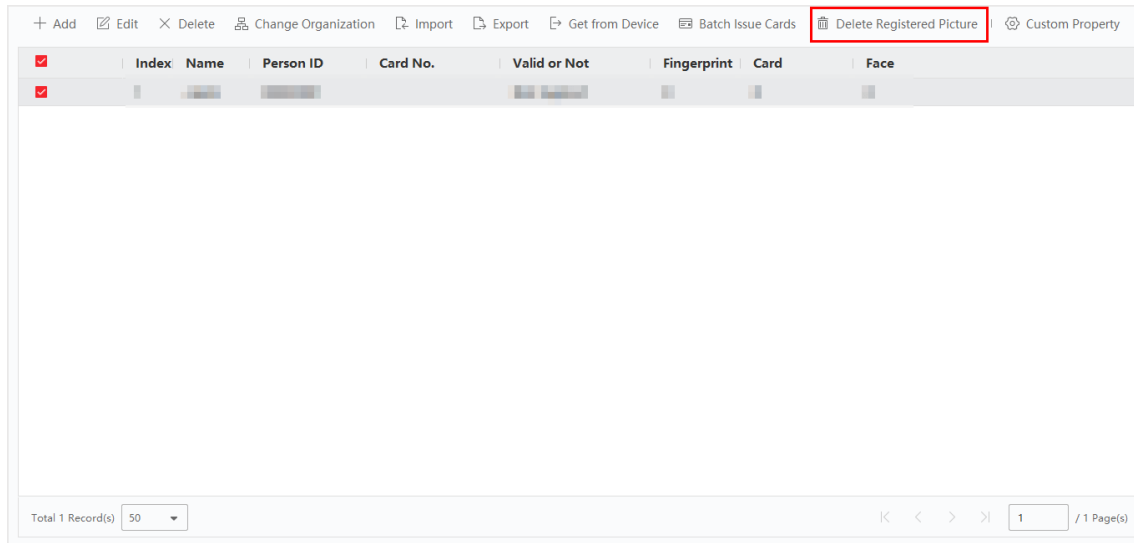
Remark

Figur 14-1 Konfigurer grundlæggende oplysninger

Bemærk

Når gyldighedsperioden er udløbet, vil personens legitimationsoplysninger og indstillinger for adgangskontrol være ugyldige, og personen vil ikke have tilladelse til at få adgang til doors/floors. Du kan klikke på **Forlæng** for at forlænge personens gyldighedsperiode med 1 måned, 3 måneder, 6 måneder eller 1 år.

5. Bekræft for at tilføje personen.
 - Klik på **Tilføj** for at tilføje personen og lukke vinduet Tilføj person.
 - Klik på **Tilføj og Ny** for at tilføje personen, og fortsæt med at tilføje andre personer.
6. Slet registreret ansigtsbillede



Figur 14-2 Slet registreret billede

Bemærk

Hvis **Gem billeder i strukturdataformat** er aktiveret, føjes knappen **Slet registreret billede** til siden **Person**. Generelt vil det registrerede ansigtsbillede blive slettet automatisk, når personens oplysninger anvendes på enheden. Ved at dobbeltklikke på personen vises vinduet **Rediger person**, og du kan tjekke, om det registrerede ansigtsbillede er blevet slettet. Hvis ikke, kan du vælge denne person og klikke på **Slet registreret billede** for at slette billedet manuelt.

14.2.2 Udsted et kort til én person

Når du tilføjer en person, kan du udstede et kort til ham/hende som legitimation for at få adgang til døren(e). Før du udsteder et kort til en person, skal du indstille kortudstedelsestilstanden for at få kortnummeret. Bortset fra manuel indtastning af kortnummeret tilbyder klienten også de to andre tilstande til at læse kortnummeret: lokal tilstand (via kortregistreringsstation) eller fjerntilstand (via kortlæseren på adgangskontrolenheden).

Bemærk

Der kan udstedes op til fem kort til en person.

Udsted et kort ved at indtaste kortnummer

Når der ikke er nogen enhed (kortregistreringsstation/kortlæser) til rådighed til at læse kortnummeret, kan du udstede et kort ved manuelt at indtaste kortnummeret.


Trin

1. Gå ind i Person-modulet.

2. Vælg en organisation på organisationslisten for at tilføje personen, og klik på **Tilføj for** at åbne panelet Tilføj person.

Bemærk

Indtast først personens grundlæggende oplysninger. For detaljer om konfiguration af personens grundlæggende oplysninger, se ***Konfigurer grundlæggende oplysninger***.

3. Klik på  i området **Credential** → **Card**.
4. Indtast kortnummeret manuelt på siden Tilføj.
5. Klik på **Tilføj**.
Kortet vil blive udstedt til personen.

Udsted et kort i lokal tilstand


Hvis der er en kortregistreringsstation til rådighed, kan du udstede et kort i lokal tilstand. For at læse kortnummeret skal du tilslutte kortregistreringsstationen til den pc, der kører klienten, via USB-interface eller COM, og placere kortet på kortregistreringsstationen.

Trin

1. Gå ind i Person-modulet.
2. Vælg en organisation på organisationslisten for at tilføje personen, og klik på **Tilføj for** at åbne panelet Tilføj person.

Bemærk

Indtast først personens grundlæggende oplysninger. For detaljer om konfiguration af personens grundlæggende oplysninger, se ***Konfigurer grundlæggende oplysninger***.

3. Klik på  i området **Credential** → **Card**.
4. Klik på **Indstillinger** for at åbne siden Indstillinger.
5. Vælg **Lokal** som kortudstedelsestilstand.
6. Indstil andre relaterede parametre.

Station til registrering af kort

Vælg en model af kortregistreringsstation fra rullelisten. Du kan tilslutte kortregistreringsstationen til pc'en og overføre de grundlæggende oplysninger om den tilføjede person mellem de to enheder via USB.

Korttype

Vælg korttype som EM-kort eller Mifare-kort i henhold til den aktuelle korttype.

Summende

Aktiver eller deaktiver summelyden, når kortnummeret er læst korrekt.

Kortnr. Type

Vælg typen af kortnummer efter det aktuelle behov.

M1-kortkryptering

Hvis kortet er et M1-kort, kan du aktivere M1 Card Encryption-funktionen og vælge den sektor på kortet, der skal krypteres.

7. Klik på **OK** for at bekræfte handlingen.
8. Placer kortet på kortregistreringsstationen, og klik på **Read** for at få kortnummeret. Kortnummeret vises automatisk i feltet Kortnr.
9. Klik på **Tilføj**. Kortet vil blive udstedt til personen.

Udsted et kort i fjerntilstand


Ud over at udstede et kort i lokal tilstand, kan du også stryge kortet på kortlæseren på den tilføjede adgangskontrolenhed for at få kortnummeret. Dette er relevant, når kunden og de personer, der skal udstede kort, ikke befinder sig på samme sted. Du kan f.eks. udstede kort til medarbejdere i filialen i fjerntilstand via klienten.

Trin

1. Gå ind i Person-modulet.
2. Vælg en organisation på organisationslisten for at tilføje personen, og klik på **Tilføj for** at åbne panelet Tilføj person.

Bemærk

Indtast først personens grundlæggende oplysninger. For detaljer om konfiguration af personens basisoplysninger, se [***Konfigurer basisoplysninger***](#).

3. Klik på  i området **Credential** → **Card**.
4. Klik på **Indstillinger** for at åbne siden Indstillinger.
5. Vælg **kortlæser** som kortudstedelsestilstand.
6. Vælg en adgangskontrolenhed, der er tilføjet i klienten.
7. Vælg en tilføjet adgangskontrolenhed eller tilmeldingsstationen fra rullelisten.

Bemærk

- Hvis du vælger adgangskontrolenhed, skal du sikre dig, at du har aktiveret enhederne.
 - Hvis du vælger indskrivningsstationen, skal du klikke på **Login for** at indstille enhedens relaterede parametre, herunder IP-adresse, portnummer, brugernavn og adgangskode. Du skal også kontrollere RF-korttype(r) efter behov.
-

8. Klik på **OK** for at bekræfte handlingen.
9. Placer kortet på kortlæseren, og klik på **Read** for at få kortnummeret. Kortnummeret vises automatisk i feltet Kortnr.
10. Klik på **Tilføj**. Kortet vil blive udstedt til personen.

14.2.3 Upload et ansigtsfoto fra lokal pc

Når du tilføjer en person, kan du uploade et ansigtsbillede, der er gemt på den lokale pc, til klienten som personens profil.

Trin

1. Gå ind i Person-modulet.
2. Vælg en organisation på organisationslisten for at tilføje personen, og klik på **Tilføj**.

Bemærk

Indtast først personens grundlæggende oplysninger. For detaljer om konfiguration af personens grundlæggende oplysninger, se [***Konfigurer grundlæggende oplysninger***](#).

3. Klik på **Add Face** i panelet Basic Information.
4. Vælg **Upload**.
5. Vælg et billede fra den pc, hvor klienten kører.

Bemærk

Billedet skal være i JPG- eller JPEG-format og mindre end 200 KB.

6. Valgfrit: Aktivér **Verify by Device** for at kontrollere, om ansigtsgenkendelsesenheden, der administreres i klienten, kan genkende ansigtet på billedet.

Bemærk

Denne funktion er skjult eller vist alt efter enhedens kapacitet.

7. Bekræft for at tilføje personen.
 - Klik på **Tilføj** for at tilføje personen og lukke vinduet Tilføj person.
 - Klik på **Tilføj og Ny** for at tilføje personen, og fortsæt med at tilføje andre personer.

14.2.4 Tag et billede via klienten

Når du tilføjer en person, kan du tage et billede af personen med klientens integrerede kamera, USB-kamera eller indskrivningsstation og indstille dette billede som personens profil.

Før du går i gang

Sørg for, at den pc, der kører klienten, opfylder en af følgende betingelser:

- Kunden har et kamera.
- Du har tilsluttet USB-kameraet til pc'en.
- Du har tilsluttet enrollment station til pc'en via USB-interface.

Trin

1. Gå ind i Person-modulet.
2. Vælg en organisation på organisationslisten for at tilføje personen, og klik på **Tilføj for** at åbne vinduet Tilføj person.



Bemærk

Indtast først personens grundlæggende oplysninger. For detaljer, se [***Konfigurer grundlæggende oplysninger***](#).

3. Klik på **Add Face** i området Basic Information.
4. Vælg **Tag foto** for at åbne vinduet Tag foto.
5. Klik på ▾ for at vælge det integrerede kamera eller indskrivningsstationen fra rullelisten.
6. Valgfrit: Aktivér **Verify by Device** for at kontrollere, om det optagne ansigtsfoto kan opfylde uploadkravene.

Bemærk

Denne funktion er skjult eller vist alt efter enhedens kapacitet.

7. Tag et billede.
 - 1) Vend ansigtet mod kameraet, og sørg for, at dit ansigt er midt i opsamlingsvinduet.
 - 2) Klik på  for at tage et ansigtsbillede.
 - 3) Valgfrit: Klik på  for at optage igen.
 - 4) Klik på **OK** for at gemme det optagne foto.

Figur 14-3 Tag et foto via klienten

8. Bekræft for at tilføje personen.
 - Klik på **Tilføj** for at tilføje personen og lukke vinduet Tilføj person.
 - Klik på **Tilføj og Ny** for at tilføje personen, og fortsæt med at tilføje andre personer.

14.2.5 Indsaml ansigt via adgangskontrolenhed

Når du tilføjer en person, kan du indsamle personens ansigt via en adgangskontrolenhed, der er føjet til klienten, og som understøtter ansigtsgenkendelsesfunktionen.

Trin

1. Gå ind i Person-modulet.
2. Vælg en organisation på organisationslisten for at tilføje personen, og klik på **Tilføj**.

Bemærk

Indtast først personens grundlæggende oplysninger. For detaljer om konfiguration af personens grundlæggende oplysninger, se [***Konfigurer grundlæggende oplysninger***](#).

3. Klik på **Add Face** i panelet Basic Information.
4. Vælg **Fjernindsamling**.
5. Vælg en tilføjet adgangskontrolenhed eller tilmeldingsstationen fra rullelisten.

Bemærk

Hvis du vælger indskrivningsstationen, skal du klikke på **Login for** at indstille enhedens relaterede parametre, herunder IP-adresse, portnummer, brugernavn og adgangskode. Du kan også kontrollere **Face Anti-Spoofing** og vælge liveness-niveaueet som Low, Medium eller High.


Anti-spoofing af ansigt

Hvis du markerer denne funktion, kan enheden registrere, om det ansigt, der skal indsamles, er autentisk.

6. Valgfrit: Klik på **Kortlæser**, vælg kortlæserens ID, og klik på **OK**.

Bemærk

Denne funktion skal understøttes af enheden.

7. Saml ansigt.
 - 1) Vend ansigtet mod kameraet på den valgte adgangskontrolenhed, og sørg for, at dit ansigt er midt i opsamlingsvinduet.
 - 2) Klik på  for at tage et billede.
 - 3) Klik på **OK** for at gemme det optagne foto.
8. Bekræft for at tilføje personen.
 - Klik på **Tilføj** for at tilføje personen og lukke vinduet Tilføj person.
 - Klik på **Tilføj og Ny** for at tilføje personen, og fortsæt med at tilføje andre personer.

14.2.10 Konfigurer oplysninger om adgangskontrol

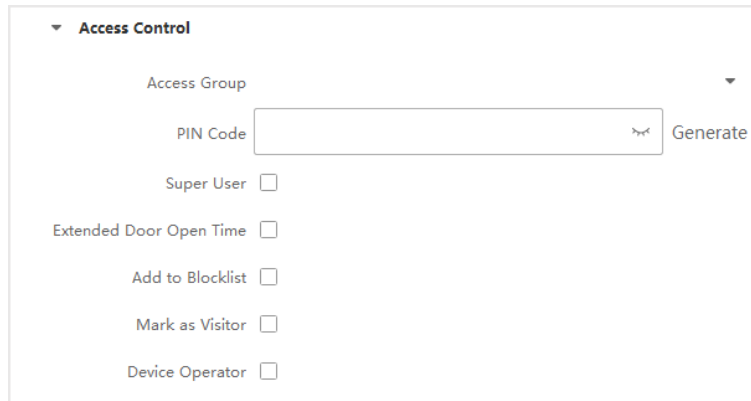
Når du tilføjer en person, kan du indstille hans/hendes adgangskontroloplysninger, såsom at knytte en adgangskontrolgruppe til personen, konfigurere PIN-kode, indstille personen som en besøgende, en bloklisterperson eller en superbruger osv.

Trin

1. Gå ind i Person-modulet.
2. Vælg en organisation på organisationslisten for at tilføje personen, og klik på **Tilføj**.
3. I området **Adgangskontrol** skal du klikke på ▼ for at vælge adgangsggruppe(r) for personen.

Bemærk

For detaljer, se [Indstil adgangsggruppe for at tildele adgangsgautorisation til personer](#).



Figur 14-4 Konfigurer oplysninger om adgangskontrol

4. Indstil en unik PIN-kode til personen, som kan bruges til adgangsgodkendelse.
- Indtast manuelt en PIN-kode med 4 til 8 cifre.

 **Bemærk**

Personers PIN-koder kan ikke gendages.

- Klik på **Generer** for tilfældigt at generere en 6-cifret PIN-kode, der ikke gendages.
-

 **Bemærk**

Hvis der er gentagne PIN-koder, vises en prompt på klienten. Administratoren kan generere en ny PIN-kode til at erstatte den gentagne PIN-kode og underrette relaterede personer.

5. Kontroller personens betjeningstilladelser.

Superbruger

Hvis personen er indstillet som superbruger, vil han/hun have adgang til alle døre/gulve og vil være undtaget fra de resterende lukkede begrænsninger, alle anti-passback-regler og førstepersonsautorisation.

Forlænget døråbningstid

Brug denne funktion til personer med nedsat mobilitet. Ved adgang til døren vil personen have mere tid end andre til at passere gennem døre.

Se Konfigurer parametre for **dør/elevator** for at få flere oplysninger om indstilling af **dørens** åbningstid.

Tilføj til blokeringsliste

Tilføj personen til blokeringslisten, og når personen forsøger at få adgang til døre/gulve, udløses en hændelse, som sendes til klienten for at underrette sikkerhedspersonalet.

Markér som besøgende

Hvis personen er en besøgende, skal du angive hans/hendes gyldige tidspunkter for besøg.

Bemærk

De gyldige tider for besøg er mellem 1 og 100. Du kan også markere **No Limit**, så er der ingen begrænsede tider for den besøgendes adgang til døre/gulve.

Enhedsoperatør

En person med rollen som enhedsoperatør er autoriseret til at betjene adgangskontrolenhederne.

Bemærk

Funktionerne Superbruger, Udvidet døråbningstid, Tilføj til blokeringsliste og Marker som besøgende kan ikke aktiveres samtidig. Hvis en person f.eks. er indstillet som superbruger, kan du ikke aktivere forlænget døråbningstid for ham/hende, tilføje ham/hende til blokeringslisten eller indstille ham/hende som besøgende.

6. Bekræft for at tilføje personen.
 - Klik på **Tilføj** for at tilføje personen og lukke vinduet Tilføj person.
 - Klik på **Tilføj og Ny** for at tilføje personen, og fortsæt med at tilføje andre personer.

14.2.11 Tilpas personoplysninger

Du kan tilpasse de personegenskaber, som ikke er foruddefinerede i klienten, efter de faktiske behov, f.eks. fødested. Efter tilpasningen kan du, når du tilføjer en person, indtaste de tilpassede oplysninger for at gøre personoplysningerne komplette.

Trin

1. Gå ind i Person-modulet.
2. Indstil felterne med brugerdefinerede oplysninger.
 - 1) Klik på **Brugerdefineret egenskab**.
 - 2) Klik på **Tilføj** for at tilføje en ny ejendom.
 - 3) Indtast ejendommens navn.
 - 4) Klik på **OK**.
3. Indstil de brugerdefinerede oplysninger, når du tilføjer en person.
 - 1) Vælg en organisation på organisationslisten for at tilføje personen, og klik på **Tilføj**.

Bemærk

Indtast først personens grundlæggende oplysninger. For detaljer om konfiguration af personens basisoplysninger, se ***Konfigurer basisoplysninger***.

- 2) Indtast personoplysningerne i panelet **Brugerdefinerede oplysninger**.
- 3) Klik på **Tilføj** for at tilføje personen og lukke vinduet Tilføj person, eller klik på **Tilføj og Ny** for at tilføje personen og fortsætte med at tilføje andre personer.

14.2.12 Konfigurer beboeroplysninger

Hvis personen er beboer, skal du indstille værelsesnummeret for ham/hende og binde en indendørs station til videointercom. Når den er bundet, kan du ringe til denne person ved at ringe til indendørsstationen og udføre videointercom med ham/hende.

Trin

1. Gå ind i Person-modulet.
2. Vælg en organisation på organisationslisten for at tilføje personen, og klik på **Tilføj**.

Bemærk

Indtast først personens grundlæggende oplysninger. For detaljer om konfiguration af personens basisoplysninger, se [***Konfigurer basisoplysninger***](#).

3. I panelet **Beboerinformation** skal du vælge indendørsstationen for at knytte den til personen.

Bemærk

Hvis du vælger **Analog indendørs station**, vises feltet **Dørstation**, og du skal vælge den dørstation, der skal kommunikere med den analoge indendørs station.

4. Indtast personens etage- og værelsesnummer.
5. Bekræft for at tilføje personen.
 - Klik på **Tilføj** for at tilføje personen og lukke vinduet Tilføj person.
 - Klik på **Tilføj og Ny** for at tilføje personen, og fortsæt med at tilføje andre personer.

14.2.13 Konfigurer yderligere oplysninger

Når du tilføjer en person, kan du konfigurere yderligere oplysninger om personen, f.eks. personens identitetstype, identitetsnummer, land osv. efter behov.

Trin

1. Gå ind i Person-modulet.
2. Vælg en organisation på organisationslisten for at tilføje personen, og klik på **Tilføj**.

Bemærk

Indtast først personens grundlæggende oplysninger. For detaljer om konfiguration af personens basisoplysninger, se [***Konfigurer basisoplysninger***](#).

3. I panelet **Yderligere oplysninger** skal du indtaste yderligere oplysninger om personen, herunder personens ID-type, ID-nummer, jobtitel osv. efter behov.
4. Bekræft for at tilføje personen.
 - Klik på **Tilføj** for at tilføje personen og lukke vinduet Tilføj person.
 - Klik på **Tilføj og Ny** for at tilføje personen, og fortsæt med at tilføje andre personer.

14.3 Import og eksport af personidentifikationsoplysninger

Du kan importere oplysninger og billeder af flere personer til klientsoftwaren i en batch. I mellemtiden kan du også eksportere personoplysningerne og billederne og gemme dem på din pc.

14.3.1 Oplysninger om importperson

Du kan indtaste oplysninger om flere personer i en foruddefineret skabelon (CSV/Excel-fil) for at importere oplysningerne til klienten i en batch.

Trin

1. Gå ind i modulet Person.
2. Vælg en tilføjet organisation på listen, eller klik på **Tilføj i** øverste venstre hjørne for at tilføje en organisation og derefter vælg den.
3. Klik på **Import** for at åbne importpanelet.
4. Vælg **Personoplysninger** som importtilstand.
5. Klik på **Download Template for Importing Person for** at downloade skabelonen.
6. Indtast personoplysningerne i den downloadede skabelon.

Bemærk

- Hvis personen har flere kort, skal du adskille kortnr. med semikolon.
- Elementer med asterisk er påkrævet.
- Som standard er ansættelsesdatoen den aktuelle dato.

-
7. Klik på **...** for at vælge CSV/Excel-filen med personoplysninger fra den lokale pc.
 8. Klik på **Import** for at starte importen.

Bemærk

- Hvis der allerede findes et personnummer i klientens database, skal du slette de eksisterende oplysninger, før du importerer.
 - Du kan ikke importere oplysninger om mere end 2.000 personer.
-

14.3.2 Import af personbilleder


Når du har importeret ansigtsbilleder af de tilføjede personer til klienten, kan personerne på billederne identificeres af en tilføjet ansigtsgenkendelsesterminal. Du kan enten importere personbilleder ét ad gangen eller importere flere billeder ad gangen alt efter behov.

Før du går i gang

Sørg for at have importeret personinformation til kunden på forhånd.

Trin

1. Gå ind i modulet Person.
-

2. Vælg en tilføjet organisation på listen, eller klik på **Tilføj i** øverste venstre hjørne for at tilføje en organisation og derefter vælg den.
3. Klik på **Import** for at åbne importpanelet, og tjek **Face**.
4. Valgfrit: Aktivér **Verify by Device** for at kontrollere, om ansigtsgenkendelsesenheden, der administreres i klienten, kan genkende ansigtet på billedet.
5. Klik på  for at vælge en ansigtsbilledfil.

Bemærk

- (Mappen med) ansigtsbillederne skal være i ZIP-format.
 - Hver billedfil skal være i JPG-format og må ikke være større end 200 KB.
 - Hver billedfil skal navngives som "Person ID_Name". Person-ID'et skal være det samme som i de importerede personoplysninger.
-

6. Klik på **Import** for at starte importen.
Importforløbet og resultatet vil blive vist.

14.3.3 Oplysninger om eksportperson

Du kan eksportere de tilføjede personers oplysninger til den lokale pc som en CSV/Excel-fil.

Før du går i gang

- Sørg for, at du har tilføjet personer til en organisation.
- Sørg for, at du har aktiveret funktionen **Eksporter personoplysninger** for at få vist knappen **Eksporter**. Se [*Indstil generelle parametre*](#) for detaljer.

Trin

1. Gå ind i modulet Person.
2. Valgfrit: Vælg en organisation på listen.

Bemærk

Alle personers oplysninger vil blive eksporteret, hvis du ikke vælger nogen organisation.

3. Klik på **Eksporter**.
4. Indtast superbrugernavnet og adgangskoden til bekræftelse.
Panelet Eksport vises.
5. Marker **Personoplysninger** som det indhold, der skal eksporteres.
6. Marker de ønskede emner, der skal eksporteres.
7. Klik på **Eksporter** for at gemme den eksporterede fil i en CSV/Excel-fil på din pc.

14.3.4 Eksport af personbilleder

Du kan eksportere ansigtsbilledfiler af de tilføjede personer og gemme dem på din pc.

Før du går i gang

- Sørg for, at du har tilføjet personer og deres ansigtsbilleder til en organisation.
- Sørg for, at du har aktiveret funktionen **Eksporter personoplysninger** for at få vist knappen **Eksporter**. Se ***Indstil generelle parametre*** for detaljer.

Trin

1. Gå ind i modulet Person.
2. Valgfrit: Vælg en organisation på listen.

Bemærk

Alle personers ansigtsbilleder vil blive eksporteret, hvis du ikke vælger nogen organisation.

3. Klik på **Eksporter** i den øverste menulinje.
4. Indtast superbrugernavnet og adgangskoden til bekræftelse.
Panelet Eksport vises.
5. Marker **Face** som det indhold, der skal eksporteres.
6. Klik på **Eksporter**, og indstil en krypteringsnøgle til at kryptere den eksporterede fil.

Bemærk

- Den eksporterede fil er i ZIP-format.
 - Det eksporterede ansigtsbillede navngives som "Person ID_Name_0" ("0" er for et fuldt frontalt ansigt).
-

14.4 Hent personoplysninger fra adgangskontrolenheden

Hvis adgangskontrolenheden er blevet konfigureret med personoplysninger (herunder personoplysninger, fingeraftryk og udstedte kortoplysninger), kan du hente personoplysningerne fra den tilføjede enhed og importere dem til klienten for yderligere operationer.

Trin

Bemærk

- Hvis det personnavn, der er gemt i enheden, er tomt, vil personnavnet blive udfyldt med det udstedte kortnummer efter import til klienten.
 - Personer vil som standard være **Male**.
 - Hvis det kortnummer eller person-ID (medarbejder-ID), der er gemt på enheden, allerede findes i klientdatabasen, vil personen med dette kortnummer eller person-ID ikke blive importeret til klienten.
-

1. Gå ind i Person-modulet.
2. Vælg en organisation til at importere personerne.
3. Klik på **Hent fra enhed**.
4. Vælg en tilføjet adgangskontrolenhed eller tilmeldingsstationen fra rullelisten.

Bemærk

Hvis du vælger indskrivningsstationen, skal du klikke på **Login og** indtaste enhedens IP-adresse, portnummer, brugernavn og adgangskode.

5. Vælg **indlæsningstilstand**.

Bemærk

Indhentningstilstanden varierer afhængigt af de forskellige enheder. Adgangskontrolenheden understøtter indhentning af personoplysninger via medarbejder-ID. Der kan angives op til 5 medarbejder-ID'er hver gang.

6. Klik på **Importer** for at begynde at importere personoplysningerne til klienten.

Bemærk

Der kan importeres op til 2.000 personer og 5.000 kort.

Personoplysningerne, herunder persondetaljer, personens fingeraftryksoplysninger (hvis konfigureret) og de tilknyttede kort (hvis konfigureret), vil blive importeret til den valgte organisation.

14.5 Flyt personer til en anden organisation

Du kan flytte de tilføjede personer til en anden organisation, hvis du har brug for det.

Før du går i gang

- Sørg for, at du har tilføjet mindst to organisationer.
- Sørg for, at du har importeret personoplysninger.

Trin

1. Gå ind i Person-modulet.
2. Vælg en organisation i venstre panel.
Personerne under organisationen vil blive vist i højre panel.
3. Vælg den person, der skal flyttes.
4. Klik på **Skift organisation**.
5. Vælg den organisation, du vil flytte personer til.
6. Klik på **OK**.

14.6 Udsted kort til personer i en batch

Klienten giver en bekvem måde at udstede kort til flere personer i en batch.



Trin

1. Gå ind i Person-modulet.
2. Klik på **Batch Issue Cards**.
Alle de tilføjede personer, der ikke har fået udstedt et kort, vil blive vist i højre panel.
3. Valgfrit: Indtast nøgleord (navn eller person-ID) i indtastningsfeltet for at filtrere den eller de personer, der skal have udstedt kort.
4. Valgfrit: Klik på **Indstillinger** for at indstille kortudstedelsesparametrene. For detaljer, se **Udstedt et kort til én person**.
5. Klik på **Initialize** for at initialisere kortregistreringsstationen eller kortlæseren, så den er klar til at udstede kort.
6. Klik på kolonnen **Kortnr.** og indtast kortnummeret.
 - Placer kortet på kortregistreringsstationen.
 - Træk kortet ind i kortlæseren.
 - Indtast kortnummeret manuelt, og tryk på Enter-tasten.Den eller de personer, der står på listen, får udstedt kort.

14.7 Tab af rapportkort

Hvis personen har mistet sit kort, kan du rapportere tabet af kortet, så den tilhørende adgangsauctorisation bliver inaktiv.

Trin

1. Gå ind i Person-modulet.
2. Vælg den person, du vil rapportere korttab for, og klik på **Rediger for** at åbne vinduet Rediger person.
3. I panelet **Credential** → **Card skal du** klikke på  på det tilføjede kort for at indstille dette kort som mistet kort.
Når du har rapporteret tab af kort, vil adgangsauctorisationen for dette kort være ugyldig og inaktiv. En anden person, der får dette kort, kan ikke få adgang til dørene ved at trække det mistede kort.
4. Valgfrit: Hvis det mistede kort bliver fundet, kan du klikke på  for at annullere tabet.
Efter annullering af korttab vil personens adgangsauctorisation være gyldig og aktiv.
5. Hvis det mistede kort er tilføjet i en adgangsgruppe, og adgangsgruppen allerede er anvendt på enheden, vil der efter rapportering af korttab eller annullering af korttab dukke et vindue op, der giver dig besked om at anvende ændringerne på enheden. Når ændringerne er blevet overført til enheden, kan de træde i kraft på enheden.

14.8 Vis ressourcestatistik

Når du har anvendt personer og adgangskontroloplysninger (herunder ansigter, kort og fingeraftryk) på enheden, kan du se ressourcestatistikker på klienten og på enheden for at vide, om ressourcerne er blevet anvendt korrekt.

Du har anvendt personer og legitimationsoplysninger på enheden. For detaljer, se [Indstil adgangsgruppe](#) for [at tildele adgangsauctorisation til personer](#).

Klik på **Personadministration** → **Ressourcestatistik** for at åbne vinduet Ressourcestatistik.

Figur 14-5 Oversigt på klienten

I området **Overview on Device** skal du vælge en enhed fra rullelisten og klikke på **Counting** for at se enhedens ressourcer, herunder personer, ansigter, kort og fingeraftryk. Ved at sammenligne ressourcerne på klienten og på enheden kan du se, om klientens ressourcer er blevet overført til enheden.

Figur 14-6 Klientressourcer anvendt på enheden



Bemærk

Denne funktion skal understøttes af enheden. Hvis enheden ikke understøtter ansigt eller fingeraftryk, vises en meddelelse i nederste højre hjørne af pc'ens skrivebord.

Kapitel 15 Adgangskontrol

Adgangskontrolmodul kan bruges til adgangskontrolenheder og videointercom-enheder. Det giver flere funktioner, herunder konfiguration af adgangsgupper, videointercom og andre avancerede funktioner.

Bemærk

For brugere med adgangskontrolmodultilladelser kan brugeren gå ind i adgangskontrolmodul og konfigurere adgangskontrolindstillingerne. Se [Tilføj](#) bruger for at indstille brugertilladelsen til adgangskontrolmodul.

15.2 Konfigurer tidsplan og skabelon

Du kan konfigurere skabelonen inklusive ferie- og ugeplan. Når du har indstillet skabelonen, kan du anvende den konfigurerede skabelon til adgangsgupper, når du indstiller adgangsgupperne, så adgangsgruppen træder i kraft i skabelonens tidsrum.

Bemærk

For indstillinger af adgangsgupper, se [Indstil adgangsgruppe for at tildele adgangsrettigheder til personer](#).

15.2.1 Tilføj ferie

Du kan oprette helligdage og indstille dagene i helligdagene, herunder startdato, slutdato og helligdagens varighed på én dag.

Trin

Bemærk

Du kan tilføje op til 64 helligdage i softwaresystemet.

1. Klik på **Adgangskontrol** → **Skema** → **Ferie** for at åbne siden Ferie.
2. Klik på **Tilføj** i venstre panel.
3. Find på et navn til ferien.
4. Valgfrit: Indtast beskrivelserne eller nogle meddelelser om denne ferie i feltet Bemærkning.
5. Tilføj en ferieperiode til ferielisten, og konfigurer feriens varighed.






Bemærk

Der kan tilføjes op til 16 ferieperioder til en ferie.

- 1) Klik på **Tilføj** i feltet Ferieliste.
 - 2) Træk markøren for at tegne tidsrummet, hvilket betyder, at den konfigurerede adgangsgruppe er aktiveret i det tidsrum.
-

Bemærk

Der kan indstilles op til 8 tidsintervaller for en ferieperiode.

- 3) Valgfrit: Udfør følgende handlinger for at redigere tidsvarighederne.
 - Flyt markøren til tidsvarigheden, og træk tidsvarigheden på tidslinjebjælken til den ønskede position, når markøren skifter til  .
 - Klik på tidsvarigheden, og rediger start-/sluttidspunktet direkte i den fremkomne dialog.
 - Flyt markøren til starten eller slutningen af tidsintervallet, og træk for at forlænge eller forkorte tidsintervallet, når markøren skifter til  .
 - 4) Valgfrit: Vælg den eller de tidsperioder, der skal slettes, og klik derefter på  i kolonnen Operation for at slette den eller de valgte tidsperioder.
 - 5) Valgfrit: Klik på  i kolonnen Operation for at slette alle tidsvarighederne i tidslinjen.
 - 6) Valgfrit: Klik på  i kolonnen Operation for at slette den tilføjede ferieperiode fra ferielisten.
6. Klik på **Gem**.

15.2.2 Tilføj skabelon

Skabelonen indeholder ugeplan og ferie. Du kan indstille ugeplanen og tildele varigheden af adgangsauctorisationen til forskellige personer eller grupper. Du kan også vælge de(n) tilføjede helligdag(e) til skabelonen.

Trin

Bemærk

Du kan tilføje op til 255 skabeloner i softwaresystemet.

1. Klik på **Adgangskontrol** → **Skema** → **Skabelon** for at åbne siden Skabelon.
-

Bemærk

Der er to standardskabeloner: All-Day Authorized og All-Day Denied, og de kan ikke redigeres eller slettes.

Autoriseret hele dagen

Adgangsauctorisationen er gyldig på alle ugens dage, og den har ingen helligdage.



Hele dagen nægtet

Adgangsautorisationen er ugyldig på alle ugens dage, og den har ingen helligdage.

2. Klik på **Tilføj** i venstre panel for at oprette en ny skabelon.
 3. Opret et navn til skabelonen.
 4. Indtast beskrivelser eller meddelelser om denne skabelon i feltet Bemærkning.
 5. Rediger ugeplanen for at anvende den i skabelonen.
 - 1) Klik på fanen **Ugeskema** i det nederste panel.
 - 2) Vælg en ugedag, og tegn tidsvarighed(er) på tidslinjen.
-

Bemærk

Der kan indstilles op til 8 tidsvarigheder for hver dag i ugeplanen.

- 3) Valgfrit: Udfør følgende handlinger for at redigere tidsvarighederne.
 - Flyt markøren til tidsvarigheden, og træk tidsvarigheden på tidslinjebjælken til den ønskede position, når markøren skifter til .
 - Klik på tidsvarigheden, og rediger start-/sluttidspunktet direkte i den fremkomne dialog.
 - Flyt markøren til starten eller slutningen af tidsintervallet, og træk for at forlænge eller forkorte tidsintervallet, når markøren skifter til .
 - 4) Gentag de to trin ovenfor for at tegne flere tidsvarigheder på de andre ugedage.
 6. Tilføj en ferie for at anvende den på skabelonen.
-


Bemærk

Der kan tilføjes op til 4 helligdage til en skabelon.

- 1) Klik på fanen **Ferie**.
 - 2) Vælg en ferie i den venstre liste, og den vil blive tilføjet til den valgte liste i højre panel.
 - 3) Valgfrit: Klik på **Tilføj** for at tilføje en ny ferie.
-

Bemærk

Se Tilføj ferie for at få flere oplysninger om, hvordan du tilføjer en **ferie**.

- 4) Valgfrit: Vælg en valgt ferie i den højre liste, og klik på  for at fjerne den valgte ferie, eller klik på **Clear** for at slette alle de valgte ferier i den højre liste.
7. Klik på **Gem** for at gemme indstillingerne og afslutte tilføjelsen af skabelonen.

15.3 Indstil adgangsgruppe for at tildele adgangsauctorisation til personer

Når du har tilføjet personen og konfigureret personens legitimationsoplysninger, kan du oprette adgangsgrupper for at definere, hvilke personer der kan få adgang til hvilke døre, og derefter

anvende adgangsgruppen på adgangskontrolenheden, så den træder i kraft.

Før du går i gang

- Tilføj en person til klienten.
- Tilføj adgangskontrolenhed til klient- og gruppeadgangspunktet. For detaljer, se [Gruppetstyring](#).
- Tilføj skabelon.

Trin

Når adgangsgruppeindstillingerne ændres, skal du anvende adgangsgruupperne på enhederne igen for at de træder i kraft. Ændringer af adgangsgruupper omfatter ændringer af skabelon, adgangsgruppeindstillinger, personens adgangsgruppeindstillinger og relaterede personoplysninger (herunder kortnummer, fingeraftryk, ansigtsbillede, kobling mellem kortnummer og fingeraftryk, kobling mellem kortnummer og fingeraftryk, kortadgangskode, kortets gyldighedsperiode osv.)

1. Klik på **Access Control** → **Authorization** → **Access Group** for at åbne Access Group-grænsefladen.
2. Klik på **Tilføj** for at åbne vinduet Tilføj.
3. I tekstfeltet **Navn** opretter du et navn til adgangsgruppen, som du ønsker.
4. Vælg en skabelon til adgangsgruppen.

Bemærk

Du bør konfigurere skabelonen, før du indstiller adgangsgruppen. Se [Konfigurer tidsplan og skabelon](#) for detaljer.

5. Vælg den eller de personer, der skal tildeles adgangsmuligheder, i venstre liste i feltet Vælg person.
6. I venstre liste i feltet Vælg adgangspunkt vælges dør(e), dørstation(er) eller etage(r), som de valgte personer skal have adgang til.
7. Klik på **Gem**.
Du kan se de(n) valgte person(er) og de(t) valgte adgangspunkt(er) i højre side af grænsefladen.

The screenshot shows the ABUS CMS software interface. On the left is a main table with columns: Name, Template, Status, and Operation. It lists three 'Access Group' entries, all with 'All-Day Authorized' templates and 'To be Applied' status. Above the table are buttons for '+ Add', 'Delete', 'Apply All to Device', 'Apply Changes to Device', and 'Applying Status'. On the right, there are two side panels. The top panel, titled 'Person', has columns for Name, Person ID, and Organization, listing 'Jane' (ID 2) and 'Mike' (ID 1), both from 'New Organization'. The bottom panel, titled 'Access Point', has columns for Access Point and Group Name, listing 'Door1_Access control host' and 'Door2_Access control host', both with 'Access control host' as the group name. Both side panels include pagination controls showing 'Total 2 Record(s)' and '1 / 1 Page(s)'.

Figur 15-2 Vis de(n) valgte person(er) og adgangspunkt(er)

8. Når du har tilføjet adgangsgrupeerne, skal du anvende dem på adgangskontrolenheden for at få dem til at træde i kraft.

- 1) Vælg den eller de adgangsgrupeer, der skal anvendes på adgangskontrolenheden.
- 2) Klik på **Apply All to Devices** for at begynde at anvende alle de valgte adgangsgrupeer på adgangskontrolenheden eller dørstationen.
- 3) Klik på **Anvend alle på enheder** eller **Anvend ændringer på enheder**.

Anvend alle på enheder

Denne handling vil slette alle eksisterende adgangsgrupeer for de valgte enheder og derefter anvende den nye adgangsgruppe på enheden.

Anvend ændringer på enheder


Denne handling sletter ikke de eksisterende adgangsgrupeer for de valgte enheder og anvender kun den ændrede del af den/de valgte adgangsgruppe(r) på enheden/enhederne.

- 4) Se den anvendte status i kolonnen Status, eller klik på **Anvendelsesstatus** for at se alle de anvendte adgangsgrupeer.

Bemærk

Du kan markere **Display Failure Only** for at filtrere de anvendte resultater.

De valgte personer i de anvendte adgangsgrupeer vil have tilladelse til at gå ind/ud af de valgte døre/dørstationer med deres tilknyttede kort eller fingeraftryk.

9. Valgfrit: Klik på  for at redigere adgangsgruppen, hvis det er nødvendigt.

 **Bemærk**

Hvis du ændrer personernes adgangsoplysninger eller andre relaterede oplysninger, vil du se meddelelsen **Access Group to Be Applied** i højre hjørne af klienten. Du kan klikke på prompten for at anvende de ændrede data på enheden. Du kan vælge enten **Anvend nu** eller **Anvend senere**.

15.4 Søg adgangsgruppe

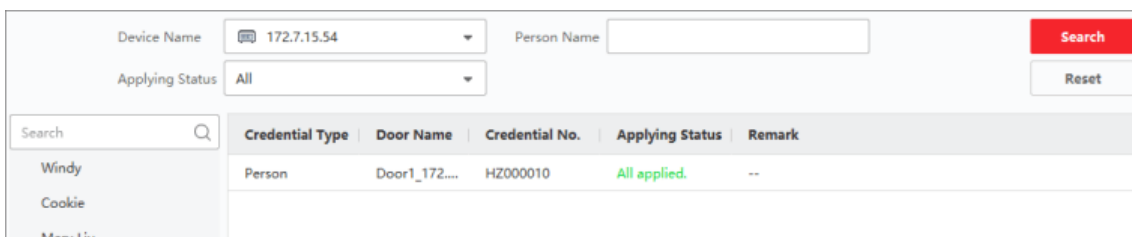
Når du har indstillet en adgangsgruppe og tildelt adgangsrettigheder til personer, kan du søge i den adgangsgruppe, som personen tilhører, og se andre relaterede oplysninger, herunder legitimationsnummer, legitimationstype, ansøgningsstatus osv.

 **Bemærk**

Sørg for, at du har indstillet adgangsgruppen til at tildele adgangsautorisation til designede personer og anvendt den. For detaljer, se [Indstil adgangsgruppe til at tildele adgangsauctorisation til personer](#).

Klik på **Adgangskontrol** → **Autorisation** → **Søg**. Vælg et enhedsnavn, og indstil søgebetiingelser (herunder personnavn og ansøgningsstatus, valgfrit), og klik derefter på **Søg**.

Du kan se den adgangsgruppe, som den søgte person tilhører, og andre oplysninger, herunder legitimationstype, dørnavn, legitimationsnummer, ansøgningsstatus, bemærkning osv.



Credential Type	Door Name	Credential No.	Applying Status	Remark
Person	Door1_172...	HZ000010	All applied.	--


Figur 15-3 Søg adgangsgruppe

15.5 Konfigurer avancerede funktioner

Du kan konfigurere adgangskontrollens avancerede funktioner, så de opfylder nogle særlige krav i

forskellige scener, f.eks. multifaktorgodkendelse, anti-passback osv.

Bemærk

- For de kortrelaterede funktioner (typen af adgangskort/multifaktorautentificering) vises kun de kort, der har adgangsgruppe, når der tilføjes kort.
 - De avancerede funktioner skal understøttes af enheden.
 - Hold markøren over den avancerede funktion, og klik derefter på  for at tilpasse de(n) avancerede funktion(er), der skal vises.
-

15.5.1 Konfigurer enhedens parametre

Når du har tilføjet adgangskontrolenheden, kan du konfigurere parametrene for adgangskontrolenheden (adgangskontroller), adgangskontrolpunkter (dør eller etage), alarmindgange, alarmudgange, kortlæsere og banekontroller.

Konfigurer parametre for adgangskontrolenhed

Når du har tilføjet adgangskontrolenheden, kan du konfigurere dens parametre, herunder overvejning af brugeroplysninger på billedet, upload af billeder efter optagelse, lagring af optagede billeder osv.


Før du går i gang

Tilføj adgangskontrolenhed til klienten.

Trin

1. Klik på **Adgangskontrol** → **Avanceret funktion** → **Enhedsparameter**.

Bemærk

Hvis du ikke kan finde Device Parameter i listen Advanced Function, skal du holde markøren over Advanced Function og derefter klikke på  for at vælge den Device Parameter, der skal vises.

2. Vælg en adgangsenhed for at få vist dens parametre på højre side.
 3. Drej kontakten til ON for at aktivere de tilsvarende funktioner.
-

Bemærk

- De viste parametre kan variere for forskellige adgangskontrolenheder.
 - Nogle af de følgende parametre er ikke angivet på siden Grundlæggende oplysninger, klik på **Mere** for at redigere parametrene.
-

RS-485 Comm. Redundans

Du bør aktivere denne funktion, hvis du tilslutter RS-485-kortlæseren til adgangskontrolenheden redundant.

Vis detekteret ansigt

Vis ansigtsbillede ved autentificering.

Vis kortnummer

Vis kortoplysningerne ved autentificering.

Vis personoplysninger

Vis personoplysningerne ved autentificering.

Overlejring af personinfo på billede

Vis personoplysningerne på det optagne billede.

Stemmeprompt

Hvis du aktiverer denne funktion, er stemmemeddelelsen aktiveret i enheden. Du kan høre stemmemeddelelsen, når du betjener enheden.

Upload billede. Efter linket optagelse

Upload automatisk de billeder, som det forbundne kamera har taget, til systemet.

Gem billede. Efter sammenkædet optagelse

Hvis du aktiverer denne funktion, kan du gemme det billede, der er taget af det forbundne kamera, på enheden.

Tryk på tasten for at indtaste kortnummer

Hvis du aktiverer denne funktion, kan du indtaste kortnummeret ved at trykke på tasten.

Wi-Fi-sonde

Hvis du aktiverer denne funktion, kan enheden undersøge de omkringliggende kommunikationsenheders MAC-adresse og uploade MAC-adressen til systemet. Hvis MAC-adressen matcher den angivne MAC-adresse, kan systemet udløse nogle sammenkoblingshandlinger.

3G/4G

Hvis du aktiverer denne funktion, kan enheden kommunikere på 3G/4G-netværk.

NFC Anti-Kloning

Hvis du aktiverer denne funktion, kan du ikke bruge det klonede kort til autentificering og yderligere forbedre sikkerheden.

4. Klik på **OK**.

5. Valgfrit: Klik på **Kopier til**, og vælg derefter adgangskontrolenhed(er) for at kopiere parametrene på siden til den/de valgte enhed(er).

Konfigurer parametre for dør/elevator

Når du har tilføjet adgangskontrolenheden, kan du konfigurere parametrene for dens adgangspunkt (dør eller etage).

Før du går i gang

Tilføj adgangskontrolenhed til klienten.

Trin

1. Klik på **Adgangskontrol** → **Avanceret funktion** → **Enhedsparameter**.
2. Vælg en adgangskontrolenhed i venstre panel, og klik derefter på ► for at vise dørene eller etagerne i den valgte enhed.
3. Vælg en dør eller etage for at få vist dens parametre på højre side.
4. Rediger dør- eller gulvparametrene.



Bemærk

- De viste parametre kan variere for forskellige adgangskontrolenheder.
 - Nogle af de følgende parametre er ikke angivet på siden Grundlæggende oplysninger, klik på **Mere** for at redigere parametrene.
-

Navn

Rediger kortlæserens navn efter ønske.

Dørkontakt

Du kan indstille dørsensoren til at forblive lukket eller åben. Normalt vil den være lukket.

Type udgangsknap

Du kan indstille exit-knappen til at forblive lukket eller åben. Normalt er den åben.

Tid for låst dør

Når det normale kort er trukket, og relæet er aktiveret, begynder timeren til låsning af døren at virke.

Forlænget åben varighed

Dørkontakten kan aktiveres med passende forsinkelse, når en person med udvidet adgangsbehov trækker sit kort.

Timeout-alarm for åben dør

Alarmen kan udløses, hvis døren ikke har været lukket i en konfigureret tidsperiode. Hvis den er sat til 0, vil der ikke blive udløst nogen alarm.

Lås døren, når den er lukket

Døren kan låses, når den er lukket, selv om **dørlåsningstiden** ikke er nået.

Tvangskode

Døren kan åbnes ved at indtaste tvangskoden, når der er tvang. Samtidig kan klienten rapportere om tvangshændelsen.

Super adgangskode

Den specifikke person kan åbne døren ved at indtaste superkodeordet.

Afvis kode

Opret en afvisningskode, som kan bruges til at stoppe kortlæserens buzzer (ved at indtaste afvisningskoden på tastaturet).

Bemærk

- Tvangskoden, superkoden og afskedigelseskoden bør være forskellige.
- Tvangskoden, superpasswordet og afskedigelseskoden skal være forskellige fra autentificeringspasswordet.
- Længden på tvangskoden, superkodeordet og afvisningskoden afhænger af enheden, men normalt skal den indeholde 4 til 8 cifre.

5. Klik på **OK**.

6. Valgfrit: Klik på **Kopier til**, og vælg derefter dør/etage(r) for at kopiere parametrene på siden til de valgte døre/etage(r).

Bemærk

Indstillingerne for dørens eller etagens statusvarighed kopieres også til den/de valgte dør(e)/etage(r).


Konfigurer parametre for kortlæser

Når du har tilføjet adgangskontrolenheden, kan du konfigurere dens kortlæserparametre.

Før du går i gang

Tilføj adgangskontrolenhed til klienten.

Trin

1. Klik på **Adgangskontrol** → **Avanceret funktion** → **Enhedsparameter**.
2. Klik på  i enhedslisten til venstre for at udvide døren, vælg en kortlæser, og du kan redigere kortlæserens parametre til højre.
3. Rediger kortlæserens grundlæggende parametre på siden Grundlæggende oplysninger.

Bemærk

- De viste parametre kan variere for forskellige adgangskontrolenheder. Der er en del parametre, der er anført som følger. Se brugervejledningen til enheden for flere detaljer.
 - Nogle af de følgende parametre er ikke angivet på siden Grundlæggende oplysninger, klik på **Mere** for at redigere parametrene.
-

Navn

Rediger kortlæserens navn efter ønske.

OK LED Polaritet/Fejl LED Polaritet/Buzzer Polaritet

Indstil OK LED Polarity/Error LED Polarity/Buzzer LED Polarity på hovedkortet i henhold til kortlæserens parametre. Generelt anvendes standardindstillingerne.

Minimumsinterval for kortgennemføring

Hvis intervallet mellem kortafspilning af det samme kort er mindre end den indstillede værdi, er kortafspilningen ugyldig. Du kan indstille den fra 0 til 255.

Max. Interval ved indtastning af PWD

Når du indtaster adgangskoden på kortlæseren, hvis intervallet mellem at trykke på to cifre er større end den indstillede værdi, slettes de cifre, du trykkede på før, automatisk.

Alarm for maks. Mislykkede forsøg

Gør det muligt at rapportere alarm, når kortlæsningsforsøgene når den indstillede værdi.

Max. Tidspunkter for kortfejl

Indstil maks. fejlforsøg ved læsning af kort.

Registrering af manipulation

Aktivér anti-tamper-detektering for kortlæseren.

Kommunikér med controlleren hver

Når adgangskontrolenheden ikke kan oprette forbindelse til kortlæseren i længere tid end den indstillede tid, vil kortlæseren automatisk gå offline.

Summende tid

Indstil kortlæserens summetid. Den tilgængelige tid spænder fra 0 til 5.999 sekunder. 0 repræsenterer kontinuerlig summen.

Kortlæser type/kortlæser beskrivelse

Hent kortlæserens type og beskrivelse. De er skrivebeskyttede.

Niveau for genkendelse af fingeraftryk

Vælg niveauet for fingeraftryksgenkendelse i rullelisten.

Standard kortlæser-godkendelsestilstand

Se kortlæserens standardgodkendelsestilstand.

Kapacitet til fingeraftryk

Se det maksimale antal tilgængelige fingeraftryk.

Eksisterende fingeraftryksnummer

Se antallet af eksisterende fingeraftryk på enheden.

Resultat

Enheden scorer det optagne billede i henhold til yaw-vinklen, pitch-vinklen og pupilafstanden. Hvis scoren er mindre end den konfigurerede værdi, vil ansigtsgenkendelsen mislykkes.

Timeout-værdi for ansigtsgenkendelse

Hvis genkendelsestiden er længere end den konfigurerede tid, vil enheden minde dig om det.

Interval for ansigtsgenkendelse

Tidsintervallet mellem to kontinuerlige ansigtsgenkendelser ved autentificering. Som standard er det 2s.

Ansigt 1:1 Matchende tærskel

Indstil tærsklen for matchning ved autentificering via 1:1 matchningstilstand. Jo større værdien er, jo mindre er den falske acceptrate, og jo større er den falske afvisningsrate ved autentificering.

1:N Sikkerhedsniveau

Indstil sikkerhedsniveauet for matchning ved autentificering via 1:N-matchningstilstand. Jo større værdien er, jo mindre er den falske acceptrate, og jo større er den falske afvisningsrate ved autentificering.

Live ansigtsgenkendelse

Aktivér eller deaktivér funktionen til registrering af levende ansigter. Hvis funktionen aktiveres, kan enheden genkende, om personen er levende eller ej.

Live ansigtsgenkendelse Sikkerhedsniveau

Når du har aktiveret Live Face Detection-funktionen, kan du indstille det matchende sikkerhedsniveau, når du udfører live ansigtsgodkendelse.

Max. Mislykkede forsøg på ansigtsgodkendelse.

Indstil det maksimale antal mislykkede forsøg på live ansigtsregistrering. Systemet låser brugerens ansigt i 5 minutter, hvis live face detection mislykkes i mere end de konfigurerede forsøg. Den samme bruger kan ikke autentificere sig via det falske ansigt inden for 5 minutter. Inden for de 5 minutter kan brugeren godkende via det rigtige ansigt to gange kontinuerligt for at låse op.

Lås-godkendelse mislykkedes Ansigt

Når Live Face Detection-funktionen er aktiveret, låser systemet brugerens ansigt i 5 minutter, hvis Live Face Detection mislykkes i mere end de konfigurerede forsøg. Den samme bruger kan ikke autentificere sig via det falske ansigt inden for 5 minutter. Inden for de 5 minutter kan brugeren godkende via det rigtige ansigt to gange kontinuerligt for at låse op.

Ansøgningstilstand

Du kan vælge indendørs eller andre anvendelsestilstande i henhold til det aktuelle miljø.

4. Klik på **OK**.

5. Valgfrit: Klik på **Kopier til**, og vælg derefter kortlæser(e) for at kopiere parametrene på siden til den/de valgte kortlæser(e).

Konfigurer parametre for alarmindgang

Når du har tilføjet adgangskontrolenheden, kan du konfigurere parametrene for dens alarmindgange.


Før du går i gang

Tilføj adgangskontrolenhed til klienten, og sørg for, at enheden understøtter alarmindgang.

Trin

Bemærk

Hvis alarmindgangen er tilkoblet, kan du ikke redigere dens parametre. Frakobl den først.

1. Klik på **Adgangskontrol** → **Avanceret funktion** → **Enhedsparameter** .
2. Klik på  i enhedslisten til venstre for at udvide døren, vælg en alarmindgang, og du kan redigere alarmindgangens parametre til højre.
3. Indstil parametrene for alarmindgangen.

Navn

Rediger navnet på alarmindgangen efter ønske.

Detektor Type

Alarmindgangens detektortype.

Zone Type

Indstil zonetyperen for alarmindgangen.

Følsomhed

Først når varigheden af det signal, der registreres af detektoren, når den indstillede tid, udløses alarmindgangen. Hvis du f.eks. har indstillet følsomheden til 10 ms, udløses denne alarmindgang kun, når varigheden af det signal, der registreres af detektoren, når 10 ms.

Udløser alarmudgang

Vælg de(n) alarmudgang(e), der skal udløses.

4. Klik på **OK**.
5. Valgfrit: Klik på kontakten i øverste højre hjørne for at tilkoble eller frakoble alarmindgangen.

Konfigurer parametre for alarmudgang

Når du har tilføjet adgangskontrolenheden, kan du konfigurere parametrene, hvis enheden linker til alarmudgange.

Før du går i gang

Tilføj adgangskontrolenhed til klienten, og sørg for, at enheden understøtter alarmoutput.

Trin

1. Klik på **Adgangskontrol** → **Avanceret funktion** → **Enhedsparameter** for at åbne siden med konfiguration af adgangskontrolparametre.

2. Klik på ► i enhedslisten til venstre for at udvide døren, vælg en alarmindgang, og du kan redigere alarmindgangens parametre til højre.
3. Indstil parametrene for alarmudgang.

Navn

Rediger kortlæserens navn efter ønske.

Aktiv tid for alarmudgang

Hvor længe alarmudgangen vil vare, efter den er udløst.

4. Klik på **OK**.
5. Valgfrit: Sæt kontakten i øverste højre hjørne på **ON** for at udløse alarmudgangen.

Konfigurer parametre for Lane Controller

Når du har tilføjet banekontrolleren til klienten, kan du konfigurere dens parametre for passage gennem banen.

Før du går i gang

Tilføj adgangskontrolenhed til klienten.

Trin

1. Klik på **Adgangskontrol** → **Avanceret funktion** → **Enhedsparameter** for at åbne siden Parameterindstillinger.
2. I enhedslisten til venstre skal du vælge en lane controller, og du kan redigere lane controllerens parametre til højre.
3. Rediger parametrene.

Passende tilstand

Vælg den controller, der skal styre enhedens barrierestatus.

- Hvis du vælger **According to Lane Controller's DIP Settings**, vil enheden følge Lane Controller's DIP-indstillinger for at styre bommen. Indstillingerne på softwaren vil være ugyldige.
- Hvis du vælger **According to Main Controller's Settings**, vil enheden følge softwarens indstillinger for at styre bommen. DIP-indstillingerne for banekontrolleren vil være ugyldige.

Godkendelse af fri passage

Hvis du aktiverer denne funktion, skal fodgængerne autentificere sig, hver gang de passerer gennem banen, når både indgangs- og udgangsbarrierens tilstand er Forbliv åben. Ellers vil der blive udløst en alarm.

Åbning/lukning af barriere Hastighed

Indstil barrierens åbne- og lukkehastighed. Du kan vælge mellem 1 og 10. Jo større værdi, jo hurtigere hastighed.

 **Bemærk**

Den anbefalede værdi er 6.

Lydprompt Varighed

Indstil, hvor længe den lyd skal vare, som afspilles, når en alarm udløses.

 **Bemærk**

0 henviser til, at alarmlyden afspilles, indtil alarmen er afsluttet.

Temperatur Enhed

Vælg den temperaturenhed, der vises i enhedens status.

4. Klik på **OK**.

15.5.2 Konfigurer resterende ulåst/låst

Du kan indstille dørens status som ulåst eller låst og indstille elevatorstyringen som fri og kontrolleret. For eksempel kan du indstille, at døren forbliver låst i ferien, og indstille, at døren forbliver ulåst i den angivne periode på arbejdsdagen.

Før du går i gang

Tilføj adgangskontrolenhederne til systemet.

Trin

1. Klik på **Access Control** → **Advanced Function** → **Remain Locked/Unlocked** for at åbne siden Remain Locked/Unlocked.
 2. Vælg den dør- eller elevatorcontroller, der skal konfigureres, på venstre panel.
 3. For at indstille dør- eller elevatorcontrollerens status i løbet af arbejdsdagen skal du klikke på **Ugeskema** og udføre følgende handlinger.
 - 1) Klik på **Forbliv ulåst**, **Forbliv låst**, **Induktiv tilstand** eller **Barrierefri tilstand** for døren.
-

 **Bemærk**



- **Induktiv tilstand:** Åbning og lukning af døren udløses af infrarød induktion fra menneskekroppen.
 - **Barrierefri tilstand:** Når et stort antal mennesker skal passere døren, vil døren forblive åben (uden hyppig autentificering), hvis person- og ID-sammenligningen lykkes. Kun når person- og ID-sammenligningen mislykkes, vil døren blive lukket.
 - Induktiv tilstand og barrierefri tilstand bør understøttes af enheden.
-

2) Klik på **Fri** eller **Kontrolleret** for elevatorstyring.

3) Træk markøren for at tegne tidsrummet, hvilket betyder, at den konfigurerede adgangsgruppe er aktiveret i det tidsrum.

Bemærk

Der kan indstilles op til 8 tidsintervaller for hver dag i ugeplanen.

- 4) Valgfrit: Udfør følgende handlinger for at redigere tidsvarighederne.
- Flyt markøren til tidsvarigheden, og træk tidsvarigheden på tidslinjebjælken til den ønskede position, når markøren skifter til  .
 - Klik på tidsvarigheden, og rediger start-/sluttidspunktet direkte i den fremkomne dialog.
 - Flyt markøren til starten eller slutningen af tidsintervallet, og træk for at forlænge eller forkorte tidsintervallet, når markøren skifter til  .
- 5) Klik på **Gem**.

Relaterede operationer






- | | |
|-------------------------|---|
| Kopi til hel uge | Vælg en varighed på tidslinjen, og klik på Copy to Whole Week for at kopiere alle varighedsindstillingerne på denne tidslinje til andre ugedage. |
| Slet valgt | Vælg en varighed på tidslinjen, og klik på Delete Selected for at slette denne varighed. |
| Klar | Klik på Ryd for at rydde alle indstillinger for varighed i ugeplanen. |

4. For at indstille dørens status i løbet af ferien skal du klikke på **Holiday** og udføre følgende handlinger.

- 1) Klik på **Forbliv ulåst**, **Forbliv låst**, **Induktiv tilstand** eller **Barrierefri tilstand**.
- 2) Klik på **Tilføj**.
- 3) Indtast startdato og slutdato.
- 4) Træk markøren for at tegne tidsrummet, hvilket betyder, at den konfigurerede adgangsgruppe er aktiveret i det tidsrum.

Bemærk

Der kan indstilles op til 8 tidsintervaller for en ferieperiode.

- 5) Udfør følgende handlinger for at redigere tidsvarighederne.
- Flyt markøren til tidsvarigheden, og træk tidsvarigheden på tidslinjebjælken til den ønskede position, når markøren skifter til  .
 - Klik på tidsvarigheden, og rediger start-/sluttidspunktet direkte i den fremkomne dialog.
 - Flyt markøren til starten eller slutningen af tidsintervallet, og træk for at forlænge eller forkorte tidsintervallet, når markøren skifter til  .
- 6) Valgfrit: Vælg den eller de tidsperioder, der skal slettes, og klik derefter på  i kolonnen Operation for at slette den eller de valgte tidsperioder.
- 7) Valgfrit: Klik på  i kolonnen Operation for at slette alle tidsvarighederne i tidslinjen.
- 8) Valgfrit: Klik på  i kolonnen Operation for at slette den tilføjede ferieperiode fra ferielisten.

- 9) Klik på **Gem**.
5. Valgfrit: Klik på **Kopier** for at kopiere dørstatusindstillingerne for denne dør til en eller flere andre døre.

15.5.3 Konfigurer multifaktorgodkendelse

Du kan administrere personer efter gruppe og indstille godkendelsen for flere personer på et adgangskontrolpunkt (dør).

Før du går i gang

Indstil adgangsgruppe, og anvend adgangsgruppen på adgangskontrolenheden. For detaljer, se **Indstil adgangsgruppe for at tildele adgangsauctorisation til personer**.

Udfør denne opgave, når du vil indstille godkendelser for flere kort på et adgangskontrolpunkt (dør).

Trin

1. Klik på **Access Control** → **Advanced Function** → **Multi-Factor Auth**.
2. Vælg en adgangskontrolenhed på enhedslisten i venstre panel.
3. Tilføj en person/kortgruppe til adgangskontrolenheden.
 - 1) Klik på **Tilføj i** højre panel.
 - 2) Opret et navn til gruppen efter ønske.
 - 3) Angiv start- og sluttidspunktet for den effektive periode for personen/kortgruppen.
 - 4) Vælg medlem(mer) og kort på listen Tilgængelig, og det/de valgte medlem(mer) og kort føjes til listen Valgt.

Bemærk

Sørg for, at du har udstedt et kort til personen.
Sørg for, at du har indstillet adgangsgruppen og anvendt adgangsgruppen på adgangskontrolenheden med succes.

- 5) Klik på **Gem**.
- 6) Valgfrit: Vælg person/kortgruppe(r), og klik derefter på **Slet** for at slette den/dem.
- 7) Valgfrit: Vælg person-/kortgruppe(r), og klik derefter på **Anvend** for at genanvende den adgangsgruppe, der ikke tidligere blev anvendt på adgangskontrolenheden.
4. Vælg et adgangskontrolpunkt (dør) for den valgte enhed på venstre panel.
5. Indtast det maksimale interval, når du indtaster adgangskoden.
6. Tilføj en godkendelsesgruppe for det valgte adgangskontrolpunkt.
 - 1) Klik på **Tilføj i** panelet Godkendelsesgrupper.
 - 2) Vælg en konfigureret skabelon som godkendelsesskabelon fra rullelisten.

Bemærk

For indstilling af skabelonen, se **Konfigurer tidsplan og skabelon**.

- 3) Vælg autentificeringstypen som **Lokal autentificering**, Lokal autentificering og **fjernåbning af dør** eller **Lokal autentificering og superadgangskode** fra rullelisten.

Lokal autentificering

Autentificering af adgangskontrolenheden.

Lokal autentificering og fjernåbning af døren

Autentificering af adgangskontrolenheden og af klienten. Når personen stryger kortet på enheden, dukker der et vindue op. Du kan låse døren op via klienten.

Figur 15-4 Fjernbetjent åbning af dør

Bemærk

Du kan markere **Offline-godkendelse** for at aktivere superadgangskode-godkendelse, når adgangskontrolenheden er afbrudt fra klienten.

Lokal autentificering og superadgangskode

Godkendelse ved hjælp af adgangskontrolenheden og superadgangskoden.

- 4) Vælg den tilføjede person/kortgruppe i den venstre liste nedenfor, og den vil blive tilføjet til Selected-listen til højre som godkendelsesgruppe.
- 5) Klik på den tilføjede autentificeringsgruppe i højre liste for at indstille autentificeringstider i kolonnen Auth Times.

Bemærk

- Autentificeringstiderne skal være større end 0 og mindre end den tilføjede personalemængde i personalegruppen.
 - Den maksimale værdi for godkendelsestider er 16.
-

- 6) Klik på **Gem**.
-

Bemærk

- For hvert adgangskontrolpunkt (dør) kan der tilføjes op til fire godkendelsesgrupper.
 - For den autentificeringsgruppe, hvor autentificeringstypen er **Lokal autentificering**, kan der tilføjes op til 8 person-/kortgrupper til autentificeringsgruppen.
 - For den godkendelsesgruppe, hvor godkendelsestypen er **Lokal godkendelse og Superadgangskode** eller **Lokal godkendelse og Fjernåbning af dør**, kan der tilføjes op til 7 person-/kortgrupper til godkendelsesgruppen.
-

7. Klik på **Gem**.

15.5.4 Konfigurer brugerdefineret Wiegand-regel

Baseret på viden om uploading af regler for tredjeparts Wiegand, kan du indstille flere tilpassede Wiegand-regler til at kommunikere mellem enheden og tredjeparts kortlæsere.

Før du går i gang

Tilslut tredjeparts kortlæsere til enheden.

Trin

Bemærk

- Som standard deaktiverer enheden den brugerdefinerede wiegand-funktion. Hvis enheden aktiverer den brugerdefinerede Wiegand-funktion, vil alle Wiegand-grænseflader i enheden bruge den brugerdefinerede Wiegand-protokol.
 - Der kan indstilles op til 5 brugerdefinerede Wiegands.
 - For detaljer om brugerdefineret Wiegand, se ***Brugerdefinerede Wiegand-regelbeskrivelser***.
-

1. Klik på **Adgangskontrol** → **Avanceret funktion** → **Brugerdefineret Wiegand** for at åbne siden Brugerdefineret Wiegand.
 2. Vælg en brugerdefineret Wiegand til venstre.
 3. Opret et Wiegand-navn.
-

Bemærk

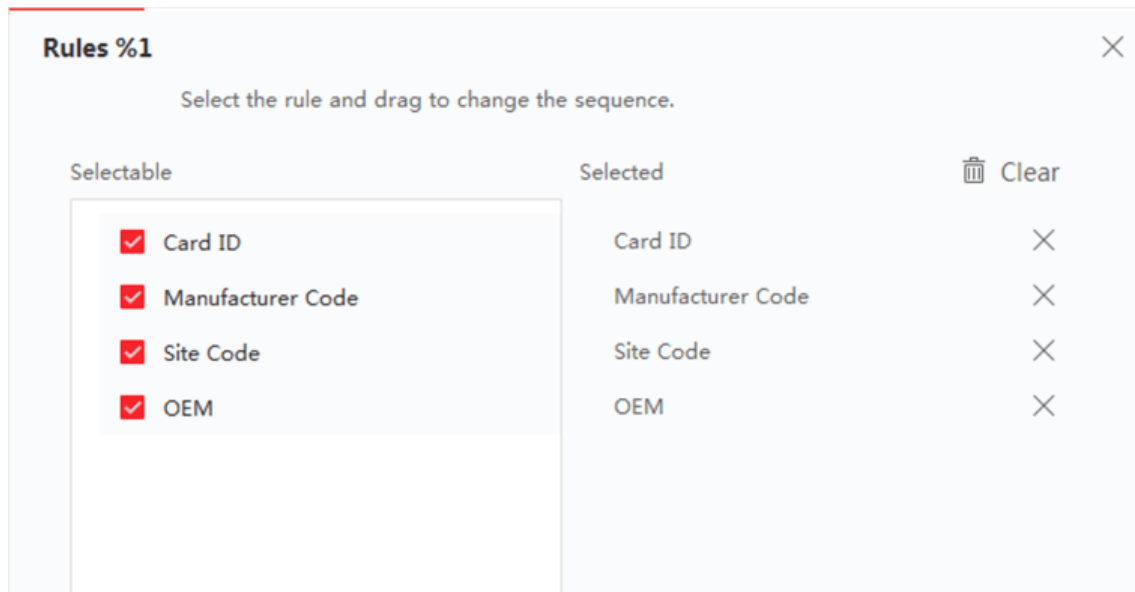
Op til 32 tegn er tilladt i det brugerdefinerede Wiegand-navn.

4. Klik på **Select Device** for at vælge den adgangskontrolenhed, der skal indstille det brugerdefinerede wiegand.
 5. Indstil paritetstilstanden i henhold til tredjeparts kortlæserens egenskaber.
-

Bemærk

- Op til 80 bits er tilladt i den samlede længde.
 - Den ulige paritetsstartbit, den ulige paritetslængde, den lige paritetsstartbit og den lige paritetslængde varierer fra 1 til 80 bit.
 - Kort-ID'ets startbit, producentkoden, stedkoden og OEM'en skal ligge mellem 1 og 80 bit.
-

6. Indstil regel for output-transformation.
 - 1) Klik på Set **Rule** for at åbne vinduet Set Output Transformation Rules.



Figur 15-5 Regel for transformation af output

- 2) Vælg regler på listen til venstre.
De valgte regler føjes til den højre liste.
- 3) Valgfrit: Træk i reglerne for at ændre rækkefølgen.
- 4) Klik på **OK**.
- 5) På fanen Custom Wiegand skal du indstille reglens startbit, længde og decimalciffer.
7. Klik på **Gem**.

15.5.5 Konfigurer kortlæserens godkendelsestilstand og tidsplan

Du kan indstille passeringsreglerne for adgangskontrolenhedens kortlæser i henhold til dine faktiske behov.

Trin

1. Klik på **Access Control** → **Advanced Function** → **Authentication** for at åbne siden til konfiguration af autentificeringstilstand.
2. Vælg en kortlæser i venstre side, som du vil konfigurere.
3. Indstil kortlæserens godkendelsestilstand.
 - 1) Klik på **Konfiguration**.

Card Reader Authentication ✕

Select the authentication mode that the card reader should support.

Selectable Mode	Selected Mode 🗑️ Clear
<input checked="" type="checkbox"/> Card+PIN	Card ✕
<input checked="" type="checkbox"/> Card	Card+PIN ✕
<input checked="" type="checkbox"/> FP	FP ✕
<input type="checkbox"/> FP+PIN	FP+Card ✕
<input type="checkbox"/> FP/Card	Face ✕
<input checked="" type="checkbox"/> FP+Card	Face + Card ✕
<input type="checkbox"/> FP+Card+PIN	Face + FP + Card ✕
<input type="checkbox"/> Face/FP/Card/PIN	Iris ✕
<input type="checkbox"/> Face + FP	
<input type="checkbox"/> Face+PIN	
<input checked="" type="checkbox"/> Face + Card	
<input checked="" type="checkbox"/> Face	
<input checked="" type="checkbox"/> Face + FP + Card	
<input type="checkbox"/> Face + PIN + FP	
<input type="checkbox"/> FP/Face	
<input type="checkbox"/> Card/Face	
<input type="checkbox"/> Card/Face/FP	
<input type="checkbox"/> Card/FP/PIN	
<input checked="" type="checkbox"/> Iris	
<input type="checkbox"/> Face, Fingerprint, Card, Password, or Iris	

OK
Cancel

Figur 15-6 Vælg kortlæserens godkendelsestilstand

Bemærk

PIN henviser til den PIN-kode, der er indstillet til at åbne døren. Se [Konfigurer oplysninger om adgangskontrol](#).

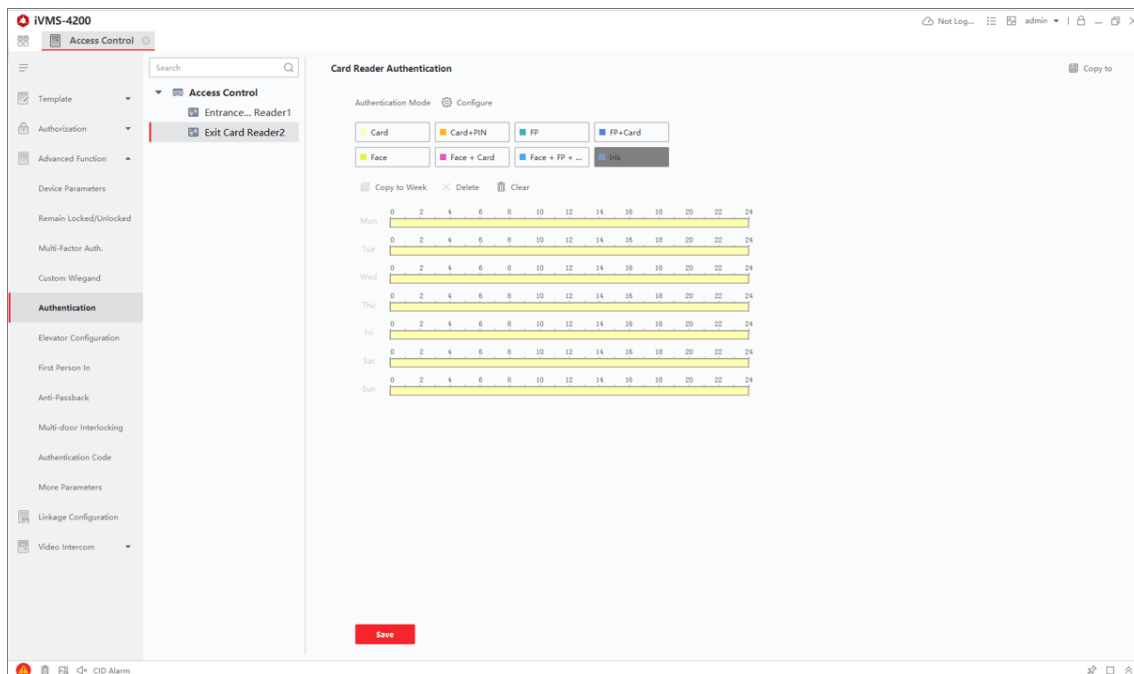
2) Tjek tilstandene på listen Tilgængelig tilstand, og de vil blive tilføjet til listen over valgte tilstande.

3) Klik på **OK**.

Når du har valgt tilstandene, vises de valgte tilstande som ikoner med forskellige farver.

4. Klik på ikonet for at vælge en kortlæsergodkendelsestilstand, og træk markøren for at tegne en farvebjælke på tidsplanen, hvilket betyder, at kortlæsergodkendelsen er gyldig i den periode.

5. Gentag ovenstående trin for at indstille andre tidsperioder.



Figur 15-7 Indstil godkendelsestilstande for kortlæsere

6. Det er valgfrit: Vælg en konfigureret dag, og klik på **Kopier til uge** for at kopiere de samme indstillinger til hele ugen.

7. Valgfrit: Klik på **Copy to** for at kopiere indstillingerne til andre kortlæsere.

8. Klik på **Gem**.

15.5.6 Konfigurer person-godkendelsestilstand

Du kan indstille adgangsreglerne for personer til den angivne adgangskontrolenhed i henhold til

dine faktiske behov.

Før du går i gang

- Tilføj en adgangskontrolenhed til klienten, og sørg for, at adgangskontrolenheden understøtter funktionen til persongodkendelse.
- Tilføj person og tildel adgangsauctorisation til designet person. For detaljer, se **Personadministration** og **Indstil adgangsgruppe for at tildele adgangsauctorisation til personer**.

Trin

1. Klik på **Adgangskontrol** → **Avanceret funktion** → **Godkendelse**.
2. Vælg en adgangskontrolenhed (understøtter funktionen personautenticering) på venstre panel for at åbne siden Personautenticeringstilstand.
3. Klik på **Tilføj** for at åbne vinduet Tilføj.
4. Vælg den eller de personer, der skal konfigureres i venstre panel.
De(n) valgte person(er) vil blive tilføjet til højre panel.
5. Vælg autentificeringstilstand på rullelisten **Authentication Mode**.
6. Klik på **OK**.

Figur 15-8 Indstil godkendelsesmetoder for personer

7. Valgfrit: Vælg person(er) på siden Persongodkendelsestilstand, og klik derefter på **Anvend for** at anvende persongodkendelsestilstanden på enheden.

Bemærk

Personautenticering har højere prioritet end andre autentificeringstilstande. Når adgangskontrolenheden er konfigureret til personautenticering, skal personen autentificere sig på denne enhed via personautenticering.

15.5.8 Konfigurer første person i

Du kan indstille flere førstepersoner til et adgangskontrolpunkt. Når den første person er autoriseret, giver det flere personer adgang til døren eller andre autentificeringshandlinger.

Før du går i gang

- Tilføj adgangskontrolenhed til klienten, og sørg for, at enheden understøtter første person i funktion.
- Tilføj person og tildel adgangsauctorisation til designet person. For detaljer, se **Personadministration** og **Indstil adgangsgruppe for at tildele adgangsauctorisation til personer**.

Trin

1. Klik på **Adgangskontrol** → **Avanceret funktion** → **Første person ind** for at åbne siden Første person ind.
2. Vælg en adgangskontrolenhed på listen i venstre panel.

3. Vælg den aktuelle tilstand som **Enable Remaining Open after First Person**, **Disable Remaining Open after First Person** eller **Authorization by First Person** fra rullelisten for hvert adgangskontrolpunkt på den valgte enhed.

Aktivér at forblive åben efter første person

Døren forbliver åben i det konfigurerede tidsrum, efter at den første person er godkendt, indtil varigheden af forbliven åben slutter. Hvis du vælger denne tilstand, skal du indstille de fortløbende godkendelsestider og intervallet for fortløbende godkendelse.

Bemærk

Varigheden for at forblive åben skal være mellem 0 og 1440 minutter. Som standard er varigheden for at forblive åben 10 minutter.

Deaktivér at forblive åben efter første person

Deaktiver funktionen for første person ind, nemlig normal godkendelse.

Autorisation af første person

Alle godkendelser (undtagen godkendelser af superkort, superkodeord, tvangskort og tvangskode) er kun tilladt efter den første persons godkendelse.

Bemærk

Du kan autentificere dig med første person igen for at deaktivere førstepersonstilstanden.

4. Klik på **Tilføj i** panelet Liste over førstepersoner.
5. Vælg person(er) i listen til venstre, og personen(erne) vil blive tilføjet til de valgte personer som den/de første person(er) i dørene.
Den/de tilføjede første person(er) vises på listen over første personer.
6. Det er valgfrit: Vælg en førsteperson fra listen, og klik på **Slet** for at fjerne personen fra listen over førstepersoner.
7. Klik på **Gem**.

15.5.9 Konfigurer anti-passback

Anti-passback-funktionen er designet til at minimere misbrug eller svigagtig brug af adgangsoplysninger, som f.eks. at give kortet tilbage til en uautoriseret person, eller skjult adgang. Anti-passback-funktionen fastlægger en bestemt rækkefølge, som adgangsoplysningerne skal bruges i for at give adgang. Du kan indstille rækkefølgen i henhold til den faktiske sti via klienten, og hvis personen bruger legitimationsoplysningerne i forkert rækkefølge, kan du også nulstille anti-password-posterne.


Før du går i gang

Tilføj en adgangskontrolenhed til klienten, og aktiver adgangskontrolenhedens anti-passing back-funktion.

Trin

Bemærk

Enten anti-passing back- eller multi-door interlocking-funktionen kan konfigureres for en adgangskontrolenhed på samme tid. For konfiguration af flerdørslåsning, se **Konfigurer flerdørslåsning**.

1. Klik på **Access Control** → **Advanced Function** → **Anti-Passback** for at åbne siden Anti-Passpack Settings.
 2. Vælg en adgangskontrolenhed på venstre panel.
 3. Vælg en kortlæser som begyndelsen på stien i feltet **Første kortlæser**.
 4. Klik på  for den valgte første kortlæser i kolonnen **Kortlæser bagefter** for at åbne dialogboksen Vælg kortlæser.
 5. Vælg de efterfølgende kortlæsere til den første kortlæser.
-

Bemærk

Op til fire efterfølgende kortlæsere kan tilføjes som efterfølgende kortlæsere til én kortlæser.

6. Klik på **OK** i dialogboksen for at gemme valgene.
7. Klik på **Gem på** siden Anti-Passback-indstillinger for at gemme indstillingerne, så de træder i kraft.

Eksempel

Indstil sti til kortgennemføring: Hvis du vælger Reader In_01 som start, og vælger Reader In_02, Reader Out_04 som de tilknyttede kortlæsere. Så kan du kun komme igennem adgangskontrolpunktet ved at trække kortet i rækkefølgen som Reader In_01, Reader In_02 og Reader Out_04.

8. Klik på **Nulstil anti-passback**, og vælg personen/personerne for at slette de relaterede anti-passback-optegnelser om personen/personerne på enheden.
-

Bemærk

Denne funktion skal understøttes af enheden.

15.5.10 Konfigurer låsning af flere døre

Du kan indstille multi-dørslåsning mellem flere døre i samme adgangskontrolenhed. For at åbne en af dørene, skal de andre døre forblive lukkede. Det betyder, at op til én dør kan åbnes på samme tid i den kombinerede dørgruppe.

Før du går i gang

Tilføj en adgangskontrolenhed til klienten, og sørg for, at enheden understøtter multi-door interlocking-funktionen.

Trin

Bemærk

- Multi-door Interlocking-funktionen understøttes kun af den adgangskontrolenhed, der har mere end ét adgangskontrolpunkt (dør).
 - Man kan konfigurere enten anti-passing back eller multi-door interlocking-funktionen for en adgangskontrolenhed på samme tid. For konfiguration af anti-passing back-funktionen, se **Konfigurer anti-passback**.
-

1. Klik på **Adgangskontrol** → **Avanceret funktion** → **Låsning af flere døre**.
 2. Vælg en adgangskontrolenhed på venstre panel.
 3. Klik på **Add (Tilføj)** på Multi-door Interlocking List-panelet for at åbne Add Access Control Point (Tilføj adgangskontrolpunkt) for at åbne vinduet Add (Tilføj).
 4. Vælg mindst to adgangskontrolpunkter (døre) fra listen.
-

Bemærk

Der kan tilføjes op til fire døre i en kombination med flere døre.

5. Klik på **OK** for at tilføje de(t) valgte adgangskontrolpunkt(er) til sammenlåsning. Den konfigurerede kombination af låsning af flere døre vises på panelet Liste over låsning af flere døre.
6. Valgfrit: Vælg en tilføjet dørkombination fra listen, og klik på **Slet for** at slette kombinationen.
7. Klik på **Anvend** for at anvende indstillingerne på adgangskontrolenheden.

15.5.11 Konfigurer autentificeringskode

Du kan konfigurere autentificeringskoden på klienten. Og derefter kan du åbne døren ved at indtaste godkendelseskoden, hvis du glemmer at tage kortet med dig.

Før du går i gang

Tilføj adgangskontrolenheden til klienten, og sørg for, at enheden understøtter autentificeringskode som autentificeringstilstand.

Trin

1. Klik på **Access Control** → **Advanced Function** → **Authentication Code** for at åbne siden til konfiguration af autentificeringskoden.
 2. Vælg en adgangskontrolenhed på listen i panelet Controller List. Alle de anvendte kort og personer vises på kortlistepanelet.
-

Bemærk

Se Indstil **adgangsgruppe** for at **tildele adgangsrettigheder til personer for at indstille** og anvende tilladelserne på enheden.

3. Klik på feltet for hvert kort i kolonnen Authentication Code (godkendelseskode) for at indtaste godkendelseskode.

Bemærk

Godkendelseskode skal indeholde 4 til 8 cifre.

4. Klik på **Gem** i øverste højre hjørne af siden Authentication Code for at gemme indstillingerne. Kortets autentificeringskodefunktion aktiveres automatisk.

Hvad du skal gøre nu

Du skal indstille adgangskontrolenhedens kortlæsergodkendelsestilstand som

Kort/Authentication Code. Se [Konfigurer kortlæsergodkendelsestilstand og tidsplan](#) for detaljer.

15.6.3 Indstilling af parametre for enhedsoptagelse

Du kan konfigurere opsamlingsparametrene for adgangskontrolenheden, herunder manuel opsamling og hændelsesudløst opsamling.

Bemærk

- Capture-funktionen skal være understøttet af enheden.
 - Før du indstiller optageparametrene, bør du først indstille billedlageret for at definere, hvor de hændelsesudløste billeder gemmes. For detaljer, se [Indstil billedlagring](#).
-

Indstil parametre for udløst optagelse

Når en hændelse indtræffer, kan kameraet på adgangskontrolenheden udløses til at tage billede(r) for at registrere, hvad der sker, når hændelsen indtræffer. Du kan se de optagne billeder, når du tjekker hændelsesdetaljerne i Event Center. Inden da skal du indstille parametrene for optagelsen, f.eks. antallet af billeder, der optages på én gang.

Før du går i gang

Før du indstiller optageparametrene, bør du først indstille billedlageret for at definere, hvor de optagne billeder skal gemmes. For detaljer, se [Indstil billedlagring](#).

Trin

Bemærk

Denne funktion skal understøttes af enheden

1. Gå ind i modulet Adgangskontrol.
 2. På navigationslinjen til venstre skal du vælge **Avanceret funktion** → **Flere parametre** → **Optagelse**.
 3. Vælg en adgangskontrolenhed på enhedslisten, og vælg **Linked Capture**.
-

4. Indstil billedstørrelse og -kvalitet.
5. Indstil optagelsestiderne, når de er udløst, hvilket definerer, hvor mange billeder der skal optages på én gang.
6. Hvis optagelsestiderne er mere end 1, skal du indstille intervallet for hver optagelse.
7. Klik på **Gem**.

Indstil manuelle indfangningsparametre

I modulet Statusovervågning kan du tage et billede manuelt med adgangskontrolenhedens kamera ved at klikke på en knap. Inden da skal du indstille parametrene for optagelsen, f.eks. billedkvalitet.

Før du går i gang

Før du indstiller optageparametrene, bør du først indstille lagringsstien for at definere, hvor de optagne billeder skal gemmes. For detaljer, se [Indstil sti til lagring af filer](#).

Trin

Bemærk

Denne funktion skal understøttes af enheden

1. Gå ind i modulet Adgangskontrol.
2. På navigationslinjen til venstre skal du vælge **Avanceret funktion** → **Flere parametre** → **Optagelse**.
3. Vælg en adgangskontrolenhed på enhedslisten, og vælg **Manual Capture**.
4. Vælg opløsningen på de optagne billeder fra rullelisten.
5. Vælg billedkvaliteten som **Høj**, **Mellem** eller **Lav**. Jo højere billedkvaliteten er, jo større bliver billedet.
6. Klik på **Gem**.

15.6.4 Indstil parametre for ansigtsgenkendelsesterminal

For ansigtsgenkendelsesterminalen kan du indstille dens parametre, herunder ansigtsbilleddatabase, QR-kodegodkendelse osv.

Trin

Bemærk

Denne funktion skal understøttes af enheden.

1. Gå ind i modulet Adgangskontrol.
2. På navigationslinjen til venstre skal du vælge **Avanceret funktion** → **Flere parametre**.
3. Vælg en adgangskontrolenhed på enhedslisten, og klik på **Terminal til ansigtsgenkendelse**.
4. Indstil parametrene.

Bemærk

Disse viste parametre varierer afhængigt af de forskellige enhedsmodeller.

COM

Vælg en COM-port til konfiguration. COM1 henviser til RS-485-grænsefladen, og COM2 henviser til RS-232-grænsefladen.

Database med ansigtsbilleder

vælg Deep Learning som ansigtsbillededatabase.

Autentificering med QR-kode

Hvis den er aktiveret, kan enhedens kamera scanne QR-koden for at godkende. Som standard er funktionen deaktiveret.

Bloklister-godkendelse

Hvis den er aktiveret, vil enheden sammenligne den person, der ønsker adgang, med personerne på blokeringslisten.

Hvis der er et match (personen er på blokeringslisten), vil adgangen blive nægtet, og enheden vil uploade en alarm til klienten.

Hvis der ikke er overensstemmelse (personen er ikke på blokeringslisten), vil adgangen blive givet.

Gem autentificerende ansigtsbillede

Hvis det er aktiveret, gemmes det ansigtsbillede, der tages ved autentificering, på enheden.

MCU-version

Se enhedens MCU-version.

5. Klik på **Gem**.

15.6.5 Aktivering af M1-kortkryptering

M1-kortkryptering kan forbedre sikkerhedsniveauet for autentificering.

Trin

Bemærk

Funktionen skal understøttes af adgangskontrolenheden og kortlæseren.

1. Gå ind i modulet Adgangskontrol.
2. På navigationslinjen til venstre skal du vælge **Avanceret funktion** → **Flere parametre**.
3. Vælg en adgangskontrolenhed på enhedslisten, og klik på **M1 Card Encryption** for at åbne siden M1 Card Encryption.
4. Sæt kontakten til on for at aktivere M1-kortets krypteringsfunktion.

5. Indstil sektor-ID'et.

Sektor-ID'et går fra 1 til 100.

6. Klik på **Gem** for at gemme indstillingerne.

15.6.6 Indstil RS-485-parametre

Du kan indstille adgangskontrolenhedens RS-485-parametre, herunder baud-hastighed, databit, stopbit, paritetstype, flowkontroltype, kommunikationstilstand, arbejdstilstand og forbindelsestilstand.

Før du går i gang

Tilføj adgangskontrolenheden til klienten, og sørg for, at enheden understøtter RS-485-interface.

Trin

1. Gå ind i modulet Adgangskontrol.
2. På navigationslinjen til venstre skal du vælge **Avanceret funktion** → **Flere parametre**.
3. Vælg en adgangskontrolenhed på enhedslisten, og klik på **RS-485** for at åbne siden RS-485-indstillinger.
4. Vælg det serielle portnummer fra rullelisten for at indstille RS-485-parametrene.
5. Indstil baud-hastighed, databit, stopbit, paritetstype, kommunikationstilstand, arbejdstilstand og forbindelsestilstand i rullelisten.

Bemærk

Når forbindelsestilstanden er **Connect Access Control Device**, kan du vælge **Card No.** eller **Person ID** som outputtype.

6. Klik på **Gem**.

- De konfigurerede parametre vil automatisk blive anvendt på enheden.
- Når du skifter arbejdstilstand eller forbindelsestilstand, genstarter enheden automatisk.

15.6.7 Indstil Wiegand-parametre

Du kan indstille adgangskontrolenhedens Wiegand-kanal og kommunikationstilstand. Når Wiegand-parametrene er indstillet, kan enheden oprette forbindelse til Wiegand-kortlæseren via Wiegand-kommunikation.

Før du går i gang

Tilføj adgangskontrolenheden til klienten, og sørg for, at enheden understøtter Wiegand.

Trin

1. Gå ind i modulet Adgangskontrol.
2. På navigationslinjen til venstre skal du vælge **Avanceret funktion** → **Flere parametre**.
3. Vælg en adgangskontrolenhed på enhedslisten, og klik på **Wiegand** for at åbne siden Wiegand-indstillinger.

4. Sæt kontakten til on for at aktivere Wiegand-funktionen for enheden.
5. Vælg Wiegand-kanalnr. og kommunikationstilstand fra rullelisten.

Bemærk

Hvis du indstiller **kommunikationsretningen** som **Sending**, skal du indstille **Wiegand Mode** som Wiegand **26** eller **Wiegand 34**.

6. Klik på **Gem**.
 - De konfigurerede parametre vil automatisk blive anvendt på enheden.
 - Når du har ændret kommunikationsretningen, genstarter enheden automatisk.

15.7 Konfigurer linkage-handlinger til adgangskontrol

Du kan konfigurere forskellige sammenkædningshandlinger for den hændelse, der registreres af adgangskontrolenheden. Derefter udløses forbindelseshandlingerne, når hændelsen sker. Denne mekanisme bruges til at underrette sikkerhedspersonalet om hændelsen eller til at udløse automatisk adgangskontrol i realtid.

Der understøttes to typer linkage-handlinger:

- **Klienthandlinger:** Når hændelsen registreres, vil den udløse handlinger på klienten, såsom at klienten udsender en akustisk advarsel...
- **Enhedshandlinger:** Når hændelsen registreres, vil den udløse handlinger på en bestemt enhed, f.eks. at en kortlæser summer, at en dør åbnes/lukkes osv.

15.7.1 Konfigurer klienthandlinger for adgangshændelse

Selv om du er langt væk fra et adgangspunkt, kan du stadig få at vide, hvad der sker, og hvor meget det haster, via klienten ved at konfigurere klienthandlinger for adgangshændelsen. Klienthandlinger henviser her til de handlinger, der automatisk udføres af klienten selv, såsom at give en akustisk advarsel og sende en e-mail. Når en hændelse er udløst, giver klienten besked til sikkerhedspersonalet, så han/hun kan håndtere hændelsen i tide.

Før du går i gang

Tilføj adgangskontrolenhed til klienten.

Trin

1. Klik på **Hændelseskonfiguration** → **Adgangskontrolhændelse**.
De tilføjede adgangskontrolenheder vises på enhedslisten.
2. Vælg en ressource (herunder enhed, alarmindgang, dør/elevator og kortlæser) fra enhedslisten.
De begivenhedstyper, som den valgte ressource understøtter, vises.
3. Vælg begivenheden/begivenhederne, og klik på **Rediger prioritet** for at definere prioriteten for begivenheden/begivenhederne, som kan bruges til at filtrere begivenheder i Event Center.
4. Indstil hændelsens forbindelseshandlinger.

- 1) Vælg begivenhed(er), og klik på **Edit Linkage** for at indstille klientens handlinger, når begivenheden(erne) udløses.

Hørbar advarsel

Klientsoftwaren giver en akustisk advarsel, når hændelsen udløses. Du kan vælge alarmlyd til den hørbare advarsel.

Bemærk

For detaljer om indstilling af alarmlyd, se [Indstil alarmlyd](#).

Send e-mail

Send en e-mailnotifikation om begivenheden til en eller flere modtagere.

For detaljer om indstilling af e-mail-parametre, se [Indstil e-mail-parametre](#).

Pop op-vindue

Pop-up-vindue til visning af hændelsesoplysninger (herunder hændelsesdetaljer, hændelsesrelaterede videooptagelser, hændelsesrelaterede billeder) på softwareklienten, når hændelsen udløses.

Visning på kort

Når begivenhedskilden tilføjes som et hot spot på kortet, vises hot spottet med et rødt tal (angiver antallet af begivenheder, og det maksimale antal er 10) ved siden af, når begivenheden udløses, hvilket hjælper sikkerhedspersonalet med at se, hvor begivenheden finder sted.

Du kan også klikke på hotspottet for at se detaljerne om begivenheden og livevideoen fra det tilknyttede kamera.

Forbundet kamera

Link det valgte kamera til at tage et billede, når adgangshændelsen udløses.

Vælg kameraet i rullelisten.

- 2) Klik på **OK**.

5. Aktivér hændelsen, så når den registreres, sendes hændelsen til klienten, og forbindelseshandlingerne udløses.

6. Valgfrit: Klik på **Copy to** for at kopiere hændelsesindstillingerne til en anden adgangskontrolenhed, alarmindgang, dør/elevator eller kortlæser.

15.7.2 Konfigurer enhedens handlinger for adgangshændelse

Du kan indstille adgangskontrolenhedens forbindelseshandlinger for adgangskontrolenhedens udløste hændelse. Når en hændelse derefter udløses, kan den udløse alarmudgang, buzzer på

adgangskontrollen og andre handlinger.

Trin

Bemærk

Koblingshandlingerne skal understøttes af enheden.

1. Klik på **Access Control** → **Linkage Configuration**.
2. Vælg adgangskontrolenheden fra listen til venstre.
3. Klik på **Tilføj** for at tilføje en ny sammenkædning.
4. Vælg **Event Linkage** som hændelseskilde.
5. Vælg hændelsestype og detaljeret hændelse for at indstille forbindelsen.
6. I området Linkage Target skal du indstille egenskabsmålet for at aktivere denne handling.

Buzzer på controller

Den akustiske advarsel fra adgangskontrolenheden vil blive udløst.

Indfangning

Der tages et begivenhedsrelateret billede, når den valgte begivenhed indtræffer.

Optagelse

Der tages et begivenhedsrelateret billede, når den valgte begivenhed indtræffer.

Bemærk

Enheden skal understøtte optagelse.

Buzzer på læseren

Den akustiske advarsel fra kortlæseren udløses.

Alarmudgang

Alarmudgangen udløses for notifikation, når den valgte hændelse sker.

Alarmindgang

Til- eller frakobl alarmindgangen.

Bemærk

Enheden skal understøtte alarmindgangsfunktionen.

Adgangspunkt

Dørens status som åben, lukket, forblive åben eller forblive lukket udløses.

Bemærk

Måldøren og kildedøren kan ikke være den samme.

Lydafspilning

Lydprompten vil blive udløst. Og det valgte lydindeksrelaterede lydindhold vil blive afspillet i henhold til den konfigurerede afspilningstilstand.

7. Klik på **Gem**.

8. Valgfrit: Når du har tilføjet enhedskoblingen, kan du gøre et eller flere af følgende:

Rediger indstillinger for sammenkædning Vælg de konfigurerede linkage-indstillinger på enhedslisten, og du kan redigere dens hændelseskildeparametre, herunder hændelseskilde og linkage-mål.

Slet indstillinger for sammenkædning Vælg de konfigurerede forbindelsesindstillinger på enhedslisten, og klik på **Slet** for at slette dem.

15.7.3 Konfigurer enhedens handlinger for kortgennemføring

Du aktiverer adgangskontrolenhedens koblingshandling (såsom at deaktivere en zone og udløse en lydprompt), når et specifikt kort trækkes. På denne måde kan du overvåge kortholderens adfærd og opholdssted.

Trin

Bemærk

Det skal understøttes af enheden.

1. Klik på **Access Control** → **Linkage Configuration**.
2. Vælg adgangskontrolenheden fra listen til venstre.
3. Klik på **Tilføj** for at tilføje en ny sammenkædning.
4. Vælg **Card Linkage** som hændelseskilde.
5. Indtast kortnummeret, eller vælg kortet fra rullelisten.
6. Vælg den kortlæser, hvor kortet skal swipes.
7. I området Linkage Target skal du indstille egenskabsmålet for at aktivere denne handling.

Buzzer på controller

Den akustiske advarsel fra adgangskontrolenheden vil blive udløst.

Buzzer på læseren

Den akustiske advarsel fra kortlæseren udløses.

Indfangning

Der tages et begivenhedsrelateret billede, når den valgte begivenhed indtræffer.

Optagelse

Der tages et begivenhedsrelateret billede, når den valgte begivenhed indtræffer.

Bemærk

Enheden skal understøtte optagelse.

Alarmudgang

Alarmudgangen vil blive aktiveret for notifikation.

Alarmindgang

Til- eller frakobl alarmindgangen.

Bemærk

Enheden skal understøtte alarmindgangsfunktionen.

Adgangspunkt

Dørens status som åben, lukket, forblive åben eller forblive lukket udløses.

Lydafspilning

Lydprompten vil blive udløst. Og det valgte lydindeksrelaterede lydindhold vil blive afspillet i henhold til den konfigurerede afspilningstilstand.

8. Klik på **Gem**.

Når kortet (konfigureret i trin 5) swipes på kortlæseren (konfigureret i trin 6), kan det udløse de tilknyttede handlinger (konfigureret i trin 7).

9. Valgfrit: Når du har tilføjet enhedskoblingen, kan du gøre et eller flere af følgende:

Slet indstillinger for sammenkædning Vælg de konfigurerede linkage-indstillinger på enhedslisten, og klik på **Slet** for at slette dem.

Rediger indstillinger for sammenkædning Vælg de konfigurerede linkage-indstillinger på enhedslisten, og du kan redigere dens hændelseskildeparametre, herunder hændelseskilde og linkage-mål.

15.7.4 Konfigurer enhedens handlinger for person-id'et

Du kan indstille adgangskontrolenhedens koblingshandlinger for det angivne person-ID. Når adgangskontrolenheden registrerer det angivne person-ID, kan den udløse alarmoutput, buzzer på

kortlæseren og andre handlinger for at implementere særlig overvågning af den angivne person.

Trin

Bemærk

Det skal understøttes af enheden.

1. Klik på **Access Control** → **Linkage Configuration**.
2. Vælg adgangskontrolenheden fra listen til venstre.
3. Klik på **Tilføj** for at tilføje en ny sammenkædning.
4. Vælg **Person Linkage** som hændelseskilde.
5. Indtast medarbejdersnummeret, eller vælg personen fra rullelisten.
6. Vælg den kortlæser, hvor kortet skal swipes.
7. I området Linkage Target skal du indstille egenskabsmålet for at aktivere denne handling.

Buzzer på controller

Den akustiske advarsel fra adgangskontrolenheden vil blive udløst.

Buzzer på læseren

Den akustiske advarsel fra kortlæseren udløses.

Indfangning

Der tages et begivenhedsrelateret billede, når den valgte begivenhed indtræffer.

Optagelse

Der tages et begivenhedsrelateret billede, når den valgte begivenhed indtræffer.

Bemærk

Enheden skal understøtte optagelse.

Alarmudgang

Alarmudgangen vil blive aktiveret for at give besked.

Alarmindgang

Til- eller frakobl alarmindgangen.

Bemærk

Enheden skal understøtte zonefunktion.

Adgangspunkt

Dørens status som åben, lukket, forblive åben eller forblive lukket udløses.

Lydafspilning

Lydprompten vil blive udløst. Og det valgte lydindeksrelaterede lydindhold vil blive afspillet i henhold til den konfigurerede afspilningstilstand.

8. Klik på **Gem**.

9. Valgfrit: Når du har tilføjet enhedskoblingen, kan du gøre et eller flere af følgende:

Slet indstillinger for sammenkædning Vælg de konfigurerede forbindelsesindstillinger på enhedslisten, og klik på **Slet** for at slette dem.

Rediger indstillinger for sammenkædning Vælg de konfigurerede linkage-indstillinger på enhedslisten, og du kan redigere dens hændelseskildeparametre, herunder hændelseskilde og linkage-mål.

15.8.1 Status for kontroldør

Du kan styre status for døren(e), herunder låse døren op, låse døren, lade døren forblive ulåst, lade døren forblive låst, lade alle døre forblive ulåste osv.

Før du går i gang

- Tilføj person og tildel adgangsautorisation til designet person, og personen vil have adgangsautorisation til adgangspunkterne (dørene). For detaljer, se [***Personadministration og Indstil adgangsgruppe for at tildele adgangsautorisation til personer***](#).
- Sørg for, at betjeningsbrugeren har tilladelse til adgangspunkterne (dørene). For detaljer, se [***Tilføj bruger***](#).

Trin

1. Klik på **Overvågning** for at åbne statusovervågningssiden.
2. Vælg en access point-gruppe i øverste højre hjørne.

Bemærk

For administration af access point-gruppen, se [***Gruppestyring***](#).

Dørene i den valgte adgangskontrolgruppe vises.

3. Klik på et dørikon for at vælge en dør, eller tryk på **Ctrl** og vælg flere døre.

Bemærk

For **Remain All Unlocked** og **Remain All Locked** skal du ignorere dette trin.

4. Klik på følgende knapper for at styre døren.

Lås op

Når døren er låst, låser du den op, og den vil være åben én gang. Efter den åbne periode vil døren automatisk blive lukket og låst igen.

Lås

Når døren er låst op, låses den, og den vil være lukket. Den person, der har adgangstilladelsen, kan få adgang til døren med legitimationsoplysninger.

Forbliv ulåst

Døren vil være ulåst (uanset om den er lukket eller åben). Alle personer kan få adgang til døren uden legitimation.

Forbliv låst

Døren vil være lukket og låst. Ingen person kan få adgang til døren, selvom han/hun har de autoriserede legitimationsoplysninger, undtagen superbrugerne.

Forbliv helt ulåst

Alle døre i gruppen vil være ulåste (uanset om de er lukkede eller åbne). Alle personer kan få adgang til dørene uden legitimation.

Forbliv alle låst

Alle døre i gruppen vil være lukkede og låste. Ingen person kan få adgang til dørene, selvom han/hun har de autoriserede legitimationsoplysninger, undtagen superbrugerne.

Indfangning

Tag et billede manuelt.



Bemærk

Capture-knappen er tilgængelig, når enheden understøtter capture-funktionen. Billedet gemmes på den pc, der kører klienten. Se Indstil sti til lagring af **filer** for at indstille **stien til lagring**.

Resultat

Dørenes ikon vil ændre sig i realtid i henhold til operationen, hvis operationen lykkes.

15.8.3 Tjek adgangsregistreringer i realtid

Adgangsprotokoller i realtid kan vises i klienten, herunder kortgennemtræk, ansigtsgenkendelse, temperaturoplysninger på hudoverfladen osv. Du kan også se personoplysningerne og se det billede, der blev taget under adgangen.

Før du går i gang

Du har tilføjet person(er) og adgangskontrolenhed(er) til klienten. For detaljer, se **Personadministration** og **Tilføj enhed**.

Trin

1. Klik på **Overvågning** for at åbne overvågningsmodulet.

Adgangsposter i realtid vises nederst på siden. Du kan se detaljer om registreringen, herunder kortnummer, personnavn, hændelsestidspunkt, dørplacering, temperatur, godkendelsestype osv.

Figur 15-12 Adgangsposter i realtid

 **Bemærk**

Du kan højreklikke på kolonnenavnet i tabellen Access Event for at vise eller skjule kolonnen efter behov.

2. Valgfrit: Vælg en access point-gruppe fra rullelisten i øverste højre hjørne for at få vist adgangsregistreringer i realtid for den valgte gruppe.
 3. Valgfrit: Tjek hændelsestype og hændelsesstatus.
De registrerede hændelser af kontrolleret type og status vises i listen nedenfor.
 4. Valgfrit: Markér **Vis seneste hændelse** for at se den seneste adgangspost.
Arkivlisten vil blive opstillet omvendt kronologisk.
 5. Valgfrit: Markér **Enable Abnormal Temperature Prompt (Aktivér unormal temperaturprompt)** for at aktivere unormal temperaturprompt på hudoverfladen.
-


 **Bemærk**

Hvis det er aktiveret, og der er oplysninger om unormal temperatur, vises et vindue med unormal temperatur, når du åbner overvågningsmodulet, med personens billede, hudoverfladetemperatur, kortnummer, personnavn osv.


6. Valgfrit: Klik på en begivenhed for at se personbilleder (inklusive taget billede og profil).
-

 **Bemærk**

I **Linked Capture** Picture-feltet kan du dobbeltklikke på det optagne billede for at se et forstørret billede.

7. Valgfrit: Klik på  for at se overvågningsdetaljer (herunder personens detaljerede oplysninger og det optagne billede).
-


 **Bemærk**

I pop op-vinduet kan du klikke på  for at se overvågningsdetaljer i fuld skærm.

Kapitel 19 Logsøgning

Der findes to logtyper: driftslog og systemlog. Driftsloggen henviser til de normale handlinger, som brugeren har udført på klienten, såsom tilføjelse af enhed, nulstilling af adgangskode, start af livevisning etc.; og systemloggen registrerer systemoplysningerne, såsom login, logout, låsning og oplåsning etc. Du kan søge i logfilerne og se logoplysningerne, herunder tid, bruger osv.


Trin

1. Gå ind i logsøgningsmodulet.
2. Klik på  for at angive start- og sluttidspunkt.

Bemærk

Du kan søge i logfilerne inden for en måned.

3. Vælg en bruger for at søge i de logfiler, der genereres, når denne bruger arbejder på klienten.
4. Vælg **Driftslog** eller **Systemlog** som logtype.
5. Klik på **Søg**.
Logfilerne mellem starttidspunktet og sluttidspunktet vises på listen. Du kan tjekke driftstid, type og andre oplysninger om logfilerne.
6. Det er valgfrit: Udfør følgende handlinger, hvis der er for mange logfiler.

Filer Klik på  på hver tabeloverskrift, og vælg at filtrere logfilerne.

Sortering Klik på tabeloverskriften for at sortere logfilerne efter tid eller bogstavrækkefølge.

Kapitel 20 Brugeradministration

For at forbedre systemsikkerheden bør administratoren oprette forskellige konti til forskellige brugere og tildele forskellige tilladelser til brugerne. For at undgå, at forskellige personer deler den samme brugerkonto, anbefaler vi, at du administrerer brugerkontiene med jævne mellemrum.

20.1 Tilføj bruger

Superbrugeren og administratoren kan tilføje nye brugere og tildele forskellige tilladelser til forskellige brugere, hvis det er nødvendigt.

Udfør denne opgave for at tilføje en brugerkonto.

Trin

Bemærk

Den brugerkonto, du registrerede for at logge på softwaren, er indstillet som superbruger.

1. Gå ind i modulet Brugeradministration.
2. Klik på **Tilføj bruger** for at vise brugerinformationsområdet.
3. Vælg brugertype fra rullelisten.

Administrator

Administratorkontoen har som standard alle tilladelser og kan ændre adgangskoder og tilladelser for alle operatører og sin egen.

Operatør

Operatørkontoen har ingen tilladelser som standard, og du kan tildele tilladelserne manuelt. En operatør kan kun ændre adgangskoderne til sin egen konto og de konti, der er tilføjet af operatøren.

4. Indtast brugernavn, adgangskode og bekræft adgangskode som ønsket.
-

Forsigtig

Styrken af enhedens adgangskode kan kontrolleres automatisk. Vi anbefaler på det kraftigste, at du ændrer adgangskoden efter eget valg (med mindst 8 tegn, herunder mindst tre slags af følgende kategorier: store bogstaver, små bogstaver, tal og specialtegn) for at øge sikkerheden for dit produkt. Og vi anbefaler, at du ændrer din adgangskode regelmæssigt, især i højsikkerhedssystemet, hvor en månedlig eller ugentlig ændring af adgangskoden kan beskytte dit produkt bedre.

Korrekt konfiguration af alle adgangskoder og andre sikkerhedsindstillinger er installatørens og/eller slutbrugers ansvar.

5. Markér afkrydsningsfelterne for at tildele tilladelser til den oprettede bruger.
6. Valgfrit: Klik på **Standardværdi** for at gendanne standardrettighederne for denne bruger.
7. Klik på **Gem**.

Bemærk

Der kan tilføjes op til 50 brugerkonti til klientsoftwaren.

- Når brugerkontoen er oprettet, føjes den til brugerlisten på siden Account Management.
8. Valgfrit: Udfør følgende handlinger, når brugerkontoen er oprettet.

Rediger bruger

Klik på en bruger fra listen for at redigere brugeroplysningerne.

Bemærk

Det er kun superbrugerens adgangskode, der kan redigeres.

Slet bruger

Vælg brugeren fra listen, og klik på **Slet bruger**.

Bemærk

Du kan ikke slette superbrugeren.

20.2 Skift brugerens adgangskode

Administratoren kan ændre den normale brugers adgangskode uden at indtaste den gamle adgangskode, mens administratoren skal indtaste den gamle adgangskode, når han ændrer sin egen adgangskode.

Før du går i gang

Tilføj bruger til softwareklienten.

Trin

1. Gå ind i modulet Brugeradministration.
 2. Vælg den bruger, der skal skifte adgangskode, og klik på **Skift**.
 3. Valgfrit: Indtast den gamle adgangskode.
-

Bemærk

Når du ændrer administratorens adgangskode, skal du først indtaste den gamle adgangskode.

4. Indtast den nye adgangskode, og bekræft den.
 5. Klik på **OK**.
-

Kapitel 21 Systemkonfiguration

21.1 Indstil generelle parametre

Du kan konfigurere de mest brugte parametre, herunder loggens udløbstid, netværkets ydeevne osv.

Trin

1. Gå ind i modulet Systemkonfiguration.
2. Klik på fanen **Generelt** for at åbne siden Generelle indstillinger.
3. Konfigurer de generelle parametre.

Datoformat / Tidsformat

Visningsstilen for dato og klokkeslæt på relaterede sider.

Periode for opbevaring af logfiler

Den tid, logfilerne skal opbevares. Når den er overskredet, slettes filerne.

Maksimal tilstand

Vælg **Maksimer** eller **Fuld skærm** som den maksimale tilstand. Maksimeringstilstand kan maksimere skærmen og vise proceslinjen. **Fuldskærmstilstand** kan vise klienten i fuldskærmstilstand.

Netværkets ydeevne

Indstil netværksforholdene til **Normal**, **Better** eller **Best**.

Gem billeder i strukturdataformat

- Når **Save Pictures in Structure Data Format** er aktiveret, vil **Delete Registered Picture** in Person-modulet være tilgængeligt. Hvis en persons oplysninger anvendes på enheden/enhederne med succes, slettes personens billede automatisk, og der vises ikke noget billede i Basisoplysninger. Ansigtsskolonnen i Person-modulet viser nummeret på de(t) tilføjede ansigtsbillede(r).
- Når **Gem billeder i strukturdataformat** er aktiveret, vises der ingen billeder i feltet Begivenhedsdetaljer i Event Center.

Aktivér tastatur og joystick

Aktivér tastaturet eller joysticket. Når det er aktiveret, kan du indstille genvejene til tastaturet og joysticket.



Bemærk

For detaljer, se [Indstil tastatur- og joystickgenveje](#).

Oplysninger om eksportperson

Hvis du aktiverer dette, vil Eksport-knappen til eksport af personoplysninger blive vist på siden Personadministration. Vær opmærksom på personoplysningernes sikkerhed.

Periode for opbevaring af hændelser

Tidsperioden for opbevaring af begivenhedsoplysningerne. Når opbevaringsperioden udløber, slettes begivenhedsoplysningerne automatisk.

Automatisk tidssynkronisering

Synkroniser automatisk tiden på de tilføjede enheder med tiden på den pc, der kører klienten, på et bestemt tidspunkt.

Automatisk opgradering af enhed

Indstil opgraderingstilstanden, når den nye version af enheden er registreret.

Deaktiver

Når den er aktiveret, vil klienten ikke downloade firmwarepakken og opgradere, selvom klienten registrerer en ny version af klienten.

Spørg mig, hvis du downloader og opgraderer

Når klienten har fundet en ny version af enheden, vil den spørge brugeren, om firmwarepakken skal downloades og opgraderes.

Download og spørg mig, hvis du opgraderer

Når klienten har registreret den nye version af enheden, downloader den automatisk firmwarepakken og spørger brugeren, om han vil opgradere.

Download og anmod automatisk

Når klienten har registreret den nye version af enhederne, downloader den firmwarepakken og opgraderer den nye version automatisk.

Du skal indstille en tidsplan i feltet **Upgrade Time**, hvor klienten automatisk opgraderer den nye version.

Land/Region

Vælg serverens region for ABUS Link Station, du kan vælge den region, du tilhører, eller den nærmeste region i nærheden.

4. Klik på **Gem**.

21.2 Indstilling af Live View- og afspilningsparametre

Du kan indstille parametrene for livevisning og afspilning, herunder billedformat, preplay-varighed osv.

Trin

1. Gå ind i modulet Systemkonfiguration.
2. Klik på fanen **Live View og Playback**.
3. Konfigurer parametrene for livevisning og afspilning.

Billedformat

Vælg **JPEG** eller **BMP** som billedformat til lagring af billeder.



Bemærk

Hvis kontakten **Display Temperature on Captured Pictures** er sat til ON, er JPEG valgt som billedformat som standard og kan ikke ændres.

Videoformat

Vælg **MP4/AVI** som format for optagede videoer.

Flet downloadede videofiler

Indstil den maksimale størrelse på den flettede videofil til download af videofilen efter dato.

Søg i videofiler gemt i

Søg efter videofiler, der er gemt på den lokale enhed, på lagerverseren eller både på lagerverseren og den lokale enhed til afspilning.

Forspil til

Indstil forspilningstiden for afspilning af begivenheder. Som standard er den 30 sekunder.

Prioriter afspilning af videofiler på storage-serveren

Afspil fortrinsvis de videofiler, der er optaget på lagerverseren. Ellers afspiller du de videofiler, der er optaget på den lokale enhed.

Genoptag seneste Live View-status efter genstart

Genoptag den seneste live view-status, når du logger ind på klienten igen.

Frakobl baggrundsvideoer i enkelt livevisning

I multi-window division-tilstand skal du dobbeltklikke på en live-video for at vise den i 1-window division-tilstand, og de andre live-videoer vil blive stoppet for at spare på ressourcerne.

Aktivér hjul til zoom

Brug musehjulet til at zoome ind eller ud på videoen i PTZ-tilstand, eller til at zoome ind eller gendanne videoen i digital zoom-tilstand. På denne måde kan du direkte zoome ind eller ud (eller gendanne) livevideoen ved at rulle med musen.

Spring over uberørt video under VCA-afspilning

Spring den uberørte video over under VCA-afspilning, og den uberørte video vil ikke blive afspillet under VCA-afspilning.

4. Klik på **Gem**.

21.3 Indstil billedparametre

Klientens billedparametre kan konfigureres, f.eks. visningskala, afspilningsydelse osv.

Trin

1. Åbn siden Systemkonfiguration.
2. Klik på fanen **Billede** for at åbne grænsefladen Billedindstillinger.
3. Konfigurer billedparametrene.

Se skala

Visningskalaen for videoen i livevisning eller afspilning. Den kan indstilles som **fuld skærm**, **4:3**, **16:9** eller **original opløsning**.

Bemærk

Du kan også indstille visningskalaen i Live View-modulet. For detaljer, se [Live View](#).

Spil forestilling

Livevideoens afspilningsperformance. Den kan indstilles som **Shortest Delay**, **Balanced** eller **Fluency**.

Du kan også vælge **Brugerdefineret** og konfigurere billedhastigheden efter dine faktiske behov.

Hardware-afkodning foretrækkes

Vælg **D3D9** eller **D3D11** for at aktivere afkodning med hardware til livevisning og afspilning. Hardwaredekodning kan give bedre dekodningsydelse og lavere CPU-brug ved afspilning af HD-video under livevisning eller afspilning.

Aktivér fremhævnings

Marker de registrerede objekter med grønne rektangler i livevisning og afspilning.

Vis transaktionsoplysninger

Vis transaktionsoplysningerne på live view-billedet.

VCA-regel

Vis VCA-reglen i live-visningen.

Aktiver Frame Extracting til højhastighedsafspilning

Når du afspiller videoen ved høj hastighed (8x hastighed og derover), kan du deaktivere denne funktion for at gøre billedet af afspilningen mere flydende, så du kan se detaljerne.

Vis målets mønster

Når den er aktiveret, kan du se målpersonens bevægelsesspor i visningsvinduet.

Overlejringsregler på optagede billeder

For den termiske enhed skal du indstille den til at vise temperaturoplysninger og oplysninger om brandkilde på de optagne billeder.

Bemærk

Når denne funktion er aktiveret, ændres det billedformat, der er konfigureret i **Systemkonfiguration** → **Livevisning og afspilning**, til JPEG og kan ikke redigeres.

Støjreduktion

Støjreduktionstilstand, som kan indstilles som **Disable**, **Self-adaptive** eller **Enable**.

4. Klik på **Gem**.

21.4 Indstil billedopbevaring

De optagne billeder, der udløses af hændelser på enhederne, kan gemmes på den pc, der kører ABUS CMS Service. Du kan indstille billedlagringsstedet manuelt her.





Trin

1. Gå ind i modulet Systemkonfiguration.
2. Klik på **Event Picture Storage**.
3. Sæt kontakten **Store Pictures in Server** til on.
Alle diske på den pc, der kører ABUS CMS-tjenesten, vises.
4. Vælg den disk, du vil gemme billederne på.
5. Klik på **Gem**.

21.5 Indstil alarmlyd

Når hændelsen udløses, kan klienten give en akustisk advarsel for at underrette sikkerhedspersonalet. Du kan indstille lyden for den akustiske advarsel i dette afsnit.

Trin

1. Åbn siden Systemkonfiguration.
2. Klik på fanen **Alarm Sound** (Alarmlyd) for at åbne siden Alarm Sound Settings (Indstillinger for alarmlyd).
3. Valgfrit: Klik på  og vælg lydfile fra den lokale sti til forskellige begivenheder.
4. Valgfri: Tilføj tilpasset alarmlyd.
 - 1) Klik på **Tilføj** for at tilføje en tilpasset alarmlyd.
 - 2) Dobbeltklik på feltet **Type** for at tilpasse navnet på alarmlyden som ønsket.
 - 3) Klik på , og vælg lydfile fra den lokale sti til forskellige alarmer.
5. Valgfrit: Klik på  for at få en test af lydfilen.
6. Valgfrit: Klik på  i kolonnen Operation for at slette den brugerdefinerede lyd.
7. Klik på **Gem**.

Bemærk

Lydfilens format kan kun være WAV.

21.6 Indstil parametre for adgangskontrol og videointercom

Du kan konfigurere parametrene for adgangskontrol og videointercom efter de faktiske behov.

Trin

1. Åbn siden Systemkonfiguration.
2. Klik på fanen **Adgangskontrol og videointercom**.
3. Indtast de nødvendige oplysninger.

Ringetone

Klik og vælg lydfilen fra den lokale sti som ringetone til indendørsstationen. Du kan også klikke for at få en test af lydfilen.

Max. Ring Varighed

Angiv det antal sekunder, som ringetonen højst må vare. Den maksimale ringetid kan indstilles fra 15s til 60s.

Max. Talevarighed med indendørs station

Angiv de sekunder, som opkaldet med indendørsstationen højst må vare. Den maksimale taletid mellem indendørsstationen og klienten kan indstilles fra 120s til 600s.

Max. Talevarighed med dørstation

Angiv de sekunder, som opkaldet med dørstationen højst må vare. Den maksimale taletid mellem dørstationen og klienten kan indstilles fra 90s til 120s.

Max. Talevarighed med adgangskontrolenhed


Angiv de sekunder, som opkaldet med adgangskontrolenheden højst må vare. Den maksimale taletid mellem adgangskontrolenheden og klienten kan indstilles fra 90s til 120s.

4. Klik på **Gem**.

21.7 Indstil sti til lagring af filer

Videooptagelserne (manuelt optaget under livevisning og udklippet under afspilning) og de optagne billeder gemmes på den lokale pc. Stien til lagring af disse filer kan indstilles.

Trin

1. Åbn siden Systemkonfiguration.
2. Klik på fanen **File** for at åbne siden File Saving Path Settings.
3. Klik på  , og vælg en lokal sti til filerne.
4. Klik på **Gem**.

21.8 Indstil ikoner, der vises på værktøjslinjen

Ikonerne og rækkefølgen på værktøjslinjen i live-visningen og afspilningsvinduet kan tilpasses. Du









kan indstille, hvilke ikoner der skal vises, og rækkefølgen af ikonerne.

Udfør følgende opgave, når du har brug for at indstille ikoner, der vises på værktøjslinjen.







Trin

1. Gå ind i modulet Systemkonfiguration.
2. Klik på fanen **Værktøjslinje** for at åbne siden Værktøjslinjeindstillinger.
3. Sæt kontakten **Enable Screen Toolbar Display** til ON for at aktivere visning af værktøjslinjen i live view- og afspilningsvinduet.
4. Klik på det ønskede ikon, der skal vises på værktøjslinjen.
5. Valgfrit: Træk ikonet for at indstille ikonrækkefølgen, når det vises på værktøjslinjen.

Tabel 21-1 Ikoner på Live View-værktøjslinjen

	Stop Live View	Stop livevisningen i displayvinduet.
	Indfangning	Optag billedet i live view-processen. Det optagne billede gemmes på pc'en.
	Rekord	Start manuel optagelse. Videofilen gemmes på pc'en.
	PTZ-styring	Start PTZ-tilstand for speed dome. Klik og træk i visningen for at udføre PTZ-kontrol.
	To-vejs lyd	Start tovejslyden med enheden i live-visning.
	Digital zoom	Aktivér den digitale zoomfunktion. Klik igen for at deaktivere funktionen.
	Øjeblikkelig afspilning	Skift til øjeblikkelig afspilning.
	Fjernkonfiguration	Åbn fjernkonfigurationssiden for kameraet i livevisning.

Tabel 21-2 Ikoner på værktøjslinjen til afspilning

	Indfangning	Optag billedet i live view-processen. Det optagne billede gemmes på pc'en.
	Rekord	Start manuel optagelse. Videofilen gemmes på pc'en.
	Digital zoom	Aktivér den digitale zoomfunktion. Klik igen for at deaktivere funktionen.
	Download	Download kameraets videofiler, og videofilerne gemmes på pc'en.
	VCA-afspilning	Indstil VCA-reglerne. Se VCA-afspilning for flere detaljer.
	Tag-kontrol	Tilføj standard- eller brugerdefineret tag til videofilerne for at markere det vigtige videopunkt. Du kan også redigere tagget.

6. Klik på **Gem**.

21.9 Indstil genveje til tastatur og joystick

Tastaturet kan tilsluttes klienten og bruges til at styre PTZ-kameraerne. Du kan indstille genveje til tastatur og joystick for at få hurtig og bekvem adgang til de mest anvendte handlinger.

Udfør denne opgave, når du har brug for at indstille tastatur- og joystickgenveje.

Trin

Bemærk

Denne konfigurationsside vises, når du har aktiveret tastatur og joystick i Generelle indstillinger. For detaljer, se [***Indstil generelle parametre***](#).

1. Gå ind i modulet Systemkonfiguration.
2. Klik på **Keyboard and Joystick** for at vise området Keyboard and Joystick Shortcut Settings.
3. Vælg COM-porten fra rullelisten for tastatur, hvis tastaturet er tilsluttet den pc, der er installeret med klienten.

Bemærk

Du kan gå ind i pc'ens Device Manger for at kontrollere den COM-port, som tastaturet er forbundet til.

4. Indstil genveje til tastatur og joystick.
 - 1) Vælg et bestemt funktionsnavn i kolonnen Funktion.
 - 2) Dobbeltklik på elementfeltet under kolonnen PC Keyboard, USB Joystick eller USB Keyboard.
 - 3) Vælg den sammensatte tasts funktion eller nummer fra rullelisten for at indstille den som genvej til funktionen på tastaturet eller USB-joysticket.
5. Klik på **Gem**.

Eksempel

Hvis du indstiller **Home**, **1** og **F1** som genveje til pc-tastaturet, USB-joysticket og USB-tastaturet for funktionen **Fokus (+)**, kan du trykke på Home-tasten på pc-tastaturet, styre joysticket i retning 1 eller trykke på F1-tasten på USB-tastaturet for at zoome ind.

21.10 Indstil e-mail-parametre

Når en begivenhed udløses, vil klienten **sende en e-mail** til modtagerne som notifikation, hvis du kan indstille **Send** e-mail som linkhandling for denne begivenhed. Du skal indstille e-

mailindstillingerne og angive målmodtagere i dette afsnit.

Trin

1. Gå ind i modulet Systemkonfiguration.
2. Klik på fanen **E-mail** for at åbne grænsefladen E-mail-indstillinger.
3. Indtast de nødvendige oplysninger.

SMTP-server

SMTP-serverens IP-adresse eller værtsnavn (f.eks. smtp.263xmail.com)

Krypteringstype

Du kan markere radioen for at vælge **Ikke-krypteret**, **SSL** eller **STARTTLS**.

Havn

Indtast den kommunikationsport, der bruges til SMTP. Porten er 25 som standard.

Afsenderadresse

Afsenderens e-mailadresse.

Sikkerhedscertifikat (valgfrit)

Hvis din e-mailserver kræver godkendelse, skal du markere dette afkrydsningsfelt for at bruge godkendelse til at logge ind på serveren og indtaste login-brugernavn og adgangskode til din e-mailkonto.

Brugernavn

Indtast brugernavnet på afsenderens e-mailadresse, hvis **Server Authentication** er markeret.

Adgangskode

Indtast adgangskoden til afsenderens e-mailadresse, hvis **Server Authentication** er markeret.

Modtager 1 til 3

Indtast modtagerens e-mailadresse. Der kan indstilles op til 3 modtagere.

4. Valgfrit: Klik på **Send test e-mail** for at sende en e-mail til modtageren til test.
5. Klik på **Gem**.

21.11 Administrer sikkerhedsgodkendelse

Af hensyn til datasikkerheden skal sikkerhedscertifikatet for klienter og tilføjede servere være det samme. Du kan indstille, at verificeringscertifikatet er påkrævet eller ej, når du aktiverer transmissionskryptering ved hjælp af TLS-protokollen (Transport Layer Security).

Før du tilføjer en server til klienten, skal du eksportere servicecertifikatet fra klienttjenesten og importere det til serveren. Hvis flere klienter bruger den samme server, skal du sørge for, at

klienternes og serverens sikkerhedscertifikater er de samme.

21.11.1 Eksportcertifikat fra Service Management

Du kan eksportere sikkerhedscertifikatet fra den aktuelle klienttjeneste og importere den eksporterede certifikatfil til andre klienter.

Trin

1. Gå ind i Service Management.
2. Klik på **Eksporter** for at gemme certifikatfilen på den lokale pc.

Bemærk

Certifikatfilen er i XML-format.

Hvad du skal gøre nu

Når du har eksporteret certifikatet, kan du kopiere det til den pc, der er installeret med klienten, og importere det til andre klienter.

21.11.2 Importer certifikat til klient

Hvis der er flere klienter, der har adgang til den samme steam media-server, skal du importere det samme certifikat til klienterne og serveren.

Før du går i gang

Sørg for, at du har eksporteret sikkerhedscertifikatet fra en af klienttjenesterne.

Bemærk

For detaljer, se [***Eksportcertifikat fra Service Management.***](#)

Trin

1. Kopier certifikatfilen, der er eksporteret fra en anden klient, til den lokale pc.
2. Gå ind i modulet Systemkonfiguration.
3. Klik på fanen **Security Authentication** for at åbne grænsefladen til indstilling af sikkerhedsgodkendelse.
4. Klik på **Importer**.
5. Vælg certifikatfilen fra din lokale pc, og klik på **Åbn**.

Bemærk

Genstart klienten, så den træder i kraft.

21.11.3 Certifikatverifikation for transmissionskryptering

På siden Security Authentication kan du indstille, om enhedens certifikatbekræftelse er påkrævet eller ej for transmissionskryptering.

Klik på **System Configuration (Systemkonfiguration)** → **Security Authentication (Sikkerhedsgodkendelse)** for at åbne grænsefladen til sikkerhedsgodkendelse. Vælg Bekræft certifikat som **Ja** eller **Nej**.

Ja


Du skal placere enhedscertifikatet i den designede mappe, hvis du aktiverer transmissionskryptering, når du tilføjer en enhed. Enheden vil blive tilføjet med transmissionskryptering, og certifikatet vil blive verificeret, hvilket forbedrer sikkerhedsniveauet.

Nej, det er det ikke

Enheds-certifikatet er ikke påkrævet, hvis du aktiverer transmissionskryptering, når du tilføjer en enhed. Og enheden vil blive tilføjet med transmissionskryptering.

Kapitel 22 Drift og vedligeholdelse

Du kan udføre vedligeholdelsesoperationer i menuen for at sikre en jævn og bekvem brug af klienten.

Klik på  → **File** → **System** → **Tool** i øverste højre hjørne af klienten, og udfør følgende handlinger.

Åbn logfil

Du kan åbne en logfil, der er gemt på din lokale pc, eller logfiler fra klienten.

Import/eksport af konfigurationsfil

Du kan importere konfigurationsfiler fra den lokale pc til klienten, hvis det er nødvendigt, og omvendt.

Automatisk sikkerhedskopiering

Vælg dag og tidspunkt for sikkerhedskopiering af konfigurationsfiler og data i databasen, eller gendan de sikkerhedskopierede data.

Udsendelse

Tjek en eller flere enheder for at aktivere broadcast-funktionen på enhederne.

Kontrol af batch-viskere

Tænd/sluk viskeren i batch.

1 VS 1 Sammenligning af ansigter

Vælg to ansigtsbilleder fra den lokale pc til sammenligning. Ligheden mellem de to billeder vil blive

vist.

Bemærk

Denne funktion kan bruges til identitetsbekræftelse og skal understøttes af DeepinMind-enheden.

Batch-tidssynkronisering

Synkroniser udvalgte enheders tid med din pc's tid.

Beskedkø

Når du har konfigureret e-mail-koblingen, vises den eller de udløste begivenheder her. Vælg en begivenhed, og annullér afsendelsen af en e-mail til modtageren.

A. Beskrivelser af brugerdefinerede Wiegand-regler

Tag Wiegand 44 som eksempel, indstillingsværdierne i fanen Custom Wiegand er som følger:

Brugerdefineret Wiegand-navn	Wiegand 44				
Total længde	44				
Transformationsregel (decimalciffer)	byFormatRule[4]=[1][4][0][0]				
Paritetstilstand	XOR Paritet				
Ulige paritet Startbit		Længde			
Startbit med lige paritet		Længde			
XOR Paritet Start Bit	0	Længde pr. gruppe	4	Total længde	40
Kort-ID Start Bit	0	Længde	32	Decimalciffer	10
Site Code Start Bit		Længde		Decimalciffer	
OEM-startbit		Længde		Decimalciffer	
Producentkode Startbit	32	Længde	8	Decimalciffer	3

Wiegand-data

Wiegand-data = gyldige data + paritetsdata

Total længde

Wiegand-datalængde.

Regel for transport

4 byte. Vis kombinationstyperne af gyldige data. Eksemplet viser kombinationen af kort-ID og producentkode. De gyldige data kan være en enkelt regel eller en kombination af flere regler.

Paritetstilstand

Gyldig paritet for Wiegand-data. Du kan vælge enten ulige paritet eller lige paritet.

Ulige paritet Startbit og længde

Hvis du vælger Odd Parity, er disse elementer tilgængelige. Hvis startbiten for ulige paritet er 1, og længden er 12, vil systemet starte beregningen af ulige paritet fra bit 1. Det vil beregne 12 bits. Resultatet vil være i bit 0. (Bit 0 er den første bit.)

Startbit med lige paritet og længde

Hvis du vælger Even Parity, er disse elementer tilgængelige. Hvis startbiten for lige paritet er 12, og længden er 12, vil systemet starte beregningen af lige paritet fra bit 12. Det vil beregne 12 bits. Resultatet vil være i den sidste bit.

XOR-paritetsstartbit, længde pr. gruppe og samlet længde

Hvis du vælger XOR Parity, er disse elementer tilgængelige. Afhængigt af tabellen ovenfor er startbiten 0, længden pr. gruppe er 4, og den samlede længde er 40. Det betyder, at systemet beregner fra bit 0, beregner hver 4. bit og beregner 40 bits i alt (10 grupper i alt). Resultatet vil være i de sidste 4 bit. (Resultatlængden er den samme som længden pr. gruppe).

Kort-ID startbit, længde og decimalciffer

Hvis du bruger transformationsreglen, er disse elementer tilgængelige. Afhængigt af tabellen ovenfor er kort-ID'ets startbit 0, længden er 32, og decimalcifret er 10. Det betyder, at fra bit 0 er der 32 bits, der repræsenterer kort-ID'et. (Længden her er beregnet efter bit.) Og decimalcifrets længde er 10 bit.

Sitekode Startbit, længde og decimalciffer

Hvis du bruger transformationsreglen, er disse elementer tilgængelige. For detaljerede oplysninger, se forklaringen af kort-ID'et.

OEM startbit, længde og decimalciffer

Hvis du bruger transformationsreglen, er disse elementer tilgængelige. For detaljerede oplysninger, se forklaringen af kort-ID'et.

Producentkode Startbit, længde og decimalciffer

Hvis du bruger transformationsreglen, er disse elementer tilgængelige. Ifølge tabellen ovenfor er producentkodens startbit 32, længden er 8, og decimaltallet er 3. Det betyder, at der fra bit 32 er 8 bit producentkode. (Længden her er beregnet efter bit.) Og decimallængden er 3.

D. Fejlkode

Kode	Fejl Navn	Beskrivelse
ABUS CMS		
317	Ingen videoer.	Det vil blive spurgt, når brugeren ikke har tilladelse til at afspille.
HCNetSDK.dll		
1	Ugyldigt brugernavn eller password.	
2	Ingen tilladelse.	Brugeren på enheden har ikke tilstrækkelig tilladelse.
4	Ugyldigt kanalnummer.	Det vil blive vist i live-visningen på fjernbetjeningen.
5	Der kan ikke tilsluttes flere enheder.	
7	Det lykkedes ikke at forbinde enheden.	
23	Understøttes ikke.	
29	Operationen mislykkedes.	
43	Ingen buffer.	Du bliver bedt om det, når du tilføjer en enhed, og enhedsporten er optaget af en webserver.
55	Ugyldig IP-adresse.	
56	Ugyldig MAC-adresse.	
91	Kanalen understøtter ikke operationen.	Den vil blive bedt om det, hvis det ikke lykkes at hente understrømmen.
96	Enheden er ikke registreret i DDNS.	
153	Brugeren er låst.	
250	Enheden er ikke aktiveret.	
404	Channel No. fejl, eller enheden understøtter ikke substreamen.	Den vil blive spurgt, hvis det ikke lykkes at hente understrømmen, eller hvis understrømmen ikke findes.
424	Kunne ikke modtage data for	Du bliver bedt om det, når du tilføjer livevisning til

Kode	Fejl Navn	Beskrivelse
	RTSP SETUP.	softwaren DVS via eksternt netværk.
800	Der kan ikke bruges mere båndbredde.	
Playctrl.dll		
2		Streamen er ikke en video- og lydstream.
6		Afspilningsvinduet bliver sort, når man indfører H.265 i 64-bit-operativsystemet.

