HikCentral Profissional V2.6.1

Especificação AE

Conteúdo

Capítulo 1 Padrão de Escrita

Divisão 28 - Segurança Eletrônica e Proteção
Seção 28 01 00 - Operação e Manutenção de Segurança Eletrônica
Seção 28 01 30 - Operação e Manutenção de Detecção, Alarme e Monitoramento de Segurança

Capítulo 2 Geral

2.1 Resumo dos Requisitos

Plataforma Profissional HikCentral

O System Management Service (SYS) fornece serviço de autenticação unificado para conexão com clientes e servidores.

Requisitos relacionados

1. Seção 27 20 00 - Comunicações de dados
2. Seção 28 05 00 - Resultados comuns de trabalho para segurança eletrônica e proteção
3. Seção 28 05 19 - Dispositivos de armazenamento para segurança eletrônica e proteção
4. Seção 28 05 19.11 - Gravadores de vídeo digitais
5. Seção 28 05 19.13 - Gravadores de vídeo digitais híbridos
6. Seção 28 05 19.15 - Gravadores de vídeo em rede
7. Seção 28 06 20 - Horários de Segurança por Vídeo
8. Seção 28 21 00 - Câmeras de segurança
9. Seção 28 21 13 - Câmeras IP
10. Seção 28 27 00 - Sensores de segurança de vídeo
11. Seção 28 33 00 - Segurança de Vídeo - Monitoramento e Controle de Segurança
12. Seção 28 51 19.15 - Paredes Inteligentes

2.2 Referências

Abreviações

1. AD - Diretório Ativo
2. AGC - Controle Automático de Ganho
3. AWB - Balanço de Branco Automático
4. BLC - Compensação de luz de fundo
5. CIF - Formato Intermediário Comum
6. CD - Dispositivo cliente
7. DDNS - Servidor de Nomes de Domínio Dinâmico
8. DHCP - Protocolo de configuração dinâmica de host
9. DNR - Redução de Ruído Digital
10. DNS - Servidor de Nomes de Domínio
11. DSCP - Ponto de Código de Serviços Diferenciados
12. DVR - Gravador de Vídeo Digital
13. FPS - quadros por segundo
14. FTP - Protocolo de Transferência de Arquivos
15. GIS - Sistema de Informação Geográfica
16. GUI - Interface Gráfica do Usuário

17. HLC - Alta compressão de luz
18. HTTP - Protocolo de Transferência de Hipertexto
19. HTTPS - HTTP seguro
20. SAN híbrida - Rede de área de armazenamento híbrida
21. ICMP - Protocolo de mensagens de controle da Internet
22. IGMP - Protocolo de Gerenciamento de Grupos da Internet
23. IP - Protocolo de Internet
24. JPEG - Grupo Conjunto de Peritos Fotográficos
25. LPR - Reconhecimento de Placas de Veículos
26. MicroSD - Cartão de memória flash digital seguro miniaturizado removível
27. MPEG - Grupo de especialistas em imagens em movimento
28. MWB - Balanço de Branco Manual
29. NAS - Armazenamento conectado à rede
30. NIC - Controlador de Interface de Rede
31. NTP - Protocolo de Tempo de Rede sobre Ethernet
32. NVR - Gravador de Vídeo em rede
33. PIR - Sensor infravermelho passivo
34. PoE - Energia sobre Ethernet
35. POS - Ponto de Venda
36. PPPoE - Protocolo ponto a ponto sobre Ethernet
37. PTZ - Panorâmica, Inclinação e Zoom
38. QoS - Qualidade de Serviço
39. ROI - Região de Interesse
40. RSM - Gerenciamento de Site Remoto
41. RTP - Protocolo de Transporte em Tempo Real
42. RTSP - Protocolo de streaming em tempo real
43. Cartão SD - Cartão de memória flash Secure Digital
44. SMTP - Protocolo Simples de Transferência de Correio
45. TCP - Protocolo de Controle de Transmissão
46. UDP - Protocolo de Datagrama do Usuário
47. UPnP - Plug and Play universal
48. UVSS - Sistema de Vigilância Subterrânea
49. VCA - Análise de Conteúdo de Vídeo
50. VMS - Sistema de gerenciamento de vídeo
51. WB - Balanço de Branco
52. WDR - Ampla Faixa Dinâmica
53. SYS - Serviço de Gestão de Sistemas

2.3 Certificações, Padrões e Classificações

Padrões de Referência

1. Padrão de Rede:
   Padrões IEEE – 802.3 Ethernet

2. Compressão de vídeo:
   Padrão ITU-T H.264 e padrão ISO/IEC MPEG-4 AVC (formalmente, ISO/IEC 14496-10 – MPEG-4 Parte 10, Codificação de Vídeo Avançada), formatos de codificação H.264+, H.265 e H.265+

2.4 Submissões

Dados do Produto
1. Folhas de dados físicas (físicas) ou eletrônicas (software) do fabricante
2. Manuais de instalação e operação para todo e qualquer equipamento necessário para um SYS (Sistema de Gerenciamento de Sistema)
3. Documentação de garantia do fabricante

2.5 Qualificações

Requisitos
1. Este produto deve ser fabricado por uma empresa cujos sistemas de qualidade estejam em conformidade direta com os protocolos ISO-9001.
2. Todas as instalações, integrações, testes, programações, comissionamentos de sistemas e trabalhos relacionados devem ser realizados por instaladores treinados, autorizados e certificados pelo fabricante.

2.6 Entrega, Armazenamento e Manuseio

Em geral
O produto deverá ser entregue de acordo com as recomendações do fabricante.

2.7 Acordos de Licenciamento e Suporte

Não requer Acordos de Suporte de Software com o fabricante.

2.8 Suporte técnico (PERMANECE O MESMO, A MENOS QUE OS TERMOS DE GARANTIA TENHAM SIDO ALTERADOS)

Apoiar
O suporte técnico será baseado em cada área.

Capítulo 3 Produto

3.1 Fabricante

Fabricante:
No.555 Qianmo Road, distrito de Binjiang, Hangzhou 310051, China
Telefone: +86-0571-8807-5998
Site: www.hikvision.com

3.2 Descrição do Serviço

Serviço de Gerenciamento de Sistema Profissional HikCentral

Capacidade máxima do SYS para gerenciamento de dispositivos e tratamento de eventos:

1. Gerencia até 2.048 recursos, incluindo dispositivos de codificação, dispositivos de controle de acesso, dispositivos de controle de elevador, dispositivo de controle de segurança, terminal de sinalização digital e sites remotos
2. Importa até 100.000 canais de vídeo (câmera de rede ou analógico/TVI)
3. Gerencia até 64 servidores de gravação por SYS
4. Importa até 3.000 entradas/saídas de alarme, respectivamente, por SYS.

Gerenciador de serviços: um aplicativo que gerencia os seguintes serviços

1. O System Management Service é o componente principal do HikCentral Professional, fornecendo serviços de autenticação, concessão de permissão e gerenciamento. Ele autentica o acesso do Control Client, gerencia os usuários, funções, permissões e monitora dispositivos, e fornece a interface para integração de sistemas de terceiros. Ele inclui o seguinte serviço:
   a. Gateway de acesso a dispositivos de terceiros: comunicação entre o SYS e o dispositivo de terceiros
   b. Serviço de Gestão de Sistemas
      - Fornecer o serviço de autenticação unificado para conexão com clientes e servidores
      - Fornece gerenciamento centralizado para usuários, funções, permissões, dispositivos e serviços.
      - Fornece a interface de configuração para o módulo de segurança e gerenciamento.
   c. Serviço de Gestão
      - O servidor de conteúdo e gateway de sinalização do HikCentral Professional
      - Principalmente responsável pelo armazenamento de páginas estáticas e proxy reverso da configuração do dispositivo
   d. Gateway de transmissão
      - Um componente do SYS que encaminha e distribui os dados de vídeo e áudio
      - Deve suportar até 200 canais de vídeo @ 2 Mbps de entrada e 200 canais de vídeo @ 2 Mbps de saída. É usado para visualização ao vivo simultânea ou reprodução
      - Não deve ser adicionado ao cliente web como servidor de streaming

2. Serviço de Proxy de Teclado
   a. Usado com teclado de rede para acessar o serviço de proxy de teclado
   b. O teclado de rede pode ser usado para operações de visualização ao vivo na parede inteligente
3. Serviço de gerenciamento de parede inteligente
   a. Gerenciar parede inteligente para exibir vídeo decodificado na parede inteligente
   b. Responde à solicitação do Control Client e envia mensagens em tempo real para o Control Client

3.3 Capacidades de Acessibilidade e Gestão

1. Até 100 Dispositivos Clientes (CDs) simultâneos devem ser capazes de se conectar usando um cliente fino ou completo por meio de um PC baseado em Windows e 100 por meio de um aplicativo em um smartphone (iOS ou Android). Não há software cliente licenciável ou licenças de conexão de software cliente necessárias
2. Deve oferecer suporte à integração do Active Directory para gerenciamento de usuários do Control Client e aplicativos móveis (sistemas operacionais móveis iOS e Android)
3. As funções de administração e as funções de operação são executadas separadamente nos seguintes clientes: Cliente Web: Toda a administração do SYS deve ser executada usando um cliente de navegador da Web via LAN, WAN ou Internet. Nenhum software cliente é necessário para a administração do sistema
   a. Cliente de controle: todos os recursos do operador de segurança devem ser acessados por meio do cliente de controle conectado ao SYS via LAN, WAN ou Internet
   b. Cliente Móvel: Os recursos básicos do operador de segurança devem ser acessados por meio do Cliente Móvel conectado ao SYS via LAN, WAN ou Internet.
4. Deve suportar os formatos de codificação H.264, H.264+, H.265 e H.265+
5. Deve dar suporte ao gerenciamento de licenças do SUP para garantir uma atualização tranquila do HikCentral Professional
6. Deve suportar o download de logs do Service Manager
7. Deve suportar vários fusos horários e horário de verão

3.4 Rede

Acesso de Segurança

1. Deve ter uma proteção de senha integrada independente do servidor
2. O Sistema deverá possuir Autenticação de Usuário
3. Ativação Segura
   a. Um algoritmo do sistema verificará a força da senha definida pelo usuário, com base nos critérios do fabricante.
   b. O sistema deve determinar e exibir o nível de segurança da senha como “fraco”, “médio” ou “forte”.
   c. A senha deve conter no mínimo dois tipos de caracteres (letras minúsculas, letras

maiúsculas, números e caracteres especiais).
d. Somente caracteres ASCII serão permitidos.
e. O comprimento da senha deve ser de no mínimo oito caracteres.

3.5 Requisitos do PC

HikCentral Professional SYS sem RSM

PC mínimo: Intel ® Core ™ i5-12500 @3.0 GHz
RAM: 8 GB
NIC: Placa de interface de rede
GbEPlaca de vídeo: NVIDIA® GeForce® GTX
Tipo de disco rígido: SATA- 7200 RPM Enterprise Class HDD
Capacidade da unidade de disco rígido: 650 GB para o HDD onde o serviço SYS está instalado
Outro: Microsoft® Windows 8.1 (64 bits)

Para HikCentral Professional SYS com RSM

PC mínimo: Intel ® Xeon ® E-2324 @3,10 GHz
RAM: 16 GBNIC: placa de interface de rede GbE
Tipo de disco rígido: SATA- 7200 RPM Enterprise Class HDD
Capacidade da unidade de disco rígido: 650 GB para o HDD onde o SYS está instalado
Outro: Microsoft® Windows Server 2012 (R2) (64 bits)

Para Servidor de Streaming

PC mínimo: Intel ® Core ™ i5-12500 @3,00 GHz
RAM: 8 GBNIC: placa de interface de rede GbE
Tipo de disco rígido: SATA-II 7200 RPM Enterprise Class HDD
Capacidade da unidade de disco rígido: 10 GB para armazenar arquivos de log

Para o Cliente de Controle Profissional HikCentral

PC mínimo: Intel (R) Core ™ i3-12100 @ 3,30 GHz
RAM: 8 GBNIC: placa de interface de rede
GbEPlaca gráfica: Intel ® UHD Graphics 730
Tipo de disco rígido: Disco rígido SATA ou superior
Capacidade do disco rígido: 60 GB para sistema operacional e HikCentral Professional Control Client
Outro: Microsoft ® Windows 10 (64 bits)

3.6 Fluxo de Sinal

3.6.1 Entrar

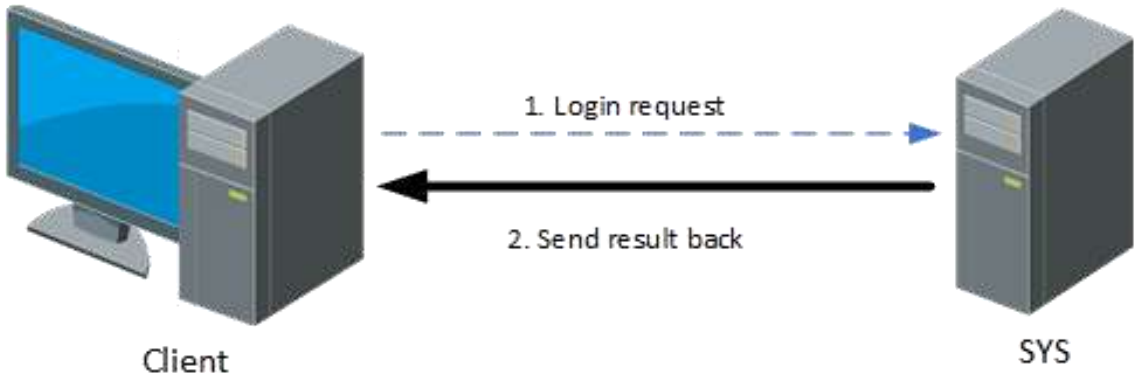


Figura 3-1 Fluxo de login

Durante o login, a sinalização será trocada entre o cliente (Web Client/Control Client/Mobile Client) e o SYS.

O processo de interação de sinalização é o seguinte:

1. Digite o nome de usuário e a senha (nome de domínio) no cliente, que serão enviados ao servidor SYS.
2. O SYS receberá as informações, verificará se o nome de usuário e a senha (nome de domínio) estão corretos e enviará o resultado ao cliente.

3.6.2 Visualização ao vivo

Visualização ao vivo para Dispositivo Conectado Diretamente

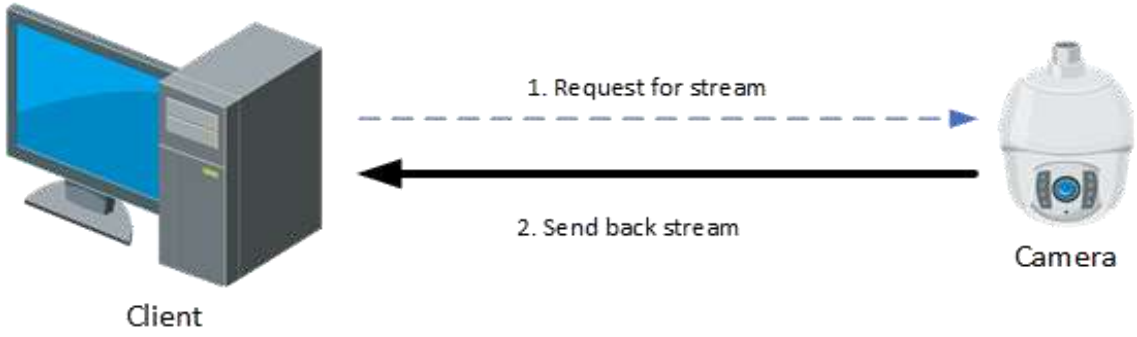


Figura 3-2 Fluxo de visualização ao vivo para dispositivo conectado diretamente

Se o SYS, os dispositivos e o cliente forem implantados na mesma rede LAN, o cliente pode obter o fluxo diretamente. O processo de sinalização é o seguinte:

1. O cliente deve enviar uma solicitação ao dispositivo para obter o fluxo.
2. O dispositivo enviará de volta o fluxo correspondente ao cliente.

Visualização ao vivo via Servidor de Streaming

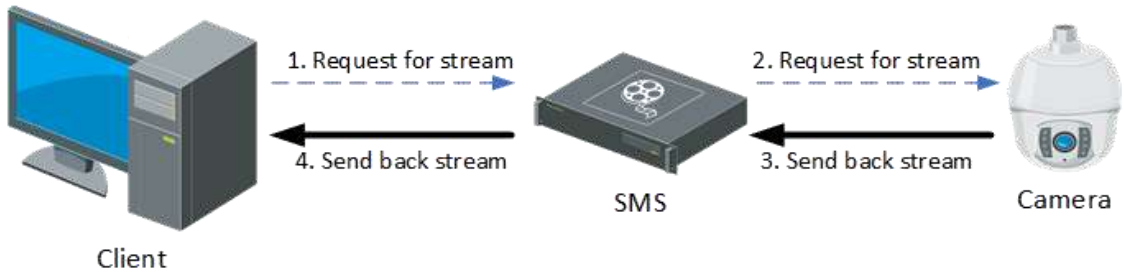


Figura 3-3 Fluxo de Visualização ao vivo via Servidor de Streaming

Nas seguintes situações o SMS (Streaming Server) deverá ser implantado:
O cliente deverá obter transmissões de dispositivos de terceiros.
Vários clientes devem solicitar o mesmo fluxo do mesmo dispositivo. Para reduzir a largura de banda para obter o fluxo, o fluxo deve ser encaminhado via SMS para resolver esse problema.
O processo de sinalização é o seguinte:

1. O cliente deverá enviar uma solicitação ao SMS para obter o fluxo.
2. O SMS encaminhará a solicitação ao dispositivo para obtenção do fluxo.
3. O dispositivo enviará de volta o fluxo correspondente ao SMS.
4. O SMS encaminhará o fluxo obtido ao cliente.

Visualização ao vivo via Servidor VSM

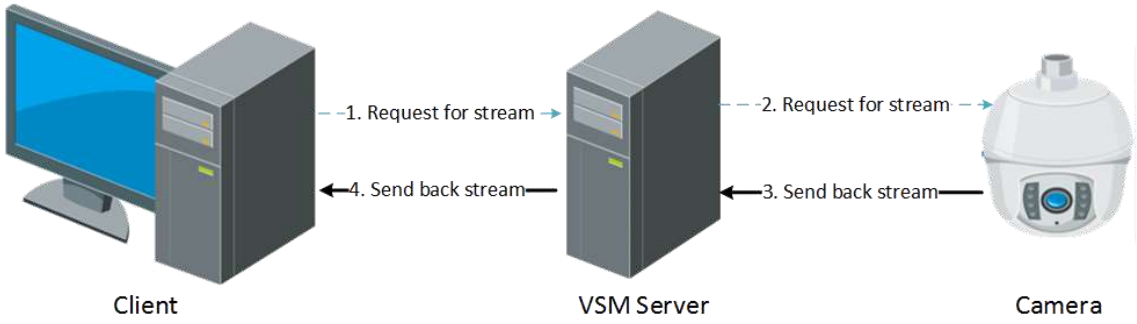


Figura 3-4 Fluxo de visualização ao vivo via Servidor VSM

O processo de sinalização é o seguinte:

1. O cliente deve enviar uma solicitação ao servidor VSM para obter o fluxo.
2. O VSM Sever encaminhará a solicitação ao dispositivo para obtenção do fluxo.
3. O dispositivo enviará de volta o fluxo correspondente ao servidor VSM.
4. O servidor VSM encaminhará o fluxo obtido para o cliente.

Controle PTZ

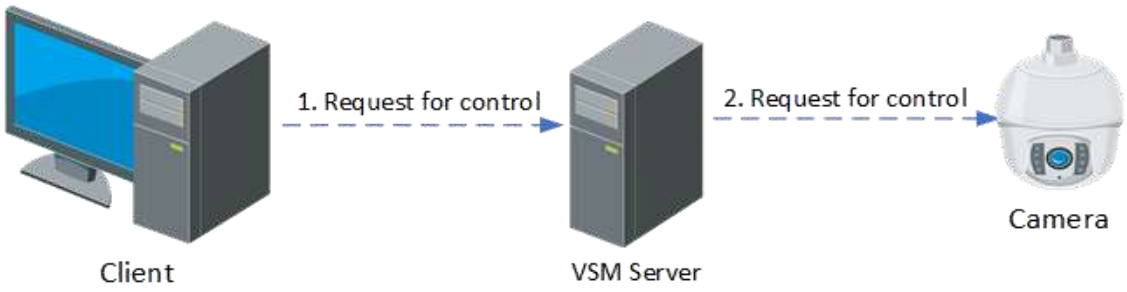


Figura 3-5 Fluxo de Controle PTZ

A plataforma controlará a câmera PTZ via SYS.
O processo de sinalização é o seguinte:

1. O cliente deverá enviar uma solicitação ao SYS para controlar a câmera PTZ.
2. O SYS encaminhará a solicitação ao dispositivo correspondente para controle PTZ.

3.6.3 Armazenamento e Reprodução de Vídeo

O armazenamento e a reprodução do dispositivo devem incluir: armazenamento de fluxo de vídeo, recuperação e reprodução de arquivos de vídeo.

Armazenamento de Vídeo em NVR/DVR

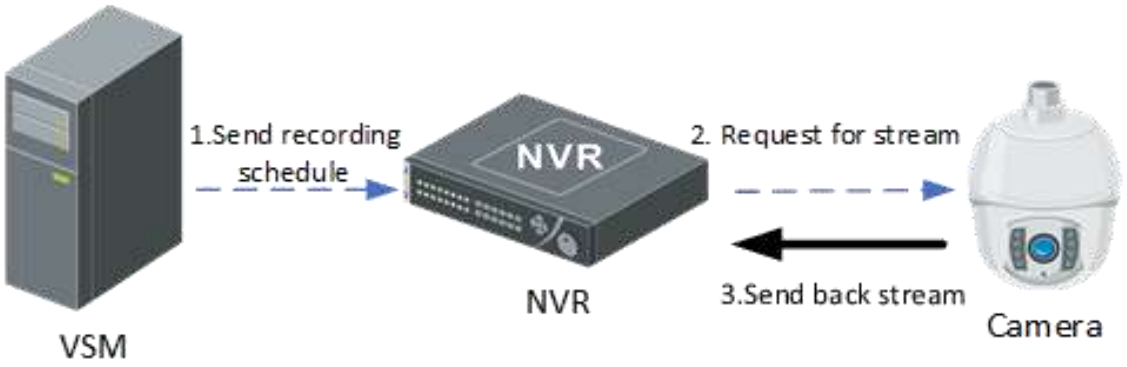


Figura 3-6 Fluxo de Armazenamento de Vídeo em NVR/DVR

Conforme mostrado na figura acima, o processo de sinalização é o seguinte:

1. O SYS enviará o cronograma de gravação (cronograma de gravação baseado em eventos e cronograma de gravação baseado em tempo) para o NVR.
2. Quando a condição de programação de gravação for atendida (dentro do segmento de tempo ou um evento for acionado), o NVR enviará uma solicitação à câmera para obter o fluxo.
3. A câmera enviará de volta o fluxo correspondente para o NVR.

Nota

Quando a gravação manual é realizada no Control Client, as etapas anteriores serão acionadas manualmente, mas não acionadas pela programação de gravação.

Armazenamento de Vídeo no Servidor de Gravação

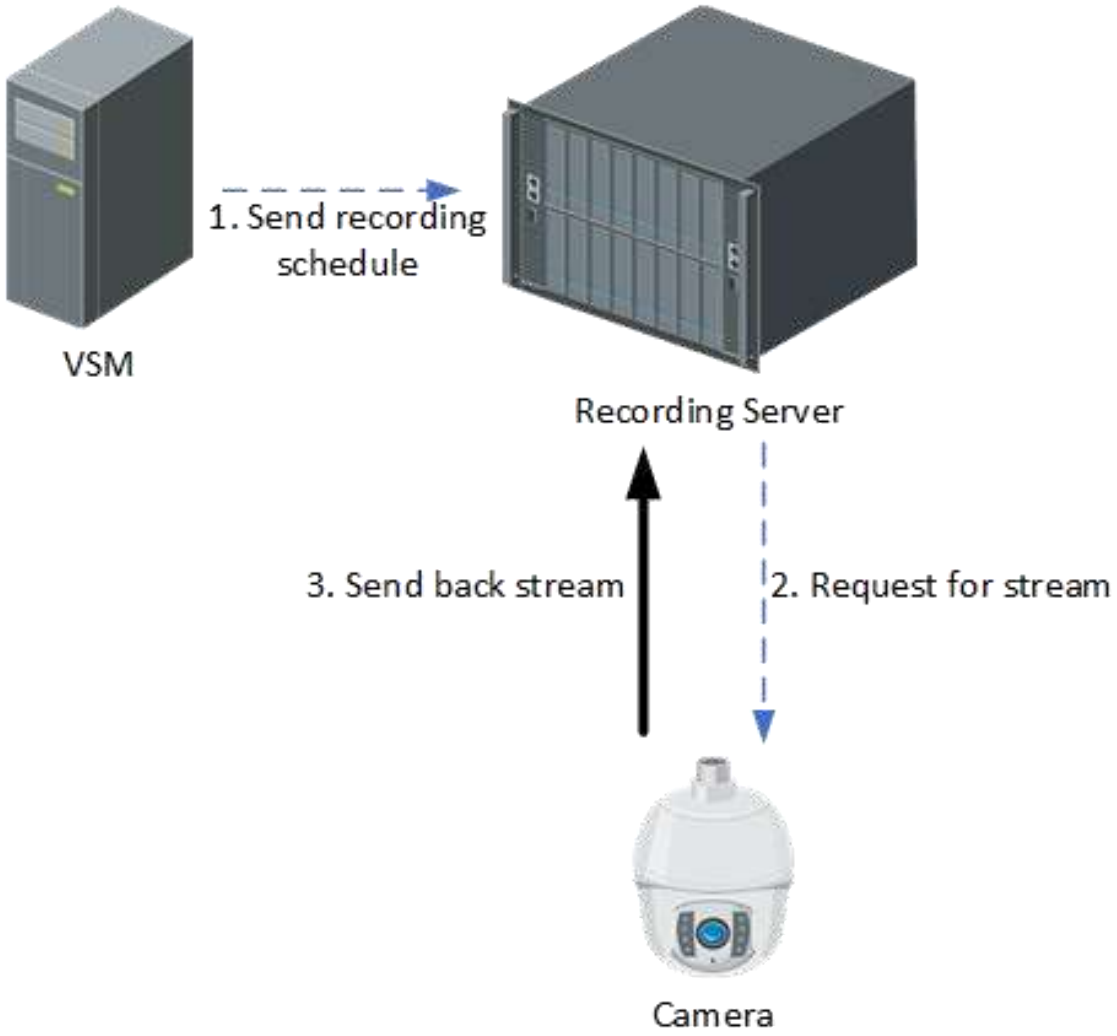


Figura 3-7 Fluxo de Armazenamento de Vídeo no Servidor de Gravação

Os Servidores de Gravação devem incluir: SAN Híbrido, armazenamento em nuvem e pStor. Se o vídeo for armazenado no servidor de gravação, o processo de sinalização é o seguinte:

1. O SYS enviará o cronograma de gravação (cronograma de gravação baseado em tempo e cronograma de gravação baseado em eventos) para o Servidor de Gravação.
2. O Servidor de Gravação enviará uma solicitação à câmera para obter o fluxo de acordo com a programação de gravação.
3. A câmera enviará de volta o fluxo correspondente ao servidor de gravação de acordo com a solicitação.

Nota

Quando a gravação manual é realizada no Control Client, as etapas anteriores serão acionadas manualmente, mas não acionadas pela programação de gravação.

Reprodução de Vídeo em NVR/DVR

Existem dois modos para reproduzir vídeo em NVR/DVR: O cliente obtém o fluxo diretamente do NVR/DVR, e o cliente obtém o fluxo do NVR/DVR via SMS. Os processos de sinalização são os seguintes:

1. Reprodução de vídeo em NVR/DVR conectado diretamente

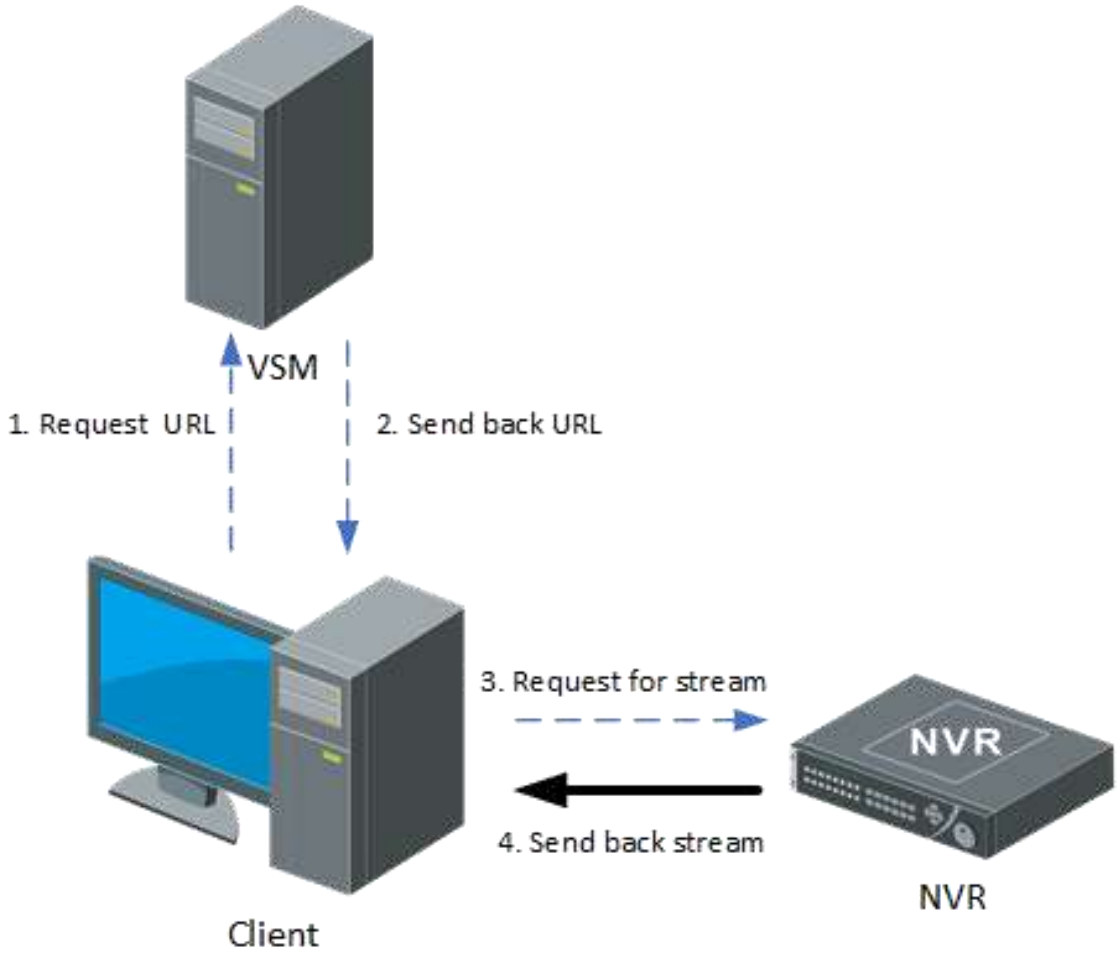


Figura 3-8 Fluxo de Reprodução de Vídeo Armazenado em NVR/DVR Conectado Diretamente

   a. O cliente deve enviar uma solicitação ao servidor SYS para obter o URL do fluxo.
   b. O SYS enviará de volta a URL do fluxo para o cliente.
   c. O cliente deverá enviar uma solicitação ao NVR para obter o fluxo.
   d. O NVR enviará de volta o fluxo correspondente ao cliente de acordo com a solicitação.

2. Reprodução de vídeo em NVR/DVR via servidor de streaming

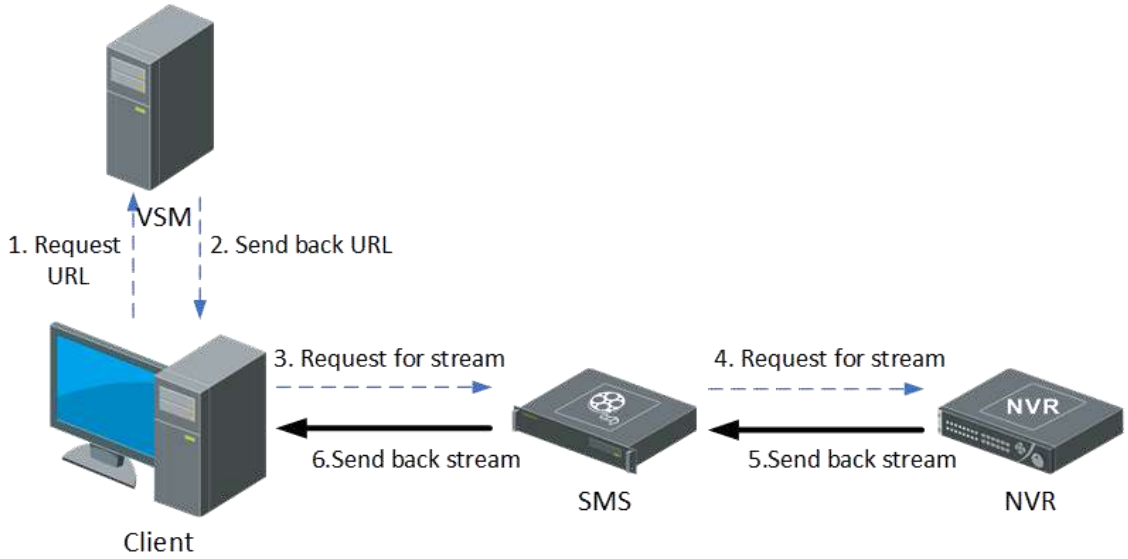


Figura 3-9 Fluxo de Reprodução de Vídeo Armazenado em NVR/DVR via Servidor de Streaming

a. O cliente deve enviar uma solicitação ao SYS para obter a URL do fluxo.
b. O SYS enviará de volta a URL do fluxo para o cliente.
c. O cliente deverá enviar uma solicitação ao SMS (Streaming Server) para obter o stream.
d. O SMS encaminhará a solicitação ao NVR para obtenção do fluxo.
e. O NVR enviará de volta o fluxo correspondente ao SMS de acordo com a solicitação.
f. O SMS encaminhará o fluxo correspondente ao cliente.

Reprodução de Vídeo no Gravador

1. Reprodução de Vídeo em Servidor de Gravação Conectado Diretamente

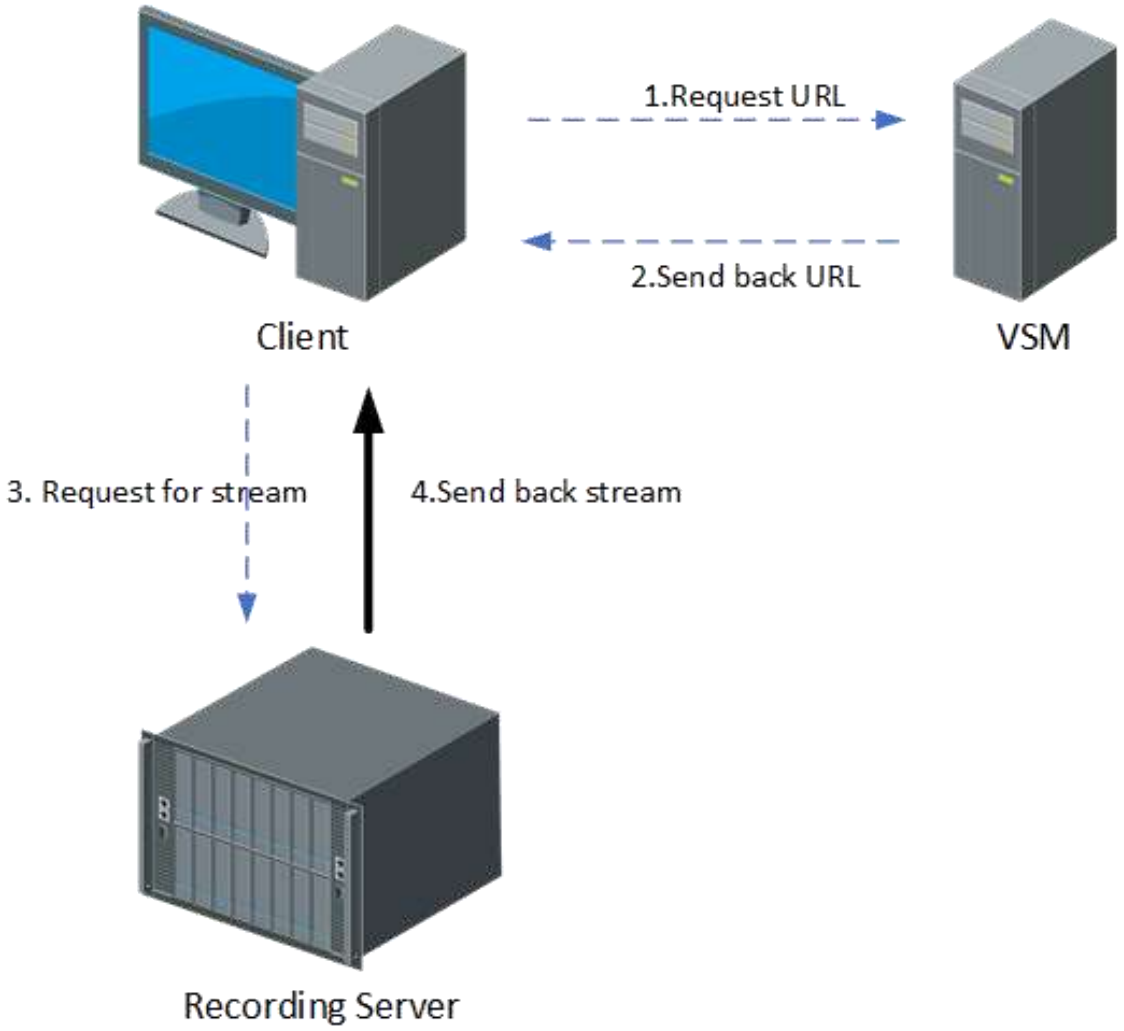


Figura 3-10 Fluxo de reprodução de vídeo armazenado em servidor de gravação conectado diretamente

a. O cliente deve enviar uma solicitação ao SYS para obter a URL do fluxo.
b. O SYS enviará de volta a URL do fluxo para o cliente.
c. O cliente deve enviar uma solicitação ao servidor de gravação para obter o fluxo.
d. O servidor de gravação enviará de volta o fluxo correspondente ao cliente de acordo com a solicitação.

2. Reprodução de vídeos no servidor de gravação via servidor de streaming

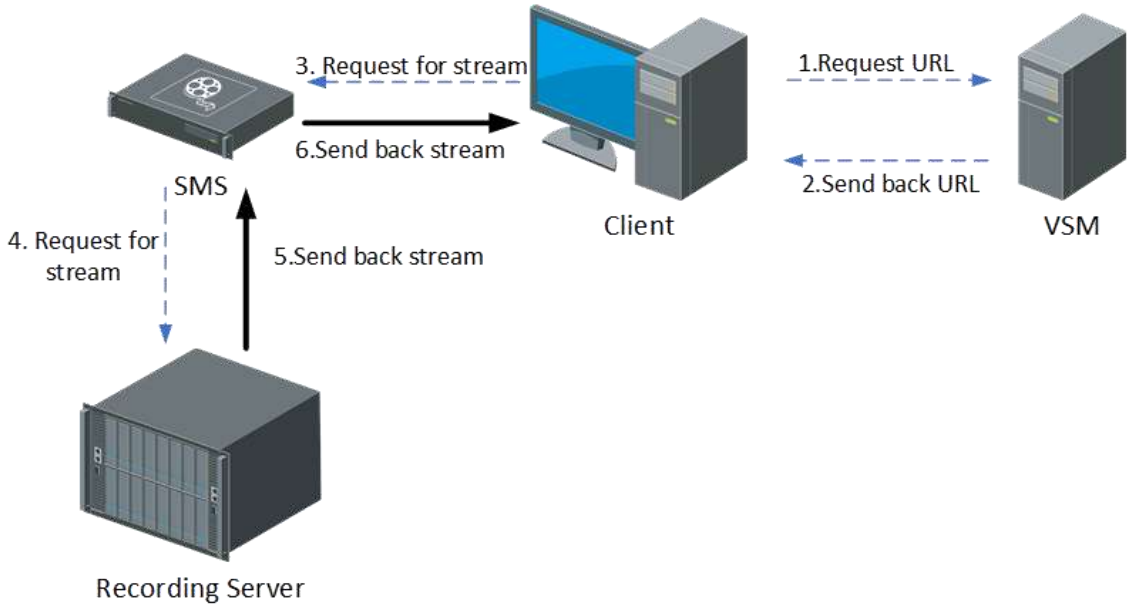


Figura 3-11 Fluxo de reprodução de vídeo armazenado no servidor de gravação via servidor de streaming

a. O cliente deve enviar uma solicitação ao SYS para obter a URL do fluxo.
b. O SYS enviará de volta a URL do fluxo para o cliente.
c. O cliente deverá enviar uma solicitação por SMS para obter o fluxo.
d. O SMS encaminhará a solicitação ao Servidor de Gravação para obtenção do fluxo.
e. O Servidor de Gravação enviará de volta o fluxo correspondente ao SMS conforme a solicitação.
f. O SMS encaminhará o fluxo correspondente ao cliente.

3.6.4 Alarme

Quando um alarme é disparado, há dois modos para o Control Client obter o fluxo relacionado ao alarme do dispositivo: Obter o fluxo via dispositivo conectado diretamente e obter o fluxo via SMS.

Os processos de sinalização são os seguintes:

Obter Fluxo Relacionado ao Alarme Diretamente

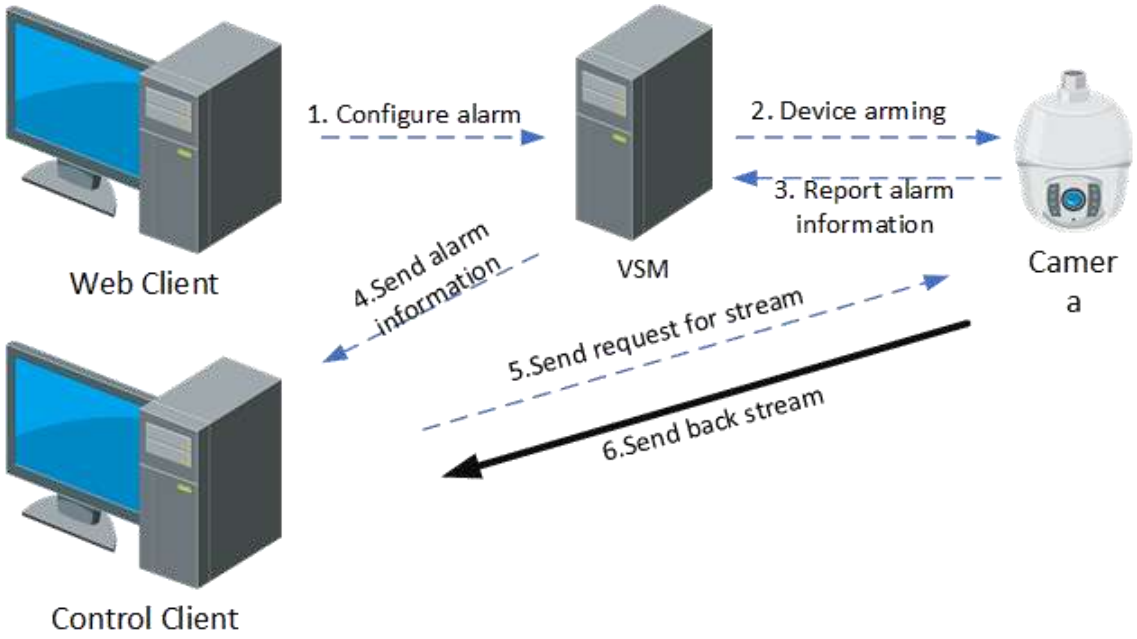


Figura 3-12 Fluxo de obtenção de fluxo relacionado ao alarme diretamente

O processo de configuração do alarme é o seguinte:

1. Configure o alarme via Web Client e a configuração do alarme será enviada para o SYS.
2. O dispositivo deve ser armado pelo SYS de acordo com o cronograma de armamento.

O processo de reporte de um alarme é o seguinte:

1. O dispositivo deve analisar o fluxo obtido. Se um alarme for disparado, o dispositivo deve reportar o alarme ao SYS.
2. O SYS enviará as informações de alarme para o Control Client.
3. Se a vinculação da visualização ao vivo para o alarme estiver configurada, o Control Client enviará uma solicitação ao dispositivo para obter o fluxo.
4. O dispositivo enviará de volta o fluxo correspondente ao Cliente de Controle de acordo com a solicitação.

Obter Fluxo Relacionado ao Alarme por meio do Servidor de Streaming

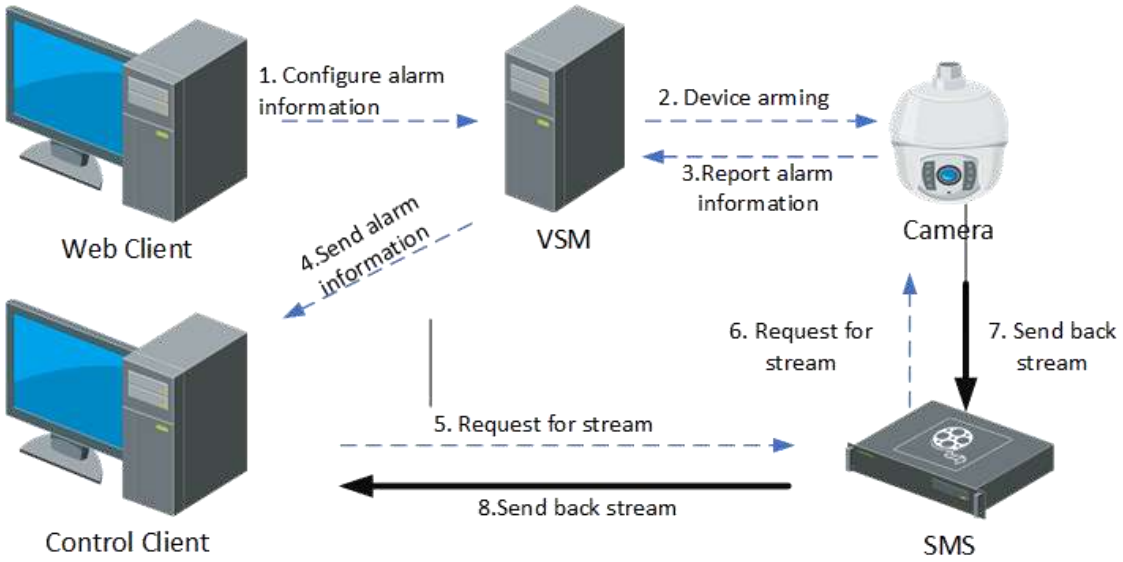


Figura 3-13 Fluxo de obtenção de fluxo relacionado a alarme por meio do servidor de streaming

O processo de configuração do alarme é o seguinte:

1. Configure o alarme via Web Client, e a configuração do alarme será enviada para o SYS.
2. O dispositivo deve ser armado pelo SYS de acordo com o cronograma de armamento.

O processo de reporte de um alarme é o seguinte:

1. O dispositivo deve analisar o fluxo obtido. Se um alarme for disparado, o dispositivo deve reportar um alarme ao SYS.
2. O SYS enviará as informações de alarme para o Control Client.
3. Se a vinculação de visualização ao vivo ou reprodução para o alarme estiver configurada, o Control Client enviará uma solicitação ao SMS para obter o fluxo.
4. O SMS encaminhará a solicitação para a câmera obter o stream.
5. A câmera enviará de volta o fluxo correspondente ao SMS de acordo com a solicitação.
6. O SMS encaminhará o fluxo para o Cliente de Controle.

3.6.5 Parede Inteligente

Exibir Vídeo no Smart Wall

1. Exibir vídeo do dispositivo conectado diretamente na parede inteligente

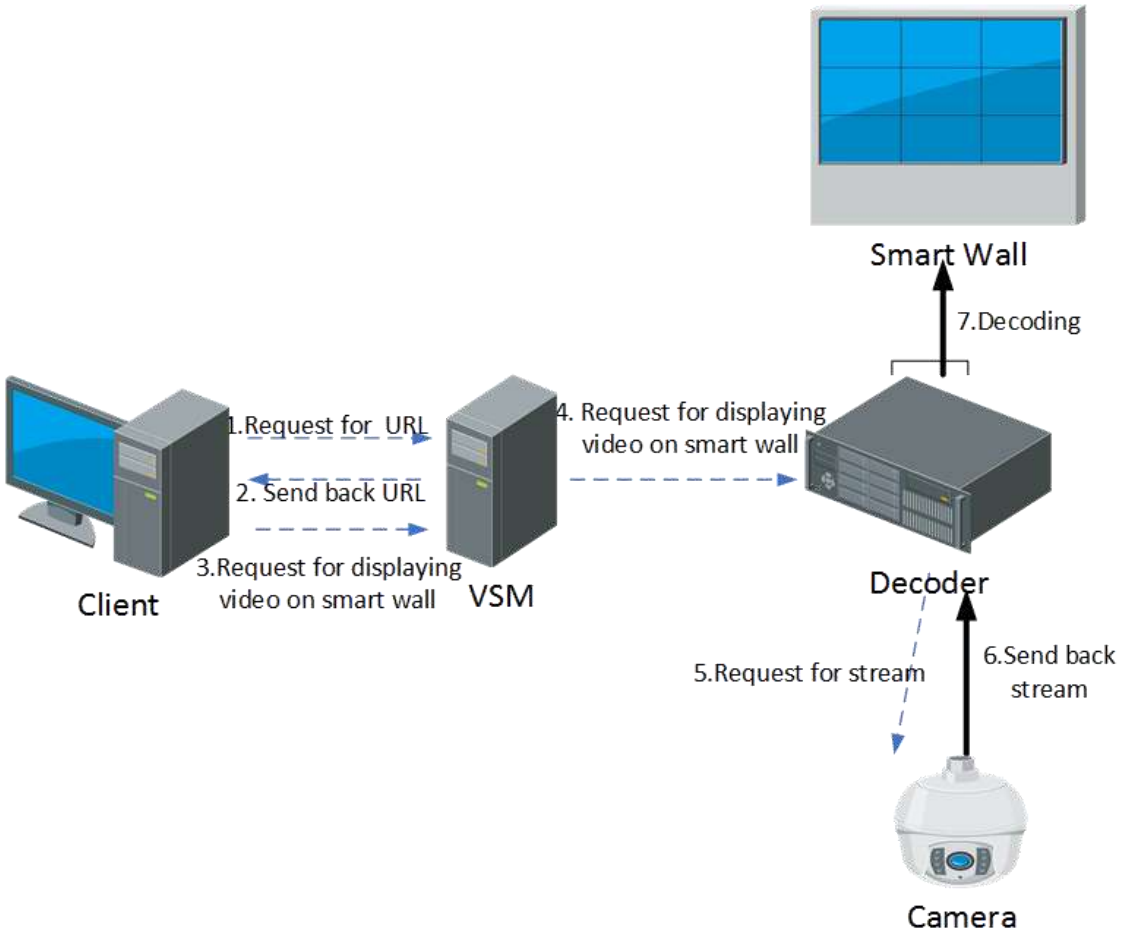


Figura 3-14 Fluxo de exibição de vídeo de dispositivo conectado diretamente no Smart Wall

Quando o decodificador obtém o fluxo diretamente do dispositivo, o processo de sinalização é o seguinte:

a. O Smart Wall Client enviará uma solicitação ao SYS para obter as informações de URL (incluindo as informações do Smart Wall e do dispositivo).
b. O SYS enviará de volta as informações de URL para o Smart Wall Client.
c. O Smart Wall Client enviará uma solicitação ao SYS para exibir o vídeo no smart wall.
d. O SYS encaminhará a solicitação ao decodificador para exibir o vídeo no smart wall.
e. O decodificador enviará uma solicitação ao dispositivo para obter o fluxo.
f. O dispositivo enviará de volta o fluxo correspondente ao decodificador.
g. O decodificador decodificará o fluxo obtido e exibirá o vídeo na parede inteligente.

2. Exibir vídeo no Smart Wall via servidor de streaming

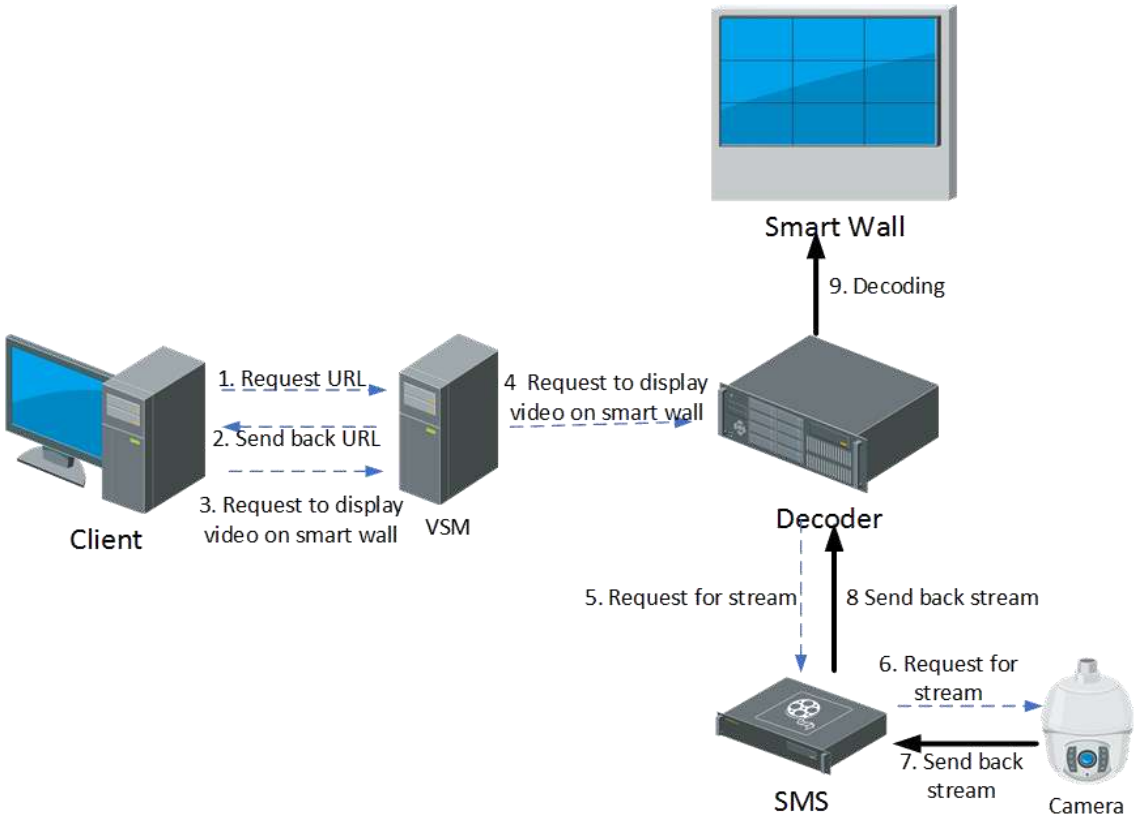


Figura 3-15 Fluxo de exibição de vídeo no Smart Wall via servidor de streaming

Se o decodificador obtiver o fluxo via SMS, o processo de sinalização será o seguinte:

a. O Smart Wall Client enviará uma solicitação ao SYS para obter as informações de URL (incluindo as informações do Smart Wall e do dispositivo).
b. O SYS enviará de volta as informações de URL para o Smart Wall Client.
c. O Smart Wall Client enviará uma solicitação ao SYS para exibir o vídeo no smart wall.
d. O SYS encaminhará a solicitação ao decodificador para exibir o vídeo no smart wall.
e. O decodificador enviará uma solicitação ao SMS (Streaming Server) para obter o fluxo.
f. O SMS encaminhará a solicitação ao dispositivo para obtenção do fluxo.
g. O dispositivo enviará de volta o fluxo correspondente ao SMS.
h. O SMS encaminhará o fluxo para o decodificador.
i. O decodificador decodificará o fluxo obtido e exibirá o vídeo na parede inteligente.

Exibir Vídeo de Alarme na Parede Inteligente

1. Exibir vídeo de alarme de dispositivo conectado diretamente na parede inteligente

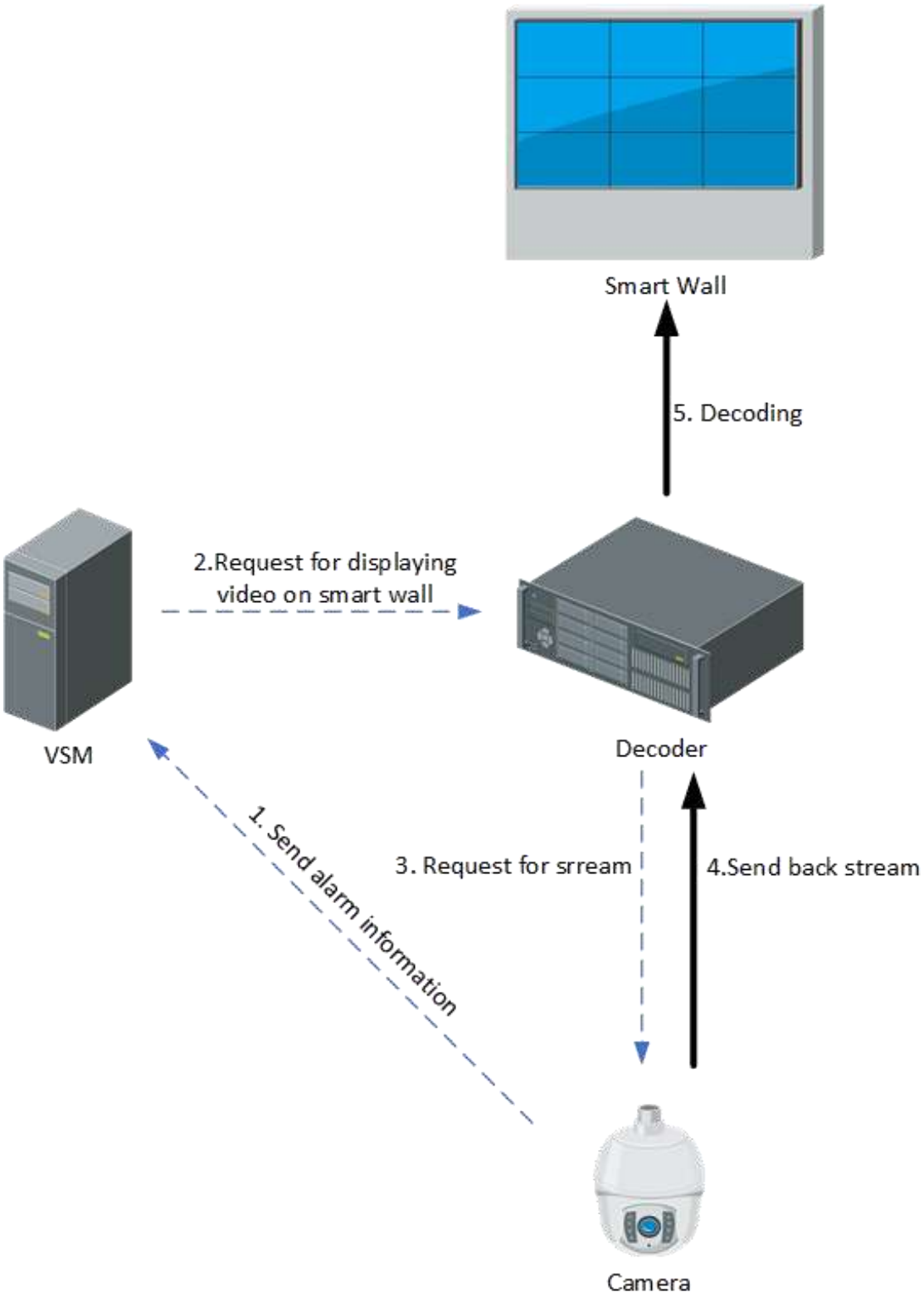


Figura 3-16 Fluxo de exibição de vídeo de alarme de dispositivo conectado diretamente no Smart Wall

O processo de exibição de vídeo de alarme de dispositivo conectado diretamente na parede

inteligente é o seguinte:

a. A câmera analisará os fluxos obtidos. Se um alarme for disparado, a câmera enviará o alarme para o SYS.
b. De acordo com o alarme, o SYS deve estimar se o vídeo da câmera precisa ser exibido na parede inteligente. Se sim, o SYS deve enviar uma solicitação ao decodificador para exibir o vídeo na parede inteligente.
c. O decodificador enviará uma solicitação à câmera correspondente para obter o fluxo de vídeo do alarme.
d. A câmera enviará de volta o fluxo de acordo com a solicitação correspondente.
e. O decodificador decodificará o fluxo obtido e exibirá o vídeo na parede inteligente.

2. Exibir vídeo de alarme no Smart Wall via servidor de streaming

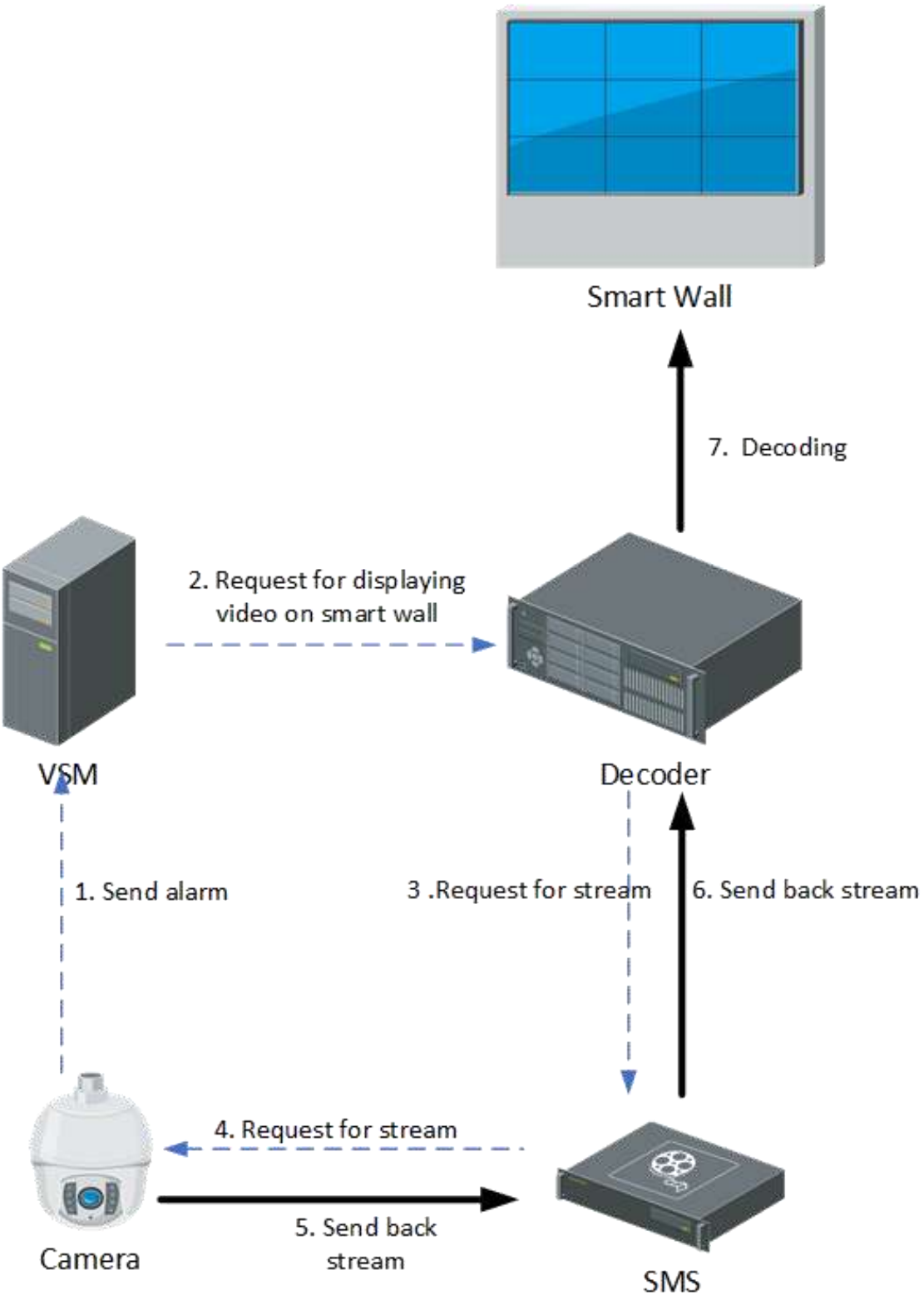


Figura 3-17 Fluxo de exibição de vídeo de alarme no Smart Wall via servidor de streaming

O processo de exibição de vídeo de alarme do dispositivo na parede inteligente via SMS é o seguinte:

a. A câmera analisará os fluxos obtidos. Se um alarme for disparado, a câmera enviará o alarme para o SYS.
b. De acordo com o alarme, o SYS deve estimar se o vídeo da câmera precisa ser exibido na parede inteligente. Se sim, o SYS deve enviar uma solicitação ao decodificador para exibir o vídeo na parede inteligente.
c. O decodificador enviará uma solicitação ao SMS (Streaming Server) para obter o fluxo.
d. O SMS encaminhará a solicitação para a câmera correspondente para obtenção do fluxo.
e. A câmera enviará o fluxo de volta para o SMS de acordo com a solicitação correspondente.
f. O SMS encaminhará os fluxos obtidos para o decodificador.
g. O decodificador decodificará o fluxo obtido e exibirá o vídeo na parede inteligente.

Exibir Vídeo Controlado pelo Teclado no Smart Wall

1. Exibir vídeo de dispositivo conectado diretamente controlado por teclado no Smart Wall

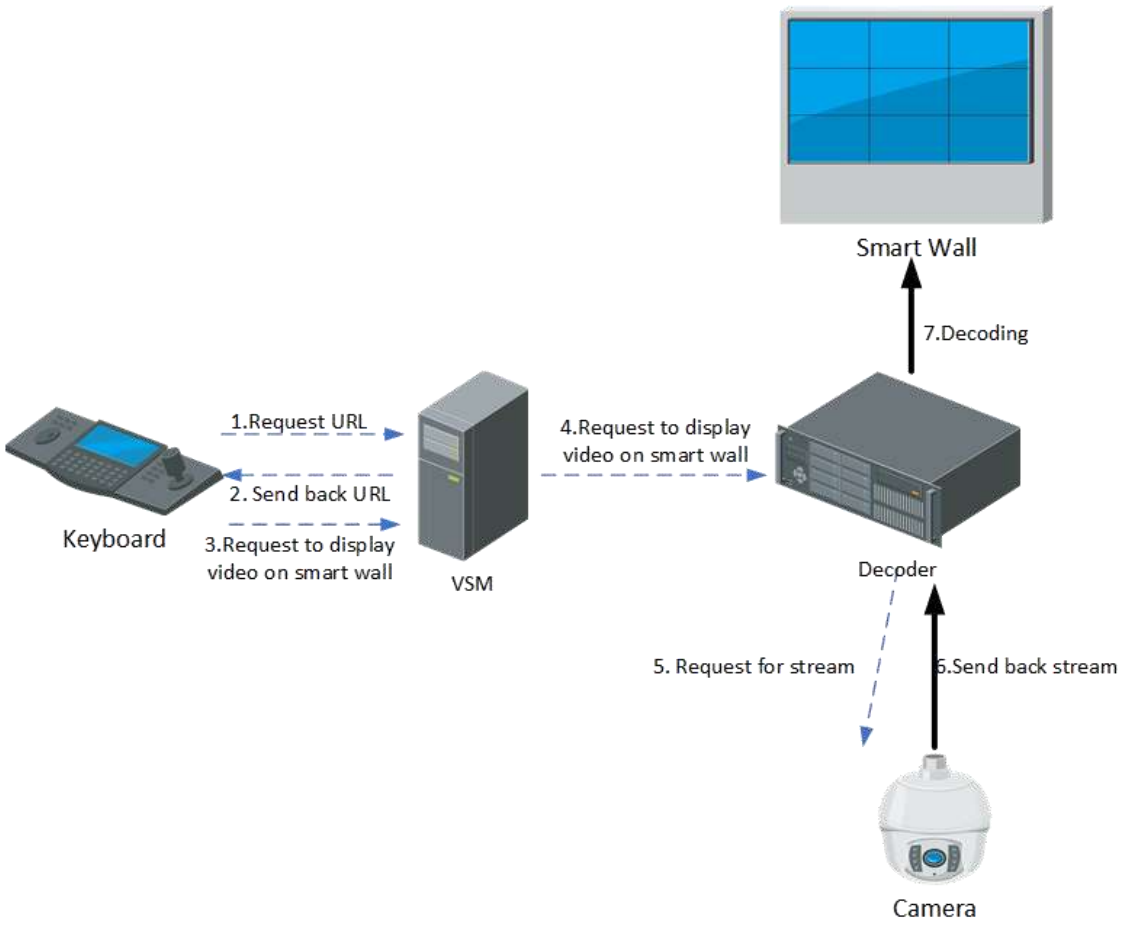


Figura 3-18 Fluxo de exibição de vídeo de dispositivo conectado diretamente controlado por teclado no Smart Wall

Se o decodificador obtiver o fluxo diretamente do dispositivo, o processo de sinalização será o seguinte:

a. O teclado enviará uma solicitação ao SYS para obter as informações de URL (incluindo as informações do smart wall e do dispositivo).

b. O SYS enviará de volta as informações de URL para o teclado.
c. O teclado enviará uma solicitação ao SYS para exibir o vídeo no smart wall.
d. O SYS encaminhará a solicitação ao decodificador para exibir o vídeo no smart wall.
e. O decodificador enviará uma solicitação ao dispositivo para obter o fluxo.
f. O dispositivo enviará de volta o fluxo correspondente ao decodificador.
g. O decodificador decodificará o fluxo obtido e exibirá o vídeo na parede inteligente.

2. Exibir vídeo controlado pelo teclado no Smart Wall via servidor de streaming

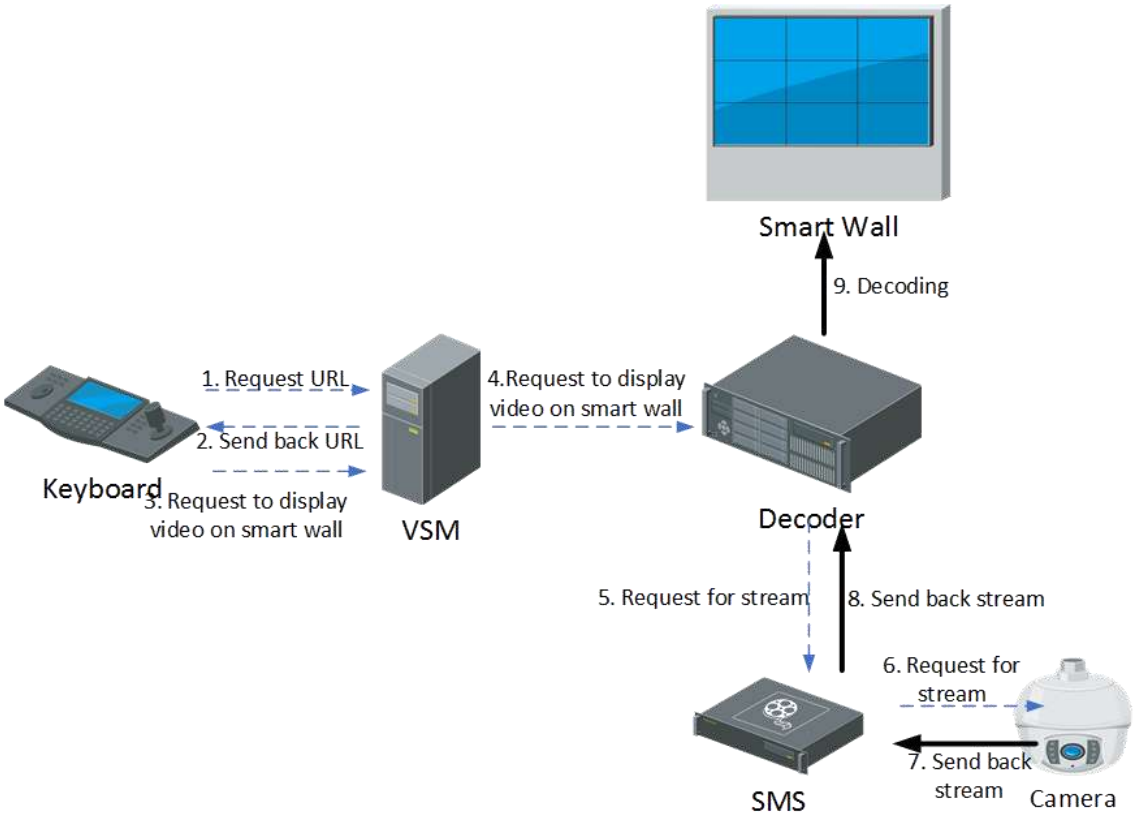


Figura 3-19 Fluxo de exibição de vídeo controlado pelo teclado no Smart Wall via servidor de streaming

Se o decodificador obtiver o fluxo via SMS, o processo de sinalização será o seguinte:

a. O teclado enviará uma solicitação ao SYS para obter as informações de URL (incluindo as informações do smart wall e do dispositivo).
b. O SYS enviará de volta as informações de URL para o Smart Wall Client.
c. O teclado enviará uma solicitação ao SYS para exibir o vídeo no smart wall.
d. O SYS encaminhará a solicitação ao decodificador para exibir o vídeo no smart wall.
e. O decodificador enviará uma solicitação ao SMS (Streaming Server) para obter o fluxo.
f. O SMS encaminhará a solicitação ao dispositivo para obtenção do fluxo.
g. O dispositivo enviará de volta o fluxo correspondente ao SMS.
h. O SMS encaminhará o fluxo para o decodificador.
i. O decodificador decodificará o fluxo obtido e exibirá o vídeo na parede inteligente.

Exibir Vídeo no Smart Wall (placa gráfica)

1. Exibir vídeo do dispositivo conectado diretamente na parede inteligente (placa gráfica)

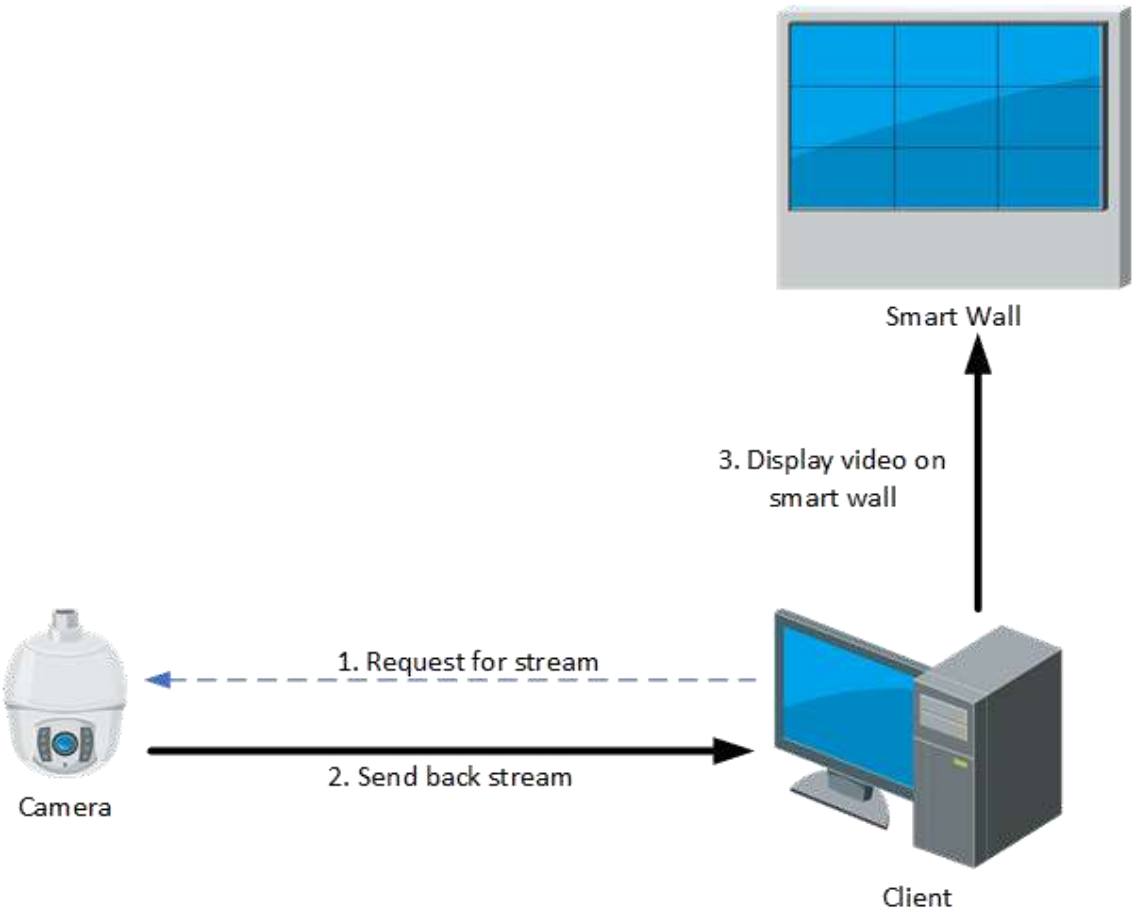


Figura 3-20 Fluxo de exibição de vídeo de dispositivo conectado diretamente no Smart Wall (placa gráfica)

   a. O cliente deverá enviar uma solicitação à câmera para obter o fluxo.
   b. A câmera enviará de volta o fluxo correspondente ao cliente.
   c. O cliente deverá enviar o stream para exibição no Smart Wall (placa gráfica).
2. Exibir vídeo no Smart Wall (placa gráfica) via servidor de streaming

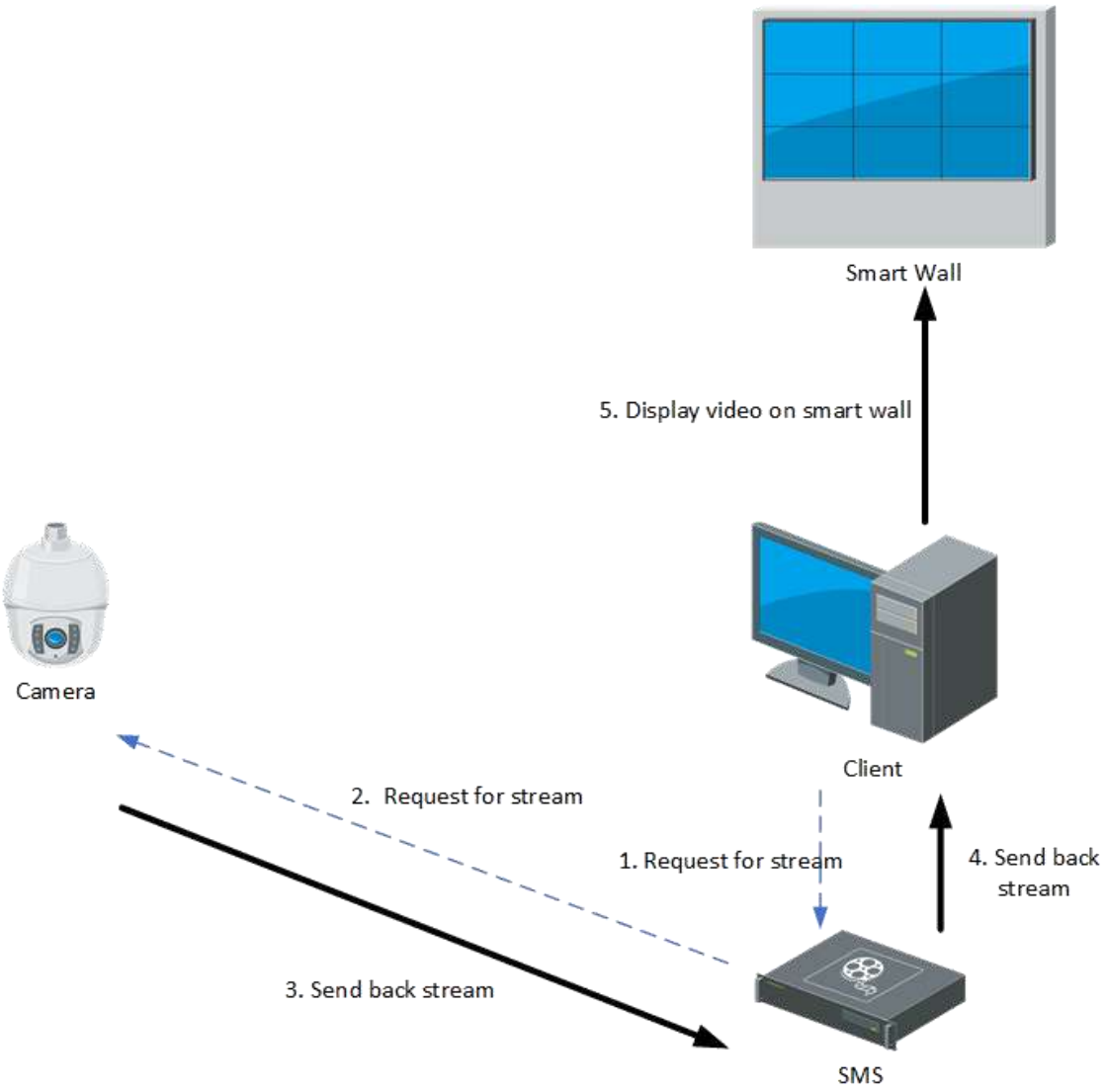


Figura 3-21 Fluxo de exibição de vídeo no Smart Wall (placa gráfica) via servidor de streaming

a. O cliente deverá enviar uma solicitação ao SMS (Streaming Server) para obter o stream.
b. O SMS encaminhará a solicitação para a câmera obter o stream.
c. A câmera enviará de volta o fluxo correspondente ao SMS.
d. O SMS encaminhará o fluxo obtido ao cliente.
e. O Cliente deverá enviar o stream para exibição no Smart Wall (Placa Gráfica).

3.6.6 Controle de Acesso

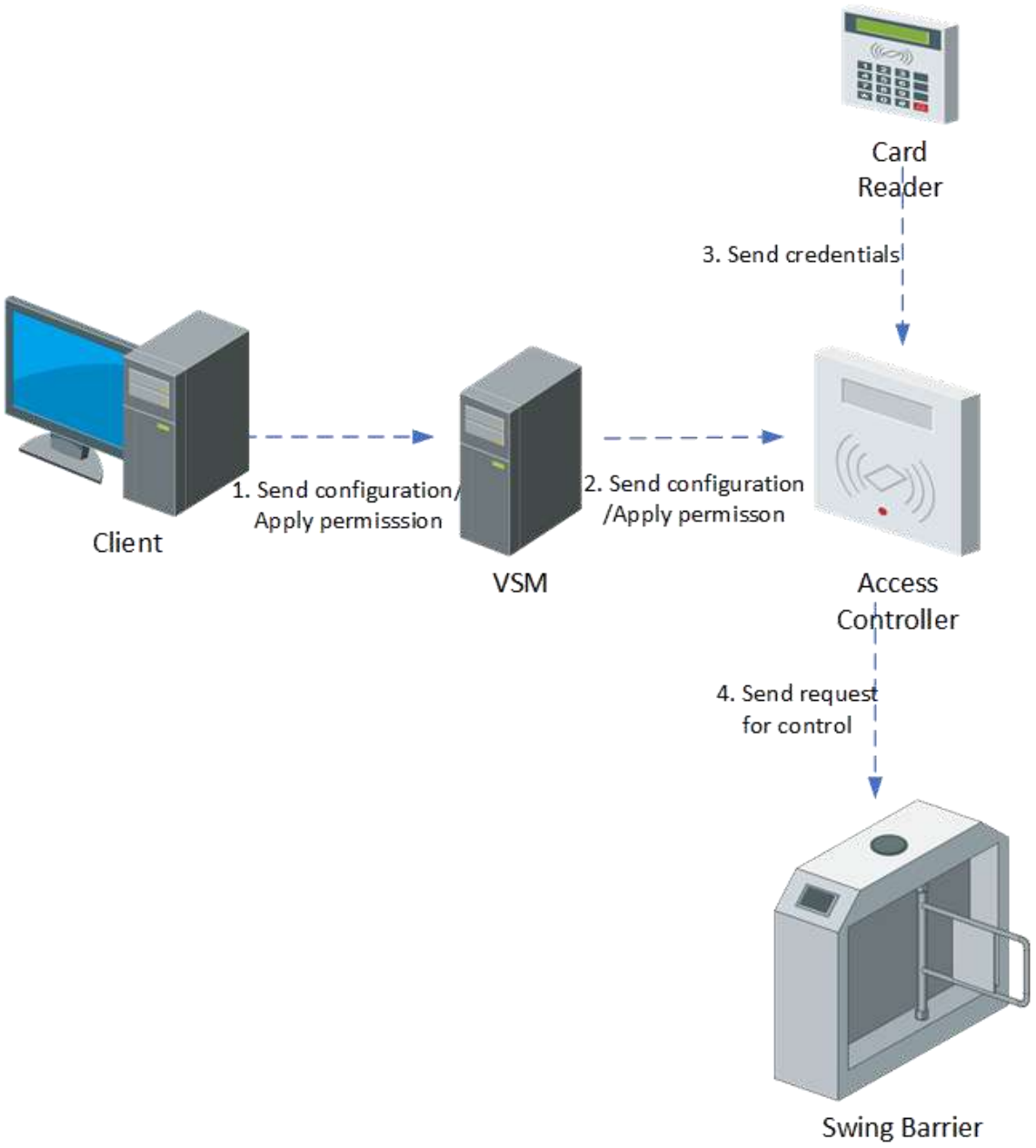


Figura 3-22 Fluxo de controle de acesso

O processo de sinalização de controle e gerenciamento de acesso é o seguinte:

1. O Web Client enviará um comando de configuração de controle de acesso (incluindo permissão de pessoal, configuração de dispositivo e configuração de evento) para o SYS.
2. O SY enviará o comando de configuração para o dispositivo.
3. O leitor de cartão obterá as instruções correspondentes e enviará as informações de credencial ao controlador de acesso.
4. O controlador de acesso deve enviar a solicitação de controle para a barreira giratória de acordo com a instrução obtida para controlar o status do interruptor da barreira giratória.

3.6.7 ANPR

Ver Fotos Capturadas pela Câmera ANPR

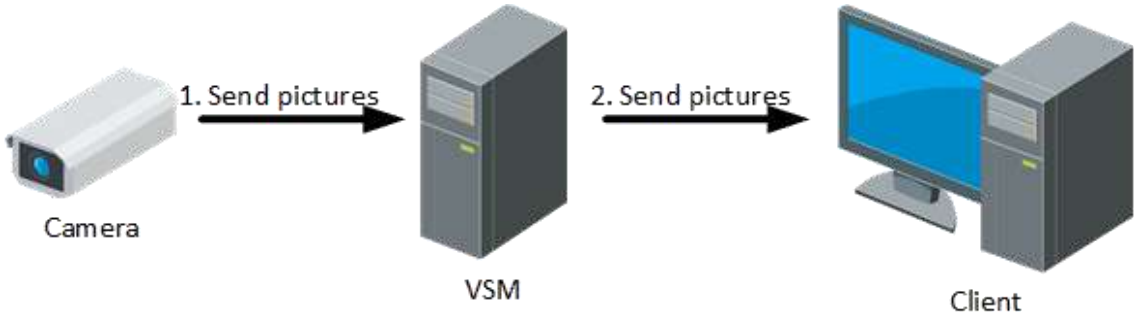


Figura 3-23 Fluxo de visualização de imagens capturadas pela câmera ANPR

De acordo com as configurações da plataforma, as imagens podem ser armazenadas no SYS localmente ou no servidor de armazenamento de imagens.

Se a imagem estiver armazenada no SYS, o processo de sinalização será o seguinte:

1. A câmera ANPR capturará a imagem e a enviará para o SYS.
2. O SYS enviará a imagem obtida ao Control Client para exibição.

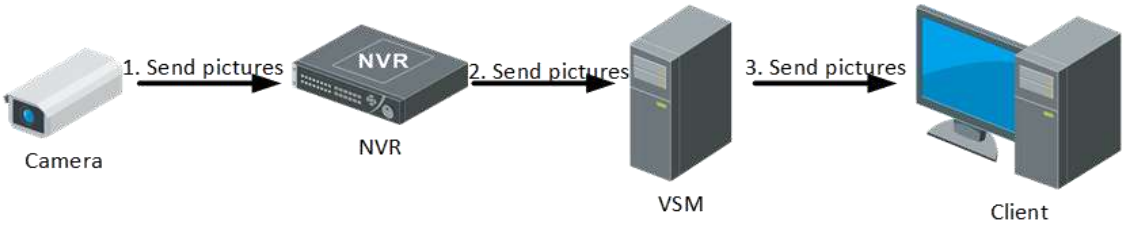


Figura 3-24 Fluxo de visualização de imagens armazenadas no servidor de gravação e capturadas pela câmera ANPR

Se a imagem for armazenada no servidor de armazenamento de imagens (por exemplo, NVR), o processo de sinalização será o seguinte:

1. A câmera ANPR capturará a imagem e a enviará para o NVR.
2. O NVR enviará a imagem obtida para o SYS.
3. O SYS enviará a imagem obtida ao Control Client para exibição.

Imagens de Recuperação Armazenadas no SYS

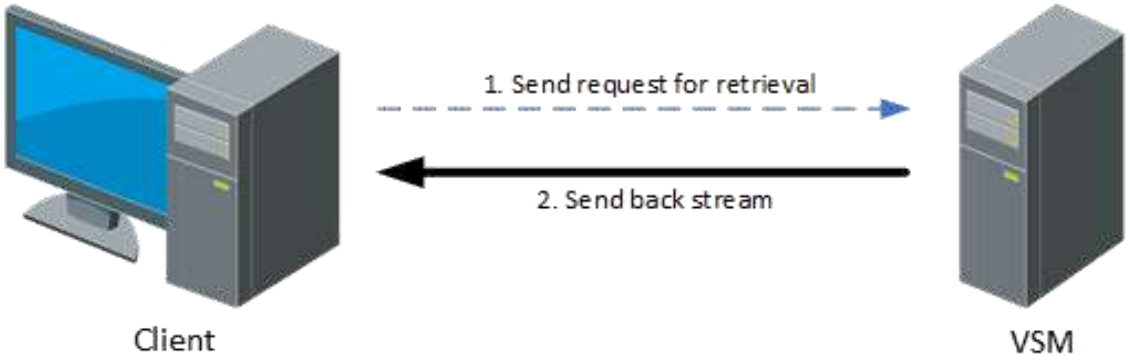


Figura 3-25 Fluxo de pesquisa de imagens armazenadas no SYS

Se as imagens ANPR forem armazenadas no SYS, o processo de sinalização de recuperação e exibição das imagens ANPR será o seguinte:

1. O Cliente de Controle enviará uma instrução de recuperação de imagem para o SYS.
2. O SYS pesquisará as imagens necessárias e enviará o resultado ao Control Client.

Recuperação de Imagens Armazenadas no NVR

1. Cliente e NVR estão na mesma LAN

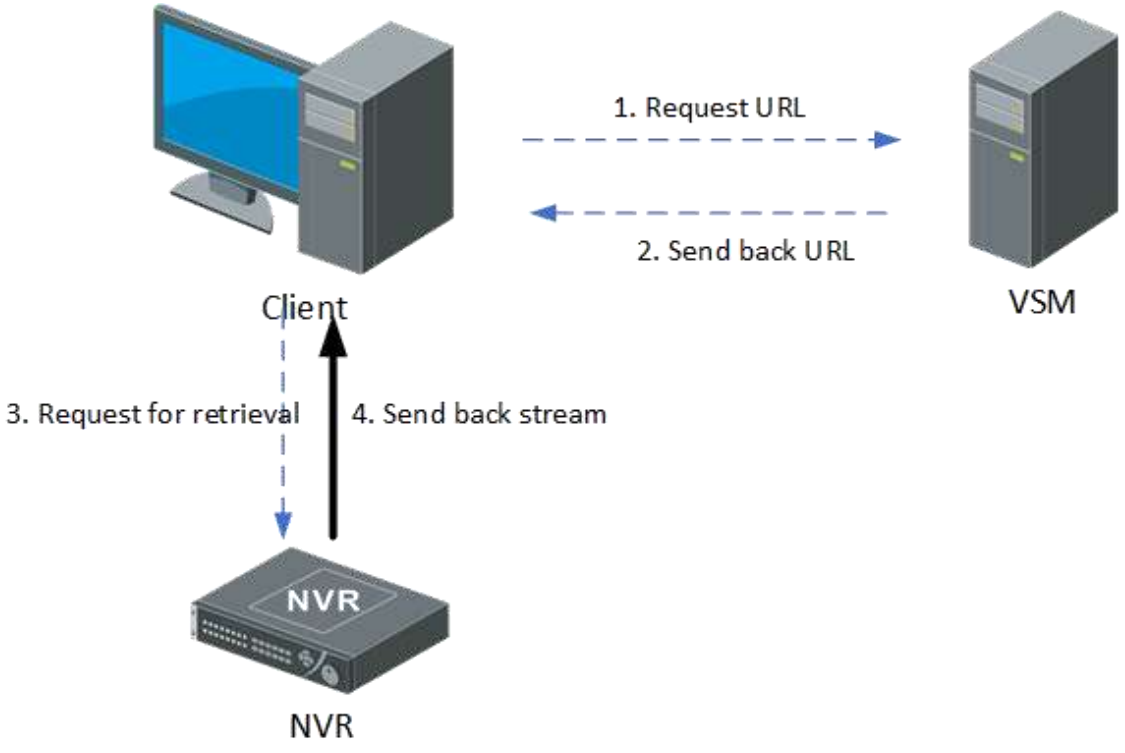


Figura 3-26 Fluxo de busca de imagens armazenadas no NVR quando o cliente e o NVR estão na mesma LAN

Se o vídeo estiver armazenado no NVR que está na mesma rede do Control Client, o processo

de obtenção das imagens capturadas pelas câmeras ANPR é o seguinte:

a. O Control Client enviará uma solicitação ao SYS para obter as informações de URL do NVR.
b. O SYS enviará as informações de URL correspondentes ao Cliente de Controle.
c. De acordo com as informações de URL obtidas, o Cliente de Controle deverá enviar uma instrução ao NVR para obter as imagens capturadas pela câmera ANPR.
d. O NVR enviará as imagens correspondentes ao Cliente de Controle de acordo com as instruções obtidas.

2. O cliente e o NVR estão em LANs diferentes

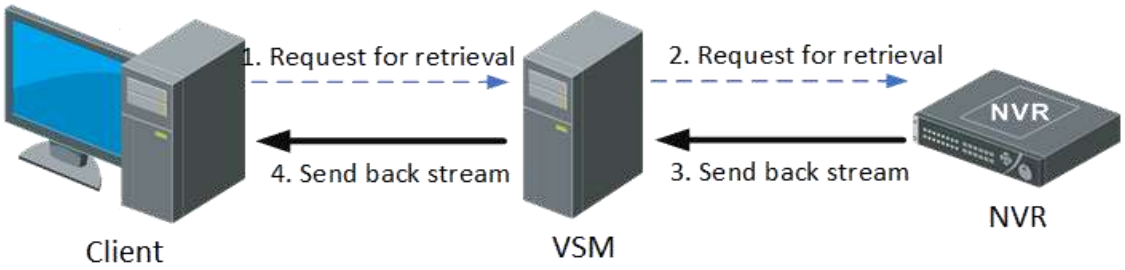


Figura 3-27 Fluxo de busca de imagens armazenadas no NVR quando o cliente e o NVR estão em LANs diferentes

Caso o vídeo esteja armazenado no NVR que não esteja na mesma rede do Control Client, o processo de obtenção das imagens capturadas pelas câmeras ANPR é o seguinte:

a. O Cliente de Controle enviará uma solicitação ao SYS para recuperação de imagem.
b. O SYS enviará a solicitação de recuperação ao NVR.
c. O NVR enviará de volta a imagem capturada pela câmera ANPR para o SYS de acordo com a solicitação.
d. O SYS encaminhará a imagem obtida ao Cliente de Controle de acordo com as instruções reais.

3.6.8 Cliente Móvel

Visualização ao vivo

O Mobile Client, assim como outros clientes, pertencerá ao cliente HikCentral Professional. Portanto, o processo de obtenção de streams é o mesmo que o de outros clientes.

1. Visualização ao vivo para dispositivo conectado diretamente

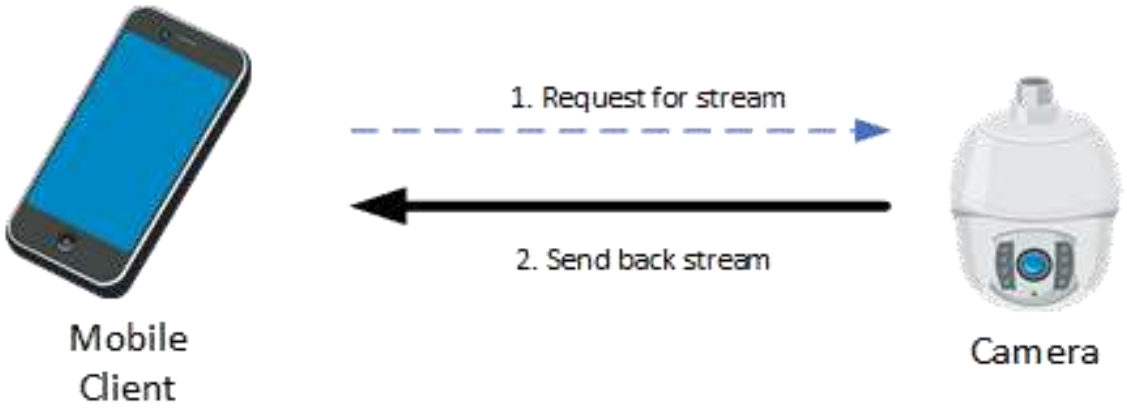


Figura 3-28 Fluxo de visualização ao vivo para dispositivo conectado diretamente no cliente móvel

Se o Mobile Client e o dispositivo estiverem conectados diretamente, o processo de visualização ao vivo no Mobile Client será o seguinte:

a. O Cliente Móvel enviará uma solicitação ao dispositivo para obter o fluxo.
b. O dispositivo enviará de volta o fluxo correspondente ao Cliente Móvel.

2. Visualização ao vivo via servidor de streaming

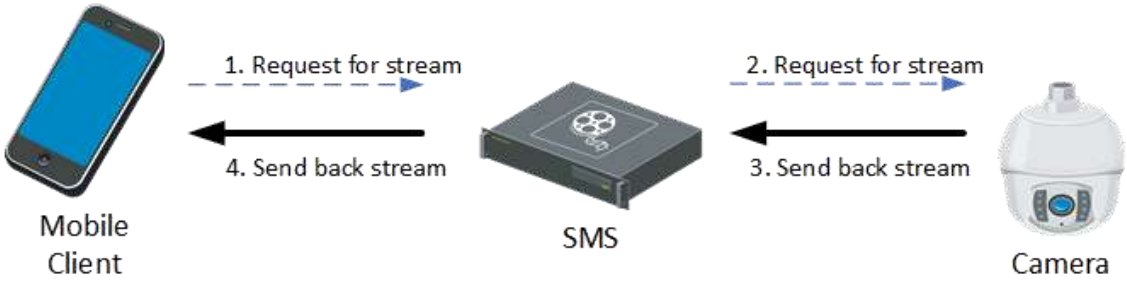


Figura 3-29 Fluxo de visualização ao vivo via servidor de streaming no cliente móvel

Se o Cliente Móvel obtiver o fluxo do dispositivo via SMS (Servidor de Streaming), o processo será o seguinte:

a. O Cliente Móvel deverá enviar uma solicitação ao SMS para obtenção do fluxo.
b. O SMS encaminhará a solicitação ao dispositivo para obtenção do fluxo.
c. O dispositivo deve enviar de volta o fluxo correspondente ao SMS de acordo com a solicitação.
d. O SMS enviará o fluxo de volta para o Cliente Móvel.

Reprodução

1. Reprodução de vídeo em dispositivo conectado diretamente

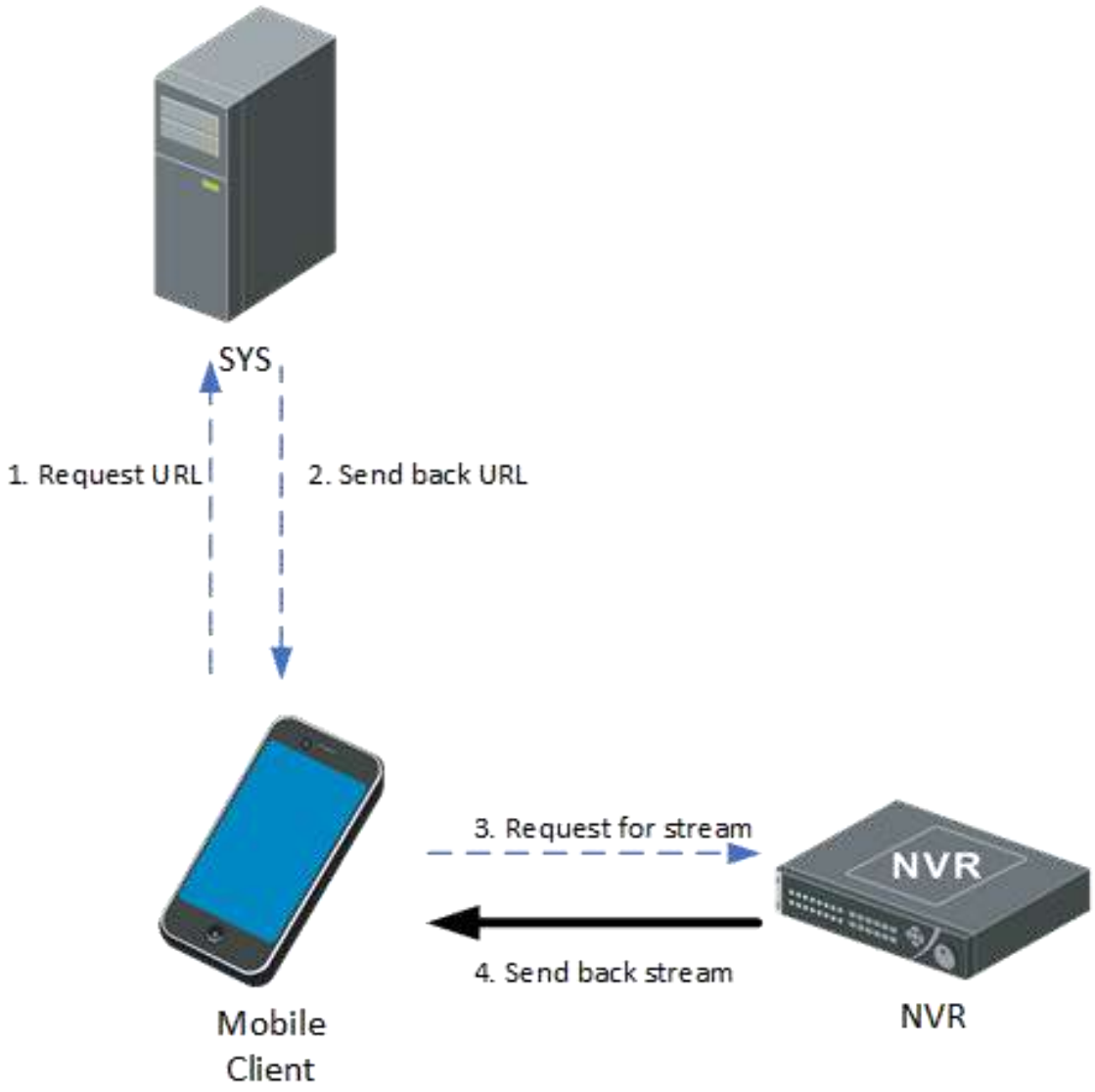


Figura 3-30 Fluxo de reprodução de vídeo em dispositivo conectado diretamente no cliente móvel

Se o arquivo de vídeo estiver armazenado diretamente no dispositivo, o processo será o seguinte:

a. O Cliente Móvel deverá enviar uma solicitação ao SYS para obter a URL do fluxo.
b. O SYS enviará as informações de URL do fluxo para o Mobile Client.
c. O Cliente Móvel enviará uma solicitação ao dispositivo de armazenamento conectado diretamente para obter o fluxo.
d. O dispositivo de armazenamento enviará de volta o fluxo de reprodução correspondente ao Cliente Móvel.

2. Reprodução via servidor de streaming

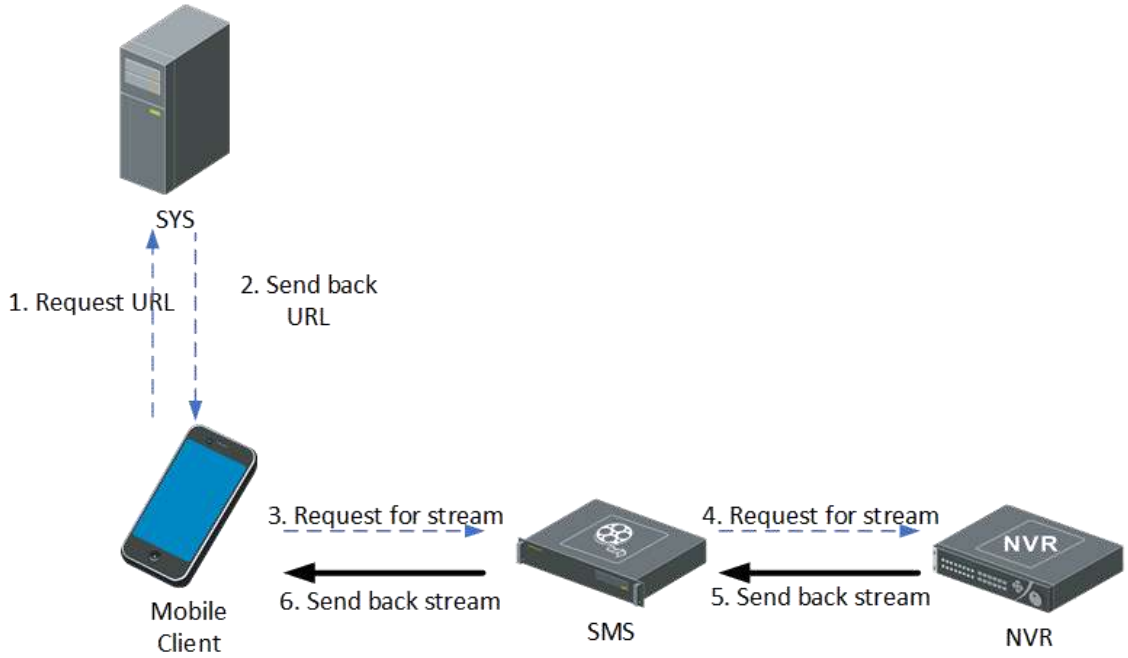


Figura 3-31 Fluxo de reprodução via servidor de streaming no cliente móvel

Se o Cliente Móvel obtiver o fluxo via SMS, o processo será o seguinte:

a. O Cliente Móvel deverá enviar uma solicitação ao SYS para obter a URL do fluxo.
b. O SYS enviará as informações de URL do fluxo para o Mobile Client.
c. O Cliente Móvel deverá enviar uma solicitação ao SMS para obtenção do fluxo.
d. O SMS encaminhará a solicitação ao NVR para obtenção do fluxo.
e. O NVR enviará de volta o fluxo de reprodução para o SMS.
f. O SMS encaminhará o fluxo obtido para o Cliente Móvel.

Alarme

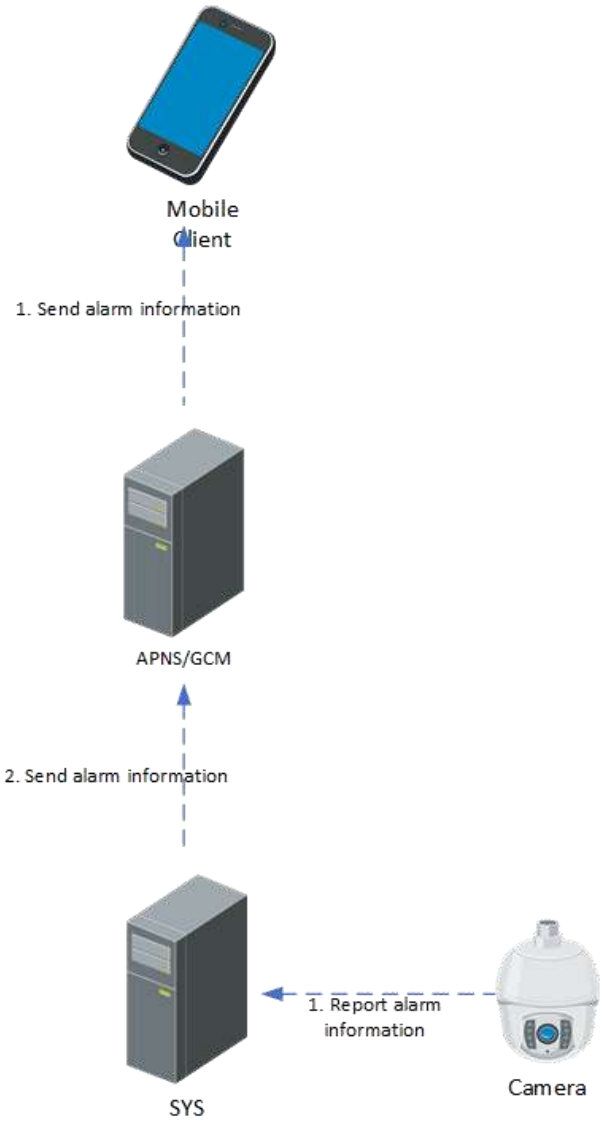


Figura 3-32 Fluxo de alarme no cliente móvel

Semelhante aos outros clientes, o processo de recebimento de vídeo de alarme no Mobile Client é o seguinte:

1. O dispositivo deve reportar um alarme ao SYS.
2. O SYS enviará as informações de alarme obtidas para o servidor APNS/GCM.
3. O servidor APNS/GCM enviará as informações de alarme correspondentes ao Cliente Móvel.

3.6.9 Monitoramento de Status

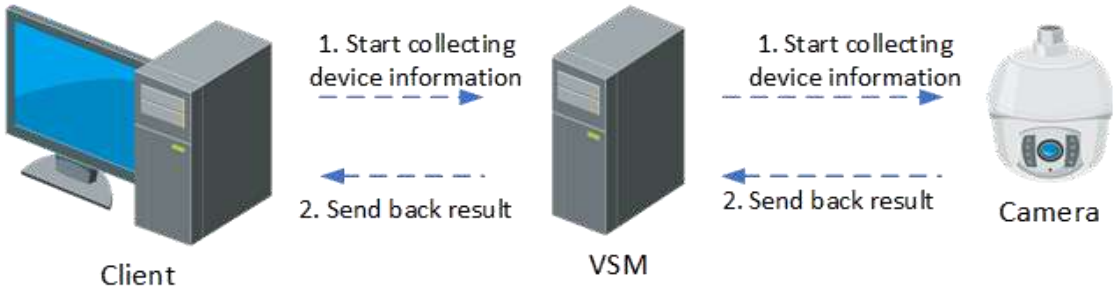


Figura 3-33 Fluxo de monitoramento de status

A inspeção de status do dispositivo consistirá nas duas situações a seguir: interação entre o cliente e o SYS, e entre o dispositivo e o SYS.
A plataforma iniciará informações de inspeção a cada 3 minutos.

Interação entre SYS e Dispositivo

1. O SYS enviará um comando de inspeção ao dispositivo.
2. O dispositivo deve enviar de volta o status do dispositivo para o SYS.

Interação entre Cliente e SYS

1. O Cliente de Controle enviará um comando de inspeção ao SYS.
2. O SYS enviará o status atual do dispositivo para o Control Client.

3.7 Segurança do Sistema

3.7.1 Visão Geral do Design de Segurança

A plataforma HikCentral Professional deve consistir no servidor, cliente, componente de serviço e plataforma SDK. A interação entre servidor e cliente, servidor e componente de serviço, servidor e plataforma SDK deve suportar HTTP e HTTPS.
Para garantir a segurança do armazenamento de dados, todos os dados sensíveis armazenados no servidor devem ser criptografados. Todas as informações sensíveis que não precisam ser descriptografadas devem ser criptografadas por esquema de criptografia irreversível. Todas as informações sensíveis que precisam ser descriptografadas devem ser criptografadas por esquema de criptografia que pode ser descriptografado.
O HikCentral Professional deve adotar os seguintes algoritmos de criptografia: RSA, AES, SHA e MD5. Todos os algoritmos de criptografia devem vir da biblioteca padrão de código aberto OpenSSL-1.0.2K. A versão OpenSSL deve ser atualizada de acordo com as políticas do laboratório de segurança Hikvision.

3.7.2 Solução de Segurança do Sistema

Protocolo de Acesso

Por padrão, o protocolo HTTP é usado para acesso à web. Opcionalmente, os usuários podem habilitar o protocolo HTTPS.
HTTPS: Os usuários podem importar o certificado HTTPS para melhorar a segurança da transmissão de dados.
HTTP: No modo HTTP, a plataforma deve fornecer uma solução de segurança independente para evitar ataques de repetição.

Autenticação do Servidor de Streaming

Para garantir a segurança geral da plataforma, quando os clientes obtêm transmissões ao vivo ou de reprodução de dispositivos via SMS (Servidor de Streaming), o dispositivo deve ser autenticado pelo SMS primeiro.

Autenticação de Login

A plataforma autentica usuários com base no nome de usuário e senha. A força da senha e o tempo de expiração podem ser configurados separadamente na plataforma. Se o administrador esquecer a senha de login, a plataforma deve permitir que os usuários redefinam a senha por licença. Para garantir a segurança do sistema, as informações de entrada devem ser ocultadas durante a entrada da senha.
Durante a transmissão, a senha deve ser criptografada pelo algoritmo RSA no modo HTTP, e o mecanismo de criptografia interna HTTPS deve ser usado no modo HTTPS. Na autenticação de login da plataforma, o código de verificação + bloqueio de usuário + bloqueio de endereço IP devem ser usados para evitar quebra de força bruta de usuário malicioso, para melhorar o nível de segurança da plataforma.
Autenticação Homem-Máquina: Se uma senha incorreta for inserida durante o login, os usuários deverão inserir manualmente o código de verificação.
Bloqueio de Usuário: Este parâmetro é obrigatoriamente habilitado. Se a senha for inserida incorretamente por cinco vezes consecutivas, o usuário não poderá efetuar login no sistema em 30 minutos.
Bloqueio de Endereço IP: Este parâmetro é habilitado por padrão. Os usuários podem configurar manualmente o número de vezes de erro e o período de bloqueio. Se o número de tentativas de login incorretas para o mesmo endereço IP exceder o valor especificado, o endereço IP não poderá ser usado para fazer login no sistema dentro do período de bloqueio especificado.

Acesso à plataforma

Após o cliente efetuar login com sucesso no sistema, o servidor deve gerar aleatoriamente uma sessão para cada cliente. A sessão pode efetivamente reduzir os riscos de cracking causados pela verificação frequente de interação de nome de usuário e senha durante o negócio. Cada sessão deve ter uma vida útil fixa. Quando uma sessão carregada por um cliente expira, o usuário deve efetuar login na plataforma novamente.
No modo HTTP, para garantir que a plataforma não seja atacada por ataques de repetição, cada sessão deve carregar um token anti-reprodução, que é único em cada sessão. O token é inválido

imediatamente após cada solicitação para evitar ataques de token repetidos. O token deve ser criptografado usando AES.

Processamento de Informações Sensíveis

Para informações confidenciais, como nome de usuário e senha, que são usadas diariamente, a HikCentral Professional fornecerá soluções de segurança com base nos cenários reais de serviço. Todas as informações sensíveis são criptografadas durante a interação entre o cliente e o servidor. No modo HTTP, a criptografia AES deve ser usada para gerar uma chave AES aleatória para cada login, para garantir que os dados não sejam facilmente roubados. No modo HTTPS, a criptografia do certificado SSL deve ser usada.

Para o armazenamento de informações sensíveis, a HikCentral Professional deve fornecer um esquema de armazenamento diferente de acordo com os diferentes requisitos comerciais. Para evitar que o vazamento da chave de criptografia de uma plataforma afete outras plataformas, a HikCentral Professional deve adotar o esquema de criptografia AES dinâmico para informações sensíveis (como a senha de acesso ao banco de dados e a senha de acesso ao dispositivo) que precisam ser armazenadas localmente. Para evitar o vazamento da senha do usuário do sistema causado pelo vazamento do arquivo de dados do sistema, a senha do usuário da plataforma deve ser criptografada pelo algoritmo SHA e armazenada em texto cifrado.

Capítulo 4 Função

A plataforma suportará as funções abaixo.

4.1 Gestão de Pessoas

- ***Gestão de Pessoas***
- ***Gerenciamento de Credenciais***
- ***Gestão de Demissão***
- ***Gestão de posição***

4.1.1 Gestão de Pessoas

Informações Pessoais

- A plataforma deve suportar a entrada de informações pessoais, incluindo informações básicas, nível de acesso, cronograma de turnos, biblioteca de imagens faciais, grupo de estação de ancoragem, informações de residentes e informações públicas personalizadas. Informações básicas: ID (16 dígitos e letras); departamento; primeiro nome (até 128 caracteres); sobrenome (128 caracteres); temperatura e status da superfície da pele; período efetivo (10 anos a partir do momento atual); e-mail; número de telefone; superusuário; acesso estendido; administrador do dispositivo; código PIN; observação; informações privadas personalizadas.
- A plataforma dará suporte à mudança da organização de uma pessoa.
- A plataforma oferecerá suporte à exportação de todas as informações da pessoa adicionada como um arquivo ZIP e à definição de uma senha para descompactar o arquivo ZIP.
- A plataforma oferecerá suporte à segmentação de informações pessoais por abas na página Adicionar Pessoa.
- A plataforma oferecerá suporte à exportação de informações pessoais com itens adicionais.
- A plataforma oferecerá suporte à exportação de fotos de perfil de pessoas selecionadas como um arquivo ZIP e à definição de uma senha criptografada.
- A plataforma oferecerá suporte à exportação de informações e informações adicionais sobre pessoas selecionadas.
- A plataforma oferecerá suporte à importação de informações pessoais por meio de modelo com itens adicionais.
- A plataforma oferecerá suporte para adicionar uma pessoa ao grupo de contagem de emergência.
- A plataforma oferecerá suporte à edição de credenciais (incluindo cartão, impressão, rosto e íris) na lista de pessoas.
- No Web Client, se a função Usar este dispositivo como dispositivo de registro estiver habilitada na página de configuração do dispositivo, as informações sobre pessoas e credenciais adicionadas e credenciais editadas no dispositivo serão sincronizadas automaticamente com a plataforma.

Gerenciamento de Pessoas em Lote

- A plataforma suportará o ajuste em lote do período efetivo para pessoas.
- A plataforma oferecerá suporte à filtragem e exportação em lote de informações de pessoas vencidas.
- A plataforma suportará perda de cartões de relatórios em lote.
- A plataforma oferecerá suporte à desativação e restauração temporária dos níveis de acesso de pessoas.

Personalizar Informações Pessoais

- A plataforma oferecerá suporte à personalização de até 20 itens de informações privadas e 4 tipos por item de informação, incluindo texto, valor, data e seleção única (limitado pela permissão da plataforma).
- A plataforma suportará a personalização de até 20 itens de informação pública e um tipo (somente texto) por item de informação (limitado pela permissão da plataforma).

Login

- A plataforma oferecerá suporte ao administrador para habilitar o login de autoatendimento dos funcionários (habilitado por padrão) e definir a senha dos funcionários (ID do funcionário por padrão).
- A plataforma oferecerá suporte ao login de autoatendimento dos funcionários na plataforma.
- A plataforma deve suportar o bloqueio de endereço IP por um período de tempo especificado após um número específico de tentativas de senha com falha.
- A plataforma deve suportar a definição de idade máxima para senhas.
- A plataforma oferecerá suporte à solicitação de alteração de senha pelos funcionários no primeiro login, ao envio de notas quando a senha expirar e à redefinição de uma nova senha caso os funcionários a esqueçam.
- A plataforma suportará login que expira após um período em que nenhuma ação acontece.

Upload de Informações Pessoais por Autoatendimento

- A plataforma oferecerá suporte à entrada na página de autorregistro por meio da digitalização do código QR de autorregistro, inserção e envio de informações pessoais para a plataforma.
- A plataforma deve suportar a habilitação da verificação da qualidade da imagem facial do dispositivo. Após ela ser habilitada, você pode escolher qualquer dispositivo com a função de verificação da qualidade da imagem facial como um dispositivo para verificação. Ela é desabilitada por padrão.
- A plataforma deve suportar a função de habilitar Review Self-Registered Persons. Após ser habilitada, todas as informações de pessoas enviadas de forma self-service devem ser revisadas e aprovadas pelo Administrador antes de serem importadas para a plataforma.
- A plataforma oferecerá suporte à importação de informações pessoais adicionadas de forma autônoma para uma organização específica (a organização raiz é o padrão).
- A plataforma dará suporte aos administradores na verificação de informações pessoais enviadas por autoatendimento: aprovar, rejeitar e excluir.

Pessoas Importadoras

- A plataforma oferecerá suporte à importação de informações pessoais por meio de arquivo Excel e à definição de parâmetros sobre a substituição de pessoas e números de cartão duplicados.
- A plataforma oferecerá suporte à importação de fotos de perfil em formato ZIP e habilitar/desabilitar a avaliação da qualidade da foto do rosto.
- A plataforma oferecerá suporte à importação de pessoas de dispositivos.

Sincronização de Domínio do AD

- A plataforma dará suporte à configuração da relação de mapeamento entre o domínio do AD e a pessoa.
- A plataforma deve suportar a sincronização do domínio do AD com a pessoa ou o grupo de pessoas.
- A plataforma oferecerá suporte à sincronização do domínio do AD com o grupo de segurança.
- A plataforma oferecerá suporte à sincronização de pessoas ou grupos de pessoas do domínio do Azure AD.
- A plataforma oferecerá suporte à vinculação de ID de pessoa com itens no domínio do AD.

Lidando com Permissões de Pessoas Rapidamente

- A plataforma oferecerá suporte à compensação de permissões.
- A plataforma oferecerá suporte à detecção de status de permissão.
- A plataforma oferecerá suporte à desativação de níveis de acesso e à restauração de níveis de acesso em lote.

Renúncia de Pessoa

- A plataforma dará suporte ao gerenciamento de demissões.
- A plataforma oferecerá suporte à exclusão dos níveis de acesso das pessoas que se demitiram na data da demissão.
- A plataforma deverá oferecer suporte à ativação/desativação do cálculo de frequência durante o período entre a solicitação de demissão e a data da demissão.
- A plataforma oferecerá suporte à busca de registros de acesso e frequência de pessoas demitidas.

4.1.2 Gerenciamento de Credenciais

Gestão de Cartões

1. A plataforma suportará até 20 dígitos para um número de cartão.
2. A plataforma suportará adicionar até cinco cartões por pessoa.
3. A plataforma suportará a inserção manual do número do cartão.
4. A plataforma oferecerá suporte a estações de registro de cartões que leiam números de cartões.
5. Ao ler o número do cartão por meio de uma estação de registro de cartão, a plataforma deverá

oferecer suporte à seleção do formato do cartão.

6. A plataforma suportará a criptografia de setores do cartão (um setor por vez) somente quando a criptografia for feita por meio da estação de registro do cartão (comunicando-se com a plataforma via USB).
7. A plataforma deve suportar estações de registro (comunicando-se com a plataforma via rede) lendo números de cartão (tipos de cartão suportados, incluindo EM, M1, ID, DESfire, FeliCa e CPU).
8. A plataforma suportará estações de registro (comunicando-se com a plataforma via USB) lendo números de cartão (tipos de cartão suportados, incluindo EM, M1, ID, DESfire, FeliCa e CPU).
9. A plataforma suportará qualquer leitor de cartão de dispositivos de controle de acesso remoto que leia números de cartão.
10. Tipos de cartas: comum, coação e dispensar.
11. A plataforma suportará a emissão de cartões em lote.
12. A plataforma oferecerá suporte para notificação de perda de cartão e cancelamento do relatório de perda de cartão.

Gerenciamento de Impressão Digital

1. A plataforma suportará até 10 impressões digitais por pessoa.
2. A plataforma oferecerá suporte a dispositivos de registro de impressões digitais.
3. A plataforma suportará o registro de impressões digitais por meio da estação de registro (comunicando-se com a plataforma via rede).
4. A plataforma suportará o registro de impressões digitais por meio da estação de registro (comunicando-se com a plataforma via USB).
5. A plataforma suportará qualquer leitor de cartão de dispositivos de controle de acesso remoto que registrem impressões digitais.
6. Tipos de impressão digital: comum, coação e rejeição.
7. A plataforma oferecerá suporte à verificação de duplicatas de impressões digitais e à classificação da qualidade das impressões digitais.

Gerenciamento de Imagem Facial

1. A plataforma suportará apenas uma foto de rosto por pessoa.
2. A plataforma oferecerá suporte ao upload de fotos de rostos locais.
3. A plataforma suportará o uso de uma câmera USB ou de um laptop com uma câmera que registre fotos de rosto.
4. A plataforma suportará inversão de imagem espelhada ao capturar fotos de rosto com uma câmera USB.
5. A plataforma oferecerá suporte ao registro de fotos faciais por meio da estação de registro (comunicando-se com a plataforma via rede).
6. A plataforma suportará o registro de fotos faciais por meio da estação de registro (comunicando-se com a plataforma via USB).
7. A plataforma oferecerá suporte à coleta de imagens faciais por meio de dispositivos de controle de acesso remoto.
8. A plataforma oferecerá suporte à exportação de todas as fotos faciais de todas as pessoas adicionadas como um arquivo ZIP e à definição de uma senha para descompactar o arquivo

ZIP.

9. A plataforma deve oferecer suporte à exclusão de credenciais faciais ou à exclusão em lote de credenciais faciais.
10. A plataforma oferecerá suporte ao salvamento de dados de modelagem ilegíveis de fotos de perfil na plataforma, para que as fotos de perfil reais não sejam exibidas na plataforma.
11. A plataforma oferecerá suporte a testes de qualidade de imagem de perfil por dispositivos de controle de acesso e dispositivos de videoporteiro.
12. A plataforma oferecerá suporte a testes de qualidade de imagem de perfil por barreiras vinculadas a um terminal de reconhecimento facial MinMoe.

Posto de Matrícula

A plataforma suportará o salvamento automático dos parâmetros da estação de inscrição, mantendo a última configuração após o novo login.

Gerenciamento de Senhas

1. A plataforma deverá suportar a definição de senha (única, contendo de 4 a 8 dígitos, e apenas uma senha por pessoa)
2. A plataforma suportará a geração automática de código PIN.

Gestão de Íris

1. A plataforma permitirá a coleta de 2 íris para cada pessoa.
2. A plataforma oferecerá suporte à coleta de íris por dispositivo remotamente como credenciais pessoais e à aplicação de íris aos dispositivos.

Código QR Estático

1. A plataforma suportará a geração de código QR estático com base no número do cartão da pessoa.
2. A plataforma oferecerá suporte à visualização e ao download de códigos QR estáticos para distribuí-los aos funcionários.

Código QR Dinâmico

1. A plataforma oferecerá suporte à seleção do modo de código QR como estático ou dinâmico.
2. A plataforma suportará a configuração do período de validade (1 min por padrão) de um código QR dinâmico.
3. A plataforma oferecerá suporte aos funcionários para visualizar o código QR dinâmico (atualizado automaticamente conforme programado) e atualizar manualmente o código QR após efetuar login no Mobile Client.

4.1.3 Gestão de Demissões

1. A plataforma dará suporte ao gerenciamento de demissões.
2. A plataforma oferecerá suporte à exclusão dos níveis de acesso das pessoas que se demitiram na data da demissão.
3. A plataforma deverá oferecer suporte à ativação/desativação do cálculo de frequência durante

o período entre a solicitação de demissão e a data da demissão.
4. A plataforma oferecerá suporte à busca de registros de acesso e frequência de pessoas demitidas.

4.1.4 Desautenticação de Pessoa

A plataforma deverá suportar as seguintes funções:
1. Desautorizar pessoas selecionadas.
2. Selecione uma causa personalizada de desautorização ao desautorizar pessoas. Cancele a desautorização de pessoas.
3. Para pessoas não autorizadas, seus níveis de acesso, permissão de veículos, etc. também serão desabilitados.
4. A autenticação do controle de acesso por pessoas não autorizadas disparará alarmes.

4.1.5 Gestão de Posições

1. A plataforma oferecerá suporte para adicionar, excluir e editar posições.
2. A plataforma suportará a importação de posições em lote.
3. A plataforma deverá suportar a vinculação de uma posição a diferentes pessoas.
4. A plataforma deve oferecer suporte à vinculação de uma pessoa a uma posição na página de informações da pessoa.
5. A plataforma suportará a visualização do número de pessoas de um cargo e do número de pessoas que se demitiram.

4.2 Veículo

Gestão de Veículos

1. A plataforma suportará adicionar, editar e excluir veículos, incluindo veículos registrados, veículos temporários e veículos de visitantes. As informações editáveis incluem informações do veículo e informações do proprietário do veículo (nome, número de telefone).
2. A plataforma oferecerá suporte à adição de informações personalizadas sobre veículos.
3. A plataforma suportará a importação de veículos por lista de veículos para configuração.
4. A plataforma oferecerá suporte à adição de veículos à lista de bloqueio, à edição de veículos na lista de bloqueio e à remoção de veículos da lista de bloqueio.
5. A plataforma oferecerá suporte ao carregamento de cartões de estacionamento para veículos registrados e ao carregamento das contas dos proprietários dos veículos.
6. A plataforma oferecerá suporte à aplicação de listas de veículos à câmera ANPR para controlar a cancela por meio da câmera.

ANPR (Reconhecimento Automático de Placas)

1. Adicione um módulo independente para procurar veículos que passam e gerar relatórios de análise de veículos.

2. A plataforma oferecerá suporte à busca de veículos que passam, detectados apenas por câmeras ANPR e UVSSs (Under Vehicle Surveillance Systems).
3. A plataforma oferecerá suporte à geração de relatórios de análise de veículos para mostrar o número de veículos que passam detectados por câmeras ANPR especificadas durante períodos de tempo especificados (que são movidos do módulo Análise Inteligente para o módulo ANPR).
4. A plataforma oferecerá suporte à definição de uma regra de envio regular de relatórios de análise de veículos aos destinatários-alvo.
5. A plataforma oferecerá suporte ao reconhecimento de placas dos Emirados Árabes Unidos.
6. O usuário poderá definir a duração dos vídeos relacionados ao ANPR.

4.3 Gerenciamento do Sistema

- ***Configurações gerais***
- ***Segurança do Sistema***
- ***Gerenciamento de licenças***
- ***Outros***
- ***Compatibilidade de dados***

4.3.1 Configurações Gerais

A plataforma deverá suportar os seguintes recursos:

Início Rápido

- Exibindo instruções de novos recursos e notas de versão na página inicial.
- Barra de navegação totalmente nova (o menu de primeiro nível é exibido na parte superior; o menu de segundo e terceiro níveis é exibido à esquerda; as páginas de guias são exibidas à direita).
- Guia de configuração rápida para Controle de Acesso e Controle de Ponto.
- Até 20 inicializações rápidas para diferentes funções.
- Centro de downloads e centro de tarefas.

Painel

O Painel oferecerá suporte à exibição dos seguintes dados e à execução das seguintes tarefas:

- Estatísticas de pessoas, dispositivos e resultados de atendimento.
- Tarefas pendentes do fluxo de solicitação de presença.
- Eventos em tempo real e notificações de alarme.
- O Status da Credencial da Pessoa, o Status do Dispositivo e o Relatório de Presença na página inicial permitem clicar no gráfico de pizza para obter detalhes.

Acesso Rápido a Funções Comuns

O acesso rápido às funções comuns deve oferecer suporte aos seguintes recursos:

1. Funções comuns do sistema
   a. Adicionando rapidamente dispositivos de controle de acesso.

   b. Adicionando rapidamente dispositivos de videoporteiro.
   c. Adicionando pessoas rapidamente.
   d. Obtendo rapidamente informações pessoais de dispositivos.
   e. Configuração de gravação de pré e pós gravação nos dispositivos remotos.
   f. Configuração de Taxa de Quadros, Resolução, Compressão, Bitrate nos dispositivos remotos.
2. Funções comuns de controle de acesso
   a. Importação rápida de eventos de controle de acesso de dispositivos.
   b. Atribuição rápida de níveis de acesso a pessoas.
3. Funções comuns de atendimento
   a. Agendamento rápido.
   b. Visualização rápida do cartão de ponto total.
   c. Visualizando rapidamente os detalhes semanais.
   d. Visualizando rapidamente os detalhes mensais.

Sistema

1. Autoadaptável a telas com diferentes resoluções.
2. Personalizar itens de coluna de tabelas em toda a plataforma e salvar automaticamente os itens de coluna selecionados.
3. Exibindo colunas de tabelas completas ou incompletas.

Preferência do Usuário

1. Definindo o nome do site.
2. Definir o primeiro dia da semana.
3. Definir a unidade de temperatura exibida para a plataforma, incluindo Celsius, Fahrenheit e Kelvin.
4. Definir se as funções relacionadas à máscara devem ser exibidas.
5. Definir o tipo de calendário exibido para a plataforma, incluindo calendário gregoriano, calendário tailandês e calendário nepalês.

Configurações da Impressora

Adicionando impressoras à plataforma.

Modelo de Cartão

Configurando modelos para impressão de cartões.

Configurações de Rede

1. Sincronizando o tempo.
2. Configurando o domínio do AD (Active Directory) para sincronizar informações pessoais.
3. Fornecendo protocolos para dispositivos acessando a plataforma. Os tipos de protocolo suportados incluem o protocolo ONVIF e ISUP v5.0 ou abaixo.
4. Configurando portas para acesso WAN.
5. Redefinindo informações de rede do dispositivo.

Configurações de Armazenamento

1. Definir o local de armazenamento local, a cota de imagens ou arquivos e a estratégia de substituição de imagens e arquivos.
2. Definir o período de retenção (unidade: ano) para os dados gerais (como eventos, logs) e os dados de função (como registros de leitura de cartão).

Outras Configurações

1. Estabelecendo feriados e a estratégia de repetição. O tipo de feriado inclui feriado regular (por exemplo, May Day) e feriado irregular (por exemplo, Mother's Day).
2. Definir modelos de e-mail (incluindo destinatários, assunto e conteúdo) para enviar regularmente relatórios ou eventos/alarmes às pessoas relacionadas.

Configurações de Fuso Horário

1. Lendo a lista de fusos horários do sistema operacional.
2. Definir o fuso horário para dispositivos e obter o fuso horário do dispositivo.

Gestão de Organização Multinível

1. Até 10 níveis inferiores de uma organização exibidos como uma estrutura de árvore.
2. Informações básicas: grupo de origem, nome da organização e descrição.

4.3.2 Segurança do Sistema

Segurança do Sistema

1. Suporte para configuração do protocolo de transferência para HTTPS e configuração do endereço IP para receber informações do dispositivo
2. Suporte para configuração de senha para o banco de dados local
3. Suporte para visualização do certificado do componente de serviço, incluindo Serviço de Streaming e Serviço de Armazenamento em Nuvem.
4. Suporte para definição de estratégia de segurança para login, incluindo bloqueio de endereço IP se as tentativas de login com falha excederem o limite, habilitação de idade máxima de senha, bloqueio automático do Control Client após o período de inatividade definido e configuração de autenticações duplas

Segurança do Usuário

1. Suporte para configuração de permissões para funções, incluindo permissões de acesso a recursos, permissões de recursos, permissões de configuração e operação, status do usuário (inativar ou ativar) e período efetivo da função
2. Suporte para adicionar manualmente usuários e grupos de usuários, importar usuários de domínio do AD (Activate Directory), ativar ou desativar usuários, forçar logout e assim por diante
3. Suporte para habilitar a atualização automática no Web Client para permitir que os clientes sejam atualizados automaticamente caso haja novas versões disponíveis.
4. Suporte a atrelar uma conta de usuário a endereçamento MAC com data de experiação do

acesso.

4.3.3 Backup e Restauração de Dados

A plataforma deverá suportar as seguintes funções:
1. Faça backup dos dados no PC local, incluindo dados de configuração e registros.
2. Restaurar dados.
3. Faça backup dos dados no servidor FTP, incluindo dados de configuração e registros.

4.3.4 Sistema Hot Spare

Rose quente sobressalente
Suporte para habilitar a função hot spare e definir a propriedade hot spare (servidor host e servidor reserva).

4.3.5 Gerenciamento de Licenças

Gestão Básica

1. Suporte para ativação de licenças no modo online ou offline
2. Suporte para atualização de licenças no modo online ou offline
3. Suporte para desativação de licenças no modo online ou offline
4. Suporte para visualizar os detalhes da licença

Configurações do Aviso de Expiração do SSP

Suporte para configuração do prompt de expiração (atualização ou adição de valores) para SSP (Software Service Program)

Configurações da Licença da Câmera

Suporte para configuração de licenças de câmera de reconhecimento facial, câmera ANPR e câmera térmica para reconhecimento facial, reconhecimento de placa e relatório de temperatura

Detecção de Exceção de Licença

1. Suporte para detectar se o arquivo de licença está danificado
2. Suporte para detectar se o número de recursos excedeu o limite
3. Suporte para detectar se o código de ativação básico está disponível
4. Suporte para detectar se há vários códigos de ativação básicos anormais
5. Suporte para detectar se a atualização é limitada
6. Suporte para detectar se a exceção ocorreu ao atualizar a licença
7. Suporte para restaurar o servidor após a ocorrência da exceção

Ativação do Serviço de Computação em Nuvem

1. Suporte para ativação do Amazon Web Service (AWS) e Microsoft Azure
2. Suporte para ativação de serviço em nuvem, exceto Amazon Web Service (AWS) e Microsoft

Azure

4.3.6 Outros

Aviso de Expiração do SSP

Suporte para configuração de prompt de expiração de SSP para enviar um e-mail de lembrete ao usuário quando o SSP ou SUP estiver prestes a expirar

Informações da Empresa

Suporte para configuração das informações da empresa

4.3.7 Compatibilidade de Dados

A plataforma suportará a importação de arquivos de configuração (incluindo informações sobre dispositivos, pessoas e eventos) do iVMS-4200 e do iVMS-4200 AC.

4.4 Manutenção

- ***Relatório Agendado***
- ***Gerenciamento de Rede de Servidores***
- ***Monitoramento de Saúde***
- ***Status do Recurso***
- ***Log do Sistema***

4.4.1 Relatório Agendado

Suporte ao cálculo regular de logs de recursos e logs de dispositivos, além de suporte ao envio de relatórios por e-mail.

4.4.2 Gerenciamento de Rede de Servidores

Limite de Uso do Servidor

1. Suporte para configuração de limites de uso de CPU e RAM de todo o servidor.
2. Suporte ao monitoramento do uso de CPU e RAM em tempo real.

Tempo Limite da Rede

Suporte para configuração de timeout de solicitação de interação de acordo com o status da rede. O timeout padrão é 60s, que pode ser configurado como 90s ou 120s.

Frequência de Verificação de Saúde

1. Suporte para verificação de status do dispositivo e do serviço.
    a. Dispositivo: dispositivo de codificação, dispositivo de controle de acesso, dispositivo de

controle de elevador, dispositivo de interfone de vídeo, dispositivo de controle de segurança, estação de acoplamento e dispositivo de rede.

b.Servidor: servidor de gravação e servidor de análise inteligente.

c.Frequência de verificação: minuto, hora, dia (mínimo: 1 minuto; máximo: 30 dias; padrão: 3 minutos).

2. Suporte para verificação de recursos do dispositivo.
   Frequência de verificação: minuto, hora, dia (mínimo: 1 minuto; máximo; 30 dias; padrão: 3 minutos).
3. Suporte para verificação do status da gravação.
   Frequência de verificação: minuto, hora, dia (mínimo: 1 minuto; máximo; 30 dias; padrão: 3 minutos).
4. Suporte para habilitar alarme/evento.
   Frequência de verificação: minuto, hora, dia (mínimo: 1 minuto; máximo: 30 dias; padrão: 3 minutos).

4.4.3 Monitoramento de Saúde

Visão Geral em Tempo Real

1. Suporte para exibição de status do dispositivo (normal e exceção), exibição de status do servidor e do recurso (normal, exceção e aviso). (Detalhes do status da câmera: câmera offline, perda de vídeo, exceção de comunicação, exceção de gravação, nenhuma programação de gravação configurada e exceção de armar).
2. Suporte para atualização manual e atualização regular do status do dispositivo, recurso e servidor.
3. Suporte para configuração de atualização regular no cliente móvel (por padrão, atualização regular no cliente web a cada 3 minutos).
4. Suporte à exportação de dados de todos os status do dispositivo e status dos recursos no formato EXCEL ou CSV.
5. Suporte à exportação dos dados selecionados (todos os dados ou dados de exceção).
6. Suporte à exportação somente de topologia ou topologia com dados quando houver topologia.
7. Suporte para mostrar e atualizar a hierarquia de topologia da rede.
8. Suporte para aumentar e diminuir o zoom da topologia, ampliar a visualização, tela cheia e autoadaptável.
9. Suporte à busca de localização de recursos e caminho de conexão.
10. Suporte para visualização de detalhes, configuração remota e registros de dispositivos.
11. Suporte à exibição de dados normais e de exceção do System Management Server.
12. Suporte para exibição em tempo real de CPU, RAM, espaço de armazenamento de imagens, rede (envio e recebimento) e gateway de streaming.
13. Suporta exibição em lote de status de câmeras, codificadores e decodificadores em sites remotos RSM.
14. Suporte para exibição do status da rede (de ruim a bom) para o Smart Managed Switch.

Visão Geral da História

1. Suporte para visualização da taxa de recurso on-line.
2. Suporte à classificação de recursos por total de tempo offline e tempo offline.
3. Suporte para visualização de taxa de dispositivo on-line.
4. Suporte para classificação de dispositivos por tempo total offline e offline.
5. Suporte ao redirecionamento para a página de Logs do dispositivo.
6. Suporte para visualização da taxa de integridade da gravação.
7. Suporte para atualização manual.
8. Suporte à exportação de dados (todos os dados ou dados de exceção) no formato EXCEL ou CSV.
9. Suporte à exportação dos dados selecionados (todos os dados ou dados de exceção).

4.4.4 Status do Recurso

Porta

1. A plataforma oferecerá suporte ao status da porta (status da rede, status da rede do terminal de reconhecimento facial, status da porta, status da porta configurada e status do leitor de cartão) e ao horário de verificação.
2. A plataforma suportará atualização manual e atualização regular
3. A plataforma suportará a exportação de dados de status de portas.
4. A plataforma deverá suportar a visualização de detalhes da porta.
5. A plataforma oferecerá suporte à visualização do status dos terminais de reconhecimento facial.
6. A plataforma deve suportar a visualização do status do leitor de cartão.
7. A plataforma suportará o controle remoto do status da porta.

Elevador

1. A plataforma oferecerá suporte à visualização do status da porta (status da rede e status do leitor de cartão) e à verificação do horário.
2. A plataforma suportará atualização manual e atualização regular
3. A plataforma suportará a exportação de dados de status do elevador.
4. A plataforma oferecerá suporte à visualização do status dos recursos do elevador.
5. A plataforma deve suportar a visualização do status do leitor de cartão.

Câmera

1. A plataforma suportará a visualização do status da câmera (sinal de vídeo, status de gravação e status de armação).
2. A plataforma oferecerá suporte à atualização manual e regular.
3. A plataforma suportará a exportação de dados de status da câmera.
4. A plataforma oferecerá suporte à visualização de detalhes dos recursos da câmera.
5. A plataforma oferecerá suporte à visualização do status da câmera no Site Remoto.
6. A plataforma suportará a visualização do resultado do diagnóstico de imagem da câmera.
7. A plataforma oferecerá suporte à visualização do relatório de dados móveis da câmera solar.

Dispositivo de Controle de Acesso

1. A plataforma oferecerá suporte à visualização do status do dispositivo de controle de acesso (status da rede, rede do controlador da faixa principal/secundária, componente, status de armação, violação e central de chamadas do dispositivo) e verificação de tempo.
2. A plataforma oferecerá suporte à atualização manual e regular.
3. A plataforma oferecerá suporte à exportação de dados de status do dispositivo de controle de acesso.
4. A plataforma oferecerá suporte à visualização de detalhes do dispositivo e informações detalhadas dos recursos vinculados (porta e câmera).

Dispositivo de Controle do Elevador

1. A plataforma oferecerá suporte à visualização do status do dispositivo de controle do elevador (status da rede, status da bateria, status de armação e status do dispositivo de controle do elevador distribuído) e à verificação do tempo.
2. A plataforma suportará atualização manual e atualização agendada
3. A plataforma suportará a exportação de dados do status do dispositivo de controle do elevador.
4. A plataforma deve suportar a visualização de detalhes do dispositivo de controle do elevador.
5. A plataforma suportará o controle remoto do elevador.

Dispositivo de Intercomunicação de Vídeo

1. A plataforma oferecerá suporte à visualização do status do dispositivo de interfone com vídeo (status da rede, status de armação e central de chamadas do dispositivo) e à verificação da hora.
2. A plataforma oferecerá suporte à atualização manual e regular.
3. A plataforma suportará a exportação de dados de status do dispositivo de videoporteiro.
4. A plataforma oferecerá suporte à visualização de detalhes do dispositivo de interfone com vídeo.
5. A plataforma suportará discagem no Cliente Móvel para estação interna.

Entrada de Alarme

1. A plataforma oferecerá suporte à visualização do status de entrada do alarme (nome, área, número de série, versão, status do disco, status da rede, status de armação e primeira hora adicionada) e verificação da hora.
2. A plataforma oferecerá suporte à atualização manual e regular.
3. A plataforma suportará a exportação de dados de status de entrada de alarme.
4. A plataforma oferecerá suporte à visualização de detalhes do recurso de entrada de alarme.
5. A plataforma suportará a visualização do status de entrada do alarme de acordo com o tipo de dispositivo.

UVSS

1. A plataforma oferecerá suporte à visualização do status do UVSS (status da rede, status da câmera de varredura de linha, status da câmera de captura e status de armazenamento) e verificação de tempo.

2. A plataforma deve suportar atualização manual e atualização regular. A plataforma deve suportar atualização manual e atualização regular.
3. A plataforma oferecerá suporte à exportação de dados de status do UVSS.
4. A plataforma oferecerá suporte à visualização de detalhes do UVSS

Recurso Optimus

1. A plataforma suportará a visualização do status dos recursos do Optimus (status da rede e status dos recursos) e do fabricante.
2. A plataforma oferecerá suporte à atualização manual e regular.
3. A plataforma suportará a exportação dos dados de status dos recursos do Optimus.
4. A plataforma oferecerá suporte à visualização dos detalhes dos recursos do Optimus.

Servidor de Streaming

1. A plataforma oferecerá suporte à visualização do status do servidor de mídia de transmissão (transmissões totais, transmissões de entrada, transmissões de saída, uso da CPU e uso da RAM) e à verificação do tempo.
2. A plataforma oferecerá suporte à atualização manual e regular.
3. A plataforma suportará a exportação de dados do status do servidor de mídia de streaming.
4. A plataforma oferecerá suporte à visualização de detalhes do servidor de mídia de streaming.

Servidor de Gravação

1. A plataforma oferecerá suporte à visualização do status do servidor de gravação (status da rede, uso da CPU, uso da RAM, propriedades de hot spare, status da gravação, status do hardware, uso do HDD) e verificação do tempo.
2. A plataforma oferecerá suporte à atualização manual e regular.
3. A plataforma suportará a exportação de dados de status do servidor de gravação.
4. A plataforma oferecerá suporte à visualização de detalhes do servidor de gravação.

Servidor de Análise Inteligente

1. A plataforma oferecerá suporte à visualização do uso da CPU e da RAM do Intelligent Analysis Server e à verificação do tempo.
2. A plataforma oferecerá suporte à atualização manual e regular.
3. A plataforma oferecerá suporte à exportação de dados de status do Intelligent Analysis Server.
4. A plataforma oferecerá suporte à visualização de detalhes do Intelligent Analysis Server.

Dispositivo de Codificação

1. A plataforma oferecerá suporte à visualização do status do dispositivo de codificação (status da rede, uso do HDD, status da gravação, fabricante, propriedades de hot spare, matriz de disco, status de armação) e verificação de tempo.
2. A plataforma oferecerá suporte à atualização manual e regular.
3. A plataforma oferecerá suporte à exportação de dados de status do dispositivo de codificação.
4. A plataforma oferecerá suporte à visualização de detalhes do dispositivo de codificação.
5. A plataforma oferecerá suporte à visualização do status da bateria da câmera solar.
6. A plataforma oferecerá suporte à visualização de detalhes da câmera.

7. A plataforma oferecerá suporte à alternância de tipo de fluxo e modo de acesso no Mobile Client.
8. A plataforma suportará a visualização do status N+1 do NVR.

Dispositivo de Controle de Segurança

1. A plataforma oferecerá suporte à visualização do status do dispositivo de alarme (status da rede, status da bateria e status de armação) e à verificação da hora.
2. A plataforma oferecerá suporte à atualização manual e regular.
3. A plataforma suportará a exportação de dados de status do dispositivo de alarme.
4. A plataforma oferecerá suporte à visualização de detalhes do dispositivo de alarme.

Estação de Atracação

1. A plataforma oferecerá suporte à visualização do status da estação de acoplamento (status da rede e uso do HDD) e à verificação do tempo.
2. A plataforma oferecerá suporte à atualização manual e regular.
3. A plataforma oferecerá suporte à exportação de dados de status da estação de acoplamento.
4. A plataforma oferecerá suporte à visualização de detalhes da estação de atracação.

Dispositivo de Bordo

1. A plataforma oferecerá suporte à visualização do status do dispositivo de bordo, como o status da rede.
2. A plataforma oferecerá suporte à exportação de dados de status do dispositivo de bordo.

Dispositivo de Transmissão de Rede

1. A plataforma suportará o status do dispositivo de transmissão de rede (status da rede, uso de POE) e a hora de verificação.
2. A plataforma oferecerá suporte à atualização manual e regular.
3. A plataforma oferecerá suporte à exportação de dados de status do dispositivo de rede.
4. A plataforma oferecerá suporte à visualização do status do dispositivo de transmissão de rede (status da rede, uso da CPU, uso da RAM, portas ocupadas, uso de PoE, exceção do dispositivo como primeira vez adicionada) e verificação de tempo.

Dispositivo de Decodificação

1. A plataforma oferecerá suporte à visualização do status da rede do dispositivo de decodificação e à verificação do tempo.
2. A plataforma oferecerá suporte à atualização manual e regular.
3. A plataforma suportará a exportação de dados de status do dispositivo de decodificação.
4. A plataforma oferecerá suporte à visualização de detalhes do dispositivo de decodificação.

Alto-Falante IP

1. A plataforma oferecerá suporte à visualização do status do palestrante IP.
2. A plataforma oferecerá suporte à exportação de dados de status do alto-falante IP.
3. A plataforma oferecerá suporte à visualização de detalhes dos recursos do alto-falante IP.

Dispositivo de Inspeção de Segurança

1. A plataforma oferecerá suporte à visualização do status do dispositivo de inspeção de segurança.
2. A plataforma oferecerá suporte à exportação de dados de dispositivos de inspeção de segurança.
3. A plataforma oferecerá suporte à visualização de detalhes dos recursos do dispositivo de inspeção de segurança.

Dispositivo BACnet

1. A plataforma oferecerá suporte à visualização do status do dispositivo BACnet.
2. A plataforma oferecerá suporte à exportação de dados de status do dispositivo BACnet.
3. A plataforma oferecerá suporte à visualização de detalhes dos recursos do dispositivo BACnet.

Terminal de Sinalização Digital

1. A plataforma oferecerá suporte à visualização do status do terminal de sinalização digital.
2. A plataforma oferecerá suporte à exportação de dados de status do terminal de sinalização digital.
3. A plataforma oferecerá suporte à visualização de detalhes dos recursos do terminal de sinalização digital.

Painel Plano Interativo

1. A plataforma oferecerá suporte à visualização do status do painel plano interativo.
2. A plataforma oferecerá suporte à exportação de dados de status do painel plano interativo.
3. A plataforma oferecerá suporte à visualização de detalhes de recursos de tela plana interativa.

Site Remoto

1. A plataforma oferecerá suporte à visualização do status do site remoto (status da rede e fluxo padrão) e à verificação do tempo.
2. A plataforma oferecerá suporte à atualização manual e regular.
3. A plataforma oferecerá suporte à exportação de dados de status de sites remotos.
4. A plataforma oferecerá suporte à visualização de detalhes do site remoto.
5. A plataforma suportará a alternância do tipo de fluxo (fluxo principal/subfluxo) e do modo de acesso (conexão direta ou proxy) no Mobile Client.
6. A plataforma oferecerá suporte à visualização de cronogramas de gravação configurados e status de gravação de sites remotos.

4.4.5 Log do Sistema

Logs do Servidor

1. Suporte à busca do log de acordo com o Site Remoto, tipo de log, gatilho de log, recurso filtrado e tempo selecionado.
2. Suporte à exportação de logs de sites remotos e logs do sistema central em formato EXCEL ou CSV.

Registros do Dispositivo

1. Suporte à busca de logs locais de dispositivos de codificação, dispositivos de controle de segurança, dispositivos de decodificação, dispositivos de controle de acesso, dispositivos de controle de elevador e dispositivos de rede.
2. Suporte à exportação de logs locais do dispositivo.
3. Suporte à exportação de logs online/offline de vários dispositivos.
4. Suporte à exportação de logs online/offline para o dispositivo.
5. Suporte à exibição por gráfico e lista de registros de duração do dispositivo online e do último tempo offline.

Registros de Recursos

1. Suporte à busca de status de gravação de recurso.
2. Suporte para visualização do status da gravação em cada ponto do tempo.
3. Suporte para busca de log online/offline.
4. Suporte à exibição por gráfico e lista de registros de duração do dispositivo online e do último tempo offline.
5. Suporte à exportação de logs de recursos.

Registros de Manutenção

1. Suporte à busca de logs de manutenção de acordo com o nome da tarefa pendente, objetos passando pela verificação de integridade, nível de risco, manipulador, tempo de tratamento e status de tratamento.
2. Suporte para visualização de logs de manutenção.
3. Suporte à exportação de logs de manutenção.

4.4.6 Verificação de Saúde

Visão Geral da Saúde

1. Suporte para visualização do último resultado da verificação, incluindo o horário da última verificação e a visão geral do problema.
2. Suporte para visualizar as tarefas pendentes anteriores.

Verificação Manual

1. Suporte à verificação manual do status de integridade de dispositivos, sistemas e serviços.
2. Suporte à verificação de vários itens, incluindo pré-alarmes de operação de plataforma, exceções de recebimento de registros, dispositivos ou recursos offline, exceções de bateria de energia do dispositivo, exceções de disco ou HDD, segurança do dispositivo, exceções de componentes do dispositivo, exceções de configuração de alarme de evento, exceções de configuração de relatório agendado, exceções de gravação de vídeo e exceções de imagem de vídeo.
3. Suporte para visualização dos resultados da verificação, incluindo nome do item, descrição do item, sugestão de manuseio, nível de risco e hora da verificação.
4. Suporte para ignorar certos itens de verificação, e os itens ignorados serão ignorados nas

verificações seguintes.
5. Suporte para visualização dos resultados da verificação de acordo com o tipo e o objeto da verificação.
6. Suporte à filtragem dos resultados da verificação pelas seguintes condições: item de verificação, tipo de objeto de verificação, nível de risco, status de tratamento e condições personalizadas.
7. Suporte para ignorar determinados itens de verificação ou adicionar itens de verificação em lote à lista de tarefas pendentes.
8. Suporte para exportação da lista de resultados de verificação.

Tarefa Pendente

1. Suporte para visualização de tarefas pendentes importadas.
2. Suporte para edição do nome da tarefa pendente, nível de risco e nota.
3. Suporte ao processamento em lote, ignorando, excluindo, exportando tarefas pendentes e definindo notificações por e-mail.
4. Suporte para adicionar tarefas pendentes personalizadas.

Verificação de Saúde Agendada

Suporte à configuração de verificações de integridade agendadas, incluindo o item de verificação, o período de verificação e o envio automático do relatório de verificação de integridade.

4.5 Painel de Controle

Funções Básicas

1. Suporte para registro por endereço IP ou nome de domínio e suporte para habilitar login automático
2. Suporte para lembrar endereços históricos de servidores e usuários conectados
3. Suporte para agrupamento de módulos e personalização do arranjo dos módulos no painel de controle
4. Suporte para adicionar módulos à barra de navegação, clicar em um módulo na barra de navegação para acessar rapidamente o módulo e pesquisar módulos
5. Suporte para exibir o indicador de atualização de recursos, tempo e uso da CPU/velocidade da rede na barra de título do Control Client
6. Forneça orientação sobre como começar a usar o Control Client para o usuário que faz o primeiro login

Operações do Painel de Controle

1. Suporte para exibir o painel de controle padrão para o usuário de primeiro login
2. Suporte para edição do nome e do layout (incluindo adição de janelas, exclusão de janelas, edição de janelas, movimentação de janelas e ajuste do tamanho da janela) do painel de controle
3. Suporte para restauração do painel de controle padrão durante a edição
4. Suporta layout autoadaptável com base em diferentes resoluções de tela

5. Suporte ao gerenciamento de vários painéis de controle, incluindo adição, exclusão e troca de painéis de controle
6. Suporte para abertura e fechamento de tela auxiliar para o painel de controle
7. Suporte para exibir o painel de controle no modo de tela cheia e sair do modo, maximizar ou minimizar a janela e exibir a janela na tela auxiliar
8. Suporte para restaurar o painel de controle após reiniciar o Control Client ou alternar usuários

Configuração do Sistema e Ajuda

1. Suporte para configuração de parâmetros gerais, incluindo parâmetros de rede, modo de exibição em grande escala, modo máximo e caminho para salvar arquivos
2. Suporte para alternar modos de página inicial, incluindo Modo de Menu e Modo de Visualização. As configurações entrarão em vigor após reiniciar o Control Client.
3. Suporte para exibir as informações da licença da plataforma

4.6 Vídeo Básico

- ***Gerenciamento de sistemas e recursos***
- ***Segurança de vídeo***
- ***Pesquisa e exportação de vídeos***
- ***Gerenciamento de Permissões***
- ***Gestão de Evidências***
- ***Evento e Alarme***
- ***Estação de encaixe e câmera corporal***

4.6.1 Gerenciamento de Sistemas e Recursos

Gerenciamento de Rede

1. A plataforma deve suportar a descoberta de dispositivos online. A plataforma deve suportar a descoberta de dispositivos na mesma rede que o cliente para que os dispositivos possam ser adicionados em LAN/WAN.
2. A plataforma oferecerá suporte à adição de dispositivos de codificação por endereço IP, nome de domínio e Hik-Connect NNDS via ISUP para que os dispositivos possam ser adicionados em LAN/WAN.
3. A plataforma suportará a adição de dispositivos de um segmento de rede diferente que pode ser acessado pelo servidor.
4. A plataforma suportará a adição de dispositivos de codificação por IPv4/IPv6.

Hora e DST

1. A plataforma deve suportar a configuração manual do fuso horário e a obtenção do fuso horário do dispositivo. A plataforma deve suportar a configuração do horário do Cliente/Horário do Servidor como o horário do Cliente.
2. A plataforma deve suportar o horário de verão. A plataforma deve suportar a marcação do vídeo repetido causado pelo horário de verão.

Gerenciamento de Dispositivos

1. A plataforma oferecerá suporte à adição de câmeras Hikvision, NVRs e DVRs.
2. A plataforma oferecerá suporte à adição de câmeras por meio de interface de vídeo em rede aberta.
3. A plataforma oferecerá suporte à adição de câmeras corporais.
4. A plataforma suportará a adição de estações de acoplamento.
5. A plataforma suportará a importação de canais gerenciados no Hik-Partner Pro.
6. A plataforma oferecerá suporte à importação de dispositivos Dahua.
7. A plataforma oferecerá suporte à exibição de detalhes do dispositivo, como número de série, versão do firmware e informações sobre câmeras vinculadas, entrada de alarme e saída de alarme.
8. . Consulte ***Manutenção .***
9. A plataforma oferecerá suporte à exibição de detalhes do dispositivo para gerenciamento de dispositivos, incluindo o número de série do dispositivo, versão do firmware, canais de câmera suportados pelos dispositivos de codificação, entradas de alarme e saídas de alarme.

Gerenciamento de Servidor

1. A plataforma suportará servidor de streaming de mídia.
2. A plataforma oferecerá suporte a servidores de armazenamento como pStor Cluster Service, Hybrid SAN, Cluster Storage e NVR (somente para armazenamento de imagens).
3. A plataforma suportará servidor de análise inteligente.
4. A plataforma deve suportar o monitoramento da capacidade de armazenamento do disco local. A plataforma deve suportar a visualização dos canais configurados com servidores de armazenamento. A plataforma deve suportar a exibição da versão do servidor. A plataforma deve suportar ir para a página de configuração dos servidores de armazenamento.

Gestão de Recursos

1. A plataforma suportará o agrupamento de dispositivos de codificação, incluindo câmeras e entradas/saídas de alarme.
2. A plataforma suportará a adição em lote de recursos, como câmeras, entradas/saídas de alarmes ao E-map para visualizar os efeitos do monitoramento.
3. A plataforma oferecerá suporte à configuração remota de dispositivos.
4. A plataforma oferecerá suporte à alteração em lote de senhas de dispositivos.
5. A plataforma suportará aplicação em lote e obtenção de nomes de canais.
6. A plataforma suportará a obtenção em lote de predefinições configuradas de câmeras PTZ.
7. A plataforma suportará a obtenção em lote do cronograma de gravação configurado dos dispositivos.
8. A plataforma suportará a cópia em lote dos parâmetros da câmera para atender aos requisitos de gerenciamento multicanal em vários dispositivos.

Atualização de Firmware em Lote

1. A plataforma suportará atualização via Web Client atual, via Hik-Connect, via FTP. A plataforma suportará exibição de status de atualização.
2. A plataforma suportará a atualização de dispositivos por meio da rede do servidor e da rede do

cliente.

Configuração de Armazenamento Confiável e Flexível

1. A plataforma deve suportar a configuração de parâmetros para armazenar vídeos. A plataforma deve suportar a configuração do tipo de fluxo, programação de gravação de tempo ou evento e o tempo expirado do vídeo.
2. A plataforma deve suportar a configuração de definições de armazenamento de vídeo. A plataforma deve suportar o armazenamento de vídeo em tempo real em dispositivo de codificação/pStor/CVR/servidor de armazenamento em nuvem.
3. A plataforma deve suportar a configuração de definições de armazenamento de imagens. A plataforma deve suportar o armazenamento de imagens no servidor local/dispositivo de codificação/pStor/CVR/servidor de armazenamento em nuvem.
4. A plataforma deve suportar a configuração do cronograma de gravação em tempo real. A plataforma deve suportar a configuração do dispositivo de codificação/pStor/CVR/servidor de armazenamento em nuvem como o armazenamento principal e pStor/CVR/armazenamento em nuvem como o armazenamento auxiliar.
5. A plataforma deve suportar a configuração de gravação copy-back. A plataforma deve suportar a configuração de dispositivo de codificação/pStor/CVR/servidor de armazenamento em nuvem como o armazenamento principal, e pStor/CVR/armazenamento em nuvem como o armazenamento auxiliar.
6. A plataforma suportará a configuração de N+1 hot spare para NVR para aumentar a responsabilidade do armazenamento de vídeo.
7. A plataforma suportará a configuração do cluster pStor e do hot spare N+1 para CVR.
8. A plataforma deve suportar a configuração do horário de início/término do envio do vídeo gravado pelo CVR de volta para a plataforma. A plataforma deve suportar o envio do vídeo gravado anteriormente de volta para a plataforma.
9. A plataforma deve suportar o gerenciamento do servidor CVR, servidor de nuvem, pStor. A plataforma deve suportar a adição deles, visualizar o status do armazenamento, visualizar os canais configurados para o servidor, exibir a versão do servidor e pular para a página da web para configurar os servidores de armazenamento. A plataforma deve suportar o gerenciamento de servidores de gravação (servidor CVR, servidor de nuvem e pStor).

Gerenciamento de Fluxo

1. A plataforma suportará streaming diretamente do dispositivo, para que os dispositivos e o Cliente possam trabalhar na mesma LAN.
2. A plataforma oferecerá suporte a streaming por meio da mídia de streaming interna do HikCentral Professional para que vários clientes possam transmitir de um dispositivo simultaneamente, o usuário na WAN possa acessar o dispositivo na LAN e o HCP possa transmitir de dispositivos acessados na plataforma via ISUP.
3. A plataforma deve suportar a adição de um Stream Media Server externo. A plataforma deve suportar streaming de um stream media server externo designado.
4. A plataforma oferecerá suporte à configuração do modo de transmissão para dispositivo e cliente.

Gerenciamento de Largura de Banda

1. A plataforma deve suportar o fluxo suave. A plataforma deve suportar o início da visualização/reprodução ao vivo no fluxo suave, que pode se autoadaptar à largura de banda.
2. A plataforma suportará ajuste automático de transmissão alternando entre transmissão principal/secundária/suave na visualização ao vivo.
3. A plataforma deve suportar a alternância para subfluxo na reprodução se a gravação de fluxo duplo estiver configurada.
4. A plataforma deve suportar download de largura de banda. A plataforma deve suportar configuração em lote da largura de banda máxima de download de vídeo do NVR para o Cliente.
5. A plataforma deve suportar o download de largura de banda do Cliente. A plataforma deve suportar a configuração da largura de banda máxima de download de vídeos do pStor para o Cliente.
6. A plataforma deve suportar atualização de firmware em lote. A plataforma deve suportar configuração da quantidade máxima de firmware que é atualizada simultaneamente.
7. A plataforma deve suportar a cópia de largura de banda de volta. A plataforma deve suportar a configuração da largura de banda máxima de cópia de vídeo de volta.

Segurança de Rede

1. A plataforma deve suportar criptografia de fluxo. Os usuários só poderão iniciar a visualização/reprodução ao vivo após inserir a chave de criptografia.
2. A plataforma oferecerá suporte à alteração em lote de senhas de dispositivos.

4.6.2 Segurança de Vídeo

Exibir Status do Canal

1. A plataforma oferecerá suporte à visualização de miniaturas de câmeras na árvore de recursos.
2. A plataforma deve suportar a exibição do número de câmeras online / câmeras totais em cada área na árvore de recursos. A plataforma deve suportar somente a exibição de câmeras online.
3. A plataforma oferecerá suporte à exibição do status do alarme na árvore de recursos e no mapa, além da visualização dos detalhes do alarme.

Operação de Canal Único

1. A plataforma suportará arrastar a câmera do mapa para iniciar a visualização/reprodução ao vivo.
2. A plataforma suportará a localização de uma única câmera no mapa.
3. A plataforma suportará captura e busca de imagens VCA (dispositivos inteligentes).
4. A plataforma oferecerá suporte para ligar/desligar o áudio e ajustar o volume e, ao ligar o áudio, um prompt de status será exibido.
5. A plataforma oferecerá suporte à configuração para habilitar ou não o áudio por padrão para todos os canais.
6. A plataforma deve suportar a criação de uma área de zoom. A plataforma deve suportar rolar o mouse para dar zoom. A plataforma deve suportar a exibição de vídeos em miniatura.

7. A plataforma suportará áreas de armar/desarmar manualmente por câmeras para receber alarmes sonoros e visuais. A plataforma suportará a limpeza de alarmes sonoros e visuais.
8. A plataforma suportará a função PTRZ (panorâmica, inclinação, rotação e zoom).
9. A plataforma suportará aprimoramento de vídeo. A plataforma suportará ajuste de brilho, contraste, saturação e matiz.
10. A plataforma suportará a alternância do tipo de fluxo entre fluxo principal, subfluxo, fluxo suave e quarto fluxo.
11. A plataforma oferecerá suporte à alternância do tipo de fluxo entre fluxo principal, subfluxo e fluxo suave.
12. A plataforma deve suportar múltiplos modos de dewarping fisheye. A plataforma deve suportar expansão fisheye e seleção de modo de instalação. A plataforma deve suportar um máximo de 14 modos de expansão.
13. A plataforma suportará a exibição de vídeo na parede inteligente por meio de decodificador ou placa gráfica.
14. A plataforma deve suportar controle PTZ (somente em visualização ao vivo). A plataforma deve suportar tempo de bloqueio, limpadores únicos/em lote, posicionamento 3D, predefinições (obter predefinições do dispositivo, configuração e chamada), patrulha, padrão, foco, distância focal, íris, foco rápido, luz, inicialização de lente, rastreamento manual, captura manual de rosto, prioridade de controle configurável e ação de estacionamento.
15. A plataforma deve suportar reprodução instantânea (somente em visualização ao vivo); A plataforma deve suportar a seleção do tempo de reprodução: 30s, 1 min, 3 min, 5 min, 8 min e 10 min.
16. A plataforma suportará controle de saída de alarme.
17. A plataforma suportará áudio bidirecional.
18. A plataforma suportará a impressão de imagens capturadas.
19. A plataforma suportará busca imagem por imagem (dispositivos inteligentes).
20. A plataforma oferecerá suporte à exibição de informações da câmera: taxa de quadros, fluxo, padrão de vídeo, total de câmeras conectadas, status da rede, status do sinal, status do vídeo, modo de acesso, tipo de canal, nome do dispositivo, endereço IP, tipo de protocolo, armazenamento principal/auxiliar e área.
21. A plataforma suportará controle de armar: armar ou desarmar câmeras.
22. A plataforma suportará a criação de áreas de zoom e a exibição delas em uma nova janela.
23. A plataforma deve suportar marcação de vídeos. A plataforma deve suportar a configuração do intervalo de tempo e descrição para marcações.
24. A plataforma suportará análise de densidade de pessoas (servidor de análise inteligente).
25. A plataforma suportará pesquisa VCA.
26. A plataforma apoiará a ação do parque.
27. A plataforma suportará a exportação de arquivos de vídeo (somente em reprodução).
28. A plataforma suportará recortes de vídeo (somente em reprodução).
29. A plataforma suportará bloqueio de vídeo (somente na reprodução).
30. A plataforma suportará reprodução com extração de quadros.
31. A plataforma suportará a rotação de uma imagem.
32. A plataforma suportará a geração de imagens panorâmicas de RV e o clique para visualizar uma imagem específica.

33. A plataforma oferecerá suporte à adição de câmeras com o recurso de varredura de perímetro e à execução de operações de ROI.
34. A plataforma oferecerá suporte à captura de imagens em tempo real e à visualização de vídeos relacionados de acordo com as imagens capturadas.
35. A plataforma deve suportar a exibição de câmeras corporais no Google Map. A plataforma deve suportar a exibição de câmeras corporais em uma área selecionada.

Shortcuts

1. A plataforma deve suportar operação de atalho. A plataforma deve suportar habilitar/desabilitar expansão fisheye, captura manual, gravação manual (somente em visualização ao vivo), zoom in/out, troca de fluxo, iniciar/parar visualização ao vivo e operações PTZ (somente em visualização ao vivo).
2. A plataforma oferecerá suporte à personalização do ID lógico da câmera.
3. A plataforma suportará a configuração de atalhos para diferentes funções.
4. A plataforma suportará pressionar Ctrl para selecionar câmeras de diferentes áreas para executar a troca automática e a visualização ao vivo de câmeras adicionadas a diferentes áreas.

Página da Internet

1. A plataforma suportará a adição de múltiplas páginas da web à janela de exibição.
2. A plataforma oferecerá suporte à adição de páginas da web aos Favoritos.

Visualização ao vivo

1. A plataforma suportará no máximo 64 câmeras em visualização ao vivo de janela única. A plataforma suportará no máximo 256 câmeras em visualização ao vivo de quatro janelas.
2. A plataforma deve suportar a visualização ao vivo inicial de uma ou mais câmeras.
3. A plataforma deve suportar janelas de troca automática com o intervalo de tempo de troca de 5s, 10s, 20s, 30s, 1min, 3min, 5min. A plataforma deve suportar pausar e reproduzir vídeos.
4. A plataforma suportará a exibição de eventos de passagem de veículos. A plataforma suportará a adição de número de licença do veículo à lista de placas do veículo.

Reprodução

1. A plataforma suportará a reprodução de no máximo 16 câmeras em visualização de janela única.
2. A plataforma deve suportar a exibição de dias com vídeo gravado. A plataforma deve suportar a reprodução de um determinado dia/hora. A plataforma deve suportar arrastar o controle deslizante de tempo.
3. A plataforma oferecerá suporte à filtragem de vídeo por tipo de vídeo (programação de gravação de tempo, programação de gravação de evento, gravação manual e gravação ANR), por tipo de tag (tag de evento, tag de gravação manual e outras tags) e por tipo de armazenamento.
4. A plataforma oferecerá suporte ao agrupamento de vídeos por pessoa e veículo, à marcação de pessoa e veículo no vídeo e à filtragem de vídeo de acordo com o tipo de aparência da pessoa ou do veículo.

5. A plataforma oferecerá suporte à exibição da imagem quando você arrastar o controle deslizante de tempo.
6. A plataforma suportará a alternância entre reprodução síncrona/assíncrona.
7. A plataforma deve suportar a exibição da imagem de vídeo em miniatura durante a reprodução. A plataforma deve suportar ir para o tempo correspondente se os usuários clicarem na miniatura.
8. A plataforma suportará a reprodução do vídeo nas velocidades de 1x, 2x, 4x, 8x, /2x, 1/4x e 1/8x.
9. A plataforma suportará busca de meio intervalo.
10. A plataforma oferecerá suporte para reprodução, pausa e reprodução normal/reversa de quadro único.

Rastreamento Visual

1. A plataforma oferecerá suporte à alternância de uma câmera atual para as câmeras associadas no modo de rastreamento visual durante a visualização ao vivo.
2. A plataforma oferecerá suporte à alternância de uma câmera atual para as câmeras associadas no modo de rastreamento visual durante a reprodução e à exportação do vídeo.
3. A plataforma oferecerá suporte à alternância para subfluxo para câmeras configuradas no rastreamento visual.
4. A plataforma oferecerá suporte à configuração para iniciar automaticamente a reprodução do vídeo gravado.

Gerenciamento de Visualização

1. A plataforma suportará visualização privada e visualização pública.
2. A plataforma oferecerá suporte para salvar visualizações durante a exibição ao vivo ou reprodução, além de oferecer suporte para salvar câmeras, divisões de janelas, predefinições, configurações de troca automática, configurações de zoom digital, mapa e página da web.
3. A plataforma deve suportar a adição de visualizações diretamente adicionando câmeras em lote em diferentes áreas. A plataforma deve suportar a configuração do tipo de fluxo de câmera. A plataforma deve suportar a configuração do intervalo de troca automática.
4. A plataforma oferecerá suporte à visualização de visualizações em miniatura.
5. A plataforma deve suportar arrastar uma câmera para a visualização para iniciar a visualização ao vivo ou a reprodução.
6. A plataforma deve suportar edição de visualizações. A plataforma deve suportar edição de intervalo de troca automática, pausa, mudança de visualização, edição de informações da câmera, etc. ao reproduzir o vídeo.
7. Suporta compartilhamento de visualizações privadas.
8. A plataforma oferecerá suporte à exibição de visualizações na parede inteligente.
9. A plataforma oferecerá suporte à configuração da visualização padrão no próximo login.

Favoritos

1. A plataforma oferecerá suporte para adicionar câmeras usadas com frequência aos Favoritos.
2. A plataforma oferecerá suporte ao compartilhamento de recursos com outros usuários e à exibição dos recursos favoritos que outros compartilharam com você.

3. A plataforma suportará troca automática de acordo com as visualizações nos Favoritos.

Diagnóstico de Falhas

1. A plataforma deve suportar a visualização de códigos de erro e mensagens de erro quando a inicialização da visualização ao vivo falhar. A plataforma deve suportar a ilustração do caminho de streaming detalhado. A plataforma deve suportar o status de saúde relacionado ao nó, logs e eventos de histórico. A plataforma deve suportar o envio de motivos de falha de operação.
2. A plataforma deve suportar a exibição de códigos de erro de reprodução, mensagens de erro, caminho de streaming. A plataforma deve suportar status de saúde relacionados ao nó, logs e eventos de histórico. A plataforma deve suportar o envio de motivos de falha de operação.

4.6.3 Pesquisa e Exportação de Vídeos

Pesquisa de Vídeo

1. Suporte para pesquisa por intervalo de tempo, tipo de fluxo, local de armazenamento e segmentação de vídeo.
2. Suporte para pesquisa por tag e palavra-chave.
3. Suporte à busca de imagens de vídeo acionadas por eventos de transação que contenham informações de PDV.
4. Suporte à busca de imagens de vídeo acionadas pelo evento ATM.
5. Suporte à busca de arquivos de vídeo onde ocorrem eventos VCA. Eventos VCA incluem análise dinâmica, cruzamento de linha e detecção de intrusão.
6. Suporte para busca de filmagens de vídeo bloqueadas da câmera.

Exportação de Vídeo

1. Suporte para exportação/exportação em lote de vídeos.
2. Suporta vários formatos, incluindo MP4, AVI e EXE.
3. Suporte para configuração do caminho de armazenamento do arquivo a ser exportado. Suporte para backup dos arquivos em disco de rede.
4. Suporte à exportação após criptografia.
5. Suporte para combinar arquivos exportados em um único arquivo.
6. Suporte para gerenciar tarefas de download. Suporte para iniciar/parar/excluir/baixar todas as tarefas. Suporte para continuar baixando após a rede ser reconectada.
7. Suporte ao agendamento de 4 períodos de tempo para download de vídeos no tempo livre.
8. Suporte para salvar vídeos como evidência.

4.6.4 Gerenciamento de Permissões

1. Suporte para iniciar visualização ao vivo, captura manual, impressão, pesquisa de vídeo, exportação de vídeo, gravação manual, iniciar áudio bidirecional e habilitar permissão de áudio pela câmera.
2. Suporte para habilitar/desabilitar permissão de reprodução por câmera. Suporte para configurar permissão de reprodução do usuário por minuto/hora/dia.

3. Suporte para habilitar/desabilitar tag de vídeo, permissão de bloqueio por câmera. Permissões de bloqueio de vídeo incluem configuração de permissão para adicionar, excluir, editar e pesquisar vídeo.
4. Suporte para habilitar/desabilitar permissão PTZ. Suporte para configurar e operar PTZ.
5. Suporte à configuração de autenticação dupla para visualização ao vivo, reprodução e exportação de vídeo.
6. Suporte para habilitar/desabilitar a permissão de visualização pública. Suporte para adicionar, excluir e editar permissões de câmera.
7. Suporte para habilitar/desabilitar a permissão de rastreamento visual.
8. Suporte para configuração de permissões de tipo de transmissão na visualização ao vivo: transmissão principal, transmissão secundária e transmissão suave.

4.6.5 Gestão de Evidências

Suporte ao gerenciamento de evidências. Consulte ***Gerenciamento de evidências*** .

4.6.6 Câmera Programada

Captura Programada

1. Suporte para configuração de cronogramas de captura para múltiplas câmeras. Para speed domes, suporte para configuração de presets e captura de imagens em presets.
2. Suporte ao envio de relatórios de captura agendados por e-mail.
3. Suporte para busca de capturas programadas por agendamento, câmera e hora. Suporte para visualização e exportação de capturas e envio de capturas por e-mail.

Fotografia com lapso de tempo

1. Suporte à geração de vídeos em lapso de tempo com base em múltiplas imagens capturadas.
2. Suporte à busca de vídeos de lapso de tempo em NVRs por duração do vídeo, período de tempo e intervalo de tempo total.

4.6.7 Evento e Alarme

Suporte a gerenciamento de eventos e alarmes. Consulte ***Evento e Alarme*** .

4.6.8 Estação de Encaixe e Câmera Corporal

Gestão de Estações de Atracação

1. Suporte ao gerenciamento de grupos de dock station. Suporte à importação de pessoas e exibição de níveis de permissão de pessoas.
2. Suporte a gerenciamento de permissão de três níveis: grupo de dock station, superusuário e pessoa. Suporte a configuração de pessoa como superusuário.
3. Suporte a vários grupos de pessoas na estação de acoplamento.

4. Suporte para aplicação de informações pessoais (que devem corresponder às informações da conta da câmera corporal) na estação de acoplamento.
5. Suporte ao gerenciamento de cartões e à aplicação de informações de cartões em estações de acoplamento.
6. Suporte ao gerenciamento de impressões digitais. Suporte à aplicação de informações de impressão digital em estações de encaixe.
7. Suporte ao gerenciamento de perfis e à aplicação de perfis em estações de acoplamento.
8. Suporte a filtragem de acordo com o status de aplicação. Suporte a exibição de usuários que falharam na aplicação e reaplicá-los.
9. Suporte para configuração de tempo de copyback para dock stations. Suporte para configuração de local de armazenamento para CVR ou pStor.

Pesquisa e Gerenciamento de Arquivos

1. Suporte à busca de arquivos por hora, grupo de estações de acoplamento, formato de arquivo (vídeo, imagem e áudio).
2. Suporte para exportar arquivos pesquisados e salvar vídeos como evidência.
3. Suporte à busca de vídeos para reprodução de trilhas de GPS.
4. Suporte para configuração de canais visíveis de acordo com áreas para usuários na situação de múltiplos gerentes.

Câmera Corporal

1. Suporte para localizar câmeras corporais no Google Maps. Suporte para localizar câmeras corporais em uma área específica.
2. Suporte para visualização ao vivo, reprodução e áudio bidirecional para câmeras corporais.
3. Suporte a ações de vinculação no cliente para eventos de câmera corporal.

4.7 Parede Inteligente

- ***Gerenciamento de dispositivos***
- ***Configuração e Gerenciamento***
- ***Gestão de sistemas***

4.7.1 Gerenciamento de Dispositivos

1. Detectar dispositivos online: no mesmo segmento de rede com o servidor ou o cliente via SADP.
2. Adicione dispositivos via endereço IP, segmento IP e segmento de porta.
3. Acesse a página de configuração remota do dispositivo via navegador da web.
4. Configuração em cascata de decodificadores (série 69) e controladores de parede inteligentes (série C10S).
5. Visualize o status da subplaca da fonte do sinal e da saída de decodificação, bem como o status do sinal.
6. Exibir a visualização especificada na parede inteligente.

4.7.2 Configuração e Gerenciamento

Gestão de Paredes Inteligentes

1. A plataforma oferecerá suporte para adicionar, excluir e editar a parede inteligente LCD.
2. A plataforma oferecerá suporte para adicionar, excluir e editar a parede inteligente de LED.
3. A plataforma suportará resoluções de edição em lote das saídas dos decodificadores.
4. A plataforma deve suportar a vinculação da saída de decodificação com a janela e a liberação dessa vinculação.
5. A plataforma suportará a configuração da porta de áudio da parede inteligente.
6. A plataforma deve suportar a definição da cor de fundo/imagem da saída.
7. A plataforma suportará a exibição do número da porta de saída de decodificação na tela grande.
8. A plataforma oferecerá suporte à configuração de tipos de fluxo (subfluxo/fluxo principal) e à troca automática do tipo de fluxo.
9. A plataforma suportará a exibição e o download do ID da câmera.
10. A plataforma suportará fontes de sinal transmitindo a exibição ao vivo de canais em lote.
11. A plataforma deve suportar a especificação do tempo de reprodução agendado para uma visualização. A visualização será exibida uma vez dentro do tempo especificado.
12. A plataforma suportará a reprodução em lote de vídeos sequencialmente nas janelas seguintes, começando na janela especificada.

Abra a Janela e Exiba na Parede Inteligente

1. A plataforma suportará o modo de divisão de janelas (4/9/16/36 janelas), bloqueio de janelas e ampliação/restauração do tamanho da subjanela por clique duplo.
2. A plataforma oferecerá suporte à criação de janelas de roaming, exclusão, movimentação, fixação em cima/em baixo e alteração do tamanho das janelas de roaming.
3. A plataforma deve suportar a ativação/desativação da regra VCA.
4. A plataforma deverá suportar a exibição da janela nº.
5. A plataforma oferecerá suporte à exibição da fonte de sinal local (única ou em lote) na parede inteligente via ONVIF, Protocolo Hikvision ou o nome de domínio da câmera.
6. A plataforma oferecerá suporte ao controle da exibição do mural de vídeo de uma câmera para troca automática em uma única janela, incluindo pausar, continuar, visualizar a última/próxima troca automática e ajustar a programação de troca automática.
7. A plataforma deve suportar a troca manual do fluxo principal/secundário da fonte de sinal.
8. A plataforma suportará controle PTZ.
9. A plataforma oferecerá suporte à personalização do ID da câmera exibido na parede inteligente.
10. A plataforma oferecerá suporte ao cliente para exibir as mesmas imagens que estão no smart wall completo, reproduzir o smart wall e controlar a imagem do vídeo na janela.
11. A plataforma oferecerá suporte à exibição do status das saídas de decodificação e fontes de sinal.
12. A plataforma oferecerá suporte ao cliente para exibir as imagens da mesma forma que as do smart wall completo.
13. A plataforma suportará a adição de um logotipo na janela.

14. A plataforma suportará a configuração da imagem de fundo.
15. A plataforma suportará a exibição da área de trabalho na parede inteligente.
16. A plataforma deverá suportar janelas articuladas.
17. A plataforma suportará a exibição da área de trabalho na parede inteligente.

Aplicação APP

1. A plataforma suportará a comutação da fonte do sinal para exibição na parede inteligente por meio de um painel.
2. A plataforma suportará paredes inteligentes de LED e LCD.
3. A plataforma suportará até 8 paredes inteligentes.
4. A plataforma suportará divisão de tela virtual, arrastar para abrir uma janela, percorrer janelas, aplicar zoom em uma janela, divisão de janelas, etc.

Parede Inteligente LED

1. A plataforma suportará legendas estáticas/rolantes.
2. A plataforma suportará a visualização do layout da parede inteligente.
3. A plataforma deverá suportar a junção de janelas.
4. A plataforma suportará divisão de janelas personalizada e virtual.

Visualizar

1. A plataforma oferecerá suporte para adicionar, excluir, editar e pesquisar a visualização/grupo de visualizações.
2. A plataforma oferecerá suporte à alternância de agendamentos de exibição por semanas e à reprodução de exibições em horários específicos.
3. A plataforma oferecerá suporte à exibição de visualizações no smart wall conforme a programação.
4. A plataforma suportará a edição do cronograma de visualização.
5. A plataforma oferecerá suporte à definição de visualizações públicas e privadas.
6. A plataforma oferecerá suporte à visualização de miniaturas de visualizações passando o cursor sobre a lista de visualizações.

Teclado

1. A plataforma suportará o acesso a teclados de rede (Modelo: DS-1100KI(B), DS-1105KI e DS-1600KI(B)).
2. A plataforma oferecerá suporte à comutação automática de alarmes na parede inteligente e interromperá a exibição após o alarme ser reconhecido.
3. A plataforma suportará a exibição na parede inteligente pressionando o ID da câmera no teclado.

4.7.3 Gerenciamento do Sistema

Gerenciamento de Permissões

1. Suporte ao controle da permissão de acesso ao módulo de parede inteligente.
2. Suporte à atribuição de permissões de operação por paredes inteligentes.

3. Suporte à atribuição de permissões para adicionar, excluir, editar e pesquisar dados por paredes inteligentes.
4. Suporte à atribuição de permissões de acordo com decodificadores e controladores de divisão.
5. Suporte para adicionar, excluir, editar e pesquisar permissões por decodificadores e controladores de parede inteligentes.

Configuração de Streaming

1. Suporta configurações globais do tipo de fluxo (fluxo secundário/principal) do display de parede inteligente e alterna o tipo de fluxo de acordo com o modo de divisão da janela.
2. Suporte para configuração de mídia de streaming de acordo com áreas para exibição na parede inteligente.

Ligação de Alarme

1. Suporte à exibição de parede inteligente para vinculação de alarme de uma câmera específica em uma ou várias janelas.
2. Suporte para exibir a visualização de uma parede de decodificação específica vinculada a uma visualização de monitor na parede inteligente.
3. Suporte para configurar a duração da exibição de alarmes na parede inteligente, se está substituindo o alarme anterior e o tipo de fluxo do display da parede inteligente (fluxo secundário/principal).
4. Suporte à divisão automática de janelas para alarmes de vinculação exibidos na parede inteligente.
5. Suporte para alarmes de ligação destacados em moldura vermelha exibidos na parede inteligente.
6. Suporte para configuração de alarme de detecção online/offline de decodificadores/controladores de parede inteligentes.

Backup e Restauração de Dados

Suporte para backup e restauração de dados de paredes inteligentes.

Status de Manutenção

Suporte para visualização do status de manutenção de decodificadores e controladores de parede inteligentes.

4.8 Gerenciamento de Site Remoto

Gerenciamento de Site

1. A plataforma oferecerá suporte ao gerenciamento de 1.024 Sites Remotos, incluindo a adição manual de sites ou o registro de sites no Sistema Central.
2. A plataforma oferecerá suporte à configuração remota dos Sites Remotos, obtendo e visualizando as alterações de recursos dos Sites Remotos.
3. A plataforma suportará o backup do banco de dados de Sites Remotos para o Sistema Central manualmente ou por período (dia, semana ou mês).

4. A plataforma oferecerá suporte ao gerenciamento de Sites Remotos e câmeras de Sites Remotos no mapa.

Gerenciamento de Câmera

1. A plataforma suportará ir para o Remote Site. As configurações no Remote Site são as mesmas do Central System.
2. A plataforma oferecerá suporte ao gerenciamento de câmeras do Site Remoto: selecionar câmeras do Site Remoto para importá-las para o Sistema Central, obter e aplicar nomes de câmeras, importar câmeras, exibir as câmeras importadas no Sistema Central após alternar os sites.
3. A plataforma oferecerá suporte à aplicação de cronogramas de gravação e configurações de armazenamento do Sistema Central para câmeras no Site Remoto, além da cópia em lote das configurações das câmeras no Site Remoto.

Gestão de Portas

1. A plataforma suportará ir para o Remote Site. As configurações no Remote Site são as mesmas do Central System.
2. A plataforma oferecerá suporte ao gerenciamento de portas do Site Remoto, incluindo a seleção de portas do Site Remoto para importá-las para o Sistema Central, obtendo e aplicando os nomes das portas, obtendo e controlando remotamente o status das portas, exibindo os canais de câmera integrados importados do dispositivo de controle de acesso no Sistema Central após alternar os sites.

Gestão de Streaming

A plataforma oferecerá suporte à configuração de Servidores de Streaming para Sites Remotos no Sistema Central e à obtenção de streaming por meio de até dois Servidores de Streaming (no site e no Sistema Central).

Aplicação de Vídeo, Pesquisa e Exportação

Consulte ***o vídeo básico*** .

Gestão de Evidências

Consulte ***Gerenciamento de evidências*** .

Evento e Alarme

1. A plataforma oferecerá suporte à importação de eventos e alarmes de câmeras no Site Remoto para o Sistema Central para configuração de parâmetros relacionados a alarmes.
2. A plataforma oferecerá suporte ao recebimento e reconhecimento de eventos e alarmes (com informações de manutenção) de câmeras no Site Remoto.
3. A plataforma oferecerá suporte ao recebimento e reconhecimento de eventos de entrada de alarme e alarmes de dispositivos de codificação no Site Remoto.
4. A plataforma oferecerá suporte ao recebimento e reconhecimento de alarmes relacionados a rostos (incluindo rostos correspondentes/não correspondentes, que aparecem com frequência/raridade, temperatura anormal e ausência de máscara) do Site Remoto.

5. A plataforma oferecerá suporte ao recebimento e reconhecimento de alarmes relacionados à manutenção de controle de acesso de dispositivos de codificação, dispositivos de decodificação, servidores de gravação e servidores de streaming no site remoto.
6. A plataforma oferecerá suporte à importação de eventos e alarmes de portas no Site Remoto para o Sistema Central para configuração de parâmetros relacionados a alarmes.
7. A plataforma oferecerá suporte ao recebimento e reconhecimento de eventos e alarmes (com informações de manutenção) de portas no Site Remoto.

ANPR

1. A plataforma oferecerá suporte ao recebimento de resultados ANPR de câmeras no Site Remoto.
2. A plataforma oferecerá suporte à busca de registros ANPR de câmeras no Site Remoto.
3. A plataforma oferecerá suporte à busca e exportação de relatórios de análise de veículos gerados por câmeras no Site Remoto.

Face

1. A plataforma oferecerá suporte à busca de imagens de rostos capturadas por câmeras no Site Remoto.
2. A plataforma oferecerá suporte à busca de imagens de rostos de câmeras no Site Remoto por imagem.
3. A plataforma oferecerá suporte à busca de imagens de rostos de câmeras no Site Remoto por recurso de pessoa.
4. A plataforma oferecerá suporte à visualização de imagens de rostos capturadas em tempo real e resultados de comparação no Site Remoto.

Corpo Humano

1. A plataforma oferecerá suporte à busca de imagens do corpo humano capturadas por câmeras no Site Remoto.
2. A plataforma oferecerá suporte à busca de imagens de corpos humanos de câmeras no Site Remoto por imagem.

Análise Inteligente

1. A plataforma oferecerá suporte à importação de câmeras do Sistema Central para o Site Remoto para configurar relatórios de análise inteligentes, incluindo relatórios de contagem de pessoas, relatórios de análise de densidade de pessoas, relatórios de análise de calor, relatórios de análise de filas e relatórios de análise de características de pessoas.
2. A plataforma suportará a importação de câmeras do Sistema Central para o Site Remoto para configuração de relatórios de análise de temperatura.
3. A plataforma oferecerá suporte à busca e exportação de relatórios de análise inteligente gerados por câmeras importadas para o Sistema Central , incluindo relatórios de contagem de pessoas, relatórios de análise de densidade de pessoas, relatórios de análise de calor, relatórios de análise de filas e relatórios de análise de características de pessoas.
4. A plataforma oferecerá suporte à busca e exportação de relatórios de análise de temperatura gerados por câmeras importadas para o Sistema Central.

Manutenção

1. A plataforma suportará a obtenção de informações de manutenção das câmeras no Site Remoto, que são as mesmas exibidas no Sistema Central.
2. A plataforma deve suportar a obtenção de informações de manutenção de dispositivos de codificação, dispositivos de decodificação, Servidores de Gravação e Servidores de Streaming no Site Remoto. As informações de manutenção do site são as mesmas que as exibidas no Sistema Central, mas os usuários não podem clicar para ir rapidamente para a página de detalhes.
3. A plataforma suportará a exibição em lote do status de câmeras, codificadores e decodificadores em locais remotos.

4.9 Reconhecimento Inteligente

- ***Gerenciamento de sistemas e recursos***
- ***Reconhecimento facial***
- ***Reconhecimento do corpo humano***
- ***Gestão de Arquivos***
- ***Reconhecimento de Veículos***
- ***Armazenamento de registros***

4.9.1 Gerenciamento de sistemas e recursos

Gestão de Recursos

1. Suporte para adicionar servidores de análise inteligentes à plataforma; os servidores de análise inteligentes adicionados oferecem suporte aos seguintes recursos:
   a. Acessando servidores de análise inteligentes pela internet.
   b. Saltar para a página web de um servidor de análise inteligente para configurar seus parâmetros.
   c. Vinculando câmeras a servidores de análise inteligente para análise inteligente.
2. Suporte para adicionar câmeras de reconhecimento facial à plataforma e todos os recursos para o gerenciamento básico de dispositivos de codificação.
3. Suporte para adicionar NVRs DeepinMind e todos os recursos para o gerenciamento básico de dispositivos de codificação.
4. Suporte para especificar os canais para análise de veículos e análise de características faciais/corporais humanas na página de detalhes da licença.

Bibliotecas de Imagens de Rosto

1. Suporte aos seguintes recursos relacionados a bibliotecas de imagens de rosto:
   a. Adicionar e gerenciar várias bibliotecas de imagens de rosto.
   b. Adicionar pessoas à lista de pessoas ou remover pessoas da lista.
   c. Exibindo o número de imagens de rosto em cada biblioteca de imagens de rosto."
2. Suporte à importação de bibliotecas de listas de faces e dados faciais.

3. Suporte à importação de dados faciais de estações de inscrição.
4. Suporte à importação de dados faciais selecionados de dispositivos de codificação e servidores de reconhecimento facial.
5. Suporte para exportação da lista da biblioteca de faces.
6. Suporte à aplicação em lote de dados faciais em dispositivos e à exibição das seguintes informações de aplicação de dados no Centro de Aplicação:
   a. Todos os dados faciais falharam ao serem aplicados.
   b. O número de itens de dados faciais a serem aplicados.
   c. A lista de itens de dados faciais a serem aplicados.
   d. O número de câmeras nas quais os dados faciais não foram aplicados.
   e. A lista de câmeras nas quais os dados faciais não foram aplicados.
   f. O número de câmeras às quais os dados faciais NÃO foram aplicados.
   g. A lista de câmeras às quais os dados faciais NÃO foram aplicados.

4.9.2 Reconhecimento Facial

Tarefas de Comparação de Imagens Faciais

1. Suporte para configuração de tarefas de comparação de imagens faciais para câmeras, NVRs DeepinMind e servidores de análise inteligentes.
2. Suporte para configuração de tarefas de comparação de imagens faciais para câmeras de reconhecimento facial, DeepinMind NVRs, servidores de análise inteligente. As opções de configuração incluem:
   - Modelos de cronograma de tarefas
   - Dispositivos / Câmeras que realizam a análise
   - bibliotecas de imagens de rosto
   - Semelhanças
3. Suporte para exibir a lista de tarefas de comparação de imagens faciais e filtrar as tarefas por nome, programação de armamento, dispositivo para análise, biblioteca de imagens faciais e câmera.

Análise de Pessoas Frequentemente Aparecidas

1. Suporte para configuração de tarefas de análise de pessoas que aparecem com frequência para NVRs DeepinMind e servidores de análise inteligentes.
2. Suporte para configuração de parâmetros para uma tarefa de pessoa que aparece com frequência, incluindo o modelo de agendamento de tarefas, dispositivo para análise/câmera, biblioteca de imagens de rosto, período de tempo, horários de aparecimento, intervalo de contagem e similaridade.
3. Suporte para exibir as tarefas de análise de pessoas que aparecem com frequência em uma lista e filtrar tarefas na lista por nome da tarefa, modelo de agendamento de tarefas, dispositivo para análise e câmera.

Análise de Pessoa Raramente Aparecida

1. Suporte para configuração de tarefas de análise de pessoas raramente exibidas para NVRs

DeepinMind.
2. Suporte para configuração de parâmetros para uma tarefa de análise de pessoa que raramente aparece , incluindo o modelo de agendamento de tarefa, dispositivo para análise/câmera, biblioteca de imagens de rosto, período de tempo, horários de aparecimento, intervalo de contagem, similaridade e tempo de relatório.
3. Suporte para exibir tarefas de análise de pessoas que raramente aparecem em uma lista e filtrar as tarefas por nome da tarefa, modelo de agendamento de tarefas, dispositivo para análise e câmera.

Armazenamento de Dados Faciais

1. Suporte ao armazenamento de imagens de rostos correspondentes na plataforma ou no servidor de armazenamento se apenas as câmeras de reconhecimento facial forem usadas para reconhecimento facial.
2. Suporte ao armazenamento de imagens faciais capturadas e correspondentes nos NVRs DeepinMind se a combinação de câmeras de rede e NVRs DeepinMind for usada para reconhecimento facial.
3. Suporte ao armazenamento de imagens faciais capturadas e correspondentes nos servidores de análise inteligente se a combinação de câmeras de rede e servidores de análise inteligente for usada para reconhecimento facial.

Evento e Alarme

1. Suporte para receber eventos de comparação de imagens faciais quase instantâneos das bibliotecas de imagens faciais selecionadas.
2. Suporte para receber eventos de incompatibilidade de rosto quase instantâneos das bibliotecas de imagens de rosto selecionadas; O mecanismo de incompatibilidade é o seguinte: se uma imagem de rosto capturada não puder corresponder a nenhuma imagem de rosto nas bibliotecas de imagens de rosto especificadas dentro do período de tempo especificado em um alarme combinado, o evento será considerado um evento de incompatibilidade de rosto; enquanto que se a imagem de rosto capturada não corresponder às imagens de rosto em todos os grupos, o evento será considerado um evento estranho.
3. Suporte para busca de eventos de pessoas raramente aparecidos por dispositivo e biblioteca de imagens de rosto.
4. Suporte para busca de eventos de pessoas que aparecem com frequência por dispositivo.
5. Suporte para busca de eventos sem máscara facial por canal e biblioteca de imagens de rosto.
6. Suporte a outros eventos relacionados à detecção de rostos realizados por câmeras, como eventos de captura de rostos e eventos de detecção de rostos.

Monitoramento baseado em rosto

1. Suporte para exibição de imagens de rosto capturadas quase em tempo real; Suporte para visualização de vídeo ao vivo transmitido por uma câmera se as imagens capturadas corresponderem às imagens de rosto em bibliotecas de imagens de rosto.
2. Suporte para visualização de estatísticas de fotos de rostos capturadas no dia atual e eventos de correspondência facial que ocorreram no dia atual.
3. Suporte ao monitoramento com base nas bibliotecas de imagens faciais; Suporte ao

monitoramento de vários grupos ao mesmo tempo.
4. Suporte ao monitoramento de eventos relacionados ao reconhecimento facial em tempo quase real, incluindo eventos de captura facial, eventos de correspondência facial, eventos de incompatibilidade facial, eventos de pessoas que aparecem com frequência e eventos de pessoas que aparecem raramente; assim que o sistema detectar um desses eventos, uma janela mostrando fotos/vídeos relacionados aparecerá em tempo quase real no Control Client.
5. Suporte para adicionar as imagens de rosto capturadas às bibliotecas de imagens de rosto.
6. Suporte à geração de padrões (ou seja, os rastros de pessoas detectadas) com base em suas imagens faciais (ou seja, as imagens faciais capturadas).
7. Suporte para verificar a identidade das pessoas por meio de suas fotos faciais (ou seja, as fotos faciais capturadas).
8. Suporte para visualização dos históricos de captura das pessoas correspondentes no módulo de monitoramento.
9. Suporte para selecionar características faciais das imagens capturadas e exibir essas características.
10. Suporte para exibir características faciais quase em tempo real, incluindo sorriso ou não, usando óculos ou máscara.

Pesquisa e Exportação de Registros

1. Suporte à busca de imagens de rosto capturadas por dispositivos por canal, hora e características faciais (se usando óculos e sorrindo ou não).
2. Suporte para busca de imagens de rosto por imagem; as condições de busca disponíveis incluem hora, canal, similaridade e imagem de rosto.
3. Suporte para busca em bibliotecas de imagens de rostos por hora, nome do grupo e informações da pessoa (nome da pessoa ou ID).
4. Suporte para busca de pessoas que aparecem com frequência por hora, tarefa e horários de aparecimento.
5. A busca de suporte raramente aparecia por pessoas por hora, tarefa e horários de aparecimento.
6. Suporte à exportação dos resultados correspondentes para o PC local; as informações exportadas incluem informações da pessoa e do vídeo.
7. Suporte para adicionar imagens de rosto correspondentes às bibliotecas de imagens de rosto.
8. Suporte à verificação de identidade de acordo com a imagem facial capturada; as condições de pesquisa disponíveis incluem a imagem facial capturada, a imagem facial correspondente e a similaridade.

Geração de Padrões

1. Suporte para geração de padrões (ou seja, trilhas de pessoas) das pessoas correspondentes.
2. Suporte para reproduzir os padrões em sequência temporal no mapa.

4.9.3 Reconhecimento do Corpo Humano

Gerenciamento de Tarefas

1. Suporte à configuração de tarefas de reconhecimento do corpo humano para NVRs DeepinMind e servidores de análise inteligentes.
2. Suporte à configuração de parâmetros para uma tarefa de reconhecimento do corpo humano, incluindo o modelo de agendamento de tarefas, dispositivo para análise/câmera e área de detecção.
3. Suporte para exibir tarefas de reconhecimento do corpo humano em uma lista. As informações exibidas de uma tarefa incluem seu nome, modelo de agendamento de tarefa, dispositivo para análise e câmera.

Monitoramento baseado no corpo humano

1. Suporte para exibir imagens do corpo humano capturadas por uma câmera quase em tempo real e visualizar o vídeo ao vivo transmitido pela câmera.
2. Suporte para exibir o número de fotos do corpo humano capturadas no dia atual quase em tempo real.
3. Suporte ao monitoramento de eventos de reconhecimento do corpo humano em tempo real. Se um evento for detectado, uma janela mostrando imagem(ns) / vídeo(s) relacionado(s) aparecerá no Control Client.
4. Suporte para exibir características do corpo humano quase em tempo real, incluindo sorriso ou não, uso de óculos, uso de máscaras faciais, estilo de cabelo, mochila, tipo de blusa, cor da blusa, tipo de calça, cor da calça, bolsa e se está andando de bicicleta.

Armazenamento de Dados Corporais

1. Suporte ao armazenamento de imagens capturadas do corpo humano nos NVRs DeepinMind se a combinação de câmeras de rede e NVRs DeepinMind for usada para reconhecimento do corpo humano.
2. Suporte ao armazenamento de imagens capturadas do corpo humano em servidores de análise inteligentes se a combinação de câmeras de rede e servidores de análise inteligentes for usada para reconhecimento do corpo humano.

Evento e Alarme

Suporte a outros eventos relacionados a rostos detectados por câmeras, como captura de rosto e detecção de rosto.

Pesquisa de Registros

1. Suporte à busca de eventos de detecção do corpo humano por canal e características do corpo humano (se está usando óculos, tipo de blusa, cor da blusa, tipo de calça, cor da calça, se está usando uma mochila, se está levantando algo, se está andando de bicicleta).
2. Suporte para busca de imagens do corpo humano por imagem; as condições de busca incluem evento, câmera e imagem capturada.
3. Suporte para seleção de câmeras AcuSearch.

4.9.4 Gerenciamento de Arquivos

Gerenciamento de Tarefas

1. Suporte à configuração de tarefas de análise de arquivo para servidores de análise inteligentes.
2. Suporte à configuração de parâmetros para uma tarefa de análise de arquivo, incluindo o modelo de agendamento de tarefas, dispositivo para análise/câmera, biblioteca de imagens de rosto e similaridade.
3. Suporte para exibir tarefas de análise de arquivo em uma lista e filtrar essas tarefas por nome da tarefa, modelo de agendamento de tarefas, dispositivo para análise e câmera.

Pesquisa de Arquivo

1. Suporte para enviar uma foto de rosto para verificar se a pessoa é um estranho.
2. Suporte para upload de uma foto de rosto para verificar se a pessoa pertence à biblioteca de fotos de rosto especificada.
3. Suporte à exportação dos registros correspondentes.

Verificação de Identidade

1. Suporte para carregar uma foto de rosto e compará-la com fotos de rosto nas bibliotecas de fotos de rosto para verificar a identidade da pessoa.
2. Suporte para carregar uma foto de rosto e especificar as informações da pessoa (nome ou documento de identidade) para pesquisar a identidade da pessoa.
3. Suporte à exportação dos registros correspondentes.

4.9.5 Reconhecimento de Veículos

Gerenciamento de Tarefas

1. Suporte à configuração de tarefas de reconhecimento de veículos para servidores de análise inteligentes.
2. Suporte à configuração de parâmetros para uma tarefa de reconhecimento de veículos, incluindo modelo de agendamento de tarefas, dispositivo para análise/câmera, biblioteca de imagens faciais e similaridade.
3. Suporte para exibir tarefas de reconhecimento de veículos em uma lista e filtrar as tarefas por nome da tarefa, modelo de agendamento de tarefas, dispositivo para análise e câmera.

Gerenciamento de Lista de Veículos

O mesmo que os recursos de gerenciamento de lista de veículos no módulo Entrada e Saída.

Armazenamento de Dados do Veículo

1. Suporte ao armazenamento de imagens de reconhecimento de veículos na plataforma ou no servidor de armazenamento caso somente câmeras de reconhecimento de veículos sejam usadas para reconhecimento de veículos.
2. Suporte ao armazenamento de imagens de reconhecimento de veículos e imagens de veículos capturadas nos NVRs DeepinMind se a combinação de câmeras de rede e NVRs DeepinMind

for usada para reconhecimento de veículos; Suporte à pesquisa de registros de veículos que passam na plataforma.
3. Suporte ao armazenamento de imagens de reconhecimento de veículos e imagens capturadas de veículos nos servidores de análise inteligente se a combinação de câmeras de rede e servidores de análise inteligente for usada para reconhecimento de veículos.

Evento e Alarme

O mesmo que os recursos de eventos e alarmes do módulo de Entrada e Saída.

Monitoramento de Veículos

1. Suporte para exibir as imagens capturadas do veículo quase em tempo real e visualizar o vídeo ao vivo transmitido pelas câmeras que capturam essas imagens.
2. Suporte à exibição de características de veículos que passam quase em tempo real, incluindo tipo de veículo, cor do veículo e marca do veículo.
3. Suporte ao monitoramento de eventos de detecção de veículos em tempo real, incluindo eventos de veículos correspondentes e eventos de veículos estranhos. Assim que o sistema detectar um desses eventos, uma janela mostrando imagens e vídeos relacionados aparecerá no Control Client.
4. Suporte para exibir o número de veículos que passam no dia atual.

Pesquisa de Registros

Suporte à busca de veículos que passam por hora, origem, marca, país e região, número da placa, tipo de veículo, marca do veículo, cor do veículo, direção de direção, lista de veículos e condições personalizadas.

4.9.6 Arme Inteligente

1. Suporte para aplicação de bibliotecas de imagens faciais em vários dispositivos para armamento de pessoas.
2. Suporte para aplicação de números de placas em vários dispositivos para armar veículos.

4.9.7 Armazenamento de Registros

Suporte para definição do período de retenção de registros de reconhecimento facial e de veículos: 1/2/3/4/5/6/7/15 dia(s), 1/2/3/6 mês(es) ou 1/2/3 ano(s).

4.10 Detecção de Alarme

- ***Gestão de Recursos***
- ***Gerenciamento de detecção de alarmes***
- ***Gestão de Radar de Segurança***
- ***Gerenciamento de alarme de pânico***
- ***Monitoramento de vídeo***

- ***Aplicação de Mapa***
- ***Aplicação de alarme***
- ***Manutenção de Recursos***
- ***Pesquisa de Log do Dispositivo***
- ***Ferramenta***

4.10.1 Gerenciamento de Recursos

Dispositivo e Servidor

a. A plataforma deve oferecer suporte à adição de painéis de controle de segurança, radares de segurança e dispositivos de alarme de pânico por endereço IP, segmento IP, segmento de porta, Hik-Connect DDNS ou importação em lote desses dispositivos para a plataforma para gerenciamento: Para painéis de controle de segurança, a plataforma deve oferecer suporte à adição deles por meio do Hikvision Private Protocol, Hikvision ISUP Protocol e Hik-Connect Protocol;
b. Para radares de segurança, a plataforma oferecerá suporte para adicioná-los por meio do Protocolo Privado Hikvision;
c. Para dispositivos de alarme de pânico, a plataforma oferecerá suporte para adicioná-los por meio do Hikvision Private Protocol e do Hikvision ISUP Protocol.

2.
3. A plataforma oferecerá suporte à busca de dispositivos online e à adição deles à lista de dispositivos após a ativação.
4. A plataforma oferecerá suporte à configuração remota de dispositivos.

Área

1. A plataforma oferecerá suporte à adição de câmeras em áreas para gerenciamento.
2. A plataforma oferecerá suporte à adição de entradas de alarme a áreas para gerenciamento, exibindo o status das entradas de alarme (status de bypass, status de falha, status de alarme, status da bateria, status de armação, status de conexão do detector, status online/offline), ignorando entradas de alarme e recuperando as entradas de alarme ignoradas.
3. A plataforma oferecerá suporte à adição de saídas de alarme às áreas para gerenciamento.
4. A plataforma oferecerá suporte à adição de radares de segurança às áreas para gerenciamento, armando/desarmando-os e exibindo seu status online/offline.

4.10.2 Gerenciamento de Detecção de Alarmes

Gerenciamento de Partição de Controle de Segurança (Área)

1. A plataforma suportará a importação de partições (áreas) de dispositivos e seu gerenciamento.
2. A plataforma oferecerá suporte à exibição de informações básicas sobre as partições (áreas) e informações sobre o status de suas zonas relacionadas.
3. Alguns painéis de controle de segurança sem fio de nova versão devem suportar a vinculação de uma zona com várias partições (áreas).

Gerenciamento de Detectores

1. A plataforma oferecerá suporte à relação de detectores com recursos e à exibição deles no mapa.
2. A plataforma suportará a captura de imagens com o módulo de câmera do detector externo e o salvamento delas no seu PC.

Operação de Partição de Controle de Segurança (área)

1. A plataforma oferecerá suporte à execução das seguintes operações em partições (áreas): desarmar, armar ausente e armar presente (com suporte dos painéis de controle de segurança da série EN), armar instantaneamente e limpar alarmes.
2. A plataforma suportará a configuração de agendamentos de armar/desarmar partições (áreas).
3. A plataforma suportará a configuração em lote do cronograma de armamento para múltiplas partições (áreas) de múltiplos dispositivos.

Operação de Zona

1. A plataforma suportará zonas de desvio e recuperação das zonas ignoradas.
2. A plataforma suportará armar/desarmar uma única zona.

Notificação de Status

A plataforma oferecerá suporte ao recebimento de alterações no status de partições (áreas) e zonas de dispositivos e à atualização das informações de status em tempo real.

Notificação de Evento

A plataforma oferecerá suporte ao envio de eventos disparados em partições (áreas) e zonas para dispositivos relacionados para disparar ações de vinculação, como disparar alarmes em dispositivos de alarme relacionados.

Gerenciamento de Usuários

1. A plataforma deve suportar o gerenciamento de usuários do tipo Operador. O usuário deve ser capaz de adicionar usuários, excluir usuários e aplicar usuários a dispositivos.
2. A plataforma deve suportar a especificação de informações do usuário (Operador): propriedade do usuário, senha do teclado, senha de coação e permissões de operação de partição (área).
3. A plataforma suportará a exclusão rápida de todos os usuários (Operadores) de um dispositivo específico ou de todos os dispositivos.

4.10.3 Gerenciamento de Radar de Segurança

Configuração do Radar de Segurança

1. A plataforma oferecerá suporte à vinculação de câmeras a um radar de segurança e à visualização ao vivo das câmeras no Control Client.
2. A plataforma oferecerá suporte à calibração de câmeras relacionadas a radares de segurança (a precisão da calibração afetará a vinculação inteligente).

3. A plataforma oferecerá suporte para que os radares de segurança monitorem os padrões de movimento dos objetos por meio de câmeras calibradas relacionadas.
4. A plataforma oferecerá suporte ao desenho de zonas na área de detecção de um radar e ao gerenciamento delas.
5. A plataforma oferecerá suporte ao desenho de linhas de gatilho na área de detecção de um radar e ao gerenciamento delas.

Operação de Radar de Segurança

A plataforma suportará armar e desarmar radares.

Notificação de Status

A plataforma oferecerá suporte ao recebimento de alterações no status de armar/desarmar radares e no status online/offline dos dispositivos, além de atualizar as informações de status em tempo real.

Notificação de Evento

A plataforma oferecerá suporte ao recebimento de alarmes disparados nas zonas e linhas de disparo de um radar, e à visualização das informações de alarme em outros módulos.

Padrão de Movimento

1. A plataforma suportará o recebimento do padrão de movimento do objeto em tempo real do radar de segurança e a exibição dele no mapa.
2. A plataforma deve suportar a busca pelo padrão histórico de movimento de um radar. Atualmente, o padrão histórico de movimento só pode ser exibido no Alarm Center. Quando um alarme é disparado nas zonas e linhas de disparo de um radar, a plataforma buscará o padrão histórico de movimento registrado 5 segundos antes e depois do tempo de disparo e o exibirá no Alarm Center.
3. A plataforma oferecerá suporte ao envio do padrão de movimento de um objeto em tempo real e à exibição do padrão no mapa.

Ligação Inteligente

A plataforma suportará a visualização do padrão de movimento de um objeto e a visualização ao vivo de câmeras relacionadas ao radar de segurança.

4.10.4 Gerenciamento de Alarme de Pânico

Notificação de Evento

A plataforma oferecerá suporte ao recebimento de alarmes de pânico e à visualização das informações de alarme em outros módulos.

Controle de Vídeo Porteiro

A plataforma suportará áudio bidirecional entre o Control Client e os dispositivos por meio de dispositivos de intercomunicação de vídeo.

Adição de Dispositivo via Protocolo ISUP

A plataforma suportará a adição de dispositivos de alarme de pânico à plataforma por meio do protocolo ISUP.

Dispositivo de Alarme de Pânico Solar

A plataforma oferecerá suporte à adição de dispositivos de alarme de pânico solar.

4.10.5 Monitoramento de Vídeo

Visualização ao vivo

1. A plataforma suportará visualização ao vivo das câmeras relacionadas aos dispositivos de alarme.
2. A plataforma suportará a visualização ao vivo das câmeras relacionadas aos radares de segurança.

Reprodução

A plataforma suportará a reprodução das câmeras relacionadas aos dispositivos de alarme. Os arquivos de vídeo podem ser armazenados em CVR, servidor de armazenamento em nuvem e pStor.

4.10.6 Aplicação de Mapa

Aplicação de Partição de Controle de Segurança (Área)

1. A plataforma suportará a adição de partições (áreas) ao mapa.
2. A plataforma oferecerá suporte à execução das seguintes operações em partições (áreas) no mapa: desarmar, armar ausente e armar presente (com suporte dos painéis de controle de segurança da série EN), armar instantaneamente e limpar alarmes.
3. A plataforma suportará armar/desarmar partições (áreas) e exibir seu status de alarme no mapa (as informações de status serão atualizadas em tempo real de acordo com as notificações de mudança de status).

Aplicação de Entrada de Alarme

1. A plataforma suportará a adição de entradas de alarme com seus detectores relacionados ao mapa.
2. A plataforma suportará o desvio de entradas de alarme e a recuperação das entradas de alarme ignoradas.
3. A plataforma oferecerá suporte à exibição de informações de status (status de bypass, status de alarme, etc.) das entradas de alarme no mapa (as informações de status serão atualizadas em tempo real de acordo com as notificações de alteração de status).

Aplicação de Radar de Segurança

1. A plataforma suportará a adição de radares de segurança ao mapa.
2. A plataforma suportará armar e desarmar radares no mapa.

3. A plataforma suportará a exibição do padrão do objeto detectado por um radar de segurança no mapa.
4. A plataforma oferecerá suporte à exibição do status de armamento dos radares no mapa.
5. A plataforma suportará a reprodução de vídeos ao vivo transmitidos pelas câmeras relacionadas a um radar.
6. A plataforma deverá suportar a exibição da velocidade do objeto detectado.

4.10.7 Aplicação de Alarme

Operação de Alarme no Dispositivo de Alarme

1. A plataforma oferecerá suporte à configuração de eventos e alarmes para dispositivos de alarme, exibindo notificações de alarme e pesquisando alarmes históricos.
2. A plataforma suportará o salto para o Controle de Entrada de Alarme para verificar o dispositivo correspondente e executar operações relacionadas após receber um alarme de dispositivo.

Operação de Alarme na Entrada de Alarme

A plataforma oferecerá suporte à configuração de eventos e alarmes para entradas de alarme, exibindo notificações de alarme e pesquisando alarmes de histórico.

Operação de Alarme na Partição (área)

1. A plataforma oferecerá suporte à configuração de eventos e alarmes para partições (áreas), exibição de notificações de alarme e busca de alarmes históricos.
2. A plataforma suportará saltos para o Controle de Entrada de Alarme para verificar a partição (área) correspondente e executar operações relacionadas após receber um alarme da partição (área).

Operação de alarme em radar de segurança

A plataforma oferecerá suporte à configuração de eventos e alarmes para zonas de radares e linhas de disparo, exibindo notificações de alarme e pesquisando alarmes históricos.

Controle de Armar

1. A plataforma oferecerá suporte à exibição da configuração de eventos e alarmes para câmeras, entradas de alarme e radares.
2. A plataforma oferecerá suporte à execução das seguintes operações em partições (áreas): desarmar, armar ausente e armar presente (com suporte dos painéis de controle de segurança da série EN), armar instantaneamente e limpar alarmes.
3. A plataforma suportará o bypass das entradas de alarme adicionadas às partições (áreas).
4. A plataforma suportará armar e desarmar radares.

4.10.8 Manutenção de Recursos

Entrada de Alarme

1. A plataforma oferecerá suporte à visualização das informações de status das entradas de alarme (status da rede, status de armação, status de bypass, status de falha, status de alarmes, status de conexão do detector e status da bateria) e o tempo de inspeção.
2. A plataforma oferecerá suporte à atualização do status das entradas de alarme manualmente ou por programação.
3. A plataforma suportará a exportação das estatísticas de status das entradas de alarme para o PC local.
4. A plataforma oferecerá suporte à visualização de informações detalhadas sobre entradas de alarme.
5. A plataforma oferecerá suporte à visualização do status das entradas de alarme por tipo de dispositivo.

Dispositivo de Alarme

1. A plataforma oferecerá suporte à visualização de informações de status (status da rede, status de energia, status de armar/desarmar) e tempo de inspeção dos dispositivos de alarme.
2. A plataforma oferecerá suporte à atualização do status dos dispositivos de alarme manualmente ou por programação.
3. A plataforma suportará a exportação de estatísticas de status de dispositivos de alarme para o PC local.
4. A plataforma oferecerá suporte à visualização de informações detalhadas sobre os dispositivos de alarme.

4.10.9 Pesquisa de Log do Dispositivo

1. A plataforma suportará a busca de logs armazenados em dispositivos de alarme.
2. A plataforma suportará a exportação dos logs armazenados em dispositivos de alarme para o PC local.

4.10.10 Ferramenta

Controle de Saída de Alarme

A plataforma suportará o controle da sirene, lâmpada de alarme, fechadura elétrica e saída de alarme comum das saídas de alarme.

Radiodifusão

A plataforma suportará transmissão por meio de estações de alarme de pânico.

4.11 Monitoramento de AR

- ***Gestão de AR***
- ***Operação de cena***
- ***Evento e Alarme***
- ***Gerenciamento de tags***

4.11.1 Gestão de Contas a Receber

Suporte ao gerenciamento de cenas de RA:

1. Suporte ao gerenciamento de cenas, incluindo a vinculação de câmeras de RA com cenas e a configuração da localização geográfica de uma cena adicionando-a a um mapa.
2. Suporte ao gerenciamento de múltiplas cenas.
3. Suporte para calibração de câmeras e speed domes da série AR PanoVu.

4.11.2 Operação de Cena

Seleção de Cena

1. Suporte para seleção de cenas por meio da lista de cenas ou por pesquisa de nome.
2. Suporte à seleção de cenas com base em suas localizações no mapa.
3. Suporte para configuração de planos de troca automática para alternar cenas automaticamente pelo intervalo de tempo definido (10 seg, 20 seg, 40 seg, 1 min, 3 min, 5 min ou um intervalo de tempo personalizado).

Gerenciamento de Câmera AR

1. Suporte para captura de imagens por câmeras de RA.
2. Suporte para gravação de vídeos por câmeras de RA.
3. Suporte ao posicionamento 3D de câmeras de RA.
4. Suporte ao controle PTZ de câmeras AR.
5. Suporte à reprodução de vídeos por câmeras de RA.
6. Suporte ao rastreamento panorâmico de alvos (se a cena estiver vinculada a um domo de velocidade).
7. Suporte para chamar as predefinições de uma speed dome.

4.11.3 Evento e Alarme

Monitoramento de Alarme

1. A plataforma oferecerá suporte à exibição dos 5 alarmes não tratados mais recentes em uma lista e à filtragem desses alarmes por tipo.
2. A plataforma suportará a exibição dos alarmes de todas as tags adicionadas à cena.
3. A plataforma oferecerá suporte aos seguintes tipos de alarme: eventos VCA, eventos de detecção de rosto, eventos de detecção de veículos, eventos de imagem térmica e eventos de

manutenção de câmera.
4. A plataforma oferecerá suporte à visualização de informações de alarme e ao tratamento de alarmes da mesma forma que o oferecido na central de alarmes.

Detecção de Eventos

1. A plataforma oferecerá suporte à detecção de eventos de correspondência facial.
2. A plataforma oferecerá suporte à detecção de eventos de correspondência de veículos.

4.11.4 Gerenciamento de Tags

Adicionando Tag

1. Suporte para adicionar várias pastas para gerenciar tags favoritas.
2. Suporte para adicionar tags à imagem panorâmica e adicionar as tags adicionadas aos seus favoritos.

Tag da Câmera

1. Suporte para execução de operações básicas, como visualização ao vivo e reprodução de tags de câmera.
2. Suporte a operações como ignorar alarmes, visualizar histórico de alarmes e executar controles de armamento.
3. Suporte à troca dinâmica de tags de câmera de uma speed dome conforme a câmera aumenta/diminui o zoom ou gira.

Tag de Cena

1. Suporte para adição de tags de cena.
2. Suporte para alternar para a cena especificada por uma tag. As operações suportadas após a troca de cena devem permanecer as mesmas.

Tag do Mapa

1. Suporte para adição de tags de mapa.
2. Suporte para abrir a pré-visualização do mapa, visualizar detalhes do mapa e executar outras operações básicas do mapa.

Tag de Controle de Acesso

1. A plataforma oferecerá suporte à assinatura de eventos e alarmes das tags de controle de acesso e à visualização dos detalhes relacionados.
2. A plataforma deve suportar a visualização das informações básicas dos pontos de controle de acesso e os últimos 10 alarmes e eventos de controle de acesso. A plataforma deve suportar a visualização do status da porta e portas de controle. A plataforma deve suportar a assinatura e a visualização de eventos de controle de acesso de porta.
3. A plataforma oferecerá suporte à visualização de eventos de controle de acesso na central de alarmes em tempo real e na lista de eventos.

Tag de Recurso de Alarme

1. A plataforma suportará a exibição de alarmes de partições (áreas) e zonas vinculadas a partições (áreas).
2. A plataforma deve suportar a exibição de informações básicas de partição (área), status de armamento em detalhes de tag. Armar, desarmar, armar ausente, armar em permanência e silenciar alarmes.
3. A plataforma deve suportar a visualização de listas de zonas e status de zonas em detalhes de tag. A plataforma deve suportar armar, desarmar e ignorar uma zona.

Tag de Radar

1. A plataforma oferecerá suporte à exibição de alarmes de radares, status de alarme e eventos em tempo real.
2. A plataforma suportará a exibição de informações, incluindo informações de radar e câmeras vinculadas. A plataforma suportará armar e desarmar um radar.
3. A plataforma deve suportar a exibição de partição (área), zona e alarmes de radares na lista de alarmes em tempo real.

Tag de Entrada e Saída

1. A plataforma oferecerá suporte à assinatura de registros de controle de acesso para exibir registros relacionados.
2. A plataforma deve suportar a visualização de registros de uma entrada e saída. A plataforma deve suportar a visualização de informações de entrada e saída, vídeos vinculados (capturas), eventos de passagem de veículos e alarmes em detalhes de tag.

Tag do Alto-Falante da Rede

1. A plataforma suportará a exibição de alarmes de alto-falantes de rede.
2. A plataforma oferecerá suporte à exibição de status de alarme, imagem de visualização ao vivo e informações de recursos em detalhes de tags.
3. A plataforma suportará transmissão inicial e áudio bidirecional.

Pesquisa de Tags

1. Suporte à busca de tags por nome ou tipo de tag (câmera, cena e mapa).
2. Suporte para filtragem de tags favoritas por pasta.

4.12 Gerenciamento de Mapas

- ***Configurações do Mapa***
- ***Gestão de Recursos***
- ***Operações de Recursos***
- ***Operações Gerais***
- ***Estatísticas***

4.12.1 Configurações do Mapa

1. A plataforma suportará a adição de mapas do Google.
2. A plataforma suportará a adição de mapas de satélite do Google.
3. A plataforma suportará a adição de E-maps.

4.12.2 Gerenciamento de Recursos

1. A plataforma oferecerá suporte para adicionar, excluir, editar e pesquisar pontos de acesso.
2. A plataforma oferecerá suporte para adicionar, excluir, editar e pesquisar câmeras.
3. A plataforma oferecerá suporte para adicionar, excluir, editar e pesquisar estacionamentos.
4. A plataforma oferecerá suporte para adicionar, excluir, editar e pesquisar dispositivos de alarme.
5. A plataforma oferecerá suporte para adicionar, excluir, editar e pesquisar sites remotos.
6. A plataforma suportará a adição de zonas.
7. A plataforma oferecerá suporte para adicionar, excluir, editar e pesquisar entradas de alarme.
8. A plataforma oferecerá suporte para adicionar, excluir, editar e pesquisar saídas de alarme.
9. A plataforma suportará adicionar, excluir, editar e pesquisar dispositivos de controle de acesso. Personalize os ícones dos dispositivos de controle de acesso.
10. A plataforma oferecerá suporte para adicionar, excluir, editar e pesquisar dispositivos de áudio.
11. A plataforma suportará adicionar, excluir e editar áreas geográficas. A plataforma suportará adicionar recursos a áreas geográficas.
12. A plataforma oferecerá suporte para adicionar, excluir, editar e pesquisar recursos de terceiros.
13. A plataforma oferecerá suporte à adição de grupos de intertravamento de múltiplas portas aos mapas.
14. A plataforma oferecerá suporte à adição de grupos anti-passback aos mapas.
15. A plataforma oferecerá suporte à adição de grupos de contagem de entradas e saídas aos mapas.
16. A plataforma suportará a adição de alarmes combinados aos mapas.

4.12.3 Operações de Recursos

Gerenciamento de Alarmes

1. A plataforma oferecerá suporte ao reconhecimento de alarmes de recursos adicionados aos mapas e à visualização de detalhes dos alarmes.
2. A plataforma oferecerá suporte à visualização das taxas de ocupação das vagas de estacionamento e informações sobre a duração do estacionamento.
3. A plataforma oferecerá suporte para ignorar alarmes em um mapa.

Área Geográfica

1. A área piscará se algum dos recursos dentro de uma área geográfica relatar um alarme.

2. A plataforma oferecerá suporte à ignorância em lote de todos os alarmes dentro de uma área geográfica.
3. A plataforma oferecerá suporte ao controle de alarmes de luz estroboscópica dentro de uma área geográfica.
4. A plataforma suportará a transmissão em lote dos recursos dentro de uma área geográfica.

Câmera

1. A plataforma oferecerá suporte para iniciar a visualização ao vivo e a reprodução de uma câmera.
2. A plataforma oferecerá suporte à exibição de registros de passagem de veículos pelas câmeras ANPR.
3. A plataforma suportará seleção em lote de câmeras e início da visualização ao vivo (Cliente de Controle).
4. A plataforma suportará o controle de câmeras FoV: o ângulo de visão e a visão de campo mudarão conforme a câmera muda seu ângulo.
5. A plataforma suportará o controle em lote de alarmes de luz estroboscópica.
6. A plataforma suportará o controle em lote de alarmes de áudio.

Região Quente

1. A plataforma oferecerá suporte ao clique em uma região ativa para visualizar outro mapa.

Análise Inteligente

1. A plataforma oferecerá suporte à contagem de pessoas em grupos: A plataforma oferecerá suporte à visualização em tempo real do número de pessoas que entraram, saíram ou permaneceram na região.
2. A plataforma oferecerá suporte à adição de grupos de análise de caminhos: a plataforma oferecerá suporte à visualização em tempo real do número de pessoas que passam no módulo Monitoramento no Cliente de Controle.

Palestrante

1. A plataforma oferecerá suporte para iniciar transmissões e reproduzir áudios.

Dispositivos Portáteis

1. A plataforma deve suportar a localização de dispositivos em um mapa. A plataforma deve suportar a inicialização de visualização ao vivo, reprodução e áudio bidirecional.

Controle de Acesso

1. A plataforma oferecerá suporte a grupos de análise de caminhos: A plataforma oferecerá suporte à visualização em tempo real do número de pessoas que passam no módulo Monitoramento no Cliente de Controle.
2. A plataforma oferecerá suporte a grupos de contagem de entradas e saídas: A plataforma oferecerá suporte à visualização em tempo real do número de pessoas que entraram, saíram da região ou permaneceram na região no módulo Monitoramento no Cliente de Controle.
3. A plataforma deverá suportar grupos anti-passback: Quando um alarme anti-passback for

acionado pelas portas do grupo, a região do grupo deverá ser destacada no mapa.
4. A plataforma deverá suportar grupos de intertravamento de múltiplas portas: quando o alarme de intertravamento de múltiplas portas for acionado pelas portas do grupo, a região do grupo deverá ser destacada no mapa.
5. A plataforma oferecerá suporte à verificação de registros de controle de acesso, exceções de reconhecimento, etc. do dia atual.

4.12.4 Operações Gerais

1. A plataforma suportará zoom in e zoom out de mapas.
2. A plataforma suportará captura e impressão de mapas.
3. A plataforma deve suportar adicionar, excluir, editar e pesquisar tags. A plataforma deve suportar personalizar tags.
4. A plataforma oferecerá suporte à filtragem por tipos de recursos nos mapas.
5. A plataforma oferecerá suporte à exibição/ocultação de nomes de recursos em mapas.
6. A plataforma oferecerá suporte à exibição/ocultação de efeitos de campo de visão.
7. A plataforma deve suportar a ativação/desativação do modo 3D.

4.12.5 Estatísticas

A plataforma oferecerá suporte à exibição de dados sobre controle de acesso, alarme, manutenção e análise inteligente.

4.13 Evento e Alarme

- ***Evento de Disparo***
- ***Recepção de Eventos***
- ***Ligação de Alarme***
- ***Alarme Combinado***
- ***Configuração e Gerenciamento***
- ***Exibição de Alarme em Tempo Real***
- ***Operação de Alarme***
- ***Pesquisar e Exportar***
- ***Estatística e Análise***
- ***Gerenciamento de Permissões***

4.13.1 Evento de Disparo

Classificação

1. Os eventos de disparo devem ser classificados por módulos, incluindo vídeo, controle de acesso, veículo, alarme, grupo de análise inteligente, sinalização digital, manutenção, usuário, evento definido pelo usuário, evento genérico, visitante, transmissão e inspeção de segurança.

2. A página Editar Alarme deve fornecer o ícone para configuração remota da fonte de disparo. Os usuários devem poder clicar no ícone para abrir a página de configuração remota do dispositivo ou servidor.

Evento Genérico

1. A plataforma deve suportar a configuração do tipo de transporte como TCP, UDP, HTTP ou HTTPS.
2. A plataforma deve oferecer suporte à definição do tipo de correspondência como Pesquisa por Expressão, Correspondência por Expressão ou Pesquisa por Palavra-chave e especificar palavras-chave da fonte de dados, título e descrição.
3. A plataforma deve suportar a seleção de AND ou OR como expressão.
4. A plataforma suportará a importação em lote de eventos genéricos.
5. A plataforma suportará o monitoramento de eventos genéricos via mapa.

Evento Definido pelo Usuário

A plataforma deverá suportar a configuração de eventos autodefinidos caso os eventos monitorados pelo sistema ou o evento genérico não possam atender às necessidades dos usuários.

4.13.2 Recebimento de Eventos

Cronograma de Recebimento de Eventos

1. A plataforma deverá suportar a configuração de eventos autodefinidos caso os eventos monitorados pelo sistema ou o evento genérico não possam atender às necessidades dos usuários.
2. A plataforma deve suportar a configuração de recebimento de modelo de agenda de eventos, incluindo modelo de Dia Inteiro, Dia da Semana e Feriado. Os usuários podem selecionar os modelos definidos pela plataforma ou personalizar um modelo.
3. A página Adicionar evento e alarme deve oferecer suporte à ativação da função de ignorar eventos ou alarmes recorrentes, e os usuários podem configurar a duração para ignorar.
4. A plataforma oferecerá suporte à configuração de grupos de destinatários de alarmes: após adicionar usuários ao grupo de destinatários de alarmes, os usuários do grupo receberão notificações assim que os alarmes forem disparados, sem precisar definir destinatários para cada alarme.
5. A plataforma oferecerá suporte à adição em lote de usuários como destinatários de alarmes.
6. A plataforma oferecerá suporte à seleção de destinatários de alarmes ou grupos de destinatários de alarmes para cada alarme.
7. A plataforma oferecerá suporte à configuração de eventos de disparo e alarmes para uma fonte.
8. A plataforma deve suportar a configuração de um ou vários feriados para um modelo de programação de recebimento de alarmes.

4.13.3 Ligação de Alarme

Ações de Ligação

1. A plataforma suportará a configuração de cores para eventos.
2. A plataforma oferecerá suporte à adição de modelos coloridos para reutilização posterior.
3. A plataforma deve suportar a configuração de Capturar Imagem como a ação de vinculação: defina a duração da captura de imagem antes ou depois que o evento ocorra.
4. A plataforma oferecerá suporte à configuração do Trigger Record como a ação de vinculação: iniciar a gravação antes que o evento aconteça e continuar a gravação após o evento acontecer, bloquear os vídeos gravados e definir a duração do bloqueio.
5. A plataforma deve oferecer suporte à configuração do Trigger PTZ como a ação de vinculação: selecione a chamada da predefinição, patrulha ou padrão da câmera PTZ vinculada.
6. A plataforma deve suportar a configuração Create Tag como a ação de vinculação. Selecione as câmeras para gravar vídeo quando o evento ou alarme ocorrer e defina o local de armazenamento para armazenar os arquivos de vídeo. O sistema adicionará uma tag à filmagem de vídeo acionada para uma pesquisa conveniente. Defina o intervalo de tempo para definir o comprimento marcado da filmagem de vídeo.
7. A plataforma deve suportar a definição de Link Access Point como a ação de vinculação: vincular todos os pontos de acesso ou pontos de acesso especificados.
8. A plataforma deve suportar a configuração Link Alarm Input como a ação de vinculação. Selecione entradas de alarme e essas entradas de alarme serão armadas ou desarmadas quando o alarme ocorrer.
9. A plataforma deve suportar a configuração de Link Alarm Output como a ação de vinculação. Selecione diferentes maneiras de fechar a saída de alarme quando a saída de alarme funcionar, defina o status de vinculação como On ou Off e defina para fechar a saída de alarme automaticamente ou manualmente.
10. A plataforma deve suportar a configuração Link Third-Party Integrated Resource como a ação de vinculação. Selecione o controle sobre as operações de detalhes que acontecerão quando o alarme ocorrer.
11. A plataforma deve suportar a configuração Enviar e-mail como a ação de vinculação. Selecione um modelo de e-mail para enviar as informações de alarme de acordo com as configurações de e-mail definidas. O usuário deve ser capaz de alterar o modelo de e-mail quando você configurar a ação de vinculação.
12. A plataforma deve suportar a configuração Link Printer como a ação de vinculação. Se o tipo de fonte for entrada de alarme, os usuários podem vincular para imprimir o relatório de contagem de entrada e saída de determinado grupo de contagem de entrada e saída.
13. A plataforma deve suportar a configuração Link Speak Unit como a ação de vinculação. Após vincular unidades de alto-falante a um evento ou alarme e selecionar um arquivo de áudio para ser reproduzido, o arquivo de áudio selecionado será reproduzido pelas unidades de alto-falante selecionadas quando o evento ou alarme for acionado.
14. A plataforma deve suportar a configuração de Link Alarm Partition (Area) como a ação de vinculação. Você pode armar ou desarmar as partições (áreas) quando ocorrerem alarmes.
15. A plataforma deve suportar o acionamento de um evento definido pelo usuário.

16. A plataforma deve suportar a configuração Trigger Remaining Open for Entrance and Exit como a ação de vinculação. Quando o evento ou alarme for disparado, a(s) entrada(s) e saída(s) selecionada(s) mudarão para o status de permanecer aberta(s) para que os veículos possam entrar ou sair do estacionamento sem autenticação ou permissão de guardas.
17. A plataforma deve oferecer suporte à configuração Enviar solicitação HTTP como a ação de vinculação para enviar solicitações HTTP para a plataforma de terceiros.

Gerenciamento de Alarmes em Tempo Real

1. A janela pop-up de alarmes deve suportar a edição da prioridade do alarme. Por padrão, três prioridades são fornecidas: alta, média e baixa.
2. A janela pop-up de alarmes deve suportar a edição do tipo de alarme. Por padrão, quatro tipos são fornecidos: true, false, to be recognized e to be verified.
3. O Web Client deve suportar a configuração se um evento pode ser disparado como um alarme. Ao configurar isso, os usuários podem selecionar os destinatários do alarme e definir a prioridade do alarme.
4. O Web Client deve suportar a configuração do Restrict Alarm Handling Time para o alarme. A saída de alarme vinculada ou eventos definidos pelo usuário devem ser acionados após a duração configurada.
5. O Web Client oferecerá suporte à ativação das seguintes funções para um alarme: janela pop-up, exibição de vídeo relacionado ao alarme no smart wall, relação de um alarme a um mapa e disparo de aviso sonoro.
6. Quando os usuários definem a gravação como a ação de vinculação, a plataforma deve oferecer suporte à seleção de exibição de vídeo gravado ou visualização ao vivo quando o alarme ocorrer.
7. A plataforma suportará o reconhecimento automático de alarmes pela plataforma. Quando a duração do atraso terminar, o alarme será reconhecido automaticamente.
8. A plataforma oferecerá suporte à exibição de vários alarmes não tratados e do número total de alarmes não tratados em uma janela de alarme pop-up no Control Client.

4.13.4 Alarme Combinado

Configuração de Regras

1. A plataforma suportará a vinculação de um alarme combinado com uma área de alarme acionado, que será usada para contar os alarmes acionados na área.
2. A plataforma oferecerá suporte à função de ignorar alarmes recorrentes, e os usuários poderão configurar a duração para ignorar.
3. A plataforma oferecerá suporte à configuração de quaisquer tipos de fontes de disparo.
4. A plataforma suportará quatro lógicas de disparo de alarme e suportará a configuração do intervalo de disparo entre dois alarmes.
5. A plataforma deve suportar a ativação ou desativação de alarmes. Ao desativar um alarme, os usuários podem definir o horário de início e a duração da desativação. Uma vez que um alarme é desativado, os usuários não receberão as notificações de alarme.
6. O alarme combinado deve suportar todas as ações de vinculação, exceto Vincular impressora.

Exibição de Alarme Combinada

1. A plataforma suportará a adição de um alarme combinado ao mapa.
2. A plataforma suportará a cópia das configurações de um alarme combinado para outros alarmes combinados.
3. A plataforma suportará o teste de um alarme combinado.

4.13.5 Configuração e Gerenciamento

1. Ao adicionar um evento, a plataforma deverá oferecer suporte à seleção de múltiplos eventos e fontes de disparo.
2. A plataforma oferecerá suporte à exclusão rápida de todos os eventos inválidos clicando no botão Excluir todos os itens inválidos.
3. A plataforma oferecerá suporte à configuração de vários eventos como alarmes em um lote.
4. A plataforma oferecerá suporte à ativação e desativação de vários alarmes em um lote.
5. A plataforma suportará alarmes de teste.
6. A plataforma suportará a filtragem de eventos definidos como alarmes.
7. A plataforma oferecerá suporte à filtragem de eventos e alarmes por tipo de fonte, nome do evento e alarme, área, fonte e evento de disparo.
8. A plataforma oferecerá suporte para destacar eventos e alarmes anormais com um ponto de exclamação vermelho.
9. A plataforma oferecerá suporte ao destaque de eventos e alarmes que não são suportados pelas fontes.
10. A plataforma suportará estatísticas de eventos e alarmes.
11. A plataforma suportará a classificação de eventos e alarmes por módulos.

4.13.6 Exibição de Alarme em Tempo Real

Relatório de Alarme

1. Após iniciar o Control Client, o usuário poderá receber os últimos 500 alarmes não reconhecidos.
2. A plataforma deve suportar números de todos os alarmes na plataforma, incluindo alarmes blindados, alarmes desabilitados, entradas de alarme, zonas e radares de segurança.
3. O usuário deverá poder exibir somente alarmes blindados.
4. O usuário deverá poder exibir alarmes que são exibidos somente na parede inteligente.
5. A plataforma deve suportar a exibição de fontes de alarme, tipos de alarme e os tempos de disparo de cada alarme. A plataforma deve suportar a expansão de um tipo de alarme para exibir toda a lista de alarmes.

Central de Alarme

1. A plataforma oferecerá suporte à seleção de diferentes layouts do Centro de Alarmes do Cliente de Controle, a saber: Vídeo e Imagem Relacionados, Mapa e ambos.
2. A plataforma suportará a exibição de mapas, vídeos e imagens relacionados a alarmes em uma tela auxiliar.

3. A plataforma oferecerá suporte à seleção dos itens exibidos na lista de alarmes, como status de marcação, prioridade, número, fonte, área, evento de disparo.
4. A plataforma suportará a personalização de ícones exibidos na coluna Operação da Central de Alarmes.
5. A plataforma deve suportar a seleção de vídeo ou imagem como o conteúdo padrão exibido nas informações de alarme. Imagem é recomendada para baixa largura de banda.
6. A plataforma oferecerá suporte à seleção do tipo de fluxo padrão para vídeo de vinculação na janela pop-up.
7. A plataforma deverá suportar o acionamento da janela pop-up de alarme.
8. A plataforma deverá suportar a ativação de aviso sonoro para um alarme.
9. A plataforma suportará a configuração de som de alarme para alarmes com prioridades diferentes.
10. A plataforma suportará a configuração dos horários de reprodução do som do alarme.
11. A plataforma suportará a filtragem de lista de alarmes em tempo real por prioridade, status de marcação e status de alarme.
12. A plataforma oferecerá suporte à desativação do prompt de voz após o reconhecimento de determinados alarmes.
13. A plataforma suportará a configuração de alarmes de baixa prioridade sem som de alarme.
14. A plataforma deve suportar reconhecimento em lote de todos os alarmes. Não mais do que 2.000 alarmes podem ser reconhecidos de uma vez.
15. A plataforma suportará alarmes agrupados por hora e agregação de alarmes por nome na Central de Alarmes do Cliente de Controle.
16. A plataforma oferecerá suporte à adição de uma categoria para personalizar as condições do filtro com base em suas necessidades no Alarm Center.

Mapa

O usuário poderá visualizar um alarme no mapa, visualizar detalhes do alarme no mapa e reconhecer um alarme no mapa.

4.13.7 Operação de Alarme

1. A plataforma deve suportar a exibição de detalhes de alarme, incluindo mapa relacionado, vídeo, imagem, descrição, logs de operação. Para diferentes tipos de eventos, os detalhes variam.
2. A página Visão geral oferecerá suporte à seleção de um evento ou alarme e alternará para a página Pesquisa de eventos e alarmes para pesquisar seus eventos/alarmes históricos.
3. A plataforma oferecerá suporte à reprodução de vídeos ao vivo e gravados de alarmes no Control Client, além de permitir arrastar a barra de tempo e ligar/desligar o áudio ao reproduzir o vídeo gravado.
4. A janela de vídeo relacionada ao alarme deve suportar áudio bidirecional entre as pessoas no local e o usuário da plataforma.
5. A janela de vídeo relacionada ao alarme deve suportar controle PTZ.
6. A plataforma oferecerá suporte à exibição de vídeos relacionados a alarmes na parede inteligente.

7. A plataforma suportará o download de informações de um alarme, incluindo detalhes do alarme, imagem, vídeo e mapa.
8. A plataforma deverá suportar blindagem e alarme.
9. A plataforma deve suportar o reconhecimento de um alarme ou reconhecimento de lote. Uma vez reconhecidos, os alarmes serão removidos da página Overview.
10. A plataforma deve suportar a edição de alarmes reconhecidos como não reconhecidos.
11. A plataforma suportará alarmes de marcação para destaque.
12. A plataforma deve suportar desabilitação de alarmes. Após desabilitar, o usuário não receberá o alarme quando ele for disparado.
13. A plataforma deverá suportar a ativação de alarmes após a desativação.
14. A plataforma deve suportar o bypass ou a restauração de entradas de alarme ignoradas.
15. A plataforma suportará armar e desarmar partições (áreas), entradas de alarme e radares de segurança.
16. A plataforma deverá suportar o acionamento manual de eventos definidos pelo usuário
17. A janela pop-up de alarme oferecerá suporte ao envio de e-mails contendo informações de alarme após selecionar os destinatários e o modelo de e-mail e inserir a descrição.
18. A plataforma oferecerá suporte ao encaminhamento de um alarme para usuários específicos.

4.13.8 Pesquisar e Exportar

Pesquisa de Eventos e Alarmes

1. A plataforma oferecerá suporte à busca de eventos por hora, área, tipo de evento e nome do evento.
2. A plataforma oferecerá suporte à busca de alarmes por hora de disparo, status de marcação, prioridade, tipo de alarme, status de reconhecimento, área, tipo de evento e nome do alarme.
3. A plataforma suportará a busca de eventos e alarmes pelas mesmas condições.
4. Após pesquisar eventos e alarmes, a plataforma oferecerá suporte à visualização de detalhes de eventos e alarmes e registros de operação.

Operações de Alarme

1. Os registros de operação de um alarme devem conter todas as operações no alarme, incluindo registros de encaminhamento, blindagem, recebimento, marcação, desativação e informações do usuário relacionadas às operações.
2. A plataforma deve suportar a exibição do mapa vinculado na janela pop-up de alarme e na página de detalhes do alarme. O mapa deve suportar a exibição de fontes de alarme, recursos ao redor dos recursos de alarme e a cobertura da área relacionada. A plataforma deve suportar alarmes ignorados em lote, iniciar áudio bidirecional e habilitar o áudio.
3. A plataforma deve suportar a abertura da janela do mapa por meio da janela pop-up de alarme e da página de detalhes do alarme. A plataforma deve suportar a exibição do mapa vinculado e executar operações relacionadas por meio do mapa.

Exportar Eventos e Alarmes

1. Após a busca por eventos e alarmes, a plataforma suportará a exportação dos resultados da

busca para o PC como um arquivo CSV/PDF. A plataforma suportará até 5.000 informações. A plataforma suportará a exportação de imagens relacionadas de no máximo 500.
2. A plataforma oferecerá suporte à exportação de alarmes correspondentes ou não correspondentes com informações detalhadas, como informações pessoais, número do cartão, número da placa e assim por diante.

4.13.9 Estatística e Análise

Visão Geral do Alarme

A plataforma suportará a contagem de alarmes do dia atual, incluindo alarmes reconhecidos e não reconhecidos.

Tendência de Alarme

1. A plataforma suportará a contagem de alarmes disparados nos últimos 7 e 30 dias.
2. A plataforma suportará a geração de mapas de tendências de tipos de eventos especificados.
3. A plataforma suportará a geração e exportação de mapas de tendências de alarmes de 7 dias nos formatos PDF, PNG e JPG.

Top 5 Análise de Alarme

1. A plataforma oferecerá suporte à exibição dos 5 principais eventos e alarmes acionados hoje ou nos últimos 7 e 30 dias.
2. A plataforma oferecerá suporte à exibição das 5 principais áreas de todos os eventos e alarmes disparados de hoje, dos últimos 7 e 30 dias.
3. A plataforma oferecerá suporte à contagem de tipos de eventos especificados e à geração dos 5 principais tipos de eventos.
4. A plataforma suportará a exportação de eventos em formato PDF, PNG ou JPG.

Relatório Agendado de Eventos e Alarmes

1. A plataforma oferecerá suporte ao envio regular de relatórios de eventos e alarmes por e-mail.
2. A plataforma suportará o envio de relatórios diários contendo informações sobre alarmes e eventos disparados no dia anterior ao dia atual.
3. A plataforma suportará o envio de relatórios semanais contendo informações sobre alarmes e eventos disparados nos últimos 7 ou 14 dias.
4. A plataforma suportará a definição de data e hora de envio de relatórios de eventos/alarmes.
5. A plataforma suportará a geração de relatórios de alarmes em formato Excel ou PDF.
6. A plataforma oferecerá suporte à geração de relatórios de alarme em vários idiomas.
7. A plataforma oferecerá suporte ao backup regular de relatórios de eventos e alarmes para o servidor SFTP.
8. A plataforma oferecerá suporte ao backup regular de relatórios de eventos e alarmes para o SYS.

4.13.10 Gerenciamento de Permissões

Permissão para Recebimento de Eventos e Alarmes

A plataforma deve suportar a seleção de destinatários de um alarme. Os usuários com permissão para receber alarmes podem receber as informações do alarme.

Permissão de Operação de Evento e Alarme

1. A plataforma deve suportar a atribuição de permissão de usuário para armar ou desarmar entrada de alarme.
2. A plataforma deve suportar a atribuição de permissão de usuário para ignorar ou recuperar entrada de alarme ignorada do dispositivo de controle de segurança.
3. A plataforma deve suportar a atribuição de permissão de usuário para reconhecimento de alarme.
4. A plataforma oferecerá suporte à atribuição de permissão de usuário para reconhecimento de alarmes em lote.
5. A plataforma oferecerá suporte à atribuição de permissão de usuário para reconhecer alarmes sem inserir comentários.
6. A plataforma oferecerá suporte à atribuição de permissão de usuário para encaminhamento de alarmes.
7. A plataforma deve oferecer suporte à atribuição de permissão do usuário para marcar o reconhecimento de alarme como não reconhecido.

Permissão de Pesquisa de Eventos e Alarmes

A plataforma oferecerá suporte à atribuição de permissão de usuário para pesquisa de eventos e alarmes.

4.14 Gestão de Evidências

Implantação e Acesso

1. A plataforma oferecerá suporte à configuração do servidor HCP como o servidor de gerenciamento de evidências.
2. A plataforma deve suportar a configuração do servidor SFTP como servidor de gerenciamento de evidências.
3. A plataforma oferecerá suporte à entrada de informações de gerenciamento de evidências por vários clientes: cliente móvel, cliente web e cliente de controle.
4. A plataforma oferecerá suporte ao gerenciamento do servidor Secure File Transfer Protocol (SFTP) (endereço/nome de usuário/senha).

Fonte do Arquivo

1. A plataforma suportará o upload de arquivos locais e a especificação da tag e da descrição do arquivo.
2. A plataforma oferecerá suporte para salvar os arquivos em Live View, Playback, Video Search e PC local no Evidence Management Center.

3. A plataforma oferecerá suporte para salvar os arquivos no Alarm Center e na Pesquisa de Eventos e Alarmes no Evidence Management Center.
4. A plataforma oferecerá suporte para salvar os arquivos (vídeos, eventos em tempo real, informações ANPR, eventos de direção, rastreamento de veículos, rotas) no módulo de Monitoramento de Bordo no Centro de Gerenciamento de Evidências.
5. A plataforma oferecerá suporte para salvar os arquivos no Módulo de Pesquisa de Pessoas, gerados a partir de páginas como Pesquisar Imagem Facial, Pesquisar Imagem Corporal Humana, Pesquisar Rostos Correspondentes, Pesquisar Pessoa por Frequência, Pesquisar Arquivo e Verificação de Identidade, no Centro de Gerenciamento de Evidências.
6. A plataforma oferecerá suporte para salvar os arquivos de contagem de entradas e saídas na página de Recuperação de Controle de Acesso no Centro de Gerenciamento de Evidências.
7. A plataforma oferecerá suporte para salvar os registros de eventos na página de Pesquisa de Patrulha no Centro de Gerenciamento de Evidências.
8. A plataforma oferecerá suporte para salvar os arquivos no módulo Estacionamento, gerados a partir de páginas como Pesquisa de Veículos Passantes na Entrada e Saída, Registros de Pagamento, Pesquisa de Veículos Estacionados, Registros de Estacionamento e Vários Veículos em um Status de Conta no Centro de Gerenciamento de Evidências.
9. A plataforma oferecerá suporte para salvar os arquivos de gravação de tela e os arquivos baixados no Centro de Download/Tarefas no Centro de Gerenciamento de Evidências.
10. A plataforma oferecerá suporte ao upload de evidências da câmera relacionada: selecione a câmera, o arquivo de evidência será carregado da câmera no horário especificado ou carregado quando o Wi-Fi estiver conectado.
11. A plataforma oferecerá suporte à definição de hora de início do upload/hora de término do upload/hora de início da gravação/hora de término da gravação.
12. A plataforma suportará múltiplos arquivos de evidências: fotos, vídeos, áudios e outros (arquivos no formato Excel, CSV, PDF, etc.).

Pesquisa de Arquivo

1. A plataforma oferecerá suporte à busca de arquivos por nome, remetente ou descrição.
2. A plataforma oferecerá suporte à busca de arquivos por tipo de arquivo, incluindo vídeo, áudio, imagem e outros.
3. A plataforma oferecerá suporte à busca de arquivos por tag de arquivo.
4. A plataforma oferecerá suporte à busca de arquivos por hora de início e término.
5. A plataforma oferecerá suporte à busca de arquivos por hora de upload.
6. A plataforma oferecerá suporte para salvar condições de pesquisa de arquivos para a próxima pesquisa.

Gerenciamento de Arquivos

1. A plataforma oferecerá suporte à edição do nome do arquivo e à visualização do tamanho/origem do arquivo.
2. A plataforma suportará a edição da tag do arquivo.
3. A plataforma oferecerá suporte à verificação da integridade do arquivo comparando o valor de verificação de integridade da plataforma e o do arquivo exportado.
4. A plataforma oferecerá suporte à exportação e exclusão de arquivos.

5. A plataforma oferecerá suporte à visualização dos registros de upload/download de arquivos.
6. A plataforma deve suportar o controle da permissão de arquivos vinculados a casos por pessoa. Apenas proprietários de arquivos, supervisores de proprietários de arquivos e destinatários de arquivos compartilhados devem poder visualizar o arquivo.
7. A plataforma oferecerá suporte ao compartilhamento de arquivos.
8. A plataforma oferecerá suporte à adição de marca d'água em vídeos, fotos e arquivos para proteção da privacidade de dados.
9. A plataforma deve suportar a vinculação de arquivo(s) a caso(s).

Gestão de Casos

1. A plataforma oferecerá suporte à busca de casos por nome/ID/descrição.
2. A plataforma oferecerá suporte à busca de casos por tipo de caso.
3. A plataforma oferecerá suporte à busca de casos por status do caso.
4. A plataforma oferecerá suporte à busca de casos por hora de criação.
5. A plataforma oferecerá suporte à busca de casos por hora de início/término.
6. A plataforma oferecerá suporte à exportação e exclusão de casos.
7. A plataforma oferecerá suporte à edição do nome do caso, ID do caso, ID do CAD, tipo de caso, status do caso, hora de início/término do caso e descrição do caso.
8. A plataforma oferecerá suporte à vinculação de um caso com vários arquivos.
9. A plataforma deve suportar o controle da permissão do caso por pessoa. Apenas proprietários do caso, supervisores de proprietários do caso e destinatários do caso compartilhado devem poder visualizar o caso.
10. A plataforma deve suportar edição de arquivos de vídeo de casos por meio de recorte, adição de mosaico, adição de texto, ativação/desativação de som. Esta função só estará disponível quando a licença Evidence Collection estiver habilitada.
11. A plataforma deve suportar a verificação da integridade de um arquivo de caso comparando o valor de verificação de integridade da plataforma e o do arquivo exportado. Esta função só estará disponível quando a licença de gerenciamento de evidências for adicionada.
12. A plataforma oferecerá suporte ao download de relatórios de casos.
13. A plataforma oferecerá suporte ao compartilhamento de casos.
14. A plataforma dará suporte à abertura ou fechamento dos casos.

Mapa de Evidências

O usuário poderá pesquisar e gerenciar arquivos/casos no Google Maps.

4.15 Controle de Acesso

- ***Guia de Aplicação***
- ***Gerenciamento de Dispositivos de Controle de Acesso***
- ***Gestão de Recursos em Múltiplas Áreas***
- ***Impressão de Cartões***
- ***Gerenciamento de Nível de Acesso***
- ***Gerenciamento de Funções Avançadas***

- ***Monitoramento em Tempo Real***
- ***Resposta Eficaz a Emergências***
- ***Registros de Acesso***
- ***Relatório Visualizado***
- ***Configurações de Proteção de Privacidade***

4.15.1 Guia de Aplicação

Assistente de configuração do controle de acesso que fica à direita e será exibido quando você passar o cursor sobre ele.

4.15.2 Gerenciamento de Dispositivos de Controle de Acesso

Acesso ao Dispositivo por meio de Vários Protocolos

1. Suporte ao acesso a dispositivos via Device Network SDK por endereço IP, segmento IP ou importação em lote.
2. Suporte ao acesso de dispositivos via ISUP por ID do dispositivo, segmento de ID ou importação em lote.
3. Lista de informações do dispositivo: nome do dispositivo, endereço, número de série, número da versão, número de portas, número de leitores, status da rede e força da senha.
4. A plataforma oferecerá suporte ao acesso de dispositivos via ISAPI por endereço IP, segmento IP ou importação em lote.

Configuração do Dispositivo

1. Configuração da plataforma (Device Network SDK): endereço IP, porta, alias, nome de usuário, senha, fuso horário e recurso de canal.
2. Configuração da plataforma (ISUP): ID do dispositivo, chave, alias, configuração de armazenamento, fuso horário e recurso de canal.
3. Suporte para definir um dispositivo de controle de acesso como um dispositivo de registro para que as informações pessoais e as credenciais adicionadas pelo dispositivo sejam sincronizadas automaticamente com a plataforma.
4. Suporte para acessar a página web de configuração do dispositivo.
5. Suporte para adicionar dispositivos de controle de acesso por meio de nome de domínio.
6. Para dispositivos que não suportam configuração via navegador da web, ele suporta ir para a página de configuração remota.

Controle Remoto do Dispositivo

1. Suporte para edição de senhas uma por uma ou em lote.
2. Configurações de fuso horário: suporte para configuração de fuso horário um por um ou em lote; suporte para obtenção de configurações de fuso horário de dispositivos e aplicação de configurações de fuso horário a dispositivos.
3. Suporte para restauração das configurações padrão dos dispositivos, um por um ou em lote.

Monitoramento de Status do Dispositivo em Tempo Real

1. Suporte para visualização de status online.
2. Suporte para visualização do status da rede.
3. Suporte para visualização do status do controlador da faixa principal e secundária (somente para catracas).
4. Suporte para visualização do status dos componentes da catraca (somente para catracas).
5. Suporte para visualização do status de armamento.
6. Suporte para visualização do status de violação do dispositivo.
7. Suporte para visualização do status da fonte de alimentação.
8. Suporte para visualização do primeiro tempo adicionado e do tempo de inspeção.

Abertura de Porta pelo Cliente Móvel

A plataforma suportará abertura de porta via bluetooth.

4.15.3 Gestão de Recursos em Múltiplas Áreas

Gestão de Portas

1. Informações básicas: nome da porta, dispositivo, sensor magnético da porta, tipo de botão de saída, duração da porta aberta, duração estendida da porta aberta, alarme de tempo limite de porta aberta, duração máxima da porta aberta, código de coação, super senha e código de coação. Os parâmetros reais dependem da capacidade do dispositivo.
2. A plataforma deverá suportar vinculação a câmeras: não mais do que duas câmeras podem ser vinculadas a cada porta.
3. A plataforma suportará a ligação de terminais de reconhecimento facial a uma cancela para controlar o acesso de pessoas.
4. A plataforma suportará a ligação de terminais de reconhecimento facial a um controlador de acesso para controlar o acesso de pessoas.
5. Armazenamento de imagens: armazenamento local, CVR, armazenamento em nuvem, pStor e Network Video Recorder (NVR). É válido quando as câmeras estão vinculadas e o armazenamento de imagens está habilitado.
6. Leitor: habilitar ou não, nome do leitor, tipo de leitor, intervalo mínimo de passagem do cartão, redefinição das configurações de entrada, alarme de tentativas de cartão com falha, detecção de violação, polaridade do LED OK, polaridade do LED ERR, polaridade do buzzer e nível de segurança da impressão digital. Os parâmetros reais dependem da capacidade do dispositivo.
7. Lista de informações de recursos: nome da porta, endereço IP do dispositivo, dispositivo, status da rede, informações do leitor, status de aberto/fechado restante e área.
8. A plataforma oferecerá suporte à obtenção de nomes de portas dos dispositivos.
9. A plataforma oferecerá suporte à aplicação de nomes de portas aos dispositivos.
10. A plataforma oferecerá suporte à definição da prioridade de captura para câmeras vinculadas.

Gestão de Piso

1. Informações básicas: nome do elevador, dispositivo, duração da porta aberta, duração

estendida da porta aberta, alarme de tempo limite de porta aberta, duração máxima da porta aberta, código de coação, super senha e código de coação. Os parâmetros reais dependem da capacidade do dispositivo.
2. Piso: Nº e nome. A plataforma suportará a redefinição de pisos em lote.
3. A plataforma deverá suportar vinculação a câmeras: não mais do que duas câmeras podem ser vinculadas a cada porta.
4. Armazenamento de imagens: armazenamento local, CVR, armazenamento em nuvem, pStor e Network Video Recorder (NVR). É válido quando as câmeras estão vinculadas e o armazenamento de imagens está habilitado.
5. Leitor: habilitar ou não, nome do leitor, tipo de leitor, intervalo mínimo de passagem do cartão, redefinição das configurações de entrada, alarme de tentativas de cartão com falha, detecção de violação, polaridade do LED OK, polaridade do LED ERR, polaridade do buzzer e nível de segurança da impressão digital. Os parâmetros reais dependem da capacidade do dispositivo.
6. Lista de informações de recursos: nome do elevador, endereço IP do dispositivo, dispositivo, status da rede e área.
7. A plataforma oferecerá suporte à obtenção de nomes de andares de dispositivos.
8. A plataforma oferecerá suporte à aplicação de nomes de piso aos dispositivos.
9. A plataforma oferecerá suporte à configuração de relações entre relés de controle de elevador e andares na página de configuração remota.

Gerenciamento de Entrada de Alarme

1. Informações básicas: nome e dispositivo de entrada do alarme.
2. Lista de informações de recursos: nome da entrada do alarme, endereço IP do dispositivo, dispositivo, número da partição, área e status da rede.

Gerenciamento de Saída de Alarme

1. Informações básicas: nome da saída de alarme.
2. Lista de informações de recursos: nome da saída do alarme, endereço IP do dispositivo, dispositivo e área.

Gestão de Recursos por Área

1. A plataforma suportará a adição de múltiplas áreas e cada área contém múltiplos recursos diferentes.
2. A plataforma oferecerá suporte a vários níveis de áreas.

4.15.4 Gerenciamento de Credenciais

Gestão de Cartões

1. A plataforma suportará até 20 dígitos para um número de cartão.
2. A plataforma suportará adicionar até cinco cartões por pessoa.
3. A plataforma suportará a inserção manual do número do cartão.
4. A plataforma oferecerá suporte a estações de registro de cartões que leiam números de cartões.

5. Ao ler o número do cartão por meio de uma estação de registro de cartão, a plataforma deverá oferecer suporte à seleção do formato do cartão.
6. A plataforma suportará a criptografia de setores do cartão (um setor por vez) somente quando a criptografia for feita por meio da estação de registro do cartão (comunicando-se com a plataforma via USB).
7. A plataforma deve suportar estações de registro (comunicando-se com a plataforma via rede) lendo números de cartão (tipos de cartão suportados, incluindo EM, M1, ID, DESfire, FeliCa e CPU).
8. A plataforma suportará estações de registro (comunicando-se com a plataforma via USB) lendo números de cartão (tipos de cartão suportados, incluindo EM, M1, ID, DESfire, FeliCa e CPU).
9. A plataforma suportará qualquer leitor de cartão de dispositivos de controle de acesso remoto que leia números de cartão.
10. Tipos de cartas: comum, coação e dispensar.
11. A plataforma suportará a emissão de cartões em lote.
12. A plataforma oferecerá suporte para notificação de perda de cartão e cancelamento do relatório de perda de cartão.

Gerenciamento de Impressão Digital

1. A plataforma suportará até 10 impressões digitais por pessoa.
2. A plataforma oferecerá suporte a dispositivos de registro de impressões digitais.
3. A plataforma suportará o registro de impressões digitais por meio da estação de registro (comunicando-se com a plataforma via rede).
4. A plataforma suportará o registro de impressões digitais por meio da estação de registro (comunicando-se com a plataforma via USB).
5. A plataforma suportará qualquer leitor de cartão de dispositivos de controle de acesso remoto que registrem impressões digitais.
6. Tipos de impressão digital: comum, coação e rejeição.
7. A plataforma oferecerá suporte à verificação de duplicatas de impressões digitais e à classificação da qualidade das impressões digitais.

Gerenciamento de Imagem Facial

1. A plataforma suportará apenas uma foto de rosto por pessoa.
2. A plataforma oferecerá suporte ao upload de fotos de rostos locais.
3. A plataforma suportará o uso de uma câmera USB ou de um laptop com uma câmera que registre fotos de rosto.
4. A plataforma suportará inversão de imagem espelhada ao capturar fotos de rosto com uma câmera USB.
5. A plataforma oferecerá suporte ao registro de fotos faciais por meio da estação de registro (comunicando-se com a plataforma via rede).
6. A plataforma suportará o registro de fotos faciais por meio da estação de registro (comunicando-se com a plataforma via USB).
7. A plataforma oferecerá suporte à coleta de imagens faciais por meio de dispositivos de controle de acesso remoto.
8. A plataforma oferecerá suporte à exportação de todas as fotos faciais de todas as pessoas

adicionadas como um arquivo ZIP e à definição de uma senha para descompactar o arquivo ZIP.
9. A plataforma deve oferecer suporte à exclusão de credenciais faciais ou à exclusão em lote de credenciais faciais.
10. A plataforma oferecerá suporte ao salvamento de dados de modelagem ilegíveis de fotos de perfil na plataforma, para que as fotos de perfil reais não sejam exibidas na plataforma.
11. A plataforma oferecerá suporte a testes de qualidade de imagem de perfil por dispositivos de controle de acesso e dispositivos de videoporteiro.
12. A plataforma oferecerá suporte a testes de qualidade de imagem de perfil por barreiras vinculadas a um terminal de reconhecimento facial MinMoe.

Posto de Matrícula

A plataforma suportará o salvamento automático dos parâmetros da estação de inscrição, mantendo a última configuração após o novo login.

Gerenciamento de Senhas

1. A plataforma deverá suportar a definição de senha (única, contendo de 4 a 8 dígitos, e apenas uma senha por pessoa)
2. A plataforma suportará a geração automática de código PIN.

Gestão de Íris

1. A plataforma permitirá a coleta de 2 íris para cada pessoa.
2. A plataforma oferecerá suporte à coleta de íris por dispositivo remotamente como credenciais pessoais e à aplicação de íris aos dispositivos.

Código QR Estático

1. A plataforma suportará a geração de código QR estático com base no número do cartão da pessoa.
2. A plataforma oferecerá suporte à visualização e ao download de códigos QR estáticos para distribuí-los aos funcionários.

Código QR Dinâmico

1. A plataforma oferecerá suporte à seleção do modo de código QR como estático ou dinâmico.
2. A plataforma suportará a configuração do período de validade (1 min por padrão) de um código QR dinâmico.
3. A plataforma oferecerá suporte aos funcionários para visualizar o código QR dinâmico (atualizado automaticamente conforme programado) e atualizar manualmente o código QR após efetuar login no Mobile Client.

4.15.5 Impressão de Cartões

Personalização do modelo de cartão

1. Suporte para personalizar modelos de cartão: defina o formato como vertical ou horizontal, defina o estilo da frente e/ou verso, insira imagens, insira texto e insira campos de

informações pessoais.
2. Suporte para inserção de linhas de corte em modelos de cartão.
3. Suporte à impressão de códigos QR estáticos de pessoas em cartões.
4. Suporte para pré-visualização do modelo de cartão.
5. Suporte ao alinhamento de texto e conteúdo.
6. Suporte para ajustar a camada de conteúdo e texto no cartão.
7. Suporte para personalizar o tamanho do texto no cartão e o alinhamento horizontal.
8. Suporte para personalizar o tamanho das imagens adicionadas ao cartão.
9. Suporte para configuração de cor de fonte e fonte em negrito.
10. Suporte para quebra de linha automática de texto inserido, nome, nome, sobrenome, e-mail, observação e informações personalizadas.

Compatível com impressoras de cartão convencionais

1. A plataforma oferecerá suporte a impressoras de cartão convencionais, como HID Fargo e Magicard; a especificação de cartão suportada é CR80; suporte a impressão de um ou dois lados.
2. A plataforma suportará Zebra ZC350 para impressão de cartões.
3. A plataforma oferecerá suporte ao acesso de impressoras de cartões via USB.

Impressão rápida de cartões

Suporte para impressão de cartões um por um ou em lote.

4.15.6 Gerenciamento de nível de acesso

Painel

1. A plataforma oferecerá suporte a assistente, status de integridade do dispositivo, status de credencial da pessoa, tendência de acesso, top 5 de registros anormais, contagem de entradas e saídas e eventos de entrada e saída em tempo real.
2. A plataforma oferecerá suporte à configuração rápida do controle de acesso na página Visão geral do controle de acesso.

Gestão de Férias

A plataforma suportará a configuração de até 32 feriados regulares ou irregulares.

Gerenciamento de modelos de agendamento de acesso

1. A plataforma deve suportar três modelos de agendamento de acesso padrão: modelo de dia inteiro, modelo de dia da semana e modelo de fim de semana. Os modelos padrão não podem ser editados ou excluídos.
2. A plataforma deve suportar a criação de novos modelos de cronograma de acesso ou a cópia de um modelo existente. Os modelos incluem cronogramas semanais e cronogramas de feriados.
3. A plataforma oferecerá suporte à entrada manual de hora e minuto precisos para desenhar períodos de tempo de modelos de cronograma.

Gerenciamento de nível de acesso

A plataforma oferecerá suporte à configuração de níveis de acesso para todos ou pontos de acesso específicos.

Atribuição de nível de acesso multidimensional

1. A plataforma oferecerá suporte à atribuição de níveis de acesso por nível de acesso.
2. A plataforma oferecerá suporte à atribuição de níveis de acesso por pessoa.
3. A plataforma oferecerá suporte à atribuição de níveis de acesso por organização.
4. A plataforma oferecerá suporte à atribuição de níveis de acesso específicos por grupo de acesso.
5. A plataforma oferecerá suporte à busca de pessoas por nome e ID do funcionário.
6. A plataforma oferecerá suporte à aplicação automática de configurações de nível de acesso aos dispositivos após atribuir níveis de acesso a pessoas, departamentos e grupos de acesso.

Aplicação manual do nível de acesso

1. A plataforma oferecerá suporte à especificação de pessoas e dispositivos para aplicar níveis de acesso imediatamente ou posteriormente.
2. A plataforma deverá suportar a aplicação de níveis de acesso inicialmente (primeiro limpar e depois aplicar).
3. A plataforma oferecerá suporte à exibição do progresso da aplicação e aos detalhes das falhas na aplicação.
4. A plataforma deve suportar estatísticas de status da aplicação de níveis de acesso.

Aplicação automática de nível de acesso

1. A plataforma suportará a aplicação automática de níveis de acesso em um horário fixo todos os dias. O horário pode ser configurado e é 1:00 da manhã por padrão.
2. A plataforma suportará a aplicação automática de níveis de acesso a cada certas horas todos os dias. O intervalo pode ser configurado e é de 1 hora por padrão.

Processamento rápido de exceções

1. A plataforma oferecerá suporte a estatísticas de status de credenciais: número de pessoas, rostos, cartões, impressões digitais e pessoas sem credenciais; A plataforma oferecerá suporte à visualização e exportação de estatísticas de pessoas de diferentes status.
2. A plataforma oferecerá suporte a estatísticas de status do dispositivo: exceção do dispositivo, a ser aplicado e excepcional ao aplicar. A plataforma oferecerá suporte à visualização e exportação de estatísticas do dispositivo de diferentes status.
3. A plataforma deve oferecer suporte à detecção do status de aplicação do nível de acesso por pessoa especificada, incluindo aplicação com falha, aplicação bem-sucedida e a ser aplicada; A plataforma deve oferecer suporte à aplicação de níveis de acesso novamente.
4. A plataforma deve oferecer suporte à detecção de nível de acesso aplicado por ponto de acesso especificado, incluindo aplicação com falha e aplicação bem-sucedida; A plataforma deve oferecer suporte à aplicação de níveis de acesso novamente.

Visão geral do nível de acesso

1. A plataforma deve fornecer estatísticas dos resultados da aplicação do nível de acesso, incluindo o número total de pessoas, o número de pessoas com nível de acesso anormal/anormal e o número de pessoas com nível de acesso não aplicado.
2. A plataforma oferecerá suporte à visualização do resultado da aplicação do nível de acesso de qualquer pessoa.
3. A plataforma oferecerá suporte à aplicação manual de todos os níveis de acesso de uma pessoa ou à execução manual da aplicação inicial para qualquer pessoa.

4.15.7 Gerenciamento de Funções Avançadas

Primeira pessoa em

1. A plataforma oferecerá suporte para permanecer aberta com o primeiro cartão e a primeira autorização de cartão.
2. A plataforma oferecerá suporte para permanecer aberta com autorização em primeira pessoa.

Autenticação multifator

1. A plataforma oferecerá suporte à adição de grupos de autenticação multifator.
2. A plataforma oferecerá suporte à configuração de regras de autenticação multifator com base no grupo de autenticação multifator, incluindo modelo de agendamento de acesso, modo de autenticação, ordem de leitura do cartão do grupo de autenticação e intervalo de leitura do cartão.
3. A plataforma oferecerá suporte à especificação de usuários para abrir a porta remotamente.

Intertravamento de várias portas

A plataforma suportará intertravamento de múltiplas portas de um dispositivo.

Anti-Passback

1. A plataforma deve suportar anti-passback de área de um dispositivo ou entre vários dispositivos.
2. A plataforma deve suportar anti-passback de rota de um dispositivo ou entre vários dispositivos.
3. A plataforma deve oferecer suporte à ativação ou desativação do anti-passback de perdão regular.
4. A plataforma oferecerá suporte à configuração de anti-passback para cancelas.

Anti-Passback controlado por plataforma

1. A plataforma deve oferecer suporte à configuração de anti-passback de área controlada pela plataforma de um único dispositivo ou de vários dispositivos.
2. A plataforma deve oferecer suporte à configuração de anti-passback de rota controlada pela plataforma de um único dispositivo ou de vários dispositivos.
3. A plataforma oferecerá suporte à configuração do tempo de perdão regular das regras anti-passback controladas pela plataforma.

4. A plataforma deve suportar a ativação/desativação da regra anti-passback controlada pela plataforma.

Permanecendo aberto ou fechado

A plataforma suportará a configuração de agendamentos de acesso livre e acesso proibido em lote.

Modo de autenticação

1. A plataforma oferecerá suporte à configuração de modos de autenticação do leitor.
2. A plataforma oferecerá suporte à configuração de modos de autenticação privada de pessoas.

Código de autenticação

A plataforma suportará a configuração de até 500 códigos de autenticação diferentes. Somente o controlador de acesso DS-K260X suporta esta função.

Porta Aberta pelo Cliente Móvel

1. A plataforma suportará abertura automática de portas via Bluetooth.
2. A plataforma suportará a abertura da porta via bluetooth girando o smartphone.
3. A plataforma suportará abertura de porta via NFC.

Aplicando Anúncio

A plataforma oferecerá suporte à aplicação de anúncios em dispositivos de controle de acesso.

Transmissão de áudio

1. A plataforma suportará a configuração em lote de transmissões de áudio, incluindo transmissões de áudio diárias e transmissões de áudio específicas.
2. A plataforma oferecerá suporte à visualização de detalhes de registros de dispositivos e imagens capturadas (se houver) no módulo Recuperação de Dados Gravados do Dispositivo.

4.15.8 Monitoramento em tempo real

Monitoramento de status de porta em tempo real

1. A plataforma deverá suportar a exibição do status do magnético da porta/fechadura da porta.
2. A plataforma oferecerá suporte à exibição de status de bloqueio de porta com ícones coloridos: amarelo para permanecer bloqueado, verde para permanecer desbloqueado e cinza para bloqueio e desbloqueio.
3. A plataforma oferecerá suporte à visualização ao vivo de câmeras vinculadas.
4. A plataforma suportará a seleção de múltiplos pontos de acesso (você pode arrastar o mouse ou clicar para selecionar enquanto pressiona a tecla Shift).
5. A plataforma oferecerá suporte à seleção de todos os pontos de acesso.

Monitoramento de eventos em tempo real

1. A plataforma suportará o upload de eventos em tempo real.
2. A plataforma suportará filtragem por tipo de evento.

3. A plataforma suportará filtragem por ponto de acesso.
4. A plataforma suportará a personalização das colunas a serem exibidas.
5. A plataforma oferecerá suporte à assinatura de tipos específicos de eventos.
6. A plataforma deve suportar uma exibição duradoura das informações sobre a pessoa reconhecida no momento, incluindo foto de perfil, foto de rosto e introdução da pessoa. A plataforma deve suportar a transformação da janela em uma janela de miniatura.

Monitoramento em tempo real no mapa

1. A plataforma oferecerá suporte à exibição do status dos recursos em tempo real (ponto de acesso, entrada de alarme e saída de alarme).
2. A plataforma suportará controle remoto em tempo real (ponto de acesso, entrada de alarme e saída de alarme).
3. A plataforma suportará a exibição de alarmes de recursos (ponto de acesso, entrada de alarme e saída de alarme) em tempo real.
4. A plataforma suportará visualização ao vivo em tempo real da câmera vinculada à porta.
5. A plataforma oferecerá suporte à exibição de contagens regionais de entradas e saídas em tempo real.
6. A plataforma oferecerá suporte à exibição de intertravamento de múltiplas portas em tempo real.
7. A plataforma suportará a exibição de anti-passback em tempo real.

4.15.9 Resposta eficaz a emergências

Controle de porta emergente em lote

Suporte para controle remoto de portas, uma por uma ou em lote, em tempo real.

Chamada

1. Suporta a vinculação de entrada de alarme para manter automaticamente todas as portas ou portas de uma área específica abertas.
2. Suporte para acionar automaticamente a impressora para imprimir a lista de pessoas hospedadas de todas as áreas ou de uma área específica.

4.15.10 Registros de acesso

Recuperação de Registros de Acesso de Identidade

1. A plataforma oferecerá suporte à filtragem de pessoas resignadas.
2. A plataforma oferecerá suporte à busca de registros de acesso de identidade e exportação para arquivos Excel ou CSV.
3. A plataforma oferecerá suporte à exportação de registros de entrada e saída para arquivos PDF.
4. A plataforma oferecerá suporte à obtenção automática de registros de acesso de identidade perdidos do dispositivo por meio de programação.
5. A plataforma oferecerá suporte à obtenção manual de todos os registros de acesso de

identidade durante o período de tempo especificado do dispositivo.
6. A plataforma oferecerá suporte à importação manual de registros de acesso de identidade exportados do dispositivo para a plataforma.
7. A página Pesquisa de Acesso à Identidade deve oferecer suporte à personalização de itens de coluna a serem exibidos.

Recuperação de dados gravados do dispositivo

1. A plataforma oferecerá suporte à busca de dados registrados do dispositivo que podem ser exportados para arquivos Excel ou CSV.
2. A plataforma oferecerá suporte à exportação de logs de dispositivos para arquivos PDF.

Recuperação de Contagem de Entrada e Saída

1. A plataforma oferecerá suporte à busca de resultados de contagem de entradas e saídas que podem ser exportados para arquivos Excel ou CSV.
2. A plataforma oferecerá suporte à exportação de estatísticas de contagem de autenticação final para arquivos PDF.

4.15.11 Relatório Visualizado

1. Suporte aos registros de acesso atuais que podem ser exportados para arquivos PDF, JPG ou PNG.
2. Suporte à tendência de acesso atual, que pode ser exportada para arquivos PDF, JPG ou PNG.
3. Suporte aos 5 principais registros anormais de hoje, que podem ser exportados para arquivos PDF, JPG ou PNG.
4. Apoie a contagem regional de pessoas que ficaram.

4.15.12 Configurações de proteção de privacidade

1. Configuração de armazenamento de eventos: substituir, excluir eventos antigos regularmente e excluir eventos antigos em um horário especificado.
2. Configuração de autenticação: se deseja exibir a foto, o nome, o número do funcionário e a temperatura no resultado da autenticação.
3. Configuração de upload e armazenamento de imagens: carregar imagens reconhecidas ou capturadas, salvar imagens reconhecidas ou capturadas, salvar fotos de perfil, carregar imagens de eventos e alarmes, salvar imagens de eventos e alarmes, carregar imagens térmicas e salvar imagens térmicas.
4. Limpe rapidamente as imagens armazenadas no dispositivo: limpe as imagens de rosto e as imagens reconhecidas ou capturadas.
5. Exclua fotos de rosto de uma pessoa ou de todas as pessoas.

4.16 Gestão de Visitantes

- ***Reserva e check-in/out***

- ***Passe de visitante***
- ***Terminal de visitantes***
- ***Acesso de visitantes***
- ***Registros de visitantes***

4.16.1 Reserva e Check-In/Out

Reserva de Visitante

1. O administrador pode fazer reservas para visitantes no Web Client e no Mobile Client.
2. A plataforma oferecerá suporte à importação em lote de informações de reservas de visitantes e à substituição de visitantes repetidos.

Reserva de autoatendimento

1. Os funcionários podem fazer reservas para visitantes em um navegador da web escaneando um código QR usando um telefone celular.
2. A plataforma oferecerá suporte à exibição do código QR do visitante logo após a reserva de autoatendimento bem-sucedida no Mobile Client.
3. A plataforma deve oferecer suporte à verificação da qualidade facial em um dispositivo que tenha esse recurso.
4. A plataforma deve suportar a habilitação de aprovação de reserva de autoatendimento. Quando estiver habilitada, todas as reservas de autoatendimento serão efetivadas após a revisão e aprovação do administrador.
5. A plataforma oferecerá suporte à definição do grupo de visitantes padrão para reserva de autoatendimento.
6. O administrador pode revisar os registros de reservas de autoatendimento e então aprovar, rejeitar ou excluir as reservas.
7. A plataforma oferecerá suporte à configuração de fluxos de aprovação de visitantes.
8. A plataforma oferecerá suporte aos revisores especificados nos fluxos de aprovação de visitantes para aprovar e rejeitar as reservas dos visitantes após o login de autoatendimento.
9. A plataforma oferecerá suporte à configuração de níveis de acesso para visitantes ao fazer reservas de autoatendimento.
10. A plataforma oferecerá suporte à atribuição de permissão para revisão de reservas a usuários específicos.

Envio automático do código de reserva do visitante

A plataforma oferecerá suporte ao envio automático de um código de reserva de 4 ou 6 dígitos ao visitante por e-mail ao fazer reservas.

Estacionamento para visitantes

A plataforma oferecerá suporte à abertura da cancela quando os veículos dos visitantes chegarem, desde que o número da placa seja preenchido no momento da reserva.

Check-in de visitantes

1. Para visitantes com reserva, eles podem fazer check-in fornecendo o código de reserva,

número de telefone ou número do certificado. As informações dos visitantes serão mostradas e podem ser editadas ou repostas.
2. Para visitantes sem reserva, os usuários podem fazer o check-in no local preenchendo as informações dos visitantes.
3. Para visitantes sem reserva, mas que já visitaram o local anteriormente, os usuários podem selecionar as pessoas do grupo de visitantes para fazer um check-in rápido para eles.
4. A plataforma oferecerá suporte à exportação de informações de check-in de visitantes e registros de acesso.
5. A plataforma oferecerá suporte à verificação rápida de qualquer visitante do histórico, independentemente de o visitante ter sido excluído ou não.
6. A plataforma oferecerá suporte à leitura das informações do passaporte por meio do leitor de passaporte KR420.
7. A plataforma oferecerá suporte à leitura de informações do cartão de identificação dos Emirados Árabes Unidos por meio do leitor de cartão de identificação dos Emirados Árabes Unidos conectado ao PC.
8. A plataforma deve suportar a leitura das informações do cartão de identificação tailandês por meio do leitor de cartão de identificação tailandês conectado ao PC. Leitores de cartão de identificação tailandês suportados: HawkEye (TRK2700RB e TRK2700R), Elyctis (IDBox PDK3302R2S).

Envio automático de código QR de acesso

A plataforma suportará o envio do QR code de acesso às áreas permitidas para o e-mail dos visitantes, caso o endereço de e-mail seja preenchido no momento do check-in.

Código QR dinâmico

1. A plataforma suportará a alternância entre o código QR estático e o código QR dinâmico.
2. A plataforma suportará a configuração do período de validade do código QR dinâmico (1 minuto por padrão).
3. A plataforma oferecerá suporte à verificação do código QR dinâmico, à atualização automática do código QR dinâmico e à atualização manual do código QR pelos visitantes após a reserva bem-sucedida.

Check-out do visitante

1. A plataforma oferecerá suporte à finalização de compra manual para os visitantes.
2. A plataforma oferecerá suporte à configuração de vários pontos de acesso como pontos de check-out de autoatendimento.
3. A plataforma oferecerá suporte à configuração de vários leitores de cartão como pontos de check-out de autoatendimento.
4. A plataforma oferecerá suporte ao check-out nos pontos de check-out de autoatendimento.
5. A plataforma deve oferecer suporte à ativação de "Check-out automático para visitante após período efetivo" para que a plataforma não emita alarmes de permanência excedente.
6. A plataforma deve suportar a verificação rápida de um visitante por meio do número de identificação do visitante, número de telefone, nome ou número do cartão, ou escaneando o QR Code no passe do visitante. Para disponibilizar a digitalização de QR codes, os usuários

precisam adicionar dispositivos de digitalização à plataforma.

7. A plataforma oferecerá suporte à busca de visitantes para que possam fazer o check-out passando o passaporte no leitor de passaportes KR420 conectado ao PC onde o Web Client é executado.

Personalização de acordo com as necessidades dos usuários

1. A plataforma oferecerá suporte à personalização dos motivos das visitas.
2. A plataforma oferecerá suporte à personalização de grupos de visitantes.
3. A plataforma oferecerá suporte à personalização de modelos de e-mail de reserva.
4. A plataforma oferecerá suporte à personalização de modelos de e-mail de check-in.
5. A plataforma suportará a personalização dos dígitos do código de reserva.
6. A plataforma oferecerá suporte à personalização do horário padrão de check-out.
7. A plataforma oferecerá suporte à personalização dos campos de informações na página de reserva do visitante ou na página de check-in do visitante.

Check-in não necessário se a reserva for confirmada

1. A plataforma deverá oferecer suporte para habilitar/desabilitar a plataforma para fazer o check-in automático dos visitantes quando reservas forem feitas para eles."
2. Quando o recurso estiver habilitado, os visitantes não farão check-in na área de recepção. Eles poderão acessar os pontos de acesso especificados diretamente por meio dos códigos QR em seus passes de visitante. Quando o recurso estiver desabilitado, os visitantes deverão fazer check-in na área de recepção primeiro antes de poderem acessar os pontos de acesso.

Notificar pessoas relacionadas por e-mail

1. A plataforma oferecerá suporte ao envio automático de um e-mail ao anfitrião quando uma reserva for feita.
2. A plataforma oferecerá suporte ao envio automático de um e-mail ao anfitrião quando uma reserva não for efetuada.
3. A plataforma oferecerá suporte ao envio automático de um e-mail ao visitante quando a reserva do visitante não for efetuada.
4. A plataforma oferecerá suporte ao envio automático de um e-mail ao anfitrião quando o visitante correspondente fizer check-in.
5. A plataforma fornecerá modelos de e-mail padrão.

Envie os resultados da reserva via WhatsApp

1. A plataforma oferecerá suporte à digitalização do código QR do WhatsApp fornecido pelo anfitrião com o WhatsApp e à realização de uma reserva no WhatsAPP.
2. A plataforma oferecerá suporte ao recebimento dos resultados da reserva via WhatsApp após a reserva, incluindo os detalhes da reserva e o código QR do visitante (código QR estático ou URL do código QR dinâmico).
3. Consulte ***Integração de protocolos*** para configurações de contas do WhatsApp.
4. A plataforma oferecerá suporte ao toque no botão nas mensagens do WhatsApp recebidas pelos visitantes para abrir os links de reserva, links de QR code estáticos e links de QR code dinâmicos.

4.16.2 Passe de Visitante

1. A plataforma suportará impressora termossensível de 58 mm.
2. A plataforma oferecerá suporte à edição do modelo de passe de visitante personalizado de forma visualizada e à pré-visualização do modelo.
3. A plataforma oferecerá suporte à configuração dos campos de informações do visitante, imagem de fundo, imagens personalizadas, textos personalizados, fonte e tamanho da fonte do modelo de passe de visitante.
4. A plataforma oferecerá suporte à definição de cores de texto para modelos de passes de visitantes.
5. A plataforma oferecerá suporte à impressão automática de um passe de visitante quando o visitante fizer o check-in; oferecerá suporte à impressão manual de um passe de visitante a qualquer momento.

4.16.3 Terminal de Visitantes

1. Os modelos de terminais de visitantes suportados devem incluir DS-K5032 (Autoatendimento), DS-K5032-D (Serviço de equipe), DS-K5032-3XFD (Serviço de equipe e triagem de temperatura).
2. A plataforma oferecerá suporte ao gerenciamento básico de terminais de visitantes, incluindo adição e exclusão de terminais de visitantes, alteração de senhas, configuração de fuso horário, restauração de parâmetros padrão, atualização de firmware e busca de terminais de visitantes na mesma LAN por meio do SADP.
3. A plataforma oferecerá suporte à aplicação de níveis de acesso aos terminais de visitantes adicionados à plataforma.
4. A plataforma oferecerá suporte à aplicação das informações do host aos terminais de visitantes adicionados à plataforma.
5. A plataforma oferecerá suporte à aplicação de códigos de reserva aos terminais de visitantes adicionados à plataforma.
6. A plataforma deverá suportar a sincronização bidirecional das informações dos visitantes registrados (da plataforma para os terminais dos visitantes ou vice-versa).

4.16.4 Acesso de Visitantes

Acesso restrito para visitantes

1. A plataforma oferecerá suporte à definição dos níveis de acesso dos visitantes e à definição de um nível de acesso padrão para novos visitantes.
2. A plataforma oferecerá suporte à aplicação automática de níveis de acesso aos dispositivos de controle de acesso após o check-in.
3. A plataforma oferecerá suporte à retirada dos níveis de acesso dos visitantes após o check-out.

Lista de bloqueio de visitantes

1. A plataforma oferecerá suporte à movimentação de visitantes para a lista de bloqueio.

2. A plataforma oferecerá suporte à remoção de visitantes da lista de bloqueio.
3. A plataforma oferecerá suporte à importação em lote de informações de visitantes para lista de bloqueio e substituição de visitantes repetidos.
4. Os usuários não poderão fazer reservas ou check-in para os visitantes na lista de bloqueio. A plataforma deverá suportar a notificação do usuário ao reservar ou fazer check-in para visitantes na lista de bloqueio.

Foto do certificado de visitante

1. Ao fazer uma reserva ou fazer o check-in de um visitante, os usuários poderão enviar uma foto ou tirar uma foto do certificado por meio da webcam do PC (Web Client) ou da câmera do celular (Mobile Client).
2. A plataforma oferecerá suporte à exibição da foto do certificado durante a finalização da compra.

Verificação de pertences de visitantes

1. Ao fazer o check-in de um visitante, os usuários poderão enviar uma foto ou tirar uma foto dos pertences do visitante por meio da webcam do PC (Web Client) ou da câmera do celular (Mobile Client).
2. A plataforma deve suportar a exibição da foto pertencente ao finalizar a compra. O usuário pode escolher tirar a foto novamente.

Alarme de permanência excessiva de visitante

1. A plataforma deve suportar a notificação de um alarme quando um visitante não fizer o check-out após o horário de check-out. O usuário pode escolher habilitar o check-out automático ou habilitar a detecção de alarme para detectar visitantes que estão excedendo o horário de check-out.
2. A plataforma oferecerá suporte à exibição de informações do visitante ao emitir um alarme de permanência excessiva.

Lista de observação de visitantes

1. A plataforma deve suportar a configuração da lista de observação para monitorar visitantes especiais por nome, empresa e número de ID. Os procedimentos envolvidos incluem reserva, revisão de reserva e check-in.
2. A plataforma deve suportar a abertura automática de uma janela de notificação quando um visitante registrado no processo de reserva ou check-in tiver atributos que correspondam a entidades na lista de observação; suporte para fazer uma reserva, fazer check-in ou rejeitar o visitante. Além disso, as estatísticas de tempos de rejeição são suportadas.

Gerenciar permissão para acessar o grupo de visitantes

A plataforma oferecerá suporte à atribuição de permissão de acesso a um grupo específico de visitantes a usuários específicos.

4.16.5 Registros de visitantes

Estatísticas diárias de visitantes

1. A plataforma oferecerá suporte à exibição do número total de visitantes e visitantes não registrados no dia atual.
2. A plataforma oferecerá suporte à filtragem e listagem de informações dos visitantes (categorizadas por total ou visitantes não verificados).
3. A plataforma oferecerá suporte à exportação dos resultados da pesquisa.

Pesquisa de registros de acesso de visitantes

1. A plataforma oferecerá suporte à busca de visitantes definindo condições, incluindo número do certificado, nome, número de telefone, empresa, visitante, motivo da visita, horário da visita, status de check-in/out e status da temperatura da superfície da pele.
2. A plataforma oferecerá suporte à exportação dos resultados da pesquisa.
3. A plataforma suportará o registro do último ponto de acesso de um visitante.

Pesquisa de Registros de Entrada e Saída

Consulte ***Registros de acesso*** .

Painel de visitantes

A plataforma oferecerá suporte à visualização da visão geral dos dados relacionados aos visitantes em um painel, incluindo o número de visitantes no dia atual, visitantes que fizeram check-in, visitantes que fizeram check-out e visitantes que fizeram check-in, mas não fizeram check-out.

4.17 Estacionamento

- ***Operação de estacionamento***
- ***Cobrança de Taxa de Estacionamento***
- ***Configuração do estacionamento***
- ***Alarmes no estacionamento***

4.17.1 Configuração do estacionamento

Parâmetros básicos

1. A plataforma oferecerá suporte à adição de vários estacionamentos para gerenciamento.
2. A plataforma deve suportar adicionar, excluir e editar estacionamentos. As configurações básicas para um estacionamento incluem o número de faixas, o número de vagas de estacionamento, o número de vagas de estacionamento vagas, o número de vagas de estacionamento para veículos registrados, o número de vagas de estacionamento vagas para veículos registrados, a duração máxima de estacionamento permitida, etc.
3. A plataforma adicionará subestacionamentos a um único estacionamento.
4. A plataforma oferecerá suporte à configuração das faixas adicionadas à entrada e saída de um

estacionamento, incluindo o nome da faixa, horário de entrada e saída, regra de entrada e saída para diferentes tipos de veículos, etc.

5. A plataforma deverá suportar a configuração das seguintes formas de abertura da cancela na entrada e saída:
   a. Abra após reconhecer o número da placa;
   b. Aberto após o proprietário do veículo passar seu cartão;
   c. Aberto após receber confirmação do centro.
6. A plataforma suportará áudio bidirecional entre a entrada e saída e o call center por meio de dispositivos de interfone de vídeo.
7. A plataforma suportará áudio bidirecional entre a entrada e saída e o call center por meio da estação de entrada/saída.
8. A plataforma oferecerá suporte à configuração de telas de orientação para entradas e saídas, e à configuração das informações exibidas nas telas de orientação, incluindo número da placa, taxa de estacionamento, etc.
9. A plataforma suportará a adição de dispositivos de controle de entrada/saída à plataforma no Web Client.
10. A plataforma oferecerá suporte ao gerenciamento de vagas de estacionamento ao ar livre e à configuração de orientação de estacionamento ao ar livre no Web Client.
11. A plataforma suportará a adição de dispositivos de controle de entrada/saída via ISUP.
12. A plataforma oferecerá suporte à conexão de câmeras às faixas para monitoramento diário.
13. A plataforma deve suportar a configuração do modo de taxa de estacionamento para um estacionamento. Se os usuários definirem o modo de taxa de estacionamento como "Cobrar", os usuários podem selecionar uma moeda de acordo com o país onde o estacionamento está localizado.
14. A plataforma deve suportar a ligação de uma estação de entrada/saída com uma linha para controlar a barreira. Após um veículo temporário ou um veículo sem placa receber um tíquete ou cartão de uma estação de entrada/saída, a estação controlará o portão da barreira para abrir e deixar o veículo entrar.
15. A plataforma dará suporte à busca de veículos que passam nas entradas e saídas de um estacionamento.
16. A plataforma oferecerá suporte à pesquisa de duração de estacionamento e registros de estacionamento de um veículo específico.
17. A plataforma oferecerá suporte à pesquisa da taxa de ocupação de diferentes andares e diferentes tipos de vagas de estacionamento.
18. A plataforma deverá suportar a ligação de uma faixa com dois dispositivos de controle de acesso.
19. A plataforma oferecerá suporte à atribuição de permissão de estacionamento por usuário.
20. A plataforma oferecerá suporte à configuração do número da placa exibida como número da placa registrada ou número da placa capturada pelo ANPR.
21. O usuário deverá ser capaz de configurar o toque para chamadas dos dispositivos do estacionamento no Control Client. O usuário deverá ser notificado com um som quando uma chamada for recebida.
22. A plataforma suportará a exibição de um texto de teste nas telas de exibição para testar a conexão do dispositivo.

Regra de entrada e saída

1. A plataforma oferecerá suporte à configuração do modo de entrada e saída, incluindo:
   a. Modo de entrada: sem entrada repetida, correspondência de placa e cartão;
   b. Modo de saída: correspondência de placa e cartão, se deve permitir que um veículo saia quando sua taxa de estacionamento for 0.
23. A plataforma deve oferecer suporte para habilitar ou desabilitar a dedução automática da conta.
24. A plataforma deve suportar a configuração do método de entrada e saída para veículos de acordo com seus tipos (veículo registrado/veículo temporário/veículo visitante). O método pode ser "Manual" ou "Automático", e o último. A plataforma deve suportar a configuração do intervalo de tempo de entrada e saída.
25. A plataforma oferecerá suporte à configuração para permitir a entrada de veículos registrados/temporários/visitantes quando não houver vagas de estacionamento disponíveis.
26. A plataforma oferecerá suporte à configuração do método de entrada e saída ("Manual" ou "Automático") por lista de veículos e intervalo de tempo de entrada e saída.
27. A plataforma oferecerá suporte à configuração para permitir ou não a entrada de veículos na lista quando não houver vagas de estacionamento disponíveis.
28. A plataforma suportará a configuração do número de vagas de estacionamento e do número de vagas de estacionamento vagas por lista de veículos, e os parâmetros configurados serão aplicados somente aos veículos dessa lista de veículos.
29. A plataforma oferecerá suporte à configuração de entrada e saída gratuitas em feriados.
30. A plataforma oferecerá suporte à configuração do modo de precificação para vários veículos em uma conta, incluindo pagamento por veículo extra e pagamento pelo primeiro veículo que sair.
31. A plataforma suportará a ligação de duas unidades de captura com uma faixa.
32. A plataforma suportará a ligação de uma câmera ANPR com duas faixas para ser aplicável à entrada e saída sem cancela instalada.
33. A plataforma oferecerá suporte à configuração do modo de entrada como Correspondência de Pessoa e Placa no Cliente Web.
34. A plataforma deve suportar a configuração de ligação de alarme. Quando o alarme for disparado, as entradas e saídas selecionadas ou todas permanecerão abertas.

Regra de taxa de estacionamento

   a. A plataforma suportará a configuração da regra de tarifa de estacionamento para veículos em lista e veículos temporários, a regra inclui: Gratuito;
   b. Cobrar por duração de estacionamento da unidade;
   c. Cobrar por sessão;
   d. Cobrar por intervalo de tempo;
   e. Cobrar por hora do relógio;
   f. Cobrança por tempo e sessão, durante o dia e a noite;
   g. Cobrar por intervalo de tempo unitário.
2. A plataforma oferecerá suporte para relacionar um passe de estacionamento a um veículo registrado. Os tipos de passe de estacionamento são: anual, mensal, personalizado (dias),

mensal (tempo ocioso).
3. A plataforma oferecerá suporte à visualização e verificação da regra de tarifa de estacionamento para garantir que ela atenda aos requisitos dos usuários.
4. A plataforma deve suportar a configuração do método de desconto para uma regra de desconto. O método inclui desconto percentual, desconto de taxa, estacionamento gratuito e redução da duração do estacionamento.
5. A plataforma oferecerá suporte à configuração da regra de taxa de estacionamento para passes excepcionais para cobrar uma taxa fixa para passes excepcionais.
6. A plataforma suportará configurações adicionais para configurar a duração do estacionamento gratuito após o pagamento.
7. A plataforma oferecerá suporte à emissão de cartões temporários.

Orientação de estacionamento

1. A plataforma deverá suportar a adição de andares a um estacionamento e a adição de terminais de orientação e telas de orientação aos andares adicionados.
2. A plataforma oferecerá suporte à adição de um mapa a um estacionamento e à configuração de vagas de estacionamento para o estacionamento no mapa, incluindo a posição dos estacionamentos e a vaga de estacionamento nº.
3. A plataforma deve suportar a configuração de vagas de estacionamento reservadas. Quando várias vagas de estacionamento são monitoradas por uma câmera ANPR, as vagas de estacionamento reservadas são consideradas ocupadas.
4. A plataforma suportará telas de orientação de marcação no mapa para exibir o número de vagas de estacionamento vagas.
5. A plataforma oferecerá suporte à configuração do tipo de vaga de estacionamento, como vaga de estacionamento privada ou vaga de estacionamento com cobrança.
6. A plataforma oferecerá suporte à configuração de tipos e cores de vagas de estacionamento.
7. A plataforma suportará a montagem de câmeras ANPR no último andar para contar o número de veículos que entram e saem. O número de vagas de estacionamento vagas será exibido no terminal de orientação.
8. A plataforma suportará a contagem de vagas de estacionamento em diferentes andares pela câmera ANPR. Com as câmeras ANPR, o número de veículos que entram e saem de um andar pode ser contado, e o número de vagas de estacionamento em tempo real de um andar pode ser exibido.
9. A plataforma deve suportar a habilitação ou desabilitação de estatísticas de vagas de estacionamento para andares específicos de acordo com o modelo de tempo. Durante o tempo de desabilitação, as vagas de estacionamento vagas de andares específicos não serão incluídas nas estatísticas de vagas de estacionamento vagas ou exibidas na tela de orientação de entrada.
10. A plataforma oferecerá suporte à verificação das informações exibidas atualmente em uma tela de orientação interna (DS-TVL121) e à visualização de informações detalhadas sobre as vagas de estacionamento vinculadas a ela, como número da vaga, andar onde a vaga está localizada, se a vaga está ocupada e a imagem da vaga capturada no momento.
11. A plataforma oferecerá suporte à relação de listas de veículos com a vaga de estacionamento ao configurar os tipos de vaga de estacionamento.

12. A plataforma oferecerá suporte à exibição de dados de outros estacionamentos na tela de orientação do estacionamento atual.
13. A plataforma suportará a adição direta de telas de orientação de entrada à plataforma sem adicionar um terminal de estacionamento com o modelo TPE400.
14. A plataforma suportará a adição direta de câmeras de estacionamento.

Cliente de localização de veículos de autoatendimento

1. A plataforma oferecerá suporte à exibição da posição do proprietário do veículo no Self-Service Vehicle Finding Client.
2. O Self-Service Vehicle Finding Client (Android) deve ser instalado no DS-TPW332-C Query Terminal (Android) ou nos terminais de consulta de terceiros. O Client deve ajudar a encontrar veículos no estacionamento facilmente. Quando o proprietário do veículo estiver procurando o veículo, ele deve oferecer suporte à exibição do proprietário do veículo e da posição do veículo no mapa.
3. O Cliente deverá dar suporte ao planejamento da rota de localização do veículo.

4.17.2 Cobrança de Taxa de Estacionamento

Métodos para cobrança de estacionamento

1. Pague no Centro de Pedágio (ambos suportados no Web Client e no Control Client): A plataforma deve suportar a busca por um veículo específico para obter sua taxa de estacionamento inserindo o número da placa, selecionando a imagem exibida (se a placa de um veículo não for capturada e registrada), passando o cartão temporário ou escaneando o recibo de estacionamento. A taxa de estacionamento será cobrada manualmente pelo operador no centro de pedágio. Após o pagamento da taxa de estacionamento, o veículo deve sair do estacionamento dentro de um período especificado.
2. Pagamento no guichê: a plataforma oferecerá suporte à busca de um veículo específico para obter sua taxa de estacionamento, inserindo o número da placa ou passando o cartão temporário para coletar manualmente a taxa de estacionamento e permitir que o veículo saia do estacionamento.

Recibo de estacionamento

1. A plataforma suportará a impressão do recibo de estacionamento.
2. A plataforma oferecerá suporte à impressão de recibos após a recarga dos cartões de estacionamento.

4.17.3 Operação do estacionamento

Visão geral do espaço de estacionamento

1. A plataforma oferecerá suporte à visão geral das vagas de estacionamento para visualizar as estatísticas das vagas, incluindo a taxa de ocupação das vagas, o número de vagas, o número de vagas vagas, o número de vagas ocupadas, etc.
2. A plataforma oferecerá suporte à visualização de informações detalhadas sobre uma vaga de

estacionamento no mapa.
3. A plataforma oferecerá suporte à busca de veículos por número de vaga de estacionamento, número da placa e tempo de estacionamento.
4. A plataforma oferecerá suporte à exportação de detalhes de vagas de estacionamento com status desconhecido, como números de vagas de estacionamento relacionadas e informações correspondentes sobre o estacionamento e o andar, para o PC local como um arquivo XLSX.

Pesquisa de Registros

1. A plataforma oferecerá suporte à busca fuzzy de placas, e os usuários poderão personalizar as regras de busca.
2. A plataforma oferecerá suporte à busca de veículos que passam detectados por entradas e saídas, e à exibição das informações relacionadas.
3. A plataforma oferecerá suporte à busca de registros de veículos de visitantes por hora, nome do visitante, etc., e à exibição de informações relacionadas.
4. A plataforma oferecerá suporte à busca de registros de estacionamento por hora, número da placa, status do estacionamento, etc., e exibirá as informações relacionadas.
5. A plataforma oferecerá suporte à busca de veículos estacionados em estacionamentos e à exibição de informações relacionadas.
6. A plataforma oferecerá suporte à busca de registros de pagamento por hora, número da placa, operador, tipo de veículo, etc., e exibirá informações relacionadas.
7. A plataforma oferecerá suporte à busca de registros de recarga e reembolso por hora, número da placa, tipo de veículo, tipo de transação, método de transação, etc., e exibirá informações relacionadas.
8. A plataforma oferecerá suporte à busca de registros de transações de contas por hora, conta do proprietário do veículo, tipo de transação, etc., e exibirá informações relacionadas.
9. A plataforma oferecerá suporte à busca de registros de turnos de operadores por hora e operador, além de exibir informações relacionadas.
10. Na página de Busca de Registro de Estacionamento, a plataforma oferecerá suporte para pular para a página de Busca de Pessoas e procurar por pessoas que passaram pelo veículo dentro do período de estacionamento do veículo.
11. A plataforma oferecerá suporte à busca de registros de cupons por tipo de veículo, status do cupom, regra de desconto, etc., e à exibição de informações relacionadas.

Estatísticas e Relatórios

1. A plataforma oferecerá suporte à visualização de estatísticas de estacionamentos, como a integridade dos dispositivos (terminais de orientação, câmeras de estacionamento, etc.).
2. A plataforma oferecerá suporte à exibição de estatísticas de operação do estacionamento por tempo, incluindo estatísticas em tempo real de vagas de estacionamento, taxa de ocupação de um estacionamento, distribuição da duração do estacionamento, fluxo de tráfego, etc. A plataforma oferecerá suporte à exportação do relatório estatístico para o PC local.
3. A plataforma oferecerá suporte à exibição de estatísticas de transações por tempo, incluindo o tipo de receita, tendência de receita, etc., e a plataforma oferecerá suporte à exportação do relatório estatístico para o PC local.
4. A plataforma suportará o envio do relatório de análise da operação do estacionamento por

dia, semana ou mês.
5. A plataforma oferecerá suporte à personalização do layout de exibição do relatório de análise de operação selecionando diferentes tipos de estatísticas.

Controle de entrada e saída

1. A plataforma oferecerá suporte à exibição de imagens capturadas em tempo real de veículos que passam e exibirá informações relacionadas, incluindo número da placa, tempo de passagem, etc.
2. A plataforma oferecerá suporte à adição do número da placa de um veículo que passa à lista de veículos na plataforma para gerenciamento ao visualizar os registros de passagem de veículos em tempo real.
3. A plataforma oferecerá suporte à busca de veículos que passam e à visualização de vídeos das câmeras ANPR e das câmeras vinculadas.
4. A plataforma suportará a reprodução de vídeos ao vivo transmitidos pelas câmeras relacionadas a entradas e saídas.
5. A plataforma deve suportar a abertura e o fechamento da cancela, e fazer com que a cancela permaneça aberta manualmente.
6. A plataforma oferecerá suporte à edição manual do número da placa caso a câmera ANPR reconheça o número da placa incorretamente.
7. A plataforma deverá suportar a exibição de informações sobre turnos de operadores e a impressão de informações sobre o pagamento gerenciado pelos operadores, incluindo o valor total arrecadado, o valor total do desconto, etc.
8. A plataforma oferecerá suporte à exibição de vagas de estacionamento vagas de diferentes listas de veículos nas telas de orientação na faixa de entrada e saída de um estacionamento.
9. A plataforma deverá suportar a exibição do número de vagas de estacionamento disponíveis para veículos na lista quando os veículos na lista entrarem no estacionamento.
10. A plataforma oferecerá suporte à configuração do prompt de entrada e saída não permitidas para informar ao motorista os motivos pelos quais a entrada/saída não é permitida.

4.17.4 Alarmes no estacionamento

1. A plataforma oferecerá suporte ao upload regular de relatórios de horas extras de estacionamento para o SFTP ou armazenamento local para gerenciamento de evidências.
2. A plataforma deverá suportar o alarme de condução na linha da faixa.
3. A plataforma suportará o alarme de detecção de movimento TPM.

4.18 Inspeção de Segurança

- ***Canal de Inspeção de Segurança***
- ***Visualização de inspeção de segurança***
- ***Recebimento de alarme em tempo real***
- ***Estatísticas e Relatórios***
- ***Pesquisa de dados históricos***

4.18.1 Canal de Inspeção de Segurança

1. A plataforma suportará adicionar canais de inspeção de segurança à área. Suportará excluir e editar canais de inspeção de segurança.
2. A plataforma deve suportar dispositivos de ligação ao canal de inspeção de segurança. Até 1 analisador e 3 detectores de metal walk-through podem ser ligados.
3. A plataforma deve suportar vinculação de câmera de rede para cada canal de inspeção de segurança. Até 8 câmeras de rede são permitidas para cada canal de inspeção de segurança.

4.18.2 Visualização da inspeção de segurança

Visualização baseada em canais de inspeção de segurança

1. Suporte para visualização de informações sobre pacotes em tempo real, incluindo a imagem do pacote, o número total de pacotes, o número total de pacotes com artigos proibidos e o número total de artigos proibidos.
2. Suporte para marcação de artigos detectados em imagens de pacotes. As imagens podem ser ampliadas.
3. Suporte à configuração de artigos proibidos para alarmes em tempo real.
4. Suporte para visualização da imagem em tempo real do proprietário do pacote.
5. Suporte para visualização da imagem em tempo real da pessoa revistada, do número total de pessoas revistadas e do número total de pessoas que portavam metal.
6. Suporte para visualização da temperatura em tempo real da pessoa verificada (se o detector de metais for compatível com medição de temperatura).

Visualização Baseada em Analisadores

1. Suporte à visualização ao vivo e reprodução dos vídeos de inspeção do analisador.
2. Suporte para marcação de artigos detectados em fluxo de vídeo. Suporte para visualização de vídeo no modo de tela cheia, captura, gravação e troca entre fluxo principal e fluxo secundário.
3. Suporte para visualização de fotos do pacote e do proprietário do pacote.

Visualização baseada em detectores de metais walk-through

1. Suporte para visualização de informações detectadas em tempo real
2. Suporte para visualização de informações de temperatura em tempo real da pessoa detectada (se o detector de metais walk-through suportar a função de medição de temperatura).

4.18.3 Recebimento de Alarme em Tempo Real

Alarme de Artigo Proibido

A plataforma suportará o recebimento de alarmes em tempo real quando o artigo proibido for detectado.

Alarme de detecção de metais

A plataforma suportará o recebimento de alarmes em tempo real quando o metal for detectado.

Alarme de ausência

A plataforma oferecerá suporte ao recebimento de alarmes em tempo real quando for detectada a ausência anormal do pessoal de segurança.

Manuseio de Artigos Proibidos

1. A plataforma oferecerá suporte à configuração de tipo de artigo proibido para artigos proibidos.
2. A plataforma oferecerá suporte à seleção de uma ação de manuseio para artigos proibidos detectados em sistemas de inspeção de segurança, analisadores ou detectores de metais.

4.18.4 Estatísticas e Relatórios

Detecção de Pacotes

1. Suporte à geração de relatórios de detecção de pacotes por dia, semana, mês e ano.
2. Suporte para visualização do número total de pacotes detectados e do número total de pacotes com artigos proibidos de canais de inspeção de segurança específicos dentro de um período específico.
3. Suporte para visualização da porcentagem de pacotes com artigos proibidos de canais específicos de inspeção de segurança dentro de um período específico.
4. Suporte para visualização de tipos de artigos proibidos dentro de um período específico.

Inspeção de Pessoas

1. Suporte para geração de relatórios de inspeção de pessoas por dia, semana, mês e ano.
2. Suporte para visualização do número total de pessoas detectadas e do número total de pessoas com metais de canais de inspeção de segurança específicos dentro de um período específico.
3. Suporte à visualização da porcentagem de alarmes de detecção de metais de canais específicos de inspeção de segurança dentro de um período específico.

4.18.5 Pesquisa de Dados Históricos

Pesquisa de registro de detecção de pacote

1. Suporte à busca de registros de detecção de pacotes por hora, tipo de artigo proibido e canal. O resultado inclui hora de detecção de pacotes, local, tipo de artigo e número de artigos proibidos.
2. Suporte para visualização de detalhes do pacote, incluindo fotos do pacote, fotos capturadas do proprietário do pacote e vídeos gravados antes/depois do pacote ser detectado.

Pesquisa de registro de detecção de metais

1. Suporte à busca de registros de detecção de metais por hora e canal. O resultado inclui hora de detecção, local e intensidade do sinal do metal.
2. Suporte à visualização de detalhes do metal, incluindo localização do metal, intensidade do sinal e vídeos gravados antes/depois da detecção do metal.

Pesquisa de Registro de Ausência

1. Suporte à busca de registros de ausência por hora e canal. O resultado inclui tempo de ausência, local e duração da ausência.
2. Suporte para visualização de detalhes de ausência, incluindo os vídeos gravados antes da saída do pessoal e depois do retorno do pessoal.

4.19 Triagem de Temperatura

- ***Configuração de serviço***
- ***Cadastro de Pessoa***
- ***Monitoramento de temperatura***
- ***Estatísticas e Relatórios***

4.19.1 Configuração de Serviço

Gerenciamento de dispositivos

Suporte para adição de câmeras com funções de triagem de temperatura.

Configuração de triagem de temperatura

1. Suporte à criação de grupos de pontos de triagem de temperatura e à adição de pontos de triagem de temperatura aos grupos.
2. Suporte para configuração do limite para triagem de temperatura.
3. Suporte para configuração do limite para alarmes de temperatura.

4.19.2 Registro de Pessoa

Suporte ao registro de informações pessoais caso a pessoa rastreada não esteja registrada, incluindo nome, documento de identidade, número de telefone, se é de áreas de alto risco, descrição, etc.

4.19.3 Monitoramento de temperatura

Monitoramento de temperatura

1. Suporte ao registro de informações pessoais caso a pessoa rastreada não esteja registrada, incluindo nome, documento de identidade, número de telefone, se é de áreas de alto risco, descrição, etc.
2. Suporte para visualização de imagens capturadas em tempo real do grupo de pontos de triagem de temperatura especificado.
3. Suporte para visualização de imagens capturadas anteriormente no modo miniatura com a imagem do rosto da pessoa, temperatura, cor da marca de temperatura, status de uso da máscara, etc.

4. Suporte para visualização de informações de alarme do grupo de pontos de triagem de temperatura especificado, incluindo a imagem capturada da pessoa, temperatura, cor da marca de temperatura, status de uso da máscara, etc.
5. Suporte para visualização de imagens capturadas em tempo real do ponto de triagem de temperatura especificado.
6. Suporte para visualização de imagens capturadas anteriormente no modo miniatura com a imagem do rosto da pessoa, temperatura, cor da marca de temperatura, status de uso da máscara, grupo de pessoas, etc.
7. Suporte para visualização de eventos de triagem de temperatura em tempo real, incluindo nome da pessoa, temperatura, cor da marca de temperatura, status de uso da máscara, etc.

Dados históricos

1. Suporte à busca por dados históricos de triagem de temperatura do grupo de pontos de triagem de temperatura especificado. O resultado inclui a imagem capturada da pessoa, temperatura, cor da marca de temperatura, status de uso da máscara, grupo de pessoas, etc.
2. Suporte para busca de informações de pessoas registradas. O resultado inclui nome da pessoa, ID, número de telefone, se é de áreas de alto risco, responsável pelo registro, horário de registro, horário de triagem, etc.
3. Suporte à busca por eventos de triagem de temperatura do ponto de triagem de temperatura especificado. O resultado inclui hora do evento, canal, status de uso da máscara, se a temperatura está anormal, etc.

4.19.4 Estatísticas e Relatórios

1. Suporta os seguintes tipos de relatórios: relatório diário, relatório semanal, relatório mensal, relatório anual e relatório com intervalo de tempo personalizado.
2. Suporte para análise de resultados por ponto de triagem de temperatura. Suporte para exibição de estatísticas gerais de triagem e estatísticas de pessoas com temperatura anormal ou aquelas que não usam máscaras faciais.
3. Suporte para análise de resultados por departamento. Suporte para exibição de estatísticas gerais de triagem e estatísticas de pessoas com temperatura anormal ou aquelas que não usam máscaras faciais.
4. Suporte para exportar o relatório para o PC local.

4.20 Vídeo porteiro

- ***Módulo Independente***
- ***Gerenciamento de dispositivos de intercomunicação de vídeo***
- ***Áudio bidirecional ao vivo***
- ***Aviso de Aplicação***
- ***Registro de chamadas***
- ***Centralizada do Módulo de Vídeo Porteiro***

4.20.1 Módulo Independente

1. Suporta módulo de interfone de vídeo independente e entrada independente para o módulo.
2. Suporta o painel que inclui manutenção do dispositivo, estatísticas diárias de avisos aplicados e estatísticas de chamadas do dia atual.
3. Suporta configuração em lote de parâmetros para dispositivos de intercomunicação de vídeo.

4.20.2 Gerenciamento de dispositivos de intercomunicação de vídeo

Acessando dispositivos por meio de vários protocolos

1. A plataforma oferecerá suporte ao acesso de dispositivos via Device Network SDK ou endereço IP.
2. A plataforma oferecerá suporte à exibição de informações do dispositivo, incluindo nome do dispositivo, localização, número de série, versão, número de portas, número de câmeras, número de entradas de alarme, número de localização, status da rede e força da senha.

Configuração do dispositivo

1. Configuração de parâmetros da plataforma (SDK de rede do dispositivo): endereço IP, porta, alias, nome de usuário, senha, fuso horário e recurso de canal.
2. A plataforma suportará a configuração em lote do tempo para dispositivos de videoporteiro.
3. Configuração do número de localização do dispositivo
   - Estação interna: nº da comunidade, nº do prédio, nº da unidade e nº da sala.
   - Estação de porta: nº da comunidade, nº do prédio e nº da unidade.
   - Estação externa/Estação principal: comunidade No.
4. A plataforma deverá suportar a configuração do número do andar para estações internas.
5. A plataforma deverá suportar a vinculação de informações dos moradores (somente para a estação interna).
6. A plataforma deve suportar o salto para a página de configuração do dispositivo.
7. A plataforma deve suportar o acesso à biblioteca de configuração (somente para dispositivos que não suportam a configuração via navegador da web).
8. A plataforma suportará a conexão de estações internas com câmeras (até 16 câmeras por estação interna).
9. A plataforma deverá suportar a ligação da campainha com a estação interna.
10. A plataforma oferecerá suporte à aplicação de pacotes de software em estações internas em lote.

Configurações do dispositivo aplicadas

A plataforma suportará a aplicação do número de localização e dos parâmetros de rede correspondentes de todos os dispositivos de intercomunicação de vídeo a todos os dispositivos.

Controle remoto do dispositivo

1. A plataforma deverá suportar a alteração da senha (única ou em lote).
2. Configurações de fuso horário: obter as configurações de fuso horário de um dispositivo e aplicar essas configurações a outros dispositivos (individualmente ou em lote).

3. A plataforma deve suportar a restauração do parâmetro padrão (único ou em lote).

Detecção em tempo real do status do dispositivo

1. A plataforma oferecerá suporte à exibição do status online do dispositivo.
2. A plataforma oferecerá suporte à visualização do status da rede do dispositivo.
3. Status de conexão persistente do áudio bidirecional chamado pelo dispositivo.
4. A plataforma deve suportar a visualização do status de armamento.
5. A plataforma oferecerá suporte à visualização do status da bateria do dispositivo.
6. A plataforma oferecerá suporte à visualização do momento em que o dispositivo é adicionado pela primeira vez e do momento de sua primeira inspeção.

4.20.3 Áudio Bidirecional ao vivo

Cronograma de chamadas da estação de porta

1. A plataforma deverá suportar a configuração de agendamentos para chamada da estação interna ou da central de gerenciamento (plataforma ou estação principal).
2. A plataforma suportará a importação de agendamentos de chamadas de estações de porta em lote. (Excel)

Áudio bidirecional entre a plataforma e a estação de porta

1. A plataforma suportará áudio bidirecional.
2. A plataforma suportará visualização ao vivo durante áudio bidirecional.
3. A plataforma suportará gravação e salvamento de vídeo e áudio no PC local.
4. A plataforma suportará controle remoto de porta durante áudio bidirecional.
5. A plataforma oferecerá suporte ao desbloqueio remoto da porta antes de atender a chamada.

Áudio bidirecional entre a plataforma e a estação interna

1. A plataforma suportará áudio bidirecional.
2. A plataforma suportará visualização ao vivo durante áudio bidirecional.
3. A plataforma oferecerá suporte ao início de áudio bidirecional na janela pop-up do evento.

Especificar pessoas para atender chamadas

1. A plataforma oferecerá suporte a pessoas específicas para atender a chamada no dispositivo.
2. A plataforma oferecerá suporte a pessoas específicas para atender chamadas em períodos de tempo específicos.

Áudio bidirecional entre o dispositivo e o cliente da Web

A plataforma oferecerá suporte a chamadas para estações internas e atendimento de chamadas de dispositivos por meio do Web Client.

Sequência de Atendimento de Chamadas

Quando dispositivos de intercomunicação de vídeo ligarem para a Central, a primeira chamada não atendida será listada como a primeira a ser atendida.

Salvando automaticamente o volume do áudio bidirecional

No módulo de interfone de vídeo, o volume de áudio bidirecional do microfone e do alto-falante será salvo e usado no áudio bidirecional seguinte.

4.20.4 Aviso de Aplicação

Aplicação em lote de avisos para estações internas

1. Suporta a aplicação em lote de avisos para estações internas. Os avisos podem incluir imagens e textos que podem ser exibidos em vários idiomas, por exemplo, russo.
2. Oferece suporte à pesquisa de avisos de histórico definindo condições, incluindo tema, conteúdo, residente, tipo e hora.
3. Suporta exportação de avisos de histórico.
4. Suporte à aplicação de avisos relacionados a eventos/alarmes.

4.20.5 Registro de Chamadas

Chamadas entre plataformas e estações internas / estações de porta

1. Suporta salvar registros de chamadas entre a plataforma e estações internas/estações de porta.
2. Suporta visualização rápida de estatísticas de chamadas (número e registros de chamadas atendidas ou não atendidas).
3. Suporta pesquisa de registros de chamadas definindo condições, incluindo dispositivo, duração da chamada (hora de início e hora de término) e status da chamada.
4. Suporta visualização de detalhes de qualquer registro de chamadas e chamada para a estação interna novamente.

4.20.6 Gestão Centralizada do Módulo de Vídeo Porteiro

1. A plataforma suportará módulo de interfone de vídeo independente e entrada independente para o módulo.
2. A plataforma dará suporte ao painel que inclui manutenção do dispositivo, estatísticas diárias de avisos aplicados e estatísticas de chamadas do dia atual.
3. A plataforma suportará parâmetros de configuração em lote para dispositivos de interfone de vídeo.
4. A plataforma oferecerá suporte à atualização de firmware de estações de porta em lote.

4.21 Monitoramento de bordo

- ***Implantação em vários cenários***
- ***Monitoramento de direção***
- ***Estatísticas e Relatório***
- ***Pesquisa e exportação de registros históricos***

- ***Evento e Alarme***
- ***Gestão de Evidências***
- ***Gerenciamento de Permissões***
- ***Manutenção do dispositivo***

4.21.1 Implantação em vários cenários

Gerenciamento de dispositivos

1. A plataforma oferecerá suporte à adição de dispositivos de bordo detectados on-line.
2. A plataforma oferecerá suporte ao acesso a dispositivos de bordo via ISUP quando os dispositivos estiverem conectados à Internet ou Wi-Fi.
3. A plataforma deve suportar a sincronização do fuso horário com o do dispositivo de bordo e a configuração manual do fuso horário do dispositivo de bordo.
4. A plataforma oferecerá suporte à obtenção e exibição de informações do dispositivo para gerenciamento do dispositivo, incluindo número de série do dispositivo, versão do firmware, canais do dispositivo de codificação para vinculação com câmeras, informações de entrada/saída de alarme e status do ACC.
5. A plataforma oferecerá suporte à obtenção e exibição de informações do dispositivo para gerenciamento do dispositivo, incluindo o número de série do dispositivo, a versão do firmware, os canais do dispositivo de codificação para vinculação com câmeras e informações de entrada/saída de alarme.
6. A plataforma oferecerá suporte ao acesso à página da Web do dispositivo para configuração remota, incluindo a configuração de parâmetros do dispositivo e dos canais vinculados.
7. A plataforma oferecerá suporte à atualização em lote de pacotes de firmware (via FTP e HTTP) e à definição de simultaneidade para gerenciamento de largura de banda de pacotes.

Solução de armazenamento

1. A plataforma oferecerá suporte à configuração de parâmetros de armazenamento, incluindo tipo de fluxo de vídeo (principal/secundário/duplo), programação de gravação baseada em tempo/evento e tempo de expiração do arquivo de vídeo.
2. A plataforma deve suportar armazenamento redundante 4G em tempo real. Quando um evento ocorre, a primeira cópia é armazenada no dispositivo de codificação onboard e a segunda cópia é armazenada no pStor/HybridSAN/armazenamento em nuvem para fins de segurança.
3. A plataforma suportará a cópia de vídeo de volta para o armazenamento central para backup via W-Fi ou 4G. Assim que um veículo chegar ao seu destino e o dispositivo de bordo se conectar com sucesso ao Wi-Fi ou 4G lá, o vídeo gravado durante a viagem será copiado de volta para o armazenamento central (pStor/HybridSAN/armazenamento em nuvem) para backup.
4. A plataforma suportará a configuração do armazenamento de imagens (armazenamento local/pStor/HybridSAN/armazenamento em nuvem).
5. A plataforma deve suportar a cópia de vídeos de volta do HybridSAN especificando o horário de início e término. A plataforma deve suportar a cópia de vídeos armazenados antes que o

dispositivo de bordo seja adicionado à plataforma. A cooperação entre a cópia de vídeo de volta e o armazenamento local do dispositivo de bordo pode atender melhor às necessidades dos usuários.

Streaming para multi-cliente em WAN

1. Com a mídia de streaming integrada, vários clientes na WAN poderão acessar e transmitir de um dispositivo adicionado via ISUP na LAN.
2. A plataforma deve suportar a adição de servidor SMS externo. A plataforma deve suportar streaming de dispositivos por meio de múltiplos canais via mídia de streaming externa com base na área especificada.
3. A plataforma deverá suportar o desligamento automático do streaming após a duração configurada.
4. A plataforma deve suportar a habilitação da criptografia de fluxo. Ao iniciar a visualização ao vivo ou a reprodução remota, o cliente verificará a chave de criptografia de fluxo para fins de segurança.

Gestão de Veículos

1. A plataforma dará suporte à criação de áreas para gerenciamento de veículos.
2. A plataforma deve suportar a adição do número da placa do veículo ao qual o dispositivo de bordo está relacionado. A plataforma deve suportar a adição do veículo a uma área existente ou a uma área recém-criada. A plataforma deve suportar a edição dos nomes de diferentes recursos, incluindo câmeras, entradas de alarme e saídas de alarme.
3. A plataforma oferecerá suporte ao gerenciamento de informações do veículo, incluindo número da placa, nome do proprietário do veículo, telefone, tipo de veículo, cor do veículo, marca do veículo, foto do veículo e dispositivos vinculados.

Configuração de regra de condução para vários cenários

1. A plataforma oferecerá suporte ao fornecimento de visão geral do monitoramento de bordo, assistente de configuração, informações básicas de manutenção (número total/online de dispositivos de bordo, número total/online de câmeras, exceção/número total de entradas de alarme), estatísticas e relatórios (distância de direção dos últimos 7 dias, duração da direção dos últimos 7 dias e eventos de direção dos últimos 7 dias) para que os usuários possam iniciar rapidamente a configuração do monitoramento de bordo e a manutenção do sistema.
2. A plataforma deve suportar a configuração de quilômetro ou milhagem como unidade de distância para exibir a velocidade e a distância.
3. A plataforma oferecerá suporte à definição da URL da API do Google Maps.
4. A plataforma suportará a configuração do período de retenção de dados de GPS (7/15/30/60/90/180 dias ou 1 ano). Período mais curto significa menor espaço de armazenamento de dados.
5. A plataforma deve suportar a configuração da frequência na qual as informações de GPS são reportadas à plataforma (5/10/15/30/60 segundos). Frequência mais alta significa mais consumo de largura de banda e maior precisão das informações de GPS.
6. A plataforma oferecerá suporte à definição de diversas regras de cerca, incluindo nome, descrição, modelo de cronograma de regras, lista de veículos, tipo de cerca (para detecção de

entrada/saída) e área da cerca no mapa do Google.
7. A plataforma oferecerá suporte à definição de várias regras de cerca, incluindo nome, descrição, modelo de programação de regras, lista de veículos, tipo de cerca (para detecção de entrada/saída), limite para acionamento de regra e área de cerca no mapa do Google.
8. A plataforma oferecerá suporte à definição de várias regras de desvio, incluindo nome, descrição, modelo de cronograma de regras, lista de veículos, limite de desvio e rota no mapa do Google.

4.21.2 Monitoramento de direção

Painel de monitoramento

A plataforma oferecerá suporte ao monitoramento de bordo por meio do painel de monitoramento para obter informações em tempo real, como lista de veículos, mapa do Google, vídeos ao vivo e eventos de direção.

Operação do veículo

1. A plataforma suportará a exibição da área à qual o veículo pertence, lista de veículos, canais relacionados. A plataforma suportará a busca de veículos e áreas.
2. A plataforma deve suportar a exibição do número total de veículos, número de veículos on-line e número de veículos localizados.
3. A plataforma deve suportar a exibição da lista de veículos on-line/localizados.
4. A plataforma suportará adicionar veículos à lista de Favoritos. A plataforma suportará visualizar todos os veículos na lista de Favoritos.
5. A plataforma deverá suportar a exibição do status de alarme dos dispositivos de bordo.
6. A plataforma oferecerá suporte à exibição dos detalhes do veículo: número da placa, motorista, número de telefone do motorista, tipo de veículo, cor do veículo, marca do veículo e foto do veículo.
7. A plataforma oferecerá suporte à seleção de vários veículos para localizá-los no mapa.
8. A plataforma suportará a colocação de um veículo localizado no centro do mapa.
9. A plataforma suportará áudio bidirecional com o motorista do veículo selecionado.
10. A plataforma oferecerá suporte à seleção de vários veículos para transmissão.
11. A plataforma oferecerá suporte à obtenção da localização em tempo real do veículo selecionado e à exibição de sua rota em tempo real no mapa.
    a. A plataforma deve suportar a reprodução da rota do veículo selecionado. A plataforma deve suportar a reprodução da rota no mapa e do vídeo gravado simultaneamente. A plataforma deve suportar a configuração da duração da reprodução (última 1 hora, últimas 6 horas, hoje, ontem, duração personalizada).
    b. A plataforma dará suporte à seleção das câmeras montadas no veículo.
    c. A plataforma suportará a configuração da velocidade de reprodução (1/8X, 1/4X, 1/2X, 1X, 2X, 4X, 8X).
    d. A plataforma suportará a colocação do veículo no centro do mapa.
    e. A plataforma deverá suportar a exibição do limite de velocidade de condução.
    f. A plataforma oferecerá suporte para pular o período sem vídeo gravado.

g. A plataforma deve suportar a interrupção/início da reprodução da rota.

12. A plataforma deve suportar o controle das saídas de alarme do veículo. A plataforma deve suportar a habilitação/desabilitação de saídas de alarme específicas.

Operação de Mapa

1. A plataforma suportará a exibição do mapa em tela cheia ou na tela auxiliar.
2. A plataforma oferecerá suporte à exibição da regra de cerca configurada e da regra de desvio no Google Maps.
   a. A plataforma suportará o desenho de uma área redonda no mapa. Os veículos na área serão exibidos e suportará a seleção de um veículo específico. A plataforma suportará a visualização de detalhes do veículo, incluindo informações de GPS e velocidade de direção.
   b. A plataforma suportará áudio bidirecional com o driver.
   c. A plataforma oferecerá suporte ao rastreamento de veículos em tempo real.
   d. A plataforma oferecerá suporte à reprodução das rotas percorridas pelos veículos.
   e. A plataforma suportará controle de saída de alarme.
3.
4. A plataforma deve suportar a especificação do ponto inicial e do ponto final no mapa para medir a distância real entre eles. A plataforma deve suportar a exibição de múltiplas linhas para medir distâncias no mapa.
5. A plataforma oferecerá suporte à exibição do status do alarme do veículo que foi localizado no mapa e visualizará os detalhes do alarme.

Monitoramento de câmera no veículo

1. A plataforma suportará a exibição do módulo de vídeo em modo de tela cheia ou na tela auxiliar.
2. A plataforma suportará visualização ao vivo ou reprodução de no máximo 16 câmeras montadas em veículos, predefinindo e personalizando a divisão de janelas.
3. A plataforma oferecerá suporte à visualização ao vivo ou à reprodução de câmeras individuais ou de todas as câmeras montadas no veículo.
4. A plataforma oferecerá suporte às seguintes funções para canal único: captura, áudio bidirecional, zoom digital, controle de áudio, comutação de fluxo principal/secundário, controle de saída de alarme, adição de tags, gravação manual (somente para visualização ao vivo), recorte de vídeo (somente para reprodução), expansão olho de peixe, aprimoramento de imagem, controle PTZ (somente para visualização ao vivo), alternância para reprodução instantânea, impressão, zoom nas áreas selecionadas e exportação de vídeos.
5. A plataforma oferecerá suporte ao controle PTZ para câmeras PTZ (somente para visualização ao vivo): controle de configuração de prioridade, tempo de bloqueio, limpador múltiplo/único, posicionamento 3D, predefinição (obtenção, configuração e chamada de predefinições de dispositivos), padrão, patrulha, foco, distância focal, íris, foco de um toque, luz, inicialização de lente, rastreamento manual, captura manual de imagem facial, configuração de prioridade do usuário e estacionamento.
6. A plataforma oferecerá suporte à exibição do status da câmera: incluindo taxa de quadros, informações de transmissão, padrão de vídeo, número de conexões, status da rede, status do sinal, status da gravação, modo de acesso, tipo de canal, nome do dispositivo, endereço, tipo

de protocolo, informações de armazenamento (armazenamento principal e armazenamento auxiliar) e área.

7. A plataforma oferecerá suporte à marcação de dias em que os vídeos são gravados no calendário, à reprodução de vídeos em dias e horários específicos e ao arrastar a linha do tempo para frente ou para trás para posicionar o segmento de vídeo desejado.
8. A plataforma oferecerá suporte à busca de arquivos de vídeo definindo condições, incluindo tipo de gravação (programação de gravação baseada em tempo, programação baseada em evento, gravação manual e gravação ANR), tipo de tag (tipo de evento, tag adicionada manualmente e outras tags) e local de armazenamento.
9. A plataforma suportará reprodução rápida de 1, 2, 4 e 8 vezes, reprodução lenta de 1/2, 1/4 e 1/8 vezes.
10. A plataforma suportará reprodução síncrona e reprodução assíncrona.
11. A plataforma suportará a reprodução de miniaturas: exibindo miniaturas ao passar o cursor sobre a linha do tempo e clicando na miniatura para reproduzir o vídeo correspondente.
12. A plataforma oferecerá suporte à reprodução e pausa de vídeos, além de avanço e retrocesso de quadro único.
13. A plataforma oferecerá suporte ao download em lote de vídeos gravados por câmeras montadas em veículos.

Monitoramento de eventos de condução

1. A plataforma oferecerá suporte à detecção de eventos de direção no módulo de monitoramento de bordo sem qualquer configuração.
2. A plataforma oferecerá suporte à seleção de eventos de direção que precisam de monitoramento: evento de monitoramento de direção, evento de monitoramento de status do motorista e evento ADAS.
3. A plataforma suportará eventos de monitoramento de direção: Cerca, Desvio, Excesso de velocidade, Colisão, Capotamento e Alarme de Emergência. Esses eventos também estão disponíveis para pesquisa e função de alarme de evento.
4. A plataforma deve suportar eventos de monitoramento de status do motorista: incluindo fumar, usar celular, dirigir com fadiga, mão não no volante, mãos não no volante, usar celular e mão não no volante, distração, cinto de segurança desafivelado, ausência, bocejar, usar óculos de sol com infravermelho interrompido e adulteração de vídeo. Esses eventos também estão disponíveis para pesquisa e função de alarme de evento.
5. A plataforma suportará eventos ADSA: Colisão Frontal, Alerta de Monitoramento de Faixa, Desvio de Faixa, Alerta de Colisão de Pedestres, Alerta de Limite de Velocidade, Não Ceder Passagem para Pedestres, Excesso de Velocidade em Faixa de Pedestres e Alerta de Ponto Cego. Esses eventos também estão disponíveis para pesquisa de eventos e função de alarme de eventos.
6. A plataforma oferecerá suporte à exibição de detalhes do monitoramento de eventos em tempo real: número da placa, área, motorista, número do evento (suporta agrupamento por dispositivo de bordo), hora, tipo de evento, informações de GPS (clique para visualizar a localização), direção de direção e status do alarme (disparado ou não).
7. A plataforma oferecerá suporte à exibição de detalhes e localização em tempo real dos veículos: incluindo número da placa, área, hora, informações de GPS , direção de direção e

velocidade.

8. A plataforma oferecerá suporte para acessar a página de busca de eventos de direção a partir da página de lista de eventos.
9. A plataforma deve suportar a visualização de informações ANPR, incluindo número da placa, área, hora (dispositivo), tipo de evento, informações de GPS e direção de direção. A plataforma deve suportar o salto para o módulo ANPR para visualizar as informações do veículo que passa.

4.21.3 Gerenciamento de motorista

Gestão de motoristas

1. Suporte ao gerenciamento da lista de motoristas, incluindo nome do motorista, ID, e-mail, número de telefone, observação, carteira de motorista (número e foto).
2. Suporte ao gerenciamento de grupos de motoristas. Suporta adicionar vários motoristas a um grupo.
3. Suporte para vincular um motorista/grupo de motoristas ao adicionar um veículo com a finalidade de obter estatísticas do motorista.

Estatísticas e Relatório

1. Suporte para visualização de estatísticas do motorista durante os últimos 7 dias / últimos 30 dias / um período personalizado.
2. Suporte para visualização de detalhes do motorista, incluindo nome, foto de perfil, distância percorrida, duração da viagem, eventos por 100 quilômetros, número de eventos, consumo total de combustível, taxa de partida pontual, taxa de chegada pontual, partidas/chegadas não pontuais e observação.
3. Suporte para definição de tipos de eventos para cálculo.
4. Suporte às principais estatísticas de distribuição de eventos durante os últimos 7 dias / últimos 30 dias / um período personalizado.
5. Suporte para visualizar a tendência de consumo de combustível por 100 quilômetros em uma base diária, semanal ou mensal, ou por um período personalizado.
6. Suporte para visualizar a tendência da distância percorrida diariamente, semanalmente ou mensalmente, ou por um período personalizado.
7. Suporte para visualizar a tendência da duração da condução em uma base diária, semanal ou mensal, ou por um período personalizado.
8. Suporte para visualizar a tendência de eventos de direção em uma base diária, semanal ou mensal, ou por um período personalizado.
9. Suporte para visualização da tendência de eventos por 100 quilômetros durante os últimos 7 dias / últimos 30 dias / um período personalizado.

4.21.4 Gerenciamento de Rotas

Monitoramento de direção

1. Suporte para adicionar paradas no mapa. Suporte para definir o nome e habilitar/desabilitar a contagem de pessoas para a parada.

2. Suporte para adicionar rotas de direção selecionando paradas, configurando a rota e definindo cronogramas de turnos.
3. Suporte à geração automática de uma rota entre várias paradas.
4. Suporte para definir um cronograma de turnos por semana. Suporte para definir dias da semana para repetição e o horário de início para entrar em vigor.
5. Suporte para definir um cronograma de turnos para uma data fixa.
6. Suporte para definir um cronograma de turnos para um período de tempo.
7. Suporte à definição de cronogramas de turnos em lote para uma rota.
8. Suporte para definir o horário de chegada/partida para cada parada e a diferença de tempo permitida (com precisão de minuto).
9. Suporte para definir as causas de partidas/chegadas fora de hora para diferentes rotas.
10. Suporte para configuração de regras de parada de eventos. Suporte para configuração de paradas que permitem/proíbem entradas de alarme de disparo.
11. Suporte para configuração de regras de eventos de rota. Suporte para configuração de paradas de permitir/proibir entradas de alarme de disparo.

Monitoramento de rota

1. Suporte para exibir o status de todas as rotas, incluindo rotas pontuais e não pontuais.
2. Suporte à filtragem de rotas de acordo com paradas e nomes de rotas.
3. Suporte para exibir as paradas de uma rota e o status de um veículo (chegada pontual, atrasada ou antecipada).
4. Suporte para visualizar os detalhes de uma rota clicando na rota, incluindo a pontualidade dos veículos em uma parada e a pontualidade de todos os veículos em cada parada.
5. Suporte para adicionar notas durante o monitoramento de rota selecionando causas predefinidas. As notas adicionadas serão incluídas no relatório.
6. Suporte ao clicar no ícone de um veículo específico para visualizar as informações de monitoramento de direção, incluindo localização em tempo real, rotas, alarmes acionados, informações do motorista e operações do veículo.

Parar relatório analítico

1. Suporte à geração de relatórios estatísticos de todas as paradas ou paradas selecionadas.
2. Suporte para visualizar informações de parada dos últimos 7 dias, dos últimos 30 dias ou de um período personalizado.
3. Suporte para mostrar a análise geral de cada parada, incluindo a taxa média de partidas pontuais, a taxa média de chegadas pontuais, o tempo médio de permanência (em minutos), o total de chegadas não pontuais e o total de partidas não pontuais.
4. Suporte mostrando as 10 melhores / 10 piores classificações de paradas para taxa de partida pontual, taxa de chegada pontual.
5. Suporte mostrando as 10 melhores / 10 piores classificações de paradas para taxa de chegada pontual.
6. Suporte para exibição das 10 melhores/10 piores classificações de paradas para tempo total de direção, duração real de direção e duração programada de direção.

Busca de rota

1. Suporte à busca de rotas percorridas de acordo com nomes de rotas, nomes de paradas, motorista/grupo de motoristas e informações do veículo.
2. Suporte para exibir tempo de rota, cronograma de turnos, veículo, motorista/grupo de motoristas, tempo de partida do veículo, duração da condução. Suporte para gerenciar cada registro de rota.
3. Suporte para exibir informações de rota de cada turno de trabalho, incluindo tempo de condução programado, tempo de condução real, hora de partida programada em uma parada, hora de partida real em uma parada, hora de chegada programada em uma parada e hora de chegada real em uma parada.
4. Suporte à exportação de registros de rotas percorridas.

4.21.5 Gestão do Consumo de Combustível

Configuração de monitoramento do nível de combustível

1. Suporte para configuração da unidade de consumo de combustível.
2. Suporte à configuração de tanques de combustível, incluindo nomes, capacidade do tanque, nível de combustível e limite de consumo de combustível.
3. Suporte para ter uma visão geral dos níveis de combustível de acordo com os parâmetros dos tipos de tanques de diferentes veículos.
4. Suporte para configuração de um limite de diferença de nível de combustível. Quando a diferença exceder o valor configurado, um alarme será disparado.

Pesquisa de registros de nível de combustível

1. Suporte à busca de registros de nível de combustível de acordo com o horário, veículo, motorista/grupo de motoristas.
2. Suporte para exibição do consumo de combustível por 100 quilômetros de um motorista selecionado e do consumo de combustível de cada motorista.
3. Suporte para exibir os registros de consumo de combustível relatados por cada motorista, incluindo motorista, consumo de combustível, distância percorrida e consumo de combustível por 100 km.
4. Suporte para exibir a tendência de consumo de combustível de um veículo especificado.
5. Suporte para exibir a localização do relatório de consumo de combustível em tempo real no mapa.
6. Suporte para exibição de veículo, motorista, consumo de combustível, capacidade total do tanque e informações de GPS vinculadas a uma determinada unidade de consumo de combustível.
7. Suporte à exportação de relatórios.

4.21.6 Estatísticas e Relatório

Vários tipos de relatórios

1. Suporte à visão geral das estatísticas de monitoramento a bordo e relatórios, incluindo os seis tipos de relatórios: informações de GPS, distância de direção, duração da direção, tempos de excesso de velocidade, eventos de direção e taxa on-line do dispositivo.
2. Suporte para geração de relatórios sobre informações relacionadas ao GPS de veículos específicos em um período específico.
3. Suporte para exibir simultaneamente ou separadamente os tempos de relatório de GPS de todos os veículos ou veículos selecionados.
4. Suporte para visualização de detalhes do GPS.
5. Suporte para geração de relatório sobre a taxa on-line dos dispositivos de bordo montados nos veículos selecionados em um período específico.
6. Suporte para exibir simultaneamente ou separadamente a tarifa on-line de todos os veículos ou veículos selecionados em um período específico.
7. Suporte para visualizar os detalhes da tarifa on-line.
8. Suporte para gerar o relatório sobre a distância percorrida por veículos específicos em um período específico.
9. Suporte para exibir simultaneamente ou separadamente a distância percorrida por todos os veículos ou veículos selecionados em um período específico.
10. Suporte para visualizar detalhes da distância percorrida.
11. Suporte para gerar relatórios sobre a duração do excesso de velocidade de veículos específicos em uma velocidade específica (0, 20 km/h, 40 km/h, 60 km/h, 80 km/h) em um período específico.
12. Suporte para exibir simultaneamente ou separadamente a distância percorrida por todos os veículos ou veículos selecionados em um período específico.
13. Suporte para visualizar detalhes da distância percorrida.
14. Suporte para gerar relatórios sobre a duração da condução de veículos específicos a uma determinada velocidade (0km/h, 20km/h, 40km/h, 60km/h, 80km/h) em um período específico.
15. Suporte para exibir simultaneamente ou separadamente a duração da condução de todos os veículos ou veículos selecionados em um período específico.
16. Suporte para visualizar os detalhes da duração da condução.
17. Suporte para geração de relatórios sobre eventos de condução de veículos específicos em um período específico.
18. Suporte para exibir simultaneamente ou separadamente o número de eventos de condução de veículos específicos em um período específico.
19. Suporte para visualização de detalhes do evento de direção.
20. Suporte para geração de relatório sobre contagem de passageiros de veículos específicos em um período específico.
21. Suporte para exibir simultaneamente ou separadamente o número de passageiros que embarcaram e/ou desembarcaram de veículos específicos em um período específico.
22. Suporta três tipos de modo de visualização: entrar, sair e entrar/sair.

23. Suporte ao cálculo do tráfego de passageiros de diferentes paradas ou períodos de tempo: exibindo os dados de contagem de pessoas em um período especificado de diferentes veículos ou todos os veículos ao mesmo tempo ou separadamente, incluindo passageiros chegando, saindo ou ambos.
24. Suporte ao cálculo do tráfego de passageiros de diferentes rotas ou períodos de tempo: exibindo a contagem de pessoas em um período especificado de diferentes veículos ou todos os veículos ao mesmo tempo ou separadamente, incluindo passageiros chegando, saindo ou ambos.
25. Suporte aos seguintes tipos de relatórios para os relatórios acima: relatório diário, relatório semanal, relatório mensal, intervalo de tempo personalizado.
26. Suporte para exportação do relatório.

Relatório agendado

1. Suporte para configuração do envio regular de relatórios semanais ou mensais.
2. Suporte ao envio regular de relatórios, incluindo análise do motorista, análise do nível de combustível e relatório de análise do tráfego de passageiros no local.
3. Suporte para seleção de listas de drivers a serem analisados.
4. Suporte para definir um horário de envio regular.
5. Suporte para definir o modelo de e-mail.
6. Suporte para definir um formato de relatório: Excel ou CSV.
7. Suporte para produção de relatórios em vários idiomas.
8. Suporte ao upload regular de relatórios para o SFTP.
9. Suporte ao upload de relatórios para servidores locais regularmente.

4.21.7 Pesquisa e exportação de registros históricos

1. Suporte à busca de rotas de veículos pelas seguintes condições: hora, veículo, faixa de velocidade e tipo de evento.
2. Suporte para gravação de detalhes da rota do veículo: hora, velocidade máxima, velocidade mínima, evento acionado.
3. Suporte à pesquisa de eventos de direção pelas seguintes condições: hora, veículo, tipo de evento e área especificada no mapa.
4. Suporte para gravação de detalhes do evento de direção: número da placa, área, hora, tipo de evento, informações de GPS e direção de direção.
5. Suporte para pesquisa e exportação de rotas percorridas por veículos históricos ou rotas de eventos de condução.
6. Suporte à exportação do arquivo de registro de rota (no formato Excel ou CSV) e do arquivo de vídeo (no formato MP4 ou AVI).

4.21.8 Evento e Alarme

1. A plataforma oferecerá suporte ao recebimento de eventos de direção: evento de monitoramento de bordo, comportamento do motorista e evento ADAS.
2. A plataforma oferecerá suporte ao recebimento de eventos acionados pela manutenção do

dispositivo de bordo: Dispositivo de bordo on-line, Dispositivo de bordo off-line, Perda de vídeo, HDD cheio, Erro de leitura e gravação do HDD, Incompatibilidade de padrão de vídeo e Exceção de armazenamento de vídeo.

3. A plataforma suportará o recebimento de eventos disparados pela entrada de alarme do dispositivo de bordo.
4. A plataforma deve suportar o recebimento de eventos acionados pela câmera montada no veículo (o tipo de evento suportado está sujeito à câmera montada no veículo).
5. A plataforma oferecerá suporte a todas as funções do módulo Evento e Alarme: configuração de ações de vinculação para eventos e alarmes detectados, monitoramento de alarmes, pesquisa de informações históricas de alarmes, análise de operação de alarmes e eventos, etc.
6. A plataforma suportará a exportação em lote dos arquivos de registro de rota (no formato Excel ou CSV) e do arquivo de vídeo (no formato MP4 ou AVI).

4.21.9 Gestão de Evidências

Suporte ao gerenciamento de evidências. Consulte ***Gerenciamento de evidências*** .

4.21.10 Gerenciamento de Permissões

1. Consulte Gerenciamento de evidências para obter detalhes
2. Suporte para configuração da permissão do módulo do veículo: configurações básicas e configuração de regras.
3. Suporte na configuração da permissão: monitoramento de bordo, busca de veículos, estatísticas e relatórios de veículos.
4. Suporte para configuração da permissão do evento e busca de alarme de entrada de alarme.
5. Suporte para configuração da permissão de saída de alarme.
6. Suporte à visão geral do status de saúde de acordo com os recursos: entrada de alarme, saída de alarme, dispositivo de bordo e câmera.
7. Suporte para configuração das seguintes permissões para câmeras: visualização ao vivo, captura de tela e impressão, pesquisa de vídeo, exportação de vídeo, gravação manual de vídeo, áudio bidirecional e reprodução de áudio.
8. Suporte para configuração da permissão de reprodução da câmera.
9. Suporte para reprodução de gravação de vídeo em um período de tempo recente (minuto/hora/dia).
10. Suporte para configuração da permissão PTZ da câmera: configuração e operação de PTZ.

4.21.11 Manutenção do dispositivo

1. A plataforma oferecerá suporte à visualização do status em tempo real de todos os dispositivos: MVR (gravador de vídeo móvel)/DVR (gravador de vídeo digital), câmera montada no veículo e entrada de alarme.
2. A plataforma suportará estatísticas históricas de taxas on-line do dispositivo de bordo.
3. A plataforma oferecerá suporte a estatísticas de taxas on-line de câmeras montadas em

veículos.

4. A plataforma suportará estatísticas de taxa de integridade de gravação de câmeras montadas em veículos.
5. A plataforma oferecerá suporte à exibição da lista de verificação de integridade do dispositivo na página de visão geral: visualização e exportação de detalhes da verificação de integridade do dispositivo de um veículo específico por data, filtragem da lista de verificação de integridade por veículo, etc.
6. A plataforma oferecerá suporte à obtenção remota de registros de dispositivos de bordo.

4.22 Aplicação Portátil

Configuração básica

- A plataforma suportará a configuração da unidade de distância para Quilômetro (km) ou Milha (mi).
- A plataforma oferecerá suporte à definição do período de retenção de dados de GPS, incluindo 7 dias, 15 dias, 30 dias, 60 dias, 180 dias e um ano.

Gerenciamento de dispositivos

- A plataforma suportará a adição de estações de acoplamento.
- A plataforma suportará a adição de dispositivos portáteis.
- A plataforma oferecerá suporte à aplicação de parâmetros globais a dispositivos portáteis: frequência de relatórios de GPS.
- A plataforma suportará a aplicação de parâmetros globais a dispositivos portáteis: endereço da plataforma de registro.
- A plataforma oferecerá suporte à aplicação de parâmetros globais a dispositivos portáteis: ID do dispositivo e senha.
- A plataforma oferecerá suporte à aplicação de parâmetros globais a dispositivos portáteis: informações de Wi-Fi.
- A plataforma deve suportar a aplicação de parâmetros globais a dispositivos portáteis: se deve permitir gravação forçada. Quando a gravação forçada está habilitada, o usuário não tem permissão para desligar a gravação.
- A plataforma oferecerá suporte à aplicação de parâmetros de gravação em dispositivos: resolução de vídeo e duração da pré e pós gravação.
- A plataforma suportará edição em lote de senhas de vários dispositivos portáteis.
- A plataforma oferecerá suporte à detecção automática de dispositivos portáteis em estações de acoplamento.

Gestão de Pessoas

- A plataforma oferecerá suporte à visualização da visão geral do aplicativo de pessoas, que exibe os números de pessoas válidas, inválidas e não configuradas.
- A plataforma oferecerá suporte à vinculação de pessoas a um dispositivo portátil exclusivo.
- A plataforma oferecerá suporte à importação de pessoas do domínio AD.
- A plataforma oferecerá suporte à aplicação de informações pessoais (que devem corresponder

às informações da conta da câmera corporal) na estação de acoplamento.
- A plataforma oferecerá suporte ao gerenciamento de cartões e à aplicação de informações de cartões às estações de acoplamento.
- A plataforma deve suportar o gerenciamento de impressões digitais. A plataforma deve suportar a aplicação de informações de impressão digital em estações de encaixe.
- A plataforma oferecerá suporte ao gerenciamento de perfis e à aplicação de perfis em estações de acoplamento.
- A plataforma deve suportar filtragem de acordo com o status de aplicação. A plataforma deve suportar a exibição de usuários que não foram aplicados e a reaplicação deles.

Monitoramento em tempo real

- A plataforma oferecerá suporte a operações relacionadas ao monitoramento na página, o que inclui lista de pessoas, mapa do Google, janela de visualização ao vivo e eventos relacionados à estação de acoplamento.
- A plataforma suportará a desativação do mapa GIS para a página Monitoramento em Tempo Real.
- A plataforma deve suportar a exibição dos números de todas as pessoas e pessoas localizadas. A plataforma deve suportar a troca para a lista de pessoas on-line/localizadas.
- A plataforma oferecerá suporte à busca de pessoas.
- A plataforma oferecerá suporte para localizar uma pessoa no mapa ou desenhar uma área no mapa para localizar pessoas.
- A plataforma oferecerá suporte à reprodução do trajeto da pessoa no mapa.
- A plataforma deve suportar áudio bidirecional com a pessoa.
- A plataforma oferecerá suporte à seleção em lote de pessoas e à transmissão para elas.
- A plataforma deve suportar a localização de câmeras corporais no Google Maps. A plataforma deve suportar a localização de câmeras corporais em uma área específica.
- A plataforma oferecerá suporte para visualização ao vivo, reprodução e áudio bidirecional para câmeras corporais.
- A plataforma oferecerá suporte ao recebimento de alarmes de pânico de dispositivos portáteis.

Gerenciamento de arquivos

- A plataforma oferecerá suporte ao armazenamento de gravações acionadas por alarmes em dispositivos portáteis.
- A plataforma oferecerá suporte à transmissão de dispositivos portáteis e ao armazenamento de gravações no armazenamento central.
- A plataforma oferecerá suporte ao backup de todos os arquivos (incluindo fotos, áudios e vídeos) nos dispositivos portáteis para o sistema central.
- A plataforma oferecerá suporte ao backup de arquivos marcados (incluindo fotos, áudios e vídeos) nos dispositivos portáteis para o sistema central.

Pesquisa de arquivo

- A plataforma oferecerá suporte à busca de arquivos por hora, grupo de estações de acoplamento e formato de arquivo (vídeo, imagem e áudio).
- A plataforma oferecerá suporte à busca de arquivos em dispositivos portáteis por tipo de

arquivo (importante ou sem importância).
- A plataforma oferecerá suporte à busca de arquivos por dispositivos portáteis.
- A plataforma oferecerá suporte à busca de arquivos em dispositivos portáteis por pessoas.
- A plataforma oferecerá suporte à exportação de arquivos pesquisados e ao salvamento de vídeos como evidência.
- A plataforma oferecerá suporte à busca de vídeos para reprodução de trilhas GPS.
- A plataforma oferecerá suporte à configuração de canais visíveis de acordo com as áreas para usuários na situação de múltiplos gerentes.

Pesquisa de trilha

A plataforma oferecerá suporte à busca de faixas por meio da seleção de pessoas.

Intercomunicador de grupo

A plataforma oferecerá suporte à adição da função de intercomunicação de grupo: criação de grupo, configuração do servidor de streaming e aplicação ao dispositivo.

Pesquisa de Registros

- A plataforma oferecerá suporte à busca de registros detalhados de recebimento de dispositivos portáteis por dispositivo, com condições de busca, incluindo hora de recebimento e status de retorno.
- A plataforma oferecerá suporte à busca de registros detalhados de recebimento de dispositivos portáteis por hora de recebimento, status de retorno e dispositivo.
- A plataforma oferecerá suporte à exibição de detalhes de cada registro, incluindo pessoa, departamento, nome do dispositivo, estatísticas do registro, hora de recebimento, hora de retorno, duração do uso, total de arquivos gerados, duração do vídeo, detalhes do recebimento, informações do arquivo e bateria ao receber/devolver.

Segurança de rede

- A plataforma suportará a adição do modo HTTPS para acesso IP.
- A plataforma oferecerá suporte à criptografia AES256 para imagens de dispositivos portáteis.
- A plataforma oferecerá suporte à criptografia de fluxo de vídeo diretamente por meio de streaming de dispositivos portáteis.

4.23 Relatório de Análise Inteligente

Cenário de troca
Solução de problemas

Cenário de Varejo/Supermercado

- ***Gestão de Loja***
- ***Painel para cenário de varejo/supermercado***
- ***Relatório de loja única***
- ***Relatório de várias lojas***
- ***Relatório de comparação de duas lojas***

- ***Relatório do Dia da Promoção***
- ***Centro de Análise***

Cenário Público

- ***Painel***
- ***Relatório agendado***
- ***Contagem de Pessoas***
- ***Análise de características pessoais***
- ***Análise de calor***
- ***Análise de Caminho***
- ***Análise de fila***
- ***Análise de temperatura***

4.23.1 Cenário de troca

Cenário de troca

1. A plataforma oferecerá suporte a cenários públicos e de varejo/supermercado.
2. A plataforma oferecerá suporte à visualização de relatórios coletados de um grupo de análise ou câmera no cenário público.
3. A plataforma oferecerá suporte à visualização de relatórios de uma única loja ou de várias lojas.

4.23.2 Gestão de Loja

Gestão de Loja

1. A plataforma oferecerá suporte à adição de lojas, incluindo a definição do nome da loja, a seleção de uma área para a loja, a definição do horário comercial, a definição da localização da loja e a configuração do(s) andar(es) da loja.
2. A plataforma suportará configurações de vários andares, incluindo a configuração da localização do andar e a adição de recursos a cada andar.
3. A plataforma oferecerá suporte à configuração de horários de funcionamento das lojas.
4. A plataforma suportará a configuração de vários dias de promoção.

Teste de Capacidade de Recursos

1. A plataforma deve suportar teste de habilidade de recursos de contagem de pessoas. A plataforma deve suportar exibição se deve habilitar o algoritmo, se deve habilitar o recurso, se deve habilitar dados de upload, estatísticas de pessoas na última hora e configuração remota.
2. A plataforma deve suportar teste de capacidade de recursos de análise de calor. A plataforma deve suportar exibição se deve habilitar o algoritmo, se deve habilitar o recurso, se deve habilitar o upload de dados, estatísticas de pessoas na última hora e configuração remota.
3. A plataforma deve suportar teste de capacidade de câmera. A plataforma deve suportar exibição se deve habilitar o algoritmo, se deve habilitar o recurso, se deve habilitar o upload de dados e operação remota.

4. A plataforma suportará testes de outras habilidades de câmera. A plataforma suportará relatórios de exportação de características de pessoas, análise de calor, análise de caminho e análise de fila.
5. A plataforma suportará testes de capacidade de contagem de pessoas por câmera e exportação de relatórios por hora.

Contagem de pessoas na loja

1. A plataforma oferecerá suporte à adição de recursos de contagem de pessoas à loja e configurará a contagem de pessoas (passagem), contagem de pessoas (entrada) e tráfego de pedestres (entrada+passagem).
2. A plataforma oferecerá suporte à vinculação de entradas e saídas com câmeras.
3. A plataforma suportará a adição de entradas e saídas para configuração de contagem de pessoas.
4. A plataforma oferecerá suporte à configuração do Limite de Capacidade da Loja para ser notificado quando o número de pessoas na loja exceder o limite.
5. A plataforma deve oferecer suporte à configuração de Limpar tudo regularmente para que todos os dados sejam limpos no horário definido.
6. A plataforma oferecerá suporte à configuração de quem será excluído na contagem de pessoas (para funcionários).
7. A plataforma suportará a configuração da localização de entradas e saídas no mapa.
8. A plataforma oferecerá suporte à adição da mesma câmera em diversas entradas e saídas de uma loja.

Análise do caminho da loja

A plataforma oferecerá suporte à adição de uma câmera a um mapa estático e definirá seus caminhos e direções no mapa.

Análise de calor da loja

A plataforma oferecerá suporte à configuração de uma câmera com regras de mapa de calor para uma área necessária.

4.23.3 Painel para cenário de varejo/supermercado

Em geral

1. A plataforma oferecerá suporte à exibição de estatísticas de diversas lojas no painel.
2. A plataforma oferecerá suporte à exibição de informações do painel por Dia/Semana/Mês/Ano/Dia da Promoção/Personalizado.

Conteúdo do relatório

A plataforma oferecerá suporte à exibição de conteúdos como contagem de pessoas, taxa de entrada e tempo médio de espera.

Classificações

1. A plataforma oferecerá suporte à exibição das lojas com contagem de 5 pessoas no

topo/fundo.
2. A plataforma oferecerá suporte à exibição das lojas com as 5 maiores/menores taxas de entrada.
3. A plataforma oferecerá suporte à exibição das lojas com os 5 melhores/piores tempos médios de espera.
4. A plataforma deverá suportar a exibição das áreas de calor com contagem de 5 pessoas no topo/fundo.

Tendência de contagem de pessoas

A plataforma oferecerá suporte à exibição de tendências e à comparação ciclo a ciclo da contagem de pessoas, tráfego de pedestres e taxa de entrada.

Distribuição geral

1. A plataforma oferecerá suporte à exibição da análise de características da pessoa em um gráfico de pizza.
2. A plataforma oferecerá suporte à exibição da localização GPS de todas as lojas.

4.23.4 Relatório de loja única

Em geral

1. A plataforma oferecerá suporte aos seguintes tipos de relatórios: Relatório diário, Relatório semanal, Relatório mensal, Relatório anual e Intervalo de tempo personalizado.
2. A plataforma oferecerá suporte à personalização dos conteúdos exibidos no relatório.
3. A plataforma oferecerá suporte à exportação de relatórios de loja única com conteúdo de relatório personalizado.
4. A plataforma oferecerá suporte à exportação de relatórios conforme programado.

Conteúdo do relatório

1. A plataforma oferecerá suporte à exibição do número atual, do número de pico, da data do número de pico e das estatísticas de ciclo a ciclo do tráfego de pedestres (entrada+passagem), contagem de pessoas (entrada) e taxa de entrada.
2. A plataforma oferecerá suporte à exibição da quantidade de pessoas que permanecem por hora no relatório diário.
3. A plataforma oferecerá suporte à exibição do valor atual, estatísticas de ciclo a ciclo e o número de vezes que os alarmes de fila acionam o tempo médio de espera.
4. A plataforma oferecerá suporte à exibição de classificações de tráfego de pedestres (entrada+passagem), contagem de pessoas (entrada) e taxa de entrada entre todas as lojas.
5. A plataforma deverá suportar a exibição do número de vezes de excesso de capacidade das lojas.
6. A plataforma oferecerá suporte à exibição da área com maior taxa de permanência.

Características da pessoa

A plataforma oferecerá suporte à exibição da análise de características da pessoa em um gráfico de pizza.

Contagem de Pessoas

1. A plataforma deve suportar a exibição da tendência de contagem de pessoas por contagem de pessoas (entrada), tráfego de pedestres (entrada+passagem) e taxa de entrada. A plataforma também deve suportar a exibição do número de entradas e saídas.
2. A plataforma oferecerá suporte à exibição do número de pessoas em cada entrada e saída e a localização de entrada e saída em cada andar.
3. A plataforma oferecerá suporte à exibição das classificações de todas as estatísticas de entrada e saída e contagem de pessoas em um período de tempo específico.
4. A plataforma deverá suportar a exibição das direções de fluxo de cada entrada/saída.

Análise de calor

1. A plataforma suportará a troca de áreas de calor e a troca do modo de representação de cores do mapa de calor.
2. A plataforma suportará a exibição do mapa de calor por andar.
3. A plataforma oferecerá suporte à exibição do total de pessoas, total de pessoas residentes, taxa de permanência e duração média de permanência de um andar específico em uma área aquecida.
4. A plataforma oferecerá suporte à exibição das classificações de todas as áreas de aquecimento.
5. A plataforma deve oferecer suporte à especificação de quanto tempo será considerado como permanência para taxa de permanência: >15s, >30s, >60s, >300s.

Análise de Caminho

A plataforma oferecerá suporte à exibição de todos os caminhos por andar e informações de contagem de pessoas para cada caminho.

Análise de fila

1. A plataforma oferecerá suporte à exibição de estatísticas de tempos de alarme, incluindo tempos de espera extras e tempos de excesso de capacidade na fila.
2. A plataforma oferecerá suporte à exibição do número atual e estatísticas de ciclo a ciclo de tempos de alarme.
3. A plataforma deve suportar a exibição da porcentagem de distribuição do intervalo estatístico definido de tempo de espera. A plataforma deve suportar a exibição do diagrama de tendência correspondente.
4. A plataforma deve suportar a exibição da porcentagem de distribuição do número definido de pessoas na fila. A plataforma deve suportar a exibição do diagrama de tendência correspondente.
5. A plataforma oferecerá suporte à definição do intervalo estatístico de tempo de espera e número de pessoas na fila.

4.23.5 Relatório de várias lojas

Em geral

1. A plataforma oferecerá suporte aos seguintes tipos de relatórios: Relatório diário, Relatório semanal, Relatório mensal, Relatório anual e Intervalo de tempo personalizado.
2. A plataforma oferecerá suporte à seleção de várias lojas e exportará um relatório de várias lojas.
3. A plataforma oferecerá suporte à personalização dos conteúdos exibidos no relatório.
4. A plataforma oferecerá suporte à exportação de relatórios de várias lojas com conteúdo de relatório personalizado.
5. A plataforma oferecerá suporte à exportação de relatórios conforme programado.

Conteúdo do relatório

1. A plataforma oferecerá suporte à exibição do número atual, do número de pico, da data do número de pico e das estatísticas de ciclo a ciclo do tráfego de pedestres (entrada+passagem), contagem de pessoas (entrada) e taxa de entrada.
2. A plataforma oferecerá suporte à exibição do valor atual, estatísticas de ciclo a ciclo e o número de vezes que os alarmes de fila acionam o tempo médio de espera.
3. A plataforma oferecerá suporte à exibição da área com maior taxa de permanência.
4. A plataforma deve suportar a exibição das lojas com contagem de pessoas superior/inferior 1 (entrada).
5. A plataforma oferecerá suporte à exibição da loja com o primeiro aumento na contagem de pessoas (entrada).
6. A plataforma deve suportar a exibição da loja com a redução do número de pessoas no topo 1 (entrada).
7. A plataforma deve suportar a exibição da loja com tráfego de 1 pé na parte superior/inferior (entrada+passagem).
8. A plataforma oferecerá suporte à exibição da loja com maior aumento no tráfego de pedestres (entrada+passagem).
9. A plataforma deve oferecer suporte à exibição da loja com a primeira redução no tráfego de pedestres (entrada+passagem).
10. A plataforma deve suportar a exibição da loja com taxa de entrada superior/inferior 1.
11. A plataforma oferecerá suporte à exibição da loja com o maior aumento na taxa de entrada.
12. A plataforma oferecerá suporte à exibição da loja com redução na taxa de entrada no top 1.
13. A plataforma suportará a exibição da loja com taxa de permanência superior/inferior 1.
14. A plataforma oferecerá suporte à exibição da loja com maior aumento na taxa de permanência.
15. A plataforma oferecerá suporte à exibição da loja com a primeira redução na taxa de permanência.

Classificações e tendências de contagem de pessoas

1. A plataforma oferecerá suporte à classificação de todas as lojas selecionadas por contagem de pessoas.
2. A plataforma oferecerá suporte à classificação de lojas por contagem de pessoas (entrada),

tráfego de pedestres (entrada+passagem), taxa de entrada e tempo médio de espera.
3. A plataforma oferecerá suporte à classificação de lojas por esses itens e à exibição de estatísticas de ciclo em ciclo.
4. A plataforma oferecerá suporte à exibição da tendência de contagem de pessoas por contagem de pessoas (entrada), tráfego de pedestres (entrada+passagem) e taxa de entrada.
5. A plataforma oferecerá suporte à exibição da tendência de contagem de pessoas por contagem de pessoas (saída) somente para relatórios diários.

Classificações de área de calor

1. A plataforma oferecerá suporte à classificação de áreas de calor para todas as lojas selecionadas.
2. A plataforma oferecerá suporte à classificação de áreas de calor por total de pessoas residentes, total de pessoas, taxa de permanência e duração média de permanência.

4.23.6 Relatório de comparação de duas lojas

Em geral

1. A plataforma oferecerá suporte aos seguintes tipos de relatórios: Relatório diário, Relatório semanal, Relatório mensal, Relatório anual e Intervalo de tempo personalizado.
2. A plataforma suportará a exportação de um relatório de comparação de duas lojas selecionadas.
3. A plataforma oferecerá suporte à exportação de relatórios conforme programado.

Classificações de contagem de pessoas

A plataforma oferecerá suporte à classificação de lojas por contagem de pessoas (entrada), tráfego de pedestres (entrada+passagem), taxa de entrada e tempo médio de espera.

4.23.7 Relatório do Dia da Promoção

Dia da promoção

A plataforma oferecerá suporte à seleção de um dia de promoção para gerar um relatório das lojas selecionadas naquele dia.

Conteúdo do relatório

A plataforma oferecerá suporte à exibição do número atual, do número de pico, da data do número de pico e das estatísticas de ciclo a ciclo do tráfego de pedestres (entrada+passagem), contagem de pessoas (entrada) e taxa de entrada.

Classificações de contagem de pessoas

1. A plataforma oferecerá suporte à classificação de lojas por contagem de pessoas (entrada), tráfego de pedestres (entrada+passagem), taxa de entrada e tempo médio de espera.
2. A plataforma oferecerá suporte à classificação de lojas por esses itens e à exibição de estatísticas de ciclo em ciclo.

Tendências de contagem de pessoas

1. A plataforma oferecerá suporte à exibição da tendência de contagem de pessoas por contagem de pessoas (entrada), tráfego de pedestres (entrada+passagem) e taxa de entrada.
2. A plataforma oferecerá suporte à exibição da tendência diária antes e depois do dia da promoção, ou da tendência horária no dia da promoção.

Exportação de Relatório

A plataforma oferecerá suporte à exportação do relatório do dia de promoção da loja.

4.23.8 Centro de Análise

Relatório Alvo

1. A plataforma deve oferecer suporte à seleção de loja/entrada e saída/câmera como destino do relatório para contagem de pessoas.
2. A plataforma deve suportar a seleção de loja/câmera como o alvo do relatório para análise de características pessoais. O conteúdo do relatório deve ser o mesmo com um único relatório de loja.
3. A plataforma oferecerá suporte à seleção de loja/câmera como alvo do relatório para análise de calor.
4. A plataforma oferecerá suporte à seleção da loja como alvo do relatório para análise de caminho.
5. A plataforma deve suportar a seleção de loja/câmera como o alvo do relatório para análise de fila. O conteúdo do relatório deve ser o mesmo com um único relatório de loja se você selecionar câmera como o alvo do relatório; o conteúdo do relatório inclui apenas horários de alarme se você selecionar loja como o alvo do relatório.

4.23.9 Painel

Configuração do painel

1. A plataforma oferecerá suporte à personalização dos relatórios a serem exibidos no painel, incluindo contagem de pessoas, análise de densidade de pessoas, análise de calor, análise de fila, análise de caminho, análise de características da pessoa, temperatura da superfície da pele, análise de temperatura e análise de veículos.
2. A plataforma suportará a configuração do tipo de análise: via grupo de recursos ou via canal.

Painel de instrumentos

1. A plataforma deve suportar a troca do tempo de visualização. A plataforma deve suportar a edição do tipo de relatório e tempo.
2. A plataforma oferecerá suporte à atualização manual do conteúdo do relatório.
3. A plataforma oferecerá suporte à exportação do conteúdo do relatório no painel.

Exportação de dados

1. A plataforma oferecerá suporte à exportação de relatórios no Painel.

2. A plataforma oferecerá suporte à seleção do nome do relatório para exportá-lo.
3. A plataforma suportará a exportação do relatório nos formatos de arquivo Excel, CSV e PDF.

4.23.10 Relatório agendado

1. A plataforma oferecerá suporte à configuração do relatório agendado diário, semanal ou mensal.
2. A plataforma suportará a configuração do horário de envio do relatório agendado.
3. A plataforma oferecerá suporte à configuração do modelo de e-mail para relatório agendado.
4. A plataforma oferecerá suporte à seleção do idioma do relatório.
5. A plataforma suportará o upload de relatórios de eventos e alarmes agendados para o servidor SFTP.
6. A plataforma suportará o upload de backup de relatórios de eventos e alarmes agendados para armazenamento local.

4.23.11 Tipo de alvo múltiplo

Exibição e exportação de relatórios

1. A plataforma oferecerá suporte à geração de relatórios de análise de múltiplos alvos, exibindo informações incluindo o número de pessoas, veículos motorizados e veículos não motorizados dentro de um período especificado.
2. A plataforma deve suportar a visualização dos seguintes tipos de relatórios: Relatório Diário, Relatório Semanal, Relatório Mensal, Relatório Anual e Intervalo de Tempo Personalizado. Visualize estatísticas de relatórios por hora, dia e mês.
3. A plataforma suportará a exportação de relatórios em formato PDF, EXCEL ou CSV.

4.23.12 Contagem de Pessoas

Grupo de contagem de pessoas

1. A plataforma oferecerá suporte à seleção de diversas câmeras e leitores de cartão das portas selecionadas como recurso estatístico.
2. A plataforma oferecerá suporte à configuração da direção de entrada e saída de recursos no grupo de contagem de pessoas.
3. A plataforma oferecerá suporte à definição de um horário para limpeza regular de todos os dados de contagem de pessoas.
4. A plataforma deverá suportar a habilitação da capacidade máxima e a configuração do número máximo de pessoas autorizadas a entrar.

Evento e Alarme

A plataforma deve oferecer suporte à configuração de alarme de quantidade de pessoas acima do limite e pré-alarme de quantidade de pessoas acima do limite para o grupo de contagem de pessoas selecionado.

Monitoramento em tempo real

1. A plataforma deve suportar monitoramento em tempo real do(s) grupo(s) de contagem de pessoas selecionado(s). A plataforma deve suportar visualização da visualização ao vivo de vários grupos de contagem de pessoas simultaneamente.
2. A plataforma oferecerá suporte à visualização do número de pessoas restantes no grupo de contagem de pessoas e do número de pessoas autorizadas a entrar.
3. A plataforma oferecerá suporte à correção manual dos dados dos grupos de contagem de pessoas.
4. A plataforma oferecerá suporte à configuração de exibição bilíngue para grupos de contagem de pessoas.

Exibição e exportação de relatórios

1. A plataforma oferecerá suporte à exibição dos resultados da análise por câmera(s) ou por grupo(s) de contagem de pessoas.
2. A plataforma oferecerá suporte à classificação de grupos de recursos e câmeras de acordo com o número de pessoas que entraram e o número de pessoas que saíram.
3. A plataforma oferecerá suporte à definição da direção como Entrada, Saída ou Entrada e Saída para análise estatística.
4. A plataforma oferecerá suporte à exibição do número de pessoas que entraram, pessoas que passaram e taxa de entrada.
5. A plataforma oferecerá suporte aos seguintes tipos de relatórios: Relatório diário, Relatório semanal, Relatório mensal, Relatório anual e Intervalo de tempo personalizado.
6. A plataforma oferecerá suporte à exibição de estatísticas comparativas com o dia anterior, a semana anterior, o mês anterior, o ano anterior e o horário personalizado.
7. A plataforma oferecerá suporte à exibição do pico do total de pessoas por diferentes dimensões.
8. A plataforma suportará a exportação do relatório.

4.23.13 Análise de características pessoais

Grupo de Análise de Características Pessoais

1. A plataforma oferecerá suporte à adição e ao gerenciamento de grupos de análise de características pessoais.
2. A plataforma oferecerá suporte à exibição dos resultados da análise por câmera(s) ou por grupo(s) de análise de características pessoais.

Exibição e exportação de relatórios

1. A plataforma oferecerá suporte aos seguintes tipos de relatórios: Relatório diário, Relatório semanal, Relatório mensal, Relatório anual e Intervalo de tempo personalizado.
2. A plataforma oferecerá suporte à seleção do conteúdo estatístico por tempo.
3. A plataforma suportará a exibição dos resultados da análise em gráfico de pizza.
4. A plataforma suportará a exportação do relatório.

4.23.14 Análise de calor

Grupo de Análise de Calor

1. A plataforma oferecerá suporte à seleção de diversas câmeras e leitores de cartão das portas selecionadas como recurso de contagem de pessoas.
2. A plataforma oferecerá suporte à definição da direção como Entrada ou Saída de recursos no grupo.
3. A plataforma oferecerá suporte à seleção de diversas câmeras como recurso estatístico para análise de calor.

Exibição e exportação de relatórios

1. A plataforma oferecerá suporte à exibição do resultado da análise por câmeras ou por grupos de contagem de pessoas.
2. A plataforma oferecerá suporte à classificação entre grupos de recursos e câmeras de acordo com a contagem de pessoas, tempo médio de permanência, número de pessoas que permanecem e taxa de permanência.
3. A plataforma oferecerá suporte a três tipos de estatísticas: tempo de permanência, quantidade de pessoas e tempo médio de permanência.
4. A plataforma suportará a definição de quanto tempo será considerado como permanência para taxa de permanência: >0s,>15s,>30s,>60s.
5. A plataforma suportará a exibição de mapa de calor global. A plataforma suportará a vinculação de múltiplas câmeras com um mapa.
6. A plataforma deve suportar a exibição de cores diferentes para regiões de calor diferente no mapa. A plataforma deve suportar a visualização do mapa de calor de uma câmera. A imagem da câmera é codificada por cores.
7. A plataforma oferecerá suporte à exibição de estatísticas comparadas com ontem, a semana anterior, o mês anterior, o ano anterior, o dia da promoção anterior e o horário personalizado.
8. A plataforma oferecerá suporte à exibição do momento de pico da contagem de pessoas, tempo de permanência e taxa de permanência.
9. A plataforma oferecerá suporte aos seguintes tipos de relatórios: Relatório diário, Relatório semanal, Relatório mensal, Relatório anual e Intervalo de tempo personalizado.
10. A plataforma suportará a exportação do relatório.

4.23.15 Análise de Caminho

Grupo de Análise de Caminhos

A plataforma oferecerá suporte à adição de diversas câmeras ao mapa e à definição de suas localizações no mapa.

Exibição e exportação de relatórios

1. A plataforma oferecerá suporte aos seguintes tipos de relatórios: Relatório diário, Relatório semanal, Relatório mensal, Relatório anual e Intervalo de tempo personalizado.
2. A plataforma oferecerá suporte à seleção do conteúdo estatístico por tempo.

3. A plataforma oferecerá suporte à exibição dos resultados da análise no mapa, incluindo a cor do calor de cada caminho e o número de pessoas em cada caminho.
4. A plataforma suportará a exportação do relatório.

4.23.16 Análise de fila

1. A plataforma suportará os seguintes tipos de relatórios: Relatório Diário, Relatório Semanal e Relatório Anual.
2. A plataforma oferecerá suporte à seleção do conteúdo estatístico por tempo.
3. A plataforma oferecerá suporte a dois tipos de análise, incluindo duração de espera e tamanho da fila.
4. A plataforma deverá suportar a exibição do número de exceções (tempo limite de espera).
5. A plataforma deverá suportar a exibição do tempo de espera para filas com diferentes números de pessoas (comprimento da fila).
6. A plataforma deverá suportar a exibição do número de exceções (quantidade de pessoas excedendo).
7. A plataforma oferecerá suporte à exibição de estatísticas de contagem de pessoas com diferentes durações de espera.
8. A plataforma suportará a exportação do relatório.

4.23.17 Análise de densidade de pessoas

Exibição e exportação de relatórios

1. A plataforma oferecerá suporte aos seguintes tipos de relatórios: Relatório diário, Relatório semanal, Relatório mensal, Relatório anual e Intervalo de tempo personalizado.
2. A plataforma suportará a exibição da análise em gráfico de linhas.
3. A plataforma suportará a exportação do relatório de análise.

4.23.18 Análise de temperatura

1. A plataforma oferecerá suporte aos seguintes tipos de relatórios: Relatório diário, Relatório semanal, Relatório mensal, Relatório anual e Intervalo de tempo personalizado.
2. A plataforma deve suportar a seleção de Hora para o relatório diário. A plataforma deve suportar a exibição da temperatura mais alta e mais baixa do ponto de triagem de temperatura específico em um minuto.
3. A plataforma suportará a exibição do número de exceções de temperatura das predefinições.
4. A plataforma oferecerá suporte à comparação da temperatura mais alta entre vários pontos de triagem de temperatura.
5. A plataforma oferecerá suporte à comparação da temperatura mais baixa entre vários pontos de triagem de temperatura.
6. A plataforma suportará a exportação do relatório.

4.23.19 Solução de problemas

Solução de problemas

1. A plataforma deve suportar teste de capacidade de câmera. A plataforma deve suportar exibição se deve habilitar o algoritmo, se deve habilitar o recurso, se deve habilitar o upload de dados e operação remota.
2. A plataforma suportará testes de outras habilidades de câmera. A plataforma suportará relatórios de exportação de características de pessoas, análise de calor, análise de caminho, análise de fila e análise de temperatura.
3. A plataforma suportará testes de capacidade de contagem de pessoas por câmera e exportação de relatórios por hora.

4.24 Tempo e Presença

- ***Assistente de Atendimento***
- ***Regras de Presença***
- ***Gestão de licenças***
- ***Relatórios de Presença***
- ***Operação do Sistema de Atendimento***
- ***Autoatendimento para funcionários***
- ***Check-In&Check-Out via Cliente Móvel***
- ***Integração de terceiros***

4.24.1 Assistente de Atendimento

Forneça orientação para ajudar o usuário a configurar um sistema de presença.

4.24.2 Regras de Presença

Grupo de Atendimento

1. A plataforma oferecerá suporte para adicionar, excluir e editar grupos de presença.
2. A plataforma oferecerá suporte para adicionar pessoas aos grupos de atendimento.

Regra de Presença

1. A plataforma oferecerá suporte à configuração de regras de presença globais e departamentais.
2. A plataforma oferecerá suporte à configuração de regras de presença em grupo.
3. A plataforma oferecerá suporte à definição do horário de mudança do dia.
4. A plataforma oferecerá suporte à adição de códigos de pagamento.
5. A plataforma suportará a edição de códigos fixos.

Horário de Intervalo

1. A plataforma oferecerá suporte à adição de horários de intervalos.
2. A plataforma deve oferecer suporte à definição de uma duração fixa de intervalo ou ao cálculo da duração do intervalo pelo intervalo real de check-in/out.
3. A plataforma deverá suportar a marcação de retorno antecipado como hora extra (nível 1/2/3).
4. A plataforma deve oferecer suporte à marcação de retorno tardio como duração normal, tardia, antecipada ou de ausência.
5. A plataforma suportará o cálculo da duração das pausas pelo intervalo do primeiro e último check-in/out ou pelo intervalo de cada check-in/out.
6. A plataforma oferecerá suporte à ativação do status de presença em dispositivos de verificação de presença.
7. A plataforma oferecerá suporte à contagem de tempo de retorno antecipado ou tardio por ponto de tempo.
8. A plataforma oferecerá suporte à contagem do tempo de retorno antecipado ou tardio por duração.

Horário

1. A plataforma oferecerá suporte à adição de horários de trabalho.
2. A plataforma oferecerá suporte à adição de horários normais e definirá o modo flexível para Permitir chegada tardia/saída antecipada ou Período flexível.
3. A plataforma oferecerá suporte à adição de horários flexíveis.
4. O cronograma deve permitir a definição de um período válido de check-in e de um período válido de check-out superior a 24 horas.
5. A plataforma oferecerá suporte à definição do período válido de check-in/out abrangendo 4 dias consecutivos.
6. A plataforma oferecerá suporte à adição de vários horários de intervalo em um único horário.
7. A plataforma oferecerá suporte à visão geral do cronograma.
8. A plataforma deve suportar a definição de uma regra de ausência dedicada para um horário, cuja prioridade é maior do que a regra de ausência global. A plataforma deve suportar a marcação de check-in tardio e check-out antecipado como ausente. A plataforma deve suportar a marcação de nenhum check-in ou check-out como ausente ou atrasado.
9. A plataforma suportará o cálculo das horas de trabalho pelo intervalo do primeiro e último check-in/out ou pelo intervalo de cada check-in/out.
10. A plataforma oferecerá suporte à ativação do status de presença em dispositivos de verificação de presença.
11. A plataforma oferecerá suporte à configuração do último horário de check-in.
12. A plataforma oferecerá suporte à visualização das alterações da linha do tempo ao configurar o horário.
13. A plataforma oferecerá suporte à configuração de horários seguindo as abas, incluindo Configurações Básicas, Período de Intervalo, Horas Extras e Cálculo de Presença.
14. A plataforma deverá suportar a configuração da duração do intervalo, excedendo a qual o intervalo será excluído do horário de trabalho.

Mudança

1. A plataforma suportará a adição de turnos.
2. A plataforma oferecerá suporte à definição do padrão de repetição do turno: Por semana (1 a 52 semanas), Por dia (1 a 31 dias) e Por mês (1 a 12 meses).
3. A plataforma deve suportar a definição do ciclo de repetição para semana ou dia.
4. A plataforma simplificará o gerenciamento de turnos, excluindo o modo de cálculo e a regra de horas extras.
5. A plataforma selecionará tanto o horário normal quanto o horário flexível para um turno.
6. A plataforma suportará o cálculo das horas de trabalho pelo intervalo do primeiro e último check-in/out ou pelo intervalo de cada check-in/out.
7. A plataforma oferecerá suporte à ativação do status de presença em dispositivos de verificação de presença.
8. A plataforma deve suportar a definição de uma regra de hora extra dedicada para um turno, cuja prioridade é maior do que a regra de hora extra global. A plataforma deve suportar a definição da taxa de hora de trabalho de cada nível de hora extra, regra de cálculo de hora extra em dias úteis, regra de hora extra em feriados e se deve calcular a hora extra que não está em período de verificação de presença válido.
9. A plataforma suportará a configuração de feriados para um turno. A verificação de presença será desabilitada em feriados.
10. A plataforma oferecerá suporte à exibição de vários turnos de uma pessoa no módulo Visão geral da programação.
11. A plataforma oferecerá suporte à configuração de diferentes períodos efetivos para diferentes cronogramas ao atribuir cronogramas por pessoa ou departamento.

Agendar

1. A plataforma oferecerá suporte à visão geral do cronograma.
2. A plataforma oferecerá suporte à visualização geral da programação por mês e semana.
3. A plataforma oferecerá suporte à atribuição de um cronograma aos departamentos.
4. A plataforma oferecerá suporte à atribuição de uma agenda às pessoas.
5. A plataforma oferecerá suporte à atribuição de um cronograma temporário para pessoas em diferentes departamentos.
6. A plataforma oferecerá suporte à atribuição de um cronograma aos grupos de atendimento.
7. A plataforma oferecerá suporte à definição do período efetivo, à exigência de check-in/check-out e à efetivação de horas extras ao atribuir um cronograma.
8. A plataforma oferecerá suporte à adição de vários turnos a uma programação.
9. A plataforma oferecerá suporte à vinculação de um cronograma aos pontos de verificação de presença.
10. A plataforma oferecerá suporte à configuração rápida de cronogramas temporários no calendário.
11. A plataforma dará suporte à seleção de horários para os horários temporários.
12. A plataforma oferecerá suporte à configuração rápida de agendas e ao uso de cores diferentes para marcar diferentes agendas no calendário.

Regra global de horas extras

1. A plataforma oferecerá suporte à definição da taxa de hora de trabalho para 3 níveis de horas extras.
2. A plataforma deve suportar a configuração da regra de horas extras em dias úteis. A plataforma deve suportar a configuração do modo de cálculo de horas extras para ""Por Hora Total de Trabalho"" ou ""Por Pontos de Tempo""
   - Por Hora Total de Trabalho - Conte as horas extras de trabalho como hora extra. A plataforma deve suportar a configuração do modo de cálculo da duração da hora extra para ""Fixed"" ou ""Actual"".
   - Por Pontos de Tempo - Contabilize check-in antecipado ou check-out tardio como hora extra. A plataforma deve suportar a configuração do modo de cálculo de duração."
3. A plataforma oferecerá suporte à definição da regra de horas extras nos fins de semana, definindo um limite diário para cálculo válido de horas extras.
4. A plataforma deve suportar a definição da regra de horas extras em feriados. A plataforma deve suportar a definição de um limite diário para cálculo válido de horas extras, o limite máximo para horas extras e o nível de horas extras para cada feriado.
5. A plataforma deve oferecer suporte à definição de se deve ou não calcular as horas extras que não estão em período de verificação de presença válido.
6. A plataforma deve suportar dois dígitos após o ponto decimal ao definir a taxa de hora de trabalho.

Regra de Ausência Global

1. A plataforma oferecerá suporte à marcação do check-in tardio como ausente e à definição do limite.
2. A plataforma oferecerá suporte à marcação do check-out antecipado como ausente e à definição do limite.
3. A plataforma deve permitir que nenhum check-in seja marcado como ausente ou atrasado.
4. A plataforma não permitirá que nenhum check-out seja marcado como ausente ou atrasado.

Precisão do resultado de frequência

1. A plataforma oferecerá suporte à definição da unidade mínima, arredondamento e formato de exibição da duração de cada status de presença.
2. A plataforma suportará o cálculo de frequência por segundo.

Ponto de Verificação de Presença

1. A plataforma oferecerá suporte à verificação de presença por meio de todos os dispositivos na plataforma por padrão.
2. A plataforma deve suportar a configuração de qualquer ponto de acesso como o ponto de verificação de presença. A plataforma deve suportar a configuração do tipo de ponto de verificação de presença como Check-In & Out, Check-In Only ou Check-Out Only.
3. A plataforma deve suportar a configuração de qualquer leitor de cartão de uma porta como o ponto de verificação de atendimento. A plataforma deve suportar a configuração do tipo de ponto de verificação de atendimento para Check-In & Out, Check-In Only ou Check-Out Only.

Personalização

1. A plataforma oferecerá suporte à definição de qualquer dia da semana como fim de semana.
2. A plataforma suportará a configuração do modo de autenticação de presença para cartão, impressão digital e/ou rosto.
3. A plataforma oferecerá suporte à personalização dos tipos de licença.
4. A plataforma oferecerá suporte à configuração do modo de presença em dispositivos de verificação de presença como Manual, Automático e Manual e Automático.
5. A plataforma oferecerá suporte à personalização do nome do status de presença exibido nos dispositivos de verificação de presença, incluindo nome de check-in/check-out, nome de início/término do intervalo e nome de início/término da hora extra.
6. A plataforma oferecerá suporte à definição dos períodos de tempo de cada status de presença nos dispositivos de verificação de presença quando o modo de presença for Automático e Manual e Automático.

4.24.3 Gestão de licenças

1. A plataforma oferecerá suporte à configuração de diferentes tipos de licenças.
2. A plataforma oferecerá suporte à configuração de regras de licença.
3. A plataforma oferecerá suporte à atribuição de diferentes regras de licença às pessoas.
4. A plataforma oferecerá suporte à dedução automática dos dias restantes de licença de acordo com os pedidos de licença dos funcionários.

4.24.4 Relatórios de Presença

Relatórios de presença predefinidos

1. Suporta 4 tipos de relatórios de presença (Relatório Diário, Relatório Semanal, Relatório Mensal e Relatório Resumido) e 37 tipos de relatórios sob esses 4 tipos no total.
2. Para registro de presença, a plataforma oferecerá suporte a transações, cartão de ponto, registro de entrada e saída, relatório de primeiro e último acesso, registro de licença, registro de horas extras e relatório de correção de entrada e saída.
3. Para o Relatório Diário, a plataforma oferecerá suporte ao Cartão de Ponto Total, Horas Trabalhadas, Relatório de Horas Extras, Relatório de Licença, Relatório de Atraso, Relatório de Licença Antecipada, Relatório de Ausência, Relatório de Exceção e Vários Intervalos.
4. Para o Relatório Semanal, a plataforma suportará Detalhes Semanais, Horas Trabalhadas Semanais e Horas Extras Semanais.
5. Para o Relatório Mensal, a plataforma oferecerá suporte a Detalhes Mensais, Status Mensal, Horas Trabalhadas Mensais, Horas Extras Mensais, Tempo de Intervalo Mensal, Check-in e Check-out Mensais, Ausência Mensal, Atraso Mensal e Licença Antecipada Mensal.
6. Para o Relatório Resumido, a plataforma oferecerá suporte ao Resumo de Presença de Pessoas, Resumo de Horas Extras de Pessoas, Resumo de Licenças de Pessoas, Resumo de Presença de Departamento, Resumo de Horas Extras de Departamento, Visão Geral de Presença de Pessoas, Detalhes de Presença de Pessoas e Estatísticas de Presença de Pessoas.
7. Suporte para pré-visualização de todos os tipos de relatórios.

8. Suporte para adoção automática do tamanho e direção mais adaptáveis do papel para impressão de relatórios.
9. Suporte para personalizar o tamanho e a direção do papel para impressão de relatórios.

Personalização do modelo de relatório

1. Suporte à personalização de novos modelos de relatórios a partir de relatórios predefinidos.
2. Suporte à personalização de campos, ordem e ordem de classificação dos relatórios personalizados.
3. Suporte para selecionar todos os campos disponíveis ao personalizar relatórios.
4. Suporte à fusão de dados da mesma pessoa/departamento/data. Suporte à configuração da regra de classificação para registros, como classificação em ordem crescente de ID da pessoa.
5. Suporte para pré-visualização de relatórios personalizados.
6. Suporte para personalizar até 512 relatórios com base em relatórios de presença predefinidos e nos Arquivos Opcionais disponíveis no módulo Relatório Personalizado.

Exportação de Relatório

1. Suporte para gerar relatórios de presença de pessoas específicas (incluindo demitidos e empregados) ou departamentos.
2. A plataforma oferecerá suporte ao envio de relatórios de presença de grupos de presença específicos de acordo com um cronograma.
3. Suporte para exportação em formato PDF, Excel e CSV.
4. Se você selecionar PDF como o formato do relatório, suporte a impressão do relatório de acordo com o tamanho de papel selecionado e a direção de impressão. Se você selecionar Autoadaptação ao Papel Baseado no Conteúdo, suporte a especificação automática de um tamanho de papel de acordo com o tipo de relatório selecionado, e o tamanho de papel especificado será exibido entre colchetes atrás de Autoadaptação ao Papel Baseado no Conteúdo.
5. Suporte à exportação de relatórios de presença por diferentes dimensões de cálculo (por pessoa, departamento, data ou padrão) e à exportação nos formatos PDF, Excel e CSV.
6. Suporte à criptografia dos arquivos de relatórios exportados.

Personalização da exibição do relatório

1. Suporte para adicionar o logotipo da empresa aos relatórios.
2. Suporte para definir o formato de data e hora.
3. Suporte para definir a abreviação e a cor de cada status de presença.

4.24.5 Operação do Sistema de Atendimento

Painel

1. A plataforma deve suportar a verificação das estatísticas de frequência anormal (ausência, atraso, saída antecipada, saída tardia e antecipada) do dia atual, dia anterior, semana atual, semana passada, mês atual e mês passado, últimos 3 meses, últimos 6 meses, ano atual e período de tempo personalizado. A plataforma deve suportar a exportação do gráfico de estatísticas como um arquivo PDF, PNG ou JPG.

2. A plataforma deve suportar a verificação das estatísticas de status de frequência (normal e ausente) do dia atual, dia anterior, semana atual, semana passada, mês atual e mês passado, últimos 3 meses, últimos 6 meses, ano atual e período de tempo personalizado. A plataforma deve suportar a exportação do gráfico estatístico como um arquivo PDF, PNG ou JPG.
3. A plataforma deve suportar a verificação das estatísticas gerais de horas de trabalho/horas extras do dia atual, dia anterior, semana atual, semana passada, mês atual e mês passado, últimos 3 meses, últimos 6 meses, ano atual e período de tempo personalizado. A plataforma deve suportar a exportação do gráfico estatístico como um arquivo PDF, PNG ou JP G.

Cálculo Automático de Presença

1. A plataforma suportará o cálculo dos resultados de frequência do dia anterior às 4:00 AM. A plataforma suportará a alteração do horário de cálculo automático.
2. A plataforma oferecerá suporte à definição do tempo de recálculo dos dados históricos de frequência.

Cálculo de Presença Manual

A plataforma oferecerá suporte ao cálculo manual dos resultados de frequência de qualquer pessoa específica durante um período de tempo específico.

Gestão de transações

1. A plataforma oferecerá suporte à pesquisa e listagem de todas as transações.
2. A plataforma suportará a exportação de transações em formato PDF, Excel ou CSV.
3. A plataforma oferecerá suporte à personalização dos itens de dados, à ordem dos itens e à ordem de classificação dos registros ao exportar registros.

Resultados do cálculo de frequência

1. A plataforma oferecerá suporte à listagem de todos os resultados do cálculo de frequência.
2. A plataforma oferecerá suporte à classificação dos resultados do cálculo de frequência de acordo com o ID da pessoa ou data.
3. A plataforma oferecerá suporte para ocultar ou mostrar itens de dados específicos de registros de presença.
4. A plataforma oferecerá suporte à exportação de registros de presença em formato PDF, Excel ou CSV.
5. A plataforma oferecerá suporte à personalização dos itens de dados, à ordem dos itens e à ordem de classificação dos registros ao exportar registros.
6. A plataforma oferecerá suporte à pesquisa de registros de frequência por hora, incluindo hoje, semana atual, mês atual, este ano, ontem, últimos 7 dias, semana passada, mês anterior, últimos 3 meses, últimos 6 meses, ano passado ou personalizado.

Integridade do registro de presença

1. A plataforma oferecerá suporte à obtenção automática de registros de entrada e saída perdidos dos dispositivos.
2. A plataforma oferecerá suporte à importação manual de todos os registros de entrada e saída em um intervalo de tempo específico de dispositivos.

3. A plataforma oferecerá suporte à importação manual dos registros de entrada e saída exportados do dispositivo (arquivos) do PC local.

Tratamento de Exceções de Atendimento

- A plataforma oferecerá suporte ao envio de solicitações para que os funcionários lidem com o comparecimento excepcional (licenças, horas extras e correção de check-in/check-out).
- A plataforma oferecerá suporte à revisão de solicitações de comparecimento excepcionais de acordo com os fluxos de solicitação configurados.

Envio automático de relatórios de presença por e-mail

1. A plataforma oferecerá suporte à definição de cronogramas de relatórios para enviar relatórios predefinidos ou personalizados por e-mail.
2. A plataforma oferecerá suporte à personalização de modelos de e-mail.
3. A plataforma oferecerá suporte à seleção do idioma do relatório.
4. A plataforma oferecerá suporte à configuração do ciclo de estatísticas: Por dia (selecione um ou vários dias de segunda a domingo), Por semana (selecione um dia de segunda a domingo) ou Por mês (selecione qualquer dia do primeiro ao último dia do mês).
5. A plataforma oferecerá suporte ao envio automático do relatório de presença aos destinatários.
6. A plataforma suportará a geração de relatórios nos seguintes formatos: PDF, Excel, CSV e TXT.
7. Quando o formato do relatório for PDF, a plataforma oferecerá suporte à personalização do tamanho do papel e da direção da impressão.

4.24.6 Autoatendimento para Funcionários

Autoatendimento para funcionários

- A plataforma dará suporte ao administrador na definição da senha de autoatendimento do funcionário, que é o ID do funcionário por padrão.
- A plataforma oferecerá suporte aos funcionários no login na plataforma por meio do Web Client e do Mobile Client.
- A plataforma oferecerá suporte a painéis de autoatendimento para funcionários.
- A plataforma oferecerá suporte à busca de resultados de frequência pessoal, status e relatórios.
- A plataforma dará suporte ao envio de solicitações de frequência de exceção (ausências, horas extras, correção de check-in/check-out).
- A plataforma oferecerá suporte à busca de um aplicativo e à visualização do status do fluxo de aprovação.
- A plataforma oferecerá suporte à autodesfazimento do aplicativo enviado.
- A plataforma oferecerá suporte para revisão (aprovação ou rejeição) ou desfazimento do pedido de comparecimento de exceção (esta função é válida somente para revisores).
- A plataforma dará suporte aos funcionários na alteração de senhas de login.
- A plataforma dará suporte aos funcionários para alterar perguntas de segurança.
- A plataforma dará suporte aos funcionários que enviarem solicitações de licença.
- A plataforma dará suporte aos funcionários na busca por dias restantes de licença.

Gestão do fluxo de aprovação

- A plataforma oferecerá suporte à personalização de funções de aprovação.
- A plataforma oferecerá suporte à personalização de fluxos de aprovação.

4.24.7 Check-in e Check-out via Cliente Móvel

1. A plataforma dará suporte ao RH configurando escopo de check-in/out válido no mapa GIS. Suporte à seleção de um local e à configuração do raio máx.
2. A plataforma oferecerá suporte ao RH para habilitar e desabilitar a opção Tirar Foto.
3. A plataforma oferecerá suporte ao RH para habilitar ou desabilitar o check-in e check-out via Mobile Client para uma única pessoa ou várias pessoas.
4. A plataforma oferecerá suporte à atribuição de diferentes áreas de check-in/out por pessoas, departamentos e grupos de atendimento.
5. A plataforma dará suporte ao RH adicionando um fluxo de aprovação para grupos de presença.
6. A plataforma dará suporte ao RH para visualizar todos os aplicativos a serem revisados para check-in e check-out via Mobile Client.
7. A plataforma oferecerá suporte aos funcionários para fazer check-in e check-out via Mobile Client.
8. A plataforma oferecerá suporte aos funcionários para visualizar todos os registros de check-in e check-out do dia atual por meio do Mobile Client.
9. A plataforma dará suporte aos administradores para aprovar ou rejeitar as solicitações de check-in e check-out dos funcionários por meio do Mobile Client.
10. Quando um fluxo de aprovação de check-in e check-out via Mobile Client termina, a plataforma suportará o cálculo automático dos resultados de frequência.

4.24.8 Integração de Terceiros

Integração via Arquivos Intermediários

1. A plataforma suportará a exportação de registros de entrada e saída para o PC local como arquivos CSV ou TXT.
2. A plataforma oferecerá suporte à exportação de registros de entrada e saída para o serviço SFTP como arquivos CSV ou TXT.
3. A plataforma suportará a personalização dos campos e do formato dos dados a serem incluídos no arquivo exportado.
4. A plataforma suportará a personalização do nome do arquivo.
5. A plataforma suportará a adição de informações de data e hora no nome do arquivo.
6. A plataforma oferecerá suporte à definição da frequência e do horário de exportação dos arquivos.
7. A plataforma oferecerá suporte à definição do comprimento e ao método complementar de identificação da pessoa.
8. A plataforma oferecerá suporte à definição do comprimento e ao método complementar do número do cartão.
9. A plataforma oferecerá suporte à configuração de substituição dos arquivos exportados.

Integração via Banco de Dados

1. A plataforma oferecerá suporte à gravação de registros de entrada e saída em bancos de dados de terceiros, como PostgreSQL, MS SQL Server, MySQL e Oracle em tempo real.
2. A plataforma deverá suportar a definição do mapeamento entre os campos de dados da plataforma e aqueles do banco de dados de terceiros.
3. A plataforma deve suportar a configuração da direção como Entrada ou Saída.
4. A plataforma suportará a definição do formato de gravação de dados.
5. A plataforma oferecerá suporte à exibição do status de sincronização do banco de dados de terceiros em tempo real.
6. A plataforma suportará a inserção do endereço IP do servidor ou nome de domínio na sincronização de banco de dados de terceiros.
7. A plataforma oferecerá suporte ao envio de dados de vários caracteres para o banco de dados de terceiros.
8. A plataforma oferecerá suporte ao envio de informações adicionais à pessoa caso você tenha configurado as informações adicionais.
9. A plataforma deve suportar a configuração do intervalo de tempo de envio de registros que falharam ao serem enviados.
10. A plataforma oferecerá suporte ao diagnóstico do motivo da falha na transmissão de dados, exibindo o motivo e os dados que não foram transmitidos.

4.25 Gestão de Patrulhas

4.25.1 Configuração Básica

Configuração de parâmetros básicos

1. A plataforma oferecerá suporte à configuração dos tipos de exceções para que os patrulheiros relatem via Mobile Client.
2. A plataforma oferecerá suporte à configuração do local de armazenamento para armazenar anexos enviados durante patrulhas.
3. A plataforma oferecerá suporte à configuração do horário de notificação antecipada para lembrar os patrulheiros antes do início das patrulhas.
4. A plataforma suportará a definição de um tempo entre 20 e 60 minutos.

Configuração do ponto de patrulha

1. A plataforma suportará a configuração de até 1.024 pontos de patrulha.
2. A plataforma oferecerá suporte à configuração dos seguintes tipos de dispositivos como pontos de patrulha: terminal de reconhecimento facial, terminal de controle de acesso e estação de porta.
3. A plataforma suportará a vinculação de até 4 câmeras a cada ponto de patrulha, que podem ser câmeras de rede gerais ou câmeras de dispositivos de controle de acesso.

Verificação de GPS para patrulha de código QR

1. A plataforma suportará a configuração de pontos de patrulha do tipo QR code.
2. A plataforma oferecerá suporte à configuração de escopos de patrulha válidos para pontos de patrulha do tipo código QR com base no mapa GIS.
3. A plataforma oferecerá suporte ao upload dos locais reais de patrulha (coordenadas GPS) para a plataforma quando os patrulheiros escanearem os códigos QR dos pontos de patrulha.
4. A plataforma oferecerá suporte ao envio de alarmes para o Alarm Center quando a localização real da patrulha e o escopo válido da patrulha não corresponderem.

Configuração do grupo de pessoas de patrulha

1. A plataforma suportará a configuração de até 300 grupos de patrulheiros.
2. A plataforma oferecerá suporte à formação de grupos de patrulheiros com uma ou mais pessoas.
3. A plataforma oferecerá suporte à definição do modo de patrulha de um grupo de pessoas de patrulha como "Qualquer pessoa no grupo" ou "Todas as pessoas no grupo".
   Qualquer pessoa do grupo - Qualquer pessoa do grupo poderá fazer check-in no ponto de patrulha para realizar a patrulha.
   Todas as pessoas do grupo - Todas as pessoas do grupo devem fazer o check-in no ponto de patrulha para realizar a patrulha.

Configuração do modelo de agendamento

1. A plataforma oferecerá suporte à configuração de modelos de programação e à definição dos parâmetros relacionados, incluindo o nome do modelo, o intervalo de tempo e o ciclo de repetição para programação de patrulhas.
2. A plataforma oferecerá suporte à configuração do ciclo de repetição para "Todos os dias", "Todas as semanas" (em dias selecionados da semana) ou "Todos os meses" (em datas selecionadas do mês).

4.25.2 Configuração de Patrulha

Configuração de rota de patrulha

A plataforma oferecerá suporte à configuração de rotas de patrulha com base em mapas eletrônicos.

Configuração da tarefa de patrulha

1. A plataforma oferecerá suporte à configuração de tarefas de patrulha definindo os seguintes parâmetros: nome da rota, pessoa ou grupo de pessoas da patrulha, modelo de programação, duração da patrulha, pontos de patrulha, padrão de patrulha (por exemplo, em ordem, sem ordem, primeiro ponto primeiro, último ponto último, primeiro ponto primeiro e último ponto último), programações de turnos, se a patrulha deve ser iniciada imediatamente e o horário para notificação antecipada.
2. A plataforma deve suportar a exibição de informações de rota de patrulha de forma visualizada (em calendários ou listas). A plataforma deve suportar a exibição do status de cada

rota de patrulha (por exemplo, não iniciada, em patrulha, não habilitada).

Lembrete de tarefa de patrulha

A plataforma oferecerá suporte para lembrar os patrulheiros antes do início das patrulhas, enviando notificações antecipadas ao Cliente Móvel.

4.25.3 Monitoramento de Patrulha em Tempo Real

Monitoramento em tempo real

1. A plataforma oferecerá suporte ao monitoramento do status da rota de patrulha em tempo real.
2. A plataforma oferecerá suporte ao monitoramento do status das escalas de turnos em tempo real.
3. A plataforma oferecerá suporte ao monitoramento do status dos pontos de patrulha em tempo real.
4. A plataforma oferecerá suporte à visualização de informações detalhadas do patrulhador real/planejado de um ponto de patrulha em tempo real.
5. A plataforma oferecerá suporte ao monitoramento do status da patrulha em tempo real por meio de listas ou mapas eletrônicos.
6. A plataforma oferecerá suporte à visualização ao vivo de câmeras vinculadas a um ponto de patrulha e permitirá a gravação de vídeo (com suporte no Web Client, Control Client e Mobile Client).
7. A plataforma oferecerá suporte para iniciar ou adiar manualmente um turno.

Painel

1. A plataforma oferecerá suporte à exibição dos turnos de patrulha programados para o dia atual com informações como rota da patrulha, horário de início da patrulha e patrulheiro/grupo de patrulheiros relacionados.
2. A plataforma deverá suportar a exibição de estatísticas do status das rotas de patrulha do dia atual, ou seja, as porcentagens de rotas de patrulha com status diferentes (por exemplo, patrulha normal, patrulha omitida, patrulha substituta, etc.).

4.25.4 Gerenciamento de Exceções

Relatório de Exceções

A plataforma oferecerá suporte à notificação de exceções ocorridas durante patrulhas por meio do Mobile Client; o conteúdo relatado inclui descrição da exceção, informações sobre o ponto de patrulha e fotos e vídeos relacionados.

Alarme relacionado a patrulha

1. A plataforma oferecerá suporte aos seguintes eventos de patrulha: patrulha normal, patrulha antecipada, patrulha tardia, patrulha complementada e patrulha omitida.
2. A plataforma oferecerá suporte ao disparo de ações de vinculação para exceções ocorridas

durante patrulhas, como disparo de alarmes, gravação de vídeos e envio automático de e-mails.
3. A plataforma deve oferecer suporte ao acionamento de janelas pop-up de alarmes, que contenham as seguintes informações: tipo de evento, descrição do evento, cronograma de turnos, ponto de patrulha, pessoa de patrulha planejada, período de patrulha programado, tempo real de patrulha e visualização ao vivo da(s) câmera(s) vinculada(s) (suporte para gravação de vídeo).
4. A plataforma oferecerá suporte à exibição de informações de alarme durante o monitoramento de patrulha em tempo real (via mapa ou lista).

4.25.5 Estatísticas de Patrulha e Pesquisa de Registro de Eventos

Estatísticas e Relatório de Patrulha

1. A plataforma deve suportar a verificação e exportação de estatísticas de status de patrulha de rotas de patrulha. A plataforma deve suportar a filtragem de estatísticas especificando um intervalo de tempo.
2. .A plataforma deve suportar a verificação e exportação de estatísticas de status de patrulha de pontos de patrulha. A plataforma deve suportar a filtragem de estatísticas especificando um intervalo de tempo.
3. A plataforma deve suportar a verificação e exportação de estatísticas de status de patrulha de pessoas de patrulha. A plataforma deve suportar a filtragem de estatísticas especificando um intervalo de tempo.

Pesquisa de eventos de patrulha

A plataforma oferecerá suporte à busca de eventos de patrulha e à exportação dos registros de eventos.

4.26 Exposição Comercial

4.26.1 Visão Geral

Controle Centralizado de Dispositivos

1. A plataforma oferecerá suporte à visualização do status do dispositivo e de dispositivos offline.
2. A plataforma suportará a visualização e a execução do comando de controle combinado.
3. A plataforma oferecerá suporte à visualização do uso do painel plano na semana atual.

Comunicado de Informação

1. A plataforma oferecerá suporte para visualizar e ocultar o assistente, que inclui os assistentes de operação para adicionar dispositivos, carregar materiais, criar programas, liberar cronogramas, controlar terminais, etc.
2. A plataforma oferecerá suporte para fornecer uma orientação para liberação rápida.
3. A plataforma oferecerá suporte para fornecer orientação para liberação de conteúdo por

modelo.
4. A plataforma oferecerá suporte à visualização do uso do pool de recursos e da biblioteca de materiais.

4.26.2 Controle de Dispositivo

1. A plataforma oferecerá suporte para iniciar/desligar/reiniciar, reproduzir/parar, cortar mensagem, parar mensagem cortada/parar mensagem, limpar conteúdo no terminal, habilitar/desabilitar inicialização/desligamento temporizado, etc.
2. A plataforma oferecerá suporte à criação de comandos de controle combinados e à sua aplicação a vários dispositivos.

4.26.3 Gerenciamento de Conteúdo

Liberação rápida

A plataforma suportará o upload de fotos ou vídeos do PC local e sua rápida aplicação nos dispositivos.

Biblioteca de modelos

A plataforma oferecerá suporte ao gerenciamento de modelos por tipo, incluindo layouts, modelos gerais, alimentos e bebidas, redes de varejo, bancos financeiros, edifícios comerciais, tráfego e transporte, mídia e saúde, cultura, esportes e modelos educacionais.

Meu modelo

A plataforma oferecerá suporte à adição dos modelos fornecidos ao Meu Modelo.

Liberação por modelo

A plataforma oferecerá suporte à seleção de modelos para criação de conteúdo e, em seguida, à definição de cronogramas para lançamento de conteúdo.

Lançamento personalizado

1. A plataforma oferecerá suporte à criação de programas personalizados.
2. A plataforma oferecerá suporte à adição de janela de previsão do tempo para liberação de conteúdo após a configuração do fabricante da Web de previsão do tempo.
3. A plataforma oferecerá suporte à adição de imagem, texto e imagem/texto dinâmico e, em seguida, definirá o grau de rotação, canto arredondado e microanimação.
4. A plataforma suportará o upload e a configuração de fontes personalizadas.
5. A plataforma suportará a adição de janelas RSS para liberação de informações assinadas.

Prévia do programa

A plataforma oferecerá suporte à pré-visualização de programas, ao início ou à pausa da reprodução e ao ajuste da velocidade de reprodução para 1x, 2x ou 4x.

Programa de Parede de Vídeo

A plataforma deve suportar a criação do programa de video wall. A plataforma deve suportar a configuração e o controle do video wall.

4.26.4 Gerenciamento de Cronograma

Cronograma Ordinário

1. A plataforma oferecerá suporte à criação de uma programação diária, programação semanal, programação em loop, programação padrão ou personalização de uma programação.
2. A plataforma suportará programas de loop por semana.

Cronograma de corte

A plataforma oferecerá suporte à adição de programas e textos cortados.

Sincronização de dispositivo tocando

A plataforma deve oferecer suporte à sincronização de dispositivos.

Registro de lançamento

1. A plataforma oferecerá suporte à exibição dos registros de lançamento na lista e à filtragem dos registros.
2. A plataforma deve suportar os seguintes status de release: Releasing, Released, Releasing Failed, Release Canceled e To Be Released. Exiba o nome do terminal, o progresso do release e o status do release.
3. A plataforma deve suportar o cancelamento da liberação para terminais que não foram liberados ou estão em liberação, e a liberação novamente para terminais com falha.

4.26.5 Gerenciamento de Revisão

1. A plataforma oferecerá suporte à geração automática do processo de revisão de conteúdo e, se a revisão for aprovada, o conteúdo será aplicado ao dispositivo automaticamente.
2. A plataforma oferecerá suporte à pré-visualização do conteúdo durante a revisão.

4.26.6 Biblioteca de Materiais

Exibição de Materiais

1. A plataforma oferecerá suporte à exibição de materiais na lista ou na miniatura, e à busca de materiais por palavras-chave e por condições.
2. A plataforma oferecerá suporte à adição de materiais da lista Meus Favoritos.
3. A plataforma oferecerá suporte à visualização do uso do material e à limpeza de materiais não utilizados ou desnecessários.

Carregar Material

1. A plataforma suportará o upload dos seguintes tipos de materiais: imagem, vídeo, áudio,

documento, página da web, imagem de URL, servidor de mídia de fluxo, IPC, etc.
2. A plataforma oferecerá suporte à seleção da área para materiais durante o upload.

Aprovação de Material

A plataforma oferecerá suporte ao uso de materiais após eles serem aprovados pelos usuários da organização atual ou de uma organização de nível superior que tenham permissão para aprovar.

4.26.7 Configurações Básicas

1. A plataforma oferecerá suporte à ativação do serviço meteorológico e à configuração do fabricante do clima para os programas, incluindo informações meteorológicas.
2. A plataforma suportará a configuração do local de armazenamento de materiais.
3. A plataforma oferecerá suporte à configuração de video walls com dimensões personalizadas.

4.27 Reunião de Emergência

Configuração da solução de emergência

1. A plataforma oferecerá suporte para fornecer orientação para configurar a solução de emergência.
2. A plataforma oferecerá suporte à configuração de múltiplas portas em diferentes áreas, pois elas permanecerão destrancadas quando uma emergência for acionada.
3. A plataforma oferecerá suporte à configuração de pontos de entrada, pontos de saída e pontos de reunião.
4. A plataforma oferecerá suporte à adição de grupos de contagem de emergência para chamada nominal.

Soluções de Emergência para áreas

1. A plataforma oferecerá suporte à configuração de soluções de reunião de emergência para diversas áreas.
2. A plataforma oferecerá suporte ao acionamento ou desligamento de emergência para diversas áreas.

Resposta Rápida

1. A plataforma deve suportar iniciar e terminar uma emergência automaticamente e manualmente. Quando a plataforma estiver em emergência, a plataforma enviará um relatório contendo informações de chamada de pessoas.
2. A plataforma oferecerá suporte para iniciar e encerrar uma emergência por meio do Web Client, Control Client e Mobile Client.

Chamada em tempo real

1. A plataforma deve suportar o início de uma chamada nominal pela qual os usuários podem contabilizar todas as pessoas nos grupos de contagem de emergência. Suporta a obtenção de dados, incluindo o número total de pessoas, pessoas em perigo, pessoas fora, mas não

registradas, pessoas fora e registradas.
2. A plataforma oferecerá suporte à visualização das últimas informações de entrada/saída na lista de estatísticas em tempo real dos grupos de contagem de emergência.
3. A plataforma oferecerá suporte ao check-in de pessoas em grupos de contagem de emergência na plataforma.
4. As estatísticas em tempo real permitirão a exibição do local do último check-in.
5. A plataforma oferecerá suporte à visualização de detalhes de cada pessoa quando uma emergência for acionada.
6. A plataforma suportará o envio de relatórios manualmente.
7. A plataforma oferecerá suporte à exportação de um relatório de reunião de emergência em formato PDF.

Permissão

A plataforma oferecerá suporte à configuração da permissão de configuração de soluções de emergência e ao início de uma chamada.

4.28 Gestão de Transmissão

- ***Implantação e gerenciamento de sistemas***
- ***Biblioteca de mídia***
- ***Configuração de armazenamento para transmissão***
- ***Transmissão ao vivo***
- ***Transmissão programada***
- ***Evento e Alarme***

4.28.1 Implantação e Gerenciamento do Sistema

Gerenciamento de Dispositivos

1. Suporte para adicionar alto-falantes IP.
2. Suporte para exibição do endereço IP, nome, número de série e status da rede do alto-falante IP.
3. Suporte ao gerenciamento de palestrantes IP por áreas.
4. Suporte para vincular câmeras (no máximo 4 câmeras) com alto-falantes IP. Suporte para visualizar a visualização ao vivo das câmeras relacionadas ao alto-falante IP.
5. Suporte para adicionar e gerenciar alto-falantes IP no mapa.
6. Suporte para configuração do volume do alto-falante IP. Suporte para configuração de transmissão programada, transmissão ao vivo e transmissão vinculada.

Rede

1. Suporta adicionar alto-falantes IP à plataforma sem inserir o endereço IP do dispositivo ou o número da porta.
2. Suporte para configuração do modo de transmissão.

4.28.2 Biblioteca de Mídia

1. Suporte ao gerenciamento da biblioteca de mídia por grupo.
2. Suporte para upload do arquivo de áudio no formato MP3.
3. Suporte para exibir o formato e o tamanho do arquivo de áudio. Suporte para baixar o arquivo de áudio.

4.28.3 Configuração de Armazenamento para Transmissão

1. Suporte para configuração de local de armazenamento (PC local ou pStor) para o áudio transmitido e os arquivos de mídia enviados.
2. Suporte para habilitar/desabilitar gravação de áudio durante a transmissão ao vivo.
3. Suporte para busca de registros de transmissões ao vivo.
4. Suporte para configuração de parâmetros para transmissão ao vivo.

4.28.4 Transmissão ao vivo

Falar

1. Suporte para falar ao vivo via grupo. Suporte para selecionar as unidades de alto-falante que são agrupadas ou não agrupadas.
2. Suporte para palestras ao vivo por área.
3. Suporte para fala ao vivo ao visualizar a exibição ao vivo das câmeras relacionadas ao palestrante IP.

Arquivo de áudio

1. Suporte à transmissão do arquivo de áudio por grupo. Suporte à seleção das unidades de alto-falante que estão agrupadas ou não agrupadas. Suporte à seleção do arquivo de áudio adicionado à biblioteca de mídia.
2. Suporte à transmissão do arquivo de áudio por área. Suporte à seleção do arquivo de áudio adicionado à biblioteca de mídia.
3. Suporte à transmissão do arquivo de áudio ao visualizar a visualização ao vivo das câmeras relacionadas ao palestrante IP. Suporte à seleção do arquivo de áudio adicionado à biblioteca de mídia.

Conteúdo de transmissão personalizado

- Suporte à transmissão do conteúdo de transmissão personalizado por grupo. Suporte à seleção das unidades de alto-falante que são agrupadas ou não agrupadas.
- Suporte à transmissão de conteúdo de transmissão personalizado por área.

4.28.5 Transmissão programada

1. Suporte para adicionar múltiplas tarefas de transmissão agendadas.
2. Suporte a transmissão por grupo. Suporte a seleção de unidades de alto-falante que são

agrupadas ou não agrupadas.
3. Apoie a transmissão por área.
4. Suporte para definir o tipo de período para transmissão, incluindo Todos os dias e Todas as semanas.
5. Suporte para definir a prioridade para tarefas de transmissão agendadas.
6. Suporte para selecionar arquivos de áudio para a tarefa de transmissão agendada e definir a duração da reprodução de cada arquivo de áudio.
7. Suporte para configuração dos horários de transmissão.

4.28.6 Evento e Alarme

1. Suporte para vincular unidade(s) de alto-falante ao adicionar a ação de vinculação para evento e alarme. Suporte para selecionar o(s) arquivo(s) de áudio adicionado(s) à biblioteca de mídia. O(s) arquivo(s) de áudio relacionado(s) será(ão) reproduzido(s) quando o alarme for disparado.
2. Suporta transmissão acionada pelo alarme até que o alarme seja reconhecido.
3. Suporte a transmissão ao vivo falando ou reproduzindo arquivos de áudio ao visualizar a exibição ao vivo relacionada ao alarme no Control Client.

4.29 Consumo de Cantina

- ***Gestão de Terminais de Pagamento***
- ***Visão geral do pagamento***
- ***Configuração básica***
- ***Gestão de Comerciantes***
- ***Gestão de Grupos de Pagamento***
- ***Gestão de Estratégia de Pagamento***
- ***Pesquisa de transações***
- ***Estatísticas e Relatórios***
- ***Gestão de Visitantes***
- ***Evento e Alarme***
- ***Manutenção e Gestão***
- ***Sistema***

4.29.1 Gestão de Terminais de Pagamento

Gestão de Terminais de Pagamento

- Suporte para adicionar, excluir e editar terminais de pagamento.
- Suporte para visualização de informações do terminal de pagamento, incluindo nome, endereço, número de série, versão, status da rede e força da senha. Suporte para configuração remota.
- Suporte para adição de terminais de pagamento via segmento IP e endereço IP.
- Suporte à importação e exportação de terminais de pagamento.

Recursos do dispositivo

- Suporte para detecção de terminais de pagamento online via SADP.
- Suporte à configuração remota de terminais de pagamento nas páginas de Configuração Remota dos dispositivos.

Atualização de firmware

Suporte para atualização de firmware por meio do Web Client atual.

4.29.2 Visão Geral do Pagamento

- Suporte para exibir o número de comerciantes e pessoas com permissões de pagamento.
- Suporte para exibição de distribuição de receita, distribuição de prazos de pagamento e distribuição ao consumidor.
- Suporte para visualização do assistente do módulo de consumo da cantina.

4.29.3 Configuração Básica

Configuração Geral

- Suporte à aplicação da unidade monetária em terminais de pagamento.
- Suporte à aplicação automática de permissões e ao cálculo automático de estatísticas.
- Suporte para habilitar registros de pagamento offline para sincronizar regularmente os registros de pagamento no Web Client com os registros armazenados nos terminais de pagamento.
- Suporte para upload de registros offline.

Configuração do tipo de refeição

- Suporte para configuração de tipos de refeições e seus períodos de tempo. Suporte para períodos de tempo entre dias para tipos de refeições.
- Suporte para adicionar, editar, excluir (excluindo os 4 tipos padrão) e visualizar tipos de refeições (até 8 tipos de refeições são permitidos).

4.29.4 Gestão de comerciantes

- Suporte para adicionar, editar e excluir comerciantes.
- Suporte para vincular terminais de pagamento com comerciantes.
- Suporte para configuração de modos de consumo (Valor, Valor Fixo e Prazos de Pagamento) para terminais de pagamento vinculados a comerciantes.
- Suporte para definir regras de pagamento (Valor, Valor Fixo e Horários de Pagamento) em períodos sem refeições.

4.29.5 Gestão de Grupos de Pagamento

- Suporte para adicionar, excluir, editar e pesquisar grupos de pagamento.
- Suporte para adicionar pessoas a grupos de pagamento. Suporte para editar, excluir e pesquisar

pessoas de um grupo de pagamento.
- Apoiar a concessão de subsídios programados para grupos de pagamento.
- Apoiar a concessão de subsídios programados a pessoas de um grupo de pagamento.
- Apoiar o cancelamento de subsídios programados para grupos de pagamento.
- Apoiar o cancelamento de subsídios programados para pessoas de um grupo de pagamento.
- Suporte para fornecer manualmente o valor/vezes do subsídio, recarregar dinheiro, reembolsar dinheiro e corrigir transações para pessoas de um grupo de pagamento.
- Suporte para visualizar as informações de pessoas de um grupo de pessoas. As informações incluem foto do perfil, nome, ID, grupo de pagamento, valor restante, tempos restantes, subsídio programado e operações.

4.29.6 Gestão de Estratégia de Pagamento

Regra de Pagamento

Suporte para adicionar, excluir, editar e pesquisar regras de pagamento em períodos de refeição e períodos sem refeição.

Autorização de Grupo de Pagamento

- Suporte para vincular comerciantes e regras de pagamento com grupos de pagamento. Suporte para cancelar vinculações e visualizar vinculações.
- Suporte para autorização/desautorização de grupos de pagamento e inscrição de pessoas de grupos de pagamento nos terminais de pagamento correspondentes dos comerciantes.

Autorização de Pessoa

- Suporte para vincular comerciantes e regras de pagamento com pessoas de um grupo de pagamento. Suporte para cancelar vinculações e visualizar vinculações.
- Suporte para autorizar/desautorizar uma pessoa e aplicar a pessoa aos terminais de pagamento correspondentes dos comerciantes.

4.29.7 Pesquisa de transações

Registro de transação

Suporte à busca de registros de transações de pessoas de um grupo de pagamento.

Registro de pagamento

Suporte à busca de registros de pagamento de pessoas.

4.29.8 Estatísticas e Relatórios

1. A plataforma oferecerá suporte à geração de estatísticas de pagamento em grupo.
2. A plataforma oferecerá suporte à geração de estatísticas de pagamento de dispositivos.
3. A plataforma oferecerá suporte à geração de estatísticas de pagamento de pessoas.
4. A plataforma oferecerá suporte à geração de relatórios de receita dos comerciantes.

4.29.9 Gestão de Visitantes

1. A plataforma oferecerá suporte à configuração de permissões de consumo para visitantes.
2. A plataforma oferecerá suporte à aplicação de permissões de consumo aos dispositivos dos visitantes.

4.29.10 Evento e Alarme

Evento e Alarme

A plataforma suportará a configuração de regras para eventos acionados por terminais de pagamento.

Visão geral

A plataforma suportará a visualização do número de terminais de pagamento anormais.

4.29.11 Manutenção e Gestão

Frequência de verificação de saúde

A plataforma oferecerá suporte à configuração da frequência de verificação de integridade dos terminais de pagamento.

Status do recurso

A plataforma oferecerá suporte à visualização do status dos terminais de pagamento, como status da rede e status de ativação.

Backup e restauração de dados do sistema

A plataforma oferecerá suporte ao backup e à restauração dos dados de consumo.

Exportação de dados

A plataforma suportará a exportação de dados de terminais de pagamento, como endereço IP e número de série.

Detalhes da licença

A plataforma oferecerá suporte à visualização de detalhes da licença do módulo de consumo da cantina e do número de terminais de pagamento.

Mago

A plataforma deverá suportar a visualização de um assistente para utilização do consumo da cantina.

4.29.12 Sistema

1. A plataforma suportará a configuração do período de retenção dos registros de pagamento.

2. A plataforma oferecerá suporte à configuração de permissões de configuração do usuário do módulo de consumo da cantina e permissões de operação dos dispositivos de consumo.

4.30 Rastreamento de Encomendas

- ***Gestão de Recursos***
- ***Gestão de Pontos de Verificação***
- ***Pesquisa de registro de digitalização (cliente de controle)***
- ***Pesquisa de registro de digitalização (cliente da Web)***
- ***Configurações de permissão***
- ***Manutenção e Gestão***

4.30.1 Gestão de Recursos

Gerenciamento de dispositivos

1. A plataforma deve suportar a adição de dispositivos de digitalização por tipos de dispositivos que incluem o leitor de código inteligente Hikvision, o scanner de código de barras Hikvision, o CodePlatform e o dispositivo de digitalização de terceiros. Para o leitor de código inteligente Hikvision, suporte para habilitar o armazenamento de imagens na plataforma.
2. A plataforma deve suportar o uso do canal de câmera de um NVR adicionado à plataforma como um canal de digitalização se o NVR estiver vinculado a um dispositivo de digitalização.
3. A plataforma oferecerá suporte à exibição de informações do dispositivo de digitalização em uma lista, incluindo nome do dispositivo, endereço do dispositivo, tipo de dispositivo, modo de acesso e status da rede.
4. A plataforma suportará a adição em lote de dispositivos de digitalização.

Gestão de Área

1. A plataforma oferecerá suporte à personalização de informações adicionais das áreas.
2. A plataforma oferecerá suporte à adição de canais de dispositivos de digitalização às áreas.
3. A plataforma oferecerá suporte à configuração do local de armazenamento de imagens (pStor ou CVR) para cada canal de digitalização.

4.30.2 Gerenciamento de Pontos de Verificação

Configuração do ponto de verificação

1. A plataforma deve suportar a configuração das definições de tempo de gravação para cada ponto de verificação individual. As definições configuradas individualmente devem ter prioridade mais alta do que as definições genéricas.
2. A plataforma deve suportar adicionar/excluir/editar e pesquisar pontos de verificação. O usuário deve ser capaz de configurar informações como nome do ponto de verificação, tipo de ponto de verificação, nota, fonte de dados, configurações de tempo de gravação e câmeras vinculadas.

3. A plataforma oferecerá suporte à adição de pontos de verificação aos Favoritos para seleção rápida durante a pesquisa de registros de digitalização.
4. A plataforma oferecerá suporte à seleção de um tipo de dispositivo de digitalização para um ponto de verificação.

Configuração de parâmetros gerais

A plataforma oferecerá suporte à configuração de parâmetros gerais, como as configurações de tempo de gravação, o limite de tempo de exceção e o período de retenção dos registros de digitalização.

1. A plataforma deve suportar a habilitação do uso do código de parada para definir o intervalo de tempo do vídeo relacionado de cada varredura. Se o código de parada não estiver habilitado, o usuário poderá especificar um horário personalizado ou o horário de varredura anterior como o horário de início da gravação, e um horário personalizado ou o próximo horário de varredura como o horário de término da gravação.
2. A plataforma oferecerá suporte à personalização do limite de tempo de exceção para definir o horário de início/término da gravação quando um intervalo de verificação exceder o limite definido.
3. O usuário poderá definir o período de retenção dos registros de digitalização para 1 mês, 2 meses ou 3 meses. A plataforma oferecerá suporte para avisar os usuários quando o período de retenção for alterado para um período menor.

4.30.3 Pesquisa de registro de digitalização (Cliente de controle)

1. A plataforma oferecerá suporte à busca de registros de digitalização por hora, código de barras e ponto de verificação.
   a. Tempo: A plataforma deve suportar a especificação de um intervalo de tempo de até 7 dias.
   b. Informações de código de barras (opcional): A plataforma oferecerá suporte à busca de uma encomenda específica se o código de barras correspondente for inserido e à busca de todas as encomendas em geral se este campo for deixado em branco.
   c. Check Point (Opcional): A plataforma deve suportar a busca por registros dos check points especificados. Se este campo for deixado em branco, a plataforma deve suportar a busca por registros de todos os check points para os quais o usuário atual tem permissão. O usuário administrador deve ser capaz de procurar por registros de escaneamento de check points que foram excluídos da plataforma.
   d. A plataforma deve suportar a exibição de resultados de pesquisa em exibição de lista e exibição de galeria. Cada miniatura na exibição de galeria deve mostrar o primeiro quadro do vídeo relacionado. A plataforma deve suportar a exibição de informações como ponto de verificação, código de barras e tempo de digitalização na exibição de lista e agrupar registros de digitalização por ponto de verificação.
2. O usuário poderá clicar em um registro de leitura de código de barras para visualizar os detalhes da leitura, verificar as imagens capturadas e reproduzir o vídeo relacionado.
3. A plataforma suportará o download de até 20 registros de digitalização e as fotos/vídeos relacionados.

4.30.4 Pesquisa de registro de digitalização (cliente da Web)

Pesquisa de registro de digitalização

A plataforma oferecerá suporte à busca de registros de digitalização por hora, código de barras e ponto de verificação.

1. Tempo: A plataforma deve suportar a especificação de um intervalo de tempo de até 7 dias.
2. Informações de código de barras (opcional): A plataforma oferecerá suporte à busca de uma encomenda específica se o código de barras correspondente for inserido e à busca de todas as encomendas em geral se este campo for deixado em branco.
3. Check Point (Opcional): A plataforma deve suportar a busca por registros dos check points especificados. Se este campo for deixado em branco, a plataforma deve suportar a busca por registros de todos os check points para os quais o usuário atual tem permissão. O usuário administrador deve ser capaz de procurar por registros de escaneamento de check points que foram excluídos da plataforma.
4. A plataforma oferecerá suporte à exibição de resultados de pesquisa, como código de barras, ponto de verificação, área, nome do recurso, tipo de dispositivo e tempo de digitalização na visualização de lista.

Detalhes do registro de digitalização

O usuário poderá clicar em um registro de leitura de código de barras para visualizar os detalhes da leitura, verificar as imagens capturadas e reproduzir os vídeos relacionados.

Download de registro de digitalização

A plataforma suportará o download de até 20 registros de digitalização e as fotos/vídeos relacionados.

4.30.5 Configurações de Permissão

Acesso a recursos

A plataforma oferecerá suporte à configuração de permissão de acesso de dispositivos de digitalização, recursos de encomendas e pontos de verificação.

Permissão do usuário

A plataforma oferecerá suporte à configuração de permissões de usuário para operar o módulo de rastreamento de encomendas.

4.30.6 Manutenção e Gestão

Backup e restauração de dados do sistema

A plataforma oferecerá suporte ao backup e à restauração dos dados das encomendas.

Detalhes da Licença

A plataforma oferecerá suporte à visualização de detalhes da licença do módulo de rastreamento

de encomendas e do número de pontos de verificação.

4.30.7 API Aberta

Suporte à busca de registros de digitalização de encomendas.

4.31 Gerenciamento de Dock

4.31.1 Configuração do Dock

Configuração do Período de Retenção de Dados

Suporte para configuração do tempo de retenção dos dados do dock: 1 mês, 3 meses, 6 meses, 1 ano, 18 meses e 2 anos.

Configuração da área de dock

1. Suporte para adicionar/excluir/editar áreas de encaixe, incluindo o nome da área de encaixe e o número total de encaixes suportados.
2. Suporte à configuração de áreas de atracação, incluindo configuração de mapas e configuração de atracação.
   a. Configuração do mapa: suporta imagens nos formatos JPFG, JPG ou PNG.
   b. Configuração de dock: suporte para adicionar um único dock ou vários docks em um lote; suporte para copiar um dock existente; suporte para selecionar docks em lote/alinhar/excluir docks.

Configuração da Câmera

Suporte para vincular um único dock com 2 câmeras especificadas para dock e 2 câmeras gerais. É necessária pelo menos 1 câmera especificada para dock.

4.31.2 Monitoramento de Dock

1. Suporte para visualizar o status (ocupado, vago ou desconhecido) de cada dock e assistir a vídeos ao vivo ou gravados transmitidos por câmeras vinculadas.
2. Suporte para visualização de informações do veículo estacionado no cais, incluindo o nome do cais, o número da placa do veículo e a duração da ocupação.

4.31.3 Estatísticas de carga/descarga de docks

Pesquisa de dados de carga/descarga de veículos

Suporte para busca de dados de veículos por hora, número da placa e dock. Suporte para visualização do número da placa, área da dock, hora de entrada/saída, taxa de carregamento (entrada/saída) e tempo de permanência de cada registro correspondente. Suporte para personalização de colunas a serem exibidas.

Exportar dados de carga/descarga de veículos

Suporte à exportação de dados de carga/descarga de veículos em formato EXCEL ou CSV, incluindo número da placa, área de atracação, número da dock, taxa de carga (entrada/saída), horário de entrada/saída e tempo de permanência.

Ver dados de carga/descarga do veículo

Suporte à visualização de dados de carga/descarga do veículo por meio do Control Client, incluindo as fotos capturadas e os vídeos gravados quando o veículo entra/sai da dock.

4.31.4 Estatísticas e relatórios de dock

Suporte para visualização de estatísticas e relatórios sobre o uso do dock, rendimento do dock e tendência de uso do dock.

4.31.5 Gerenciamento de eventos de dock

Suporte ao recebimento de eventos e alarmes de dock relatados por câmeras especificadas por dock acessadas das seguintes maneiras:

1. Câmeras especificadas para dock da série H8 acessadas via HCNetSDK;
2. Câmeras especificadas para dock da série H8 adicionadas ao NVR via HCNetSDK (o NVR é acessado na plataforma via HCNetSDK ou ISUP).

4.31.6 Controle de Permissão

Permissão de recurso

Suporte à configuração de permissões de acesso a recursos pelo dock.

Permissão do usuário

Suporte à configuração de permissões de operação do usuário.

4.31.7 Manutenção e Gestão

Fazer backup e restaurar dados do sistema

Suporte para backup e restauração de dados do dock.

Detalhes da licença

Suporte para visualização dos detalhes da licença do módulo de gerenciamento de docks e do número de docks.

4.31.8 API aberta

Suporte a eventos de relatórios (incluindo entrada/saída de veículos e eventos de status de vagas

de estacionamento) relacionados ao gerenciamento de docks.

4.32 Inspeção Inteligente

Configurações de pessoa

A plataforma oferecerá suporte à configuração e ao gerenciamento de funções relacionadas aos processos de inspeção.

1. Os administradores devem ser capazes de configurar parâmetros básicos (configurações pessoais, ativos, assinatura de eventos, modelos de inspeção, cronograma de inspeção e locais de armazenamento) e tarefas de inspeção.
2. Os inspetores devem ser capazes de executar tarefas de inspeção e enviar os resultados da inspeção.
3. Os responsáveis pelo tratamento de problemas devem ser capazes de lidar com problemas enviados pelos inspetores e enviar os resultados do tratamento de problemas.
4. Os auditores devem ser capazes de auditar os resultados do tratamento de problemas enviados pelos responsáveis pelo tratamento de problemas e fechar ou devolver problemas.

Gestão de ativos

A plataforma oferecerá suporte à adição de tipos de ativos às áreas, configurando propriedades de ativos, como nome e parte.

Objeto de inspeção

1. A plataforma oferecerá suporte à adição de inspetores, responsáveis por lidar com problemas, revisores de eventos e auditores às áreas e à vinculação de pessoas a diferentes funções.
2. A plataforma deverá suportar áreas de sincronização na plataforma como áreas de inspeção.
3. A plataforma oferecerá suporte à adição de ativos e à vinculação de câmeras a eles para inspeção.

Modelo de Inspeção

1. A plataforma oferecerá suporte à adição de setores e categorias (por exemplo, comportamentos de pessoas e requisitos ambientais).
2. A plataforma deve oferecer suporte à adição de itens de inspeção (por exemplo, ambiente higiênico, status do dispositivo, comportamentos pessoais e status da classe) em uma categoria específica, selecionar um tipo de resposta, definir respostas de julgamento lógico e adicionar ações de gatilho (por exemplo, adicionar notas, enviar anexos e criar problemas) para respostas específicas.
3. A plataforma suportará a adição de modelos de inspeção, que são a coleção de categorias de inspeção.

Cronograma de Inspeção

1. A plataforma oferecerá suporte à seleção de modelos de inspeção.
2. A plataforma suportará a seleção de objetos de inspeção (áreas ou ativos). As tarefas de inspeção são geradas de acordo com o número de objetos.

3. A plataforma deve suportar a seleção de inspetores, manipuladores de problemas e auditores. Se pessoas padrão forem configuradas, elas serão automaticamente vinculadas a tarefas de inspeção. Se não, você pode selecionar pessoas.
4. A plataforma oferecerá suporte à definição de um cronograma, incluindo frequência de inspeção, hora de início da tarefa, hora de expiração da tarefa e data de início/término do cronograma.
5. A plataforma deve suportar a seleção do modo de inspeção: inspeção remota e inspeção no local. Se o modo de inspeção for inspeção remota, habilite a captura de imagem e configure câmeras vinculadas e tempo de captura.

Assinatura de evento

A plataforma deve suportar assinaturas de eventos da plataforma. Uma vez que os eventos são disparados, tarefas de auditoria de eventos relacionadas serão geradas. O revisor de eventos pode verificar os eventos e lidar com eles, se necessário.

Revisão do evento

A plataforma oferecerá suporte à verificação de eventos acionados, à confirmação de problemas válidos e ao envio de resultados de revisão.

Inspeção Remota

1. A plataforma oferecerá suporte à implementação de tarefas de inspeção por meio de visualização ao vivo, reprodução e imagens capturadas, além do envio dos resultados da inspeção.
2. A plataforma oferecerá suporte à criação de problemas, captura de imagens, inserção de descrições, seleção do manipulador de problemas e envio de problemas.

Inspeção rápida

1. A plataforma oferecerá suporte à seleção aleatória de objetos/áreas de inspeção para visualização de vídeos ao vivo ou reprodução, captura de imagens e envio de problemas, se houver, aos responsáveis pelo tratamento de problemas.
2. A plataforma oferecerá suporte à seleção de um modelo de inspeção e aos itens de inspeção necessários para iniciar a visualização ao vivo/reprodução de áreas/ativos, verificar os itens de inspeção e enviar o resultado da inspeção.

Inspeção no local

A plataforma oferecerá suporte para tirar fotos durante a inspeção no local, adicionar notas e enviar os problemas aos responsáveis.

Tratamento de problemas

A plataforma oferecerá suporte à entrada de resultados de manuseio e ao upload de imagens de manuseio.

Auditoria de Emissão

A plataforma oferecerá suporte à auditoria dos resultados do tratamento de problemas por meio da visualização de vídeos/imagens relacionados e do envio dos resultados da auditoria.

Registro de Inspeção

A plataforma oferecerá suporte à visualização e pesquisa de problemas, tarefas e registros de revisão.

4.33 API Aberta

- ***APIs de recursos físicos***
- ***APIs de recursos lógicos***
- ***APIs de serviço de alarme***
- ***APIs de controle de acesso***
- ***APIs de serviços de eventos***
- ***API comum***

4.33.1 APIs de recursos físicos

Dispositivo de codificação

Suporte para obter informações de um dispositivo de codificação específico e lista de informações de todos os dispositivos de codificação. Suporte para pesquisar dispositivos de codificação específicos por nome do dispositivo.

Dispositivo de controle de acesso

Suporte para obter as informações de um dispositivo de controle de acesso específico e lista de informações de todos os dispositivos de controle de acesso. Suporte para pesquisar dispositivos de controle de acesso específicos por nome do dispositivo.

Servidor de streaming

Suporte para obter a lista de informações de todos os servidores de streaming.

Servidor de gravação

1. Suporte para obter informações de um servidor de gravação e lista de informações de todos os servidores de gravação, incluindo status de gravação, informações do HDD, etc.
2. Suporte para obter o status de armazenamento de todas as câmeras vinculadas a um servidor de gravação.

Servidor de Análise Inteligente

Suporte para obter a lista de informações de todos os servidores de análise inteligente, incluindo endereço IP, status da rede, etc.

Servidor de gerenciamento de sistema

Suporte para obter informações do System Management Server, incluindo uso da CPU, status da rede, etc.

4.33.2 APIs de Recursos Lógicos

Organização

1. A plataforma oferecerá suporte à obtenção de informações da organização raiz e à obtenção de uma lista de informações de organizações de nível inferior pela organização pai.
2. A plataforma oferecerá suporte à obtenção de informações de uma organização específica e à lista de informações de todas as organizações.
3. A plataforma oferecerá suporte para adicionar, excluir e editar as informações de uma organização.
4. A plataforma oferecerá suporte à busca de organizações específicas por condições.

Site

A plataforma oferecerá suporte à obtenção de informações de um site específico e à lista de informações de todos os sites.
A plataforma oferecerá suporte à busca de sites específicos pelo nome do site.

Área

A plataforma oferecerá suporte à obtenção de informações de uma área específica e à lista de informações de todas as áreas.
A plataforma oferecerá suporte à obtenção de áreas de nível inferior pela área pai.

Câmera

A plataforma oferecerá suporte à obtenção de informações de uma câmera específica por ID da câmera e à obtenção de uma lista de informações de todas as câmeras.
A plataforma oferecerá suporte à busca de câmeras pelo nome da câmera.

Entrada de Alarme

A plataforma oferecerá suporte à obtenção de informações de uma entrada de alarme específica e uma lista de informações de todas as entradas de alarme.
A plataforma oferecerá suporte à busca de entradas de alarme por condições (nome do alarme de entrada, ID do dispositivo, ID da área, etc.).

Saída de Alarme

1. A plataforma oferecerá suporte à obtenção de informações de uma saída de alarme específica e uma lista de informações de todas as saídas de alarme.
   A plataforma oferecerá suporte à busca de saídas de alarme por condições (nome do alarme de entrada, ID do dispositivo, ID da área, etc.).
2. A plataforma deve suportar o controle da saída de alarme.

Veículo

1. A plataforma oferecerá suporte para adicionar, excluir e editar um grupo de veículos.
   A plataforma oferecerá suporte para obter a lista de informações de todos os grupos de veículos.
2. A plataforma oferecerá suporte à adição de informações de um veículo a um grupo específico

de veículos, à exclusão de informações de um veículo de um grupo e à edição de informações de um veículo em um grupo.
A plataforma oferecerá suporte à obtenção de informações de um veículo específico e à lista de informações de todos os veículos.

3. A plataforma oferecerá suporte à aplicação do período de validade do número da placa aos dispositivos.
4. A plataforma oferecerá suporte para adicionar, excluir, visualizar e editar informações sobre veículos na lista de bloqueio.

Ponto de acesso

1. A plataforma oferecerá suporte à obtenção de informações de um ponto de acesso específico e à lista de informações de todos os pontos de acesso.
   A plataforma oferecerá suporte para obter a lista de informações dos pontos de acesso em uma área específica.
   A plataforma oferecerá suporte à busca de pontos de acesso por condições.
2. A plataforma oferecerá suporte à obtenção de informações do leitor de cartão de um ponto de acesso específico.

Pessoa

1. A plataforma oferecerá suporte à obtenção de informações de uma pessoa específica e à lista de informações de todas as pessoas.
   A plataforma oferecerá suporte à busca de pessoas específicas por condições.
2. A plataforma oferecerá suporte ao upload da foto do perfil da pessoa ao adicioná-la.
3. A plataforma oferecerá suporte para adicionar, excluir e editar informações pessoais, incluindo informações faciais e digitais.
4. A plataforma oferecerá suporte à aplicação de configurações ou informações de nível de acesso da pessoa (ID da pessoa, nome da pessoa, foto do rosto, impressão digital, número do cartão, validade, etc.) aos dispositivos de controle de acesso.
5. A plataforma oferecerá suporte à obtenção de detalhes de status da aplicação de informações pessoais ou configurações de nível de acesso da pessoa aos dispositivos.
   A plataforma oferecerá suporte ao retorno de falhas de aplicação e informações pessoais aguardando para serem aplicadas.
6. A plataforma oferecerá suporte para obter e editar informações personalizadas de uma pessoa.
7. A plataforma oferecerá suporte à busca do status de frequência e da duração de outros status (normal, atrasado, saída antecipada, ausente e saída tardia e antecipada) de uma pessoa específica no dia atual.
8. A plataforma oferecerá suporte à atribuição de números de quartos às pessoas.
9. A plataforma oferecerá suporte à verificação da validade de imagens faciais antes que elas sejam aplicadas aos dispositivos MinMoe.

Nível de acesso

1. A plataforma oferecerá suporte à atribuição e remoção de níveis de acesso a pessoas.
2. A plataforma deve suportar a obtenção da lista de níveis de acesso.

A plataforma oferecerá suporte à obtenção de lista de pessoas relacionadas a um nível de acesso.

Biblioteca de Imagens de Rosto

1. A plataforma oferecerá suporte para obter, excluir e editar informações de uma biblioteca de imagens de rosto.
2. A plataforma oferecerá suporte à aplicação de todas as informações das pessoas nas bibliotecas de imagens faciais aos dispositivos vinculados.

Informações faciais

1. A plataforma deve suportar a adição de informações de um único rosto à biblioteca de imagens faciais especificada e a exclusão de informações de um único rosto da biblioteca de imagens faciais especificada.
2. A plataforma oferecerá suporte à busca de informações de todos os rostos na biblioteca de imagens faciais especificada.
3. A plataforma suportará o download da imagem facial especificada de acordo com a URL.
4. A plataforma suportará verificação de identidade 1V1 ou 1VN.
5. A plataforma oferecerá suporte à busca de informações sobre rostos por câmera.

Visitante

1. A plataforma oferecerá suporte à adição de informações do visitante para check-in e edição de informações do visitante.
   A plataforma oferecerá suporte à revogação da permissão de um visitante após ele efetuar o check-out.
2. A plataforma oferecerá suporte para adicionar/editar/excluir registros de reservas de visitantes.
   A plataforma oferecerá suporte à busca de registros de reservas.
3. A plataforma oferecerá suporte à busca de informações personalizadas sobre os visitantes.
   A plataforma oferecerá suporte à busca de informações sobre grupos de visitantes e informações dos visitantes.
4. A plataforma oferecerá suporte à busca de informações dos visitantes por condição.
   A plataforma oferecerá suporte para obter informações sobre uma única visita ou.
5. A plataforma oferecerá suporte à pesquisa do status do visitante especificado no dia especificado, incluindo reservado, com check-in, expirado e com check-out.
6. A plataforma oferecerá suporte à busca de registros de check-in de visitantes.
7. A plataforma oferecerá suporte à busca de detalhes de reservas pelo número de reserva.
8. A plataforma oferecerá suporte à busca de grupos de visitantes para reserva de visitantes.
9. A plataforma oferecerá suporte para aprovação ou rejeição de reservas de visitantes enviadas.

4.33.3 APIs de serviço de vídeo

Visualização ao vivo

1. Suporte para obter o URL de streaming para visualização ao vivo.
2. Suporte para especificação do tipo de fluxo e protocolo de streaming.

3. Suporte a streaming via RTSP de câmeras de CFTV adicionadas via ISUP.
4. O protocolo de streaming está disponível para:
   a. Obter transmissão no tipo personalizado da Hikvision cooperando com o VideoSDK.
   b. Obtendo fluxo via WebSocket cooperando com o JsDecoder SDK.
   c. Obtendo transmissão via RTSP padrão.

Reprodução

1. Suporte para obter o URL de streaming para reprodução.
2. Suporte para especificação de ID da câmera, hora de início e término e protocolo de streaming.
   a. O protocolo de streaming está disponível para: Obter transmissão no tipo personalizado da Hikvision cooperando com o VideoSDK.
   b. Obtendo fluxo via WebSocket cooperando com o JsDecoder SDK.

Áudio bidirecional

Suporte para obter a URL de streaming para áudio bidirecional. Atualmente, a função de áudio bidirecional só pode ser realizada com a cooperação do VideoSDK e do WebSDK.

Controle PTZ

1. Suporte para adicionar e excluir uma predefinição de uma câmera.
2. Suporte para busca de informações predefinidas de uma câmera.
3. Suporte para adicionar e excluir uma patrulha de uma câmera.
4. Suporte à busca de informações de patrulha de uma câmera.
5. Suporte ao controle do PTZ por ID da câmera.

SDK de vídeo

1. O Video SDK, sem interface de vídeo, fornece aplicativos no cliente de PC, incluindo visualização ao vivo, gravação, pesquisa de vídeo, reprodução, reprodução de quadro único, download de vídeo, captura, controle de áudio, áudio bidirecional, etc.
2. Fornece demonstrações C++ e C# para o Video SDK

Vídeo WebSDK

1. O Video WebSDK, com interface de vídeo básica e barra de ferramentas, fornece um plug-in executado no navegador da web para implementar diversas funções de vídeo, como visualização ao vivo, reprodução, criação de janela de plug-in, ajuste de tamanho de janela, divisão de janela, etc.
2. Forneça demonstrações para o WebSDK.

jsDecoder SDK

1. O jsDecoder SDK, com interface de vídeo básica, fornece uma solução sem plug-in para iniciar a visualização ao vivo (incluindo gravação manual, captura manual, controle de áudio, exibição em tela cheia, zoom digital, posicionamento 3D) e reprodução (pausar, parar, avanço rápido/lento, reprodução de quadro único, gravação manual, zoom digital, posicionamento 3D) do dispositivo por meio do navegador da web. O jsDecoder SDK oferece suporte ao tipo de

streaming WSS.
2. Forneça demonstrações para o jsDecoder SDK.
3. Suporta áudio bidirecional.

Transmissão Padrão

Suporta reprodução padrão via RTSP, visualização ao vivo e reprodução via HLS e visualização ao vivo e reprodução via RTMP.

4.33.4 APIs de análise inteligente

Estatísticas de contagem de pessoas
1. Suporte para obter estatísticas de contagem de pessoas da câmera especificada por minuto, hora, dia e mês. Suporte para carregar informações de alarme por prioridade.
2. Suporte para obter estatísticas em tempo real de grupos de recursos.
3. Suporte para obter a lista de grupos de recursos.

Mapa de Calor

Suporte para obter estatísticas sobre o tempo de permanência das pessoas e a contagem de pessoas.

4.33.5 APIs de serviço de alarme

Pesquisa de registro de alarme

Suporte à busca de registros de alarmes.

Imagem de alarme

Suporte para download de imagens de alarme.

Reconhecimento de alarme

Suporte para reconhecimento de alarmes.

Tipos de alarme/evento

1. Suporta 56 tipos de alarmes/eventos sobre a câmera, como vadiagem, aglomeração de pessoas, exceção de gravação da câmera, direção na contramão e movimento rápido.
2. Suporta 38 tipos de alarmes/eventos sobre leitura de cartão, como alarme de coação, acesso concedido por ID do funcionário e impressão digital, e acesso negado por ID do funcionário e rosto.

4.33.6 APIs de serviço ANPR

Pesquisa de registro de passagem de veículos

A plataforma oferecerá suporte à busca de registros de passagem de veículos.

Informações do evento ANPR

A plataforma oferecerá suporte a informações de eventos ANPR: número da placa, marca do veículo, proprietário do veículo, contato do proprietário, tipo de veículo, cor do veículo, país/região pertencente e direção de direção.

Foto do veículo que passa

A plataforma oferecerá suporte à busca e ao download de imagens dos veículos que passam.

4.33.7 APIs de controle de acesso

Controle de porta

Suporte ao controle de portas por ID de porta, incluindo abertura de portas, fechamento de portas, portas restantes abertas e portas restantes fechadas.

Acessar Pesquisa de Registro

Suporte à busca de registros de acesso por hora, nome da pessoa, ID do ponto de acesso e tipo de evento.

Evento de acesso

Suporte para obtenção de imagens de eventos de acesso.

4.33.8 APIs de serviço de eventos

Assinatura de evento

Suporte para assinatura de eventos por tipo de evento, como evento de intrusão, evento de alarme de temperatura, alarme de placa de carro correspondente, alarme de temperatura anormal e evento de acesso (autenticado por rosto e senha).

Pesquisa de eventos inscritos

Suporte à busca de eventos inscritos por ID de usuário.

Evento Genérico

Suporte para adicionar, excluir e editar um evento genérico. Suporte para obter a lista de informações de eventos genéricos. Suporte para configurar parâmetros para receber alarmes de eventos genéricos.

4.33.9 APIs de estacionamento

Gestão de estacionamento

A plataforma deve suportar a obtenção da lista de informações do estacionamento. Suportar a busca dos registros de passagem de veículos de um estacionamento específico e os registros de estacionamento do veículo e duração do estacionamento. Suportar a obtenção da ocupação de

vagas de estacionamento em andares específicos e vagas de estacionamento de cada tipo.

Taxa de estacionamento

1. A plataforma oferecerá suporte para obter a taxa de estacionamento e a duração do estacionamento de acordo com o número da placa.
2. A plataforma deve suportar o retorno das informações de confirmação após o pagamento da taxa de estacionamento. O veículo pode sair do estacionamento depois disso.

4.33.10 APIs de monitoramento móvel

Lista de veículos

A plataforma suportará a obtenção da lista de veículos no módulo de Monitoramento Móvel.

Informações do veículo

A plataforma oferecerá suporte à obtenção de informações detalhadas do veículo de acordo com o número do veículo.

Áudio bidirecional

A plataforma suportará áudio bidirecional direto com dispositivos móveis.

Informações de GPS

A plataforma oferecerá suporte à obtenção de informações de GPS em tempo real e à busca de informações históricas de GPS.

Relatar alarme

A plataforma oferecerá suporte à notificação de alarmes de dispositivos móveis para a plataforma, incluindo alarme de evento ADAS, alarme de evento de comportamento de direção, alarme de emergência, etc.

Baixar fotos/vídeos

A plataforma oferecerá suporte ao download de fotos e vídeos de pesquisas de eventos de monitoramento de bordo ou envio de notificações.

4.33.11 API Comum

Suporte para obter informações sobre a versão da plataforma.

4.34 Integração de Protocolo

- ***Portal BACnet***
- ***Driver de dispositivo BACnet***
- ***Portal SIA***
- ***Driver de dispositivo SIA***

4.34.1 Gateway BACnet

Configuração básica

A plataforma oferecerá suporte à configuração das seguintes informações básicas: usuário parceiro, versão do protocolo (versão 1.0), número da instância BAC, nome do dispositivo BACnet, duração do tempo limite do APDU e tempos de reenvio do APDU.

Modelo de objeto

A plataforma deve suportar a configuração do template de objeto. Os quatro tipos de objeto suportados são o valor binário, porta de acesso, saída binária e entrada binária.

Configuração do objeto

1. A plataforma deve suportar a configuração do modelo de objeto para Status de Rede e vincular recursos (propriedade somente leitura) com objetos BACnet. Os recursos de dispositivo suportados incluem dispositivos de codificação, dispositivos de controle de acesso, servidores de gravação e servidores de streaming. Os recursos lógicos suportados são câmeras, portas e saídas de alarme.
2. A plataforma deve suportar a configuração do modelo de objeto para Status da Porta e vincular o recurso da porta (propriedade de leitura e gravação) com objetos BACnet.
3. A plataforma deve suportar a configuração do modelo de objeto para Status de Saída de Alarme e vincular o recurso de saída de alarme (propriedade de leitura e gravação) com objetos BACnet.
4. A plataforma deve suportar a configuração do modelo de objeto para Status de Alarme e vincular o recurso de alarme (propriedade somente leitura) com objetos BACnet.

Ligação de Objetos

1. A plataforma oferecerá suporte à vinculação de recursos na plataforma com objetos BACnet para gerenciar recursos, incluindo dispositivos de controle de acesso e saídas de alarme em sistemas de terceiros.
2. A plataforma oferecerá suporte à notificação de eventos de alarme de recursos vinculados a objetos BACnet para sistemas de terceiros.

4.34.2 Driver de dispositivo BACnet

Acesso ao dispositivo BACnet

1. A plataforma oferecerá suporte à adição, exclusão, edição de dispositivos BACnet e adição de dispositivos BACnet on-line.
2. A plataforma oferecerá suporte à importação de objetos BACnet para áreas e à visualização de seu status.
3. A plataforma suportará a filtragem de objetos BACnet por tipos de objeto.

Gerenciamento de Permissões BACnet

A plataforma oferecerá suporte à configuração de permissão de recurso, permissão de acesso e

permissão de configuração para BACnet.

Manutenção de Objetos BACnet

1. A plataforma deve suportar a edição do valor presente de um objeto BACnet. Os tipos de objetos suportados são o valor multiestado, saída multiestado, entrada multiestado, entrada binária, saída binária, valor binário, entrada analógica, saída analógica e valor analógico.
2. A plataforma oferecerá suporte à visualização de exceções (incluindo offline, falha, em alarme, substituído e fora de serviço) de objetos BACnet.
3. A plataforma oferecerá suporte à busca de eventos de dispositivos BACnet na página de pesquisa de log do servidor.

Evento BACnet

A plataforma oferecerá suporte ao recebimento e à notificação de diferentes tipos de eventos BACnet, incluindo mudança de estado, falha de comando, falha, em alarme, fora de alcance, fora de serviço e substituído.

Monitoramento de Mapas

1. A plataforma suportará a configuração de diferentes ícones para exibir diferentes status de objetos BACnet em um mapa visual.
2. A plataforma oferecerá suporte à exibição do status em tempo real dos objetos BACnet em um mapa visual.

4.34.3 Portal SIA

Configuração básica

A plataforma oferecerá suporte à configuração das seguintes informações básicas: usuário parceiro, versão do protocolo (SIA-DCS), endereço IP do sistema de terceiros, número da porta, número da placa de linha, número do receptor e intervalo de pulsação.

Configuração do modelo de evento

1. A plataforma deve suportar a definição do tipo de fonte do evento para o evento do dispositivo de codificação, evento da câmera, evento de entrada de alarme e evento do painel de controle de segurança.
2. A plataforma oferecerá suporte à inserção de tipos de eventos personalizados e códigos SIA.
3. A plataforma oferecerá suporte à seleção de tipos de eventos padrão e códigos SIA.
4. A plataforma suportará a importação de modelos de eventos.

Configuração de Zona

A plataforma oferecerá suporte à definição da seguinte configuração de zona SIA: nome da configuração, ID da conta, ID do grupo, tipo de recurso e modelo de evento.

Encaminhamento de alarme

A plataforma suportará o encaminhamento de alarmes para sistemas de terceiros.

4.34.4 Driver de dispositivo SIA

Acesso ao dispositivo SIA

1. A plataforma oferecerá suporte à adição, exclusão e edição de dispositivos que suportem o protocolo SIA.
2. A plataforma oferecerá suporte para adicionar e editar contas SIA.
3. A plataforma oferecerá suporte para adicionar, excluir e editar zonas.
4. A plataforma oferecerá suporte à importação de zonas SIA para áreas como entradas de alarme.

Evento SIA

1. A plataforma oferecerá suporte à configuração do acesso ao evento SIA vinculando tipos de eventos com IDs de eventos.
2. A plataforma oferecerá suporte à configuração de eventos SIA e ao acionamento dos alarmes correspondentes.
3. A plataforma dará suporte ao recebimento de eventos da SIA.

Manutenção

1. A plataforma oferecerá suporte à visualização de registros de operação de dispositivos SIA.
2. A plataforma oferecerá suporte à visualização do status da zona dos dispositivos SIA.
3. A plataforma oferecerá suporte à visualização do status dos dispositivos SIA.

Monitoramento de Mapas

A plataforma oferecerá suporte à visualização das zonas da SIA em um mapa visual.

4.34.5 Modbus

Acesso ao dispositivo Modbus

1. A plataforma oferecerá suporte à adição, exclusão e edição de dispositivos Modbus, além de visualização do status do dispositivo.
2. A plataforma suportará a adição em lote de recursos Modbus à área e visualizará o status dos recursos.
3. A plataforma oferecerá suporte à configuração dos parâmetros de recursos.

Evento Modbus

1. A plataforma suportará a configuração de eventos Modbus.
2. A plataforma suportará o recebimento de eventos Modbus.
3. A ação de vinculação da edição do valor do recurso Modbus será acionada por outros eventos.

Manutenção

1. O usuário poderá visualizar os registros de operação dos dispositivos Modbus.
2. O usuário poderá visualizar o status dos recursos dos dispositivos Modbus.
3. O usuário poderá visualizar o status dos dispositivos Modbus.

Monitoramento de Mapas

A plataforma oferecerá suporte à visualização de dispositivos Modbus em um mapa visual.

4.34.6 WhatsApp

Parâmetros básicos

1. A plataforma oferecerá suporte à configuração de informações da conta do comerciante do WhatsApp, incluindo conta do comerciante, número de telefone, número do aplicativo, endereço do ponto de extremidade, token de acesso e token de verificação.
2. A plataforma deve suportar a configuração do limite superior de tempos de conversação diários e mensais. Não é mais permitido push de mensagem quando o limite superior é atingido.

Registro de revisão de modelo do WhatsApp

A plataforma oferecerá suporte à visualização do status de revisão dos modelos de mensagens do WhatsApp.

Registro de mensagem push do WhatsApp

1. A plataforma oferecerá suporte à visualização de registros de envio/recebimento de mensagens do WhatsApp.
2. A plataforma oferecerá suporte à filtragem de registros de envio/recebimento de mensagens do WhatsApp por hora, nome da conta do WhatsApp e status da mensagem.

Mensagem Push do WhatsApp

A plataforma deverá suportar a ativação ou desativação da função WhatsApp na plataforma.

Capítulo 5 Execução

5.1 Exame

1. Inspecione a área de instalação escolhida antes de receber os dispositivos e relate quaisquer condições que afetem o processo de instalação ou qualquer operação subsequente.
2. Não inicie a instalação até que todas as condições inaceitáveis sejam corrigidas.

5.2 Preparação

Dispositivos embalados de forma a ajudar a evitar qualquer dano durante a construção.

5.3 Instalação

1. Os dispositivos devem ser instalados de acordo com as instruções fornecidas pelos fabricantes, bem como instruções baseadas em quaisquer especificações de projeto de piso indicadas.
2. O local de instalação deve fornecer condições razoáveis para a funcionalidade ideal do dispositivo. As condições de temperatura e nível de umidade devem ser levadas em consideração.
3. Todas as instalações devem ser realizadas apenas por profissionais de serviço qualificados.
4. Todos os dispositivos devem ser instalados de acordo com o Código Elétrico Nacional ou códigos locais aplicáveis.
5. Certifique-se de que o local de instalação ofereça uma possibilidade mínima de danos acidentais.

5.4 Controle de Qualidade de Campo

1. Avalie a compatibilidade dos parafusos de montagem para todos os equipamentos a serem instalados.
2. Teste adequadamente todos os sistemas que não sejam de vídeo em relação aos requisitos operacionais padrão.
3. Defina, conclua e relate todos os problemas com o equipamento aos representantes de atendimento ao cliente dos fabricantes.

5.5 Ajuste

1. Execute as modificações necessárias no Sistema de Gerenciamento sem Vídeo para uma operação adequada, de acordo com as instruções fornecidas pelo fabricante.
2. Garantir que os requisitos exclusivos dos clientes sejam refletidos nas configurações de

controle de acesso.

5.6 Demonstração

Após a inspeção final, valide se o sistema sem vídeo e seu dispositivo funcionam corretamente.


See Far, Go Further

DS-K3G200LXM
Value Tripod Turnstile

By adopting the turnstile integratedly with the access control system, person should authenticate to pass through the lane via presenting cards, face, or QR code, etc. It is widely used in attractions, office, construction sites, residences, etc.

- Bidirectional (Entering/Exiting) lane.
- High-brightness LED indicates the entrance/exit and passing status except "Pg" type.
- Fire alarm passing: When triggered, the arms will be dropped automatically for emergency evacuation.
- Support IO connection for 3rd party ACS integration.
- For "Pg" type, the face terminal need purchase separately.

▪ Specification

System	
MCBF	2 Million – 24/7
Interface	
Exit button	x 2
TAMPER	NA
NC/NO	x 1
Hardware	
Access controller	Not included
Network switch	Not included
Power supply for face recognition module	Not included
Keyfob	Not supported
General	
Throughput	More than 25 persons per minute The actual throughput is affected by the person passing rate and passing method.
Lane width	550mm
Barrier material	SUS/ANSI304 stainless steel pipe
Pedestal material	SUS/ANSI304 stainless steel 1.0mm (0.03'')
Indicator	Yes, except for "Pg" type
Arm angle while resting position	120 degress
Power consumption and operation	115~240Vac – 50~60Hz / 25W (stand by) / 100W maximum (During Rotation)
Working temperature	-20 °C to 65 °C (-4 °F to 149 °F)
Working humidity	0% to 95% (No condensing)
Dimensions	Without package: 426 mm ×286 mm × 982.5 mm With package: 700 mm × 430 × 1120 mm
Weight	Without package:21 kg (46.3 lb) With package: 29.5 kg (64.9 lb)
Approval	CE, CB, RoHS, REACH, WEEE
Configuration	
Lane width	550 mm
Pedestal length	426 mm
Module selection	NO
Pedestal width	286 mm
Wall distance	60 mm
Base	YES
Barrier material	Stainless steel pipe
Base model	DS-K3G200X-BASE
Product type	Tripod Turnstile
Remote controller type	NA
Functions	
Sensor Rotation Monitoring	Yes

Power Supply Short-Circuit Protection	Yes
Anti-Reverse System	Yes < 105kgf torque

▪ Available Model

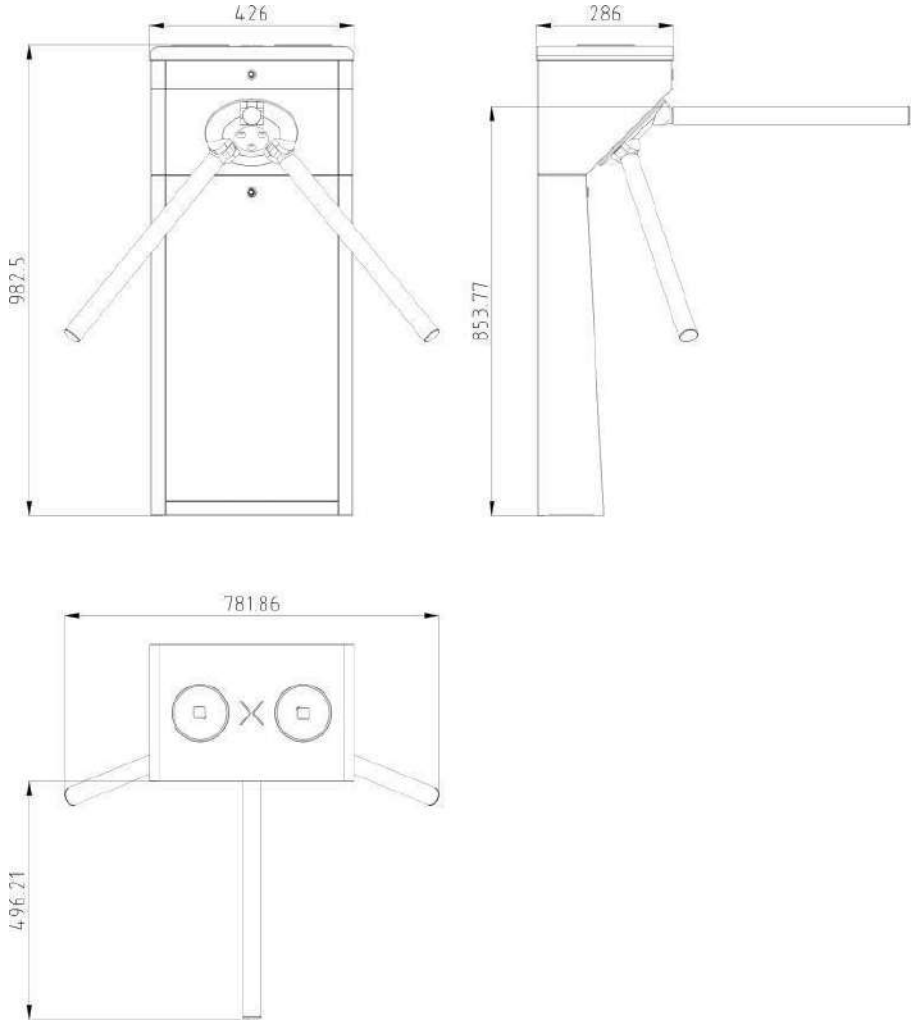
DS-K3G200LX-R/Dm55

DS-K3G200LX-R/Pg-Dm55

DS-K3G200LXM-R/Dm55

DS-K3G200LXM-R/Pg-Dm55

▪ Dimension



▪ Accessory

▪ Optional

DS-K1102A Pro 1102A Series Card Reader	DS-K7CR01	DS-KAB6-ZU1
		

DS-K1T673 Series Face Recognition Terminal

User Manual

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
FCC compliance: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
—Reorient or relocate the receiving antenna.
—Increase the separation between the equipment and receiver.
—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
—Consult the dealer or an experienced radio/TV technician for help
This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.
FCC Conditions
This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:
1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement

CE

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed

under the EMC Directive 2014/30/EU, RE Directive 2014/53/EU,the RoHS Directive 2011/65/EU

2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info

2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see:www.recyclethis.info

Safety Instruction

These instructions are intended to ensure that user can use the product correctly to avoid danger or property loss.

The precaution measure is divided into Dangers and Cautions:

Dangers: Neglecting any of the warnings may cause serious injury or death.

Cautions: Neglecting any of the cautions may cause injury or equipment damage.

⚠	⚠
Dangers: Follow these safeguards to prevent serious injury or death.	**Cautions:** Follow these precautions to prevent potential injury or material damage.

⚠ Danger:

- All the electronic operation should be strictly compliance with the electrical safety regulations, fire prevention regulations and other related regulations in your local region.
- Please use the power adapter, which is provided by normal company. This equipment is intended to be supplied from the Class 2 surge protected power source rated DC 12V, 3A.
- Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.
- When the product is installed on wall or ceiling, the device shall be firmly fixed.
- If smoke, odors or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.
- Do not ingest battery, Chemical Burn Hazard.
  This product contains a coin/button cell battery. If the coin/button cell battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death.
  Keep new and used batteries away from children. If the battery compartment does not close securely, stop using the product and keep it away from children. If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the device yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)

⚠ Cautions:

- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).
- Do not place the device in extremely hot (refer to the specification of the device for the detailed operating temperature), cold, dusty or damp locations, and do not expose it to high electromagnetic radiation.
- The device cover for indoor use shall be kept from rain and moisture.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- Do not aim the device at the sun or extra bright places. A blooming or smear may occur otherwise (which is not a malfunction however), and affecting the endurance of sensor at the same time.
- Please use the provided glove when open up the device cover, avoid direct contact with the device cover, because the acidic sweat of the fingers may erode the surface coating of the device cover.
- Please use a soft and dry cloth when clean inside and outside surfaces of the device cover, do not use alkaline detergents.
- Please keep all wrappers after unpack them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage on the device and lead to additional costs.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.
- Biometric recognition products are not completely applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.
- Working temperature: -30 °C to +60 °C
- Indoor and outdoor use. If installing the device indoors, the device should be at least 2 meters away from the light, and at least 3 meters away from the window or the door. If installing the device outdoors, you should apply Sililcone sealant among the cable wiring area to keep the raindrop from entering.
- Protection level: IP65

Available Models

Product Name	Model
Face Recognition Terminal	DS-K1T673DX
	DS-K1T673DWX
	DS-K1T673TDX
	DS-K1T673TDWX
	DS-K1T673TDX-M
	DS-K1T673TDGX
	DS-K1T673TMW
	DS-K1T673TMG

Use only power supplies listed in the user instructions:

Model	Manufacturer	Standard
C2000IC12.0-24P-DE	MOSO Power Supply Technology Co., Ltd.	CEE
C2000IC12.0-24P-GB	MOSO Power Supply Technology Co., Ltd.	BS
KPL-040F-VI	Channel Well Technology Co Ltd.	CEE

Legal Information

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (***https://www.hikvision.com***). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

- This product can only enjoy the after-sales service support in the country or region where the purchase is made.
- If the product you choose is a video product, please scan the following QR code to obtain the "Initiatives on the Use of Video Products", and read it carefully.

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR

IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Data Protection

- To protect data, the development of Hikvision Products incorporates privacy by design principles. For example, for Products with facial recognition features, biometrics data is stored in your Products with encryption method; for fingerprint Products, only fingerprint template will be saved, which is impossible to reconstruct a fingerprint image.
- As a data controller/processor, you may process personal data, including collection, storage, use, processing, disclosure, deletion, etc. You are advised to pay attention to and comply with applicable laws and regulations related to the protection of personal data, including without limitation, conducting security controls to safeguard personal data, such as, implementing reasonable administrative and physical security controls, conduct periodic reviews and the assessments of the effectiveness of your security controls.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 **Danger**	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.
 **Caution**	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 **Note**	Provides additional information to emphasize or supplement important points of the main text.

Contents

Chapter 1 Appearance

Refer to the following contents for detailed information of the face recognition terminal:

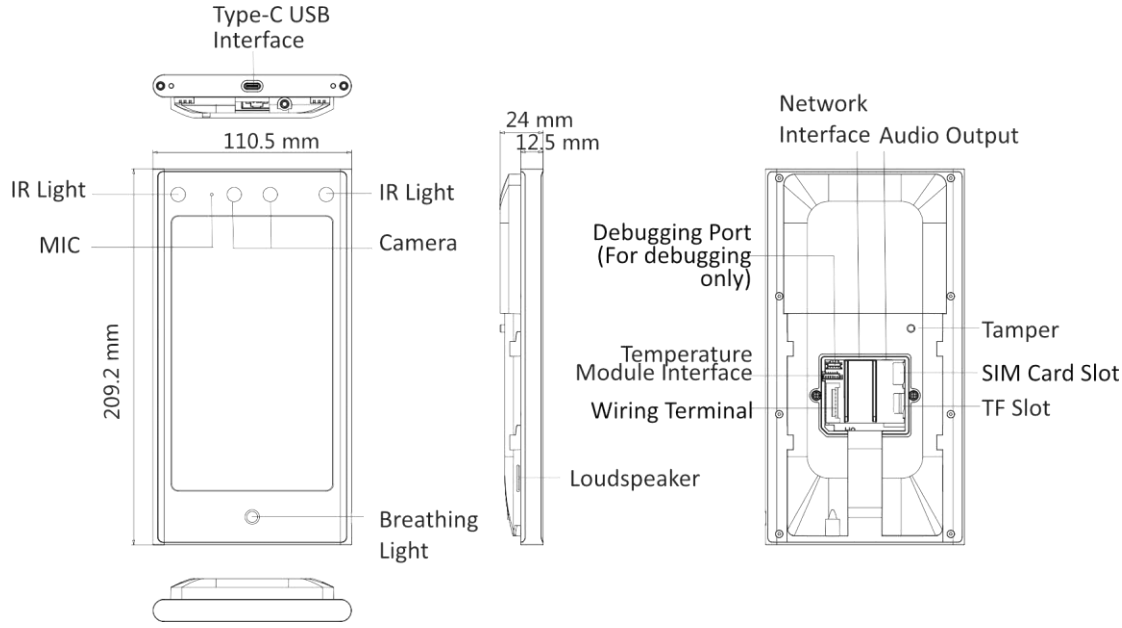


Figure 1-1 Face Recognition Terminal

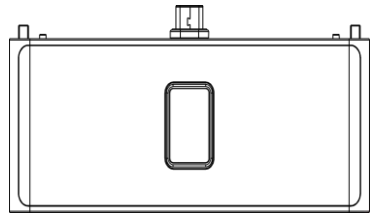


Figure 1-2 Fingerprint + Bluetooth + QR Code Module

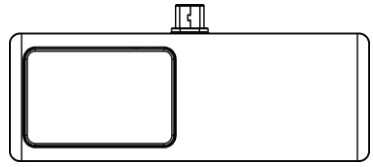


Figure 1-3 Wireless Module （433/868 Mhz）

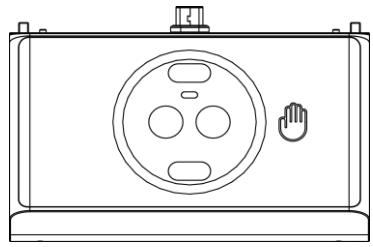


Figure 1-4 Palm Print and Palm Vein Module

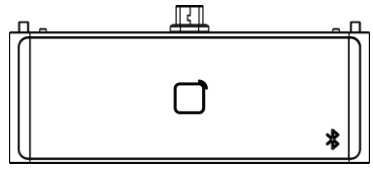


Figure 1-5 Dual-frequency Card Module（13.56 Mhz and 125 Khz）

Note

- The figures are for reference only.
- The device supports different modules, which can be accessed according to your actual needs.
- When the palm print and palm vein module access to the new face recognition terminal, the data of the peripheral module needs to be cleared and re-issued or collected.
- The surface of the peripheral module should be kept clean to avoid false alarms caused by the sensor.

Chapter 2 Installation

2.1 Installation Environment

- Avoid backlight, direct sunlight, and indirect sunlight.
- For better recognition, there should be light source in or near the installation environment.
- If you have to install the device outdoors, you should install a protective shield (optional) for the device.

Note

For details about installation environment, see *Tips for Installation Environment*.

2.2 Flush Mounting with Gang Box

Before You Start

Remove the back sheet of the device.

Steps

1. Make sure the gang box is installed on the wall.

   Note

   Gang box is not supplied.

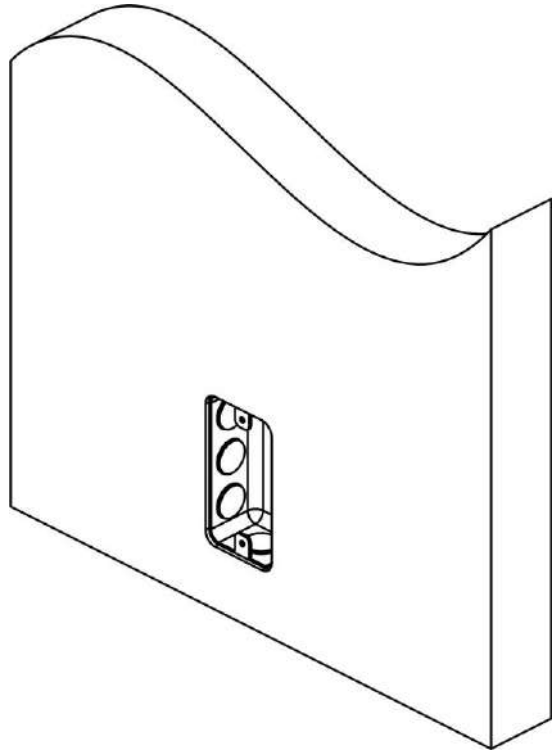


Figure 2-1 Install Gang Box

2. Secure the mounting plate on the gang box with 2 supplied screws (SC-K1A4X24_5).

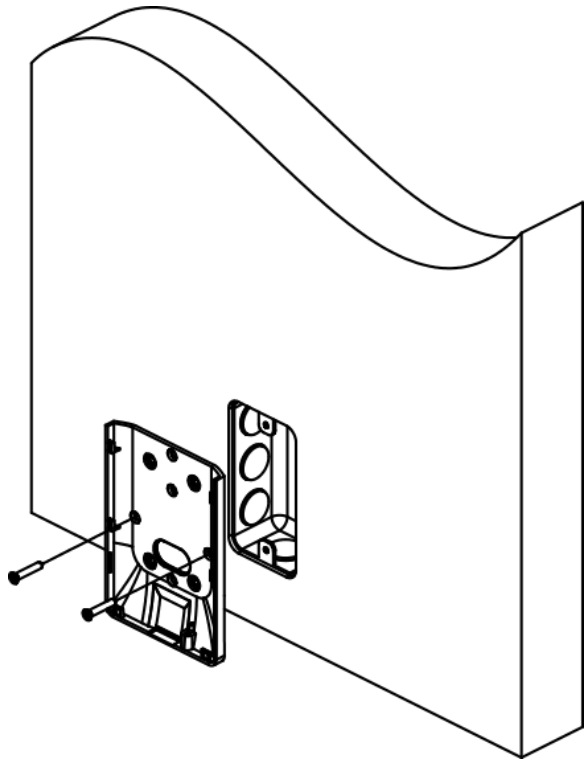


Figure 2-2 Install Mounting Plate

3. Route the cable through the cable hole, wire the cables and insert the cables in the gang box.

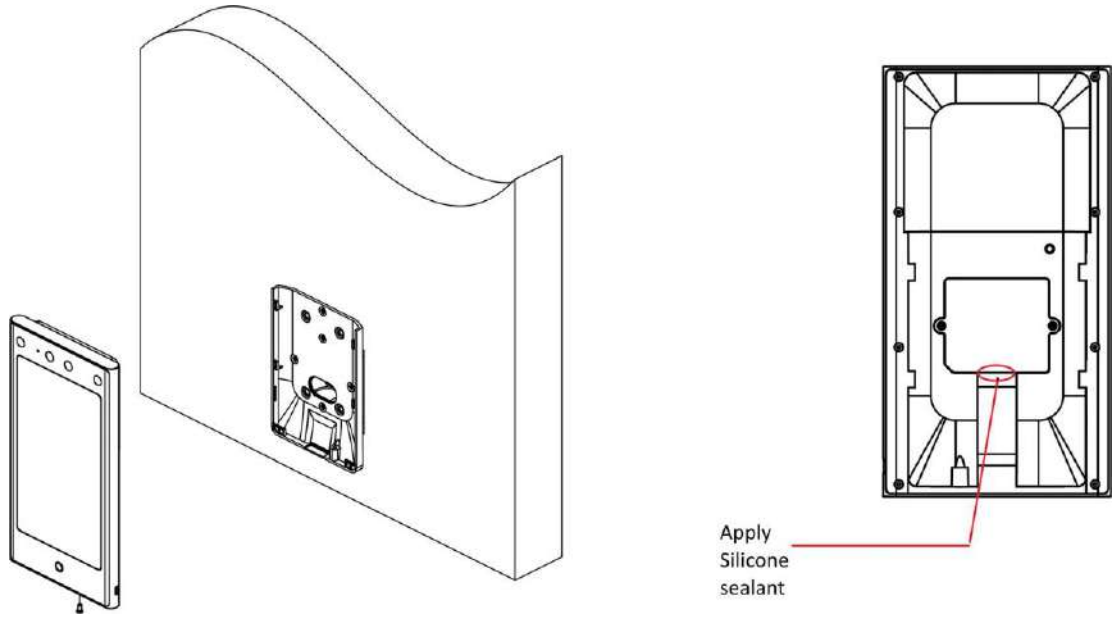


Figure 2-3 Secure Device

Note

Apply Silicone sealant among the cable wiring area to keep the raindrop from entering.

4. Align the device with the mounting plate, and secure the device on the mounting plate with 1 supplied screw (SC-KM3X6-H2-SUS).

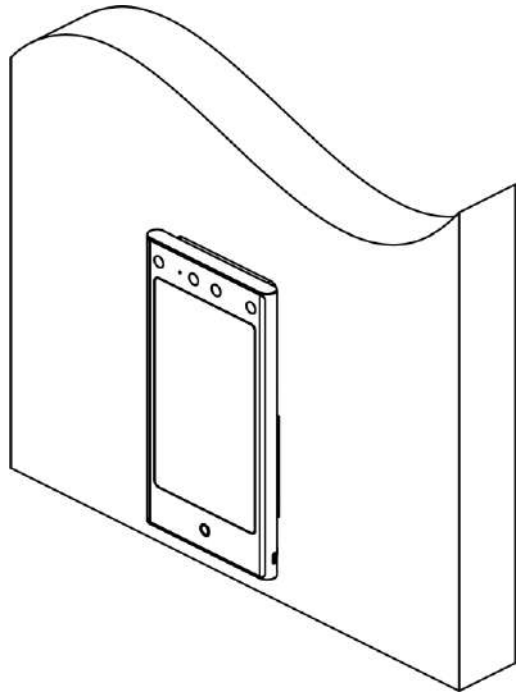


Figure 2-4 Secure Device

5. After installation, for the proper use of the device (outdoor use), stick the protection film (parts of models supplied) on the screen.

2.3 Surface Mounting

Steps

Note

The additional force shall be equal to three times the weight of the equipment. The equipment ad its associated mounting means shall remain secure during the installation. After the installation, the equipment, including any associated mounting plate, shall not be damaged.

1. According to the datum line on the mounting template, stick the mounting template on the wall or other surfaces, 1.4 meters higher than the ground.

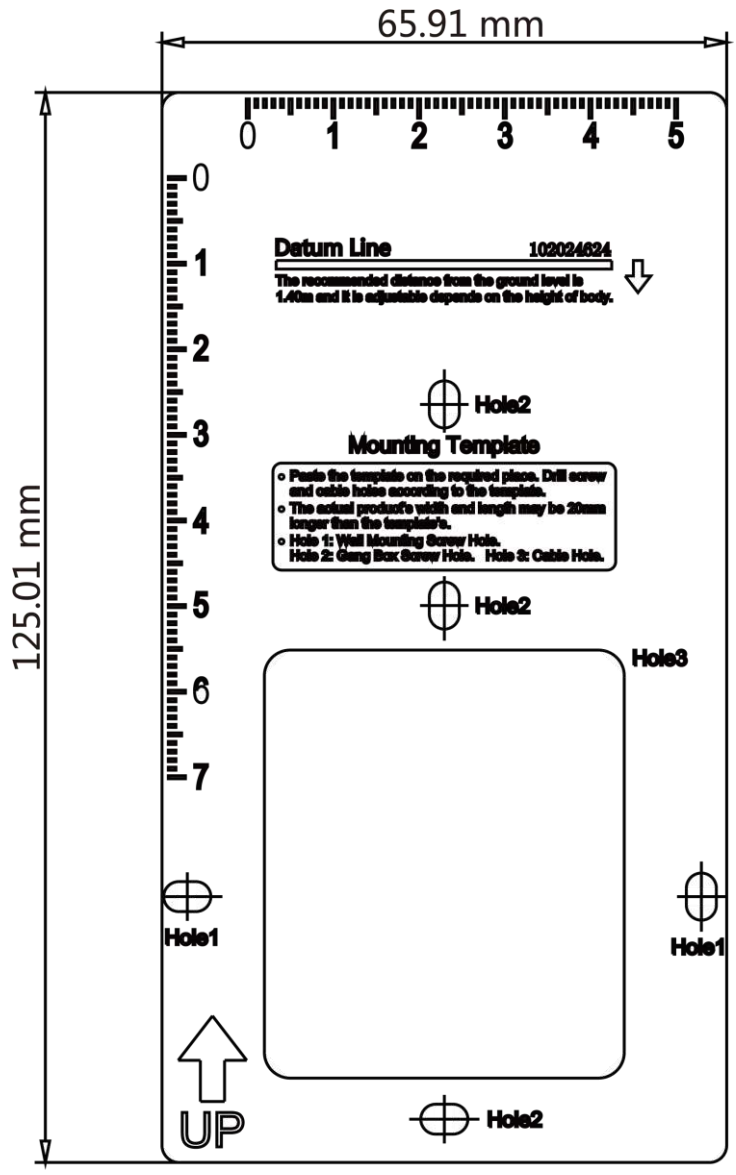


Figure 2-5 Mounting Template

2. Drill holes on the wall or other surface according to the Hole 1 on the mounting template.

3. Remove the cable hole on the mounting plate with tools.

4. Align the holes to the mounting plate and secure the mounting plate on the wall with the 2 supplied screws (K1A×24).

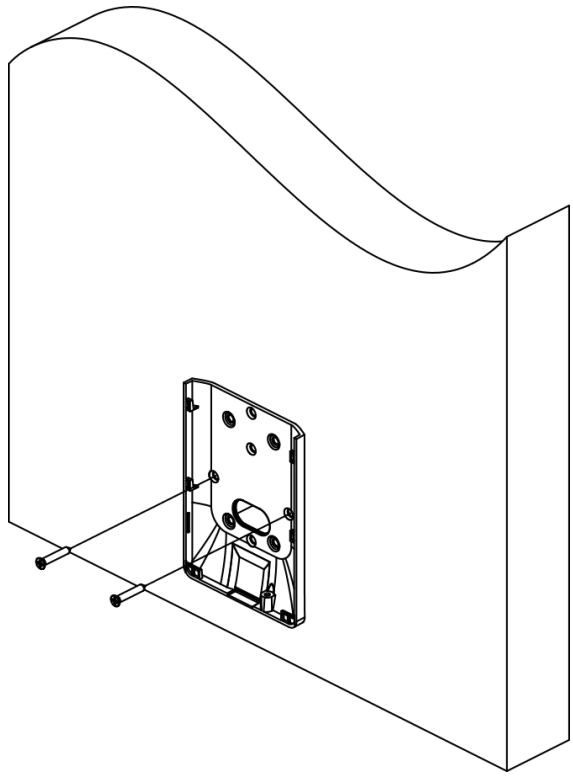


Figure 2-6 Install Mounting Plate

5. Route the cable through the cable hole of the mounting plate, and connect to corresponding peripherals cables.

Note

If the device is installed outdoor, you should apply silicone sealant to the wiring exit to avoid water from entering.

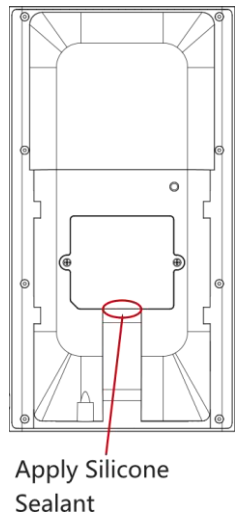


Figure 2-7 Apply Silicone Sealant

6. Align the device with the mounting plate and hang the device on the mounting plate.

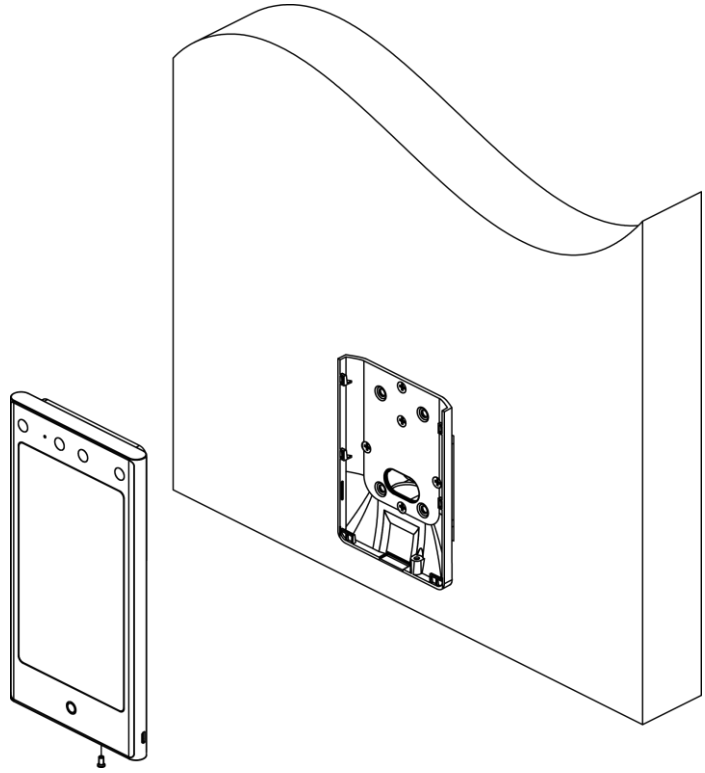


Figure 2-8 Hang Device

7. Use 1 supplied screw (KM3×6) to secure the device and the mounting plate.

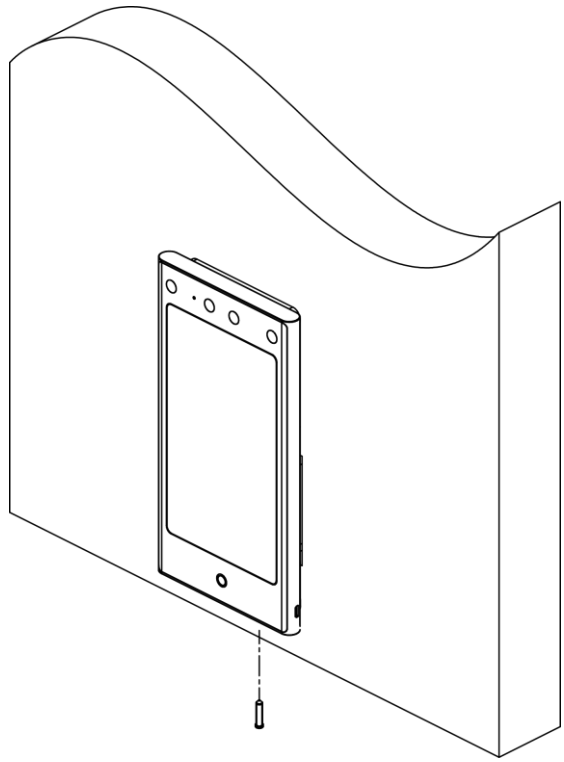


Figure 2-9 Secure Device

8. **Optional:** Connect the peripheral module according to your actual needs.
9. After installation, for the proper use of the device (outdoor use), stick the protection film (parts of models supplied) on the screen.

2.4 Mount With Bracket

2.4.1 Preparation before Mounting with Bracket

Steps

1. Drill holes on the turnstile's surface according to the figure displayed below. And install water-proof nut.

Note

Solder after pressing rivets to avoid water from entering.

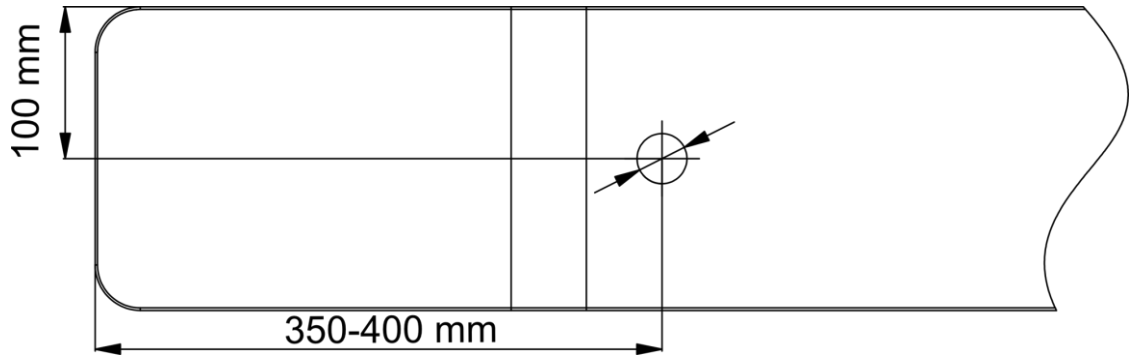


Figure 2-10 Drill Holes on Turnstile

2. If the installation angle needs to be 180° perpendicular to the body of the turnstile, the following operations are required.

1) Take off the 3 screws shown in the following figure.

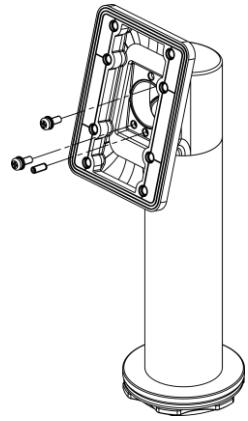


Figure 2-11 Take off Screws

2) Rotate the fixed part by 180°, and install the 3 screws back.

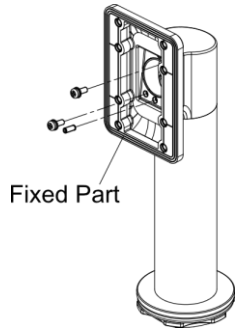


Figure 2-12 Rotate Fixed Part

2.4.2 Mount Bracket

Steps

1. Pass the bracket bottom through the turnstile, and fix it into the turnstile with self-contained nut. Adjust the bracket to the suitable angle, and fix the nut tightly by the wrench.

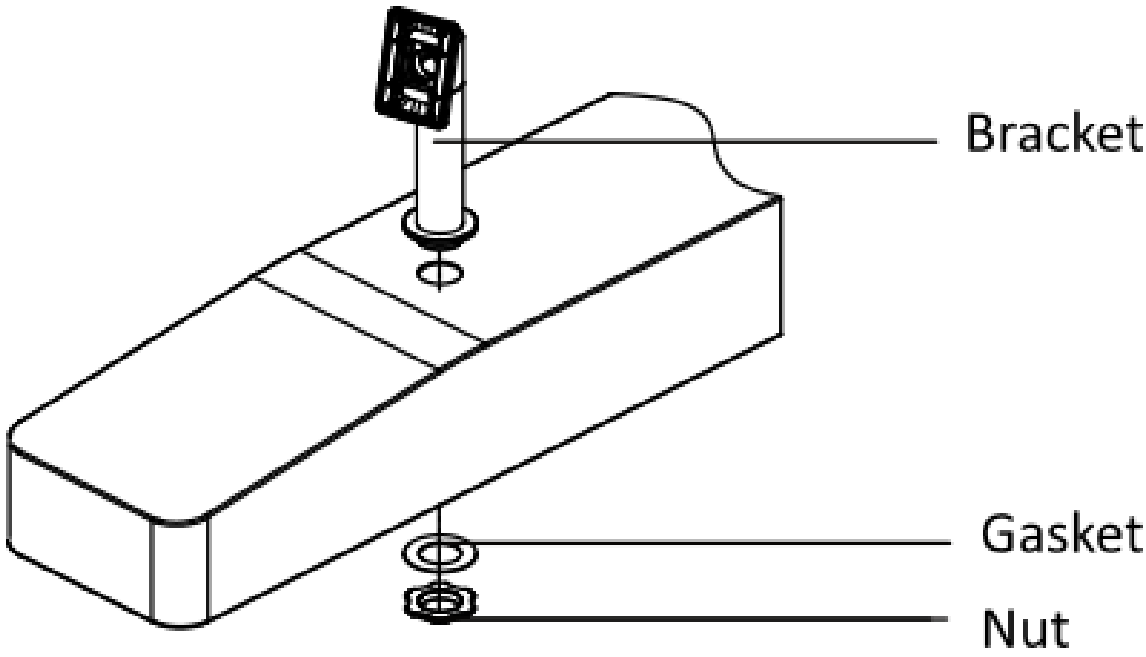


Figure 2-13 Fix Bracket

2. Fix the mounting plate into the bracket by 4 K1M4×8-SUS screws.

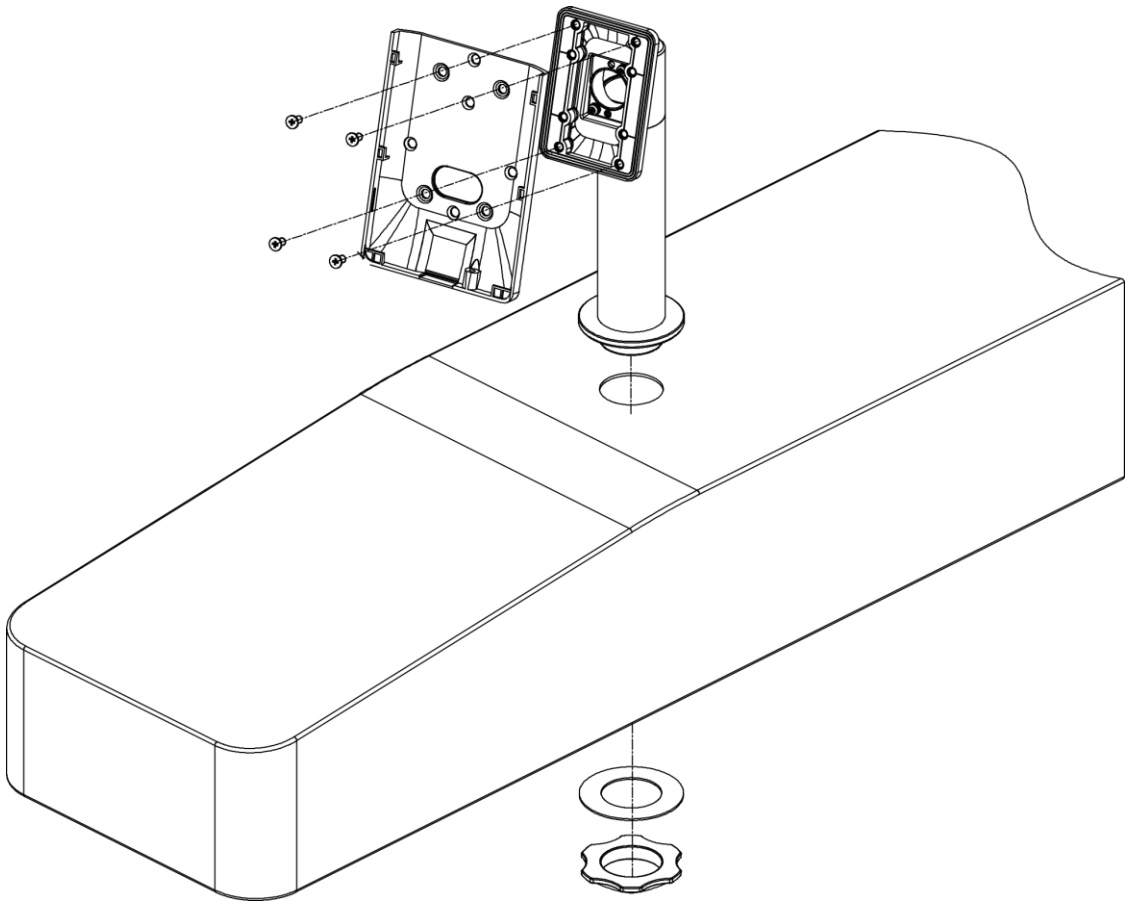


Figure 2-14 Fix Mounting Plate

3. Pass face recognition terminal cables through the cable hole, and insert them into the inner turnstile. Fix the face recognition terminal into the mounting plate with KM3×6-H2-SUS screws.

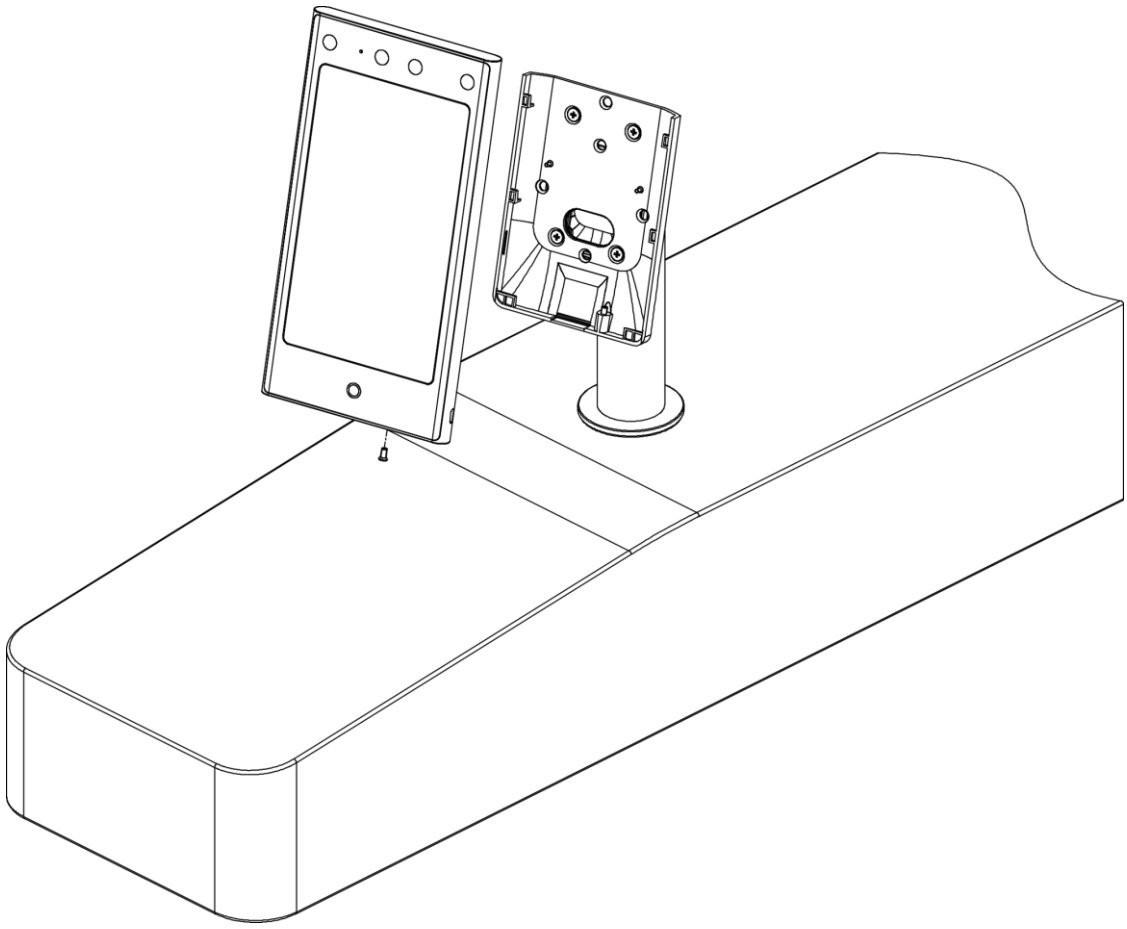


Figure 2-15 Fix Face Recognition Terminal

4. After installation, for the proper use of the device (outdoor use), stick the protection film (parts of models supplied) on the screen.

Chapter 3 Wiring

The device supports connecting to the RS-485 terminal, the door lock, the exit button, the alarm output/input devices, the Wiegand card reader, the access controller, and the power supply. You can wire the peripherals according to the descriptions below.

If connect the Wiegand card reader with the access controller, the face recognition terminal can transmit the authentication information to the access controller and the access controller can judge whether to open the door or not.

Note

- If the cable size is 18 AWG, you should use a 12 V switched-mode power supply. And the distance between the power supply and the device should be no more than 20 m.
- If the cable size is 15 AWG, you should use a 12 V switched-mode power supply. And the distance between the power supply and the device should be no more than 30 m.
- If the cable size is 12 AWG, you should use a 12 V switched-mode power supply. And the distance between the power supply and the device should be no more than 40 m.

3.1 Terminal Description

The terminals contains power input, alarm input, alarm output, RS-485, Wiegand output, and door lock.

The terminal's diagram is as follows:

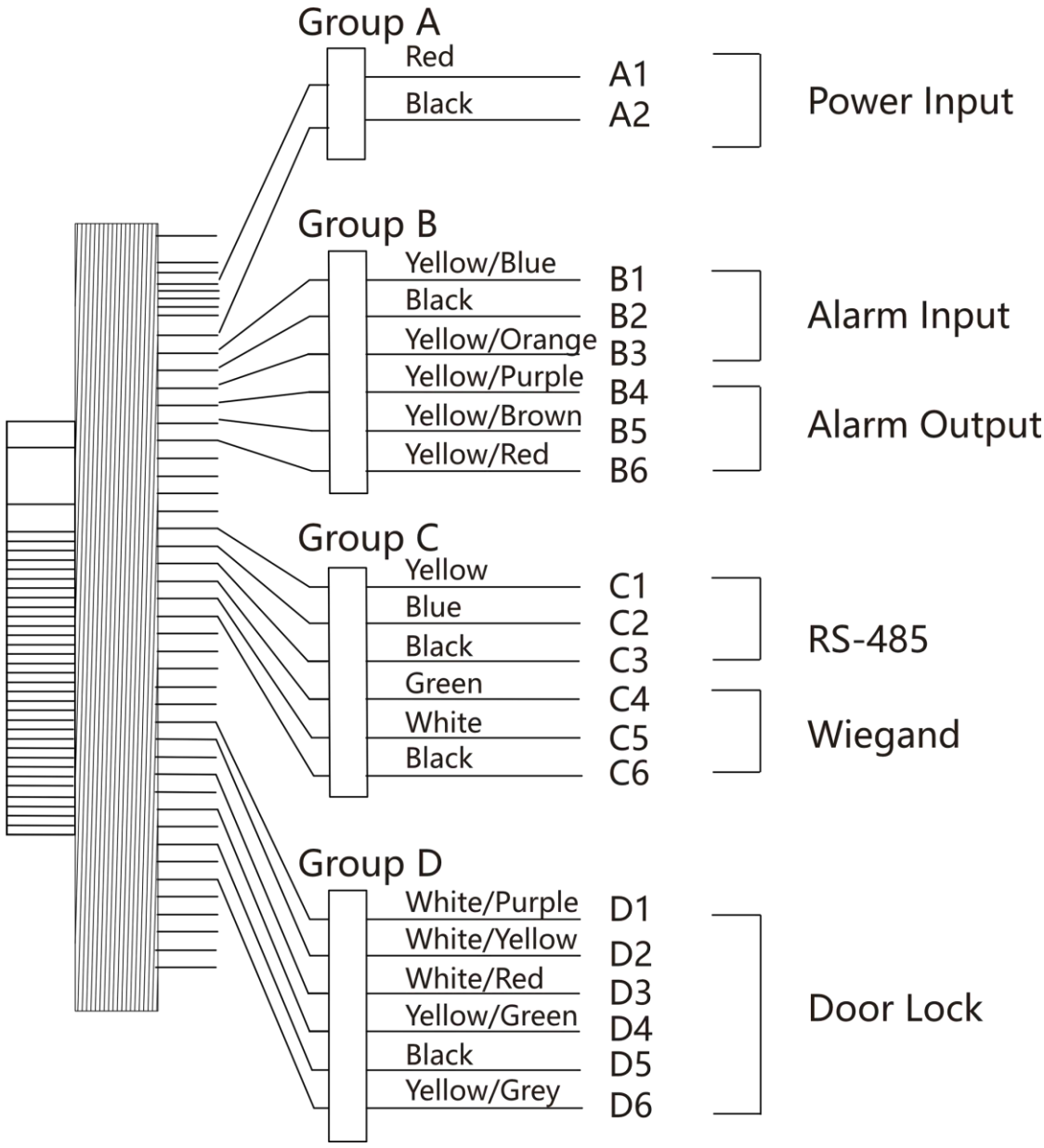


Figure 3-1 Terminal Diagram

The descriptions of the terminals are as follows:

Table 3-1 Terminal Descriptions

Group	No.	Function	Color	Name	Description
Group A	A1	Power Input	Red	+12 V	12 VDC Power Supply
	A2		Black	GND	Ground
Group B	B1	Alarm Input	Yellow/Blue	IN1	Alarm Input 1
	B2		Black	GND	Ground
	B3		Yellow/Orange	IN2	Alarm Input 2
	B4	Alarm Output	Yellow/Purple	NC	Alarm Output Wiring
	B5		Yellow/Brown	COM	
	B6		Yellow/Red	NO	
Group C	C1	RS-485	Yellow	485+	RS-485 Wiring
	C2		Blue	485-	
	C3		Black	GND	Ground
	C4	Wiegand	Green	W0	Wiegand Wiring 0
	C5		White	W1	Wiegand Wiring 1
	C6		Black	GND	Ground
Group D	D1	Door Lock	White/Purple	NC	Lock Wiring (NC)
	D2		White/Yellow	COM	Common
	D3		White/Red	NO	Lock Wiring (NO)
	D4		Yellow/Green	SENSOR	Door Contact
	D5		Black	GND	Ground
	D6		Yellow/Grey	BTN	Exit Door Wiring

3.2 Wire Normal Device

You can connect the terminal with normal peripherals.

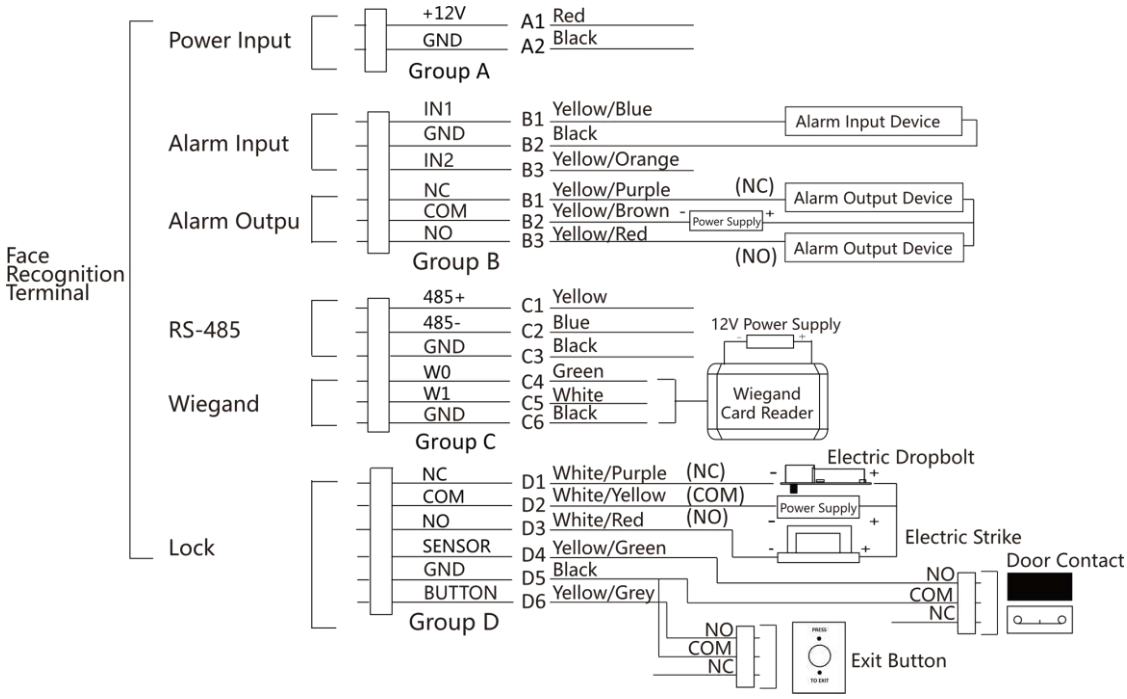


Figure 3-2 Device Wiring

Note

- You should set the face recognition terminal's Wiegand direction as **Input** to connect to a Wiegand card reader. If connects to an access controller, you should set the Wiegand direction as **Output** to transmit authentication information to the access controller.
- For details about Wiegand direction settings, see ***Set Wiegand Parameters*** .
- Do not wire the device to the electric supply directly.

3.3 Wire Secure Door Control Unit

You can connect the terminal with the secure door control unit.

The wiring diagram is as follows.

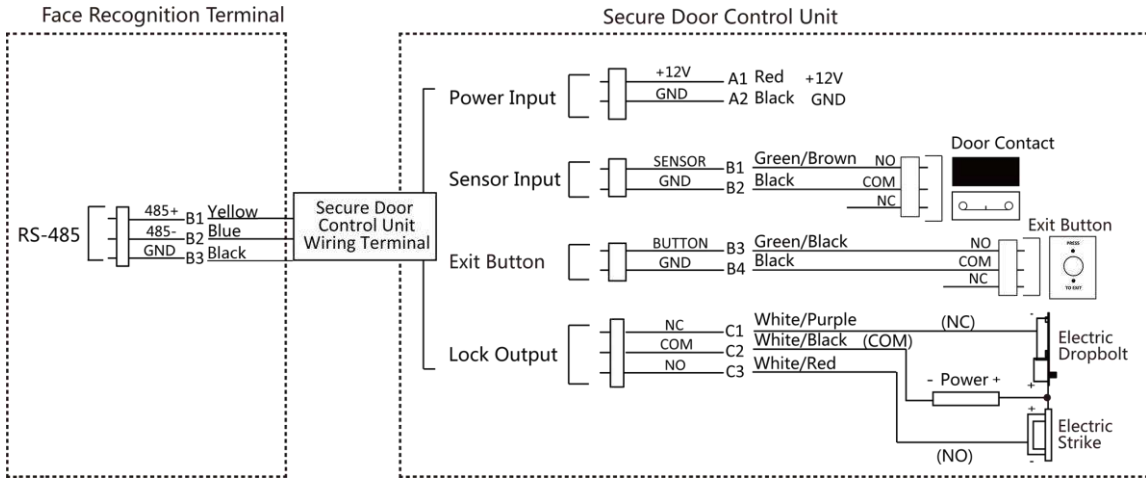


Figure 3-3 Secure Door Control Unit Wiring

Note

The secure door control unit should connect to an external power supply separately. The suggested external power supply is 12V, 0.5A.

3.4 Wire Fire Module

3.4.1 Wiring Diagram of Door Open When Powering Off

Lock Type: Anode Lock, Magnetic Lock, and Electric Bolt (NO)

Security Type: Door Open When Powering Off

Scenario: Installed in Fire Engine Access

Type 1

Note

The fire system controls the power supply of the access control system.

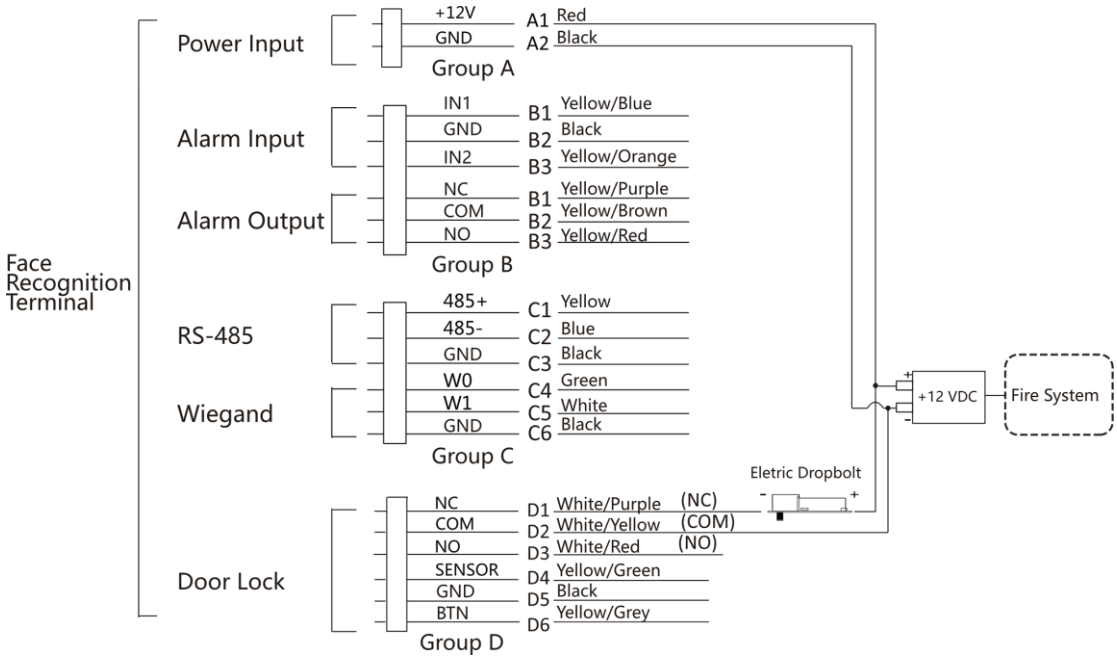


Figure 3-4 Wire Device

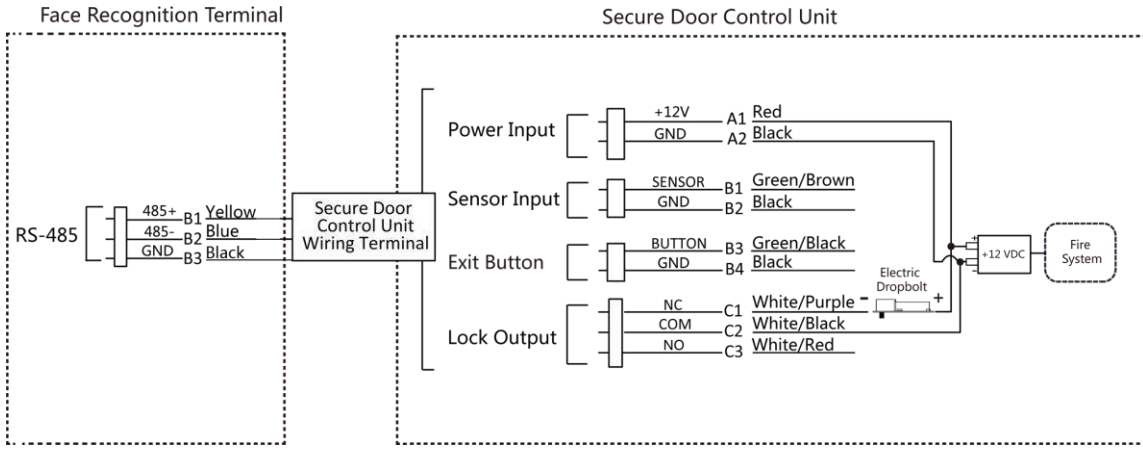


Figure 3-5 Wire Secure Door Control Unit

Type 2

Note

The fire system (NO and COM, normally open when powering off) is connected with the lock and the power supply in series. When an fire alarm is triggered, the door remains open. In normal times, NO and COM are closed.

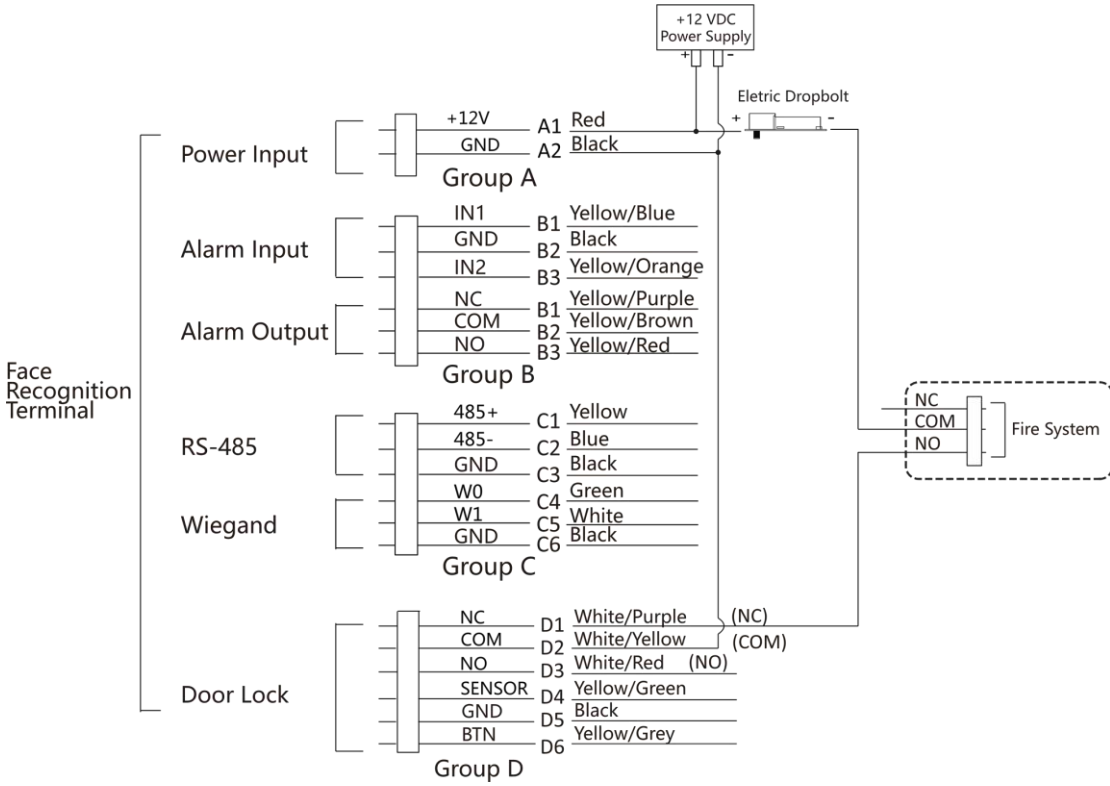


Figure 3-6 Wiring Device

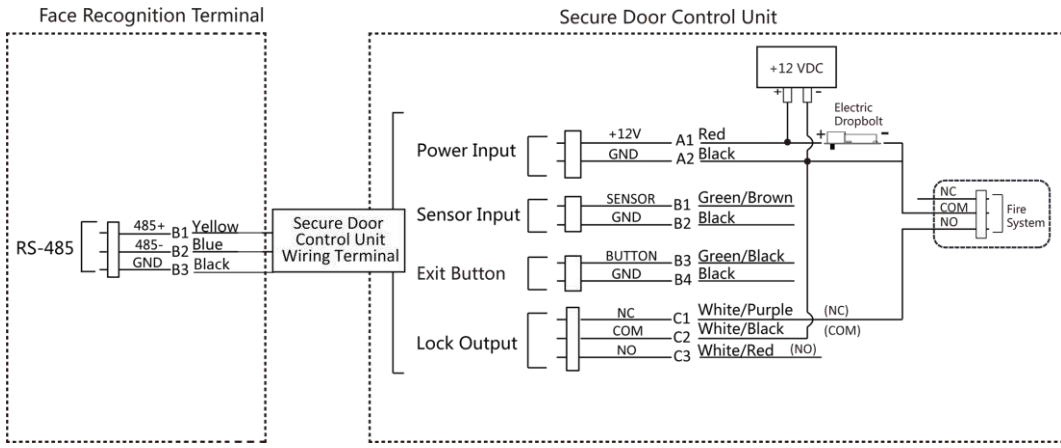


Figure 3-7 Wiring Secure Door Control Unit

3.4.2 Wiring Diagram of Door Locked When Powering Off

Lock Type: Cathode Lock, Electric Lock, and Electric Bolt (NC)

Security Type: Door Locked When Powering Off

Scenario: Installed in Entrance/Exit with Fire Linkage

Note

- The Uninterpretable Power Supply (UPS) is required.
- The fire system (NC and COM, normally closed when powering off) is connected with the lock and the power supply in series. When an fire alarm is triggered, the door remains open. In normal times, NC and COM are open.

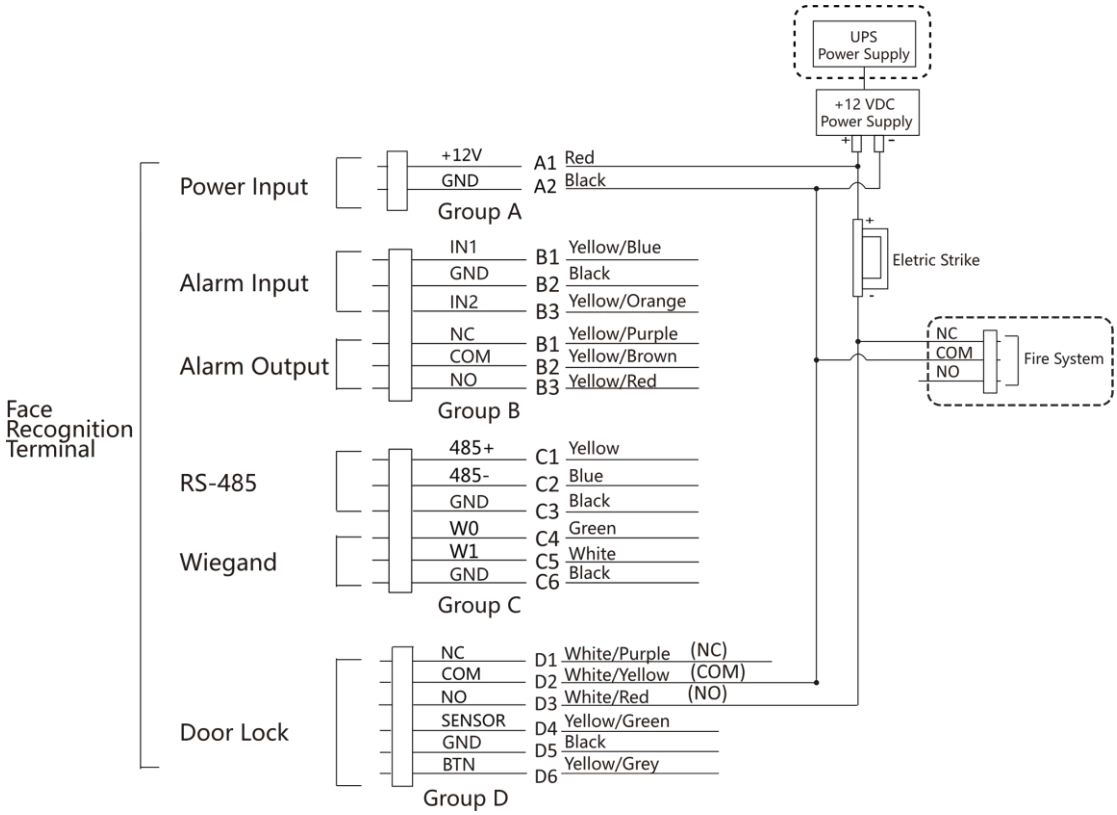


Figure 3-8 Device Wiring

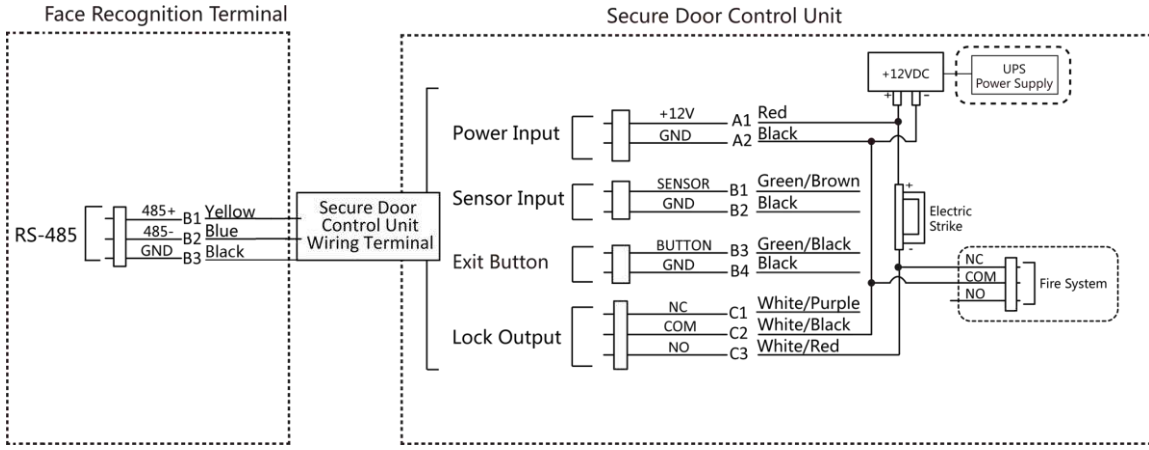


Figure 3-9 Wiring Diagram

Chapter 4 Palm Print and Palm Vein Indicator Description

Indicator	Description
Solid Red	The device is offline.
Fast-flashing Red	The palms are too close.
Slow-flashing Red	Authenticating failed.
The green light is on for 3 s	Authenticating succeed.

Chapter 5 Activation

You should activate the device before the first login. After powering on the device, the system will switch to Device Activation page.

Activation via the device, SADP tool and the client software are supported.

The default values of the device are as follows:

- The default IP address: 192.0.0.64
- The default port No.: 8000
- The default user name: admin

5.1 Activate via Device

If the device is not activated, you can activate the device after it is powered on.

On the Activate Device page, create a password and confirm the password. Tap **Activate** and the device will activated.

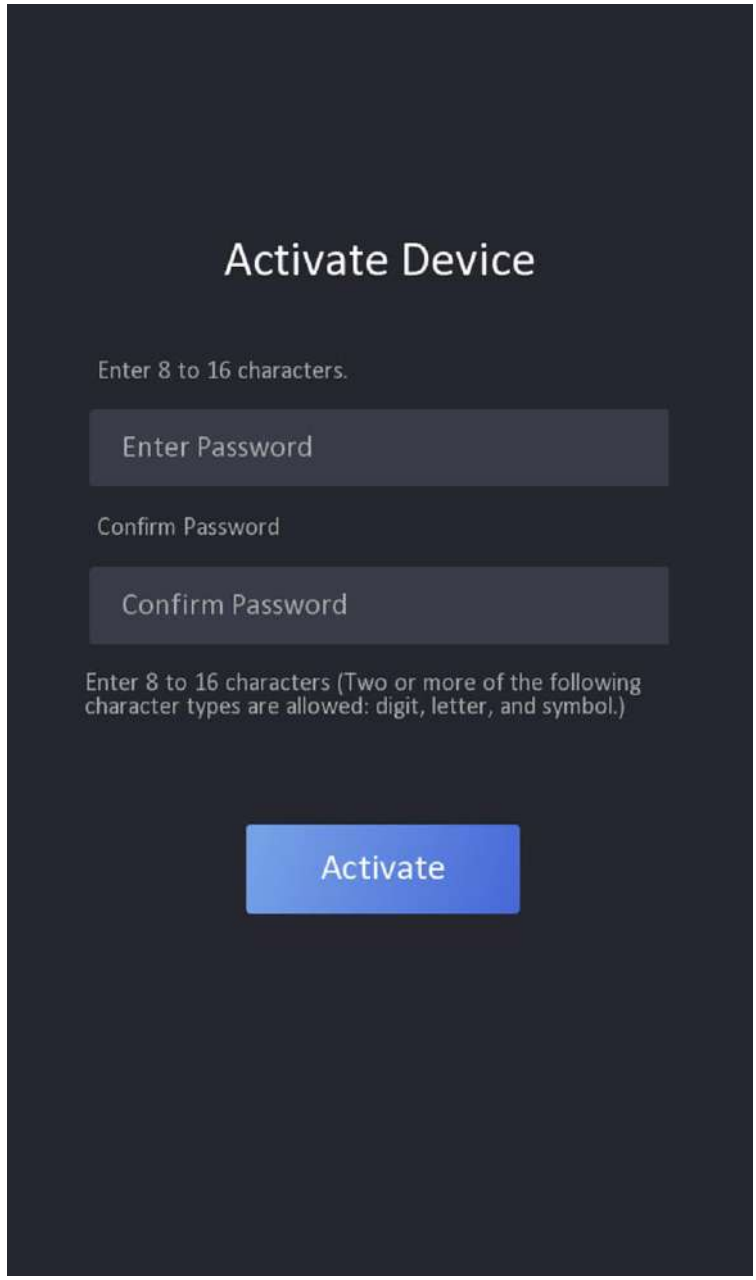


Figure 5-1 Activation Page

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 service provider and/or end-user.
- Do not contain following characters in the password: the user name, 123, admin (case-insensitive), 4 or more continuously increasing or decreasing digits, or 4 or more consecutively repeated characters.
- Password cannot contain words such as hik, hkws, and hikvision (case insensitive).

5.2 Activate via Web Browser

You can activate the device via the web browser.

Steps

1. Enter the device default IP address (192.0.0.64) in the address bar of the web browser, and press **Enter**.

   Note

   Make sure the device IP address and the computer's should be in the same IP segment.

2. Create a new password (admin password) 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 service provider and/or end-user.
   - Do not contain following characters in the password: the user name, 123, admin (case-insensitive), 4 or more continuously increasing or decreasing digits, or 4 or more consecutively repeated characters.
   - Password cannot contain words such as hik, hkws, and hikvision (case insensitive).

3. Click **Activate**.
4. Edit the device IP address. You can edit the IP address via the SADP tool, the device, and the client software.

5.3 Activate via SADP

SADP is a tool to detect, activate and modify the IP address of the device over the LAN.

Before You Start

- Get the SADP software from the supplied disk or the official website ***http://www.hikvision.com/en/*** , and install the SADP according to the prompts.
- The device and the PC that runs the SADP tool should be within the same subnet.

The following steps show how to activate a device and modify its IP address. For batch activation and IP addresses modification, refer to *User Manual of SADP* for details.

Steps

1. Run the SADP software and search the online devices.
2. Find and select your device in online device list.
3. Input new password (admin password) and confirm the password.

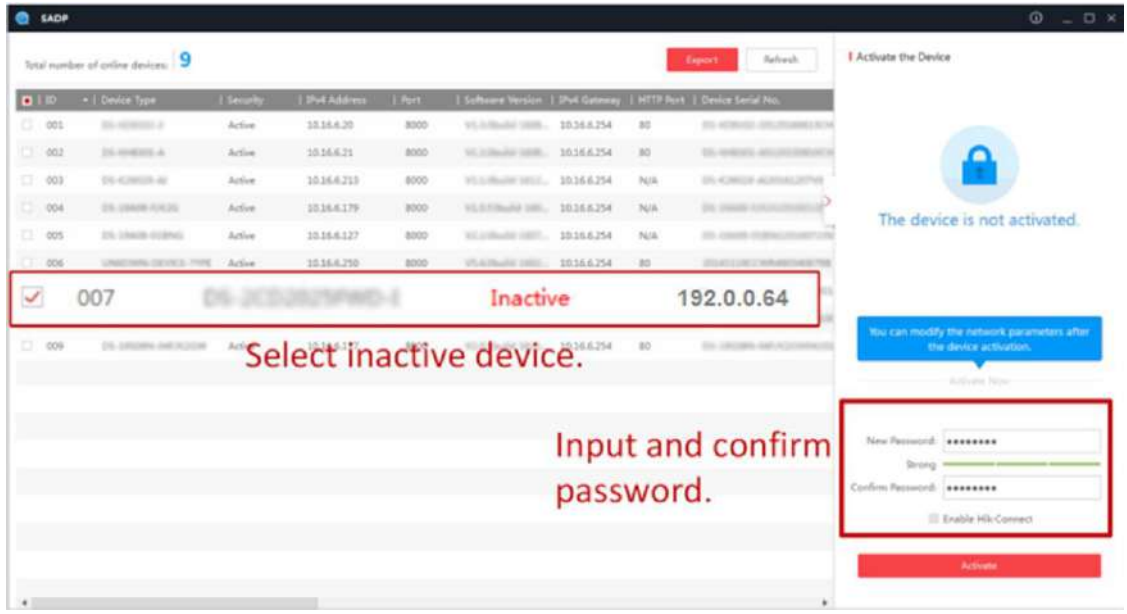
Caution

STRONG PASSWORD RECOMMENDED-We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Note

Characters containing admin and nimda are not supported to be set as activation password.

4. Click **Activate** to start activation.



Status of the device becomes **Active** after successful activation.

5. Modify IP address of the device.
   1) Select the device.
   2) Change the device IP address to the same subnet as your computer by either modifying the IP address manually or checking **Enable DHCP**.
   3) Input the admin password and click **Modify** to activate your IP address modification.

5.4 Activate Device via iVMS-4200 Client Software

For some devices, you are required to create the password to activate them before they can be added to the iVMS-4200 software and work properly.

Steps

Note

This function should be supported by the device.

1. Enter the Device Management page.
2. Click on the right of **Device Management** and select **Device**.
3. Click **Online Device** to show the online device area.

   The searched online devices are displayed in the list.
4. Check the device status (shown on **Security Level** column) and select an inactive device.
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

Characters containing admin and nimda are not supported to be set as activation password.

7. Click **OK** to activate the device.

Chapter 6 Quick Operation

6.1 Select Language

You can select a language for the device system.

After the device activation, you can select a language for the device system.

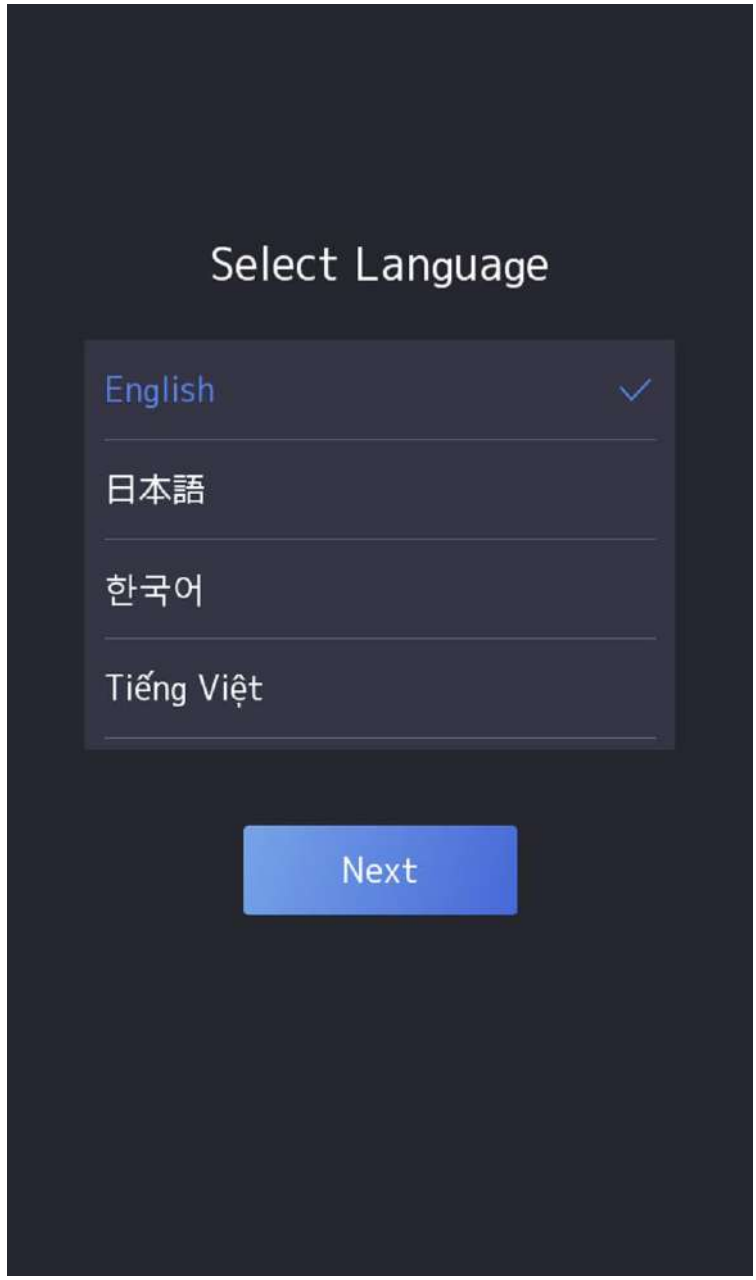


Figure 6-1 Select System Language

By default, the system language is English.

Note

After you change the system language, the device will reboot automatically.

6.2 Set Password Change Type

You can set the password change type as reserved email address or security questions. Once you forgot the device password, you can change the password via the selected change type.

Change Password via Email Address

If you need to change password via reserved email, you can enter an email address, and tap **Next**.

Change via Security Questions

If you need to change password via security questions, you can tap **Change to Security Questions** on the right corner. Select the security questions and enter the answers. Tap **Next**.

Note

You can only select one type to change password. If you need, you can enter the web page to set both of the changing types.

6.3 Set Network Parameters

You can set the network for the device.

Steps

Note

Parts of the device models supports wi-fi function. Refers to the actual device for details.

1. When you enter the Select Network page, tap **Wired Network** or **Wi-Fi** for your actual needs.

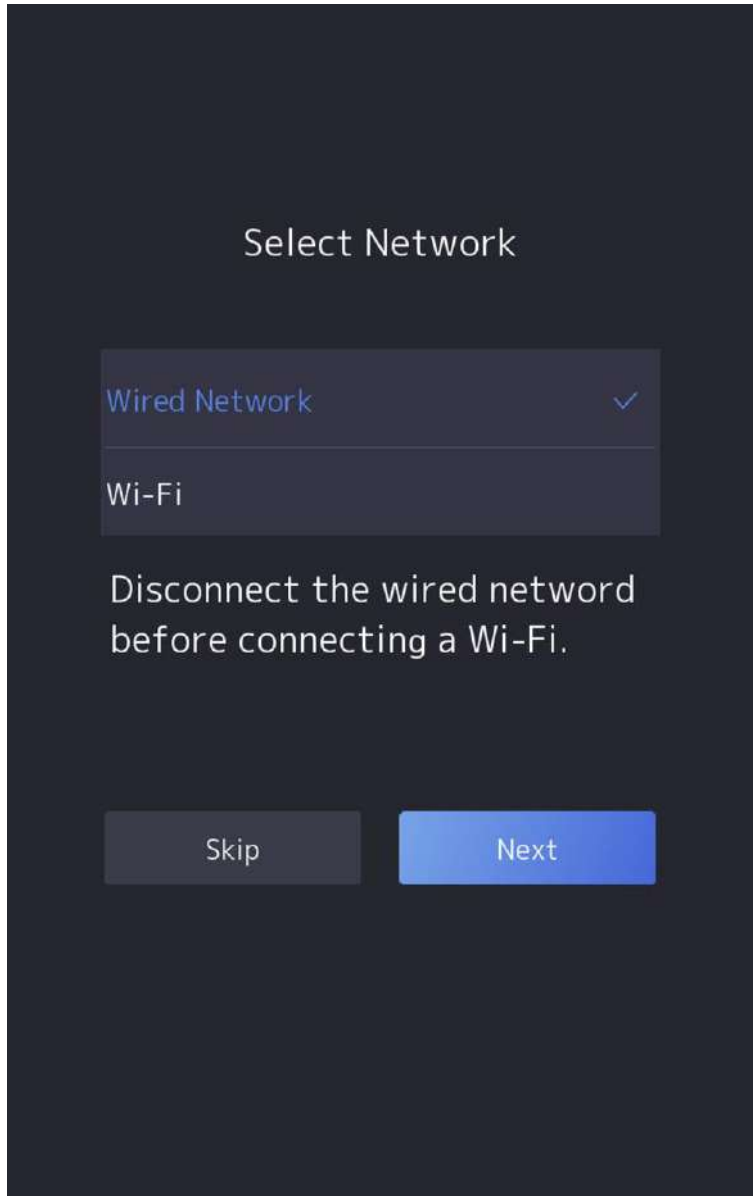


Figure 6-2 Select Network

Note

Disconnect the wired network before connecting a Wi-Fi.

2. Tap **Next**.

Wired Network

Note

Make sure the device has connected to a network.

If enable **DHCP**, the system will assign the IP address and other parameters automatically.

If disable **DHCP**, you should set the IP address, the subnet mask, and the gateway.

Wi-Fi

Select a Wi-Fi and enter the Wi-Fi's password to get connected.

Or tap **Add Wi-Fi** and enter the Wi-Fi's name and the password to get connected.

3. Optional: Tap **Skip** to skip network settings.

6.4 Access to Platform

Enable the function and the device can communicate via Hik-Connect. You can add the device to Hik-Connect mobile client and so on.

Steps

1. Enable **Access to Hik-Connect**, and set the server IP and verification code.

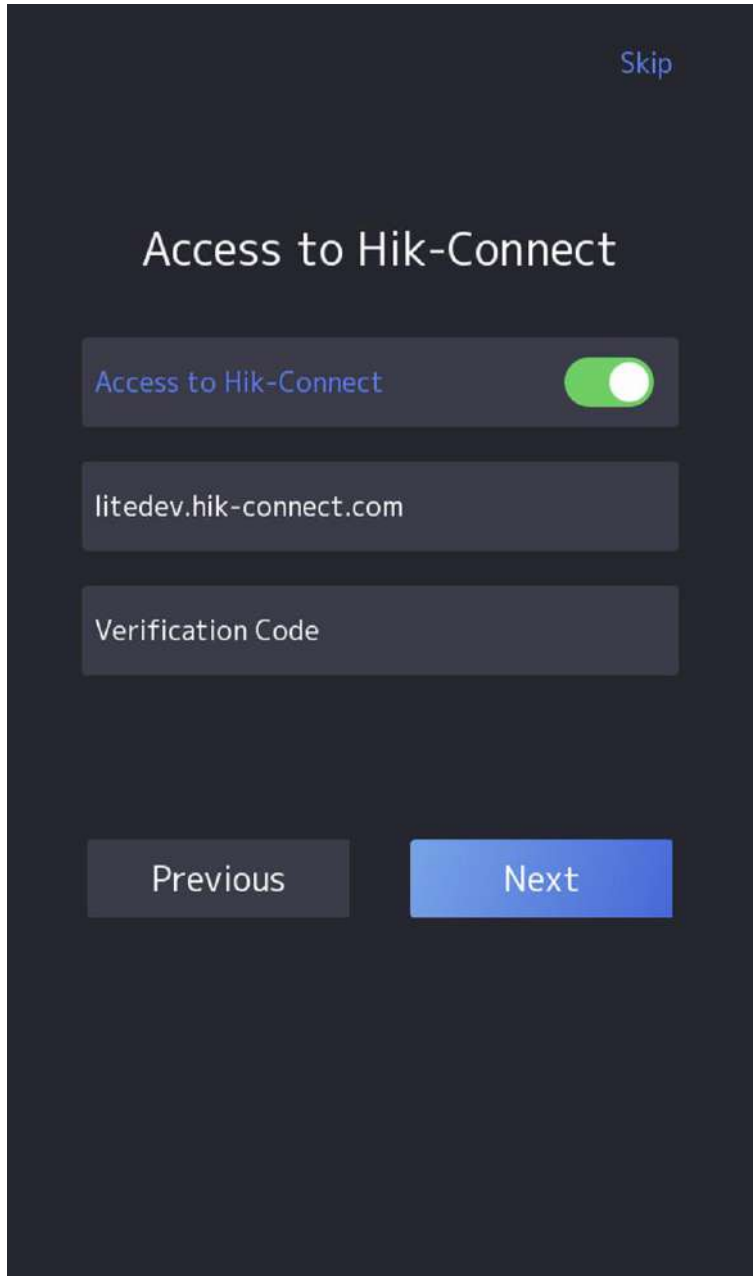


Figure 6-3 Access to Hik-Connect

2. Tap **Next**.
3. Optional: Tap **Skip** to skip the step.
4. Optional: Tap **Previous** to go to the previous page.

Note

If you tap **Previous** to return to the Wi-Fi configuration page, you need to tap the connected Wi-Fi or connect another Wi-Fi to enter the platform page again.

6.5 Privacy Settings

After activation, selecting application mode, and selecting network, you should set the privacy parameters, including the picture uploading and storage.

Select parameters according to your actual needs.

Upload Captured Pic. When Auth. (Upload Captured Picture When Authenticating)

Upload the pictures captured when authenticating to the platform automatically.

Save Captured Pic. When Auth. (Save Captured Picture When Authenticating)

If you enable this function, you can save the picture when Authenticating to the device.

Save Registered Pic. (Save Registered Picture)

The registered face picture will be saved to the system if you enable the function.

Upload Pic. After Linked Capture (Upload Picture After Linked Capture)

Upload the pictures captured by linked camera to the platform automatically.

Save Pic. After Linked Capture (Save Pictures After Linked Capture)

If you enable this function, you can save the picture captured by linked camera to the device.

Tap **Next** to complete the settings.

6.6 Set Administrator

After device activation, you can add an administrator to manage the device parameters.

Before You Start

Activate the device and select an application mode.

Steps

1. **Optional:** Tap **Skip** to skip adding administrator if required.
2. Enter the administrator's name (optional) and tap **Next**.

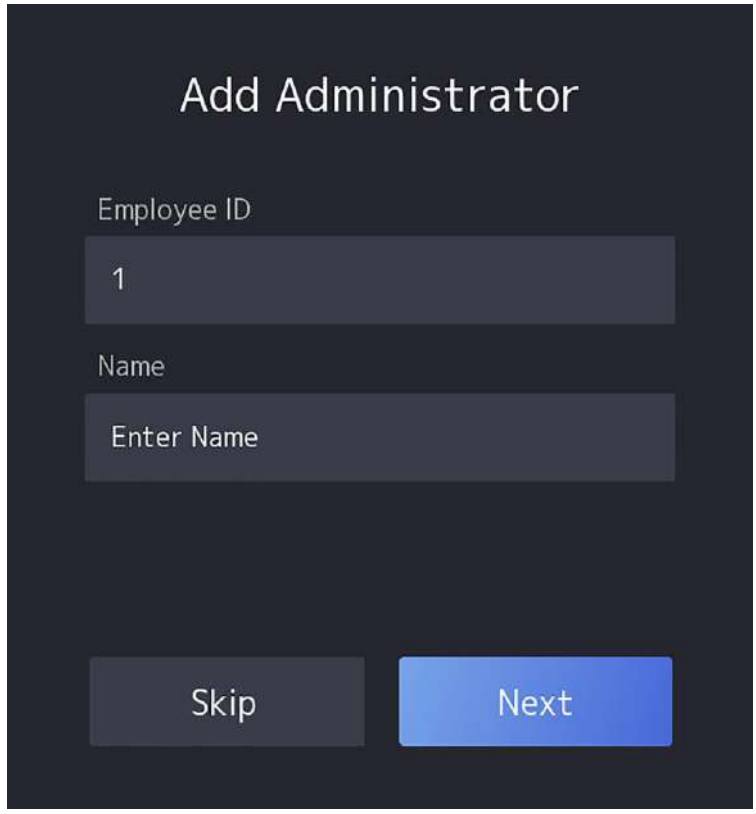


Figure 6-4 Add Administrator Page

3. Select a credential to add.

Note

Up to one credential should be added.

- : Face forward at the camera. Make sure the face is in the face recognition area. Click to capture and click to confirm.
- : Press your finger according to the instructions on the device screen. Click to confirm.
- : Enter the card No. or present card on the card presenting area. Click **OK**.

Note

Only devices connected to the external fingerprint module support fingerprint function.

4. Click **OK**.

You will enter the authentication page.

6.7 Authentication Page Instructions

Introduce the authentication page.

Status Bar Instructions

/

Device is armed/not armed.

/ /

The device' Wi-Fi is enabled and signal is strong/Wi-Fi is enabled but not connected/Wi-Fi's IP address is conflict.

/ /

The device wired network is connected/not connected/connecting failed.

/ / / / /

The device's mobile network has no signal/2G strong signal/3G strong signal/4G strong signal/5G strong signal.

/

The device is added to VoIP/not added to VoIP.

/ /

The device's SIP server is registered/registering failed/registered on door station but not on main station.

/

The palm print and palm vein module is online or offline.

The dual-frequency card module is online.

Authentication Page Icon

Note

The displayed icon on the authentication page can be controlled. For details, see shortcut key settings in ***Set Shortcut Key via Device*** .

Show QR code to the camera and you can authenticate via the QR code.

- Enter the room No., and tap **OK** to call.
- Tap to call the center.

Note

The device should be added to the center, or the calling operation will be failed.

Enter PIN to authenticate.

Chapter 7 Basic Operation

7.1 Login

Login the device to set the device basic parameters.

7.1.1 Login by Administrator

If you have added an administrator for the device, only the administrator can login the device for device operation.

Steps

1. Long tap on the initial page for 3 s and slide to the left/right by following the gesture to enter the admin login page.

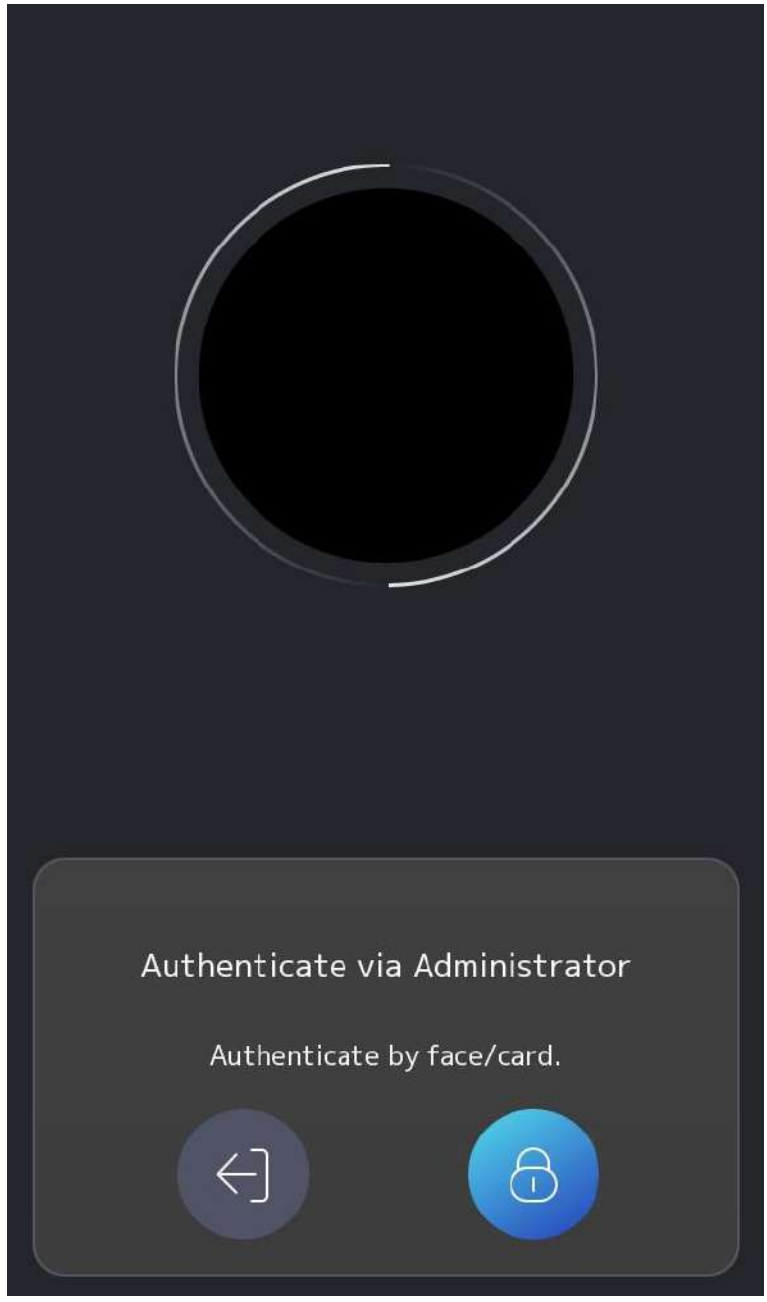


Figure 7-1 Admin Login

2. Authenticate the administrator's face, fingerprint, or card to enter the home page.

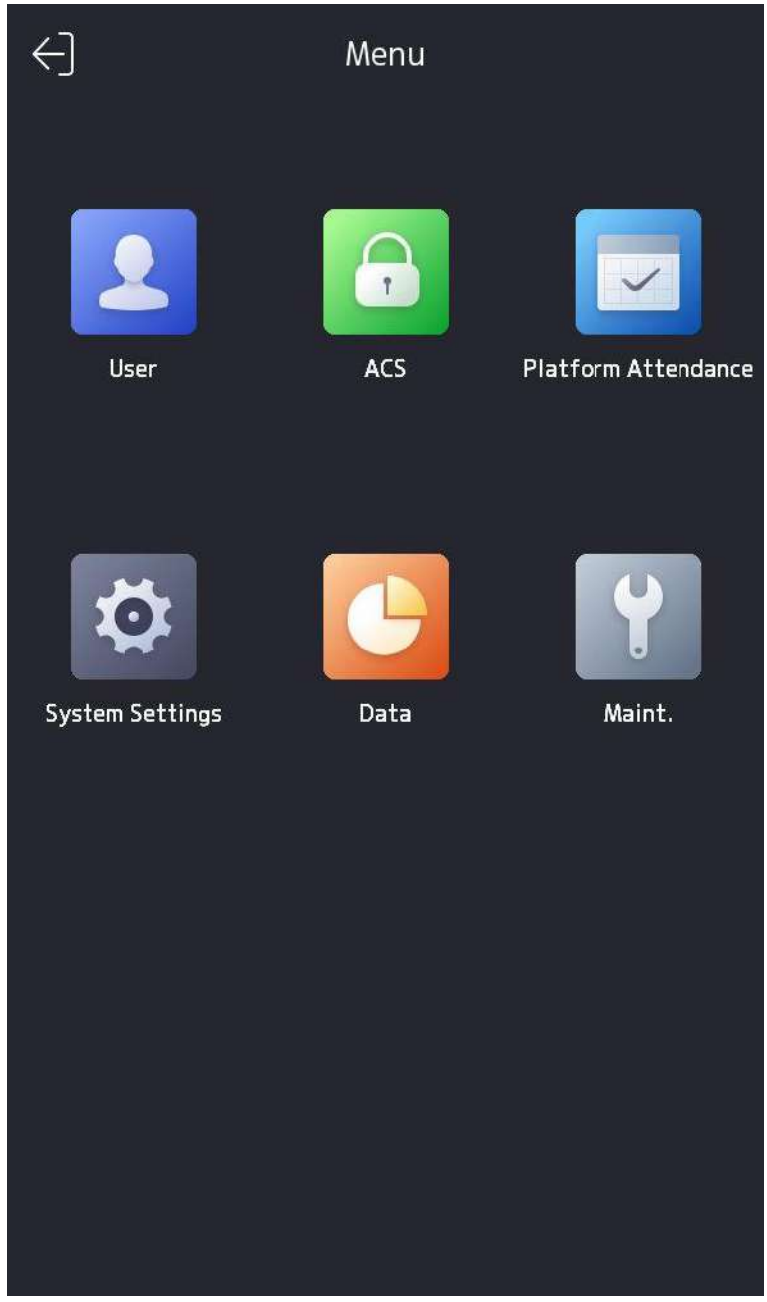


Figure 7-2 Home Page

Note

The device will be locked for 30 minutes after 5 failed fingerprint or card attempts.

3. **Optional:** Tap and you can enter the device activation password for login.
4. **Optional:** Tap and you can exit the admin login page.

7.1.2 Login by Activation Password

You should login the system before other device operations. If you do not configure an administrator, you should follow the instructions below to login.

Steps

1. Long tap on the initial page for 3 s and slide to the left/right by following the gesture to enter password entering page.
2. Enter the password.
   - If you have added an administrator for the device, tap  and enter the password.
   - If you haven't added an administrator for the device, enter the password.
3. Tap **OK** to enter the home page.

Note

The device will be locked for 30 minutes after 5 failed password attempts.

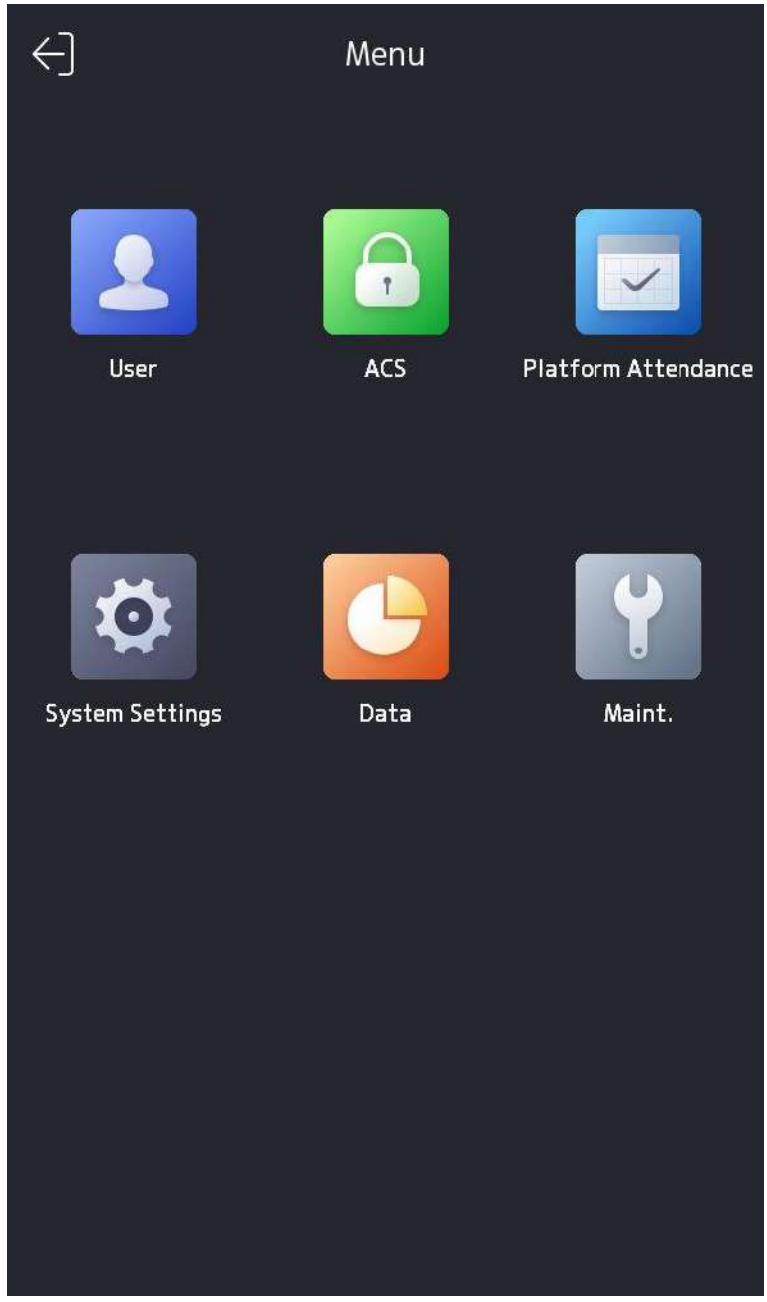


Figure 7-3 Home Page

7.1.3 Forgot Password

If you forget the password during authentication, you can change the password.

Steps

1. Hold the initial page for 3 s and slide to the left/right by following the gesture and log in the page.
2. **Optional:** If you have set an administrator, tap in the pop-up admin authentication page.
3. Tap **Forgot Password**.
4. Select a password change type from the list.

   Note

   If you have only set 1 password change type, you will go to the corresponded password change page for further settings.
5. Answer the security questions or change the password according to email address.
   - Security Questions: Answer the security questions that configured when activation.
   - Email Address

     Note

     Make sure the device has added to the Hik-Connect account.

     a. Download Hik-Connect app.
     b. Go to **More → Reset Device Password** .
     c. Scan the QR code on the device and a verification code will be popped up.

        Note

        Tap the QR code to get a larger picture.

     d. Enter the verification code on the device page.
6. Create a new password and confirm it.
7. Tap **OK**.

7.1.4 Change Device Password

You can change the device password by entering the old password.

Steps

1. Long tap on the initial page for 3 s and login the home page. Tap **System → Password** .
2. Tap **Change Device Password**.
3. Enter the device old password.

   Note

   If you forget your password, you can tap **Forgot Password** and change the password. For details, see ***Forgot Password*** .
4. Enter new password 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.

5. Tap **OK**.

7.2 Communication Settings

You can set the wired network, the Wi-Fi parameter, the RS-485 parameters, the Wiegand parameters, ISUP and access to Hik-Connect on the communication settings page.

7.2.1 Set Wired Network Parameters

You can set the device wired network parameters, including the IPv4/IPv6 IP address, the subnet mask, the gateway, and DNS parameters.

Steps

1. Tap **System → Comm.** (Communication Settings) on the Home page to enter the Communication Settings page.
2. On the Communication Settings page, tap **Wired Network**.

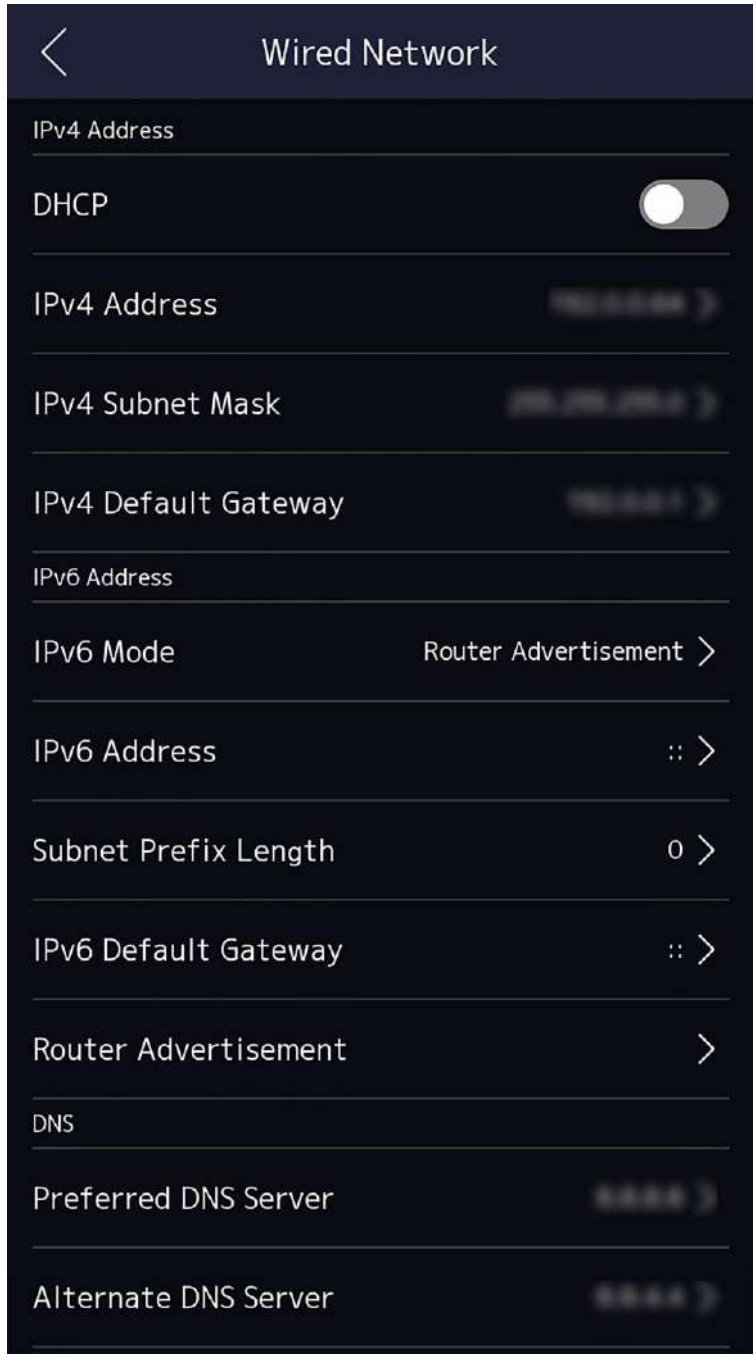


Figure 7-4 Wired Network Settings

3. Set IPv4/IPv6 IP Address, Subnet Mask, and Gateway.

- Enable **DHCP**, and the system will assign IP address, subnet mask, and gateway automatically.
- Disable **DHCP**, and you should set the IP address, subnet mask, and gateway manually.

Note

The device's IP address and the computer IP address should be in the same IP segment.

4. Set the DNS parameters. You can enable **Auto Obtain DNS**, set the preferred DNS server and the alternate DNS server.

7.2.2 Set Wi-Fi Parameters

You can enable the Wi-Fi function and set the Wi-Fi related parameters.

Steps

Note

The function should be supported by the device.

1. Tap **System → Comm.** (Communication Settings) on the Home page to enter the Communication Settings page.
2. On the Communication Settings page, tap.

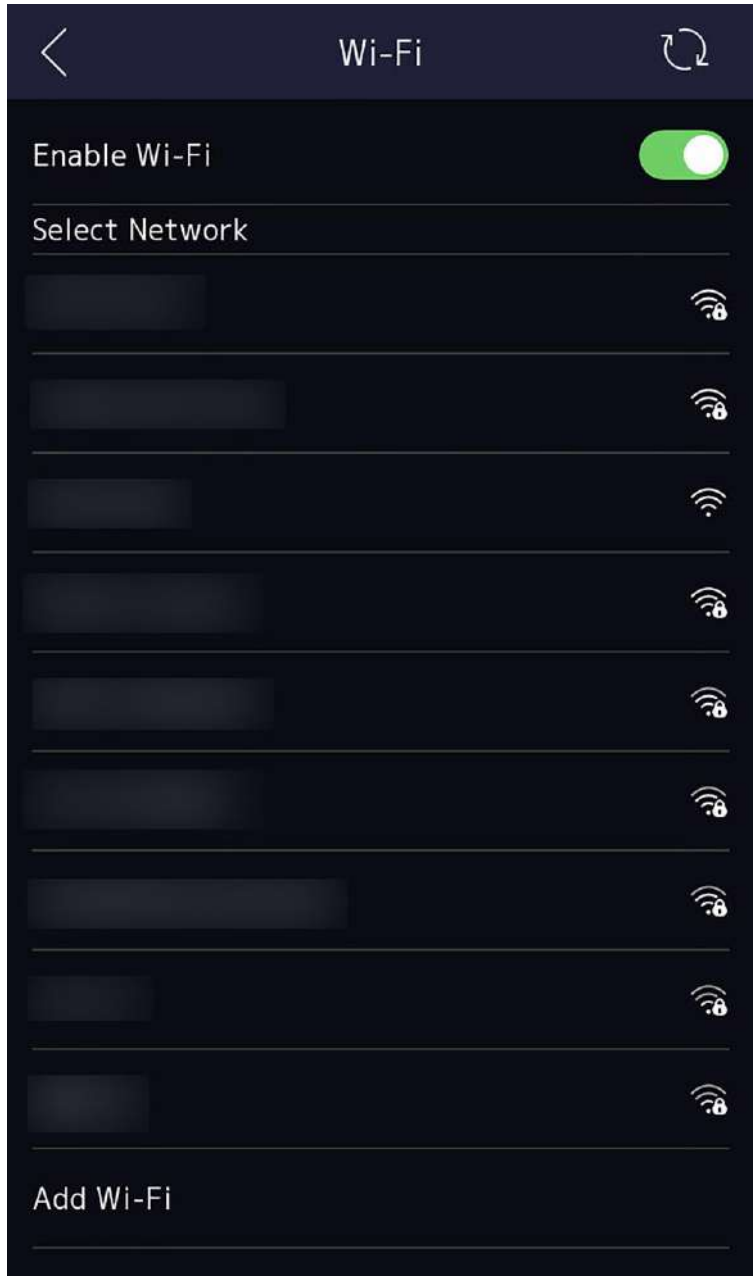


Figure 7-5 Wi-Fi Settings

3. Enable the Wi-Fi function.

4. Configure the Wi-Fi parameters.

- Select a Wi-Fi from the list, and enter the Wi-Fi's password. Tap **OK**.
- If the target Wi-Fi is not in the list,tap **Add Wi-Fi**. Enter the Wi-Fi's name and password. And tap **OK**.

Note

Only digits, letters, and special characters are allowed in the password.

5. Set the Wi-Fi's parameters.
   - By default, DHCP is enable. The system will allocate the IP address, the subnet mask, and the gateway automatically.
   - If disable DHCP, you should enter the IP address, the subnet mask, and the gateway manually.
6. Tap **OK** to save the settings and go back to the Wi-Fi tab.
7. Tap ✓ to save the network parameters.

7.2.3 Set RS-485 Parameters

The face recognition terminal can connect external access controller, secure door control unit, card reader, or QR code scanner via the RS-485 terminal.

Steps

1. Tap **System → Comm.** (Communication Settings) on the Home page to enter the Communication Settings page.
2. On the Communication Settings page, tap **RS-485** to enter the RS-485 tab.

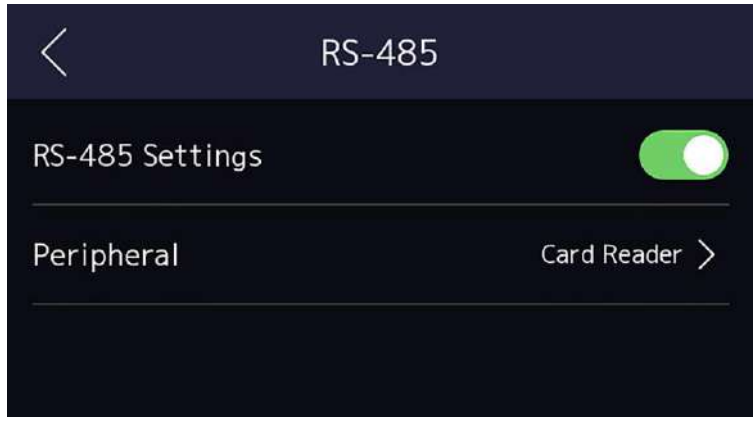


Figure 7-6 Set RS-485 Parameters

3. Select an peripheral type according to your actual needs.

Note

If you select **Access Controller**: If connect the device to a terminal via the RS-485 interface, set the RS-485 address as 2. If you connect the device to a controller, set the RS-485 address according to the door No.

4. Tap the back icon at the upper left corner and you should reboot the device if you change the parameters.

7.2.4 Set Wiegand Parameters

You can set the Wiegand transmission direction.

Steps

1. Tap **System → Comm.** (Communication Settings) on the Home page to enter the Communication Settings page.
2. On the Communication Settings page, tap **Wiegand** to enter the Wiegand tab.
3. Enable the Wiegand function.
4. Select a transmission direction.
   - Output: A face recognition terminal can connect an external access controller. And the two devices will transmit the card No. via Wiegand 34.
   - Input: A face recognition terminal can connect a Wiegand card reader.
5. Tap ✓ to save the network parameters.

Note

If you change the external device, and after you save the device parameters, the device will reboot automatically.

7.2.5 Set ISUP Parameters

Set ISUP parameters and the device can upload data via ISUP protocol.

Before You Start

Make sure your device has connect to a network.

Steps

1. Tap **System → Comm. → ISUP** (Communication Settings) on the Home page to enter the settings page.

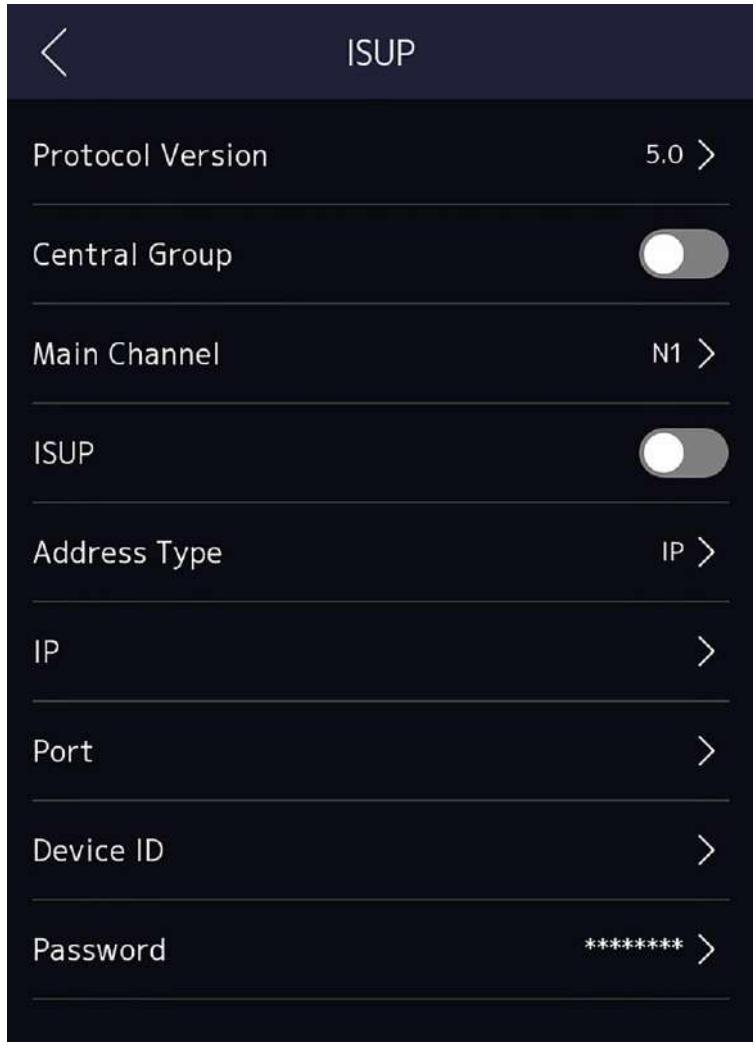


Figure 7-7 ISUP Settings

2. Enable the ISUP function and set the ISUP server parameters.

ISUP Version

Set the ISUP version according to your actual needs.

Central Group

Enable central group and the data will be uploaded to the center group.

Main Channel

Support N1 or None.

ISUP

Enable ISUP function and the data will be uploaded via ISUP protocol.

Address Type

Select an address type according to your actual needs.

IP Address

Set the ISUP server's IP address.

Port No.

Set the ISUP server's port No.

Note

Port No. Range: 0 to 65535.

Device ID

Set device serial no.

Password

If you choose V5.0, you should create an account and ISUP key. If you choose other version, you should create an ISUP account only.

Note

- Remember the ISUP account and ISUP key. You should enter the account name or the key when the device should communicate with other platforms via ISUP protocol.
- ISUP key range: 8 to 32 characters.

7.2.6 Platform Access

You can change the device verification code and set the server address before you add the device to the Hik-Connect mobile client.

Before You Start

Make sure your device has connected to a network.

Steps

1. Tap **System → Comm.** (Communication Settings) on the Home page to enter the Communication Settings page.
2. On the Communication Settings page, tap **Access to Hik-Connect**.
3. Enable **Access to Hik-Connect**
4. Enter **Server IP**.
5. Create the **Verification Code**, and you need to enter the verification code when you manage the devices via **Hik-Connect**.

7.3 Person Management

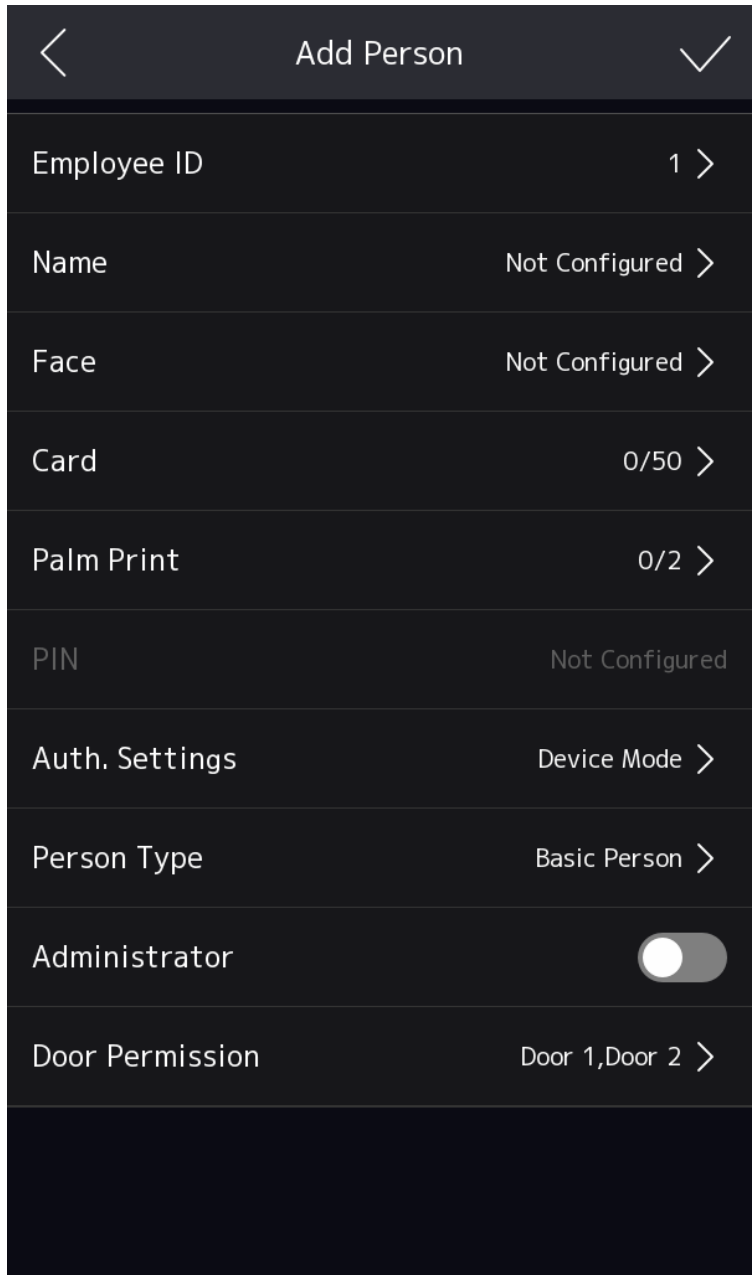
On the person management interface, you can add, edit, delete and search the person.

7.3.1 Add Administrator

The administrator can log in the device backend and configure the device parameters.

Steps

1. Long tap on the initial page for 3 s and slide to the left/right by following the gesture and enter the device backend.
2. Tap **Person → +** to enter the Add Person page.



3. Edit the employee ID.

Note

- The employee ID should be less than 32 characters. And it can be a combination of lower letters, upper letters, and numbers.
- The employee ID should not be duplicated.

4. Tap the Name field and input the person name on the soft keyboard.

Note

- Numbers, upper case letters, lower case letters, and special characters are allowed in the person name.
- Up to 32 characters are allowed in the person name.

5. Optional: Add a face picture, fingerprints, cards, PIN, palm print, keyfob for the administrator.

Note

- For details about adding a face picture, see ***Add Face Picture*** .
- For details about adding a fingerprint, see ***Add Fingerprint*** .
- For details about adding a card, see ***Add Card*** .
- For details about adding a password, see ***View PIN code*** .
- For details about adding a keyfob, see ***Add Keyfob*** .
- For details about adding a palm print, see .

6. Optional: Set the administrator's authentication type.

Note

For details about setting the authentication type, see ***Set Authentication Mode*** .

7. Enable the Administrator Permission function.

Enable Administrator Permission

The person is the administrator. Except for the normal attendance function, the person can also enter the Home page to operate after authenticating the permission.

8. Set **Door Permission**.

9. Tap ✓ to save the settings.

7.3.2 Import and Export Face and Person Data in Batch via Device

You can use the import and export function to import the data from device A to device B by USB flash drive.

Before You Start

- Login Device A (The device that you need to export data). For details, see ***Login*** .
- Insert an USB flash drive to Device A.

Note

- The supported USB flash drive format is FAT32 or exFAT.
- The system supports the USB flash drive with the storage of 1 G to 256 G. Make sure the free space of the USB flash drive is more than 512 M.

Steps

1. On Device A menu, tap **Data** and enter the **Data** page.

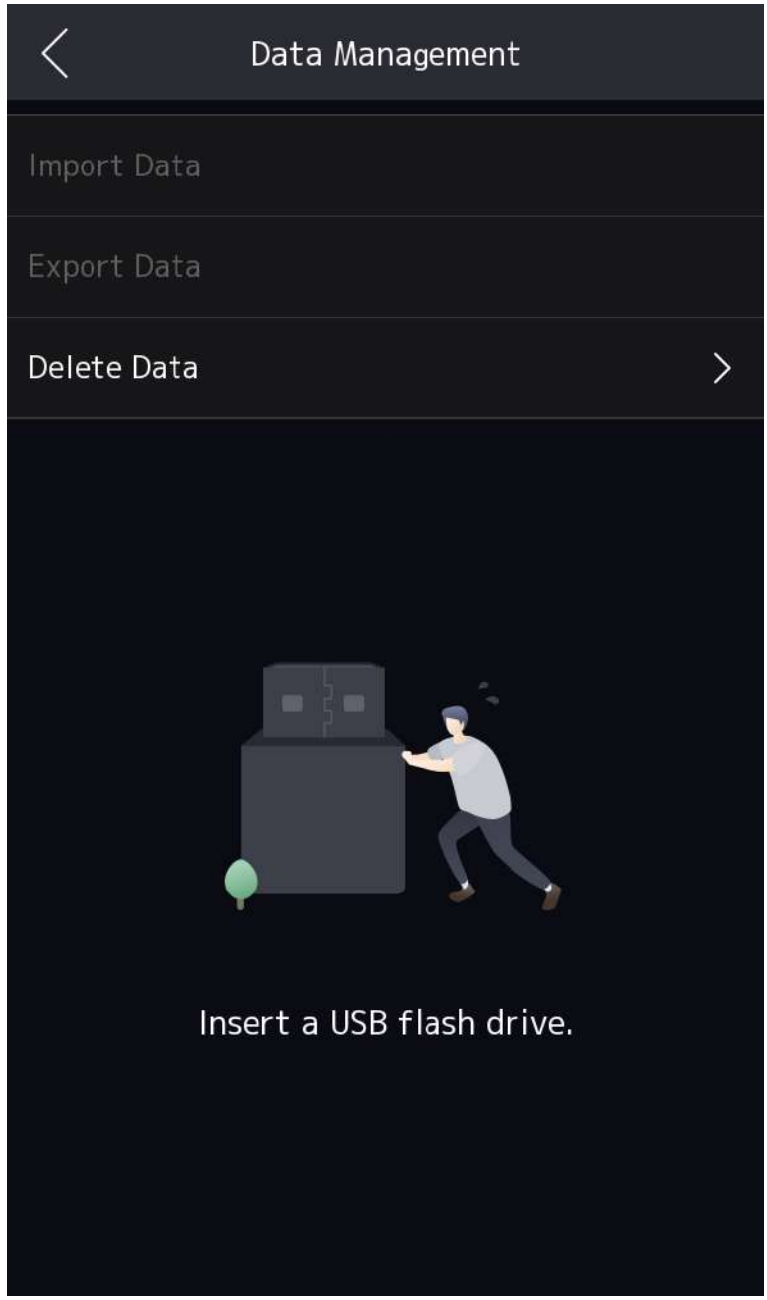


Figure 7-8 Data Management Page

2. Tap **Export Data** in the Data Management page.
3. Select **Person Data** or **Face Data**.
4. **Optional:** Create a password for exporting. When you import those data to another device, you should enter the password.

Note

- The password cannot be empty. If you do not set a password, you can view the exported data in your PC.
- If you set a password, you cannot view the exported data in your PC.
- The exported person data is a DB file, which cannot be edited.

5. Insert the USB flash drive to Device B that need to import face and person data.

Note

Make sure the two device are of the same device type.

6. On Device B menu, tap **Data**and enter the **Data** page.
7. Tap **Import Data**.
8. Select **Person Data** or **Face Data**.
9. Enter the created password when you exported the data. If you do not create a password when you exported the data, leave a blank in the input box and tap **OK**. The data will be imported from USB flash drive.

Note

- If you need to import pictures manually, you should save the pictures in the root directory (enroll_pic) of the USB flash drive. The picture's name should be follow the rule below: Card No._Name_Department_Employee ID_Gender.jpg For gender, 3 refers to male, 6 refers to female, and 0 refers to none. The employee ID should be less than 32 characters. The name should be less than 20 characters, and the card No. should be less than 20 characters.
- Up to 10,000 pictures can be saved in the Enroll_pic folder. If the folder enroll_pic cannot save all imported pictures, you can create another folders, named enroll_pic1, enroll_pic2, enroll_pic3, enroll_pic4, under the root directory. Up to 10 folders can be added. The picture name should follow the picture naming rule.
- Requirements of face picture should follow the rules below: It should be taken in full-face view, directly facing the camera. Do not wear a hat or head covering when taking the face picture. The format should be JPEG or JPG. The resolution should be 640 × 480 pixel or more than of 640 × 480 pixel. The picture size should be between 60 KB and 200 KB.

7.3.3 Add Face Picture

Add person's face picture to the device. And the person can use the face picture to authenticate.

Steps

1. Long tap on the initial page for 3 s and slide to the left/right by following the gesture and log in the backend.

2. Tap **Person → +** to enter the Add Person page.
3. Edit the employee ID.

Note

- The employee ID should be less than 32 characters. And it can be a combination of lower letters, upper letters, and numbers.
- The employee ID should not be duplicated.

4. Tap the Name field and input the person name on the soft keyboard.

Note

- Numbers, upper case letters, lower case letters, and special characters are allowed in the person name.
- The suggested person name should be within 32 characters.

5. Tap the Face Picture field to enter the face picture adding page.

Figure 7-9 Add Face Picture

6. Look at the camera.

Note

- Make sure your face picture is in the face picture outline when adding the face picture.
- Make sure the captured face picture is in good quality and is accurate.
- For details about the instructions of adding face pictures, see ***Tips When Collecting/ Comparing Face Picture*** .

After completely adding the face picture, a captured face picture will be displayed at the upper right corner of the page.

7. Tap **Save** to save the face picture.
8. **Optional:** Tap **Try Again** and adjust your face position to add the face picture again.
9. Set the person type.

Basic Person

The person is the normal person. The person can only authenticate or take attendance on the initial page. You can also set the basic person as an **Administrator** by enable the administrator function.

Visitor

The person is a visitor.

Person in Blocklist

The person is in the blocklist. When the person starts authentication, an event will be upload.

Custom Type

Set the custom person type.

10. Tap ✓ to save the settings.

7.3.4 Add Card

Add a card for the person and the person can authenticate via the added card.

Steps

Note

Each person can add up to 50 cards.

1. Long tap on the initial page for 3 s and slide to the left/right by following the gesture and log in the backend.
2. Tap **person → +** to enter the Add Person page.
3. Connect an external card reader according to the wiring diagram.
4. Tap the Employee ID. field and edit the employee ID.

Note

- The employee ID should be less than 32 characters. And it can be a combination of lower letters, upper letters, and numbers.
- The employee ID should not be duplicated.

5. Tap the Name field and input the person name on the soft keyboard.

Note

- Numbers, upper case letters, lower case letters, and special characters are allowed in the person name.
- The suggested person name should be within 32 characters.

6. Tap the Card field and tap **+**.

7. Configure the card No.
- Enter the card No. manually.
- Present the card over the card presenting area to get the card No.

Note
- The card No. cannot be empty.
- Up to 20 characters are allowed in the card No.
- The card No. cannot be duplicated.

8. Configure the card type.
9. Tap ✓ to save the settings.

7.3.5 Add Fingerprint

Add a fingerprint for the person and the person can authenticate via the added fingerprint.

Steps

Note
The function should be supported by the device.

1. Long tap on the initial page for 3 s and slide to the left/right by following the gesture and enter the device backend.
2. Tap **Person → +** to enter the Add Person page.
3. Tap the Employee ID. field and edit the employee ID.

Note
- The employee ID should be less than 32 characters. And it can be a combination of lower letters, upper letters, and numbers.
- The employee ID should not start with 0 and should not be duplicated.

4. Tap the Name field and input the person name on the soft keyboard.

Note
- Numbers, upper case letters, lower case letters, and special characters are allowed in the person name.
- The suggested person name should be within 32 characters.

5. Tap the Fingerprint field to enter the Add Fingerprint page.
6. Follow the instructions to add a fingerprint.

Note
- The same fingerprint cannot be repeatedly added.
- Up to 10 fingerprints can be added for one person.
- You can also use the client software or the fingerprint recorder to record fingerprints.

For details about the instructions of scanning fingerprints, see ***Tips for Scanning Fingerprint*** .

7. Tap ✓ to save the settings.

7.3.6 View PIN code

Add a PIN code for the person and the person can authenticate via the PIN code.

Steps

1. Long tap on the initial page for 3 s and slide to the left/right by following the gesture and log in the backend.

2. Tap **Person → +** to enter the Add Person page.

3. Tap the Employee ID. field and edit the employee ID.

Note

- The employee ID should be less than 32 characters. And it can be a combination of lower letters, upper letters, and numbers.
- The employee ID should not be duplicated.

4. Tap the Name field and input the person name on the soft keyboard.

Note

- Numbers, upper case letters, lower case letters, and special characters are allowed in the person name.
- The suggested person name should be within 32 characters.

5. Tap the PIN code to view the PIN code.

Note

The PIN code cannot be edited. It can only be applied by the platform.

6. Tap ✓ to save the settings.

7.3.7 Add Keyfob

Add a keyfob for the user.

Steps

Note

- The function should be supported by the device.
- Each person can add up to one keyfob, and the device can add up to 5,000 keyfobs.

1. Long tap on the initial page for 3 s and slide to the left/right by following the gesture and enter the device backend.

2. Tap **User → +** to enter the Add User page.

3. Tap the Employee ID. field and edit the employee ID.

Note

- The employee ID should be less than 32 characters. And it can be a combination of lower letters, upper letters, and numbers.
- The employee ID should not start with 0 and should not be duplicated.

4. Tap the Name field and input the user name on the soft keyboard.

Note

- Numbers, upper case letters, lower case letters, and special characters are allowed in the user name.
- The suggested user name should be within 32 characters.

5. Tap **Keyfob → + → Keyfob Serial No.** , and enter the serial No., and tap **OK**. Press and hold keys in the upper left and lower right corners of keyfob for 10 s to pair with face recognition terminal.

Note

The keyfob serial No. starts with Q-Z followed by 8-digit Arabic numerals.

6. Tap ✓ to save the settings.

7.3.8 Add Palm Print and Palm Vein

Add a palm print for the person and the person can authenticate via the added palm print.

Steps

Note

- The function should be supported by the device.
- Up to 10000 palm print and palm vein can be added.

1. Long tap on the initial page for 3 s and slide to the left/right by following the gesture and enter the device backend.
2. Tap **Person → +** to enter the Add Person page.
3. Tap the Employee ID. field and edit the employee ID.

Note

- The employee ID should be less than 32 characters. And it can be a combination of lower letters, upper letters, and numbers.
- The employee ID should not start with 0 and should not be duplicated.

4. Tap the Name field and input the person name on the soft keyboard.

Note

- Numbers, upper case letters, lower case letters, and special characters are allowed in the person name.
- The suggested person name should be within 32 characters.

5. Tap **Palm Print**, and tap **+** to enter the adding page.
6. Place the palm at a distance of 5 ~ 12 cm from the peripheral module of the device.
7. Tap ✓ to save the settings.

7.3.9 Set Person Type via Device

Set the person type as basic person, visitor, person in blocklist, or custom person type.

Before You Start

Login the device. For details, see ***Login*** .

Steps

1. Tap **Person → +**.

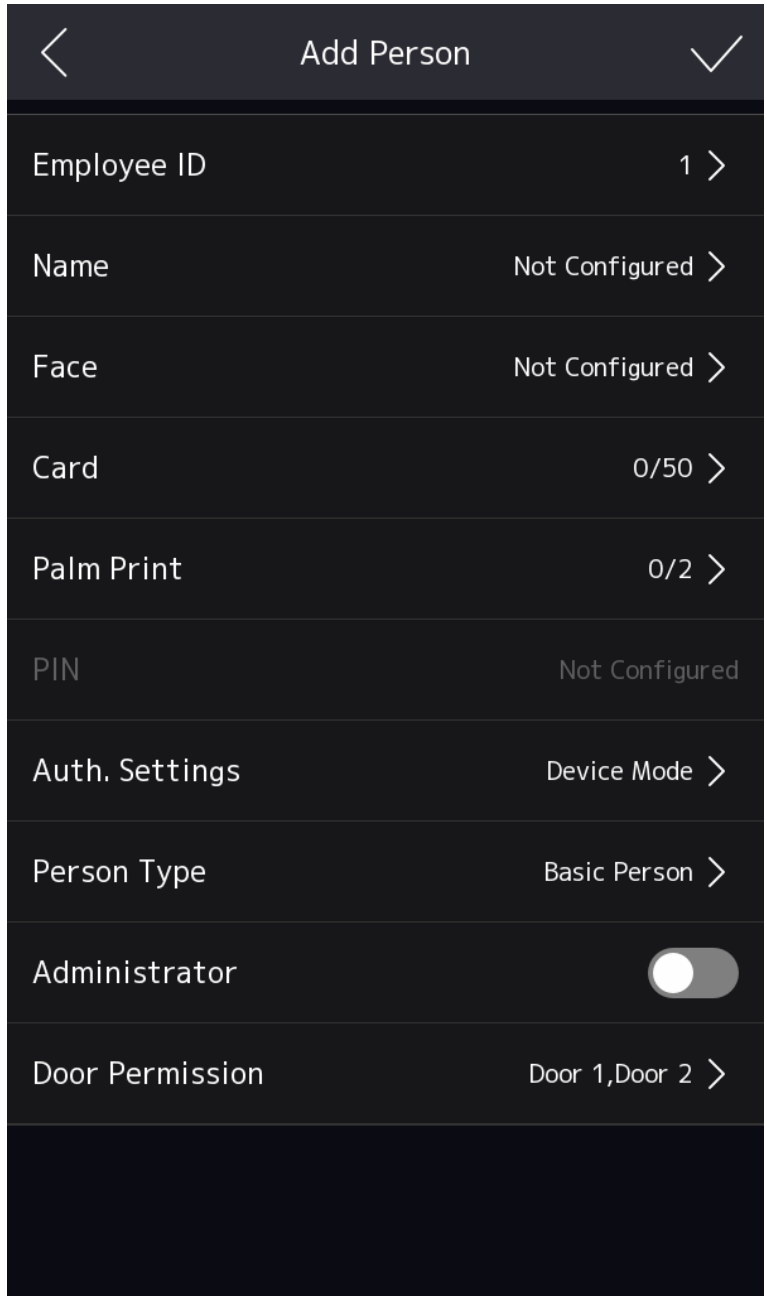


Figure 7-10 Add Person

2. Tap **Employee ID** and you can edit the Employee ID.

Note

The employee ID cannot be more than 32 characters. It can be a combination of upper case letters, lower case letters, and digits.

3. Tap **Name** and create a name. Enter the person's name according to the pop-up keyboard.

Note

- The name supports digits, upper case letters, lower case letters, and special characters.
- The name should be within 128 characters.

4. Set the face, card, fingerprint, and palm print.

Note

- Refers to ***Add Face Picture*** , ***Add Card*** , ***Add Fingerprint*** , and to add face, card, fingerprint and palm print.
- Only device with fingerprint or palm modules supports the fingerprint or palm functions.

5. Tap **Person Type** and set the type as **Basic Person**, **Visitor**, **Person in Blocklist**, or **Custom Type**.

Note

- When setting the person to visitor, administrator cannot be set. When setting the person to person in blocklist, the door permission cannot be configured.
- You should set the name of the custom type on PC web. After naming the custom type, the custom type on the device will be change to the named one. For detailed settings, see ***Person Management*** .

6. Tap ✓ to save the settings.

7.3.10 Set Authentication Mode

After adding the person's face picture, password, or other credentials, you should set the authentication mode and the person can authenticate his/her identity via the configured authentication mode.

Steps

1. Long tap on the initial page for 3 s and slide to the left/right by following the gesture and log in the backend.
2. Tap **Person → Add Person/Edit Person → Authentication Mode** .
3. Select Device or Custom as the authentication mode.

   Device

   If you want to select device mode, you should set the terminal authentication mode in Access Control Settings page first. For details see *Setting Access Control Parameters*.

   Custom

   You can combine different authentication modes together according to your actual needs.
4. Tap ✓ to save the settings.

7.3.11 Search and Edit Person

After adding the person, you can search the person and edit it.

Search Person

On the Person Management page, Tap the search area to enter the Search Person page. Tap **Card** on the left of the page and select a search type from the drop-down list. Enter the employee ID, card No., or the person name for search. Tap to search.

Edit Person

On the Person Management page, select a person from the person list to enter the Edit Person page. Follow the steps in ***Person Management*** to edit the person parameters. Tap to save the settings.

Note

The employee ID cannot be edited.

7.3.12 Set Person Door Permission via Device

Set the normal person or visitor's permission of passing door.

Before You Start

Login the device. For details, see ***Login*** .

Steps

1. Tap **Person → +**.

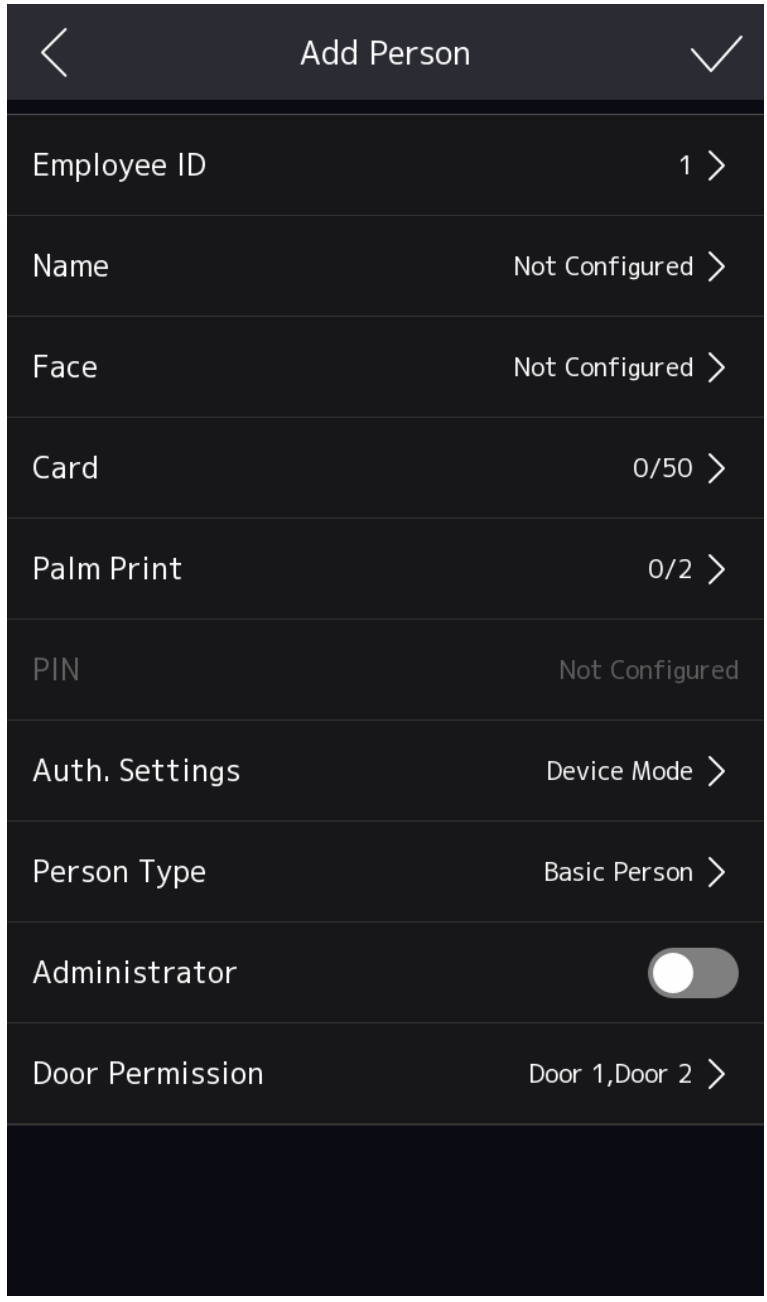


Figure 7-11 Add Person

2. Tap **Employee ID** and you can edit the Employee ID.

Note

The employee ID cannot be more than 32 characters. It can be a combination of upper case letters, lower case letters, and digits.

3. Tap **Name** and create a name. Enter the person's name according to the pop-up keyboard.

Note

- The name supports digits, upper case letters, lower case letters, and special characters.
- The name should be within 128 characters.

4. Set the face, card, fingerprint, and palm print.

Note

- Refers to ***Add Face Picture*** , ***Add Card*** , ***Add Fingerprint*** , and to add face, card, fingerprint and palm print.
- Only device with fingerprint or palm modules supports the fingerprint or palm functions.

5. Tap **Person Type** and set the type as **Basic Person** or **Visitor**.

Note

When setting the person to visitor, administrator cannot be set. If set the person as person in blocklist, you cannot configure the door permission for the person.

6. Tap **Door Permission**, and select a door for the person to pass. Door 1 means that the door is connected to the device. Door 2 means the door is connected to the secure door control unit.

Note

When remote authentication, the administrator can judge the door to open according to the person's door permission.

7. Tap ✓ to save the settings.

7.4 Data Management

You can delete data, import data, and export data.

7.4.1 Delete Data

Delete person data.

On the Home page, tap **Data → Delete Data → Person Data** . All person data added in the device will be deleted.

7.4.2 Import Data

Steps

1. Plug a USB flash drive in the device.
2. On the Home page, tap **Data → Import Data** .
3. Tap **Person Data**, **Face Data** or **Access Control Parameters** .

Note

The imported access control parameters are configuration files of the device.

4. Enter the created password when you exported the data. If you do not create a password when you exported the data, leave a blank in the input box and tap **OK** immediately.

Note

- If you want to transfer all person information from one device (Device A) to another (Device B), you should export the information from Device A to the USB flash drive and then import from the USB flash drive to Device B. In this case, you should import the person data before importing the profile photo.
- The supported USB flash drive format is FAT32.
- The imported pictures should be saved in the folder (named enroll_pic) of the root directory and the picture's name should be follow the rule below:
  Card No._Name_Department_Employee ID_Gender.jpg
- If the folder enroll_pic cannot save all imported pictures, you can create another folders, named enroll_pic1, enroll_pic2, enroll_pic3, enroll_pic4, under the root directory.
- The employee ID should be less than 32 characters. It can be a combination of lower letters, upper letters, and numbers. It should not be duplicated, and should not start with 0.
- Requirements of face picture should follow the rules below: It should be taken in full-face view, directly facing the camera. Do not wear a hat or head covering when taking the face picture. The format should be JPEG or JPG. The resolution should be 640 × 480 pixel or more than of 640 × 480 pixel. The picture size should be between 60 KB and 200 KB.

7.4.3 Export Data

Steps

1. Plug a USB flash drive in the device.
2. On the Home page, tap **Data → Export Data** .
3. Tap **Face Data**, **Event Data**, **Person Data**, or **Access Control Parameters**.

Note

The exported access control parameters are configuration files of the device.

4. **Optional:** Create a password for exporting. When you import those data to another device, you should enter the password.

Note

- The supported USB flash drive format is DB.
- The system supports the USB flash drive with the storage of 1 G to 256 G. Make sure the free space of the USB flash drive is more than 512M.
- The exported person data is a DB file, which cannot be edited.

7.5 Person Authentication

After network configuration, system parameters configuration and user configuration, you can go back to the initial page for authentication. The system will authenticate person according to the configured authentication mode.

7.5.1 Authenticate via Single Credential

Set the user authentication type before authentication. For details, see ***Set Authentication Mode*** .

Face

Face forward at the camera and start authentication via face.

Fingerprint

Place the enrolled fingerprint on the fingerprint module and start authentication via fingerprint.

Palm

Place the palm on the palm print module and start authentication via palm print.

Card

Present the card on the card presenting area and start authentication via card.

Note

The card can be normal IC card, or encrypted card.

QR Code

Put the QR code in front of the device camera to authenticate via QR code.

Note

- Authentication via QR code should be supported by the device.
- You should enable QR code function in ***Preference Settings*** .

PIN

Enter the PIN to authenticate via PIN.

Keyfob

Press door-open button on the keyfob to authenticate.

If authentication completed, a prompt "Authenticated" will pop up.

7.5.2 Authenticate via Multiple Credential

Before You Start

Set the user authentication type before authentication. For details, see ***Set Authentication Mode*** .

Steps

1. Authenticate any credential according to the instructions on the live view page.

Note

- The card can be normal IC card, or encrypted card.
- If the QR Code Scanning function is enabled, you can put the QR code in front of the device camera to authenticate via QR code.

2. After the previous credential is authenticated, continue authenticate other credentials.

Note

- For detailed information about scanning fingerprint, see *Tips for Scanning Fingerprint*.
- For detailed information about authenticating face, see *Tips When Collecting/Comparing Face Picture*.

If authentication succeeded, the prompt "Authenticated" will pop up.

7.6 Basic Settings

Long tap on the initial page for 3 s and slide to the left/right by following the gesture and login the device home page. Tap **System → Basic** .

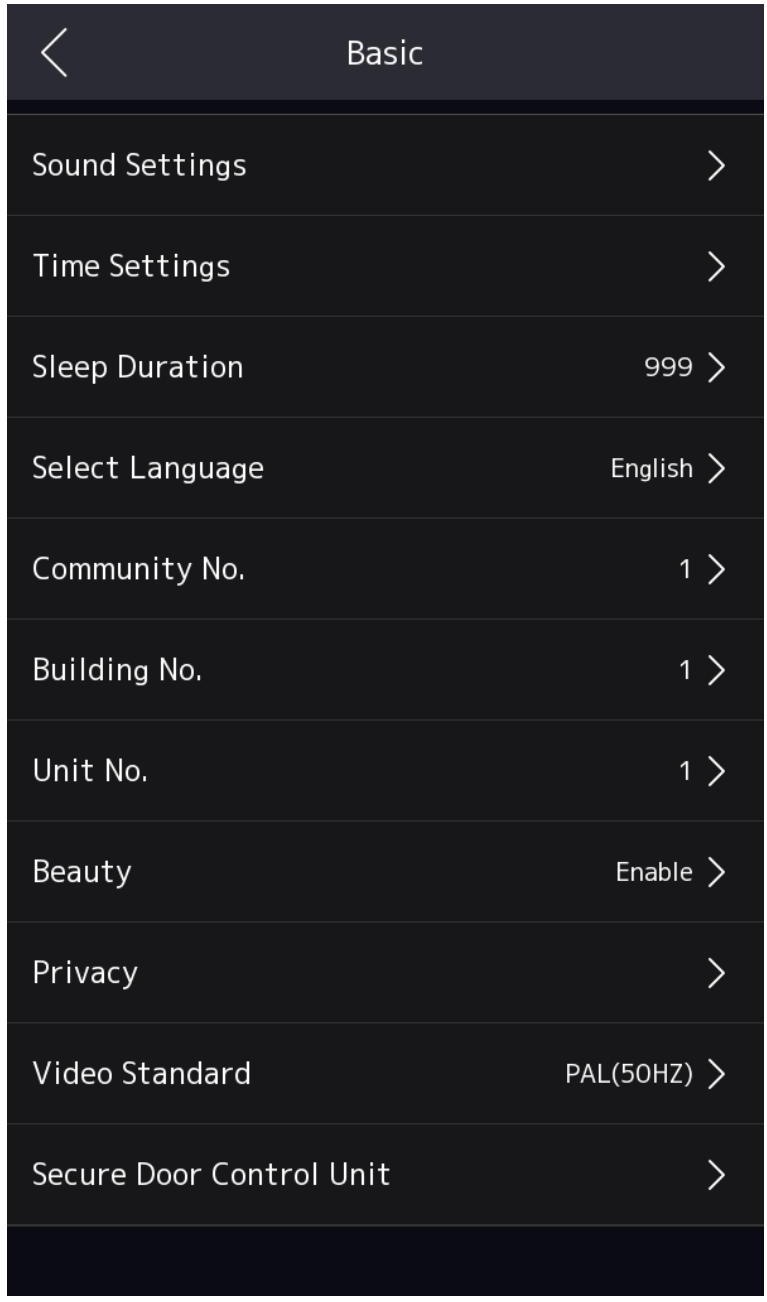


Figure 7-12 Basic Settings Page

7.6.1 Enable/Disable Voice Prompt via Device

You can enable/disable the voice prompt function and adjust the voice volume.

Login the device. For details, see ***Login*** .

Tap **System Settings → Basic → Sound Settings**.

You can enable **Voice Prompt** function and adjust the voice volume. Enable the voice prompt function and you can set the voice volume.

7.6.2 Set Device Time via Device

Set the device time.

Login the device. For details, see ***Login*** .

Tap **System Settings → Basic → Time Settings**.

Set the device time zone, current time, and DST.

7.6.3 Set Sleep Duration via Device

Set the device sleeping waiting time.

Login the device. For details, see ***Login*** .

Tap **System Settings → Basic**. And Set **Sleep Duration**.

When you are on the initial page and if you set the sleeping time to 30 s, the device will sleep after 30 s without any operation.

Note

If you set the sleeping time to 0, the device will not enter sleeping mode. The configurable sleep time is between 20 and 999s.

7.6.4 Select Language

Login the device. For details, see ***Login*** .

Tap **System Settings → Basic** . And tap **Select Language** to change the device language.

The device will reboot after changing the language.

7.6.5 Set Device Number via Device

The device can be used as access control device, door station, or outer door station. You can set the device number for video intercom.

Login the device. For details, see ***Login*** .

Tap **System Settings → Basic**. And set **Community No.**, **Building No.**, and **Unit No.**

7.6.6 Set Beauty via Device

You can enable the beauty function and set the smooth and the whiten parameter.

Login the device. For details, see ***Login*** .

Tap **System Settings → Basic → Beauty**.

Enable the beauty function and set the smooth and the whiten parameter. Tap **+** or **-** to control the effect strength.

7.6.7 Set Privacy Parameters via Device

Set the picture uploading parameters.

Note

Different device models support different functions. Refers to actual model.

Login the device. For details, see ***Login*** .

Tap **System Settings → Basic → Privacy**.

Authentication Settings

Name / Employee ID / Face Picture

You can choose to display/not display/desensitize name and Employ ID when authenticating.

Picture Uploading and Storage

Set picture uploading and storage parameters.

Save Registered Pic.

The registered face picture will be saved to the system if you enable the function.

Save Pic. After Linked Capture

If you enable this function, you can save the picture after linked capture.

Upload Pic. After Linked Capture

Upload the pictures captured after linked capture.

Save Pic When Auth.

If you enable this function, you can save the picture when authenticating to the device.

Upload Pic. When Auth.

If you enable this function, you can save the picture when authenticating to the device.

Save Palm Print Picture

If you enable this function, you can save the picture when applying.

7.6.8 Set Video Standard

Set video standard for the live view.

Login the device. For details, see ***Login*** .

Go to **System → Basic → Video Standard**。

Set the video frame rate when performing live view remotely. After changing the standard, you should reboot the device to take effect.

PAL (50HZ)

25 frames per second. Suitable for mainland China, Hong Kong (China), the Middle East countries, Europe countries, etc.

NTSC (60HZ)

30 frames per second. Suitable for the USA, Canada, Japan, Taiwan (China), Korea, the Philippines, etc.

7.6.9 Set Secure Door Control Unit Parameters

You can wire peripherals according to the secure door control unit. You can set to use door 1 or door 2 to control the secure door control unit.

Before You Start

Device is wiring the secure door control unit by RS-485. For detailed wiring method, see ***Wiring*** .

Steps

1. Login the device. For details, see ***Login*** .
2. Go to **System → Basic → Secure Door Control Unit**.
3. Select **Door 1** or **Door 2** as door No.

Note

Door 1 means that the door will be controlled by secure door control unit. The same goes to the selection of door 2.

7.7 Set Face Parameters

You can customize the face parameters to improve the face recognition performance.

Long tap on the initial page for 3 s and login the home page. Tap **System Settings → Biometrics** .

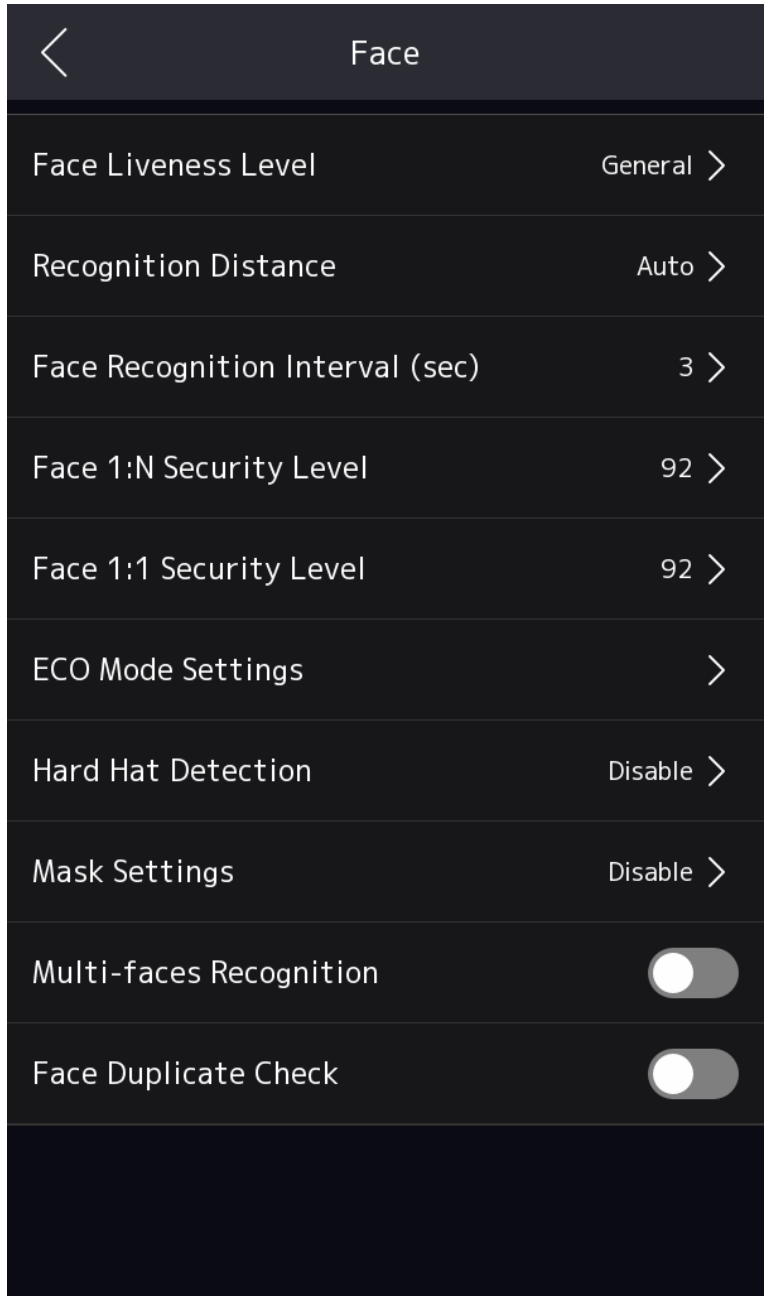


Figure 7-13 Face Settings

7.7.1 Set Face Liveness Level via Device

After enabling face anti-spoofing function, you can set the matching security level when performing live face authentication.

Login the device. For details, see ***Login*** .

Tap **System Settings → Biometrics → Face** .

Select a face liveness level.

You can select from general, advanced, and professional. The higher the level, the fault acceptance rate will be lower and the false rejection rate will be higher.

7.7.2 Set Recognition Distance via Device

Set the valid distance between the user and the camera when authenticating.

Login the device. For details, see ***Login*** .

Tap **System Settings → Biometrics → Face → Recognition Distance** .

Set the recognition distance.

7.7.3 Set Face Recognition Interval via Device

The time interval between two continuous face recognitions when authenticating.

Login the device. For details, see ***Login*** .

Tap **System Settings → Biometrics → Face → Face Recognition Interval (sec)** .

Set the face recognition interval.

Note

Please enter a number between 1 and 10.

7.7.4 Set Face 1:N Security Level via Device

Set the matching threshold when authenticating via 1:N matching mode.

Login the device. For details, see ***Login*** .

Tap **System Settings → Biometrics → Face → Face 1:N Security Level** .

Set the matching threshold when authenticating via 1:N matching mode.

The larger the value of the threshold, the fault acceptance rate will be lower and the false rejection rate will be higher when authenticating via face. The maximum value is 100.

7.7.5 Set Face 1:1 Security Level via Device

Set the matching threshold when authenticating via 1:1 matching mode.

Login the device. For details, see ***Login*** .

Tap **System Settings → Biometrics → Face → Face 1: 1 Security Level** .

Set the matching threshold when authenticating via 1:1 matching mode.

The larger the value of the threshold, the fault acceptance rate will be lower and the false rejection rate will be higher when authenticating via face. The maximum value is 100.

7.7.6 Enable/Disable ECO Mode via Device

If the ECO mode is enabled, you can authenticate faces in the low light or dark environment with IR camera.

Login the device. For details, see ***Login*** .

Tap **System Settings → Biometrics → Face → ECO Mode Settings** .

If the ECO mode is enabled, you can authenticate faces in the low light or dark environment with IR camera. You can set the ECO mode threshold, ECO mode (1:N), and ECO mode (1:1).

ECO Mode Threshold

When enabling the ECO mode, you can set the ECO mode's threshold. The larger the value, the easier the device entering the ECO mode. The threshold has relationship with the illumination.

ECO Mode (1:1)

Set the matching threshold when authenticating via ECO mode 1:1 matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate. The maximum value is 100.

ECO Mode (1:N)

Set the matching threshold when authenticating via ECO mode 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate. The maximum value is 100.

7.7.7 Enable/Disable Hard Hat Detection via Device

After enabling the hard hat detection, when the device starts face authentication, the system will detection whether the person wearing a hard hat or not.

Login the device. For details, see ***Login*** .

Tap **System Settings → Biometrics → Face → Hard Hat Detection** .

Hard Hat Detection

After enabling the hard hat detection function, you can set the strategy of door opening.

None

If the person do not wear a face mask when authenticating, the device will not prompt a notification.

Reminder of Wearing

If the person do not wear the hard hat when authenticating, the device will pop up a prompt and the door will open.

Must Wear

If the person do not wear the hard hat when authenticating, the device will pop up a prompt and the door will keep closed.

7.7.8 Enable/Disable Mask Detection via Device

After enabling the face with mask detection, the system will recognize the captured face with mask picture.

Login the device. For details, see ***Login*** .

Tap **System Settings → Biometrics → Face → Mask Settings**.

After enabling the face with mask detection, the system will recognize the captured face with mask picture. You can set **Face with Mask & Face (1:1)**、**Face with Mask & Face (1:N)**、**ECO Mode (1:1) Threshold**、**ECO Mode (1:N) Threshold**, and **Prompt Method**.

Face with Mask & Face (1:1)

Set face with mask 1:1 matching threshold. The larger the value, the smaller the false accept rate and the larger the false rejection rate. The maximum value is 100.

Face with Mask & Face (1:N)

Set face with mask 1:N matching threshold. The larger the value, the smaller the false accept rate and the larger the false rejection rate. The maximum value is 100.

ECO Mode (1:1) Threshold

After enabling the ECO mode, you can set the face with mask function. You can set the threshold.

Set the matching threshold when authenticating via ECO mode 1:1 matching mode. The larger the value of the threshold, the fault acceptance rate will be lower and the false rejection rate will be higher when authenticating via face. The maximum value is 100.

ECO Mode (1:N) Threshold

After enabling the ECO mode, you can set the face with mask function. You can set the threshold.

Set the matching threshold when authenticating via ECO mode 1:N matching mode. The larger the value of the threshold, the fault acceptance rate will be lower and the false rejection rate will be higher when authenticating via face. The maximum value is 100.

Strategy

Set **None**、**Reminder of Wearing**, and **Must Wear**.

None

If the person do not wear a face mask when authenticating, the device will not prompt a notification.

Reminder of Wearing

If the person do not wear a face mask when authenticating, the device prompts a notification and the door will open.

Must Wear

If the person do not wear a face mask when authenticating, the device prompts a notification and the door keeps closed.

7.7.9 Enable/Disable Multi-Faces Recognition

After multiple faces authentication is enabled, multiple faces authentication is supported.

Login the device. For details, see ***Login*** .

Tap **System Settings → Biometrics → Face**.

Enable **Multi-faces Recognition**. After the function is enabled, multiple faces can authenticate at the same time.

Note

- Up to 5 persons can authentication at the same time.
- After the function is enabled, card reader authentication mode, custom authentication, attendance status, manually trigger authentication via face cannot be used.

7.7.10 Face Duplicate Check via Device

After enabling the face duplicate check function, when adding person's face, the system will check the duplication. If there is duplicated face picture detected in the system, a prompt will be pop up.

Note

The function is not supported in remote adding or applying face picture in batch.

Login the device. For details, see ***Login*** .

Tap **System Settings → Biometrics → Face** .

Enable **Face Duplicate Check**. After enabling the function, when adding person's face, the system will check the duplication. If there is duplicated face picture detected in the system, a prompt will be pop up.

7.7.11 Set Palm Print

You can set palm print recognition timeout threshold and palm print recognition interval .

Login the device. For details, see ***Login*** .

Tap **System Settings → Biometrics → Palm Print** .

Set **Palm Print Recognition Timeout Threshold** and **Palm Print Recognition Interval**.

7.8 Access Control Settings

You can set the access control permissions.

On the Home page, tap **ACS** to enter the Settings page.

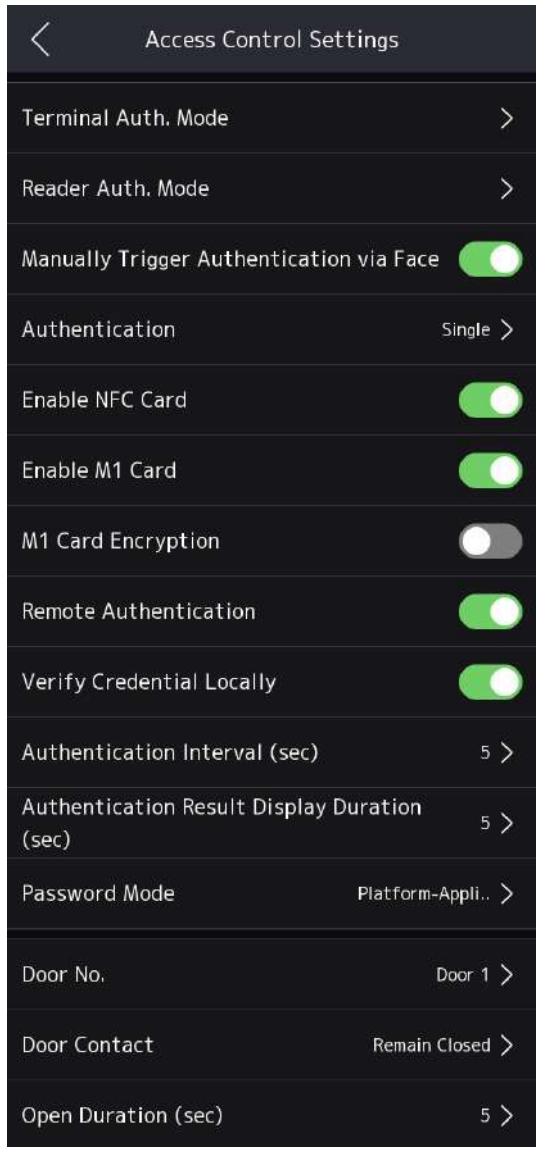


Figure 7-14 Access Control Settings

7.8.1 Set Terminal Authentication Mode via Device

Select the face recognition terminal's authentication mode. You can select different combination to authenticate.

Login the device. For details, see ***Login*** .

Tap **ACS → Terminal Auth. Mode** .

Select person authentication type and method and save the settings.

If all persons on the device's authentication mode is **Device Mode**, all persons on the device will use the device authentication mode. For detail about person authentication mode settings, see ***Set Authentication Mode*** .

Note

Device with fingerprint module supports fingerprint function.

Caution

Biometric recognition products are not completely applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.

7.8.2 Set Reader Authentication Mode via Device

Set the person authentication type on the wired external reader. You can select different combination to authenticate.

Login the device. For details, see ***Login*** .

Tap **ACS → Reader Auth. Mode** .

Select person authentication type and save the settings.

Select person authentication type and method and save the settings.

If all persons on the device's authentication mode is **Device Mode**, all persons on the device will use the device authentication mode. For detail about person authentication mode settings, see ***Set Authentication Mode*** .

Note

Device with fingerprint module supports fingerprint function.

Caution

Biometric recognition products are not completely applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.

7.8.3 Manually Trigger Face Authentication via PC Web

After enabling Manually Trigger Authentication via Face, you need to touch the screen of the device manually for face recognition.

Login the device. For details, see ***Login*** .

Tap **ACS**.

Enable **Manually Trigger Authentication via Face**, and set **Authentication** as **Single** or **Continuous**

Single

The person should tap **Authentication** on the authentication page manually to trigger recognition before each face recognition.

Continuous

After triggering the recognition, you can recognize via face until the device enter into the sleeping mode.

7.8.4 Enable/Disable NFC Card

Enable/disable NFC card function.

After login, tap **ACS**.

Tap **Enable NFC**. After enabling, the device can read NFC card.

Note

When the dual-frequency card module access to the face recognition terminal, swiping the card on the device is invalid.

7.8.5 Enable/Disable M1 Card

Enable or disable M1 card function.

Login the device. For details, see ***Login*** .

After login, tap **ACS**.

Tap **Enable M1 Card**, and the device can read M1 card.

Enable M1 Card

After enabling, the device can read M1 card.

M1 Card Encryption

After enabling M1 Card Encryption, the device will verify the M1 card sector. Go to the platform to set the M1 card's encryption sector.

Note

When the dual-frequency card module access to the face recognition terminal, swiping the card on the device is invalid.

7.8.6 Remote Authentication

Judge the authentication passes or not by remote platforms.

Login the device. For details, see ***Login*** .

Tap **ACS**.

Enable **Remote Authentication**. When there's a person is authenticating, the remote platform will judge to pass or not.

Authenticate the credential on the device and verify by the platform.

You can also enable **Verify Credential Locally** and the verification will be produced on the device.

7.8.7 Set Authentication Interval via Device

Login the device. For details, see ***Login*** .

Tap **ACS**, and set **Authentication Interval** and save.

You can set the authentication interval of the same person when authenticating. The same person can only authenticate once in the configured interval. A second authentication will be failed. Available authentication interval range: 0 to 65535.

7.8.8 Set Authentication Result Display Duration via Device

Set the authentication result display duration when authenticating.

Login the device. For details, see ***Login*** .

Tap **ACS**, and set **Authentication Result Display Duration** and save.

7.8.9 Set Password Mode

You can set the password mode and choose whether to edit password on device / PC web, or platform.

Steps

1. Login the device. For details, see ***Login*** .
2. Tap **ACS**.
3. Tap **Password Mode** and set the mode.

   Platform-Applied Personal PIN

   The PIN is managed and distributed by the platform after the device accesses the platform.

   Device-Set Personal PIN

   The PIN is set on the device or PC Web.
4. Go back to the previous page to save the settings.

7.8.10 Door Parameter Configuration

Configure parameters for unlocking doors.

Set Door No. via Device

Select a door No. for the device.

Login the device. For details, see ***Login*** .

After login, tap **ACS**.

Tap **Door No.**. Select **Door 1** or **Door 2**.

The door 1 means the device installed at the entrance. Door 2 means the device installed at the exit.

Set Door Contact via Device

Select door contact status according to the door contact's wiring method.

Login the device. For details, see ***Login*** .

Tap **ACS**.

You can select Remain Open or Remain Closed according to your actual needs. By default, it is Remain Closed.

Set Open Duration via Device

Set the door unlocking duration.

Login the device. For details, see ***Login*** .

Tap **ACS**.

Set the door unlocking duration. If the door is not opened for the set time, the door will be locked. Available door locked time range: 1 to 255s.

7.9 Platform Attendance

You can set the attendance mode as check in, check out, break out, break in, overtime in, and overtime out according to your actual situation.

Note

The function should be used cooperatively with time and attendance function on the client software.

7.9.1 Disable Attendance Mode via Device

Disable the attendance mode and the system will not display the attendance status on the initial page.

Tap **Platform Attendance** to enter the T&A Status page.

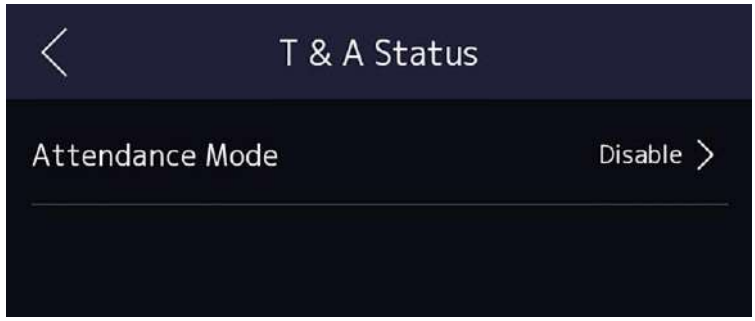


Figure 7-15 Disable Attendance Mode

Set the **Attendance Mode** as **Disable**.

You will not view or configure the attendance status on the initial page. And the system will follow the attendance rule that configured on the platform.

7.9.2 Set Manual Attendance via Device

Set the attendance mode as manual, and you should select a status manually when you take attendance.

Before You Start

Add at least one user, and set the user's authentication mode. For details, see *User Management*.

Steps

1. Tap **Platform Attendance** to enter the T&A Status page.
2. Set the **Attendance Mode** as **Manual**.

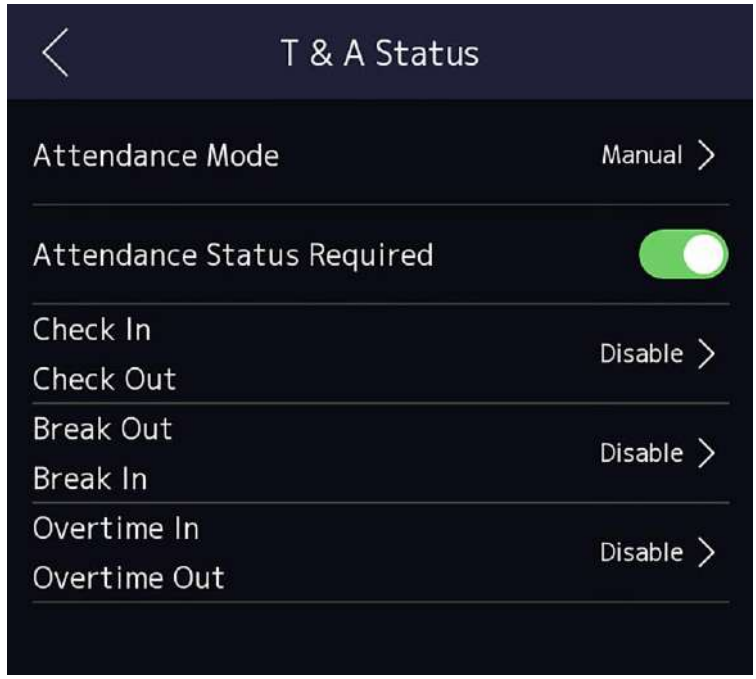


Figure 7-16 Manual Attendance Mode

3. Enable the **Attendance Status Required**.
4. Enable a group of attendance status.

Note
The Attendance Property will not be changed.

5. **Optional:** Select an status and change its name if required.
   The name will be displayed on the T & A Status page and the authentication result page.

Result

You should select an attendance status manually after authentication.

Note
If you do not select a status, the authentication will be failed and it will not be marked as a valid attendance.

7.9.3 Set Auto Attendance via Device

Set the attendance mode as auto, and you can set the attendance status and its available schedule. The system will automatically change the attendance status according to the configured schedule.

Before You Start
Add at least one user, and set the user's authentication mode. For details, see *User Management*.

Steps

1. Tap **Platform Attendance** to enter the T&A Status page.
2. Set the **Attendance Mode** as **Auto**.

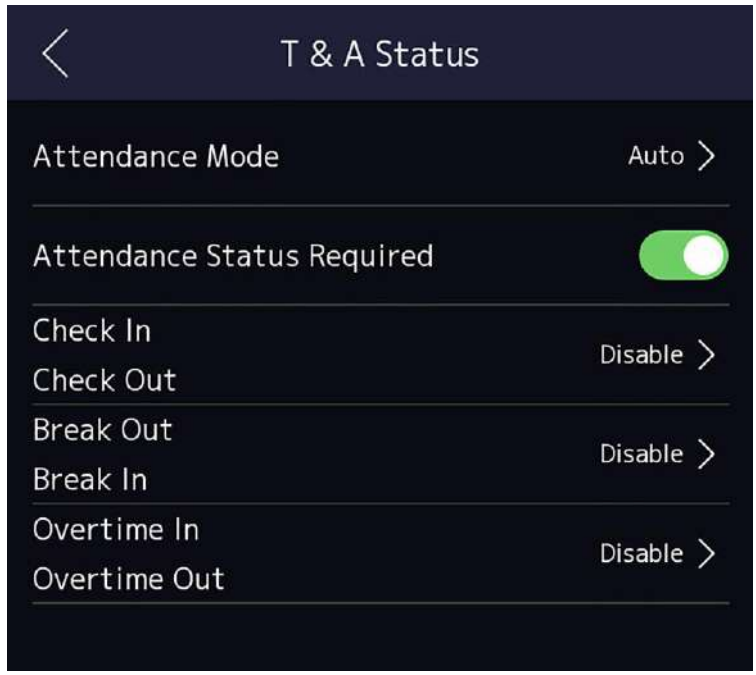


Figure 7-17 Auto Attendance Mode

3. Enable the **Attendance Status** function.
4. Enable a group of attendance status.

Note

The Attendance Property will not be changed.

5. **Optional:** Select an status and change its name if required.
   The name will be displayed on the T & A Status page and the authentication result page.
6. Set the status' schedule.
   1) Tap **Attendance Schedule**.
   2) Select **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**, or **Sunday**.
   3) Set the selected attendance status's start time of the day.
   4) Tap **Confirm**.
   5) Repeat step 1 to 4 according to your actual needs.

Note

The attendance status will be valid within the configured schedule.

Result

When you authenticate on the initial page, the authentication will be marked as the configured attendance status according to the configured schedule.

Example
If set the **Break Out** as Monday 11:00, and **Break In** as Monday 12:00, the valid user's authentication from Monday 11:00 to 12:00 will be marked as break.

7.9.4 Set Manual and Auto Attendance via Device

Set the attendance mode as **Manual and Auto**, and the system will automatically change the attendance status according to the configured schedule. At the same time you can manually change the attendance status after the authentication.

Before You Start
Add at least one user, and set the user's authentication mode. For details, see *User Management*.

Steps
1. Tap **Platform Attendance** to enter the T&A Status page.
2. Set the **Attendance Mode** as **Manual and Auto**.

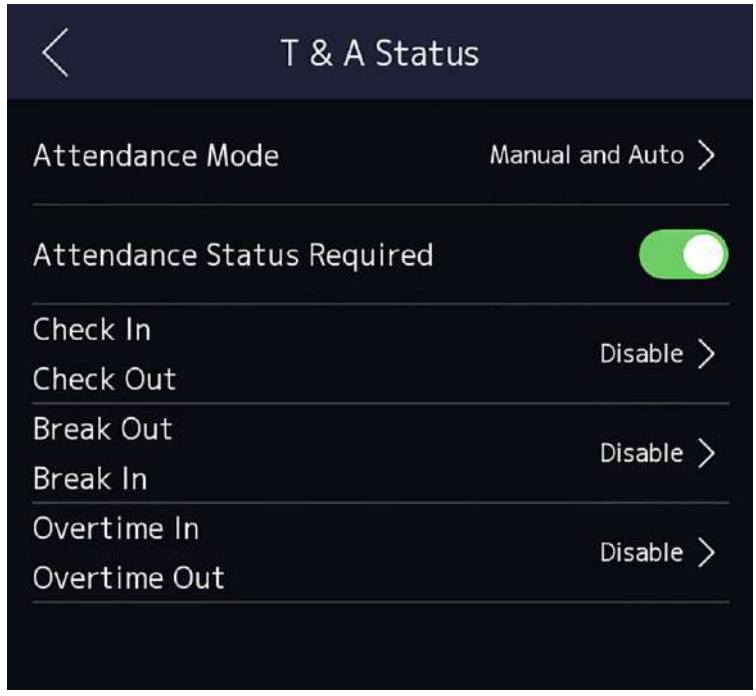


Figure 7-18 Manual and Auto Mode

3. Enable the **Attendance Status** function.
4. Enable a group of attendance status.

Note
The Attendance Property will not be changed.

5. **Optional:** Select an status and change its name if required.
   The name will be displayed on the T & A Status page and the authentication result page.

6. Set the status' schedule.
1) Tap **Attendance Schedule**.
2) Select **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**, or **Sunday**.
3) Set the selected attendance status's start time of the day.
4) Tap **OK**.
5) Repeat step 1 to 4 according to your actual needs.

Note
The attendance status will be valid within the configured schedule.

Result

On the initial page and authenticate. The authentication will be marked as the configured attendance status according to the schedule. If you tap the edit icon on the result tab, you can select a status to take attendance manually, the authentication will be marked as the edited attendance status.

Example
If set the **Break Out** as Monday 11:00, and **Break In** as Monday 12:00, the valid user's authentication from Monday 11:00 to 12:00 will be marked as break.

7.10 Preference Settings

You can configure preference settings parameters.

Steps
1. Tap **System → Preference** to enter the preference settings page.

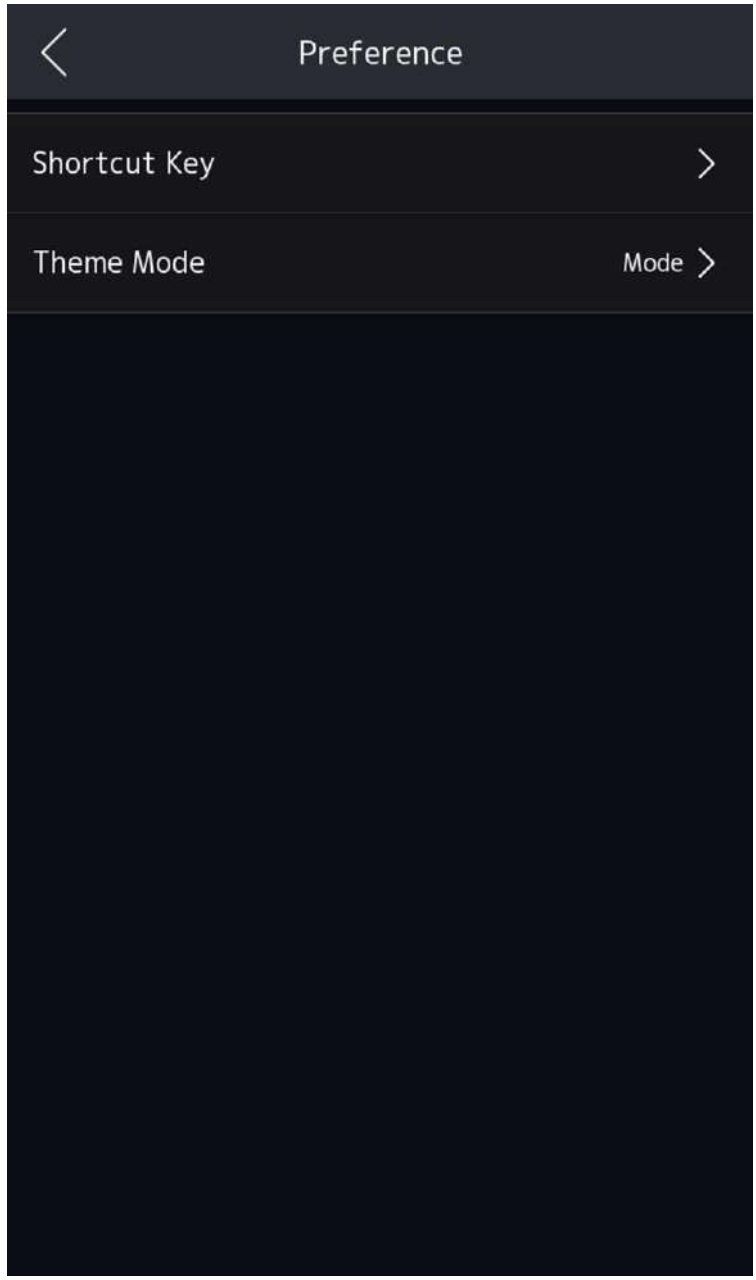


Figure 7-19 Preference Settings

7.10.1 Set Shortcut Key via Device

Choose the shortcut key that displayed on the authentication page, including the QR code function, the call function, call type, and the password entering function.

Login the device. For details, see ***Login*** .

Tap **System Settings → Preference**.

Choose the shortcut key that displayed on the authentication page, including the QR code function, the call function, call type, and the password entering function.

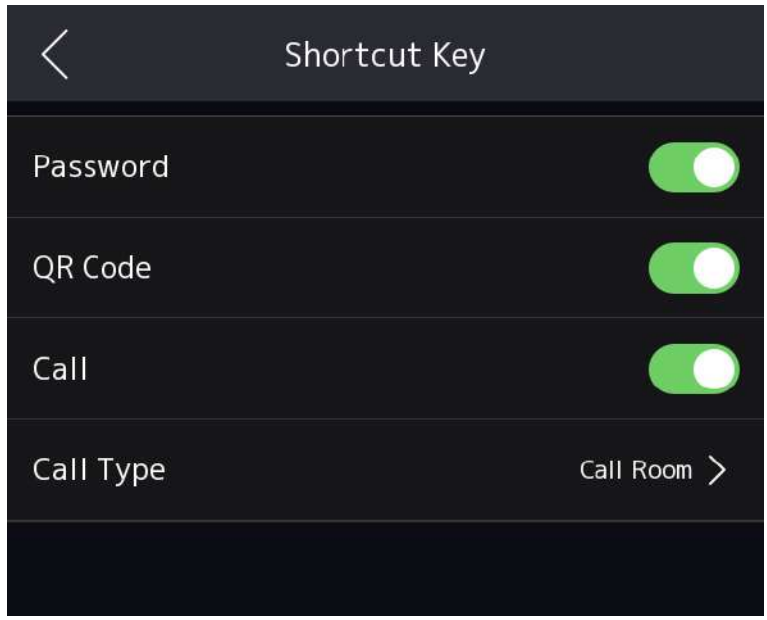


Figure 7-20 Shortcut Key Settings

Password

Enable this function and you can enter the password to authenticate via password. Tap on the authentication page to verify.

QR Code

You can use the QR code scanning function on the authentication interface. The device will upload the information associated with the obtained QR code to the platform. Tap on the authentication page to verify.

Call

You can select call types from Call Room, Call Center, Call Specified Room, or Call APP. If you select **Call Specified Room**, you should enter the room No.

Tap on the authentication page to call.

7.10.2 Theme

Select different theme and the authentication page will show different contents.

Login the device. For details, see ***Login*** .

System Settings → Preference.

Select a theme mode.

Authentication

The live view will be displayed in authentication, and in the meanwhile, the person's name, employee ID, face pictures will all displayed as well.

Advertisement

The advertising area and identification authentication area of the device will be displayed on separate screens. Video, text, welcome words will be displayed in the advertizement area.

7.11 System Maintenance

Long tap on the initial page for 3 s and slide to the left/right by following the gesture and login the home page. Tap **Maint.**

7.11.1 View System Information

View the device system information.

Long tap on the initial page for 3 s and slide to the left/right by following the gesture and login the home page. Tap **Maint. → System Info.** .

You can view the device model, serial No., versions, address, production data, QR code, and open source code license.

Note

The page may vary according to different device models. Refers to the actual page for details.

Long tap on the right corner to enter the advanced settings page. You can set biometrics parameters and view the device version information.

Biometric Parameter

Custom Anti-Spoofing Detection

Face Liveness Level

After enabling face anti-spoofing function, you can set the matching security level when performing live face authentication.

Anti-Spoofing Detection Threshold

The larger the value, the smaller the false accept rate and the larger the false rejection rate. The smaller the value, the larger the false accept rate and the smaller the false rejection rate.

Lock Face for Anti-Spoofing Protection

After enabling this function, the device will lock automatically when anti-spoofing detection failed.

Lock Duration

The lock duration after enabling **Lock Face for Anti-Spoofing Protection** when anti-spoofing detection failed.

Version Information

You can view the device information.

7.11.2 View Device Capacity via Device

You can view the device capacity.

Long tap on the initial page for 3 s and slide to the left/right by following the gesture and login the home page. Tap **Maint. → Capacity**.

You can view the number of, user, face picture, card, fingerprint, palm print and event.

Note

Only device installed with fingerprint module supports display fingerprint capacity.

7.11.3 Upgrade

Online Upgrade

You can online upgrade the device.

Long tap on the initial page for 3 s and slide to the left/right by following the gesture and login the home page. Tap **Maint. → Device Upgrade**.

If the device is connected to the network and added to Hik-Connect App, you can tap **Device Upgrade → Online Upgrade**on device for upgrading when there is an updated version in Hik-Connect App.

Local Upgrade

You can upgrade the device locally.

Long tap on the initial page for 3 s and slide to the left/right by following the gesture and login the home page. Tap **Maint. → Device Upgrade**.

Insert an USB flash drive. Tap **Device Upgrade → Update vi USB**, and the device will read the digicap.dav file in the USB flash drive to start upgrading.

7.11.4 Restore Settings

Restore to Factory Settings via Device

All parameters will be restored to the factory settings.

Long tap on the initial page for 3 s and slide to the left/right by following the gesture and login the home page. Tap **Maint. → Restore to Factory Settings**. The system will reboot to take effect.

Restore to Default Settings via Device

All parameters, except for the communication settings, remotely imported user information, will be restored to the default settings.

Long tap on the initial page for 3 s and slide to the left/right by following the gesture and login the home page. Tap **Maint. → Restore to Default Settings**. The system will reboot to take effect.

All parameters, except for the communication settings, remotely imported user information, will be restored System default settings. System will reboot after restoring the default settings.

Device Reboot

You can reboot the device manually.

Long tap on the initial page for 3 s and slide to the left/right by following the gesture and login the home page. Tap **Maint. → Reboot**.

7.12 Video Intercom

After adding the device to the client software, you can call the device from the client software, call the main station from the device, call the client software from the device, call the indoor station from the device, or call the specific room from the device.

7.12.1 Call Client Software from Device

Steps

1. Get the client software from the supplied disk or the official website, and install the software according to the prompts.
2. Run the client software and the control panel of the software pops up.
3. Click **Device Management** to enter the Device Management interface.
4. Add the device to the client software.

Note

For details about adding device, see *Add Device*.

5. Call the client software.
   1) Tap on the device initial page.
   2) Enter ***0*** in the pop-up window.
   3) Tap to call the client software.
6. Tap **Answer** on the pop-up page of the client software and you can start two-way audio between the device and the client software.

Note

If the device is added to multiple client softwares and when the device is calling the client software, only the first client software added the device will pop up the call receiving window.

7.12.2 Call Center from Device

Steps

1. Get the client software from the supplied disk or the official website, and install the software according to the prompts.
2. Run the client software and the control panel of the software pops up.
3. Click **Device Management** to enter the Device Management interface.
4. Add the main station and the device to the client software.

Note

For details about adding device, see *Add Device*.

5. Set the main station's IP address and SIP address in the remote configuration page.

Note

For details about the operation, see the user manual of the main station.

6. Call the center.
   - If you have configured to call center in the ***Basic Settings*** , you can tap to call the center.
   - If you have not configured to call center in the ***Basic Settings*** , you should tap → to call the center
7. Answers the call via the main station and starts two-way audio.

Note

The device will call the main station in priority.

7.12.3 Call Device from Client Software

Steps

1. Get the client software from the supplied disk or the official website, and install the software according to the prompts.
2. Run the client software and the control panel of the software pops up.
3. Click **Device Management** to enter the Device Management page.
4. Add the device to the client software.

Note

For details about adding device, see *Add Device*.

5. Enter the **Live View** page and double-click the added device to start live view.

Note

For details about operations in the **Live View** page, see *Live View* in the user manual of the client software.

6. Right click the live view image to open the right-click menu.
7. Click **Start Two-Way Audio** to start two-way audio between the device and the client software.

7.12.4 Call Room from Device

Steps

1. Get the client software from the supplied disk or the official website, and install the software according to the prompts.
2. Run the client software and the control panel of the software pops up.
3. Click **Device Management** to enter the Device Management interface.
4. Add the indoor station and the device to the client software.

Note

For details about adding device, see *Add Device*.

5. Link a user to an indoor station and set a room No. for the indoor station.
6. Call the room.
   - If you have configured a specified room No. in the ***Basic Settings*** , you can tap to call the room.
   - If you have not configured a specified room No. in the ***Basic Settings*** , you should tap on the authentication page of the device. Enter the room No. on the dial page and tap to call the room.
7. After the indoor station answers the call, you can start two-way audio with the indoor station.

7.12.5 Call Mobile Client from Device

Steps

1. Get the mobile mobile client from the supplied disk or the official website, and install the software according to the prompts.
2. Run the mobile client and add the device to the mobile client.

Note

For details, see the user manual of the mobile client.

3. Enter **Basic Settings → Shortcut Key** and enable **Call APP**.
4. Go back to the initial page and call the mobile client.
   1) Tap on the device initial page.
   2) Tap to call the mobile client.

Chapter 8 Operation via Web Browser

8.1 Login

You can login via the web browser or the remote configuration of the client software.

Note

Make sure the device is activated. For detailed information about activation, see ***Activation*** .

Login via Web Browser

Enter the device IP address in the address bar of the web browser and press **Enter** to enter the login page.

Enter the device user name and the password. Click **Login**.

Login via Remote Configuration of Client Software

Download and open the client software. After adding the device, click to enter the Configuration page.

8.2 Forget Password

If you forget the password when logging in, you can change the password by email address or security questions.

On the login page, click **Forget Password**.

Select **Verification Mode**.

Security Question Verification

Answer the security questions.

E-mail Verification

1. Export the QR code and send it to ***pw_recovery@hikvision.com*** as attachment.
2. You will receive a verification code within 5 minutes in your reserved email.
3. Enter the verification code into the verification code field to verify your identification.

Click **Next**, create a new password and confirm it.

8.3 Download Web Plug-In

Both non-Plug-in live view and live view after downing plug-in are available. For better live view, downloading plug-in for live view is recommended.

Click → **Download Web Pug-In** to download the pulg-in to the local.

8.4 Help

8.4.1 Open Source Software Licenses

You can view open source software licenses.

Click → **Open Source Software Statement** on the upper-right corner to view the licenses.

8.4.2 View Online Help Document

You can view the help document for Web configuration.

Click → **Online Document** on the upper right of the Web page to view the document.

8.5 Logout

Log out the account.

Click **admin → Logout → OK** to logout.

8.6 Quick Operation via Web Browser

8.6.1 Change Password

You can change the device password.

Click on the top right of the web page to enter the **Change Password** page. You can set security questions from the drop-down list and fill in the answers.

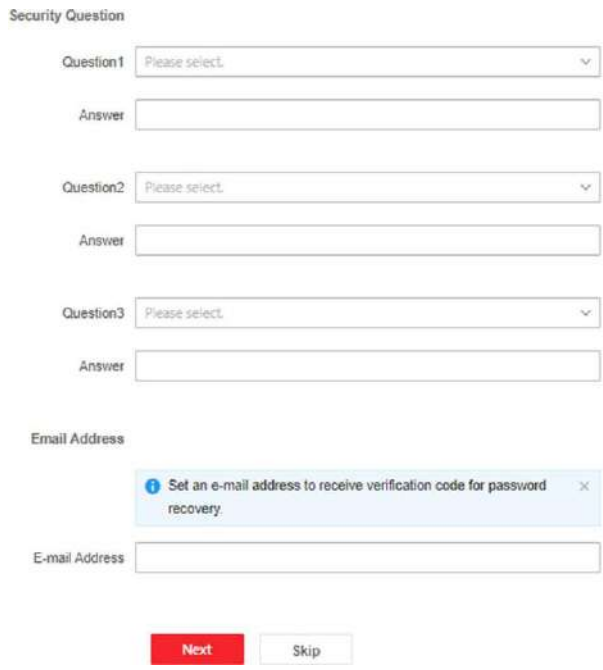


Figure 8-1 Change Password

Click **Next** to complete the settings. Or click **Skip** to skip the step.

8.6.2 Select Language

You can select a language for the device system.

Click in the top right of the web page to enter the **Device Language Settings** page. You can select a language for the device system from the drop-down list.

By default, the system language is English.

Note

After you change the system language, the device will reboot automatically.

8.6.3 Time Settings

Click in the top right of the web page to enter the wizard page. After setting device language, you can click **Next** to enter the **Time Settings** page.

Time Zone

Select the device located time zone from the drop-down list.

Time Sync.

NTP

You should set the NTP server's IP address, port No., and interval.

Manual

By default, the device time should be synchronized manually. You can set the device time manually or check **Sync. with Computer Time** to synchronize the device time with the computer's time.

Server Address/NTP Port/Interval

You can set the server address, NTP port, and interval.

DST

You can view the DST start time, end time and bias time.

Click **Next** to save the settings and go to the next parameter. Or click **Skip** to skip time settings.

8.6.4 Environment Settings

After activating the device, you should select an application mode for better device application.

Steps

1. Click in the top right of the web page to enter the wizard page. After setting device language and time, you can click **Next** to enter the **Environment Settings** page.
2. Select **Indoor** or **Other**.

Note

- If you install the device indoors near the window or the face recognition function is not working well, select **Others**.
- If you do not configure the application mode and tap **Next**, the system will select **Indoor** by default.
- If you activate the device via other tools remotely, the system will select **Indoor** as the application mode by default.

Click **Next** to save the settings and go to the next paramater. Or click **Skip** to skip environment settings.

8.6.5 Privacy Settings

Set the picture uploading and storage parameters.

Click in the top right of the web page to enter the wizard page.

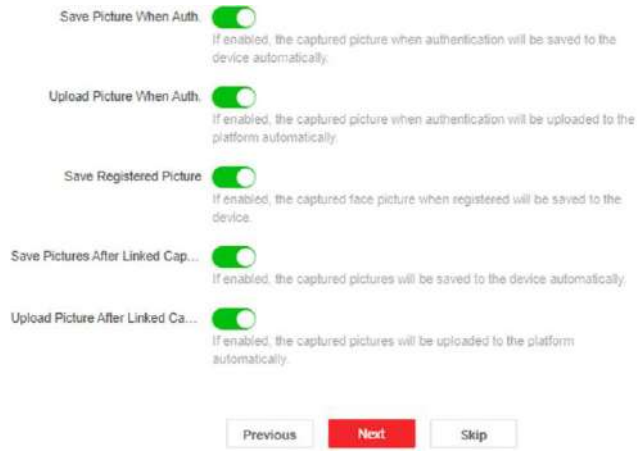


Figure 8-2 Privacy Settings

Picture Uploading and Storage

Save Picture When Authenticating

Save picture when authenticating automatically.

Upload Picture When Authenticating

Upload the pictures when authenticating to the platform automatically.

Save Registered Picture

The registered face picture will be saved to the system if you enable the function.

Upload Picture After Linked Capture

Upload the pictures captured by linked camera to the platform automatically.

Save Pictures After Linked Capture

If you enable this function, you can save the picture captured by linked camera to the device.

Click **Next** to save the settings and go to the next parameter. Or click **Skip** to skip privacy settings.

8.6.6 Administrator Settings

Steps

1. Click in the top right of the web page to enter the wizard page.
2. Enter the employee ID and name of the administrator.
3. Select a credential to add.

Note

You should select at least one credential.

1) Click **Add Face** to upload a face picture from local storage.

Note

The uploaded picture should be within 200 K, in JPG、JPEG、PNG format.

2) Click **Add Card** to enter the Card No. and select the property of the card.

Note

Up to 5 cards can be supported.

3) Click **Add Fingerprint** to add fingerprints.

Note

Up to 10 fingerprints are allowed.

Click **Complete** to complete the settings.

8.6.7 No. and System Network

Steps

1. Click in the top right of the web page to enter the wizard page. After previous settings, you can click **Next** to enter the **No. and Network System Network** settings page.
2. Set the device type.

Note

- If set the device type as **Door Station**, you can set the **Floor No.**, **Door Station No.**, **Community No.**, **Building No.**, **Unit No.**, **Floor No.**, and **Door Station No.**.
- If set the device type as **Outer Door Station**, you can set **Outer Door Station No.**, and **Community No.**

Device Type

The device can be used as a door station or outer door station. Select a device type from the drop-down list.

Community No.

Set the device community No.

Building No.

Set the device building No.

Unit No.

Set the device unit No.

Floor No.

Set the device installed floor No.

Door Station No.

Set the device installed door station No.

Note

The main door station No. is 0, and the sub door station No. ranges from 1 to 16.

Outer Door Station No.

Set the device installed outer door station No.

Note

The No. ranges from 1 to 99.

3. Set the video intercom network parameters.

Registration Password

Set the registration password of the main station for communication. Set the registration password of the main station for communication.

Main Station IP

Enter the main station's IP address that used for communication.

Private Server IP

Refers to the SIP server IP. Enter the main station's IP address that used for communication. At this time the main station is used as a SIP server. Other intercom devices should registered to this server address to realize communication.

Enable Protocol 1.0

If enabled, the door station can be registered to the main station by old protocol version. If disabled, the door station can be registered to the main station by new protocol version.

4. Click **Complete** to save the settings after the configuration.

8.7 Person Management

Click **Add** to add the person's information, including the basic information, certificate, authentication and settings.

Add Basic Information

Click **Person Management → Add** to enter the Add Person page.
Add the person's basic information, including the employee ID, the person's name, gender, and person type.
If you select **Visitor** as the person type, you can set the visit times.
If you select **Custom Type**, you can edit the name. The changed name will be applied to the device.
Click **Save** to save the settings.

Set Permission Time

Click **Person Management → Add** to enter the Add Person page.

Enable **Long-Term Effective User**, or set **Long-Term Effective User**, and the person can only has the permission within the configured time period according to your actual needs.
Set the door permission.
Click **Save** to save the settings.

Set Device No.

Click **Person Management → Add Person → Add** to enter the Add Person page.
Click the textbox of **Floor No.** and **Room No.** and enter a numeric between 1 and 999 to set the floor No. and room No.
Click **Save** to save the settings.

Authentication Settings

Click **Person Management → Add** to enter the Add Person page.
Set the authentication type.
Click **Save** to save the settings.

Add Card

Click **Person Management → Add** to enter the Add Person page.
Click **Add Card**, enter the **Card No.** and select the **Property**, and click **OK** to add the card.
Click **Save** to save the settings.

Add Face Picture

Click **Person Management → Add** to enter the Add Person page.
Click **+ Upload** to upload a face picture from the local PC.

Note
The picture format should be JPG or JPEG or PNG, and the size should be less than 200 kb.

Click **Save** to save the settings.

Add Fingerprint

Note
Only devices supporting the fingerprint function can add the fingerprint.

Click **Person Management → Add** to enter the Add Person page.
Click **Add Fingerprint**, and press your finger on the fingerprint module of the device to add your fingerprint.
Click **Save** to save the settings.

Add Palm Print

Note

- Only devices supporting the palm print function can add the palm print.
- Up to 10000 palm print and palm vein can be added.

Click **Person Management → Add Palm Print** to enter the Add Person page.
Place the palm at a distance of 5 ~ 12 cm from the peripheral module of the device.
Click **Save** to save the settings.

Add Keyfob

Click **Person Management → Add** to enter the Add Person page.
Click **+ Add Keyfob**, and enter Serial No, click **OK**. Press and hold keys in the upper left and lower right corners of keyfob for 10 s to pair with face recognition terminal.

Note

Each person can add up to one keyfob, and the device can add up to 5,000 keyfobs. The keyfob serial No. starts with Q-Z followed by 8-digit Arabic numerals.

Device No. Settings

Click **Person Management → Add** to enter the Add Person page.
Add the person's basic information. Go to the Device No. module. Click **Add** and enter the person belonged room No. and floor No. Click **Add** or **Save and Continue**.

Delete Person

On the person management page, check the person need to delete and click **Delete**.
Click **Clear All** to clear all person.

Edit Person

On the person management page, check the person need to edit. Click to edit the person information.

Filter

On the person management page, enter **Employee ID / Name / Card No.**. Select **Credential Status**, and click **Filter** to filter the person. Click **Reset** to clear all conditions.

8.8 Access Control Management

8.8.1 Overview

You can view the live video of the device, linked device, person information, network status, basic information, and device capacity.

Function Descriptions:

Door Status

Click on the video to view the device live video.

Set the volume when starting live view.

Note

If you adjust the volume when starting two-way audio, you may hear a repeated sounds.

You can capture image when starting live view.

/ / /

The door status is open/closed/remaining open/remaining closed.

You can record when starting live view.

Select the streaming type when starting live view. You can select from the main stream, sub stream or third stream.

Full screen view.

Controlled Status

You can control the door to be opened, closed, remaining open or remaining closed according to your actual needs.

Real-Time Event

You can view the event Employee ID, Name, Card No., Event Type, Time, and Operation. You can also click **View More** to enter the page of Event Search. You can select event types, enter the employee ID, the name, the card No., the start time, and the end time, and click **Search**. The results will be displayed on the right panel.

Link Device

You can view the quantity and status of linked devices.

Note

You can click **View More** to go to .

Person Information

You can view the added and not added information of person credentials.

Network Status

You can view the connected and registered status of wired network, wireless network, Hik-Connect, ISUP, OTAP, and VoIP.

Basic Information

You can view the model, serial No. and firmware version.

Device Capacity

You can view the person, face, fingerprint, card, palm print and event capacity.

Note

Only device installed fingerprint or palm print module can display the fingerprint or palm print capacity.

8.8.2 Search Event

Click **Event Search** to enter the Search page.

Enter the search conditions, including the event type, the employee ID, the name, the card No., the start time, and the end time, and click **Search**.

The results will be displayed on the right panel.

8.8.3 Door Parameter Configuration

Configure parameters for unlocking doors.

Select Door No.

Select a door to configure relative parameters.

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.

Select **Door No.**. Usually, Door 1 is the door linked with the device and door 2 is the door linked with the secure door control unit.

Set other door parameters and click **Save**.

View Device Online Status

View and refresh the device status.

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.

You can view the online status of the device. Click **Refresh** to refresh the status of the device.

Set Door Name

Create door name.

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.

Set **Door Name** and click **Save**.

Set Open Duration via PC Web

You can set the time for the door lock to open after swiping the card.

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.

Set the open duration, that is the action time after the door is unlocked. If the door is not opened within the set time, the door will automatically lock. Configurable time: 1 to 255 seconds.

Click **Save**.

Set Door Open Timeout Alarm via PC Web

If the door is not closed after reaching the lock action time, the access control point will sound an alarm.

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.

Set **Door Open Timeout Alarm**. If the door is not closed after reaching the lock action time, the access control point will sound an alarm. When set as 0, alarm will not be enabled.

Click **Save**.

Set Door Magnetic Sensor Type via PC Web

You can select door contact type according to the wiring method.

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.

Select magnetic sensor type as remain closed or remain open. By default, it is **Remain Closed** (excluding special needs).

Click **Save**.

Set Exit Button via PC Web

Set the exit button as remain open or remain closed according to the actual wiring method.

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.

Set **Exit Button Type**. By default, it is Remain Open (excluding special needs).

Click **Save**.

Set Door Lock Powering Off Status via PC Web

You can set the door lock status when the door lock is powering off.

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.

Set **Door Lock Powering Off Status**. By default, it is remain closed.

Click **Save**.

Set Extended Open Duration via PC Web

The door contact can be enabled with appropriate delay after person with extended access needs swipes her/his card.

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.

Set **Extended Open Duration**. The door contact can be enabled with appropriate delay after person with extended access needs swipes her/his card.

Click **Save**.

Set Door Remain Open Duration with First Person via PC Web

After the first person is authorized, it allows multiple persons access the door or other authentication actions.

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.

Set the door open duration when first person is in and click **Save**.

Set Duress Code via PC Web

After configuring duress code, when encountering duress, enter the code to open the door. At the same time, the access control system will report duress events.

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.

Set duress code, and click **Save**.

Note

Duress code and super password can't be duplicated, usually consisting of 4 to 8 digits.

Set Super Password via PC Web

Administrator or designated person can enter the super password to open the door.

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.

Set **Super Password**, the designated person can enter the super password to open the door.

Click **Save**.

Note

Duress code and super password can't be duplicated, usually consisting of 4 to 8 digits.

8.8.4 Authentication Settings

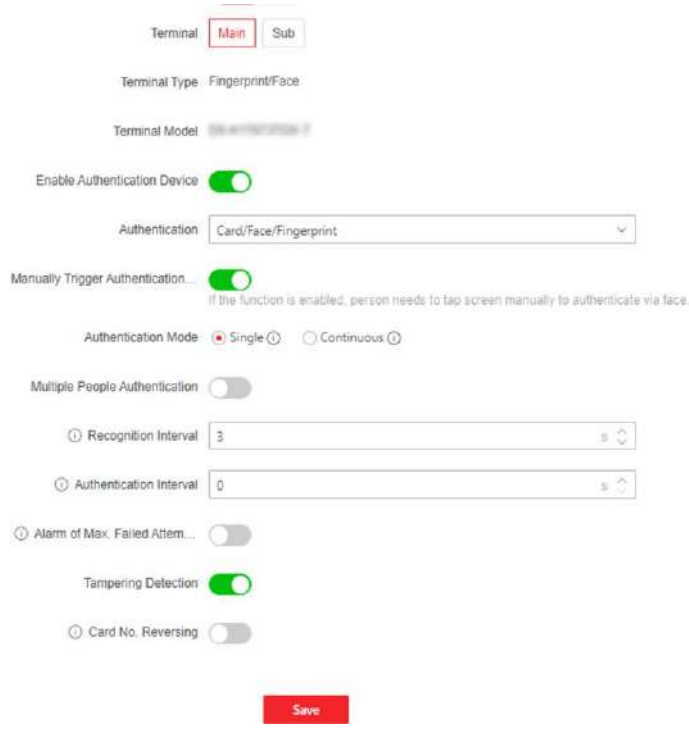


Figure 8-3 Authentication Settings

Select Main or Sub Card Reader via PC Web

Set the terminal for person authentication.

Click **Access Control → Parameter Settings → Authentication Settings** to enter the settings page.

Select the terminal as main or sub card reader.

Set other parameters and click **Save**.

View Terminal Type and Model via PC Web

You can view terminal type and model.

Click **Access Control → Parameter Settings → Authentication Settings** to enter the settings page.

View **Terminal Type** and **Terminal Model**.

Enable Authentication Device via PC Web

After enabling, the authentication terminal can be used for card swiping.

Steps

1. Click **Access Control → Parameter Settings → Authentication Settings** to enter the settings page.
2. Enable **Authentication Device**. After enabling, the terminal can be used for card swiping normally.
3. Click **Save**.

Set Authentication via PC Web

Configure Certification.

Click **Access Control → Parameter Settings → Authentication Settings** to enter the settings page.

When selecting main card reader as the Terminal, you can select Authentication from the drop-down list. When there is more than one authentication, you should set **Single Credential Authenticating Timeout** and **Control Initial Authentication Type**.

Single Credential Authenticating Timeout

You can configure the duration for each certification.

Note

The password authenticating timeout is 20 s by default, which is not limited by above settings.

Control Initial Authentication Type

If enabled, all selected types can be used for first-time authentication.

When selecting sub card reader as the Terminal, you can select Authentication from the drop-down list.

Click **Save**.

Manually Trigger Authentication via Face on PC Web

After enabling**Manually Trigger Authentication via Face**, you need to touch the screen of the device manually for face recognition.

Click **Access Control → Parameter Settings → Authentication Settings** to enter the settings page.

When the main card reader is selected as the Terminal, click to enable **Manually Trigger Authentication via Face** and choose authentication mode.

Single Recognition

After completing the previous facial recognition, no matter successful or failed, you need to tap the screen to trigger the next recognition.

Continuous

After triggering the recognition, you can recognize via face until the device enter into the sleeping mode.

Click **Save**.

Enable Multiple People Authentication via PC Web

When enabled, multiple people can simultaneously verify faces for authentication.

Click **Access Control → Parameter Settings → Authentication Settings** to enter the settings page.

When you select the terminal as main card reader, enable **Multiple People Authentication**, and click **Save**.

Set Recognition Interval via PC Web

Set the time interval between two continuous face recognitions when authenticating.

Click **Access Control → Parameter Settings → Authentication Settings** to enter the settings page.

When you select the terminal as main or sub card reader, set recognition interval, and click **Save**.

Note

Please enter a number between 1 and 10.

Set Authentication Interval via PC Web

You can set the authentication interval of the same person when authenticating. The same person can only authenticate once in the configured interval. A second authentication will be failed. If other person authenticate in the configured interval, the person can authenticate again.

Click **Access Control → Parameter Settings → Authentication Settings** to enter the settings page.

When you select the terminal as main card reader, set **Authentication Interval**, and click **Save**.

Enable Alarm of Max. Failed Attempts via PC Web

Enable to report alarm when the card reading attempts reach the set value.

Click **Access Control → Parameter Settings → Authentication Settings** to enter the settings page.

When you select the terminal as main or sub card reader, slide to enable **Alarm of Max. Failed Attempts**, and set **Max. Authentication Failed Attempts**.

Click **Save**.

Set Palm Print Recognition Timeout Threshold and Recognition Interval via PC Web

Set palm print recognition timeout threshold and the interval between two continuous palm print recognition when authenticating.

Click **Access Control → Parameter Settings → Authentication Settings** to enter the settings page.

When you select the terminal as main or sub card reader, set **Palm Print Recognition Timeout Threshold** and **Palm Print Recognition Interval**, and click **Save**.

Enable/Disable Tampering Detection via PC Web

You can enable tampering detection, the device will automatically generate tampering events when the card reader is removed or taken away.

Click **Access Control → Parameter Settings → Authentication Settings** to enter the settings page.

Enable or disable **Tampering Detection** according to your actual needs. After enabling the function, the device will automatically generate tampering events when the card reader is removed or taken away. If the function is disabled, no alarm events will be generated.

Click **Save**.

Enable/Disable Card No. Reversing via PC Web

You can enable or disable the card No. reversing function.

Click **Access Control → Parameter Settings → Authentication Settings** to enter the settings page.

Enable **Card No. Reversing**, the read card No. will be in reverse sequence.

Click **Save**.

Set Sub Card Reader Position

You can choose the position for the sub card reader.

Click **Access Control → Parameter Settings → Authentication Settings** to enter the settings page.

When Sub Card Reader is selected as the Terminal, you can select the position of sub card reader as **Different Side from Main Card Reader**or**Same Side as Main Card Reader**. Click**Save**.

Set Communication with Controller Every via PC Web

You can set communication with controller every of sub card reader. If the card reader can't connect with the access controller in the set time, the card reader is offline.

Click **Access Control → Parameter Settings → Authentication Settings** to enter the settings page.

When you select the terminal as sub card reader, set **Communication with Controller Every**, and click **Save**.

Set Timeout Duration of Entering Password via Web Client

Set the maximum interval of entering two characters of the password. After entering one character, if the next character is not entered within the set interval, the entered characters will all be automatically cleared.

Click **Access Control → Parameter Settings → Authentication Settings** to enter the settings page.

When selecting the sub card reader as the Terminal, you can set **Max. Interval When Entering Password** and click**Save**.

Set OK LED Polarity and Error LED Polarity via PC Web

Select the polarity of the diodes for OK and ERR interfaces according to actual wiring, with a default positive polarity.

Click **Access Control → Parameter Settings → Authentication Settings** to enter the settings page.

When you select the terminal as sub card reader, set **OK LED Polarity** and **Error LED Polarity**, and click **Save**.

8.8.5 Set Face Parameters

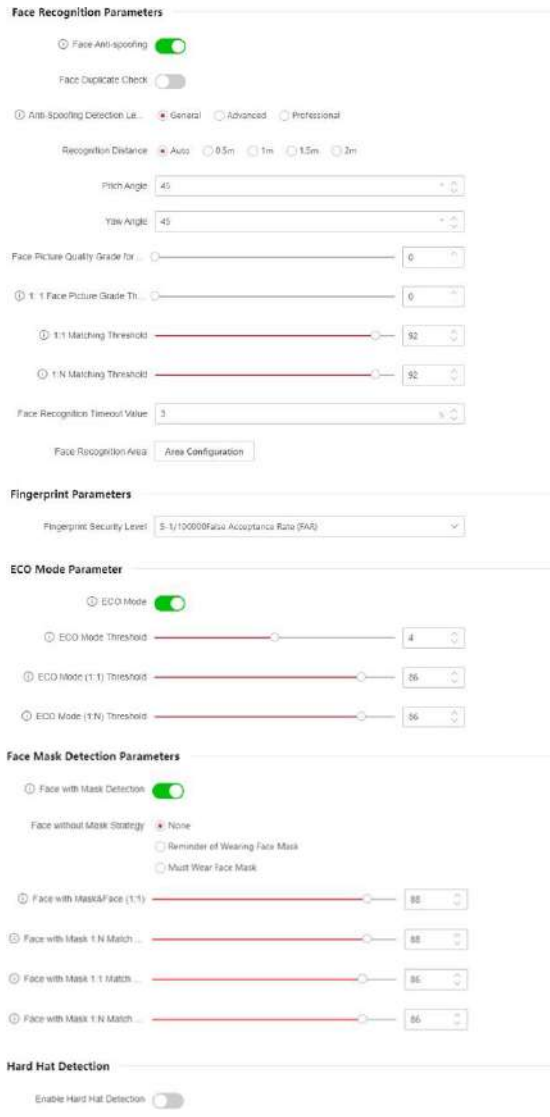


Figure 8-4 Set Face Parameters

Enable/Disable Face Anti-spoofing via Web Browser

When enabled, the device can recognize whether the person is a live one or not.

Click **Access Control → Parameter Settings → Smart** to enter the settings page.

Enable **Face Anti-spoofing** and click **Save**.

Enable or disable the live face detection function. When enabled, the device can recognize whether the person is a live one or not. If the face is not a live one, authentication will fail.

Enable/Disable Face Duplicate Check

After enabling face duplicate check and everytime adding person's face, the system will check the face's duplication. If a duplicated face is detected, a prompt will be on.

Note

The function is not supported when add face remotely or applying face in batch.

Click **Access Control → Parameter Settings → Smart** to enter the settings page.

Enable **Face Duplicate Check**.

Click **Save**.

Set Anti-Spoofing Detection Level via PC Web

After enabling the face anti-spoofing function, you can set the matching security level when performing live face authentication.

Click **Access Control → Parameter Settings → Smart** to enter the settings page.

Select the anti-spoofing detection level and click **Save**.

You can choose from general, advanced and professional. The higher the level, the lower the fake recognition rate and the higher the rejection rate.

Set Recognition Distance via PC Web

You can set the distance between the authenticating user and the device camera.

Click **Access Control → Parameter Settings → Smart** to enter the settings page.

Select the recognition distance, and click **Save**.

Set Pitch Angle via PC Web

You can set the pitch angle of the lens during face recognition and authentication.

Click **Access Control → Parameter Settings → Smart** to enter the settings page.

Note

Different models may support different parameters, please refer to the actual page.

Set **Pitch Angle** and click **Save**.

Set Yaw Angle via PC Web

You can set the yaw angle of the lens during face recognition and authentication.

Click **Access Control → Parameter Settings → Smart** to enter the settings page.

Note

Different models may support different parameters, please refer to the actual page.

Set yaw angle, and click **Save**.

Set Face Picture Quality Grade for Applying via PC Web

The grade for face authentication needs to be higher than the threshold to be successful.

Click **Access Control → Parameter Settings → Smart** to enter the settings page.

Note

Different models may support different parameters, please refer to the actual page.

Set **Face Picture Quality Grade for Applying** , the grade for face authentication needs to be higher than the threshold to be successful.

Click **Save**.

Set 1:1 Face Grade Threshold via PC Web

Set 1:1 face grade threshold.

Go to **Access Control → Parameters Settings → Smart** .

Set **1:1 Face Picture Grade Threshold**, and click **Save**.

The higher the threshold, the higher the requirements for the quality of the captured images of the front camera, and the easier to prompt authentication failure.

Set Face 1:1 Matching Threshold via PC Web

Set face 1:1 matching threshold.

Click **Access Control → Parameter Settings → Smart** to enter the settings page.

Set face 1:1 matching threshold and click **Save**.

The larger the value of the threshold, the fault acceptance rate will be lower and the false rejection rate will be higher when authenticating via face. The maxium value is 100.

Set 1:N Matching Threshold via PC Web

You can set the matching threshold for face 1:N matching.

Click **Access Control → Parameter Settings → Smart** to enter the settings page.

Set the 1:N matching threshold and click **Save**.

The larger the value, the smaller the false accept rate and the larger the false rejection rate. The maximum value is 100.

Set Face Recognition Area via Web Browser

You can set the recognition area of the lens during face recognition and authentication.

Click **Access Control → Parameter Settings → Area Configuration** to enter the settings page.

Drag the yellow box in the preview screen to adjust the effective area for face recognition on the left, right, up, and down sides.

Or drag the block or enter the number to set the effective area.

Click **Save**.

Click , , or to capture, record, or go to full screen view.

Set Fingerprint Parameters via PC Web

You can set the fingerprint parameters of the device.

Click **Access Control → Parameter Settings → Smart** to enter the settings page.

Select **Fingerprint Security Level**. The higher the level, the lower the fake recognition rate and the higher the rejection rate.

Click **Save**.

Set Palm Print Recognition Parameters via PC Web

You can set the palm print parameters of the device.

Click **Access Control → Parameter Settings → Smart** to enter the settings page.

Enable **Palm Print Anti-Spoofing Detection**. Set **Palm Print 1:1 Threshold** and **Palm Print 1:N Threshold**.

Note

The larger the value, the smaller the false accept rate and the larger the false rejection rate. The maximum value is 100.

Click **Save**.

Enable/Disable ECO Mode via PC Web

If the ECO mode is enabled, you can authenticate faces in the low light or dark environment with IR camera.

Click **Access Control → Parameter Settings → Smart** to enter the settings page.

If the ECO mode is enabled, you can authenticate faces in the low light or dark environment with IR camera. You can set the ECO mode (1:N) and ECO mode (1:1).

If the face with mask detection is enabled, you can set face mask detection parameters also.

ECO Mode (1:1) Threshold

Set the matching threshold when authenticating via ECO mode 1:1 matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate. The maximum value is 100.

ECO Mode (1:N) Threshold

Set the matching threshold when authenticating via ECO mode 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate. The maximum value is 100.

Face with Mask 1:1 Match Threshold (ECO)

Set the matching threshold when authenticating with face mask via ECO mode 1:1 matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate. The maximum value is 100.

Face with Mask 1:N Match Threshold (ECO)

Set the matching threshold when authenticating with face mask via ECO mode 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate. The maximum value is 100.

Click **Save**.

Enable/Disable Face with Mask Detection via PC Web

After enabling the face with mask detection, the system will recognize the captured face with mask picture or not.

Click **Access Control → Parameter Settings → Smart** to enter the settings page.

After enabling the face with mask detection, you can set **Face without Mask Strategy**, **Face with Mask&Face (1:1)**, **Face with Mask 1:N Match Threshold (ECO)**, **Face with Mask 1:1 Match Threshold** and **Face with Mask 1:N Match Threshold (ECO)**.

Face without Mask Strategy

You can select **None**, **Reminder of Wearing Face Mask** and **Must Wear Face Mask**.

Reminder of Wearing Face Mask

If the person do not wear the face mask when authenticating, the device will pop up a prompt and the door will open.

Must Wear Face Mask

If the person do not wear the face mask when authenticating, the device will pop up a prompt and the door will keep closed.

Face with Mask&Face (1:1)

Set the matching value when authenticating with face mask via 1:1 matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate. The maximum value is 100.

Face with Mask&Face (1:N)

Set the matching threshold when authenticating with face mask via 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate. The maximum value is 100.

Face with Mask 1:1 Match Threshold (ECO)

Set the matching value when authenticating with face mask via ECO mode 1:1 matching mode. The larger the threshold, the lower the recognition error rate and the higher the rejection rate when authenticating faces. The maximum value is 100.

Face with Mask 1:N Match Threshold (ECO)

Set the matching value when authenticating with face mask via ECO mode 1:N matching mode. The larger the threshold, the lower the recognition error rate and the higher the rejection rate when authenticating faces. The maximum value is 100.

Click **Save**.

Enable/Disable Hard Hat Detection via PC Web

After enabling the hard hat detection, the system will recognize whether the safety helmet is worn when authenticating faces.

Click **Access Control → Parameter Settings → Smart** to enter the settings page.

Enable **Hard Hat Detection** and click **Save**.

Enable Hard Hat Detection

You can set the reminder strategy.

Reminder of Wearing

If the person do not wear the hard hat when authenticating, the device will pop up a prompt and the door will open.

Must Wear

If the person do not wear the hard hat when authenticating, the device will pop up a prompt and the door will keep closed.

8.8.6 Card Settings

Enable/Disable NFC Protection via PC Web

After enabling, the device can read NFC card.

Click **Access Control → Parameter Settings → Card Settings** to enter the settings page.

Click to **Enable NFC Card** and click **Save**. After enabling, the device can read NFC card. If the data of access control devices is obtained by mobile devices, the situation of unauthenticated access may occur. To prevent this situation, you can disable NFC function.

Enable/Disable M1 Card via Web Client

After enabling, the device can recognize M1 card and users can swipe M1 card via the device.

Click **Access Control → Parameter Settings → Card Settings** to enter the settings page.

Click to **Enable M1 Card**.

M1 Card Encryption

Enable M1 Card Encryption can improve the security level of the entrance card. Therefore, the entrance card will be harder to be copied.

Sector

After enabling M1 Card Encryption, you will need to set the encrypted sector.

Note

You are advised to encrypt sector 13.

Click **Save**.

Enable/Disable EM Card via Web Client

After enabling, the device can recognize EM card and users can swipe EM card via the device.

Click **Access Control → Parameter Settings → Card Settings** to enter the settings page.

Click to **Enable EM Card** and click **Save**.

Note

- If the peripheral card reader which can read EM card is connected, after enabling this function, you can also swipe EM card via this card reader.
- When a Dual-frequency Card Module is connected, you can swipe both the EM card and the DESfire card at the same time. However, swiping the card on the device is invalid.

Enable/Disable CPU Card via Web Client

After enabling, the device can recognize CPU card and users can swipe CPU card via the device.

Click **Access Control → Parameter Settings → Card Settings** to enter the settings page.

Click to **Enable CPU Card**.

Click to **Enable CPU Card Read Content**. After enabling, the device can read content from CPU card.

Click **Save**.

Set DESFire Card

You can enable DESFire card and DESFire card read content.

Click **Parameter Settings → Card Settings** to enter the settings page.

Select **Enable DESFire Card** and **DESFire Card Read Content**and click **Save**.

Note

When a Dual-frequency Card Module is connected, you can swipe both the EM card and the DESfire card at the same time. However, swiping the card on the device is invalid.

Set FeliCa Card

You can enable FeliCa card.

Click **Parameter Settings → Card Settings** to enter the settings page.

Select **Enable FeliCa Card**.

Set Card No. Authentication Parameters via Web

Set the card reading content when authenticate via card on the device.

Go to **Access Control → Parameter Settings → Card Settings** .

Select a card authentication mode and click **Save**.

Full Card No.

All card No. will be read.

3 bytes

The device will read card via read 3 bytes.

4 bytes

The device will read card via 4 bytes.

8.8.7 Elevator Control via Web

Steps

1. Click **Access Control → Parameter Settings → Elevator Control Parameters** .

Figure 8-5 Elevator Control

2. Enable **Elevator Control**.
3. Set the elevator parameters.

Main Elevator Controller Model

Select an elevator No. for configuration.

Interface Type

Select a communication type from the drop-down list for elevator communication.

If you select **RS-485**, make sure you have connected the device to the elevator controller with RS-485 wire.

If you select **Network Interface**, enter the elevator controller's IP address, port No., user name, and password for communication.

Negative Floor Capacity

Set the negative floor number.

Installation Location

Select installation location as **Out of Elevator Cab** or **In Elevator Cab**.

Call Elevator Mode

Select call elevator mode.

Call Elevator Only

After the person passes authentication, the device will call elevator to its floor.

Call Elevator + Authorize

After the person passes authentication, the device will call elevator to its floor and authorize the permission of the floor linked to the person's room. The person can get to the target floor by pressing corresponding floor No.

Note

- Up to 4 elevator controllers can be connected to 1 device.
- Up to 10 negative floors can be added.
- Make sure the interface types of elevator controllers, which are connected to the same device, are consistent.

8.8.8 Linkage Settings

When the configured event is triggered, upload the event information to the central platform according to the configured method.

Steps

1. Click **Access Control → Parameter Settings → Linkage Settings** to enter the settings page.

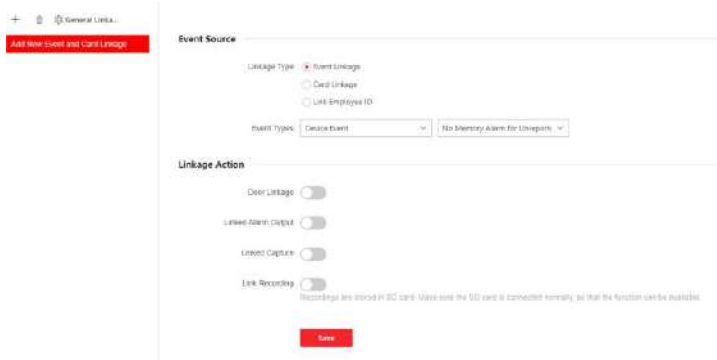


Figure 8-6 Linkage Settings

2. Click **+** .

3. Set event source. Select the linkage type as **Event Linkage**, **Card Linkage** or **Link Employee ID**.

- Select **Linkage Type** as **Event Linkage**, you can select event types according to your actual needs.
- Select **Linkage Type** as **Card Linkage**, enter **Card No.** and select **Card reader**.
- Select **Linkage Type** as **Link Employee ID**, enter **Employee ID** and select **Card reader**.

4. Set linkage action.

1) Enable **Door Linkage**, check and select door action.
2) Enable **Linked Alarm Output**, check and select alarm output action.
3) Enable **Linked Capture**.
4) Enable **Link Recording**, click **General Linkage Settings** to set pre-record time and recording delay, and enable record audio when recording video. Click **Save**.

Note

To use the recording function, you need to prepare the SD card. After recording, you can click **Event Search** to view recordings. For details, see ***Search Event***

5. Click**Save** to enable the settings.

8.8.9 Set Working Mode via PC Web

You can set the terminal parameters of the device.

Note

Only some models support this function, please refer to the specific device.

Click **Access Control → Parameter Settings → Terminal Parameters** to enter the settings page.

Working Mode

You can set the working mode as access control mode or permission free mode.

Access Control Mode

The access control mode is the device normal mode. You should authenticate your credential for accessing.

8.8.10 Set Remote Verification

The device will upload the person's authentication information to the platform. The platform will judge to open the door or not.

Go to **Access Control → Parameter Settings → Terminal Parameters**.

Click**Save** after parameters are configured.

Remote Verification

After enabling the remote verification, when authenticating, the device will upload authentication information to the platform, and the platform will confirm whether to open the door.

Verify Credential Locally

After enabling the function, the device will check permission but not estimate the plan template.

8.8.11 Privacy Settings

Set Event Storage Type via PC Web Browser

You can configure the event storage type.

Click **Access Control → Parameter Settings → Privacy Settings** to enter the settings page.

You can select **Event Storage Type** as **Delete Old Events Periodically**, **Delete Old Events by Specified Time** or **Overwriting**.

Delete Old Events Periodically

Drag the block or enter number to set the period for event deleting. All events will be deleted according to the configured time duration.

Delete Old Events by Specified Time

Set a time and all events will be deleted on the configured time.

Overwriting

The earliest 5% events will be deleted when the system detects the stored events has been over 95% of the full space.

Click **Save**.

Set Authentication Result via PC Web

Set authentication result contents, such as picture, name, employee ID, and temperature.

Click **Access Control → Access Control → Parameter Settings → Privacy Settings** .

Check the displayed contents in the authentication result, such as picture, name, employee ID.

Check **Name De-identification** and **ID De-identification** according to actual needs. After de-identification, the name and the ID will display parts of contents.

Set **Authentication Result Display Duration** and the authentication result will display the configured time duration.

Click **Save**.

Configure Picture Uploading and Storage via PC Web

You can set picture uploading and storage parameters.

Click **Access Control → Parameter Settings → Privacy Settings** to enter the settings page.

Save Picture When Auth.

Save picture when authenticating automatically.

Upload Picture When Auth.

Upload the pictures when authenticating to the platform automatically.

Picture Mode

When selecting as default, the device will capture the panoramic view. You can set the Max. picture size and picture resolution.

When selecting as matting picture mode, the devicel will only capture face. You can set the Max. picture size.

Save Registered Picture

The registered face picture will be saved to the system if you enable the function.

Save Pictures After Linked Capture

If you enable this function, you can save the picture captured by linked camera to the device.

Upload Picture After Linked Capture

Upload the pictures captured by linked camera to the platform automatically

Store Palm Print Registered Picture

If you disable this, only palm print data will be stored, and registered picture will not be stored.

Click **Save**.

Clear Device Pictures via PC Web

You can clear all registered, authenticated or captured face or pictures.

Click **Access Control → Parameter Settings → Privacy Settings** to enter the settings page.

Click **Clear** to clear all registered, authenticated, captured face pictures or palm print pictures.

Set PIN Mode via PC Web

Make sure the PIN is platform-applied personal PIN or device-set personal PIN before settings. If the PIN is device-set personal PIN, you can edit the PIN on the device or PC Web, but not set it on the platform. If the PIN is platform-applied personal PIN, you should set the PIN on the platform, but not on the device or PC Web.

Go to **Access Control → Parameter Settings → Privacy Settings**.

In the PIN Mode module, you can set the following parameters. Click **Save** after parameters settings.

Platform-Applied Personal PIN

You can create the person PIN on the platform. You should apply the PIN to the device. You cannot create or edit the PIN on the device or PC Web.

Device-Set Personal PIN

You can create or edit the PIN on the device or PC Web. You cannot set the PIN on the platform.

Click **Save**.

8.8.12 Call Settings

Set Device No. via Web

The device can be used as a door station or outer door station. You should set the device No. before usage.

Click **Access Control → Call Settings → Device No.** .

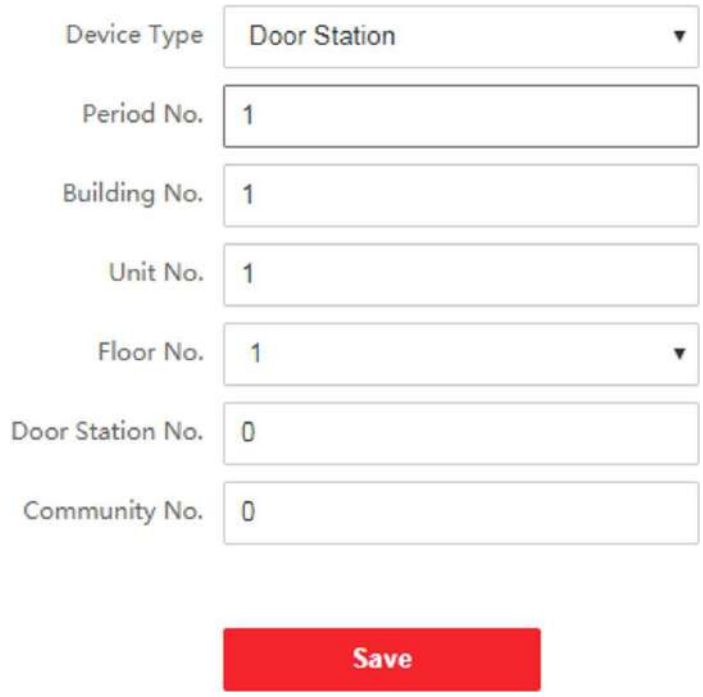


Figure 8-7 Device No. Settings

If set the device type as **Door Station**, you can set the **Floor No.**, **Door Station No.**, **Community No.**, **Building No.**, and **Unit No.**

Device Type

The device can be used as a door station or outer door station. Select a device type from the drop-down list.

Note

If you change the device type, you should reboot the device.

Floor No.

Set the device installed floor No.

Door Station No.

Set the device installed floor No.

Note

- If you change the No., you should reboot the device.
- The main door station No. is 0, and the sub door station No. ranges from 1 to 16.

Community No.

Set the device community No.

Building No.

Set the device building No.

Unit No.

Set the device unit No.

Note

If you change the No., you should reboot the device.

Click **Save** to save the settings after the configuration.

If set the device type as **Outer Door Station**, you can set outer door station No., and community No.

Outer Door Station No.

If you select outer door station as the device type, you should enter a number between **1** and **99**.

Note

If you change the No., you should reboot the device.

Community No.

Set the device community No.

Configure Video Intercom Network Parameters via Web Browser

You can set the registration password, main station IP and private server IP, and you can enable protocol 1.0 according to your actual needs.

Click **Call Settings → Video Intercom Network** to enter the settings page.

Registration Password

Set the registration password of the main station for communication. Set the registration password of the main station for communication.

Main Station IP

Enter the main station's IP address that used for communication.

Private Server IP

Refers to the SIP server IP. Enter the main station's IP address that used for communication. At this time the main station is used as a SIP server. Other intercom devices should registered to this server address to realize communication.

Enable Protocol 1.0

If enabled, the door station can be registered to the main station by old protocol version. If disabled, the door station can be registered to the main station by new protocol version.

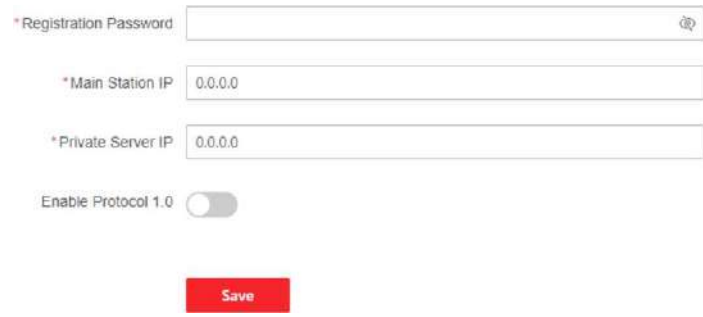


Figure 8-8 Video Intercom Network

After configuration, you can achieve communication between access control devices and video intercom door station, indoor station, main station, platforms, etc.

Click **Save**.

Set Communication Time via PC Web

Set the max. communication time.

Go to **Access Control → Call Settings → Call Settings** .

Enter the **Max. Communication Time**. Click **Save**.

Note

The Max. Communication time range is 90 s to 120 s.

Press Button to Call via PC Web

Steps

1. Click **Access Control → Call Settings → Press Button to Call** to enter the settings page.

Figure 8-9 Press Button to Call

2. Select **Call Specified Indoor Station**, **Call Management Center**, **Call Indoor Station** or **APP** at your needs.

Note

If you select **Call Specified Indoor Station**, you need to enter the **Room No.** of the indoor station.

3. Enable **Link Authentication to Call** according to your needs. After enabled, when person passes authentication, the door will be remotely opened by the target that is configured with button for automatic calling.
4. Click **Save**.

Number Settings via PC Web

Set SIP number for the room. The rooms can communicate with each other via SIP number.

Steps

1. Go to **Access Control → Call Settings → Number Settings**.

Figure 8-10 Number Settings

2. Click **Add**, and enter **Room No.** and **SIP1** phone number.
3. **Optional:** Click **Add** to add the SIP number or click to delete the number.
4. Click**Save**.
5. **Optional:** You can click **Delete** to delete room number and its SIP number.

8.9 System Configuration

8.9.1 View Device Information via PC Web

View the device name, device No., language, model, serial No., version, number of channels, IO input, IO output, lock, local RS-485 number, register number, alarm input, alarm output, and device capacity, etc.

Click **System and Maintenance → System Configuration → System → System Settings → Basic Information** to enter the configuration page.

You can view device name, device No., language, model, serial No., version, number of channels, IO input, IO output, lock, local RS-485 number, register number, alarm input, alarm output, and device capacity, etc.

Click **Upgrade** in the Firmware Version, you can go to the upgrade page to upgrade the device.

8.9.2 Set Time

Set the device's time zone, synchronization mode, server address, NTP port, and interval.

Click **System and Maintenance → System Configuration → System → System Settings → Time Settings** .

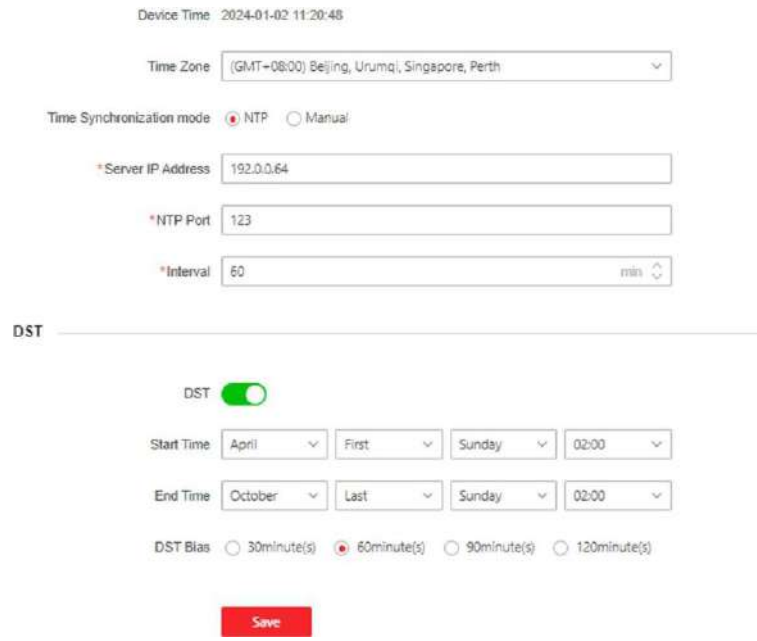


Figure 8-11 Time Settings

Click **Save** to save the settings after the configuration.

Time Zone

Select the device located time zone from the drop-down list.

Time Sync.

NTP

You should set the NTP server's IP address, port No., and interval.

Manual

By default, the device time should be synchronized manually. You can set the device time manually or check **Sync. with Computer Time** to synchronize the device time with the computer's time.

Server Address Type/Server Address/NTP Port/Interval

You can set the server address type, server address, NTP port, and interval.

8.9.3 Change Administrator's Password

Steps

1. Click **System and Maintenance → System Configuration → System → User Management → User Management** .
2. Click .
3. Enter the old password and create a new password.
4. Confirm the new password.
5. Click **Save**.

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.

8.9.4 Account Security Settings via PC Web

You can change the security questions and answers, or the email address for the device. After change the settings, once you forgot the device password, you should answer the new questions or use the new email address to reset the device password.

Steps

1. Click **System and Maintenance → System Configuration → System → User Management → User Management → Account Security Settings** .
2. Change the security questions or email address according your actual needs.
3. Enter the device password and click **OK** to confirm changing.

8.9.5 View Device Arming/Disarming Information via PC Web

View device arming type and arming IP address.

Go to **System and Maintenance → System Configuration → System → User Management → Arming/Disarming Information** .

You can view the device arming/disarming information. Click **Refresh** to refresh the page.

8.9.6 Network Settings

Set Basic Network Parameters via PC Web

Click **System and Maintenance → System Configuration → Network → Network Settings → TCP/IP** .

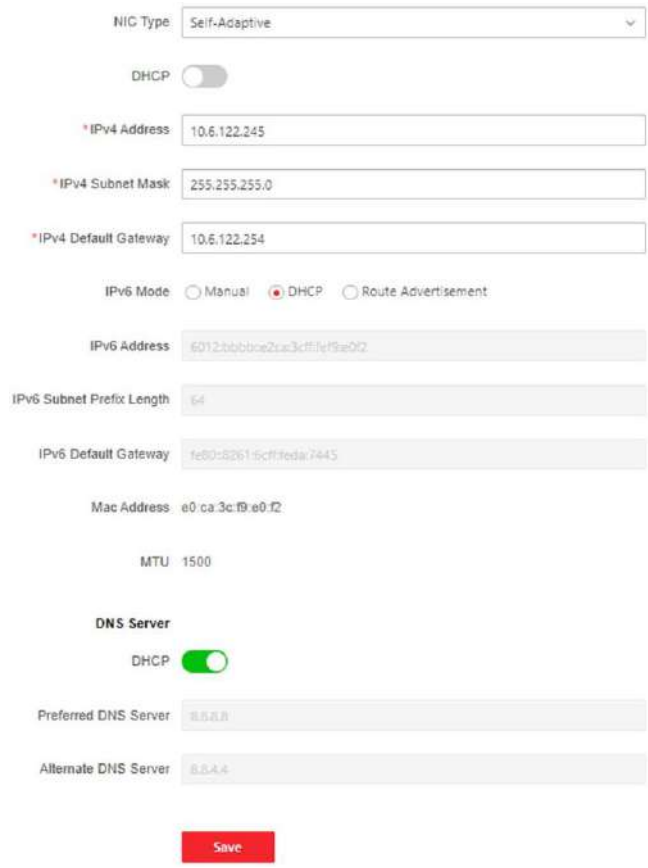


Figure 8-12 TCP/IP Settings Page

Set the parameters and click **Save** to save the settings.

NIC Type

Select a NIC type from the drop-down list. By default, it is **Auto**.

DHCP

If uncheck the function, you should set the IPv4 address, IPv4 subnet mask, IPv4 default gateway, Mac address, and MTU.

If you check the function, the system will allocate the IPv4 address, IPv4 subnet mask, the IPv4 default gateway automatically.

DNS Server

Set the preferred DNS server and the Alternate DNS server according to your actual need.

Set Wi-Fi Parameters

Set the Wi-Fi parameters for device wireless connection.

Steps

Note

The function should be supported by the device.

1. Click **System and Maintenance → System Configuration → Network → Network Settings → Wi-Fi** .

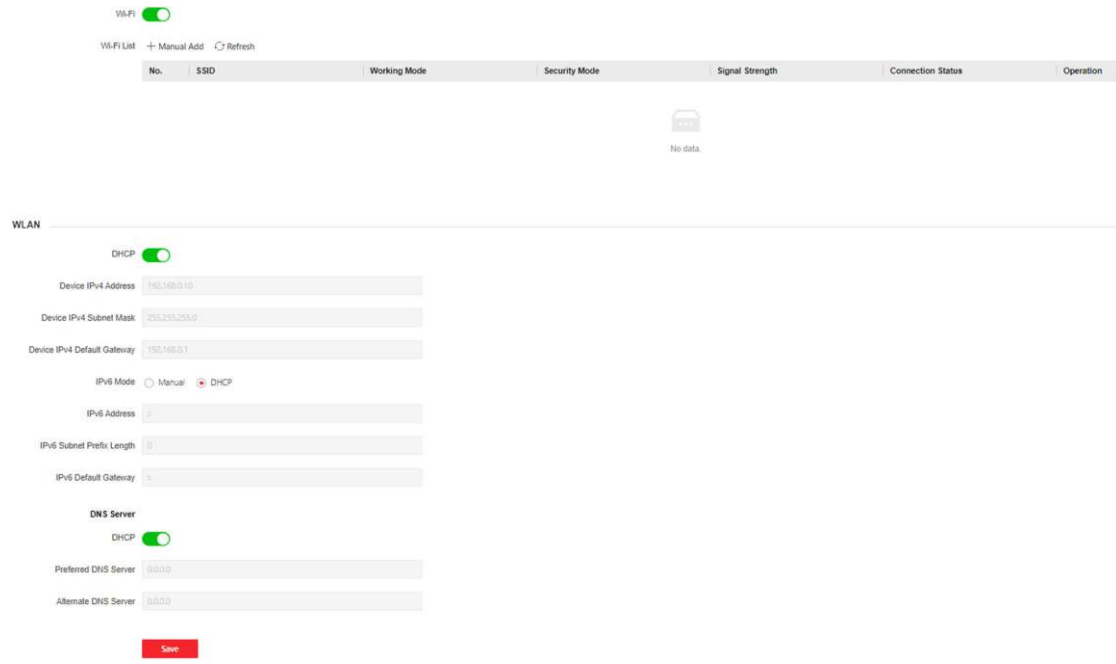


Figure 8-13 Wi-Fi Settings Page

2. Check **Wi-Fi**.
3. Select a Wi-Fi
   - Click of a Wi-Fi in the list and enter the Wi-Fi password.
   - Click **Add** and enter a Wi-Fi's name, password, and encryption type. Click **Connect**. When the Wi-Fi is connected, click **OK**.
4. **Optional:** Set the WLAN parameters.
   1) Set the IP address, subnet mask, and default gateway. Or enable **DHCP** and the system will allocate the IP address, subnet mask, and default gateway automatically.
5. Click **Save**.

Enable/Disable Bluetooth via PC Web

You can enable device bluetooth to connect a bluetooth sound.

Steps

1. Click **Access Control → System Configuration → Network → Network Settings → Bluetooth** to enter the settings page.
2. In the bluetooth parameter configuration section, enable **Open**.
3. Enter the external sound in the **Device Name**. After the bluetooth is connected, click **Save**.

Set Port via PC Web

Go to **System and Maintenance → System Configuration → Network → Network Service** .

Enable/Disable HTTP

Enable the HTTP function to improve the broswer's visiting security.

Go to **System and Maintenance → System Configuration → Network → Network Service → HTTP(S)** .

Click**Save** after parameters are configured.

HTTP Port

When you log in with a browser, you need to add the modified port number after the address. For example, when the HTTP port number is changed to 81, you need to enter http:// 192.0.0.65 : 81 when you log in with a browser.

HTTPS Port

Set the HTTPS port for visiting browser. But certification is required.

HTTP Listening

The device will send the alarm information to the destination IP or domain name by HTTP protocol. The destination IP or domain name should support HTTP protocol. Enter the destination IP or domain name, URL and port. And select the protocol type.

View RTSP Port via PC Web

The RTSP port is the port of real-time streaming protocol.

Go to **System and Maintenance → System Configuration → Network → Network Service → RTSP** .

View the Port.

Set WebSocket(s) via PC Web

View WebSocket and WebSockets port.

Go to **System and Maintenance → System Configuration → Network → Network Service → WebSocket(s)** .

View WebSocket and WebSockets port.

Enable SDK Service

After enabling SDK service, the device can be connected to the SDK server.

Click **System and Maintenance → System Configuration → Network → Device Access → SDK Server** to enter the settings page.

Enter **Server Port**.

Click **Save** to enable the settings.

Set ISUP Parameters via PC Web

Set the ISUP parameters for accessing device via ISUP protocol.

Steps

Note

The function should be supported by the device.

1. Click **System and Maintenance → System Configuration → Network → Device Access → ISUP** .
2. Check **Enable**.
3. Set the ISUP version, server address, device ID, and the ISUP status.

   Note

   If you select 5.0 as the version, you should set the encryption key as well.
4. Set the ISUP listening parameters, including ISUP alarm center IP address/domain name, ISUP alarm center URL, and ISUP alarm center port.
5. Click **Save**.

Set OTAP via PC Web

Connect the device to the platform through the OTAP protocol to obtain device information, upload operation status and alarm information, restart and upgrade the device.

Steps

1. Click **System and Maintenance → System Configuration → Network → Device Access → OTAP** .

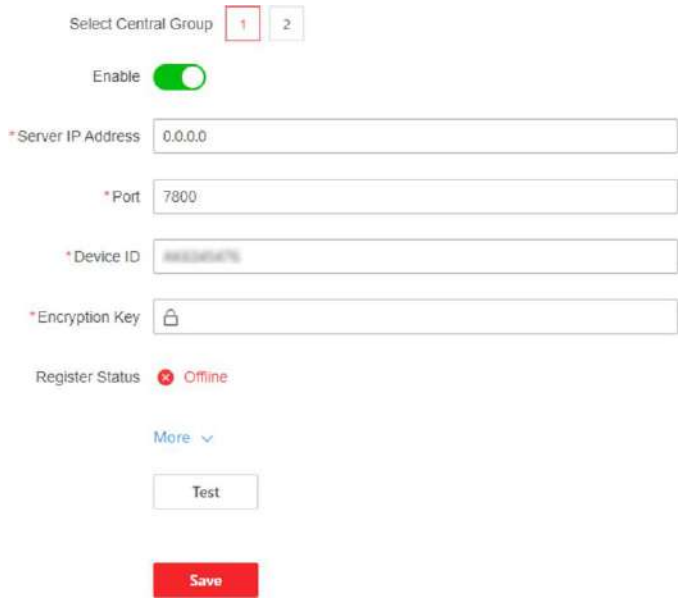


Figure 8-14 Set OTAP

2. Click to **Enable** OTAP.
3. Set **Server IP Address**, **Port**, **Device ID** and **Encryption Key**.
4. Click **Test** to ensure the device can connect to the server and register successfully. Refresh the page or restart the device to see the **Register Status**.
5. Click **More** to view the network type and access priority. Drag the operation icon upward or downward to adjust the network priority.
6. Click **Save**.

Platform Access via PC Web

Platform access provides you an option to manage the devices via platform.

Steps

1. Click **System and Maintenance → System Configuration → Network → Device Access → Hik-Connect** to enter the settings page.

   Note

   Hik-Connect is an application for mobile devices. With the App, you can view live image of the device, receive alarm notification and so on.

2. Check **Enable** to enable the function.
3. **Optional:** Check the checkbox of **Custom**, and you can set the server address by yourself.
4. Enter the verification code.
5. Click **View** to view device QR code. Scan the QR code to bind the account.

Note

8 to 32 letters (a to z, A to Z) or numbers (0 to 9), case sensitive. You are recommended to use a combination of no less than 8 letters or numbers.

6. Click **Save** to enable the settings.

VoIP Account Settings

You can realize voice call by network.

Steps

1. Go to **System and Maintenance → System Configuration → Network → Device Access → VoIP**.
2. Enable **VoIP Gateway**.
3. Set **Register User Name、Registration Password、Server IP Address、Server Port、Expiry Time、Register Status、Number、Display User Name.**

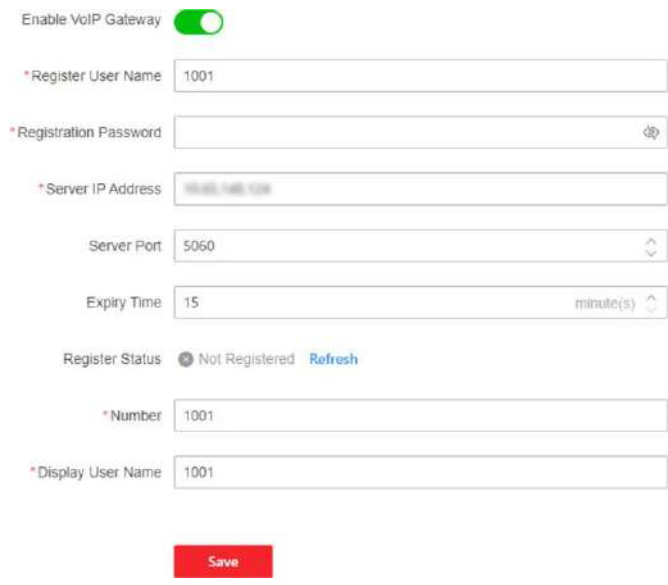


Figure 8-15 VoIP Account Settings

Registration Password

Enter the registration password for communication via SIP server. The registration password for the SIP server is configured usually in the main station's SIP settings.

Server IP Address

Enter the main station's IP address that used for VoIP communication. At this time the main station is used as a SIP server. Other intercom devices should registered to this server address to realize communication.

Number / Display User Name

The device displayed call number and user name.

4. Click **Save**.

8.9.7 Set Video and Audio Parameters via PC Web

Configure Video Parameters via Web Browser

You can set quality, resolution and other parameters of device camera.

Click **System and Maintenance → System Configuration → Video/Audio → Video** to enter the settings page.

Set camera name, stream type, video type, resolution, bit rate type, video quality, frame rate, Max. bitrate, video encoding and I frame interval.

Click **Save**.

Configure Audio Parameters via Web Browser

You can set device volume.

Click **System and Maintenance → System Configuration → Video/Audio → Audio** to enter the settings page.

Set stream type and audio encoding according to your actual needs. Slide to set input and output volume.

Slide to enable voice prompt function.

You can enable **Audio Mixing**, and set **Output Sub-Volume**.

Click **Save**.

8.9.8 Image Parameter Settings

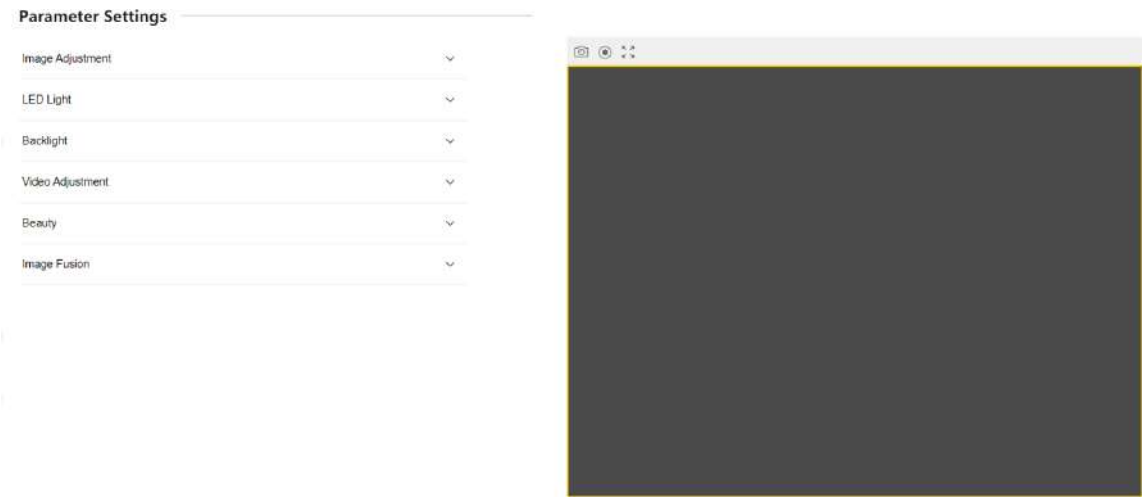


Figure 8-16 Display Settings

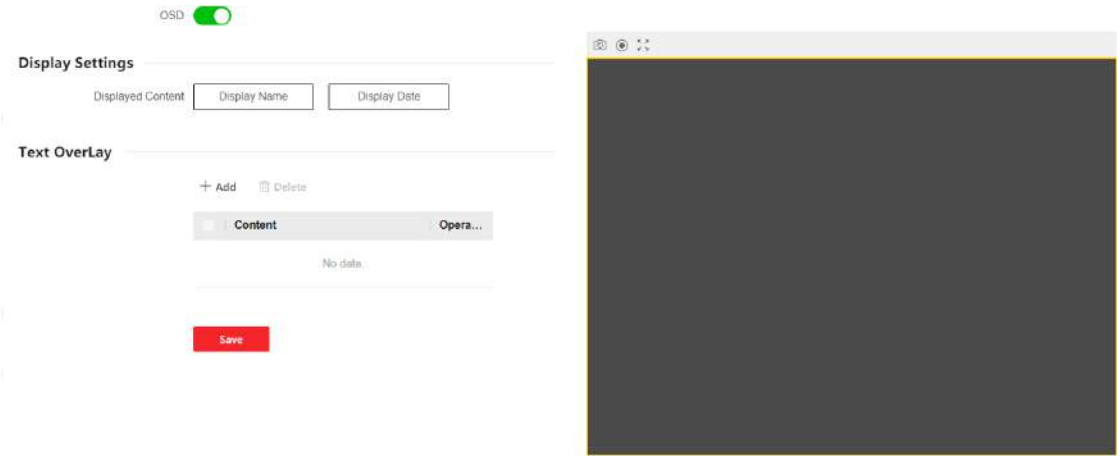


Figure 8-17 OSD Settings

Set Brightness/Contrast/Saturation/Sharpness via PC Web

You can set picture information such as brightness, contrast, saturation and sharpness of live view page.

Click **System and Maintenance → System Configuration → Image → Display Settings** to enter the settings page.

Image Adjustment

Drag the block or enter numbers to set brightness, contrast, saturation and sharpness.

Click **Restore Default Settings** to restore the to the default.

Set LED Light via PC Web

You can adjust the brightness of the supplement light.

Steps

1. Click **System and Maintenance → System Configuration → Image → Display Settings** to enter the settings page.
2. Set the type, mode and brightness of the supplement light.
3. **Optional:** Click **Restore Default Settings** to restore the to the default.

Set WDR via PC Web

Click **System and Maintenance → System Configuration → Image → Display Settings** to enter the settings page.

Enable or disable wide dynamic range. After enabling, both bright and dark parts of the scene can be seen more clearly at the same time.

Click **Restore Default Settings** to restore the to the default.

Set Video Standard via PC Web

You can set the video standard of live view page.

Click **System and Maintenance → System Configuration → Image → Display Settings** to enter the settings page.

Video Adjustment

Set the video frame rate during remote preview. You need to reboot the device to make the new settings effective.

PAL

25 frames per second. Suitable for mainland China, Hong Kong (China), the Middle East countries, Europe countries, etc.

NTSC

30 frames per second. Suitable for the USA, Canada, Japan, Taiwan (China), Korea, the Philippines, etc.

Click **Restore Default Settings** to restore the to the default.

Set Beauty Parameters via PC Web

After enabling, you can whiten or smooth authenticated pictures.

Click **System and Maintenance → System Configuration → Image → Display Settings** to enter the settings page.

Enable **Beauty**, drag the block or enter numbers to set the whiten and smooth level.

Click **Restore Default Settings** to restore the to the default.

Set Image Fusion via PC Web

You can enable the image fusion function to improve image quality.

Click **System and Maintenance → System Configuration → Image → Display Settings** to enter the settings page.

Image Fusion

Set **Image Fusion** as **Auto** or **Disable**. Drag the block or enter numbers to set sensitivity.

Click **Restore Default Settings** to restore the to the default.

Set OSD Parameters via PC Web

You can customize the camera name, time/date format, display mode, and OSD size displayed on the live view.

Steps

1. Click **System and Maintenance → System Configuration → Image → OSD Configuration** to enter the settings page.
2. Enable **OSD**.
3. Check the corresponding checkbox to select the display of camera name, date or week if required.
4. Enter **Camera Name**.
5. Select from the drop-down list to set the **Time Format** and **Date Format**.
6. Click **Add** to enter the characters in the textbox, and adjust the OSD position and alignment.

8.9.9 Alarm Settings via PC Web

Set the alarm output parameters.

Steps

1. Click **System and Maintenance → System Configuration → Event → Alarm Settings → Alarm Output** .
2. Set **Alarm Name** and mode of **Alarm Duration**.

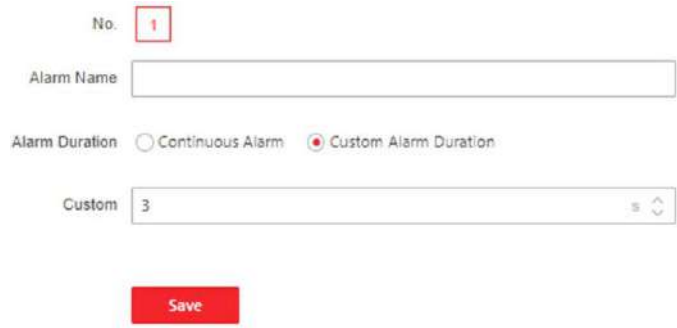


Figure 8-18 Alarm Settings

Continuous Alarm

When the alarm is triggered, it will alarm continuously.

Custom Alarm Duration

You can set **Alarm Duration** for the device when the alarm is triggered.

8.9.10 Access Configuration

Set RS-485 Parameters via PC Web

You can set the RS-485 parameters including the peripheral, address, baud rate, etc.

Click **System and Maintenance → System Configuration → Access Configuration → RS-485** .

Check **Enable RS-485**, and set the parameters.

Click **Save** to save the settings after the configuration.

No.

Set the RS-485 No.

Peripheral Type

Select a peripheral from the drop-down list according the actual situation. You can select from **Card Reader**, **Extension Module**, **Access Controller**, or **Disable**.

Note

After the peripheral is changed and saved, the device will reboot automatically.

RS-485 Address

Set the RS-485 Address according to your actual needs.

Note

If you select **Access Controller**: If connect the device to a terminal via the RS-485 interface, set the RS-485 address as 2. If you connect the device to a controller, set the RS-485 address according to the door No.

Baud Rate

The baud rate when the devices are communicating via the RS-485 protocol.

Set Wiegand Parameters via PC Web

You can set the Wiegand transmission direction.

Steps

Note

Some device models do not support this function. Refer to the actual products when configuration.

1. Click **System and Maintenance → System Configuration → Access Configuration → Wiegand Settings** .

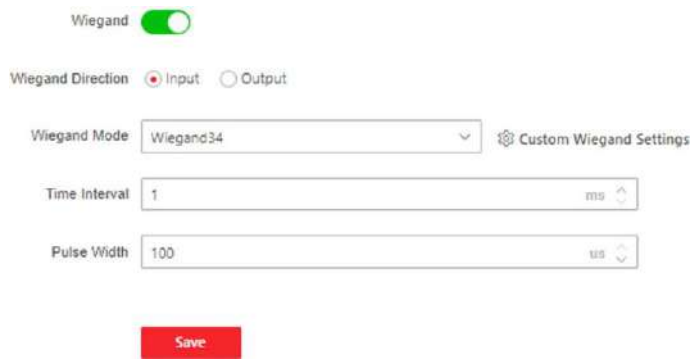


Figure 8-19 Wiegand Page

2. Check **Wiegand** to enable the Wiegand function.
3. Set a transmission direction.

   Input

   The device can connect a Wiegand card reader.

   Output

   The can connect an external access controller. And the two devices will transmit the card No. via Wiegand 26 or 34.
4. Click **Save** to save the settings.

Note

If you change the peripheral, and after you save the device parameters, the device will reboot automatically.

Set Secure Door Control Unit Parameters via PC Web

You can set secure door control unit parameters.

Steps

1. Click **System and Maintenance → Access Configuration → Secure Door Control Unit** .
2. Select door.

Note

Selecting door 1 means that the door will be controlled by secure door control unit. The same goes to the selection of door 2.

3. View secure door control unit status.
4. You can enable **Two-Door Interlocking**.

Note

If the function is enabled, the two doors cannot be opened at the same time.

8.9.11 Time and Attendance Settings

If you want to record the person's working hour, late arrivals, early departures, breaks, absenteeism, etc., you can add the person to the shift group and assign a shift schedule (a rule for the attendance defining how the schedule repeats, the shift type, break settings, and the card swiping rule.) to the shift group to define the attendance parameters for the persons in the shift group.

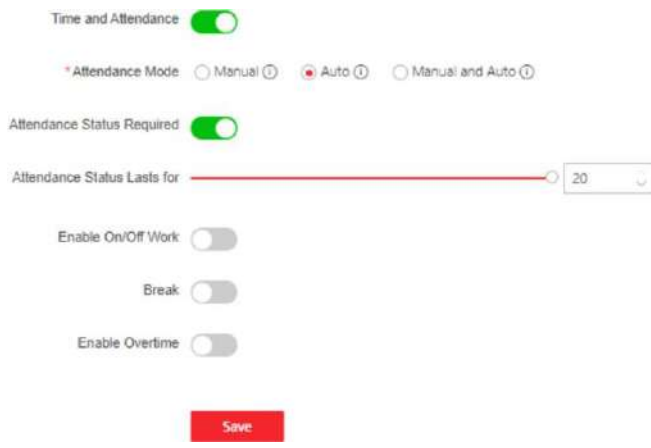


Figure 8-20 Time and Attendance

Disable Attendance Mode via Web

Disable the attendance mode and the system will not display the attendance status on the initial page.

Steps

1. Click **System and Maintenance → System Configuration → Platform Attendance** to enter the settings page.
2. Disable the **Time and Attendance**.

Result

You will not view or configure the attendance status on the initial page. And the system will follow the attendance rule that configured on the platform.

Set Manual Attendance via Web

Set the attendance mode as manual, and you should select a status manually when you take attendance.

Before You Start

Add at least one user, and set the user's authentication mode. For details, see *User Management*.

Steps

1. Click **System and Maintenance → System Configuration → Platform Attendance** to enter the settings page.
2. Set the **Attendance Mode** as **Manual**.
3. Enable the **Attendance Status Required** and set the attendance status lasts duration.

4. Enable a group of attendance status.

Note

The Attendance Property will not be changed.

5. **Optional:** Select an status and change its name if required.

Result

You should select an attendance status manually after authentication.

Note

If you do not select a status, the authentication will be failed and it will not be marked as a valid attendance.

Set Auto Attendance via Web

Set the attendance mode as auto, and you can set the attendance status and its available schedule. The system will automatically change the attendance status according to the configured schedule.

Before You Start

Add at least one user, and set the user's authentication mode. For details, see *User Management*.

Steps

1. Click **System and Maintenance → System Configuration → Platform Attendance** to enter the settings page.
2. Set the **Attendance Mode** as **Auto**.
3. Enable the **Attendance Status Required** function.
4. Enable a group of attendance status.

Note

The Attendance Property will not be changed.

5. **Optional:** Select an status and change its name if required.
6. Set the status' schedule. Refers to for details.

Set Manual and Auto Attendance via Web

Set the attendance mode as **Manual and Auto**, and the system will automatically change the attendance status according to the configured schedule. At the same time you can manually change the attendance status after the authentication.

Before You Start

Add at least one user, and set the user's authentication mode. For details, see *User Management*.

Steps

1. Click **System and Maintenance → System Configuration → Platform Attendance** to enter the settings page.
2. Set the **Attendance Mode** as **Manual and Auto**.
3. Enable the **Attendance Status Required** function.
4. Enable a group of attendance status.

Note

The Attendance Property will not be changed.

5. **Optional:** Select an status and change its name if required.
6. Set the status' schedule. Refers to for details.

Result

On the initial page and authenticate. The authentication will be marked as the configured attendance status according to the schedule. If you tap the edit icon on the result tab, you can select a status to take attendance manually, the authentication will be marked as the edited attendance status.

Example

If set the **Break Out** as Monday 11:00, and **Break In** as Monday 12:00, the valid user's authentication from Monday 11:00 to 12:00 will be marked as break.

8.10 Preference Settings

8.10.1 Set Startup Image via PC Web

Set startup image.

Go to **System and Maintenance → Preference → Screen Display** .

Figure 8-21 Startup Image

Enable **Custom Booting Picture**, click **+** and select a booting picture from local browse.

Note

Supported picture size: no more than 512 KB; resolution: 600*1024; format: jpg.

Click **Save**.

8.10.2 Set Standby Image via PC Web

Set the standby image parameters, including the time to enter satndby, screen saver picture, displayed effect, and slide show interval.

Go to **System and Maintenance → Preference → Screen Display** .

Figure 8-22 Standby Image Settings

Set the standby image parameters, and click **Save**.

Time to Enter Standby

The device will show the standby image after the configured time duration.

Screen Saver Picture

Set the standby images as default image or customized image. Select**Custom**, and click **+** to upload a standby picture from the local browse.

Note

No more than 3 picture(s) are allowed. Single picture size: no more than 1024 KB; format: jpg.

Display Effect

Set the standby picture's display effect as **Stretch**, **Adaptive**, or**Fill**.

Slide Show Interval

If you add multiple pictures, you can set the pictures' switching time.

8.10.3 Set Sleep Time via PC Web

The device will in sleep mode after the configured time duration. The function can reduce power consumption.

Go to **System and Maintenance → Preference → Screen Display** .

Figure 8-23 Sleep Settings

Slide **Sleep** and set the sleep time.

Click **Save**.

8.10.4 Customize Authentication Desk via PC Web

Customize the modules on the authentication page/desk.

Steps

1. Go to **System and Maintenance → Preference → Custom Home Page** .
2. Select **Application Mode**.

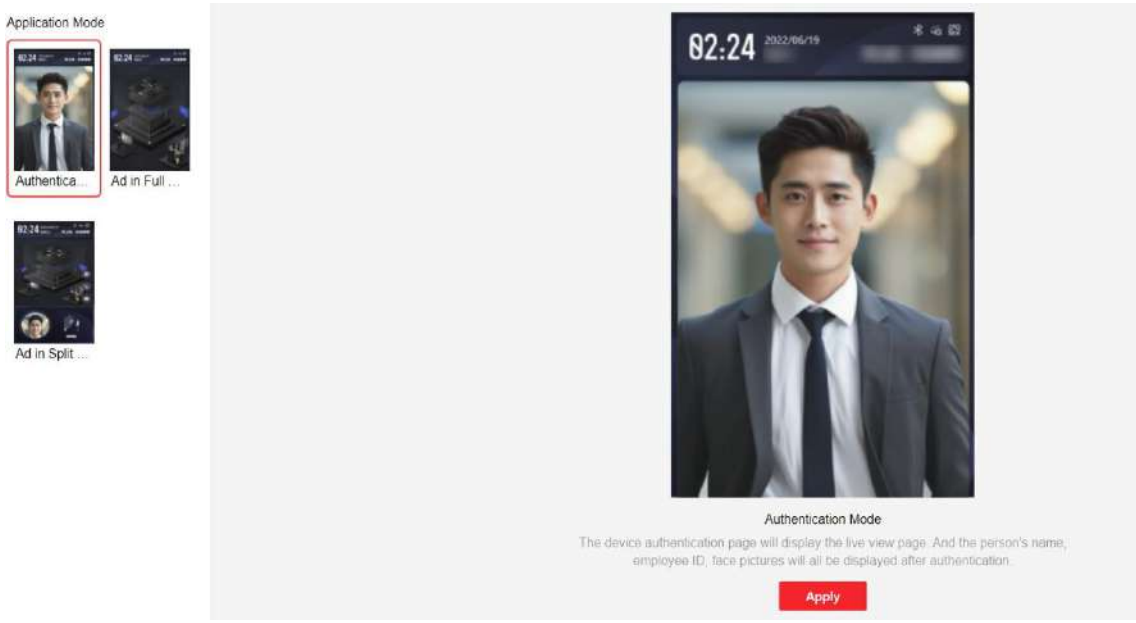


Figure 8-24 Select Application Mode

Authentication Mode

The device authentication page will display the live view page. And the person's name, employee ID, face pictures will all be displayed after authentication.

Ad in Full Screen

The ad takes up the full screen of authentication page. Screensaver, Welcome Message can be played in ad.

Ad in Split Screen

Authentication page includes ad area and authentication area. Screensaver, Welcome Message can be played in ad.

3. Click **Apply**.

8.10.5 Set Notice Publication via PC Web

You can set the notice publication for the device.

Go to **System and Maintenance → Preference → Notice Publication** .

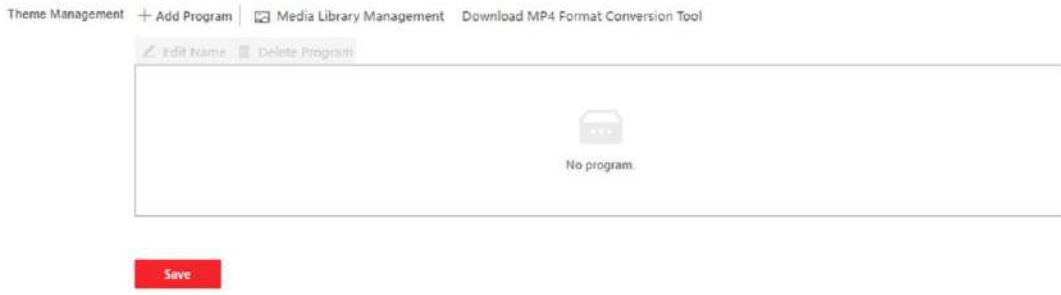


Figure 8-25 Notice Publication

Download MP4 Format Conversion Tool

You can click **Download MP4 Format Conversion Tool** if you need to change the format.

Material Management

You can click **+ Add Theme**, and set **Theme Name** and **Theme Type**.

Click **Upload**, and click **+** to upload the picture or video from the local PC.

Note

By now, there is only one theme can be added.

Add Program

You can set the program name and select program type.

Picture

If you select picture, you can click **+** to add picture.

Welcome Message

If you select welcome message, you can set the template, content, font size and color of main and sub title. You can also custom the background picture.

Standard

If you select standard, you can set the background color and picture.

Play Schedule

After you have created a theme, you can select the theme and draw a schedule on the time line.

Select the drawn schedule, and you can edit the exact start and end time.

Select the drawn schedule and you can click **Delete** or **Delete All** to delete the schedule.

Slide Show Interval

Drag the block or enter the number to set the slide show interval. The picture and video will be changed according to the interval.

8.10.6 Set Prompt Schedule via PC Web

Customize the output audio content when authentication succeeded and failed.

Steps

1. Go to **System and Maintenance → Preference → Prompt Schedule** .

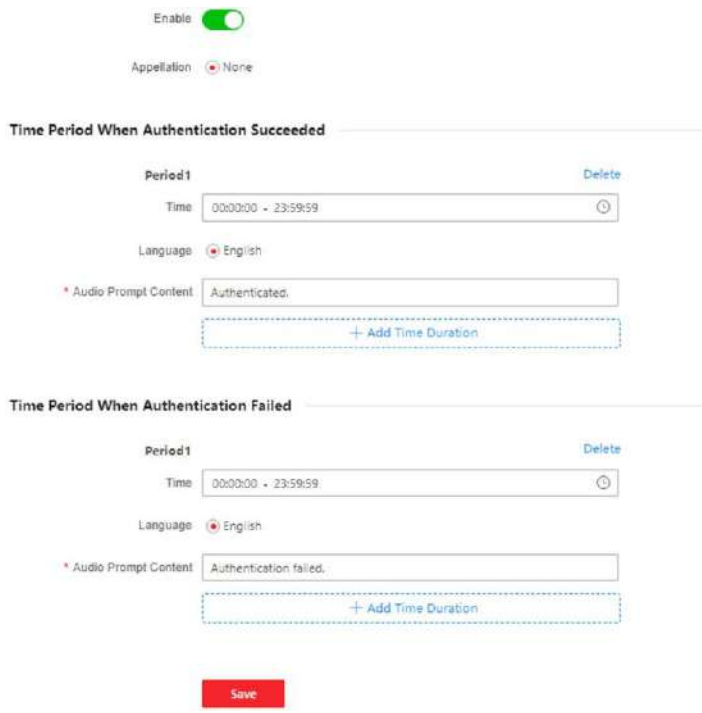


Figure 8-26 Prompt Schedule

2. Enable the function.
3. Set the appellation.

4. Select time schedule.
5. Set the time period when authentication succeeded.
   1) Click **Add Time Duration**.
   2) Set the time duration.

   Note
   If authentication is succeeded in the configured time duration, the device will broadcast the configured content.
   3) Set the audio prompt content.
   4) **Optional:** Repeat substep 1 to 3.
   5) **Optional:** Click to delete the configured time duration.
6. Set the time duration when authentication failed.
   1) Click **Add Time Duration**.
   2) Set the time duration.

   Note
   If authentication is failed in the configured time duration, the device will broadcast the configured content.
   3) Set the audio content.
   4) **Optional:** Repeat substep 1 to 3.
   5) **Optional:** Click to delete the configured time duration.
7. Click **Save** to save the settings.

8.10.7 Customize Prompt Voice via PC Web

You can customize prompt voices for the device.

Steps

1. Go to **System and Maintenance → Preference → Custom Prompt** .

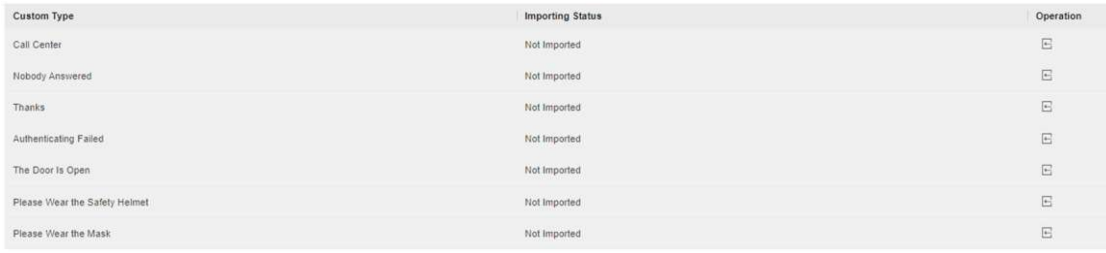


Figure 8-27 Custom Prompt

2. Click → and import audio file from local PC according to your actual needs.

Note
The uploaded audio file should be less than 512 kb, in WAV format.

8.10.8 Set Authentication Result Text via PC Web

Steps

1. Go to **System and Maintenance → Preference → Authentication Result Text** .

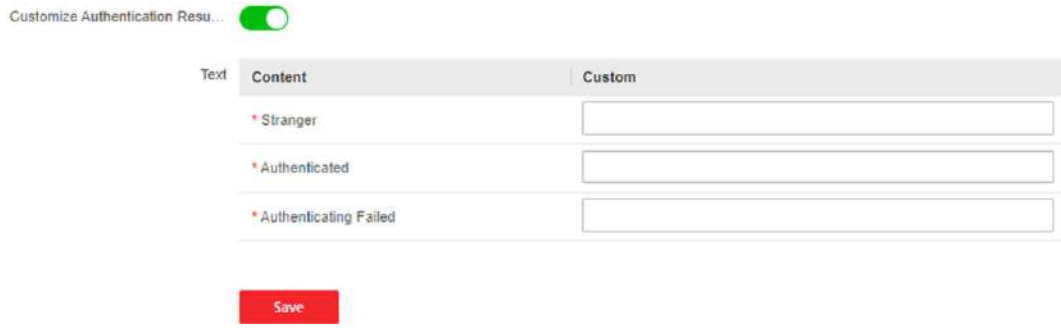


Figure 8-28 Authentication Result Text

2. Enable **Customize Authentication Result Text**.
3. Enter custom texts.
4. Click **Save**.

8.11 System and Maintenance

8.11.1 Reboot

You can reboot the device.

Click **System and Maintenance → Maintenance → Restart** to enter the settings page.

Click **Restart** to reboot the device.

8.11.2 Upgrade

Upgrade Locally via PC Web

You can upgrade the device locally.

Click **System and Maintenance → Maintenance → Upgrade** to enter the settings page.

Select an upgrade type from the drop-down list. Click and select the upgrade file from your local PC. Click **Upgrade** to start upgrading.

Online Upgrading via PC Web

You can upgrade the device online.

Click **System and Maintenance → Maintenance → Upgarde** to enter the settings page.

Click**Check for Updates**to check whether there is updated versions.

If the device is connected to the network and added to Hik-Connect App, you can tap **Device Upgrade → Online Upgrade** on device for upgrading when there is an updated version in Hik-Connect App.

8.11.3 Restoration

Restore to Factory Settings via Web Browser

You can restore device to factory settings.

Click **System and Maintenance → Maintenance → Backup and Reset** to enter the settings page.

Click **Restore All**, all parameters will be restored to the factory settings. You should activate the device before usage.

Restore to Default Settings via PC Web

You can restore device to default settings.

Click **System and Maintenance → Maintenance → Backup and Reset** to enter the settings page.

Click **Restore**, the device will restore to the default settings, except for the device IP address and the user information.

8.11.4 Export Device Parameters via PC Web

Export device parameters.

Go to **System and Maintenance → Maintenance → Backup and Reset** .

Backup

Click **Export** to export device parameters.

Note

Export device parameters and import those parameters to other devices.

8.11.5 Import Device Parameters via PC Web

Import the configuration parameters.

Go to **System and Maintenance → Maintenance → Backup and Reset** .

Import Config File

Click and select a file from local PC. Click **Import**.

8.11.6 Device Debugging

You can set device debugging parameters.

Enable/Disable SSH via Web Browser

You can enable SSH to perform remote debugging.

Click **System and Maintenance → Maintenance → Device Debugging → Log for Debugging**.

Enable SSH

SSH is used for remote debugging. When you don't need to use this service, it's recommended to disable SSH to improve security.

Print Device Log via PC Web

You can print out the device log.

Click **System and Maintenance → Maintenance → Log** to enter the settings page.

Click**Export** to print out the device log.

Capture Network Packet via PC Web

Set the capture packet duration and size and start caputre. You can view the log and debug according to the capture result.

Go to **System and Maintenance → Maintenance → Device Debugging → Log for Debugging** .

Set **Capture Packet Duration**,**Capture Packet Size**, and click **Start Capture**.

Test Protocol via PC Web

Select a protocol address, and enter the protocol to test. You can debug the device according to the response header and returned value.

Go to **System and Maintenance → Maintenance → Device Debugging → Protocol Testing** .

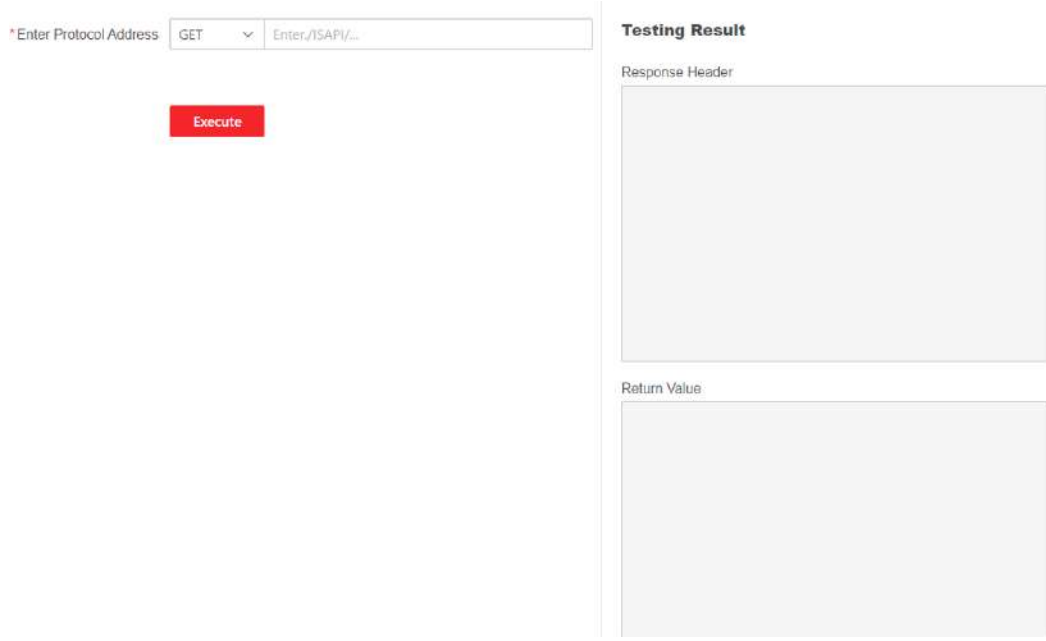


Figure 8-29 Protocol Testing

Select a protocol address, and enter the protocol. Click **Execute**.

Debug the device according to the response header and returned value.

Network Diagnosis via PC Web

Enter the device IP address or domain name, you can perform PING settings. Debug the network according to the PING result.

Go to **System and Maintenance → Maintenance → Device Debugging → Network Diagnosis** .

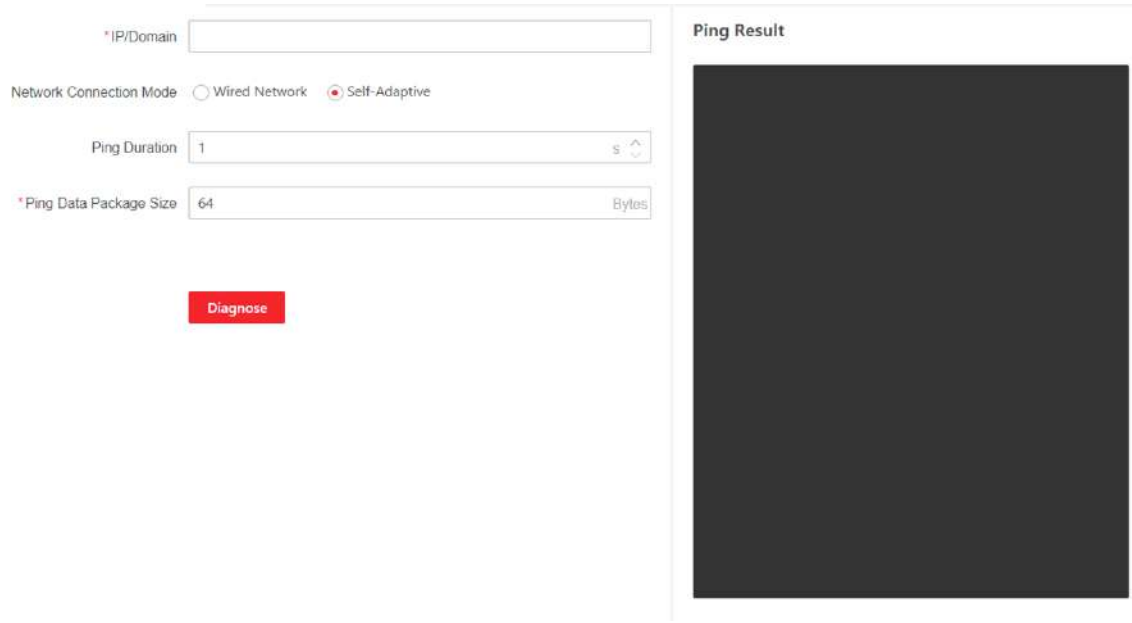


Figure 8-30 Network Diagnosis

Enter the device IP for PING operation, select the network connection mode, PING duration, and Ping data package size (default parameter is recommended.) Click **Diagnose**. The result will displayed in **PING Result**.

Set Network Penetration Service via PC Web

When the devcie is deployed in the LAN, you can enable the penetration service to realize device remote management.

Steps

1. Go to **System and Maintenance → Maintenance → Device Debugging → Network Penetration Service**.
2. Slide **Enable Penetration Service**.
3. Set **Server IP Address** and **Server Port**. Create **User Name** and **Password**.
4. **Optional:** You can set **Heartbeat Timeout**. The value range is 1 to 6000.
5. **Optional:** You can view the status of the penetration service. Click **Refresh** to refresh the status.
6. Click **Save**.

Note

The penetration service will auto disabled after 48 h.

8.11.7 View Log via PC Web

You can search and view the device logs.

Go to **System and Maintenance → Maintenance → Log** .

Set the major and minor type of the log type. Set the start time and end time for searching, and click **Search**.

The results will be displayed below, which including the No., time, the major type the minor type, the channel No., the local/remote user information, the remote host IP, etc.

8.11.8 Advanced Settings via PC Web

You can configure face parameters, palm parameters, and view version information.

Go to **System and Maintenance → Maintenance → Advanced Settings** .

Enter the device activation password and click **Enter**.

Face Parameter

Enable **Custom Anti-Spoofing Detection** and you can set the **Anti-Spoofing Detection Threshold 1:1**, **Anti-Spoofing Detection Threshold 1:N**.

Enable **Lock Face for Authentication**, and set **Lock Duration**. The face will be locked for the set lock duration after the failed attempt limit of anti-spoofing detection has been reached.

Click **Save**.

Palm Print Parameter

Enable **Custom Anti-Spoofing Detection** and you can set the **Anti-Spoofing Detection Threshold**.

Click **Save**.

Version Information

You can view the different version information here.

8.11.9 Security Management

Set security level when login the PC web.

Go to **System and Maintenance → Safe → Security Service** .

Security Mode

High security level when logging in and verify user information.

Compatible Mode

Compatible with old user verification method.

Click **Save**.

8.11.10 Certificate Management

It helps to manage the server/client certificates and CA certificate.

Note

The function is only supported by certain device models.

Create and Import Self-signed Certificate

Steps

1. Go to **System and Maintenance → Safe → Certificate Management** .
2. In the **Certificate Files** area, select a **Certificate Type** from the drop-down list.
3. Click **Create**.
4. Input certificate information.
5. Click **OK** to save and install the certificate.

   The created certificate is displayed in the **Certificate Details** area.

   The certificate will be saved automatically.
6. Download the certificate and save it to an asking file in the local computer.
7. Send the asking file to a certification authority for signature.
8. Import the signed certificate.
   1) Select a certificate type in the **Import Key** area, and select a certificate from the local, and click **Import**.
   2) Select a certificate type in the **Import Communication Certificate** area, and select a certificate from the local, and click **Import**.

Import Other Authorized Certificate

If you already has an authorized certificate (not created by the device), you can import it to the device directly.

Steps

1. Go to **System and Maintenance → Safe → Certificate Management** .
2. In the **Import Key** and **Import Communication Certificate** areas, select certificate type and upload certificate.
3. Click **Import**.

Import CA Certificate

Before You Start

Prepare a CA certificate in advance.

Steps

1. Go to **System and Maintenance → Safe → Certificate Management** .
2. Create an ID in the **Import CA Certificate** area.

   Note

   The input certificate ID cannot be the same as the existing ones.
3. Upload a certificate file from the local.
4. Click **Import**.

Chapter 9 Other Platforms to Configure

You can also configure the device via iVMS-4200 Client Software or HikCentral Access Control. For details, see the platforms' user manual.

iVMS-4200 Client Software

Click/tap the link to view the client software's user manual.

http://enpinfodata.hikvision.com/analysisQR/showQR/ca930247

HikCentral Access Control (HCAC)

Click/tap the link to view the HCAC's user manual.

http://enpinfodata.hikvision.com/analysisQR/showQR/f2f6cf42

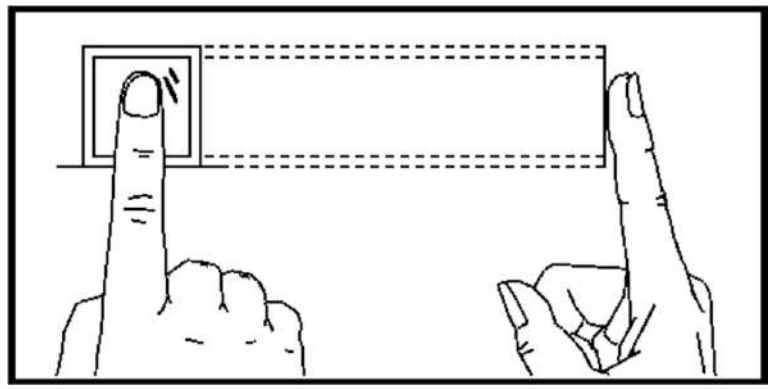
Appendix A. Tips for Scanning Fingerprint

Recommended Finger

Forefinger, middle finger or the third finger.

Correct Scanning

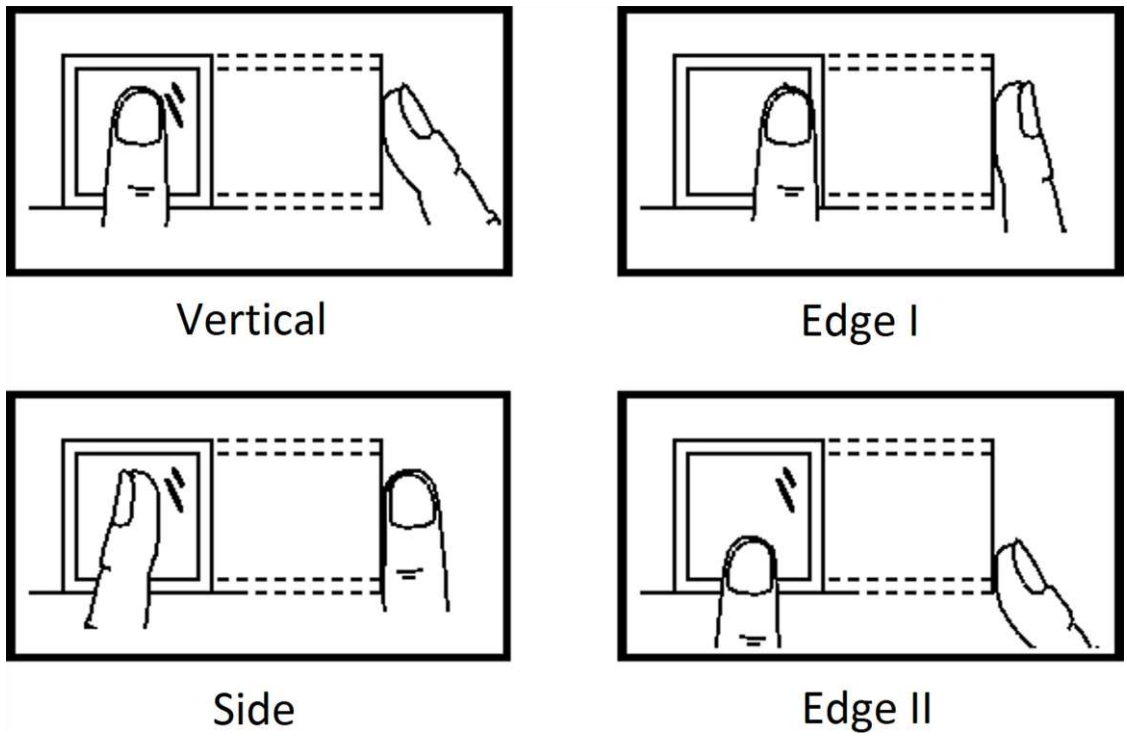
The figure displayed below is the correct way to scan your finger:



You should press your finger on the scanner horizontally. The center of your scanned finger should align with the scanner center.

Incorrect Scanning

The figures of scanning fingerprint displayed below are incorrect:



Environment

The scanner should avoid direct sun light, high temperature, humid conditions and rain.
When it is dry, the scanner may not recognize your fingerprint successfully. You can blow your finger and scan again.

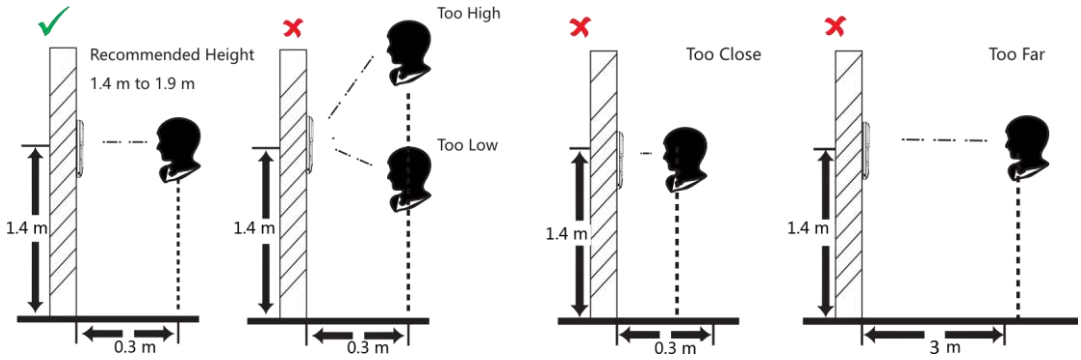
Others

If your fingerprint is shallow, or it is hard to scan your fingerprint, we recommend you to use other authentication methods.
If you have injuries on the scanned finger, the scanner may not recognize. You can change another finger and try again.

Appendix B. Tips When Collecting/Comparing Face Picture

The position when collecting or comparing face picture is as below:

Positions (Recommended Distance: 0.3 m)



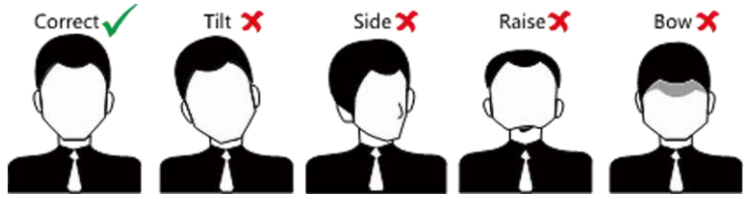
Expression

- Keep your expression naturally when collecting or comparing face pictures, just like the expression in the picture below.

- Do not wear hat, sunglasses, or other accessories that can affect the facial recognition function.
- Do not make your hair cover your eyes, ears, etc. and heavy makeup is not allowed.

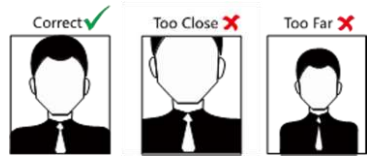
Posture

In order to get a good quality and accurate face picture, position your face looking at the camera when collecting or comparing face pictures.



Size

Make sure your face is in the middle of the collecting window.



Appendix C. Tips for Adding Palm Print and Palm Vein

- When recognizing the palm print and palm vein, place the center of the palm at a distance of 5~12 cm from the center of the device, and pay attention to keeping it parallel to the peripheral module.
- When the peripheral module access to the new face recognition terminal, the data of the peripheral module needs to be cleared and re-issued or collected.
- The palms of the hands need to be kept clean to avoid dirt.
- The surface of the peripheral module should be kept clean to avoid false alarms caused by the sensor.

Appendix D. Tips for Installation Environment

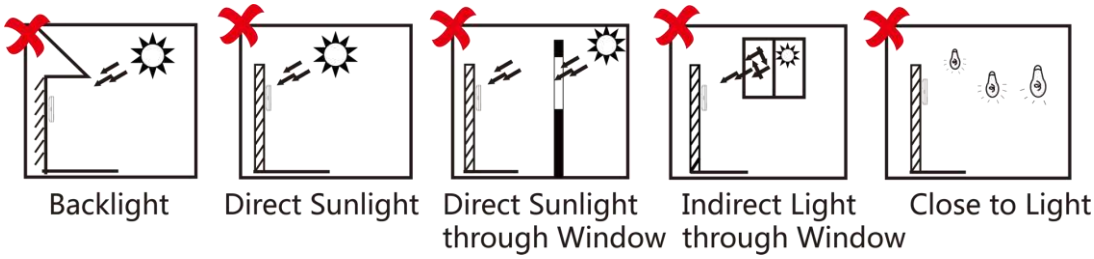
1. Light Source Illumination Reference Value

Candle: 10Lux

Bulb: 100~850Lux

Sunlight: More than 1200Lux

2. Avoid backlight, direct and indirect sunlight



Appendix E. Dimension

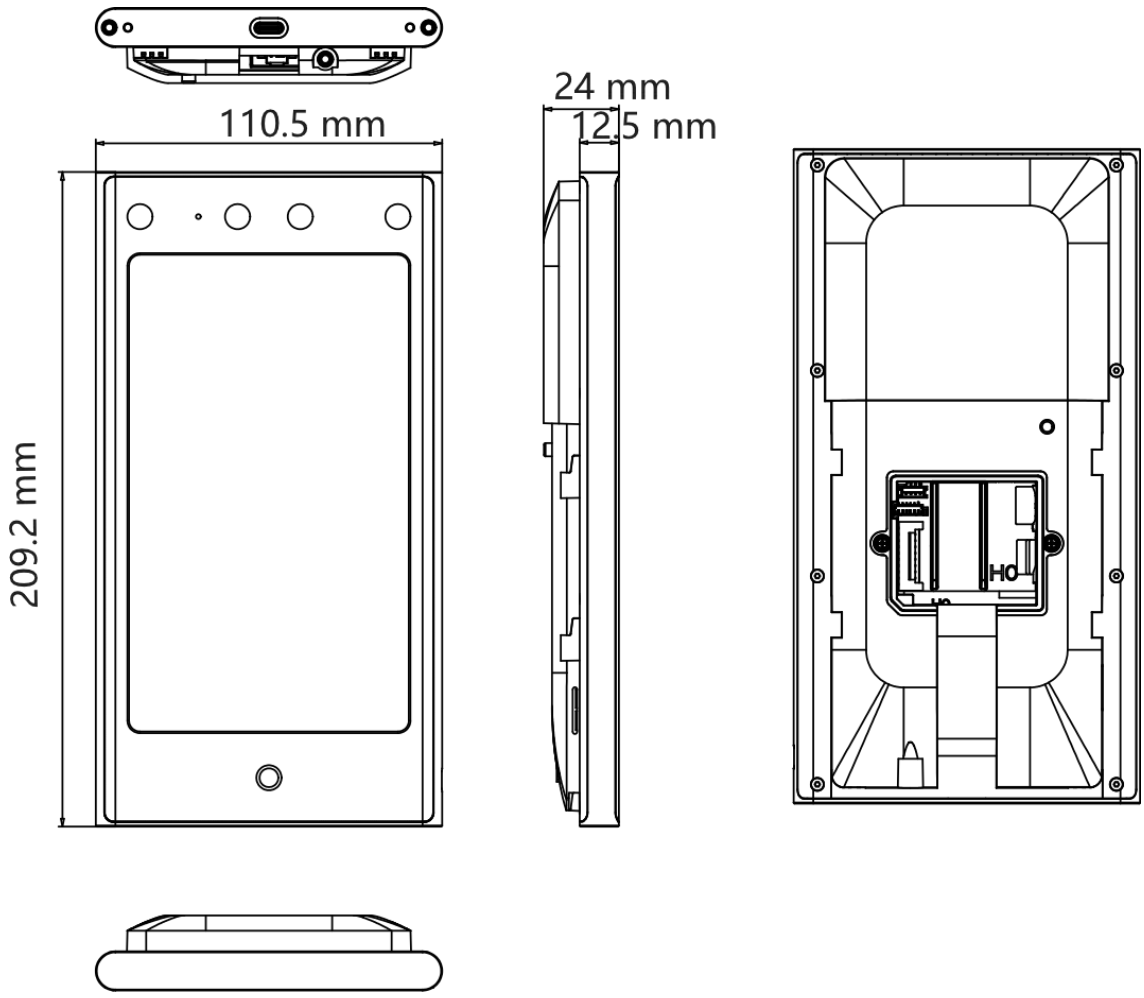


Figure E-1 Dimension


See Far, Go Further

Crachá Clamshell RFID 13,56 MHz Smart Card Mifare 1K

Descrição:

O Mifare (Smart Card Contactless - Cartão Inteligente de Proximidade) é um cartão que utiliza um microprocessador residente para armazenar e processar dados, efetuar cálculos, gerenciar arquivos e executar algoritmos de criptografia. Permite a leitura dos dados através da tecnologia de Radio Freqüência, sem a necessidade de contato físico entre o leitor e o cartão. Sua memória pode ser reutilizada, regravando novos dados por cima dos existentes, possuindo um sistema de criptografia que protege os dados do cartão, tornando-o muito seguro.

Especificação:

Cartão laminado em PVC ou ABS, nas dimensões de 86 x 54 x 1,9 mm, sem Contato – “Contactless” (ISO/IEC 10536), com memória protegida, equipado com tecnologia MIFARE Standard (Chip MF1 S50 - NXP ou compatível), com capacidade de memória EEPROM de 1Kb.

Características:

- Freqüência de operação: 13,56 MHz

- Número serial único (ID pré-gravado de fábrica) - CÓDIGO IMPRESSO

- Memória EEPROM 1Kb: 16 setores com 4 blocos de 16 bytes para armazenamento de dados

- Compatível com NFC

- ISO/IEC 7816, ISO/IEC 10536, ISO 14443-A

- Tamanho: 86 x 54 x 1,9 mm

- Distância máxima de leitura: 10cm a depender do leitor

- Duas chaves por setor com privilégios configuráveis

- Tempo de leitura: 100 ms

- Possibilidade de leitura de múltiplos cartões simultaneamente (Anti-Colisão)

- Detenção de dados de 10 anos ou 100.000 ciclos de escrita

- Temperatura de operação: -35ºC a +50

- Cor: Branco

- Furo ovoide para fixação de presilha
- Personalização através de adesivo de PVC (impresso)

DS-K3B530XM
Swing Barrier

The DS-K3B530X series swing barrier with 14 pairs of IR lights is designed to detect unauthorized entrance or exit. By adopting the swing barrier integratedly with the access control system, person should authenticate to pass through the lane via presenting IC or ID card, scanning QR code, etc. It is widely used in office building, hotels, residences, etc.

- 14 pairs of IR light detectors: Permissions validation and anti-tailgating.
- LED light indicates passing direction.
- Valid passing duration settings: System will cancel the passing permission if a person does not pass through the lane within the valid passing duration.
- Support speaker and remote control keyfob optional, need to order separately.
- Person count with 90% accuracy
- Easy of unidirectional and bidirectional configurations according to the needs of the scenario
- Customizable pictogram according to the control set for input and output

▪ Specification

System	
Motor	Servo motor (Noiseless engine)
MCBF	≥ 12 million times
Interface	
Network interface	10 M/100 M x 1
Lock control	2
Exit button	2
Alarm input	2
Alarm output	2
Capacity	
Card capacity	700,000
Event capacity	700,000
Authentication	
Card type	EM card,M1 card, DESfire card
General	
Throughput	30 to 60 persons per minute The actual throughput is affected by the person passing rate and passing method.
IR light detectors	14 pairs
Lane width	550 mm to 1100 mm (21.65" to 43.31")
Distance between Barrier and Ground	1.2 m,1.4 m,1.6 m,1.8 m
Barrier material	Acrylic glass, Stainless steel pipe, Tempered glass with an approximate thickness of 0.10mm
Pedestal material	SUS/ANSI304 stainless steel 1.5mm
Built-in access controller	Yes
Power supply	100 to 240 VAC; 50 to 60 Hz
Working temperature	-20 °C to 65 °C (-4 °F to 149 °F)
Operations Mode	Open Mode, Close Mode
Power consumption	40 W (stand by)
Working humidity	0% to 95% (No Condensing)
Dimensions	With packaging: 1610 mm (63.39'') × 410 mm (16.14'') × 1255 mm (49.41''); Without packaging: 1500 mm (59.06'') × 130 mm (5.12'') × 1000 mm (39.37'');
Weight	(Net) Left: 62.78 kg (138.4 lbs); Middle: 82.4 kg (181.7 lbs); Right: 64.78 kg (142.8lbs); (Rough) Left: 101.18 kg (223.1 lbs); Middle: 45.54 kg (286.4 lbs); Right: 103.18 kg (227.5 lbs);
Card Collector Dropbox	Optional (Request in purchase order)
Application environment	Indoor and outdoor
Protective level	IPX4 (proved by Hikvision laboratory)
Configuration	
Module selection	YES
Lane width	550,650,750,900,1100
Pedestal length	1500 mm
Pedestal width	130 mm
Wall distance	20 mm

Base	YES
Barrier material	Acrylic glass
Authentication mode	Card,Face,QR code
Card type	EM,M1,Desfire
Recommended width	650
Base model	DS-K3B530X-BASE
Product type	Swing barrier
Remote controller type	NA

Maintenance

The main element of the turnstile is stainless steel, which is rustless (antioxidant) and corrosion resistant (The anti corrosion ability in the medium of acid, alkali, and salt). In order to keep the stainless steel from being oxidized or corroded, you should clean and care the turnstile surface periodically .

The instructions and tips for maintaining the turnstile are as follows:

- Select different stainless steel types according to the variety of the environments. You can select 304 stainless steel for common circumstances and 316 stainless steel for the scenarios of seasides and chemical plants.
- Keep the device surface clean and dry.
- Use non-woven cloth and ethyl alcohol to clean the dirt on the device surface.
- Use sourcing pad (do not use mesh cleaning ball) to clean the rust on the device surface by following the wire drawing on the stainless steel. And then use non-woven cloth and stainless steel cleaner to wipe the device surface.
- Clean and maintain the device by using non-woven cloth and stainless steel cleaner periodically. It is suggest to clean the device every month in common circumstances and every week for severe environments (seaside and chemical plants for instance).
- Resistant to shear and torsional forces.

▪ Available Model

DS-K3B530XM

DS-K3B530XM-L/MPg-Dp90(O-STD)

DS-K3B530XM-M/MPg-Dp90(O-STD)

DS-K3B530XM-R/MPg-Dp90(O-STD)

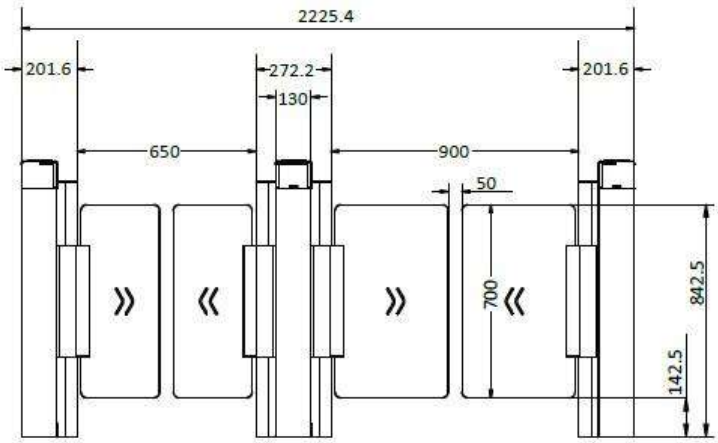
DS-K3B530XM-L/Pg-Dp65(O-STD)

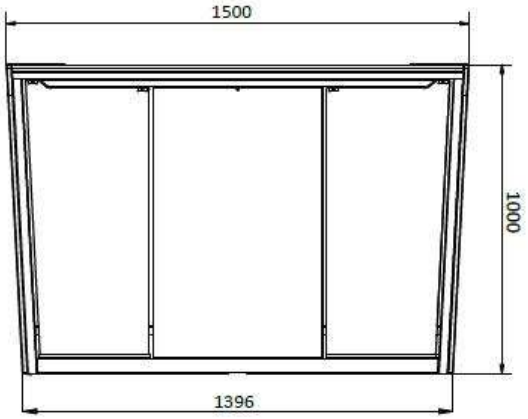
DS-K3B530XM-M/Pg-Dp65(O-STD)

DS-K3B530XM-R/Pg-Dp65(O-STD)

DS-K3B530XM-M/Pg-Dp65-90(O-STD)

▪ Dimension





▪ Accessory

▪ Optional

DS-K7SP01	DS-K7R01-433 Wireless Kefob 433MHz	DS-K7R01-868 Wireless Kefob 868MHz	DS-K3B530X-BASE
			

Headquarters
No.555 Qianmo Road, Binjiang District,
Hangzhou 310051, China
T +86-571-8807-5998
www.hikvision.com

Follow us on social media to get the latest product and solution information.

Hikvision HikvisionHQ HikvisionHQ Hikvision_Global Hikvision Corporate Channel hikvisionhq

DS-K3BC411X-RS-M1
Swing Barrier

The DS-K3BC411 series swing barrier is designed to detect unauthorized entrance or exit. By adopting the swing barrier integrated with the access control system, person should authenticate to pass through the lane via presenting IC or ID card, scanning QR code, etc. It is widely used in attractions, stadiums, construction sites, residences, etc.

- Valid passing duration settings: System will cancel the passing permission if a person does not pass through the lane within the valid passing duration
- Door remaining open when external or fire alarm triggered: The barrier will open automatically when alarm is triggered
- Barrier will be in free status when powering down
- Unauthorized person attempts to pass through the barrier, it has movement blocking

▪ Specification

System	
MCBF	> 3 million times
Motor	Brush motor
General	
Throughput	20 to 60 persons per minute The actual throughput is affected by the person passing rate and passing method.
Controller Board	Yes
Inductive Sensor	Yes
Barrier linear decelerator	Yes
Power supply method	100 to 240 VAC; 50 to 60 Hz
Working temperature	-10 °C to 60 °C
Lane width	600 mm to 1100 mm
Door opening angle	180 degrees
Barrier material	Stainless steel AISI304 ; Acrylic glass
Working humidity	10% to 95% (No Condensing)
Pedestal material	SUS/ANSI304 stainless steel
Dimensions	Without packaging: 1200 mm × 200 mm × 1020 mm (47.2" × 7.9" × 40.2") With packaging: 1408 mm × 348 mm × 1156 mm (55.4" × 13.7" × 45.5") Barrier thickness: 32mm
Application environment	Indoor
Weight	35 kg/38 kg (Left/Right) 77.2 lb/83.8 lb (Left/Right)

▪Maintenance

The main element of the turnstile is stainless steel, which is shock and vibration resistant, rustless (antioxidant) and corrosion resistant (The anti corrosion ability in the medium of acid, alkali, and salt). In order to keep the stainless steel from being oxidized or corroded, you should clean and care the turnstile surface periodically .

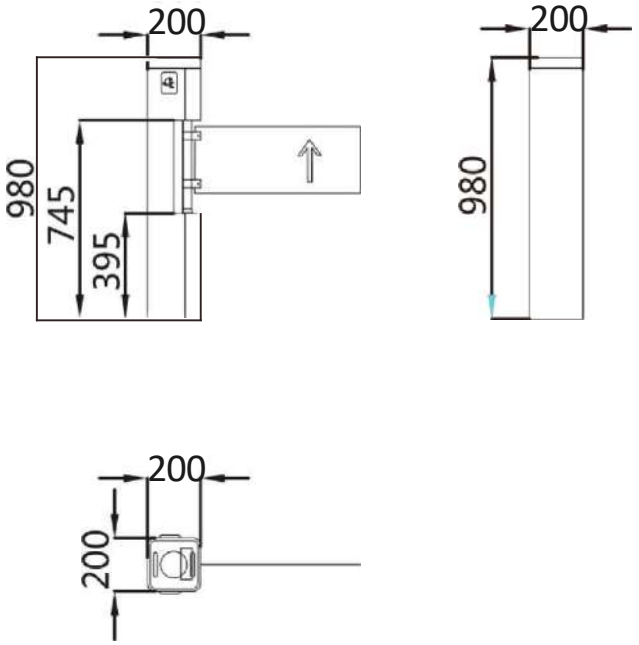
The instructions and tips for maintaining the turnstile are as follows:

- Select different stainless steel types according to the variety of the environments. You can select 304 stainless steel for common circumstances and 316 stainless steel for the scenarios of seasides and chemical plants.
- Keep the device surface clean and dry.
- Use non-woven cloth and ethyl alcohol to clean the dirt on the device surface.
- Use sourcing pad (do not use mesh cleaning ball) to clean the rust on the device surface by following the wire drawing on the stainless steel. And then use non-woven cloth and stainless steel cleaner to wipe the device surface.
- Clean and maintain the device by using non-woven cloth and stainless steel cleaner periodically. It is suggest to clean the device every month in common circumstances and every week for severe environments (seaside and chemical plants for instance).
- Maintenance access tilting top cover and side cover.

▪ Available Model

DS-K3BC411X-RS-M1/Pg-Dm90(O-STD)
DS-K3BC411X-RS-M1/Pg-Dm90(O-STD)/sensor
DS-K3BC411X-RS-M/Pg-Dm90(O-STD)
DS-K3BC411X-RS-M/Pg-Dm90(O-STD)/sensor

▪**Dimension**



DS-K4H255-LZ
Accessary of Magnetic Lock

- Bracket for DS-K4H255S
- L bracket is used for fixed lock body
- Z bracket is used for suction plate fixed, is equipped with antiskid and structure adjustment

▪ Specification

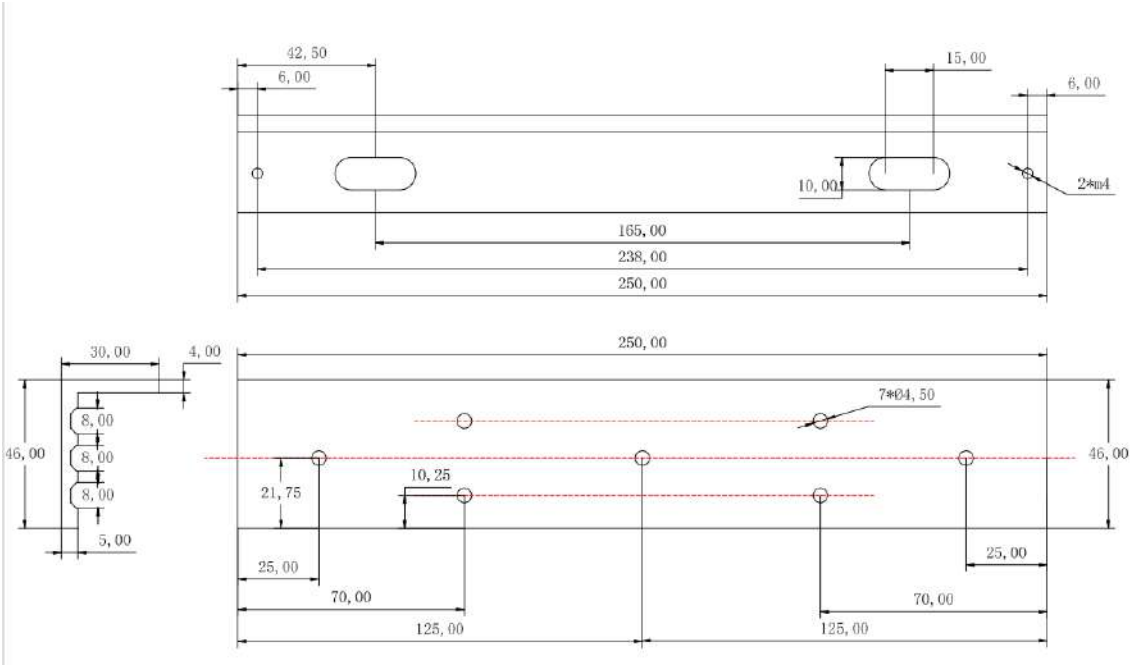
General	
Dimensions	L-bracket: 250 mm × 46 mm × 30 mm (9.8" × 1.8" × 1.2") Z-bracket: 180 mm × 47 mm × 47 mm (7.1" × 1.9" × 1.9")
Weight	0.5 kg (1.1 lb)
Material	High strength aluminum alloy surface sandblasting oxidation
Door type	Wooden Door, Glass Door, Metal Door
Bracket of Magnetic Lock	
Suitable Door	Wooden Door, Glass Door, Metal Door

**Bracket for DS-K4H255S*

▪ Available Model

DS-K4H255-LZ

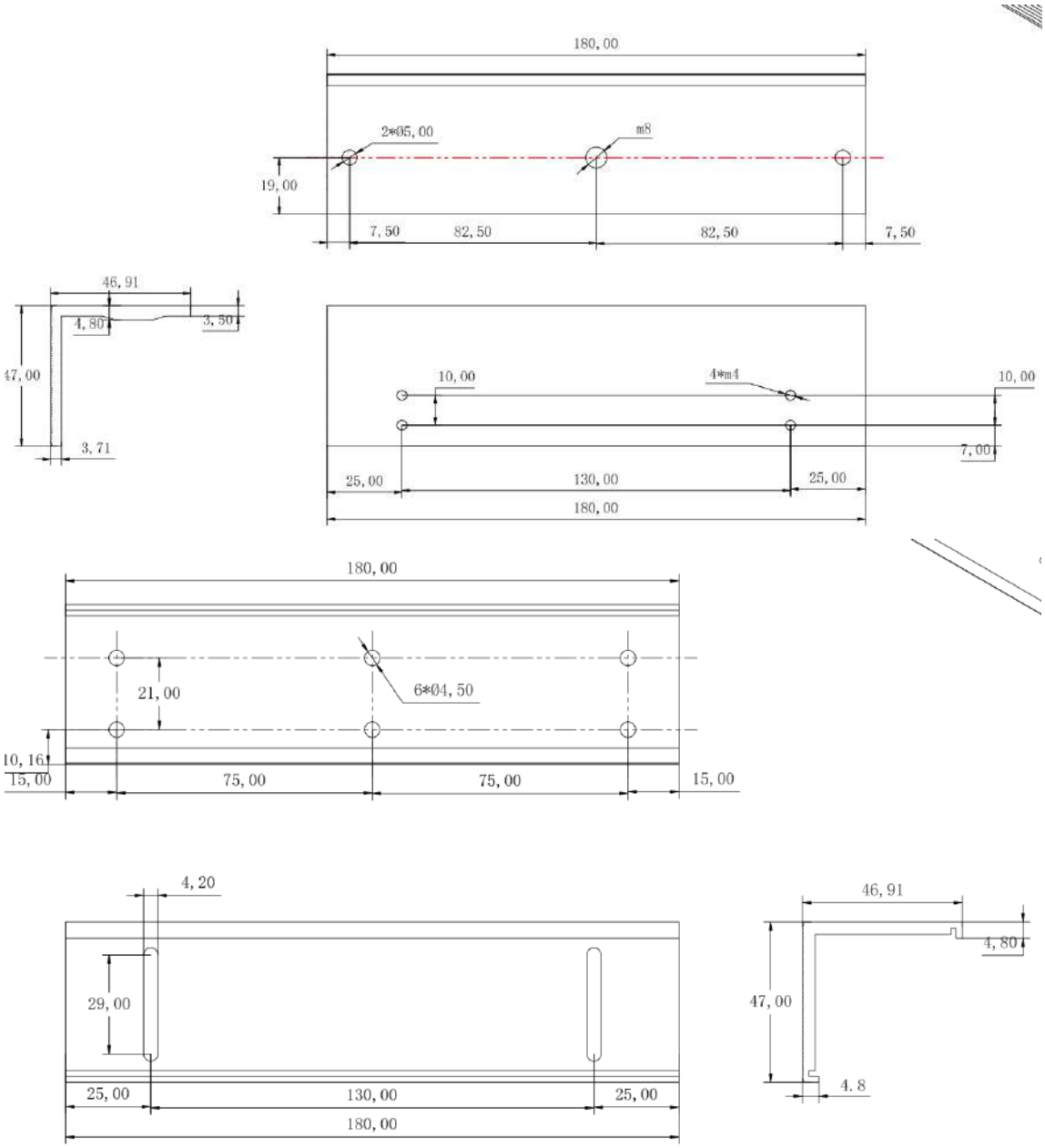
▪ Dimension



Headquarters
No.555 Qianmo Road, Binjiang District,
Hangzhou 310051, China
T +86-571-8807-5998
www.hikvision.com

Follow us on social media to get the latest product and solution information.

Hikvision HikvisionHQ HikvisionHQ Hikvision_Global Hikvision Corporate Channel hikvisionhq



Headquarters
No.555 Qianmo Road, Binjiang District,
Hangzhou 310051, China
T +86-571-8807-5998
www.hikvision.com

Follow us on social media to get the latest product and solution information.

Hikvision HikvisionHQ HikvisionHQ Hikvision_Global Hikvision Corporate Channel hikvisionhq

▪ Accessory

▪ Included

DS-K4H255S Value Magnetic Locks


Headquarters
No.555 Qianmo Road, Binjiang District,
Hangzhou 310051, China
T +86-571-8807-5998
www.hikvision.com

DS-TMG022 Vehicle Detector

Introduction

DS-TMG022 is a 2-ch loop-based digital vehicle detector. The device is designed with high reliability, and equipped with high performance microprocessor and channel sequence scanning technology. With functions of frequency self-adaption and full environment tracking, the device can track passing vehicles in a fast, effective and accurate way. The device integrates standard vehicle counting algorithm, and can be widely deployed in entrance/exit systems with traffic cameras.

Features and Functions

- 2 inputs of inductive loops
- Recognizes vehicles of more than two wheels
- Provides traffic statistics including traffic flow, speed and length
- Detects traffic events including forward/wrong-way driving and speeding
- Built-in EEPROM for saving configuration parameters in power cut
- Accepts traffic lights connection to upload light status
- Fault detection to output operating status of loops and traffic light detector
- Voltage surge protection

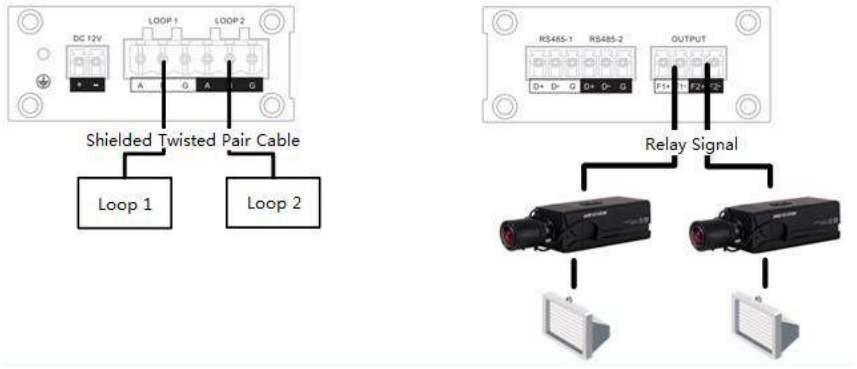
Available Models

DS-TMG022

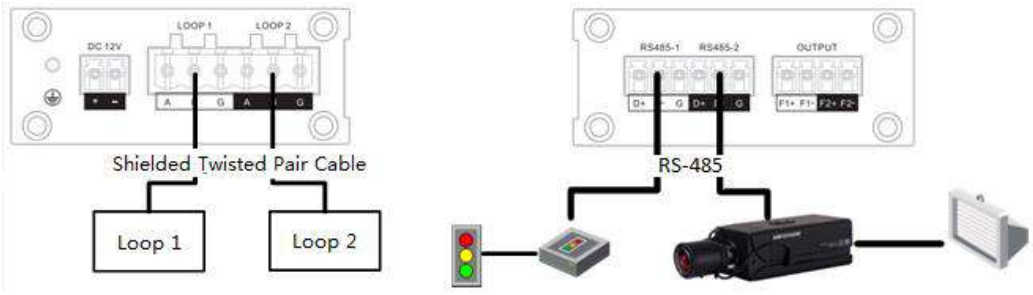
Specifications

Model	DS-TMG022
Inductance self-tuning range	20 to 1000 μH
Vehicle detection rate	≥ 99%
Sensitivity (-△L/L)	0.02% to 0.96%, 4 levels adjustable
Loop operating frequency	28 KHz to 120 KHz, 4 levels adjustable (highest, high, low, lowest)
Max. response time	32±2ms
Loop fault recovery time	≤ 100ms
Loop fault detection interval	≤ 10ms
Output port	2 relay output, VDRM 70 V, max. current 30 mA
Power supply	220 VAC
Power consumption	≤ 3 W
Operating temperature	-30 °C to +70 °C (-31 °F to 167 °F)
Operating humidity	< 90%, non-condensing
Dimensions	105 × 88 × 40mm

Typical Application



Relay Signal Application 1



Relay Signal Application 2

DS-K3B530XM
Swing Barrier

The DS-K3B530X series swing barrier with 14 pairs of IR lights is designed to detect unauthorized entrance or exit. By adopting the swing barrier integratedly with the access control system, person should authenticate to pass through the lane via presenting IC or ID card, scanning QR code, etc. It is widely used in office building, hotels, residences, etc.

- 14 pairs of IR light detectors: Permissions validation and anti-tailgating.
- LED light indicates passing direction.
- Valid passing duration settings: System will cancel the passing permission if a person does not pass through the lane within the valid passing duration.
- Support speaker and remote control keyfob optional, need to order separately.
- Person count with 90% accuracy
- Easy of unidirectional and bidirectional configurations according to the needs of the scenario
- Customizable pictogram according to the control set for input and output

▪ Specification

System	
Motor	Servo motor (Noiseless engine)
MCBF	≥ 12 million times
Interface	
Network interface	10 M/100 M x 1
Lock control	2
Exit button	2
Alarm input	2
Alarm output	2
Capacity	
Card capacity	700,000
Event capacity	700,000
Authentication	
Card type	EM card,M1 card, DESfire card
General	
Throughput	30 to 60 persons per minute The actual throughput is affected by the person passing rate and passing method.
IR light detectors	14 pairs
Lane width	550 mm to 1100 mm (21.65" to 43.31")
Distance between Barrier and Ground	1.2 m,1.4 m,1.6 m,1.8 m
Barrier material	Acrylic glass, Stainless steel pipe, Tempered glass with an approximate thickness of 0.10mm
Pedestal material	SUS/ANSI304 stainless steel 1.5mm
Built-in access controller	Yes
Power supply	100 to 240 VAC; 50 to 60 Hz
Working temperature	-20 °C to 65 °C (-4 °F to 149 °F)
Operations Mode	Open Mode, Close Mode
Power consumption	40 W (stand by)
Working humidity	0% to 95% (No Condensing)
Dimensions	With packaging: 1610 mm (63.39'') × 410 mm (16.14'') × 1255 mm (49.41''); Without packaging: 1500 mm (59.06'') × 130 mm (5.12'') × 1000 mm (39.37'');
Weight	(Net) Left: 62.78 kg (138.4 lbs); Middle: 82.4 kg (181.7 lbs); Right: 64.78 kg (142.8lbs); (Rough) Left: 101.18 kg (223.1 lbs); Middle: 45.54 kg (286.4 lbs); Right: 103.18 kg (227.5 lbs);
Card Collector Dropbox	Optional (Request in purchase order)
Application environment	Indoor and outdoor
Protective level	IPX4 (proved by Hikvision laboratory)
Configuration	
Module selection	YES
Lane width	550,650,750,900,1100
Pedestal length	1500 mm
Pedestal width	130 mm
Wall distance	20 mm

Base	YES
Barrier material	Acrylic glass
Authentication mode	Card,Face,QR code
Card type	EM,M1,Desfire
Recommended width	650
Base model	DS-K3B530X-BASE
Product type	Swing barrier
Remote controller type	NA

Maintenance

The main element of the turnstile is stainless steel, which is rustless (antioxidant) and corrosion resistant (The anti corrosion ability in the medium of acid, alkali, and salt). In order to keep the stainless steel from being oxidized or corroded, you should clean and care the turnstile surface periodically .

The instructions and tips for maintaining the turnstile are as follows:

- Select different stainless steel types according to the variety of the environments. You can select 304 stainless steel for common circumstances and 316 stainless steel for the scenarios of seasides and chemical plants.
- Keep the device surface clean and dry.
- Use non-woven cloth and ethyl alcohol to clean the dirt on the device surface.
- Use sourcing pad (do not use mesh cleaning ball) to clean the rust on the device surface by following the wire drawing on the stainless steel. And then use non-woven cloth and stainless steel cleaner to wipe the device surface.
- Clean and maintain the device by using non-woven cloth and stainless steel cleaner periodically. It is suggest to clean the device every month in common circumstances and every week for severe environments (seaside and chemical plants for instance).
- Resistant to shear and torsional forces.

▪ Available Model

DS-K3B530XM

DS-K3B530XM-L/MPg-Dp90(O-STD)

DS-K3B530XM-M/MPg-Dp90(O-STD)

DS-K3B530XM-R/MPg-Dp90(O-STD)

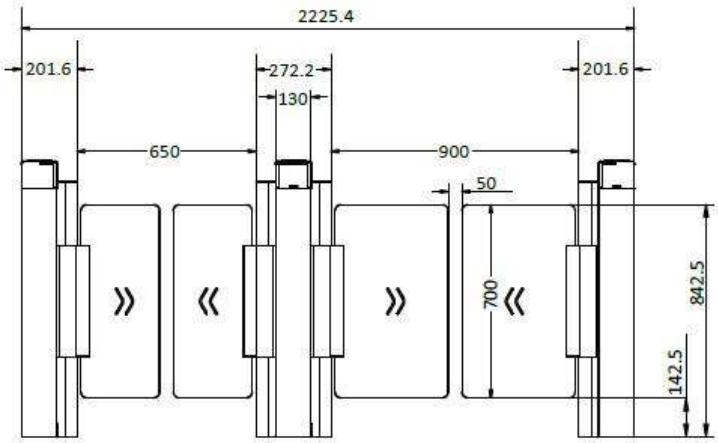
DS-K3B530XM-L/Pg-Dp65(O-STD)

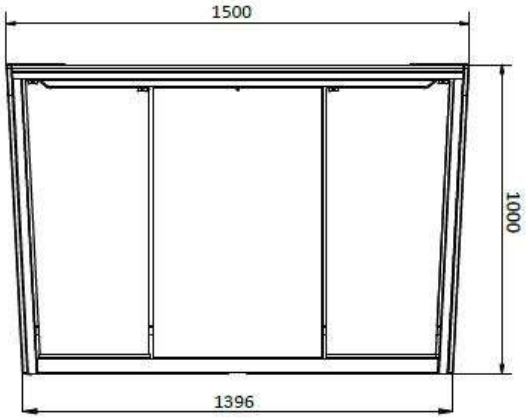
DS-K3B530XM-M/Pg-Dp65(O-STD)

DS-K3B530XM-R/Pg-Dp65(O-STD)

DS-K3B530XM-M/Pg-Dp65-90(O-STD)

▪ Dimension





▪ Accessory

▪ Optional

DS-K7SP01	DS-K7R01-433 Wireless Kefob 433MHz	DS-K7R01-868 Wireless Kefob 868MHz	DS-K3B530X-BASE
			

Headquarters
No.555 Qianmo Road, Binjiang District,
Hangzhou 310051, China
T +86-571-8807-5998
www.hikvision.com

Follow us on social media to get the latest product and solution information.

Hikvision HikvisionHQ HikvisionHQ Hikvision_Global Hikvision Corporate Channel hikvisionhq

Cliente de Controle HikCentral Professional V2.6.1

Manual do Usuário

Informação Legal

Sobre este dDocumento

- Este Documento inclui instruções para usar e gerenciar o Produto. Fotos, gráficos, imagens e todas as outras informações a seguir são apenas para descrição e explicação.
- As informações contidas no Documento estão sujeitas a alterações, sem aviso prévio, devido a atualizações de firmware ou outros motivos. Encontre a versão mais recente do Documento no site da Hikvision (***https://www.hikvision.com***). A menos que acordado de outra forma, a Hangzhou Hikvision Digital Technology Co., Ltd. ou suas afiliadas (doravante denominadas "Hikvision") não oferecem garantias, expressas ou implícitas.
- Utilize o Documento com a orientação e assistência de profissionais treinados para dar suporte ao Produto.

Sobre este Produto

Este produto só pode usufruir do suporte de serviço pós-venda no país ou região onde a compra foi feita.

Reconhecimento dos Direitos de Propriedade Intelectual

- A Hikvision detém os direitos autorais e/ou patentes relacionadas à tecnologia incorporada nos Produtos descritos neste Documento, que podem incluir licenças obtidas de terceiros.
- Qualquer parte do Documento, incluindo texto, imagens, gráficos, etc., pertence à Hikvision. Nenhuma parte deste Documento pode ser extraída, copiada, traduzida ou modificada no todo ou em parte por quaisquer meios sem permissão por escrito.
- **HIKVISION** e outras marcas registradas e logotipos da Hikvision são propriedades da Hikvision em várias jurisdições.
- Outras marcas registradas e logotipos mencionados são de propriedade de seus respectivos donos.

AVISO LEGAL

- ATÉ O LIMITE MÁXIMO PERMITIDO PELA LEI APLICÁVEL, ESTE DOCUMENTO E O PRODUTO DESCRITO, COM SEU HARDWARE, SOFTWARE E FIRMWARE, SÃO FORNECIDOS "COMO ESTÃO" E "COM TODAS AS FALHAS E ERROS". A HIKVISION NÃO OFERECE NENHUMA GARANTIA, EXPRESSA OU IMPLÍCITA, INCLUINDO, SEM LIMITAÇÃO, COMERCIALIZAÇÃO, QUALIDADE SATISFATÓRIA OU ADEQUAÇÃO A UM DETERMINADO FIM. O USO DO PRODUTO POR VOCÊ É POR SUA PRÓPRIA CONTA E RISCO. EM NENHUMA HIPÓTESE A HIKVISION SERÁ RESPONSÁVEL POR QUAISQUER DANOS ESPECIAIS, CONSEQUENCIAIS, INCIDENTAIS OU INDIRETOS, INCLUINDO, ENTRE OUTROS, DANOS POR PERDA DE LUCROS COMERCIAIS, INTERRUPÇÃO DE NEGÓCIOS OU PERDA DE DADOS, CORRUPÇÃO DE SISTEMAS OU PERDA DE DOCUMENTAÇÃO, SEJA COM BASE EM VIOLAÇÃO DE CONTRATO, ATO ILÍCITO (INCLUINDO NEGLIGÊNCIA), RESPONSABILIDADE DO PRODUTO OU DE OUTRA FORMA, EM CONEXÃO COM O USO DO PRODUTO, MESMO QUE A HIKVISION TENHA SIDO AVISADA DA POSSIBILIDADE DE TAIS DANOS OU PERDAS.

- VOCÊ RECONHECE QUE A NATUREZA DA INTERNET PROPORCIONA RISCOS DE SEGURANÇA INERENTES, E A HIKVISION NÃO ASSUMIRÁ QUALQUER RESPONSABILIDADE POR OPERAÇÃO ANORMAL, VAZAMENTO DE PRIVACIDADE OU OUTROS DANOS RESULTANTES DE ATAQUE CIBERNÉTICO, ATAQUE DE HACKER, INFECÇÃO DE VÍRUS OU OUTROS RISCOS DE SEGURANÇA DA INTERNET; NO ENTANTO, A HIKVISION FORNECERÁ SUPORTE TÉCNICO OPORTUNO, SE NECESSÁRIO.
- VOCÊ CONCORDA EM USAR ESTE PRODUTO EM CONFORMIDADE COM TODAS AS LEIS APLICÁVEIS, E VOCÊ É O ÚNICO RESPONSÁVEL POR GARANTIR QUE SEU USO ESTEJA EM CONFORMIDADE COM A LEI APLICÁVEL. ESPECIALMENTE, VOCÊ É RESPONSÁVEL POR USAR ESTE PRODUTO DE UMA MANEIRA QUE NÃO VIOLE OS DIREITOS DE TERCEIROS, INCLUINDO, MAS SEM SE LIMITAR A, DIREITOS DE PUBLICIDADE, DIREITOS DE PROPRIEDADE INTELECTUAL OU PROTEÇÃO DE DADOS E OUTROS DIREITOS DE PRIVACIDADE. VOCÊ NÃO DEVE USAR ESTE PRODUTO PARA QUALQUER USO FINAL PROIBIDO, INCLUINDO O DESENVOLVIMENTO OU PRODUÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA, O DESENVOLVIMENTO OU PRODUÇÃO DE ARMAS QUÍMICAS OU BIOLÓGICAS, QUAISQUER ATIVIDADES NO CONTEXTO RELACIONADAS A QUALQUER EXPLOSIVO NUCLEAR OU CICLO DE COMBUSTÍVEL NUCLEAR INSEGURO, OU EM APOIO A ABUSOS DE DIREITOS HUMANOS.
- EM CASO DE QUALQUER CONFLITO ENTRE ESTE DOCUMENTO E A LEI APLICÁVEL, ESTA ÚLTIMA PREVALECERÁ.

Convenções de Símbolos

Os símbolos que podem ser encontrados neste documento são definidos da seguinte forma.

Símbolo	Descrição
Perigo	Indica uma situação perigosa que, se não for evitada, poderá resultar em morte ou ferimentos graves.
Cuidado	Indica uma situação potencialmente perigosa que, se não for evitada, pode resultar em danos ao equipamento, perda de dados, degradação do desempenho ou resultados inesperados.
Observação	Fornece informações adicionais para enfatizar ou complementar pontos importantes do texto principal.

Conteúdo

Capítulo 1 Sobre o Control Client

Como um dos principais componentes do sistema, o Control Client fornece diversas funções, incluindo visualização ao vivo em tempo real, controle PTZ, reprodução e download de vídeo, recebimento de alarmes, pesquisa de registros e assim por diante.
Este manual do usuário descreve a função, configuração e etapas de operação do Control Client. Para garantir o uso adequado e a estabilidade do cliente, consulte o conteúdo abaixo e leia o manual cuidadosamente antes da operação.

Observação

As funções no Control Client variam de acordo com a Licença que você comprou e os aplicativos que você instalou e habilitou. Para informações detalhadas.

Para mais informações sobre este produto, consulte os seguintes documentos.

Aprender

- ***Ficha de dados***
- ***Requisitos e desempenho do sistema***
- ***Lista de compatibilidade***
- ***Lista de compatibilidade de produtos de terceiros***
- ***Comparação de produtos entre a versão gratuita e a versão profissional***
- ***Especificação AE***
- ***Notas de Lançamento***
- ***Lista de funções do cliente móvel***

Começar

- ***Guia de início rápido***
- ***Guia de Endurecimento***

Usar

Perguntas frequentes

Capítulo 2 Guia de Documento

Aprender

- ***Ficha de dados***
- ***Requisitos e desempenho do sistema***
- ***Lista de compatibilidade de produtos Hikvision***
- ***Lista de compatibilidade de produtos de terceiros***
- ***Comparação de produtos entre a versão gratuita e a versão profissional***
- ***Especificação AE***
- ***Notas de Lançamento***
- ***Guia de início rápido do cliente móvel***

Começar

- ***Guia de início rápido***
- ***Guia de Endurecimento***

Usar

- ***Manual do usuário do cliente da Web***
- ***Manual do usuário do cliente de controle***
- ***Perguntas frequentes***

Capítulo 3 Login

Efetue login no sistema por meio do Control Client para operações.

3.1 Primeiro Login

Quando um usuário normal (exceto o usuário administrador) faz login no sistema pela primeira vez, ele/ela deve alterar a senha inicial e definir uma nova senha para login.

Antes de começar

Ao efetuar login no sistema pela primeira vez, você deverá criar uma senha para o usuário administrador predefinido do sistema (chamado admin) no Web Client antes de poder configurar e operar o sistema corretamente.

Execute as seguintes etapas ao acessar o sistema por meio do Control Client pela primeira vez como um usuário normal (exceto administrador).

Passos

1. Clique duas vezes na área de trabalho para executar o Control Client.

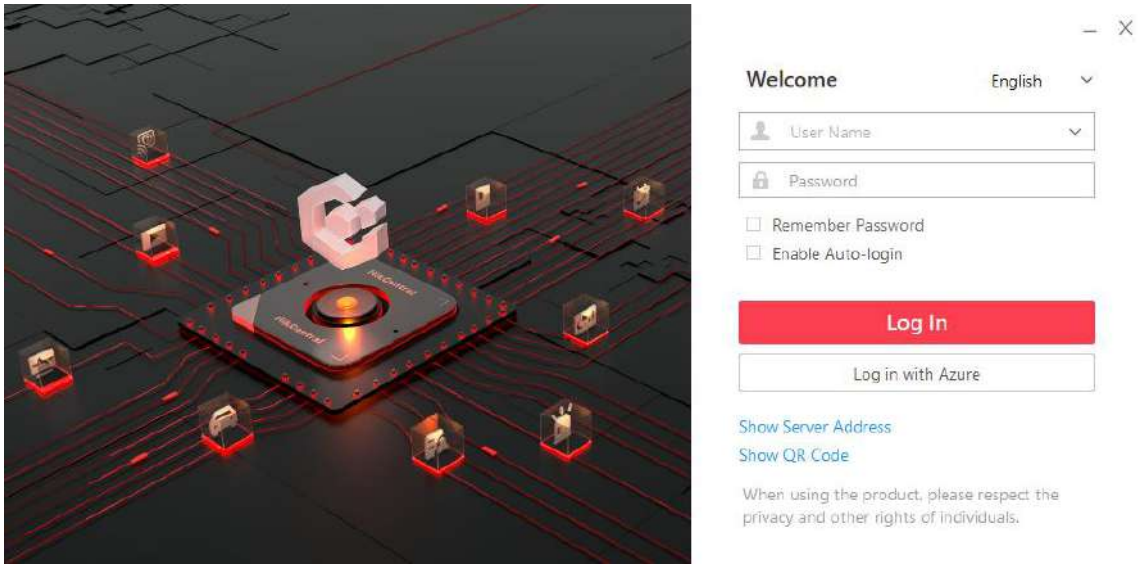


Figura 3-1 Página de login

2. Insira os parâmetros do servidor.

Observação

Você pode clicar em **Ocultar endereço do servidor** ou **Mostrar endereço do servidor** para ocultar ou mostrar as informações de rede do servidor.

Endereço do servidor

Insira o endereço (endereço IP ou nome de domínio) do servidor que executa o serviço SYS ao qual você deseja se conectar.

Porta

Insira o número da porta do servidor onde o serviço SYS está sendo executado. O número da porta padrão é 80.

3. Digite o nome de usuário e a senha do HikCentral Professional.

Observação

- Entre em contato com o administrador para obter o nome de usuário e a senha inicial.
- Para contas de usuário de domínio, você pode marcar a opção **Inicialização automática** para não precisar iniciar manualmente o Control Client na próxima vez que ligar o computador.

4. Clique **em Entrar** .
5. Defina uma nova senha e confirme-a.

Cuidado

A força da senha do dispositivo pode ser verificada pelo sistema. Recomendamos fortemente que você altere a senha de sua escolha (usando um mínimo de 8 caracteres, incluindo pelo menos três tipos das seguintes categorias: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. E recomendamos que você redefina sua senha regularmente, especialmente no sistema de alta segurança, redefinir a senha mensalmente ou semanalmente pode proteger melhor seu produto.
A configuração adequada de todas as senhas e outras configurações de segurança é de responsabilidade do instalador e/ou usuário final.

6. Clique em **Login** para alterar a senha.
   Você entra na página inicial do Control Client depois de alterar a senha.

3.2 Login Normal (Não É a Primeira Vez)

Normalmente, você pode fazer login na plataforma com o nome de usuário e a senha do HikCentral Professional como um usuário normal.

Passos

1. Clique duas vezes  na área de trabalho para executar o Control Client.

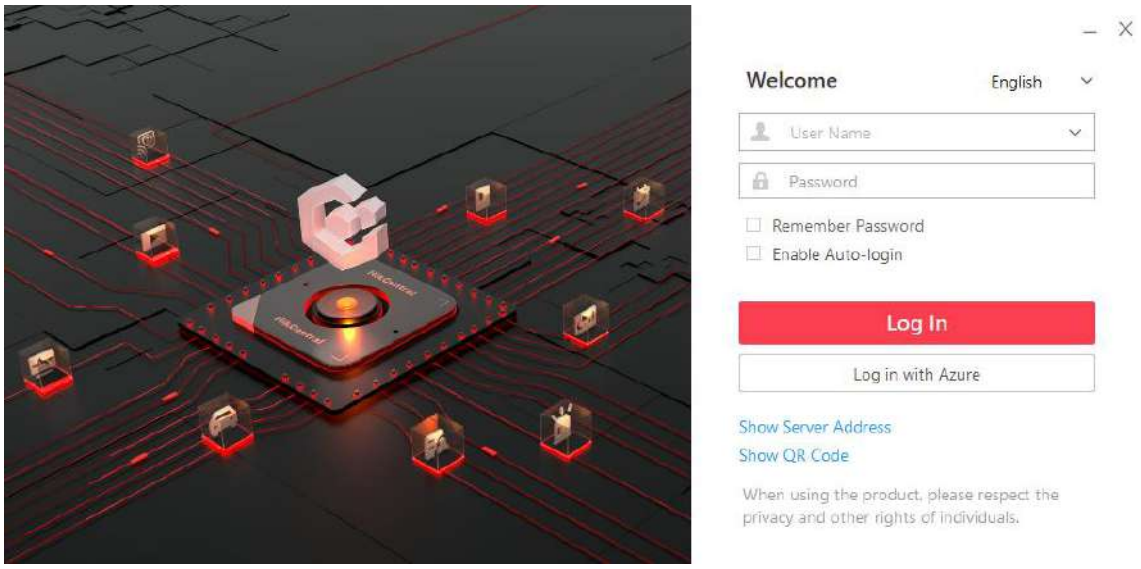


Figura 3-2 Página de login

2. Insira os parâmetros do servidor.

Observação

Você pode clicar em **Ocultar endereço do servidor** ou **Mostrar endereço do servidor** para ocultar ou mostrar as informações de rede do servidor.

Endereço do servidor

Insira o endereço (endereço IP ou nome de domínio) do servidor que executa o serviço SYS ao qual você deseja se conectar.

Porta

Insira o número da porta do servidor onde o serviço SYS está sendo executado. O número da porta padrão é 80.

3. Digite o nome de usuário e a senha do HikCentral Professional.
4. **Opcional**: marque a caixa de seleção **Lembrar senha** para manter a senha.
5. **Opcional**: marque a caixa de seleção **Habilitar login automático** para efetuar login no software automaticamente no próximo login.

Observação

Para contas de usuário de domínio, você pode marcar a opção **Inicialização automática** para não precisar iniciar manualmente o Control Client na próxima vez que ligar o computador.

6. Clique **em Entrar** .

Observação

- Se uma tentativa de senha com falha do usuário atual for detectada, você deverá inserir o código de verificação antes de poder efetuar login. A tentativa de senha com falha do cliente

atual, de outro cliente e de outro endereço exigirá o código de verificação.
- A tentativa de senha com falha do cliente atual, outro cliente (por exemplo, Control Client) e outro endereço serão todos acumulados. Seu endereço IP será bloqueado por um período de tempo especificado após um número específico de tentativas de senha ou código de verificação com falha. Para configurações detalhadas de tentativas de login com falha e duração do bloqueio, consulte o *Manual do Usuário do HikCentral Professional Web Client* .
- A conta será congelada por 30 minutos após 5 tentativas de senha com falha. A tentativa de senha com falha do cliente atual, outro cliente (por exemplo, Control Client) e outro endereço serão todos acumulados.
- Quando a conta é congelada após várias tentativas frustradas de senha, você ainda pode tentar fazer login em outro PC.
- A força da senha pode ser verificada pelo sistema e deve atender aos requisitos do sistema. Se a força da senha for menor que a força mínima necessária, você será solicitado a alterar sua senha. Para configurações detalhadas da força mínima da senha, consulte o *Manual do Usuário do HikCentral Professional Web Client* .
- Se sua senha expirou, você deve alterá-la ao fazer login. Para configurações detalhadas da idade máxima da senha, consulte o *Manual do Usuário do HikCentral Professional Web Client* .

Entre na página inicial do Control Client.

3.3 Login por Meio de Uma Conta do Azure

Após concluir as configurações necessárias na plataforma Azure e importar usuários e pessoas do domínio para o HikCentral Professional.

Antes de começar

- Conclua as configurações na plataforma Azure, incluindo a criação de locatários, registros de aplicativos e a criação de novos grupos e novos usuários.
- Conclua a configuração do diretório ativo no HikCentral Professional. Veja *o Manual do Usuário do HikCentral Professional Web Client* .
- Importe usuários de domínio e pessoas de domínio para o HikCentral Professional. Veja *o Manual do Usuário do HikCentral Professional Web Client* .

Passos

1. Clique duas vezes  na área de trabalho para executar o Control Client.

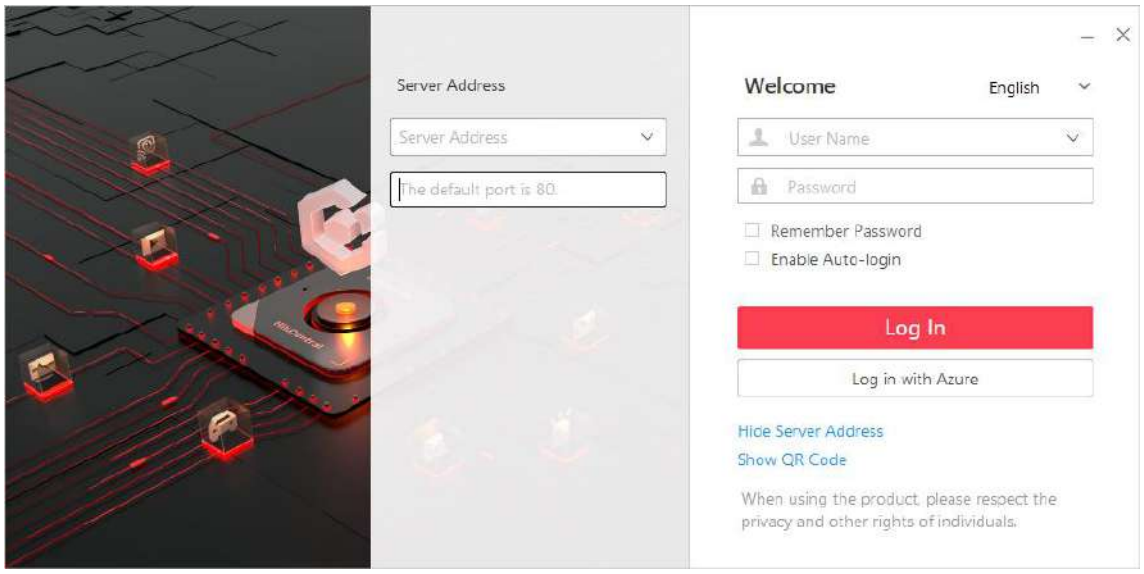


Figura 3-3 Página de login

2. Insira os parâmetros do servidor.

Observação

Você pode clicar em **Ocultar endereço do servidor** ou **Mostrar endereço do servidor** para ocultar ou mostrar as informações de rede do servidor.

Endereço do servidor

Insira o endereço (endereço IP ou nome de domínio) do servidor que executa o serviço SYS ao qual você deseja se conectar.

Porta

Insira o número da porta do servidor onde o serviço SYS está sendo executado. O número da porta padrão é 80.

3. Digite o nome de usuário e a senha do Azure.
4. Opcional: marque a caixa de seleção **Lembrar senha** para manter a senha.
5. Opcional: marque a caixa de seleção **Habilitar login automático** para efetuar login no software automaticamente no próximo login.

Observação

Para contas de usuário de domínio, você pode marcar a opção **Inicialização automática** para não precisar iniciar manualmente o Control Client na próxima vez que ligar o computador.

6. Clique em **Fazer login com o Azure** .
   No primeiro login, a página de login da Microsoft será exibida.
7. Opcional: Na página de login da Microsoft, insira sua conta de domínio e senha e efetue login na conta.
   A página inicial é exibida após você efetuar login com sucesso no sistema.

3.4 Alterar Senha para Redefinir Usuário e Login

Se a senha do usuário normal for redefinida para a senha inicial pelo administrador, ele/ela deverá alterar a senha inicial e definir uma nova senha ao efetuar login novamente.

Passos

1. Clique duas vezes na área de trabalho para executar o Control Client.

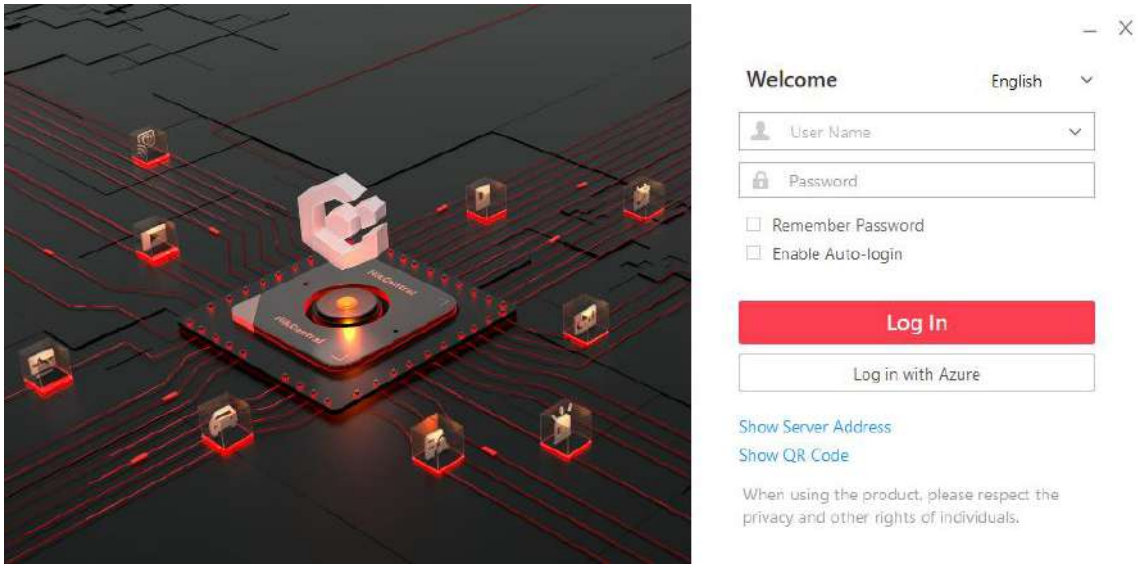


Figura 3-4 Página de login

2. Insira os parâmetros do servidor.

Endereço do servidor

Digite o endereço (endereço IP ou nome de domínio) do servidor que executa o SYS ao qual você deseja se conectar.

Porta

Insira o número da porta do servidor onde o SYS está sendo executado. O número da porta padrão é 80.

Observação

Você pode clicar em **Ocultar endereço do servidor** ou **Mostrar endereço do servidor** para ocultar ou mostrar as informações de rede do servidor.

3. Digite o nome de usuário e a senha do HikCentral Professional.

Observação

- Entre em contato com o administrador para obter o nome de usuário e a senha inicial.
- Para contas de usuário de domínio, você pode marcar a opção **Inicialização automática** para não precisar iniciar manualmente o Control Client na próxima vez que ligar o computador.

4. Clique **em Entrar** .
5. Clique em **Fechar** na caixa de diálogo pop-up para continuar.
6. Defina uma nova senha e confirme-a.

Cuidado

A força da senha do dispositivo pode ser verificada pelo sistema. Recomendamos fortemente que você altere a senha de sua escolha (usando um mínimo de 8 caracteres, incluindo pelo menos três tipos das seguintes categorias: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. E recomendamos que você redefina sua senha regularmente, especialmente no sistema de alta segurança, redefinir a senha mensalmente ou semanalmente pode proteger melhor seu produto.
A configuração adequada de todas as senhas e outras configurações de segurança é de responsabilidade do instalador e/ou usuário final.

7. Clique em **Login** para alterar a senha.
   Você entra na página inicial do Control Client depois de alterar a senha.

Capítulo 4 Visão Geral da Página Inicial

A página inicial padrão mostra um painel de controle que fornece uma visão geral da navegação sobre os módulos de função de forma visível, ou seja, Monitoramento de Alarme, Status de Saúde e Mapa, para acesso rápido e conveniente.
Clique no canto superior esquerdo do Control Client para entrar na página inicial.

Observação

- Os recursos e parâmetros suportados estão sujeitos aos aplicativos instalados.
- Você pode personalizar o painel de controle no modo Home page padrão e ajustar o arranjo do módulo como desejar. Para detalhes, consulte ***Personalizar Painel de Controle*** .
- O modo padrão da página inicial é o Modo de visualização. No primeiro login, um prompt aparecerá na parte superior da página inicial, você pode clicar em **Alternar** para alternar o modo para o Modo de menu. Se quiser restaurar o modo padrão, você pode ir para a página Sistema e definir. Para obter detalhes, consulte ***Definir frequência de atualização automática para o painel de controle digital*** .

O HikCentral Professional Control Client é composto pelos seguintes módulos de função por padrão.

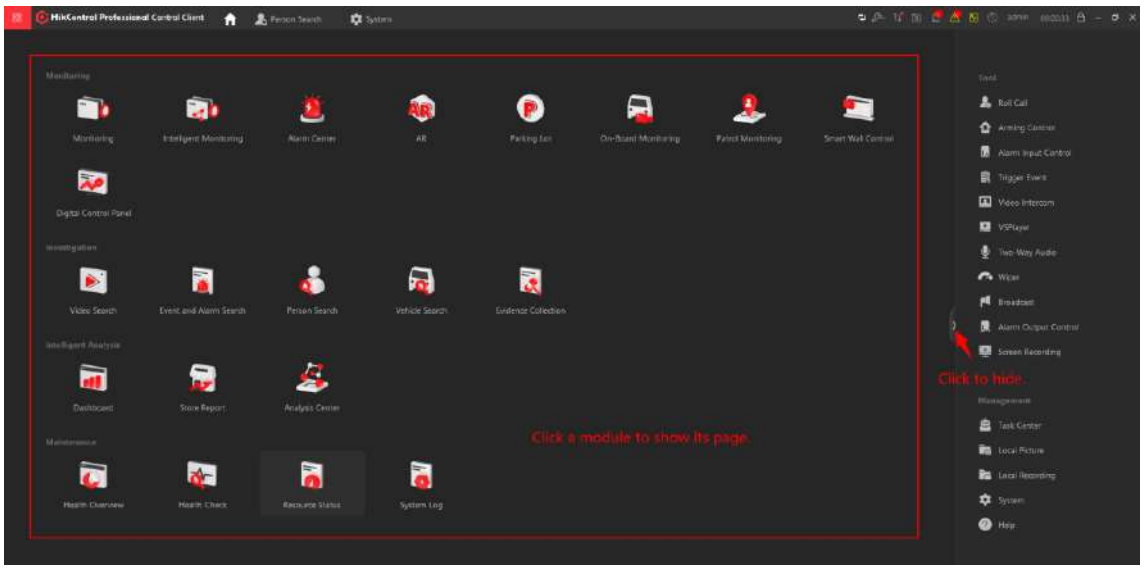


Figura 4-1 Página inicial

Tabela 4-1 Introdução à ferramenta e gerenciamento

Seção	Módulo	Descrição
Ferramenta	Chamada	O módulo de chamada fornece a função de chamada para pessoas em grupos de contagem de emergência quando ocorre uma emergência.

Seção	Módulo	Descrição
		Para mais detalhes, consulte ***Iniciar uma chamada*** .
	Controle de Armar	O módulo Arming Control fornece o arme e o desarme dos recursos gerenciados no sistema. Para obter mais detalhes, consulte ***Executar controle de armamento para alarmes*** .
	Vídeo Porteiro	O módulo de interfone com vídeo permite conversação por voz com os moradores por meio de chamadas para suas estações internas. Para mais detalhes, consulte ***Videoporteiro*** .
	VSPlayer	No módulo VSPlayer, você pode executar o software e reproduzir arquivos de vídeo armazenados no PC local. Para mais detalhes, consulte ***Reproduzir vídeo via VSPlayer*** .
	Áudio Bidirecional	O módulo de áudio bidirecional fornece a função de conversação por voz entre o Control Client e os dispositivos, além de oferecer suporte à obtenção e reprodução de áudio em tempo real no Control Client. Para mais detalhes, consulte ***Executar áudio bidirecional*** .
	Transmissão	O módulo Broadcast fornece a função de distribuir o conteúdo de áudio para o dispositivo adicionado se o dispositivo tiver uma saída de áudio. Para mais detalhes, consulte ***Transmissão para dispositivos conectados***
	Controle de Saída de Alarme	O módulo de controle de saída de alarme fornece a função de controlar a saída de alarme remotamente pelo Control Client. Para mais detalhes, consulte ***Entrada/Saída de Alarme de Controle*** .
	Telas de Gravação	A ferramenta Record Screen é usada para gravar operações nas telas. Os arquivos de vídeo gravados podem ser salvos como evidência. Para mais detalhes, consulte ***Outras ferramentas*** .
	Limpador	Clique em **Wiper** e selecione a(s) câmera(s) para habilitar o limpador rapidamente.

Seção	Módulo	Descrição
Gerenciamento	Centro de Tarefas	O módulo Central de Tarefas oferece suporte à visualização e ao gerenciamento de tarefas de download. Para mais detalhes, consulte ***Gerenciar tarefas de download/upload*** .
	Imagem Local	O módulo Imagem local fornece a pesquisa e o gerenciamento de imagens locais.
	Gravação Local	O módulo Gravação Local fornece a pesquisa e o gerenciamento de arquivos de vídeo locais.
	Sistema	O módulo Sistema fornece configurações básicas e configurações do aplicativo. Para mais detalhes, consulte ***Configurações do sistema*** .
	Ajuda	O módulo Ajuda fornece informações de ajuda, como manual do usuário, detalhes da licença e versão do software do Control Client.

4.1 Personalizar Barra de Navegação

Para acessar facilmente alguns módulos importantes ou usados com frequência, você pode personalizar a barra de navegação.

Passos

1. No canto superior esquerdo, selecione → **Todos os módulos** para exibir a barra de navegação e o painel Todos os módulos.

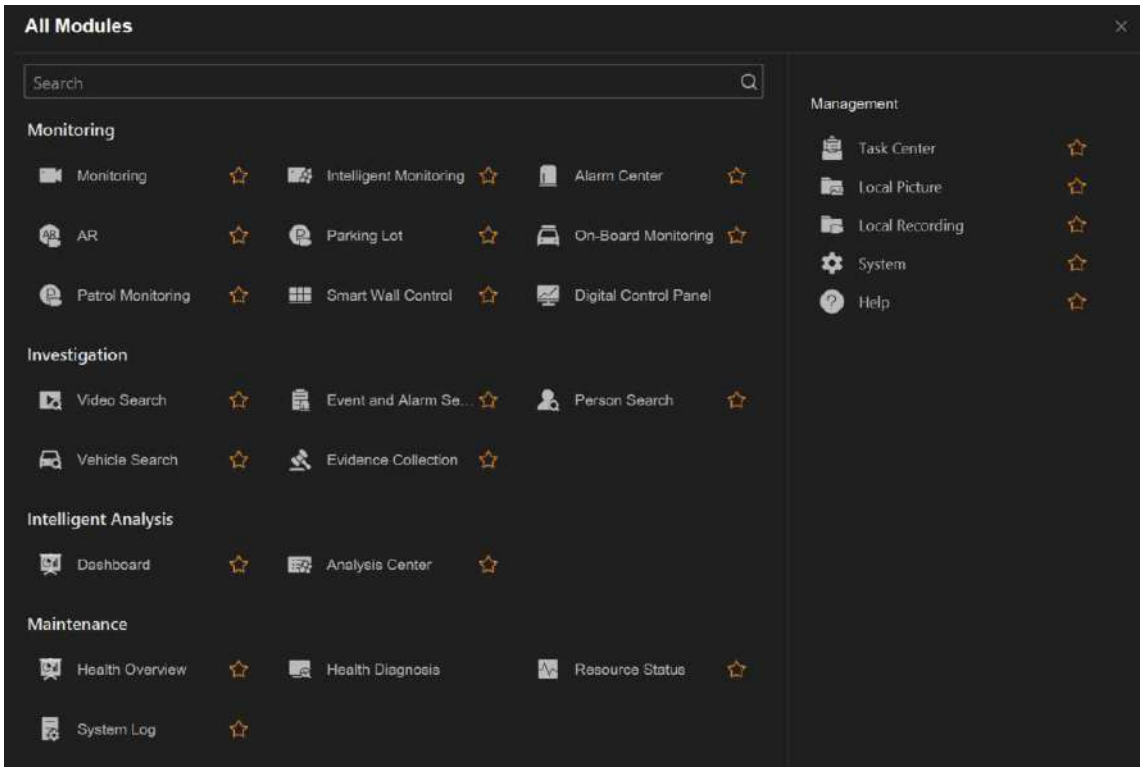


Figura 4-2 Barra de navegação e painel Todos os módulos

Observação

No painel Todos os módulos, o ícone ao lado do nome do módulo indica que este módulo foi adicionado à barra de navegação superior.

2. Opcional: clique para remover o módulo da barra de navegação.

4.2 Personalizar o Painel de Controle

Você pode selecionar módulos para exibir no painel de controle e personalizar a disposição dos módulos.

Passos

1. Na página inicial, clique em **Painel de controle digital** .
2. No canto superior esquerdo do painel de controle, clique em **Meu Painel de Controle** para desdobrar a lista suspensa.

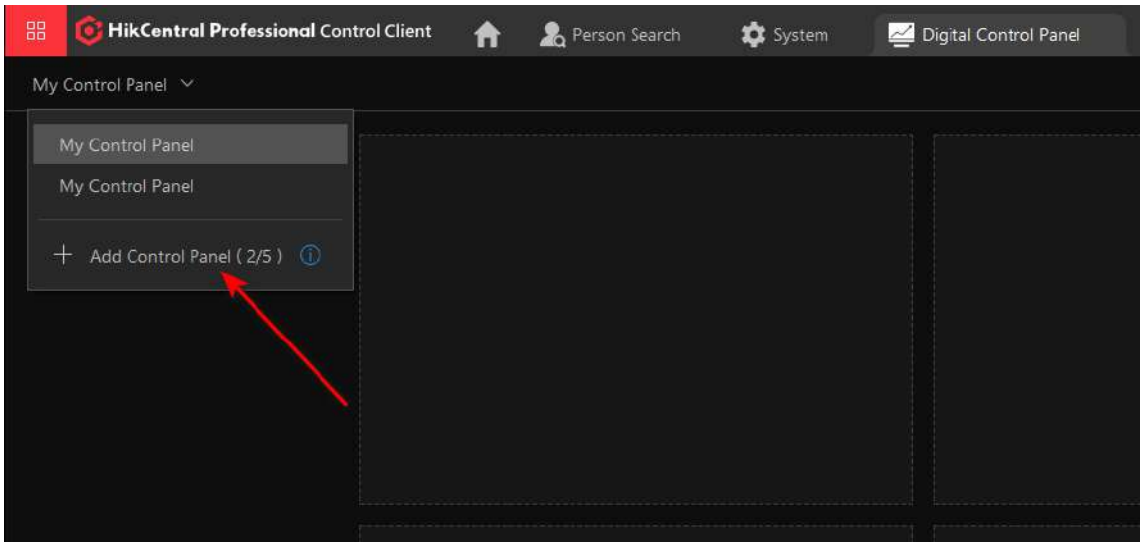


Figura 4-3 Adicionar Painel de Controle

3. Clique em **Adicionar Painel de Controle** na lista suspensa para começar a personalizar um painel de controle.
4. No canto superior esquerdo da página de adição do painel de controle, digite um nome para o painel de controle.
5. No painel direito, selecione uma janela.
6. No painel esquerdo, clique em um nome de módulo para mostrar o painel de configuração do módulo à esquerda.
7. Selecione e arraste/clique duas vezes em uma câmera/mapa/página da web ou defina os parâmetros do módulo e clique em **Salvar** .

Observação

- Ao adicionar o módulo Câmera ou Mapa, você pode editar os módulos adicionados. Mas ao adicionar outros módulos (exceto os módulos Câmera e Mapa), você não pode editar os módulos adicionados.
- Ao adicionar o módulo Health Monitoring, não é necessário definir parâmetros do módulo. Após clicar no nome do módulo, o módulo será adicionado diretamente e exibido na janela selecionada.
- Ao adicionar o módulo Página da Web, você pode inserir a URL ou o endereço IP da página da Web no campo de entrada no canto superior direito da janela e pressionar Enter no teclado para acessar a página da Web.

O módulo é adicionado à janela selecionada e exibido de forma visualizada.

8. Opcional: Execute a(s) seguinte(s) operação(ões).

Editar Parâmetros do Módulo	Clique no canto superior direito da janela para editar os parâmetros do módulo.
Remover módulo	Clique no canto superior direito da janela para remover o módulo da janela.

Personalizar arranjo de módulos	Arraste o módulo para a janela desejada para personalizar a disposição do módulo no painel de controle.

9. Opcional: No canto superior direito da página de adição do painel de controle, clique em **Cancelar** para cancelar a personalização do painel de controle.
10. Opcional: No canto superior direito da página de adição do painel de controle, clique em **Restaurar padrão** para restaurar o painel de controle padrão.
11. No canto superior direito da página de adição do painel de controle, clique em **Salvar** para salvar o painel de controle personalizado.
12. Opcional: Execute a(s) seguinte(s) operação(ões).

Editar Painel de Controle	No canto superior direito do Control Client, clique em **Editar Painel de Controle** para editar o painel de controle.
Mudar para tela cheia	No canto superior direito do Control Client, clique em **Tela Cheia** para exibir o painel de controle no modo de tela cheia.
Abrir tela auxiliar	No canto superior direito do Control Client, clique para exibir o painel de controle na tela auxiliar.

Capítulo 5 Visualização ao Vivo

Você pode visualizar o vídeo ao vivo das câmeras conectadas usando o Live View. Durante o live view, você pode controlar câmeras PTZ, gravar videoclipes, capturar imagens, visualizar a reprodução instantânea, adicionar câmeras aos Favoritos, etc. Para a câmera ANPR, você pode visualizar o número da placa de licença reconhecida. Para o dispositivo de reconhecimento facial, você pode visualizar as informações de comparação de imagens faciais dos rostos detectados. Para os pontos de acesso relacionados às câmeras, você pode controlar o status do ponto de acesso em tempo real e verificar os registros de passagem do cartão. Além disso, você pode entrar no modo smart wall (placa gráfica) e exibir os recursos no smart wall.

Painel de Navegação

	Monitoramento	Exiba recursos disponíveis para visualização ao vivo que são agrupados em áreas em cada site.
	Contagem de pessoas em tempo real	Veja o status de contagem de pessoas em tempo real de cada grupo de contagem de pessoas.
	Comparação de imagens de rosto	Visualize as informações de comparação de imagens de rosto entre os rostos detectados e as imagens de rosto em uma biblioteca de imagens de rosto.
	Parede inteligente	Entre no modo Smart Wall (placa gráfica). Defina a divisão da janela e ajuste a janela de exibição na parede inteligente.
	Adicionar janela de página da Web	Adicione página(s) da web à janela Live View ou Playback.

5.1 Visualização ao Vivo

No módulo Live View do Web Client, você pode visualizar o vídeo ao vivo das câmeras adicionadas e realizar algumas operações básicas, incluindo captura de imagens, gravação e controle de PTZ. No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Monitoramento** → **Monitoramento** .

5.1.1 Escolha 1: Iniciar Live View no Modo de Área

Observação

As áreas que o usuário atual tem permissão para acessar são listadas e os recursos que o usuário tem permissão para acessar são mostrados nas áreas correspondentes.

1. Clique no canto superior direito para alterar a divisão da janela de visualização ao vivo.
2. Iniciar visualização ao vivo.
   - Arraste uma câmera para a janela de exibição para iniciar a visualização ao vivo da câmera ou clique duas vezes na câmera para iniciar a visualização ao vivo em uma janela de exibição livre.
   - Arraste uma área para uma janela de exibição e clique em **Reprodução em lote** ou clique duas vezes na área para iniciar a visualização ao vivo de todas as câmeras na área.

5.1.2 Escolha 2: Iniciar Live View no Modo de Visualização

Uma visualização é uma divisão de janela com canais de recursos (por exemplo, câmeras e pontos de acesso) vinculados a cada janela. O modo de visualização permite que você salve a divisão de janela e a correspondência entre câmeras e janelas (ou correspondência entre mapa e janela) como padrão para que você possa acessar rapidamente esses canais e/ou mapa mais tarde. Por exemplo, você pode vincular a câmera 1, a câmera 2 e a câmera 3 localizadas em seu escritório a determinadas janelas de exibição e salvá-las como uma visualização chamada ***office*** . Então, você pode acessar a visualização ***office*** e essas câmeras serão exibidas na janela vinculada rapidamente.

Observação

- Para visualização ao vivo, o modo de visualização pode salvar o tipo de recurso, ID do recurso, tipo de fluxo, posição e escala após zoom digital, número predefinido e status de correção de distorção olho de peixe.
- Para reprodução, o modo de visualização pode salvar o tipo de recurso, a ID do recurso, a posição e a escala após o zoom digital e o status de correção de distorção olho de peixe.

1. Clique na aba no painel esquerdo.
2. Adicione um grupo de exibição personalizado.
   a. Selecione **Exibição Pública** ou **Exibição Privada** para adicionar o grupo de exibição.

      Observação

      Os grupos de exibição e as exibições que pertencem ao grupo de exibição privado ficam ocultos dos outros usuários.

   b. Clique em , defina um nome para o grupo de exibição e clique em **OK** .
3. Adicione uma visualização.
   a. Selecione um grupo de exibição, clique em e defina um nome para a exibição.
   b. Clique em **Adicionar** para selecionar câmeras.
   c. Defina os parâmetros necessários e clique em **Adicionar** para adicionar uma visualização.
4. (Opcional) Selecione uma visualização e clique em → **Compartilhar** no lado direito do nome da visualização para compartilhá-la com outras pessoas.
5. Clique duas vezes em uma visualização ou mova o cursor sobre uma visualização e clique em → **Reproduzir** ao lado do nome da visualização.

5.1.3 Escolha 3: Iniciar Visualização ao Vivo de Câmeras Favoritas

1. Clique na aba no painel esquerdo.
2. Selecione um Favorito pai, clique para adicionar um Favorito sob o Favorito pai e selecione a(s) câmera(s) a serem adicionadas aos Favoritos.

Observação

É possível adicionar até 5 níveis de Favoritos.

3. (Opcional) Selecione um Favorito e clique em → **Compartilhar** no lado direito do nome dos Favoritos para compartilhá-lo com outras pessoas.
4. Na janela Visualização ao vivo, selecione Favoritos e clique em → **Reproduzir tudo** para começar a visualizar a visualização ao vivo de todas as câmeras adicionadas aos Favoritos.

5.1.4 Escolha 4: Troca Automática de Câmeras em Uma Área

1. Inicie a troca automática na área.
   - Arraste uma área para a janela de visualização ao vivo e selecione **Troca automática de tela única** para iniciar a troca automática das câmeras da área na janela de exibição selecionada.
   - Clique no lado direito do nome da área e clique em **Troca automática de área** para alternar as câmeras da área na janela de visualização ao vivo.
2. Mova o cursor sobre a janela de visualização ao vivo e execute outras operações após o início da troca automática.

Operações	Descrições
Ajustar intervalo de comutação	Clique em ou no canto inferior esquerdo da janela de visualização ao vivo para ajustar o intervalo da troca automática.
Ver câmera anterior ou seguinte	Clique em ou no canto inferior esquerdo da janela de visualização ao vivo para ir para a câmera anterior ou seguinte.
Pausa	Clique no canto inferior esquerdo da janela de visualização ao vivo para pausar a troca automática.

5.2 Adicionar Página da Web à Janela de Exibição

Durante a visualização ao vivo e a reprodução de vídeo ou ao personalizar o Painel de Controle, você pode adicionar páginas da web a uma janela de exibição para visualizar notícias on-line, fazer login no HikCentral Professional Web Client, etc.

Passos

1. No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Monitoramento** → **Monitoramento** .

Observação

Para adicionar uma página da web ao personalizar o Painel de Controle, consulte ***Personalizar o Painel de Controle*** .

2. Clique em **Adicionar janela de página da Web** na barra de navegação esquerda.
3. Na janela Página da Web, digite o site na barra de endereços.
4. Pressione a tecla Enter para entrar na página da web correspondente.
5. Navegue pelo conteúdo da página web.
6. Opcional: Execute as seguintes operações.

Adicionar mais página da Web	Clique em **Adicionar janela de página da Web** na barra de navegação para adicionar mais páginas da Web. **Observação** É possível adicionar até 64 páginas da web.
Atualizar página da Web	Clique para atualizar a página da web, se necessário.
Adicionar página da Web aos favoritos	Clique em → **Adicionar aos Favoritos** , digite o nome para Favoritos e clique em **Adicionar** para adicionar a página da web atual aos Favoritos. **Observação** Você pode marcar **Definir como página da Web padrão** para definir a página da Web atual como a página da Web padrão e, quando você adicionar uma nova página da Web na próxima vez, a página da Web padrão será exibida.
Ajustar tamanho da página da Web	Clique em uma página da web, mova o cursor para o limite da página da web, arraste o cursor quando ele se transformar em seta dupla para ajustar o tamanho da página da web.
Fechar página da Web	Clique para fechar a página atual.

5.3 Controle PTZ

O controle PTZ para câmeras com funcionalidade pan/tilt/zoom é fornecido. Você pode definir a predefinição, patrulha e padrão para as câmeras no painel de controle PTZ.
No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Monitoramento** → **Monitoramento** .
Inicie a visualização ao vivo de uma câmera e clique em **Controle PTZ** para abrir o painel PTZ.

Observação

A função de controle PTZ deve ser suportada pela câmera.

5.3.1 Apresentar o Painel Principal

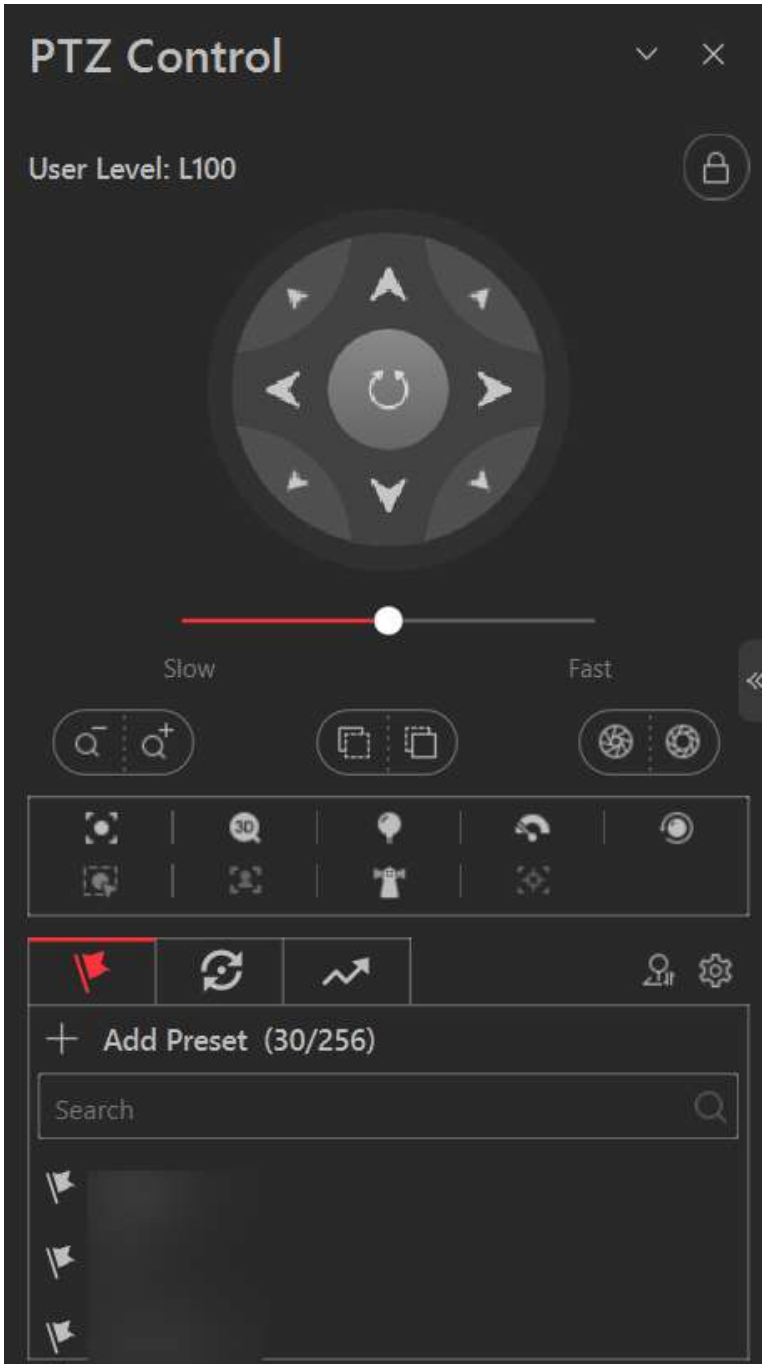


Figura 5-1 Painel de controle PTZ

Os seguintes botões estão disponíveis no painel de controle PTZ:

	Bloqueie o PTZ por um período de tempo designado. Quando o PTZ estiver bloqueado, usuários com níveis de permissão de controle PTZ mais baixos não poderão alterar os controles PTZ. **Observação** Para obter detalhes sobre como definir o nível de permissão de controle PTZ, consulte o *Manual do Usuário do HikCentral Professional Web Client* .
	Botão de direção, varredura automática e velocidade PTZ.
	Amplie ou reduza o vídeo para câmeras que não têm seus próprios recursos de zoom óptico. Clique novamente para desabilitar a função.
	Usado para ajustar a luminância da imagem. Quanto maior a íris, mais luz entra e mais brilhante a imagem será.
	Clique para mover o ponto focal para trás e clique para mover o ponto focal para frente.
	Foco auxiliar: clique para focar automaticamente.
	Posicionamento 3D: Clique na posição desejada na imagem de vídeo e arraste uma área retangular na direção inferior direita. Em seguida, o sistema de domo moverá a posição para o centro e permitirá que a área retangular seja ampliada. Clique para arrastar uma área retangular na direção superior esquerda para mover a posição para o centro e permitir que a área retangular seja ampliada.
	Luz: Clique para preencher a luz.
	Limpador: use o limpador para limpar a poeira da lente da câmera.
	Inicialização da lente: inicialize a lente e foque novamente para obter uma imagem nítida.
	Rastreamento manual: para domos de velocidade com função de rastreamento automático, ative o rastreamento automático (por meio do menu do botão direito) e clique no ícone para rastrear manualmente o alvo clicando no vídeo.
	Captura Manual de Rosto: Clique neste botão e segure o botão esquerdo do mouse para selecionar um rosto na imagem para capturá-lo. A imagem será carregada no servidor para visualização.
	Ação de estacionamento: Para o domo de velocidade com função de estacionamento de um toque, clique no ícone e o domo de velocidade salva a visualização atual na predefinição nº 32. O dispositivo começa a estacionar na predefinição nº 32 automaticamente após um período de inatividade (tempo de estacionamento). Para definir o tempo de estacionamento, consulte o manual do usuário do domo de velocidade.
	Rastreamento automático: para suporte e rastreamento de câmeras, clique no ícone e selecione o alvo (pessoa ou veículo) na visualização ao vivo para armar e rastrear esse alvo.

- Na janela de exibição de vídeo ao vivo, clique no ícone para iniciar o controle PTZ. Clique e arraste o cursor com uma seta branca para controlar a direção.
- Clique para obter a configuração PTZ do dispositivo.

5.3.2 Configurar Predefinição

Uma predefinição é uma posição de imagem predefinida que contém parâmetros de configuração para panorâmica, inclinação, zoom, foco e outros parâmetros. Você também pode definir uma predefinição virtual após habilitar o zoom digital.

1. Clique para entrar no painel de configuração predefinida de PTZ.
2. Use os botões de direção para controlar o movimento do PTZ.
3. Selecione um número predefinido de PTZ na lista de predefinições e clique para nomear e salvar as configurações.

5.3.3 Configurar Patrulha

Uma patrulha é uma trilha de varredura especificada por um grupo de predefinições definidas pelo usuário (incluindo predefinições virtuais), com a velocidade de varredura entre duas predefinições e o tempo de permanência da predefinição programáveis separadamente.
Antes de começar, certifique-se de ***ter adicionado duas ou mais predefinições*** .

1. Clique para entrar no painel de configuração de patrulha.
2. Selecione um número de patrulha PTZ e clique para definir a patrulha.
   a. Selecione ou como o tipo predefinido.

   Observação

   Uma predefinição de dispositivo ( ) é uma posição de imagem predefinida, enquanto uma predefinição virtual ( ) é uma posição de imagem predefinida e ampliada. Você pode adicionar uma predefinição virtual iniciando a visualização ao vivo, ampliando e adicionando a posição da imagem como uma predefinição virtual.

   b. Clique para adicionar uma predefinição configurada, passe o cursor sobre os valores nas colunas **Predefinição** , **Velocidade** e **Tempo** e deslize o mouse para alterar o valor.
   c. Clique em ou para ajustar a sequência de predefinições.
3. Defina outros parâmetros e clique em **OK** .

5.3.4 Configurar Padrão

Ao gravar o padrão, o caminho do movimento e o tempo de permanência em uma determinada posição podem ser gravados precisamente. Ao chamar o padrão, o PTZ móvel começa a se mover totalmente de acordo com o caminho gravado.

1. Clique para entrar no painel de configuração do padrão PTZ.
2. Clique para começar a gravar o caminho de movimento do padrão, use os botões de direção e outros botões para controlar o movimento PTZ e clique para parar e salvar a gravação do padrão.

3. Clique para chamar o padrão.

5.4 Aplicativos da Barra de Ferramentas Live View

Você pode personalizar os ícones na barra de ferramentas, iniciar o modo de correção de distorção olho de peixe, executar o rastreamento panorâmico manual e assim por diante.

5.4.1 Visualização ao Vivo da Câmera Olho de Peixe com Distorção

Você pode definir a calibração central e visualizar a visualização ao vivo de uma câmera olho de peixe no cliente. A deformação refere-se ao processo de correção de perspectiva de uma imagem, para reverter os efeitos da distorção geométrica causada pela lente da câmera olho de peixe. Ela permite que o usuário cubra uma área ampla com um único dispositivo e tenha uma visualização "normal" de uma imagem distorcida ou invertida. Além disso, durante a visualização ao vivo, você pode executar mais operações, como ajustar o ângulo de visão e aumentar/diminuir o zoom da visualização.

Passos

1. ***Inicie a visualização ao vivo*** de uma câmera olho de peixe.
2. Opcional: Defina a calibração central da câmera olho de peixe para calibrar o centro da imagem olho de peixe.
   1) Na barra de ferramentas da janela de exibição, clique em → para abrir a janela de calibração central.

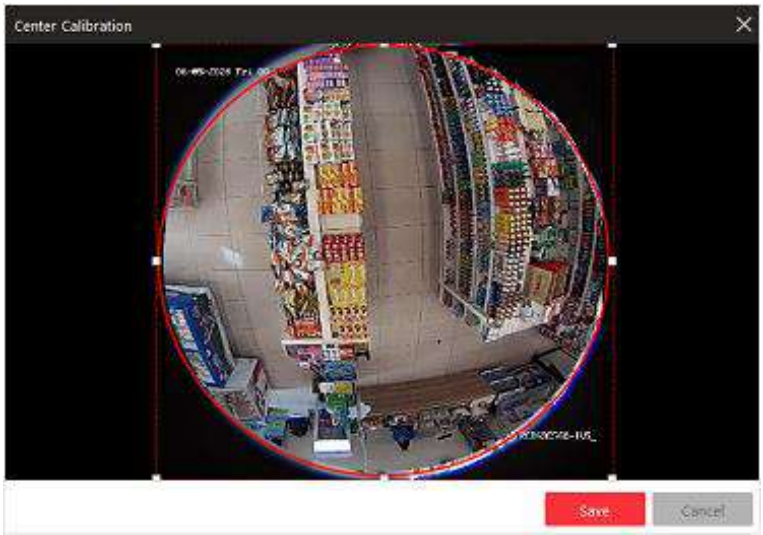


Figura 5-2 Janela de calibração central

   2) Mova ou ajuste o tamanho do retângulo na linha tracejada vermelha no vídeo para calibrar o centro da visão da câmera conforme desejado.

Observação

A calibração central deve ser operada dentro do escopo adequado, caso contrário, falhará.

3) Clique em **Salvar** .

3. Na barra de ferramentas da janela de exibição, clique para entrar no modo de distorção olho de peixe e visualizar a visualização ao vivo.

Figura 5-3 Dewarping olho de peixe

4. Opcional: execute as seguintes operações conforme desejado.

Ajustar ângulo de visão	Coloque o cursor no vídeo ao vivo e arraste o vídeo para ajustar o ângulo de visão.
Ampliar/reduzir a visualização	Coloque o cursor no vídeo ao vivo e role a roda do mouse para aumentar ou diminuir o zoom na visualização.
Executar controle PTZ	Use o painel PTZ no lado esquerdo para executar o controle PTZ da câmera.

Observação

A configuração de padrão não é suportada por câmeras olho de peixe.

5.4.2 Ver Vídeo ao Vivo da Câmera ANPR

O reconhecimento automático de placas (ANPR) é uma tecnologia que usa reconhecimento óptico de caracteres em imagens para ler placas de veículos. Durante a visualização ao vivo das câmeras

ANPR, os números das placas dos veículos que passam são reconhecidos e exibidos no lado direito da janela de visualização ao vivo. O ANPR está se tornando um componente significativo para o reconhecimento de veículos roubados. Placas reconhecidas com sucesso podem ser comparadas com bancos de dados (listas de permissão ou bloqueio, incluindo "pessoa procurada", pessoa desaparecida, suspeito de terrorismo, etc.). Você pode marcar o veículo suspeito, adicionar um novo veículo à lista de veículos e pesquisar as informações do veículo que passa.

Antes de Começar

Adicione uma câmera ANPR ao sistema por meio do Web Client. Para adicionar uma câmera, consulte o *Manual do Usuário do HikCentral Professional Web Client* .

Execute esta tarefa quando precisar visualizar o vídeo ao vivo da câmera ANPR.

Passos

1. No canto superior esquerdo da página inicial, selecione → **Todos os módulos** → **Monitoramento** → **Monitoramento** .
2. Inicie a visualização ao vivo de uma câmera ANPR.
   – Arraste uma câmera ANPR da lista de recursos à esquerda para a janela de exibição para iniciar a visualização ao vivo.
   – Clique duas vezes no nome de uma câmera ANPR na lista de dispositivos à esquerda para iniciar a visualização ao vivo.

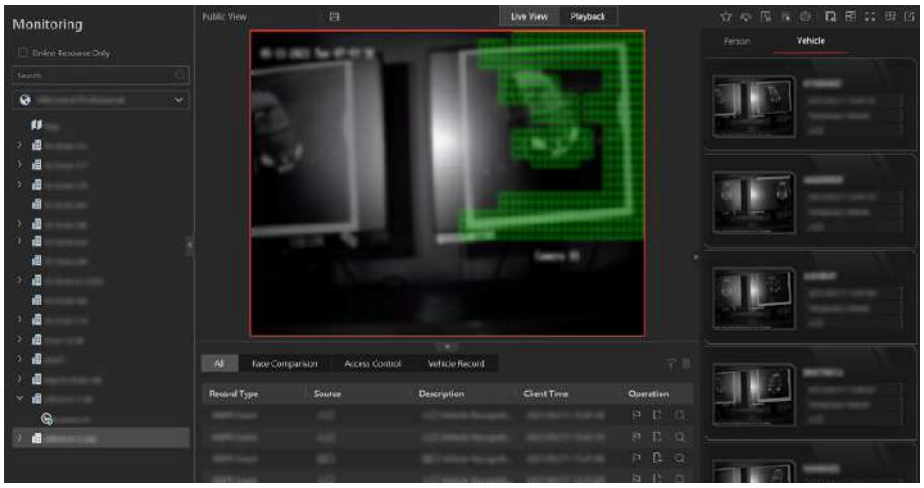


Figura 5-4 Visualização ao vivo da câmera ANPR

3. Opcional: execute a(s) seguinte(s) operação(ões), se necessário.
   – Opção 1: Clique na parte inferior da página e depois clique em **Registro do veículo** para entrar no painel de operação.
   – Opção 2: Clique no lado direito da página e depois em **Veículo** para entrar no painel de operação.

Marcar veículo	Se você acha que um veículo é suspeito, você pode marcá-lo. Os veículos marcados podem ser filtrados mais tarde ao pesquisar as informações de passagem de veículos relacionados no módulo Vehicle Search.

- Para a opção 1: clique na coluna Operação para marcar o veículo.
- Para a escolha 2: mova o cursor para a área do veículo alvo e clique para marcar o veículo

Adicionar veículo à lista de veículos

Se o Cliente reconhecer um veículo que não foi adicionado à lista de veículos, você pode adicioná-lo à lista de veículos manualmente. Veja ***Adicionar Veículo Reconhecido à Lista de Veículos*** para detalhes.

- Para a opção 1: clique para adicionar o veículo a uma lista de veículos.
- Para a opção 2: mova o cursor para a área do veículo alvo e clique para adicionar o veículo a uma lista de veículos.

Pesquisar veículo

Se você quiser saber quantas vezes o veículo entrou e saiu do estacionamento, você pode pesquisar o(s) registro(s) de passagem do veículo. Para detalhes, consulte ***Search for Passing Vehicles Detected by Cameras and UVSSs (Pesquisar por Veículos que Passam Detectados por Câmeras e UVSSs)*** .

- Para a opção 1: clique para entrar na página de pesquisa de registro de aprovação de veículo para pesquisar o(s) registro(s) de aprovação do veículo.
- Para a opção 2: mova o cursor para a área do veículo de destino e clique para entrar na página de pesquisa de registro de passagem de veículo para pesquisar o(s) registro(s) de passagem do veículo.

Excluir todos os registros

Se você entrar no painel de operação pela opção 1, poderá clicar para excluir todos os registros do veículo.

Inscreva-se em todos os eventos de veículos

Se você entrar no painel de operação pela Opção 1, poderá marcar **Inscrever-** se em todos os eventos do veículo.

5.4.3 Ver Vídeo ao Vivo da UVSS

Um sistema de vigilância sob veículos (UVSS) geralmente consiste em sistemas de imagens montados em uma estrada e usados em pontos de acesso às instalações, particularmente em instalações seguras. Ele é usado para detectar ameaças — como bombas — que estão escondidas sob os veículos. Câmeras capturam imagens do chassi do veículo para inspeção visual manual ou automatizada por pessoal ou sistemas de segurança. Conforme o veículo chega ao ponto de verificação e passa sobre a unidade de imagens, as câmeras capturam imagens do chassi e as transmitem ao Control Client. A imagem do chassi do veículo que passa é capturada e exibida na janela de visualização ao vivo. O número da placa do veículo que passa é reconhecido e exibido no

lado direito da janela de visualização ao vivo.

Antes de Começar

Adicione um UVSS ao sistema via Web Client. Consulte o *Manual do Usuário do HikCentral Professional Web Client* para obter detalhes.

Execute esta tarefa quando precisar visualizar o vídeo ao vivo do UVSS.

Passos

1. No canto superior esquerdo da página inicial, selecione → **Todos os módulos** → **Monitoramento** → **Monitoramento** .
2. Inicie a visualização ao vivo do UVSS.
   – Arraste o UVSS da lista de dispositivos à esquerda para a janela de exibição para iniciar a visualização ao vivo.
   – Clique duas vezes no nome do UVSS na lista de dispositivos à esquerda para iniciar a visualização ao vivo.

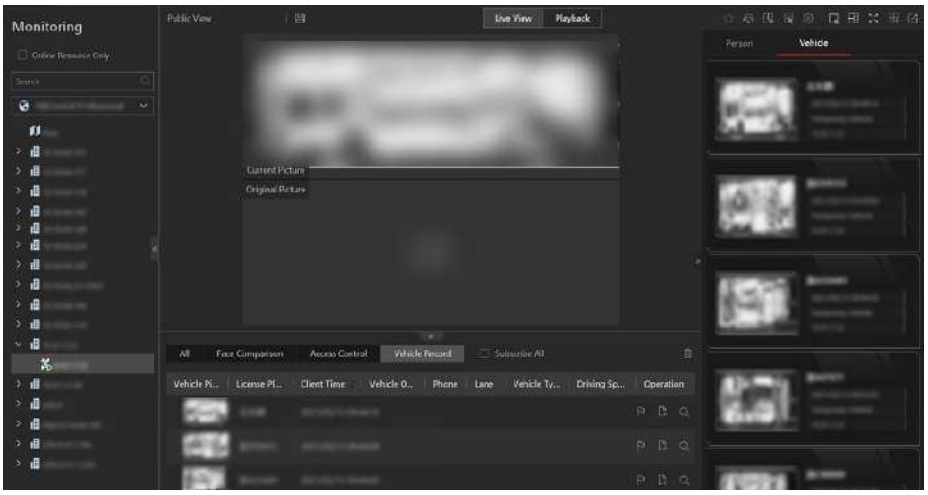


Figura 5-5 Visualização ao vivo do UVSS

Você pode ver o vídeo ao vivo da câmera vinculada ao UVSS, a imagem do chassi e o número da placa reconhecida dos veículos que passam.

3. Opcional: marque informações importantes na imagem do chassi.
   1) Mova o cursor para a imagem do trem de pouso.
   2) Clique na barra de ferramentas.
   3) Desenhe na imagem do trem de pouso para marcar informações importantes, como o explosivo.
4. Opcional: execute a(s) seguinte(s) operação(ões), se necessário.
   – Opção 1: Clique na parte inferior da página e depois clique em **Registro do veículo** para entrar no painel de operação.
   – Opção 2: Clique no lado direito da página e depois em **Veículo** para entrar no painel de operação.

Marcar veículo	Se você acha que um veículo é suspeito, você pode marcá-lo. Os veículos marcados podem ser filtrados mais tarde ao pesquisar as

	informações de passagem de veículos relacionados no módulo Vehicle Search. ● Para a opção 1: clique na coluna Operação para marcar o veículo. ● Para a escolha 2: mova o cursor para a área do veículo alvo e clique para marcar o veículo
Adicionar veículo à lista de veículos	Se o Cliente reconhecer um veículo que não está adicionado à lista de veículos, ele poderá adicioná-lo manualmente. ● Para a opção 1: clique para adicionar o veículo a uma lista de veículos. ● Para a opção 2: mova o cursor para a área do veículo alvo e clique para adicionar o veículo a uma lista de veículos.
Pesquisar veículo	Se você quiser saber quantas vezes o veículo entrou e saiu do estacionamento, você pode procurar o(s) registro(s) de passagem do veículo. ● Para a opção 1: clique para entrar na página de pesquisa de registro de aprovação de veículo para pesquisar o(s) registro(s) de aprovação do veículo. ● Para a opção 2: mova o cursor para a área do veículo de destino e clique para entrar na página de pesquisa de registro de passagem de veículo para pesquisar o(s) registro(s) de passagem do veículo.
Excluir todos os registros	Se você entrar no painel de operação pela opção 1, poderá clicar para excluir todos os registros do veículo.
Inscreva-se em todos os eventos de veículos	Se você entrar no painel de operação pela Opção 1, poderá marcar **Inscrever-** se em todos os eventos do veículo.

5.4.4 Executar Rastreamento de Panorama Manual

Durante a visualização ao vivo, você pode habilitar o rastreamento de panorama manualmente para localizar ou rastrear o alvo que apareceu na visualização da câmera bullet ou box com um speed dome vinculado. Você também pode verificar e testar os resultados da calibração sobre as configurações de rastreamento de panorama para rastreamento automático.

Antes de começar

Certifique-se de ter configurado as regras de rastreamento de panorama para a câmera box ou bullet no Web Client. Para mais detalhes, consulte o *Manual do Usuário do HikCentral Professional Web Client* .

Passos

1. No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Monitoramento** → **Monitoramento** .
2. Inicie a visualização ao vivo da câmera tipo caixa/bala e do domo de velocidade vinculado.
3. Clique na barra de ferramentas da câmera tipo caixa/bala para habilitar o rastreamento panorâmico manual.

Observação

Se você optar por habilitar o rastreamento de panorama manual, o rastreamento de panorama automático não entrará em vigor; se você optar por não habilitar o rastreamento de panorama manual e habilitar o **Rastreamento Automático** ao configurar o rastreamento de panorama no Web Client, quando o evento VCA configurado for acionado pelo alvo, o speed dome vinculado executará o rastreamento de panorama automático.

4. Clique ou desenhe um retângulo na imagem de visualização ao vivo da câmera tipo caixa/bala, e o speed dome mudará para a visualização em close-up.

Figura 5-6 Rastreamento de panorama manual

5.4.5 Criar Área de Zoom para Visualizar a Visualização ao Vivo Detalhada

Você pode reproduzir a visualização ao vivo em quadro inteiro de uma câmera e partes ampliadas lado a lado ao mesmo tempo, criando áreas de zoom.

Antes de Começar

Certifique-se de ter adicionado câmera(s) por meio do Web Client.

Passos

1. No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Monitoramento** → **Monitoramento** .
2. Inicie a visualização ao vivo de uma câmera. Veja instruções detalhadas em ***Visualização ao vivo*** .
3. Crie uma área de zoom na visualização ao vivo em tela cheia da câmera para visualizar detalhes dessa área em uma nova janela de exibição.

– Para uma câmera normal, clique e desenhe um retângulo no vídeo.

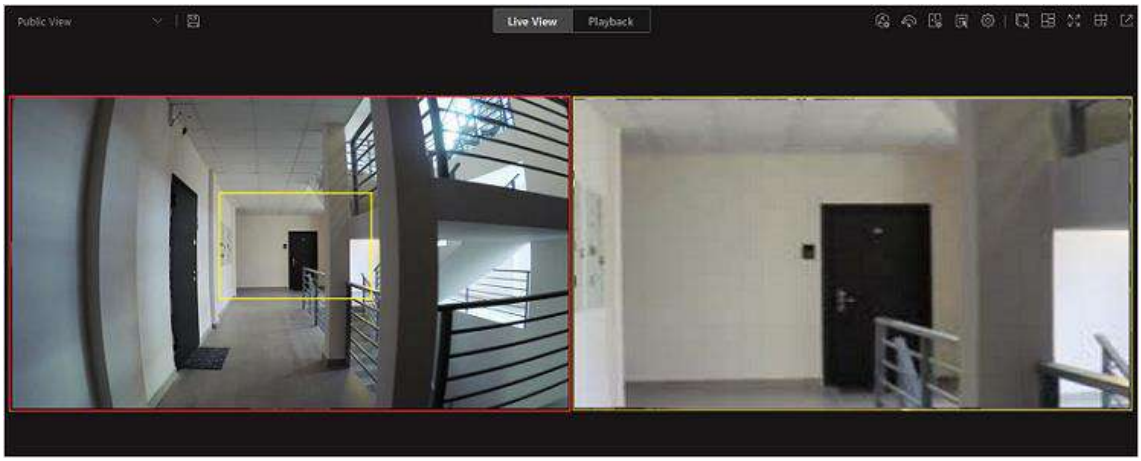


Figura 5-7 Janela da área de zoom (câmera normal)

Observação

É possível adicionar até 5 áreas de zoom.

– Para uma câmera olho de peixe, clique e desenhe um retângulo no vídeo.

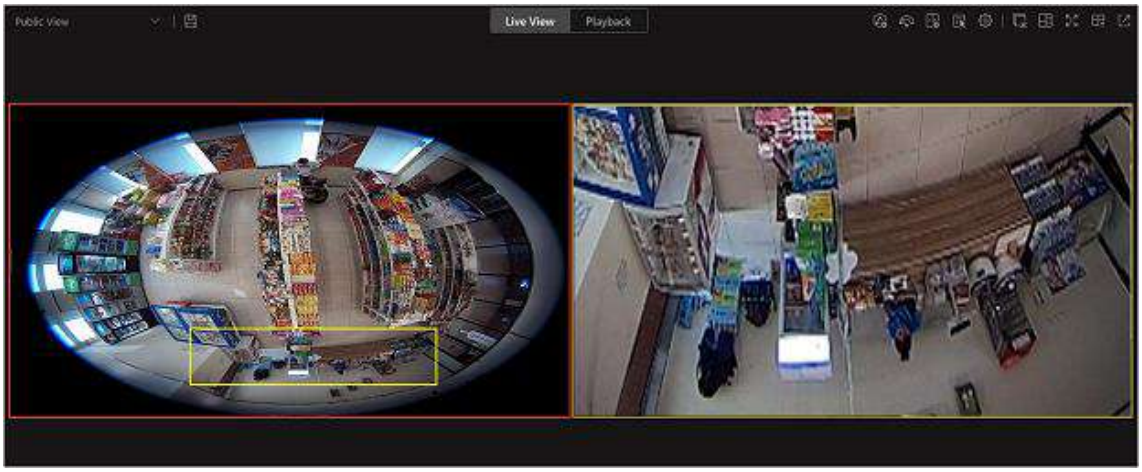


Figura 5-8 Janela de área de zoom com distorção (câmera olho de peixe)

Observação

- É possível adicionar até 8 áreas de zoom.
- Para câmeras olho de peixe, você pode visualizar a imagem com zoom desfocado na nova janela de visualização ao vivo.

A visualização ao vivo das áreas de zoom que você criar será reproduzida na(s) nova(s) janela(s) de visualização ao vivo.

4. Opcional: execute outras operações após criar uma área de zoom.

Excluir área de zoom Mova o cursor para uma área de zoom na janela principal de

	visualização ao vivo e clique para excluir a área.
Editar área de zoom	Arraste a borda de uma área de zoom para ajustar o tamanho da área.
Parar visualização ao vivo	Na janela de visualização ao vivo de uma área de zoom, clique no canto superior direito para fechar a janela de visualização ao vivo.
	Observação Se você quiser mostrar a janela de visualização ao vivo da área de zoom novamente, você precisa clicar em / na barra de ferramentas da janela principal de visualização ao vivo e a área para uma janela de visualização ao vivo.
Ajustar sequência de janelas	Arraste as janelas de visualização ao vivo para ajustar suas sequências.

5.4.6 Exibir Eevento Detectado na Visualização ao Vivo

Os eventos detectados, incluindo eventos ANPR, eventos de comparação de imagem facial, eventos de acesso e registros de veículos que passam podem ser exibidos em tempo real durante a visualização ao vivo. Você pode visualizar os detalhes do evento, filtrar os eventos e limpar os eventos.

Antes de Começar

Certifique-se de ter adicionado dispositivos e eventos.

Passos

1. No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Monitoramento** → **Monitoramento** .
2. Inicie a visualização ao vivo.
3. Clique na parte inferior do cliente para mostrar a lista de eventos.
4. Selecione a aba **Tudo** / **Comparação de imagens faciais** / **Controle de acesso** / **Registro do veículo** para visualizar as informações do evento correspondente.

Comparação de imagens de rosto

Um evento de comparação de imagens faciais refere-se a qualquer evento que envolva uma câmera com capacidade de reconhecimento facial.

Controle de acesso

Um evento de controle de acesso se refere a quaisquer eventos com um ponto de acesso envolvido. Clique em **Controle de acesso** para passar pelos eventos de controle de acesso e, no painel direito, você pode visualizar os detalhes da pessoa.

Registro de Veículo

Um registro de veículo se refere a qualquer informação de veículo que passa capturada por uma câmera ANPR.

5. Opcional: Execute outras operações.

Ver detalhes do evento	Clique para ver os detalhes do evento.
Adicionar à lista	● Se o cliente reconhecer uma pessoa que não esteja na lista de pessoas, você pode adicionar a pessoa à biblioteca de imagens de rosto clicando em . Veja os detalhes em ***Exibir rosto detectado e correspondente na visualização ao vivo*** . ● Se o cliente reconhecer uma placa de veículo que não esteja na lista de veículos, você pode adicioná-la à lista de veículos clicando em . Veja os detalhes em ***Adicionar Veículo Reconhecido à Lista de Veículos*** .
Perdoar violação anti-passback	Quando uma pessoa tenta usar um cartão fora da sequência da regra anti-passback, o acesso será negado. Isso é chamado de "Violação Anti-Passback". Quando ocorre violação anti-passback, nenhuma entrada é permitida a menos que o evento de violação anti-passback seja perdoado. Na lista de eventos de Controle de Acesso, você pode perdoar um evento anti-passback clicando na coluna Operação.
Pesquisar Registros de Acesso	Para eventos de acesso de visitantes, clique para ir para a página Recuperação de Registros de Acesso para pesquisar registros de acesso do visitante personalizando as condições de pesquisa.
Pesquisar Eventos	Para eventos de porta, clique para ir para a página de Pesquisa de Eventos e Alarmes para pesquisar eventos personalizando as condições de pesquisa.
Inscreva-se em todos os eventos de comparação de imagens de rosto	Na lista de eventos Comparação de imagens faciais, marque **Inscrever-se em tudo** para que o Cliente de controle atual possa receber eventos de todas as bibliotecas de imagens faciais e exibir os eventos na lista de eventos.
Assinar todos os registros de veículos	Na lista de Registros de Veículos, marque **Inscrever-se em Todos** para que o Cliente de Controle atual possa receber todos os registros de veículos que passam pelas câmeras ANPR e exibir os registros na lista.
Evento de filtro	Clique para selecionar o recurso para filtrar o evento relacionado.
Evento claro	Clique para limpar todos os eventos detectados.

5.4.7 Gravação e Captura Manual

Você pode gravar arquivos de vídeo e capturar imagens manualmente durante a visualização ao vivo.

Gravação Manual

Grave o vídeo ao vivo durante a visualização ao vivo, se necessário, e armazene os arquivos de vídeo no PC local.

Capturar

Capture imagens durante a visualização ao vivo, se necessário, e armazene-as no PC local.

Gravação Manual

1. No canto superior esquerdo do Control Client, selecione → **Todos os módulos** →

Monitoramento → **Monitoramento** .

2. Mova o cursor para a janela de exibição ao vivo para mostrar a barra de ferramentas.
3. Clique na barra de ferramentas da janela de exibição para iniciar a gravação manual. O ícone muda para .

Observação

Durante a gravação manual, **Gravando...** será exibido no canto superior direito da janela de exibição.

4. Clique para parar a gravação.
   Uma caixa de diálogo direcionando para o local de salvamento do arquivo é exibida.

Observação

- Você pode alterar o caminho de salvamento de arquivos de vídeo em System. Para obter detalhes, consulte ***Set General Parameters*** .
- O vídeo não pode ser salvo se o espaço livre no disco for inferior a 2 GB.

5. (Opcional) Execute outras operações na caixa de diálogo pop-up após a gravação manual.

Operação	Descrição
Abrir pasta	Clique em **Abrir pasta** para acessar a pasta do arquivo de vídeo.
Salvar como	Clique em **Salvar como** e especifique o caminho para salvar o arquivo para alterar o local de salvamento dos arquivos de vídeo gravados.
Salvar como evidência	Clique em **Salvar como** , marque **Salvar como evidência** e edite as informações para salvar a filmagem como evidência. **Observação** Consulte ***Salvar vídeo gravado manualmente no Evidence Management Center*** para obter detalhes.

Capturar Imagens

1. No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Monitoramento** → **Monitoramento** .
2. Mova o cursor para a janela de exibição ao vivo para mostrar a barra de ferramentas.
3. Clique na barra de ferramentas para capturar uma imagem.
   Uma caixa de diálogo direcionando para o local de salvamento é exibida.

Observação

- Você pode alterar o caminho de salvamento para imagens capturadas no Sistema. Para obter detalhes, consulte ***Definir parâmetros gerais*** .
- A imagem não pode ser salva se o espaço livre no disco for inferior a 512 MB.

4. (Opcional) Após a caixa de diálogo aparecer, execute a(s) seguinte(s) operação(ões).

Operação	Descrição
Verifique a imagem	Clique em **Abrir pasta** na caixa de diálogo para abrir a pasta onde as imagens capturadas foram armazenadas e visualizá-las.
Editar imagem	a. Clique em **Editar** na caixa de diálogo para abrir a janela Capturar. b. Pressione e mova o cursor na imagem para desenhar. Por exemplo, você pode marcar as pessoas suspeitas na imagem. c. Clique em **Salvar como** e especifique o caminho para salvar a imagem editada. **Observação** A imagem não pode ser salva se o espaço livre no disco for inferior a 512 MB.
Pesquisa de imagens	Clique em **Picture Search** para abrir a janela de pesquisa de vídeo. Consulte ***Search Captured Face Pictures by Feature*** para mais detalhes.

5.4.8 Executar Rastreamento Visual na Visualização ao Vivo

Durante a visualização ao vivo, se a câmera estiver configurada com câmeras associadas para rastreamento visual, você poderá rastrear facilmente o indivíduo que apareceu acessando diretamente o vídeo ao vivo das câmeras adjacentes.

Passos

1. No canto superior esquerdo da página inicial, selecione → **Todos os módulos** → **Monitoramento** → **Monitoramento** .
2. Inicie a visualização ao vivo de uma câmera configurada com rastreamento visual.
3. Na barra de ferramentas de visualização ao vivo, clique para entrar no modo de rastreamento visual.
   A visualização ao vivo da câmera atual e das câmeras associadas será exibida.
4. Quando o indivíduo sair do campo de visão da câmera, clique no ícone da câmera associada, que representa um link para pular para a visualização ao vivo da câmera associada.

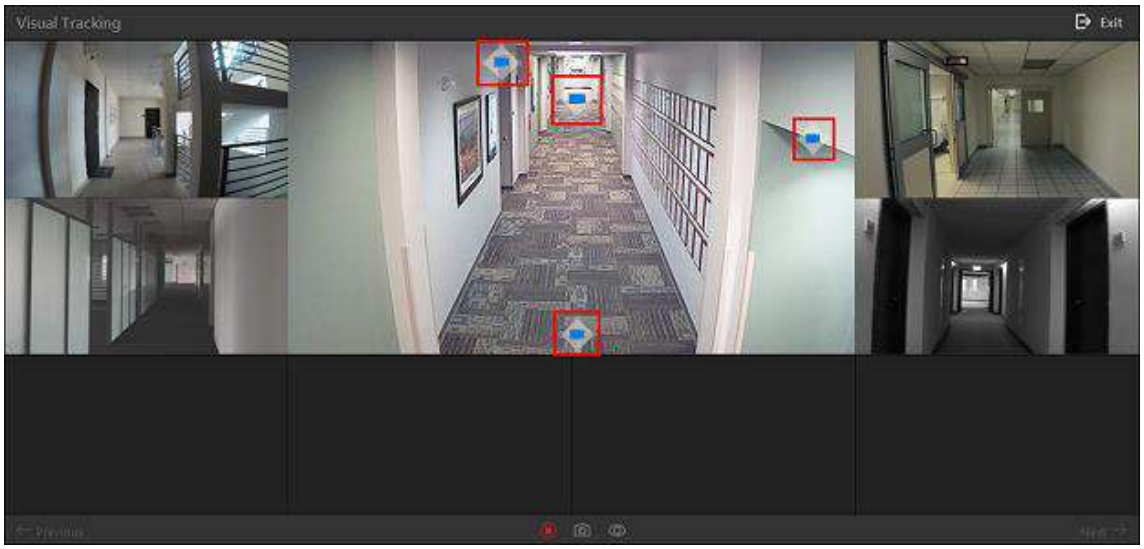


Figura 5-9 Rastreamento visual na visualização ao vivo

A visualização ao vivo da câmera associada será exibida no meio. Enquanto isso, a visualização ao vivo das câmeras associadas (se configuradas) desta câmera associada será exibida.

5. **Opcional**: Você pode executar as seguintes operações durante o rastreamento visual.

Parar gravação	Na barra de ferramentas, clique para parar de gravar o vídeo da câmera no meio. **Observação** Por padrão, a gravação de vídeo inicia automaticamente ao entrar no rastreamento visual.
Capturar uma imagem	Na barra de ferramentas, clique para capturar uma imagem para a câmera no meio. Após a captura, você pode clicar em **Pesquisa de imagens** para realizar uma pesquisa mais aprofundada. Para pesquisar imagens capturadas, consulte ***Pesquisar imagens de rosto capturadas por recurso*** . Para pesquisar no arquivo, consulte ***Pesquisar Arquivos*** .
Mostrar/Ocultar Ícone da Câmera	Na barra de ferramentas, clique em / para mostrar ou ocultar os ícones das câmeras associadas.
Ir para a câmera anterior/seguinte	Clique em ← **Anterior** ou **Próximo** → para pular para a visualização ao vivo da câmera anterior ou seguinte.

6. Clique em **Sair** no canto superior direito para sair do modo de rastreamento visual.

Observação

Na janela pop-up, você pode clicar em **OK** para salvar o arquivo de vídeo gravado. Clique em **Cancelar** ou para descartar o arquivo de vídeo gravado e voltar para a janela de visualização ao vivo.

5.4.9 Exibir Densidade de Pessoas na Visualização ao Vivo

Para uma câmera vinculada a um servidor de detecção de eventos anormais, você pode visualizar seu vídeo ao vivo, mapa de calor que mostra dados de densidade de pessoas e estatísticas em tempo real da quantidade de pessoas simultaneamente. Dessa forma, você pode monitorar a densidade de pessoas no campo de visão da câmera em tempo real, evitando assim a aglomeração excessiva de pessoas em ocasiões especiais, como surtos epidêmicos.

Antes de Começar

- Certifique-se de ter adquirido a licença que suporta análise de densidade de pessoas.
- Certifique-se de ter adicionado um servidor de detecção de eventos anormais ao SYS e câmeras vinculadas ao servidor, e de ter definido tarefas de análise de densidade de pessoas para as câmeras no Web Client. Para obter detalhes, consulte o *HikCentral Professional Web Client User Manual* .
- Certifique-se de ter configurado a análise de densidade de pessoas no servidor de detecção de eventos anormais. Para detalhes, consulte o manual do usuário do servidor.

Passos

Observação

A função deve ser suportada pela câmera.

1. Inicie a visualização ao vivo de uma câmera vinculada ao servidor de detecção de eventos anormais.

Observação

Para obter detalhes, consulte ***Visualização ao Vivo*** .

2. Passe o cursor sobre a imagem de visualização ao vivo para mostrar a barra de ferramentas e, em seguida, clique na barra de ferramentas para entrar no modo de análise de densidade de pessoas.
   A janela de exibição será dividida em três partes: o vídeo ao vivo (visão óptica) da câmera, um mapa de calor e um gráfico de linhas.
   No mapa de calor, as pessoas na imagem são destacadas, o que permite que você visualize seus movimentos claramente.
   No gráfico de linhas, são exibidas a tendência de variação da quantidade de pessoas e a quantidade de pessoas em tempo real.

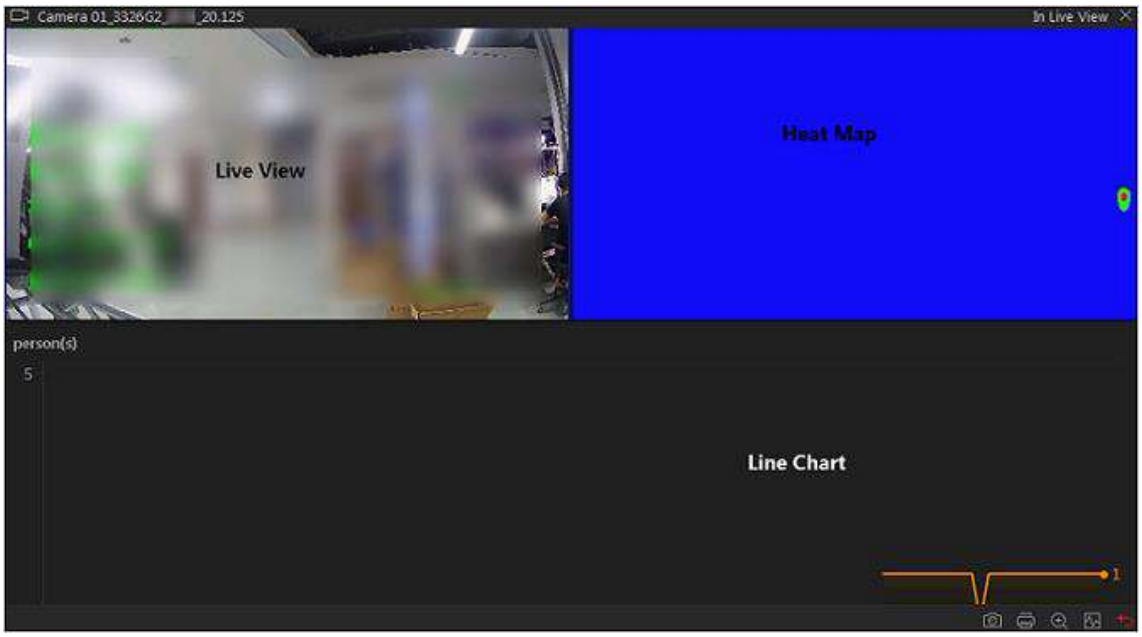


Figura 5-10 Exibir densidade de pessoas na visualização ao vivo

3. **Opcional**: execute as seguintes operações, se necessário.

Captura e gravação manual	Clique para capturar uma foto.
Imprimir imagem capturada	Clique para capturar uma imagem e depois imprimi-la.
Ver status da câmera	Clique para visualizar as informações de status da câmera, incluindo taxa de quadros, resolução, taxa de bits, status da rede, status do sinal, status da gravação, local de armazenamento de vídeo, local de armazenamento de fotos, etc.

5.4.10 Exibir Rosto Detectado e Correspondido na Visualização ao Vivo

Durante a visualização ao vivo de câmeras de reconhecimento facial, os rostos detectados serão exibidos na janela. Após definir a biblioteca de imagens faciais e aplicá-la à câmera, a imagem facial correspondente ao rosto na biblioteca de imagens faciais será exibida, mostrando os detalhes da pessoa, a imagem capturada, a imagem original da pessoa correspondente e a similaridade. Se a pessoa detectada não estiver na biblioteca de imagens faciais, você também pode adicioná-la à biblioteca de imagens faciais e aplicar a biblioteca ao dispositivo para que tenha efeito.

Antes de Começar

Adicione o dispositivo necessário e configure a biblioteca de imagens faciais. Consulte o *Manual do Usuário do HikCentral Professional Web Client* .

Passos

Observação

Esta função deve ser suportada pelo dispositivo.

1. No canto superior esquerdo da página inicial, selecione → **Todos os módulos** → **Monitoramento** → **Monitoramento** .
2. Inicie a visualização ao vivo.
   – Arraste uma câmera de reconhecimento facial da lista de câmeras à esquerda para a janela de exibição.
   – Clique duas vezes no nome de uma câmera de reconhecimento facial para iniciar a visualização ao vivo.

   Se um rosto for detectado, ele será exibido à direita da janela. Se ele/ela não for correspondido com nenhuma pessoa nas bibliotecas de imagens de rosto vinculadas da câmera, o tempo de captura será marcado com um fundo laranja, como a seguir.

Figura 5-11 Pessoa incompatível

3. Visualize pessoas correspondentes em diferentes bibliotecas de imagens de rosto.

   Exemplo

   Por exemplo, você pode visualizar as pessoas correspondentes na lista de bloqueio e na lista VIP ao mesmo tempo.

   1) Clique na aba para abrir a lista da biblioteca de imagens de rosto.
      Todas as bibliotecas de imagens de rosto adicionadas ao sistema são exibidas.
   2) Clique duas vezes no nome da biblioteca de imagens de rosto na lista ou arraste-a para a janela de exibição.
      Um painel em branco da biblioteca de imagens de rostos será exibido à direita das janelas de exibição.

   Se houver pessoas correspondentes à pessoa no grupo da biblioteca de imagens, as imagens capturadas e originais do rosto serão exibidas neste painel em pares com similaridade da seguinte forma.

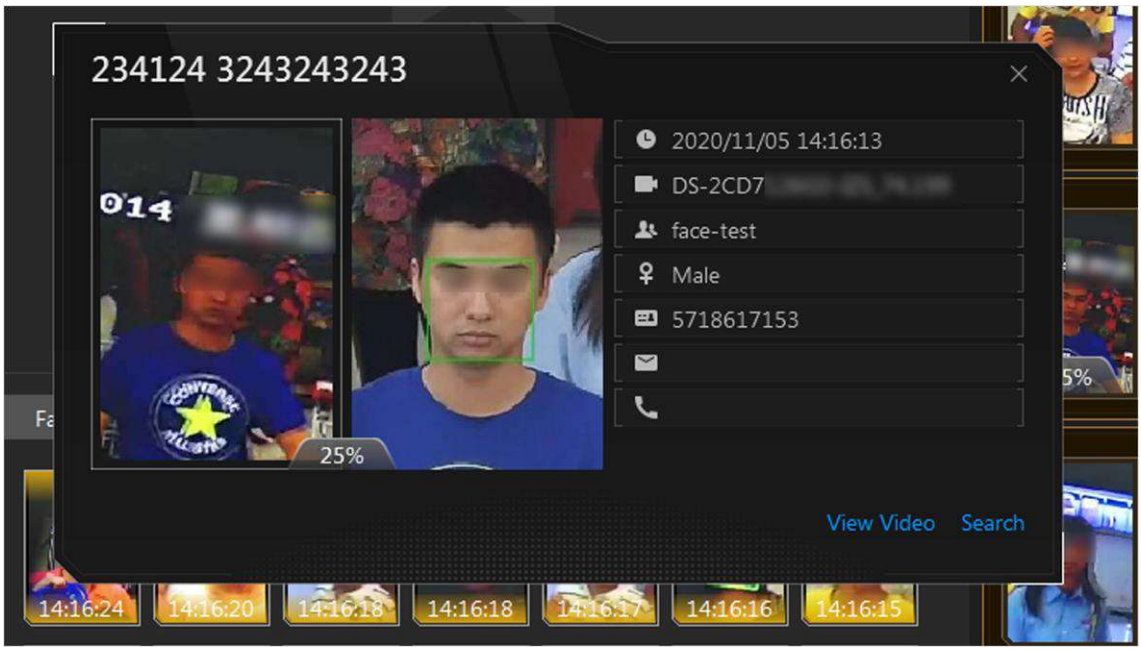


Figura 5-12 Pessoas Correspondidas

Você pode visualizar a foto do rosto capturada, o perfil da pessoa (configurado no Web Client) e a similaridade. O nome da pessoa é mostrado no perfil.

4. **Opcional**: visualize todos os eventos de comparação de imagens de rosto em tempo real.
   1) Clique na parte inferior da página para mostrar o painel da lista de eventos.
   2) Clique na aba **Comparação de imagens faciais** para visualizar todos os rostos detectados (incluindo pessoas correspondentes e não correspondentes).

Observação

Para pessoas incompatíveis, o horário de captura da imagem é marcado com um fundo laranja, conforme a seguir.

Figura 5-13 Pessoa incompatível

5. **Opcional**: Para as pessoas correspondentes, visualize os detalhes da pessoa.
   – No painel de imagens de rostos correspondentes, clique para ver os detalhes da pessoa correspondente.
   – Clique na foto do rosto da pessoa correspondente na lista de eventos de comparação de fotos para ver os detalhes da pessoa.
   – No painel da lista de todos os eventos, selecione o evento correspondente à pessoa e clique na coluna Operação para visualizar as informações da pessoa.

6. **Opcional**: Se houver várias câmeras na visualização ao vivo, você pode encontrar rapidamente a câmera que capturou determinada imagem e visualizar sua visualização ao vivo.
   – No painel de imagens de rostos correspondentes, clique em .
   – Na lista de eventos Comparação de imagens faciais, clique na imagem capturada e clique em **Visualização ao vivo** .

   A câmera que captura esta imagem será destacada com uma moldura vermelha.
7. **Opcional**: Para as imagens capturadas (pessoas incompatíveis ou correspondentes), você pode clicar na imagem e executar as seguintes operações.

Pesquisa de imagens	Clique em **Picture Search** para ir para a página Picture Search para procurar a pessoa alvo nas fotos capturadas carregando uma foto de rosto. Para informações detalhadas, veja ***Search Face Pictures by Picture*** .
Pesquisa de arquivo	Clique em **Pesquisa de arquivo** para ir para a página Pesquisa de arquivo e pesquisar no arquivo da pessoa.
Verificação de identidade	Clique em **Verificação de identidade** → **A ser verificado** para verificar a identidade da pessoa ou clique em **Verificação de identidade** → **Alvo** para definir a pessoa como alvo de comparação.

8. **Opcional**: clique duas vezes em uma imagem capturada e clique em **Baixar** para baixar a imagem capturada.

5.4.11 Adicionar Pessoa Incompatível ao Grupo de Pessoas

Durante a visualização ao vivo, se uma pessoa for detectada, mas não for correspondida com nenhuma pessoa no grupo da biblioteca de imagens, e se você quiser que a pessoa seja reconhecida na próxima vez, você pode adicionar a pessoa à biblioteca de imagens de rosto. Por exemplo, se a pessoa detectada for um VIP recém-chegado, você pode adicionar a pessoa à biblioteca de imagens de rosto VIP e aplicar essa biblioteca à câmera. Na próxima vez, a câmera reconhecerá o rosto da pessoa e a corresponderá com as informações da pessoa na biblioteca de imagens de rosto.

Passos

1. No canto superior esquerdo da página inicial, selecione → **Todos os módulos** → **Monitoramento** → **Monitoramento** e execute a comparação de imagens faciais na visualização ao vivo.

Observação

Para obter detalhes, consulte ***Exibir rosto detectado e correspondente na visualização ao vivo*** .

2. Abra o painel Adicionar ao grupo de pessoas.
   – Na parte inferior da página, clique para desdobrar o painel Todos os eventos e clique na coluna Operação para abrir a página Adicionar ao grupo de pessoas.

– Clique nas imagens de rostos incompatíveis no painel de eventos Comparação de imagens de rostos e clique em **Adicionar ao grupo de pessoas** .

3. Selecione as bibliotecas de imagens de rosto às quais você deseja adicionar esta pessoa.
4. Insira os detalhes da pessoa, como ID, nome, sobrenome, informações adicionais personalizadas, etc.
5. Clique em **Adicionar** .

O que fazer a seguir

Efetue login no Web Client e aplique a biblioteca de imagens de rosto à câmera para que tenha efeito.

5.4.12 Adicionar Veículo Reconhecido à Lista de Veículos

O número da placa do veículo reconhecido será exibido tanto na página de visualização ao vivo quanto na página de registro do veículo. Então você pode adicionar os veículos reconhecidos à lista de veículos nas duas páginas. Além disso, você pode adicionar um veículo reconhecido à lista de veículos na página de pesquisa de veículos.

No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Monitoramento** → **Monitoramento** .

Adicionar veículo reconhecido à lista de veículos na página de visualização ao vivo

Selecione uma câmera para reconhecimento de placa para iniciar a visualização ao vivo. Clique na parte inferior do cliente para mostrar a lista de eventos e, em seguida, clique na aba **Vehicle Record** para mostrar eventos de reconhecimento de veículos.

Na parte inferior da página, clique em → **Registro do veículo** → para abrir o painel Adicionar à lista de veículos; à direita da página, clique em → **Veículo** , passe o cursor sobre uma área de veículo de destino e clique para abrir o painel Adicionar à lista de veículos.

Defina as informações do veículo, incluindo número da placa, validade, características do veículo, informações do proprietário do veículo e selecione uma lista de veículos para adicionar o veículo. Clique em **Adicionar** para adicionar o veículo à lista de veículos selecionada.

Observação

Consulte ***Visualização ao vivo*** para obter detalhes sobre como iniciar a visualização ao vivo.

Adicionar veículo reconhecido à lista de veículos na página de entrada e saída

Entre na página Entrada e Saída, os veículos reconhecidos serão exibidos na aba **Registro do Veículo .**

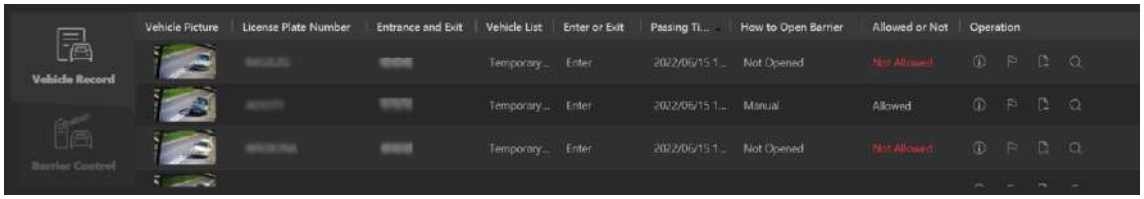


Figura 5-14 Registro do veículo

Clique na coluna Operação para abrir o painel Adicionar à lista de veículos.

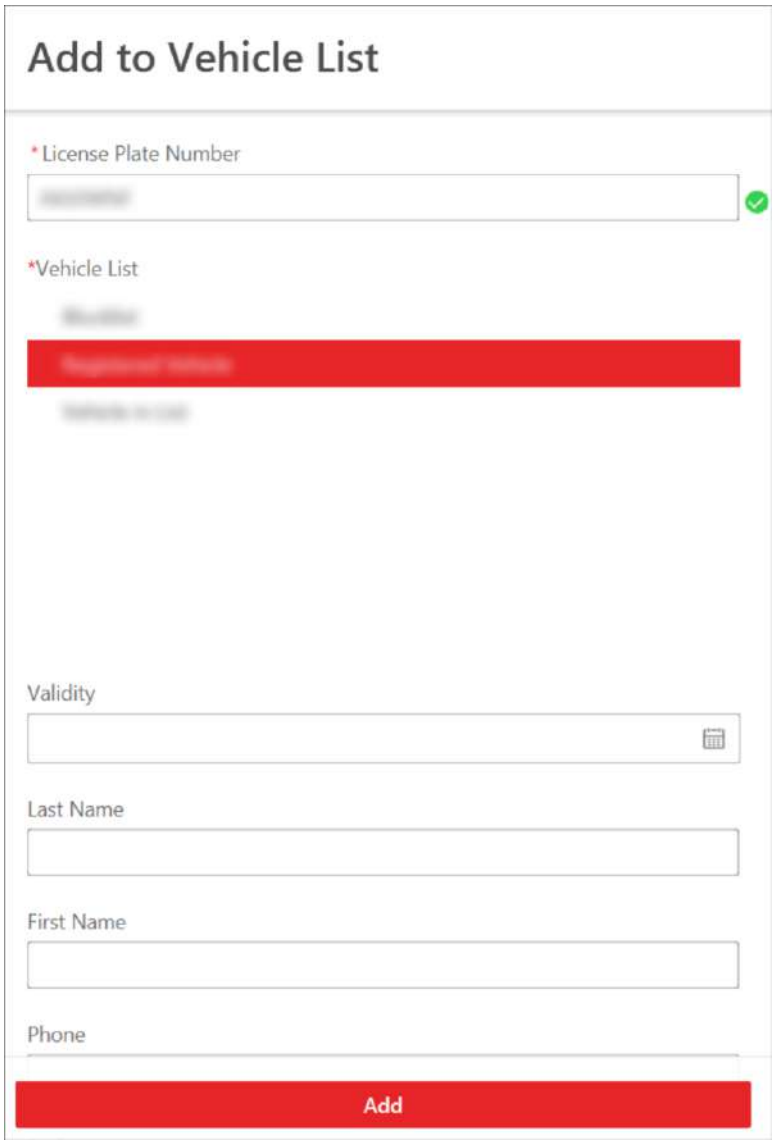


Figura 5-15 Adicionar à lista de veículos

Defina as informações do veículo, incluindo número da placa, validade, características do veículo, informações do proprietário do veículo e selecione uma lista de veículos para adicionar o veículo. Clique em **Adicionar** para adicionar o veículo à lista de veículos selecionada.

Adicionar veículo reconhecido à lista de veículos na página de pesquisa de veículos

Pesquise veículos reconhecidos por entrada e saída. Veja ***Search for Passing Vehicles Detected by Cameras and UVSSs*** para detalhes.

Na área de resultados da pesquisa, clique na coluna **Operação** para abrir o painel Adicionar à lista de veículos.

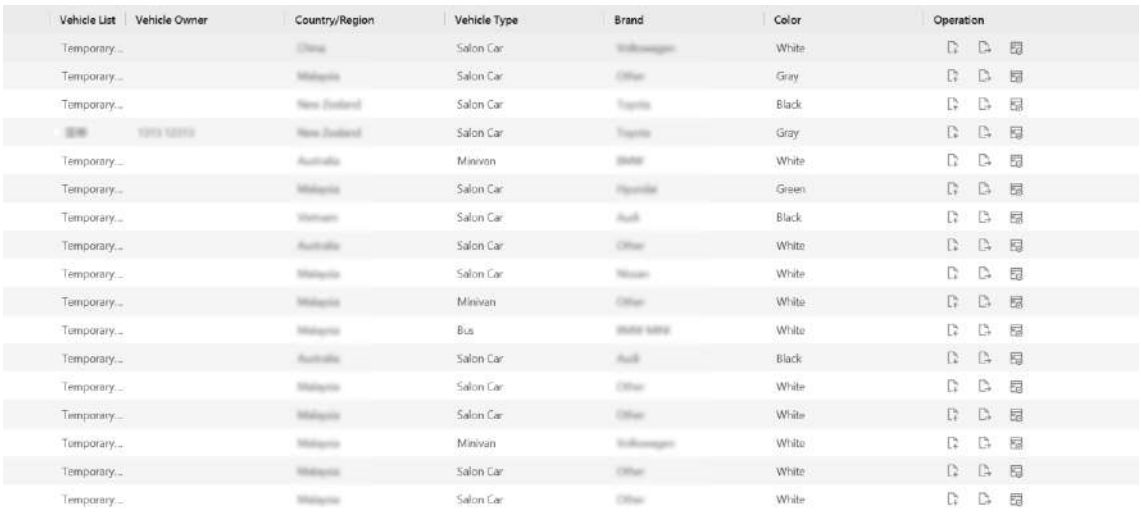


Figura 5-16 Resultados da pesquisa de veículos

Defina as informações do veículo, incluindo número da placa, validade, características do veículo, informações do proprietário do veículo e selecione uma lista de veículos para adicionar o veículo. Clique em **Adicionar** para adicionar o veículo à lista de veículos selecionada.

5.4.13 Mais Funções

Há outras funções suportadas durante a visualização ao vivo, incluindo inicialização em lote de limpadores, abertura de tela(s) auxiliar(es), etc.

Recurso Integrado de Terceiros

Clique para controlar os recursos de terceiros.

Operar Todos os Pontos de Acesso

Clique para controlar o status do(s) ponto(s) de acesso.

Personalize a Barra de Ferramentas de Visualização ao Vivo e Reprodução

Clique em → **Vídeo básico** → **Barra de ferramentas** para personalizar os ícones na barra de ferramentas de exibição ao vivo e reprodução.

Observação

Para obter detalhes sobre as diferentes funções dos ícones, consulte ***Personalizar ícones na janela de visualização ao vivo*** e ***Personalizar ícones na janela de reprodução*** .

Adicionar aos Favoritos

Clique para adicionar a câmera aos Favoritos. Você pode clicar em **Criar Favoritos** para criar um novo Favoritos.

Abrir Tela Auxiliar

O vídeo ao vivo pode ser exibido em diferentes telas auxiliares para monitorar várias cenas. Clique

acima da área da janela de exibição para abrir uma tela auxiliar. Até 4 telas auxiliares para visualização ao vivo são suportadas.

5.4.14 Personalizar Ícones na Janela Live View

Você pode personalizar os ícones na barra de ferramentas da janela de visualização ao vivo, ajustar a ordem dos ícones e controlar se deseja sempre mostrar a barra de ferramentas na janela de visualização ao vivo ou não.

Passos

1. No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Gerenciamento** → **Sistema** .
2. Selecione **Vídeo básico** → **Barra de ferramentas** .
3. Na seção **Personalizar barra de ferramentas de visualização ao vivo** , adicione ou remova os ícones para mostrar ou ocultar os ícones na barra de ferramentas de visualização ao vivo.
4. Arraste os ícones na lista de ícones para ajustar a ordem.

Tabela 5-1 Ícones na barra de ferramentas Live View

	Controle de áudio	Desligue/ligue o som e ajuste o volume.
	Capturar	Tire um instantâneo do vídeo atual e salve-o no PC atual. **Observação** Após capturar uma imagem, uma miniatura aparecerá no canto superior direito. Você pode clicar em **Picture Search** para pesquisar a imagem capturada, arquivar e verificar a identidade relacionada à imagem capturada.
	Registro	Inicie a gravação manual. O arquivo de vídeo será armazenado no PC local.
	Reprodução instantânea	Alterne para o modo de reprodução instantânea para visualizar os arquivos de vídeo gravados.
	Áudio bidirecional	Inicie o áudio bidirecional com a câmera para obter o áudio em tempo real do dispositivo e realizar uma conversa de voz com a pessoa no dispositivo.
	Zoom digital	Amplie ou reduza o vídeo para câmeras que não têm seus próprios recursos de zoom óptico. Clique novamente para desabilitar a função.
	Controle PTZ	Ative os ícones PTZ na imagem para mover, inclinar ou

		ampliar a imagem.
	Expansão Fisheye	Disponível para câmera fisheye. No modo de dewarping fisheye, o Control Client corrigirá a imagem de vídeo e reverterá os efeitos de distorções geométricas causadas pela lente da câmera fisheye. Veja ***View Dewarped Live View of Fisheye Camera*** para detalhes.
	Status da câmera	Exibe o status de gravação da câmera, status do sinal, número de conexão, etc.
	Controle de Armar	Abra a janela de controle de armar da câmera para armar ou desarmar o evento da câmera. O Control Client pode receber os eventos ou alarmes armados.
	Trocar fluxo	Alterne a transmissão de visualização ao vivo para transmissão principal, transmissão secundária (se compatível) ou transmissão suave (se compatível). **Observação** O smooth stream mostrará se o dispositivo suporta. Você pode alternar para smooth stream quando estiver em uma situação de largura de banda baixa para tornar a visualização ao vivo mais fluente.
	Exibir na parede inteligente	Exiba o vídeo ao vivo no smart wall. Veja ***Gerenciar Smart Wall (Dispositivo de decodificação)*** para detalhes.
	VCA / Pesquisa Inteligente	Exiba a janela VCA/Smart Search. Você pode definir uma regra para pesquisar arquivos de vídeo e filtrar os vídeos por tipos de eventos. Consulte ***Search VCA/Smart Event Related Video*** para obter detalhes.
	Saída de alarme	Exiba a página Alarm Output Control e ligue/desligue as saídas de alarme da câmera conectada. Veja ***Control Alarm Input/Output*** para detalhes.
	Adicionar Tag	Adicione uma tag para a filmagem de vídeo em um intervalo de tempo selecionado durante a visualização ao vivo. Veja ***Mais Funções*** para detalhes.
	Rastreamento visual	Rastreie um indivíduo (como um suspeito) em diferentes áreas sem perder o indivíduo de vista. Consulte *o Manual do Usuário do HikCentral Professional Web Client* e ***Execute Visual Tracking in Live View*** para obter detalhes.

	Zoom local	Crie área(s) de zoom na imagem de vídeo para visualizar a visualização ao vivo detalhada. Veja ***Criar área de zoom para visualizar a visualização ao vivo detalhada*** para obter detalhes.
	Criar área de zoom deformado	Crie áreas de zoom dewarped na imagem de vídeo para visualizar a visualização ao vivo detalhada. Veja ***Criar área de zoom para visualizar a visualização ao vivo detalhada*** para obter detalhes.
	Pesquisa de imagens	Procure a pessoa alvo pelas fotos capturadas. Veja ***Pesquisar Fotos de Rosto Capturadas por Característica*** para detalhes.
	Ligação manual	Localize ou rastreie o alvo que apareceu na visão da câmera bullet ou box com uma speed dome conectada.
	Densidade de Pessoas	Visualize dados de densidade de pessoas e estatísticas em tempo real da quantidade de pessoas. Veja ***Exibir densidade de pessoas em Live View*** para obter detalhes.
	Transmissão	Inicie a transmissão para as unidades de alto-falante conectadas.
	Melhoria	Ajuste a imagem do vídeo, incluindo brilho, saturação, etc.
	Girar imagem	Girar uma imagem.
	Ação do Parque	Clique no ícone e o speed dome salvará a visualização atual na predefinição nº 32. O dispositivo começa a estacionar na predefinição nº 32 automaticamente após um período de inatividade (tempo de estacionamento).
	Exibição de destino	Clique no ícone e o atributo alvo, como pessoa e veículo, será sobreposto na imagem.
	Localizar alvo	Clique no ícone para medir a distância entre a câmera e o alvo.
	Armar pessoa/veículo	Clique no ícone para iniciar o rastreamento automático de pessoas e veículos.
	Panorama	Usando a câmera AR e o domo de velocidade adicionados a uma cena, você pode executar o rastreamento panorâmico de um alvo em movimento clicando na imagem panorâmica.
	Limpar manualmente	Clique no ícone para limpar a câmera.
	Pesquisa de Objetos	Selecione uma pessoa na imagem e procure por ela.

Observação

Os ícones na barra de ferramentas na janela de visualização ao vivo variam de acordo com os recursos do dispositivo.

5. Clique em **Salvar** .

5.5 Monitoramento de Temperatura e Contagem de Pessoas em Tempo Real

Com a função de análise de contagem de pessoas, você pode monitorar as pessoas que permaneceram em uma área enquanto monitora suas características (incluindo temperatura da superfície da pele, uso ou não de máscara, semelhança com pessoas já adicionadas, etc.).
No Painel de Controle, clique em → **Todos os Módulos** → **Monitoramento** → **Monitoramento** → **Análise de Contagem de Pessoas** .

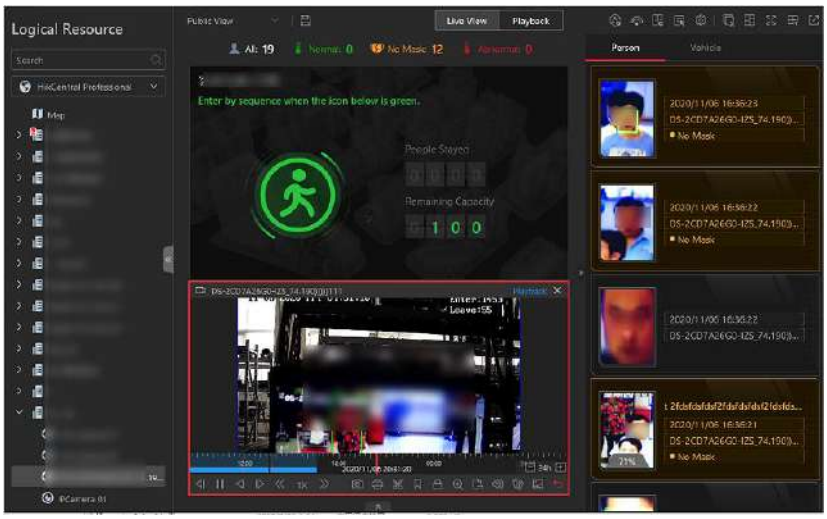


Figura 5-17 Monitoramento de temperatura e contagem de pessoas em tempo real

Triagem de temperatura em tempo real

Na página Monitoramento, após iniciar a visualização ao vivo de um ponto de triagem da superfície da pele, você pode visualizar as informações mais recentes sobre a temperatura da superfície da pele à direita.
Pessoas com características diferentes serão marcadas por cores diferentes. A cor verde indica que a temperatura da superfície da pele da pessoa detectada é normal e que a pessoa está usando uma máscara. A cor laranja indica que uma pessoa com temperatura normal da superfície da pele não usa máscara. A cor vermelha indica uma pessoa com temperatura anormal da superfície da pele.
Se houver pessoas cujas temperaturas da superfície da pele forem anormais, você saberá na primeira vez. Além disso, você poderá localizar rapidamente as pessoas de acordo com o nome do

ponto de triagem exibido.
Além disso, você pode ir para a página People Counting Analysis e arrastar o grupo de contagem de pessoas correspondente da câmera atual para a área de visualização ao vivo. Dessa forma, você pode monitorar os dados de contagem de pessoas durante a visualização ao vivo.

Contagem de Pessoas em Tempo Real

À esquerda, todos os grupos de contagem de pessoas são exibidos. Arraste um ou mais grupos de contagem de pessoas para a área de visualização ao vivo para mostrar os dados de contagem de pessoas em tempo real. Os dados de contagem de pessoas em tempo real incluem pessoas que ficaram e entradas restantes da área monitorada, e se mais pessoas têm permissão para entrar.
Vá para a página Logical Resource e inicie a visualização ao vivo da (s) câmera(s) de triagem de temperatura da superfície da pele que monitoram a mesma área com o grupo de contagem de pessoas mencionado acima. Dessa forma, enquanto monitora a quantidade de pessoas na área monitorada, você pode visualizar a visualização ao vivo da área monitorada para obter informações da pessoa, incluindo foto do rosto, temperatura da superfície da pele, uso de máscara ou não, etc. As informações mais recentes da pessoa serão exibidas à direita em formato de miniatura.

As pessoas Ficaram

A quantidade de pessoas que estão atualmente dentro da área monitorada.

Capacidade Restante

A quantidade de pessoas que podem entrar na área monitorada. Se a quantidade de pessoas que ficaram exceder o número definido ao adicionar um grupo de contagem de pessoas, nenhuma pessoa poderá entrar, e o ícone verde ficará vermelho para notificação.

Editar Informações Exibidas

Passe o cursor sobre a janela de análise de contagem de pessoas e clique para corrigir a quantidade de pessoas restantes ou editar descrições e títulos.

- Quantidade correta de pessoas: se o número real de pessoas hospedadas for diferente do número exibido no Control Client, você pode inserir a quantidade correta de pessoas **no campo Número correto de pessoas no título 01** .
- Segundo idioma: o Control Client suporta a exibição de descrições e manchetes em dois idiomas. Além do inglês, você pode inserir as descrições e manchetes em outro idioma para exibir as informações em dois idiomas simultaneamente.

Capítulo 6 Reprodução

Você pode iniciar a reprodução de uma câmera ou canal. Você também pode procurar por vídeos gravados.

6.1 Reprodução

Os arquivos de vídeo armazenados em dispositivos de armazenamento locais, como HDDs, Net HDDs e cartões SD/SDHC ou no Servidor de Gravação, podem ser pesquisados e reproduzidos remotamente por meio do navegador da web.
No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Monitoramento** → **Monitoramento** .

6.1.1 Iniciar Reprodução

Você pode pesquisar arquivos de vídeo por área ou câmera e iniciar a reprodução e baixar os arquivos de vídeo encontrados para o PC local.

Observação

- Você pode pesquisar arquivos de vídeo pelo fuso horário em que o dispositivo está localizado ou pelo fuso horário em que o PC que executa o Control Client está localizado.
- A conversão automática do horário de verão para o horário padrão é suportada, ou vice-versa.
- A reprodução síncrona ou assíncrona de dispositivos em diferentes fusos horários é suportada.

6.1.2 Iniciar Reprodução no Modo de Visualização

Clique na aba no painel esquerdo.
Clique na aba **Reprodução** para entrar na página de reprodução.
Clique em uma visualização para iniciar rapidamente a reprodução de todas as câmeras relacionadas à visualização. Clique em uma visualização para iniciar rapidamente a reprodução de todas as câmeras relacionadas à visualização.

6.1.3 Iniciar Reprodução Síncrona

Inicie a reprodução normal de pelo menos duas câmeras.
Após iniciar a reprodução normal, clique em **Reprodução Síncrona** na barra de ferramentas de reprodução para habilitar a reprodução síncrona.

6.1.4 Iniciar Reprodução Fisheye

Selecione uma câmera olho de peixe na lista de câmeras para iniciar a reprodução.

Mova o cursor para a janela de exibição e clique na barra de ferramentas que aparece para entrar no modo de correção de distorção olho de peixe.
Arraste o vídeo para ajustar o ângulo de visão e role a roda do mouse para aumentar ou diminuir o zoom na visualização.

6.1.5 Iniciar Reprodução de Câmeras Favoritas

1. Clique na aba no painel esquerdo.
2. Selecione um Favorito pai, clique para adicionar um Favorito sob o Favorito pai e selecione a(s) câmera(s) a serem adicionadas aos Favoritos.

Observação

É possível adicionar até 5 níveis de Favoritos.

3. (Opcional) Selecione um Favorito e clique em → **Compartilhar** no lado direito do nome dos Favoritos para compartilhá-lo com outras pessoas.
4. Na janela Reprodução, selecione Favoritos e clique em → **Reproduzir tudo** para começar a visualizar a exibição ao vivo de todas as câmeras adicionadas aos Favoritos.

6.2 Ver Vídeo de Rastreamento Visual

Durante a reprodução, se a câmera estiver configurada com câmeras associadas para rastreamento visual, você poderá rastrear facilmente o indivíduo que apareceu acessando diretamente o vídeo gravado das câmeras adjacentes.

Passos

1. No canto superior esquerdo da página inicial, selecione → **Todos os módulos** → **Monitoramento** → **Monitoramento** .
2. Inicie a reprodução da câmera.
3. Na barra de ferramentas de reprodução, clique para entrar no modo de rastreamento visual. O vídeo gravado da câmera atual e das câmeras associadas será exibido.
4. Quando o indivíduo sair do campo de visão da câmera, clique no ícone da câmera associada, que representa um link para a próxima câmera.

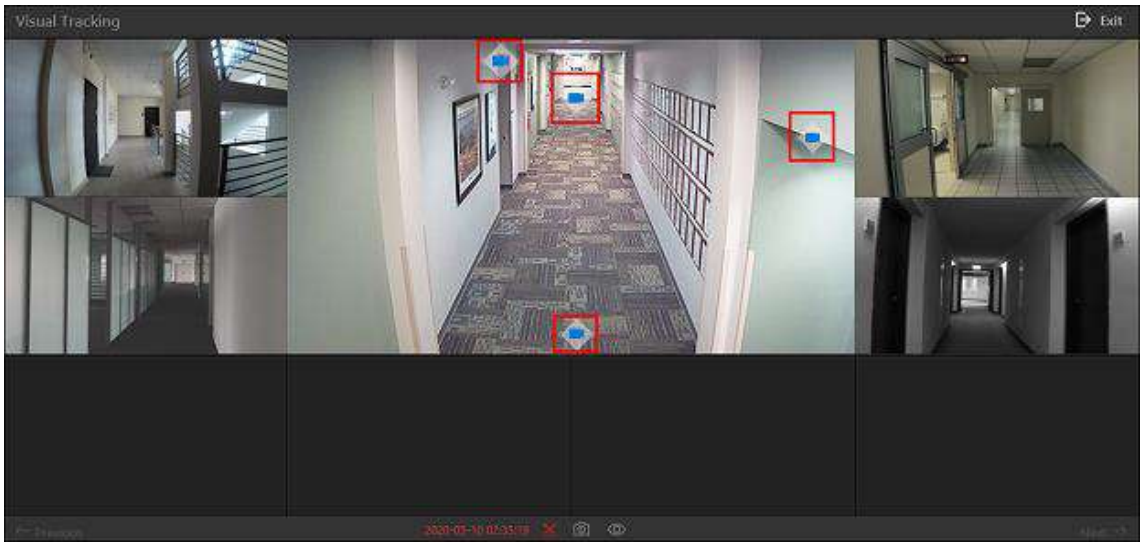


Figura 6-1 Rastreamento visual na reprodução

O vídeo gravado da câmera associada será exibido no meio. Enquanto isso, o vídeo gravado das câmeras associadas desta câmera associada será exibido.

5. **Opcional**: Você pode executar as seguintes operações durante o rastreamento visual.

Parar de cortar	Na barra de ferramentas, clique para parar de recortar a filmagem da câmera no meio.
	Observação Por padrão, o recorte de vídeo inicia automaticamente ao entrar no rastreamento visual.
Capturar uma imagem	Na barra de ferramentas, clique para capturar uma imagem para a câmera no meio. Após a captura, você pode clicar em **Pesquisa de imagens** para realizar uma pesquisa mais aprofundada. Para pesquisar imagens capturadas, consulte ***Pesquisar imagens de rosto capturadas por recurso*** . Para pesquisar no arquivo, consulte ***Pesquisar Arquivos*** .
Mostrar/Ocultar Ícone da Câmera	Na barra de ferramentas, clique em / para mostrar ou ocultar os ícones das câmeras associadas.
Ir para a câmera anterior/seguinte	Clique em ← **Anterior** ou **Próximo** → para pular para a reprodução da câmera anterior ou seguinte.

6. Clique em **Sair** no canto superior direito para sair do modo de rastreamento visual.

Observação

Na janela pop-up, você pode clicar em **OK** para salvar o arquivo de vídeo recortado. Clique em **Cancelar** ou para descartar o arquivo de vídeo recortado e voltar para a janela de reprodução.

6.3 Personalizar Ícones na Janela de Reprodução

Você pode personalizar os ícones exibidos na barra de ferramentas da janela de reprodução, ajustar a ordem dos ícones e definir se deseja sempre exibir a barra de ferramentas na janela de reprodução.

Passos

1. No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Gerenciamento** → **Sistema** .
2. Selecione **Vídeo básico** → **Barra de ferramentas** .
3. Role para baixo até a seção **Personalizar barra de ferramentas de reprodução** , adicione ou remova os ícones para mostrar ou ocultar os ícones na barra de ferramentas de reprodução.
4. Personalize a barra de ferramentas de reprodução.
   - Clique em um ícone na lista para adicioná-lo ao quadro cinza abaixo para ocultar o ícone. Os ícones no quadro cinza ficarão ocultos na barra de ferramentas da janela de reprodução.
   - Clique no ícone no quadro cinza para adicioná-lo novamente à barra de ferramentas de reprodução para mostrar um ícone na barra de ferramentas.
5. Arraste os ícones na lista de ícones para ajustar a ordem dos ícones.

Tabela 6-1 Ícones na barra de ferramentas de reprodução

	Controle de áudio	Desligue/ligue o som e ajuste o volume.
	Capturar	Tire um instantâneo do vídeo atual e salve no PC atual. **Observação** Após capturar uma imagem, uma miniatura aparecerá no canto superior direito. Você pode clicar em **Picture Search** para pesquisar a imagem capturada e a verificação de identidade relacionada à imagem capturada.
	Grampo	Recorte os arquivos de vídeo para reprodução atual e salve no PC atual. Você pode salvar o vídeo recortado como evidência e definir o caminho de salvamento para os arquivos de vídeo recortados. Para obter detalhes sobre como salvar arquivos de vídeo como evidência e definir o caminho de salvamento, consulte ***Salvar vídeo recortado na***

		reprodução no Evidence Management Center .
	Adicionar Tag	Adicione uma tag personalizada para o arquivo de vídeo para marcar o ponto importante do vídeo. Você também pode editar a tag ou ir para a posição da tag convenientemente.
	Bloquear vídeo	Bloqueie o arquivo de vídeo para evitar sua exclusão e protegê-lo de ser substituído quando o HDD estiver cheio. **Observação** Para a câmera importada do Site Remoto, se os arquivos de vídeo estiverem armazenados no dispositivo de codificação localmente, você não poderá bloquear os arquivos de vídeo.
	Zoom digital	Amplie ou reduza o vídeo para câmeras que não têm seus próprios recursos de zoom óptico. Clique novamente para desabilitar a função. **Observação** No modo de decodificação de software, você também pode capturar a imagem ampliada após habilitar a função de zoom digital.
	Exportar	Exporte os arquivos de vídeo da câmera e salve-os no seu PC ou dispositivo USB conectado. Você também pode salvar o arquivo de vídeo como evidência e definir o caminho de salvamento para os arquivos de vídeo. Para obter detalhes sobre como salvar arquivos de vídeo como evidência e definir o caminho de salvamento, consulte ***Gravação e captura manual*** .
	Expansão Fisheye	Disponível para câmera olho de peixe para entrar no modo de correção de distorção olho de peixe.
	VCA/Pesquisa inteligente	Exiba a janela VCA/Smart Search. Você pode definir uma regra para pesquisar arquivos de vídeo e filtrar os vídeos por tipos de eventos, incluindo VCA/Smart Search, Intrusion Detection e Line Crossing Detection. Consulte ***Search VCA/Smart Event Related Video*** para obter mais detalhes.
	Status da câmera	Exibe o status de gravação da câmera, status do sinal, número de conexão, etc.
	Trocar fluxo	Alterne o fluxo para fluxo principal, fluxo secundário (se suportado) ou fluxo suave (se suportado). Se o dispositivo suportar reprodução com transcodificação, inicie a transcodificação e você precisará definir a resolução, a taxa de

		quadros e a taxa de bits para a transcodificação. **Observação** ● O smooth stream mostrará se o dispositivo suporta. Você pode alternar para smooth stream quando estiver em uma situação de largura de banda baixa para tornar a reprodução mais fluente. ● Somente arquivos de vídeo armazenados em DVR e NVR série I suportam reprodução de transcodificação.
	Exibir na parede	Clique para visualizar a reprodução no smart wall. Veja ***Gerenciar Smart Wall (Dispositivo de decodificação)*** para detalhes.
	Rastreamento visual	Rastreie um indivíduo (como um suspeito) em diferentes áreas sem perder o indivíduo de vista. Consulte *o Manual do Usuário do HikCentral Professional Web Client* e ***o View Visual Tracking Video*** para obter detalhes sobre como definir e executar o rastreamento visual.
	Zoom digital	Crie áreas de zoom na imagem do vídeo para visualizar a reprodução detalhada.
	Pesquisa de imagens	Procure a pessoa alvo pelas fotos capturadas. Veja ***Pesquisar Fotos de Rosto Capturadas por Característica*** para detalhes.
	Melhoria	Ajuste a imagem do vídeo, incluindo brilho, saturação, etc.
	Áudio bidirecional	Inicie o áudio bidirecional com a câmera para obter o áudio em tempo real do dispositivo e realizar uma conversa de voz com a pessoa no dispositivo.
	Girar imagem	Girar uma imagem.
	Pesquisa de Objetos	Selecione uma pessoa na imagem e procure por ela.

Observação

Os ícones exibidos na barra de ferramentas na janela de exibição variam de acordo com os recursos do dispositivo.

6. Clique em **Salvar** para salvar as configurações acima.

6.4 Pesquisa de Vídeo

Os arquivos de vídeo armazenados em dispositivos locais ou no servidor de gravação podem ser

pesquisados.

6.4.1 Pesquisar Arquivo de Vídeo por Tag

Você pode pesquisar filmagens de vídeo por tags. Antes da pesquisa, você pode configurar o período de tempo e especificar a câmera e as tags. Após a pesquisa, você pode exportar os arquivos de vídeo correspondentes para o PC local e salvá-los como evidência no servidor SFTP.

Passos

1. No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Investigação** → **Pesquisa de vídeo** .
2. Clique em **Pesquisar filmagens de vídeo** à esquerda.
3. Defina o período de tempo para pesquisa no campo Tempo.
   – Selecione o período de tempo predefinido na lista suspensa.
   – Selecione **Intervalo de tempo personalizado** para especificar a hora de início e de término da pesquisa.
4. Selecione câmeras.
   1) Clique no painel da câmera.
   2) Selecione um site atual ou um site remoto na lista suspensa de sites para mostrar suas câmeras.
   3) Verifique uma ou várias câmeras.
   4) Clique fora da lista para confirmar a seleção.

Observação

- Até 16 recursos podem ser selecionados para pesquisa ao mesmo tempo.
- O ícone e representam o site atual e o site remoto, respectivamente.

5. **Opcional**: mova o cursor para a câmera selecionada e clique para alternar o tipo de transmissão e o local de armazenamento entre **Transmissão principal/Armazenamento principal** , **Subtransmissão/Armazenamento principal** , **Transmissão principal/Armazenamento auxiliar** ou **Subtransmissão/Armazenamento auxiliar** .

Observação

Você pode mover o cursor para e alternar em lote a condição de pesquisa, incluindo o tipo de fluxo e o local de armazenamento no site atual/remoto. Se o tipo de fluxo configurado ou o local de armazenamento não for suportado, isso não terá efeito.

6. **Opcional**: ative **a Tag** e selecione o(s) tipo(s) de tag conforme necessário.

Observação

- Se você não ativar **a opção Tag** , todas as tags serão pesquisadas.
- Por padrão, você pode selecionar **Person Detected** , **Vehicle Detected** e **None** . Outras tags são exibidas de acordo com a licença do Control Client.

Pessoa Detectada

A tag que é criada quando pessoas são detectadas na filmagem.

Veículo detectado

A tag que é criada quando veículos são detectados na filmagem.

Etiqueta de alarme de evento

A tag que é criada quando um determinado evento acontece.

Observação

Antes de selecionar esse tipo de tag, você deve ter configurado a ação de vinculação para determinados eventos. Para obter detalhes, consulte o *HikCentral Professional Web Client User Manual* .

Tag adicionada manualmente

A tag personalizada que é adicionada durante a reprodução do vídeo.

Trancar

A tag que é criada quando a filmagem é bloqueada.

Outro

Outras tags.

Nenhum

Vídeo sem tags.

7. Clique em **Pesquisar** para encontrar a filmagem relacionada.
   - Clique nas categorias na parte superior para filtrar os resultados. As categorias incluem **Vídeo regular** , **Pessoa detectada** , **Veículo detectado** , **Tag de alarme de evento** , **Tag adicionada manualmente** , **Bloqueio** e **Outros** . Você também pode clicar em **Todos** e selecionar uma categoria.
   - Os resultados da pesquisa podem ser classificados por câmeras ou tempo. Você pode filtrar os resultados da pesquisa por câmeras específicas. Você também pode clicar em ou para alternar entre o modo de lista e o modo de miniatura.
8. **Opcional**: visualize estatísticas de resultados na barra da linha do tempo.

Figura 6-2 Barra da linha do tempo

Observação

- Mova o cursor sobre a linha do tempo para ter uma visão rápida das informações do vídeo e clique nas informações exibidas para reproduzir o vídeo específico.

- Clique em / para pular para frente ou para trás para limitar a posição usando a busca de meio intervalo, reduzindo pela metade o tempo de pulo a cada mudança de direção.

9. **Opcional**: segmente a filmagem de vídeo correspondente de uma câmera específica se a filmagem ainda for muito longa para localizar as informações do vídeo de destino.
   1) Clique para exibir a filmagem correspondente no modo miniatura e, em seguida, passe o cursor sobre a miniatura e clique em → **Segmentação de vídeo** para mostrar a janela Segmentação de vídeo.
   2) Passe o cursor sobre **Segmentação de vídeo** .

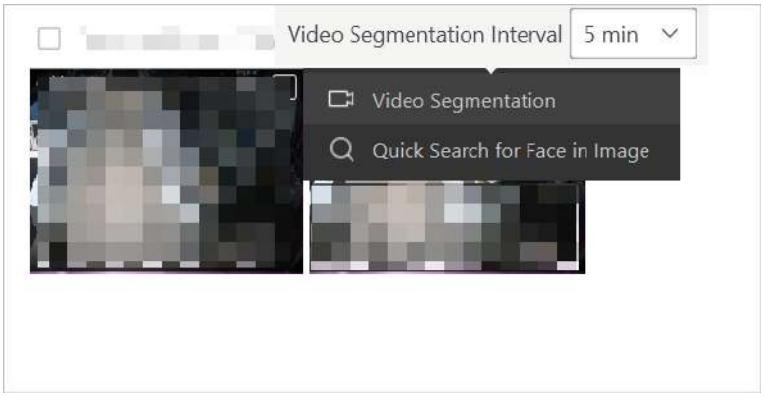


Figura 6-3 Segmento de vídeo correspondente de uma câmera específica

   3) Defina o intervalo da filmagem e clique em **Segmentação de vídeo** para segmentar a filmagem.
10. **Opcional**: Busca rápida por rosto na filmagem.
   1) Clique para exibir a filmagem correspondente no modo miniatura.
   2) Passe o cursor sobre uma miniatura e clique em → **Busca rápida por rosto na imagem** para abrir a página de busca de pessoas.
11. **Opcional**: clique em um vídeo pesquisado específico para iniciar a reprodução remota e executar mais operações.

Ver detalhes na janela auxiliar	Clique no canto superior direito para exibir a página atual em uma janela auxiliar.
Posicione o segmento de vídeo	Arraste a linha do tempo para frente ou para trás para posicionar o segmento de vídeo desejado.
Reprodução normal/reversa	Clique em / para executar a reprodução normal/reversa.
Reprodução normal/reversa de quadro único	Clique em / para executar a reprodução normal/reversa de quadro único.
Reprodução lenta/rápida	Clique / para executar a reprodução lenta/rápida.
Ir para Monitoramento	Clique em **Ir para monitoramento** para abrir a página de monitoramento.
Ícones de reprodução	Para obter detalhes sobre os outros ícones na janela de reprodução,

	consulte ***Personalizar ícones na janela de reprodução*** .
Ver localização	Clique na aba **Localização** para visualizar a localização GPS (incluindo latitude e longitude) da câmera corporal na filmagem de vídeo pesquisada e visualizar os rastros da câmera corporal no mapa GIS.

12. **Opcional**: exporte a filmagem correspondente para o armazenamento local.
   – Durante a reprodução, clique na barra de ferramentas para exportar a filmagem atual.
   – Selecione a filmagem e clique em **Exportar** para exportar todas as filmagens selecionadas.

6.4.2 Pesquisar Captura Programada

Você pode pesquisar registros de captura de acordo com nomes de agendamento e câmeras. Você também pode visualizar os arquivos de vídeo relacionados aos resultados da pesquisa, enviar registros por e-mail para um destinatário específico e exportar as imagens capturadas e os arquivos de vídeo relacionados como evidência.

Passos

1. No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Investigação** → **Pesquisa de vídeo** .
2. Clique em **Pesquisa de captura programada** à esquerda.
3. Selecione a programação de captura na lista.

Observação

- Para obter detalhes sobre o cronograma de captura, consulte o *Manual do usuário do HikCentral Professional Web Client* .
- Você pode inserir palavras-chave para pesquisar programações de captura específicas.

4. Selecione a(s) câmera(s).
5. Defina o período de tempo para pesquisa no campo Tempo.
   – Selecione o período de tempo predefinido na lista suspensa.
   – Selecione **Intervalo de tempo personalizado** para especificar a hora de início e de término da pesquisa.
6. Clique em **Pesquisar** para encontrar as imagens de captura agendadas.

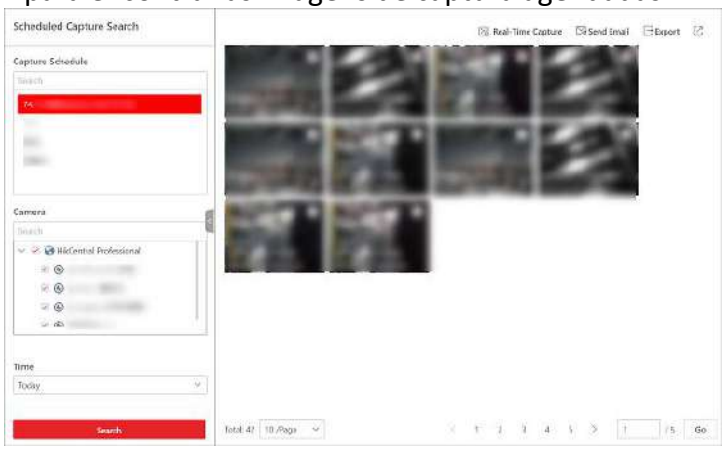


Figura 6-4 Pesquisa de captura programada

Os resultados da pesquisa podem ser classificados por câmeras ou tempo. Você pode clicar em ou para alternar entre o modo de lista e o modo de miniatura.

7. Opcional: clique em um resultado de pesquisa para visualizar seus detalhes (como nome da câmera e hora da captura) e realizar mais operações.

Baixar imagem/vídeo capturado	Clique **em Download** para baixar a imagem/vídeo capturado.
Ver pesquisa agendada anterior/seguinte	Clique em / para reproduzir o resultado da pesquisa anterior/seguinte.
Ver imagem capturada	Clique para ver a imagem capturada.
Ver vídeo capturado	Clique para ver o vídeo capturado.

Observação

Na janela de reprodução do vídeo capturado, você pode executar as seguintes operações.

- Arraste a linha do tempo para frente ou para trás para posicionar o segmento de vídeo desejado.
- Clique em / para executar a reprodução normal/reversa.
- Clique em / para executar a reprodução normal/reversa de quadro único.
- Clique / para executar a reprodução lenta/rápida.
- Clique em / para aumentar/diminuir o zoom na barra da linha do tempo.
- Clique para definir a janela de reprodução em tela cheia. Pressione Esc no teclado para sair do modo de tela cheia.
- Para obter detalhes sobre os outros ícones na janela de reprodução, consulte ***Personalizar ícones na janela de reprodução*** .

8. **Opcional**: clique em **Captura em tempo real** no canto superior direito para capturar imagens dos recursos selecionados em tempo real.
9. **Opcional**: envie um e-mail dos registros de captura agendados para um destinatário específico.
   1) Selecione um ou mais resultados de captura de programação.
   2) Clique em **Enviar e-mail** no canto superior direito.
   3) Selecione o modelo de e-mail.

Observação

Para obter detalhes sobre como definir o modelo de e-mail, consulte o *Manual do usuário do HikCentral Professional Web Client* .

   4) Informe o motivo ou problema do(s) registro(s) a ser(em) enviado(s).
   5) Clique **em OK** .
10. **Opcional**: Exportar registro(s) de captura de programação.
    1) Selecione um ou mais resultados de captura de programação.

2) Clique em **Exportar** no canto superior direito.
3) Selecione o conteúdo de exportação.
4) Selecione o formato do arquivo como Excel ou CSV.
5) Clique **em OK** .

Observação

- Até 500 registros podem ser exportados por vez.
- Você pode visualizar o progresso da tarefa de exportação no Task Center. Para obter detalhes, consulte ***Gerenciar tarefas de download/upload*** .

11. Opcional: clique em no canto superior direito para exibir a página atual em uma tela auxiliar.

6.4.3 Pesquisar Fotografia com Lapso de Tempo

Fotografia de lapso de tempo é uma técnica que pode combinar uma grande quantidade de capturas programadas feitas em um período específico para um vídeo na duração desejada. Por exemplo, 600 fotos podem ser capturadas em 2 semanas, mas elas podem ser geradas (em sequência) para um vídeo de 2 minutos por meio de fotografia de lapso de tempo. Você pode procurar por fotografia de lapso de tempo gerada de fonte, tempo e duração específicos e baixá-las para seu PC local.

Passos

1. No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Investigação** → **Pesquisa de vídeo** .
2. Clique em **Fotografia com lapso de tempo** à esquerda.
3. Selecione a fonte do material.
   – **Cronograma de Captura** : Gere fotografia de lapso de tempo por meio de capturas programadas. Você pode selecionar e pesquisar cronogramas capturados e câmeras correspondentes.

Dispositivo local : Gere fotografia de lapso de tempo por imagens capturadas carregadas do dispositivo local. Você pode selecionar e pesquisar por câmeras correspondentes.

4. Defina **o Tempo total de pesquisa de material** para especificar o período de pesquisa de materiais.
5. Defina **o tempo de busca de material para um dia** para especificar o período de busca de materiais para um dia.
6. Defina **a duração do vídeo com lapso de tempo** para especificar a duração do vídeo (unidade: seg).
7. Clique em **Pesquisar** .

Observação

Se as imagens pesquisadas para gerar a fotografia de lapso de tempo não forem suficientes, a pesquisa falhará.

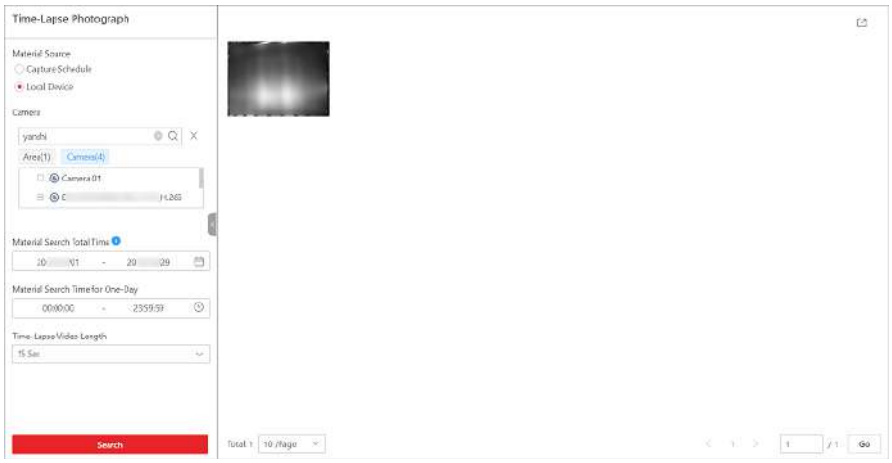


Figura 6-5 Pesquisa de fotografia com lapso de tempo

8. Opcional: mova o cursor sobre uma fotografia de lapso de tempo específica e clique em **Baixar** para baixar a fotografia de lapso de tempo no formato MP4 para o PC local.
   Você pode encontrar o progresso do download da tarefa no Task Center. Para detalhes, consulte ***Gerenciar tarefas de download/upload*** .
9. Opcional: clique em no canto superior direito para exibir a página atual em uma tela auxiliar.

6.4.4 Pesquisar Vídeo Acionado por Evento de Transação

Você pode pesquisar a filmagem de vídeo acionada pelo evento de transação que contém informações de POS. Após a pesquisa, você pode exportar a filmagem de vídeo correspondente para o PC local ou salvá-la como evidência.

Passos

1. No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Investigação** → **Pesquisa de vídeo** .
2. Clique em **Pesquisa de vídeo do dispositivo** à esquerda.
3. Selecione **Evento de transação** como o tipo de pesquisa.
4. Defina o período de tempo para pesquisa no campo Tempo.
   – Selecione o período de tempo predefinido na lista suspensa.
   – Selecione **Intervalo de tempo personalizado** para especificar a hora de início e de término da pesquisa.
5. Insira as palavras-chave contidas nas informações do PDV.

Observação

- Você pode inserir até três palavras-chave e deve separar cada uma delas com uma vírgula.
- Se você inserir mais de uma palavra-chave para pesquisa, poderá selecionar | pesquisar as informações do PDV que contêm qualquer uma das palavras-chave ou selecionar & pesquisar as informações do PDV que contêm todas as palavras-chave.

6. **Opcional**: Selecione **Diferenciar maiúsculas de minúsculas** para pesquisar as informações do PDV com diferenciação entre maiúsculas e minúsculas.

7. Selecione o dispositivo e a câmera no campo Câmera para pesquisar as informações da transação.
8. **Opcional**: Selecione uma câmera, mova o cursor e clique nela para alternar o tipo de transmissão e o local de armazenamento entre **Transmissão principal/Armazenamento principal** , **Subtransmissão/Armazenamento principal** , **Transmissão principal/Armazenamento auxiliar** ou **Subtransmissão/Armazenamento auxiliar** .

Observação

Você pode mover o cursor para e alternar em lote a condição de pesquisa, incluindo o tipo de fluxo e o local de armazenamento no site atual/remoto. Se o tipo de fluxo configurado ou o local de armazenamento não for suportado, isso não terá efeito.

9. Clique em **Pesquisar** para encontrar a filmagem relacionada.
10. Você pode executar as seguintes operações.

Mudar para o modo de lista/miniatura	Clique em ou para alternar entre o modo de lista e o modo de miniatura.
Abrir janela auxiliar	Clique no canto superior direito para exibir a página atual em uma janela auxiliar.
Iniciar reprodução	● No modo de lista, clique no item na coluna Time Range. No modo de miniatura, clique na imagem do resultado pesquisado. ● Clique em / para reproduzir o vídeo anterior ou seguinte. ● Ative **Reproduzir em ordem** para reproduzir automaticamente o próximo vídeo.
Busca de meio intervalo	Clique em / para pular para frente ou para trás para limitar a posição usando a busca de meio intervalo, reduzindo pela metade o tempo de pulo a cada mudança de direção.
Exportar vídeo	Clique para exportar a filmagem atual ou selecione a filmagem e clique em **Exportar** para exportar todas as filmagem selecionadas.

6.4.5 Pesquisar Filmagens de Vídeo Acionadas por Eventos ATM

Você pode pesquisar as filmagens de vídeo acionadas por eventos ATM, como transações e outras operações no ATM. Após a pesquisa, você pode salvar as filmagens de vídeo correspondentes no PC local e salvá-las como evidência no servidor SFTP.

Passos

1. No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Investigação** → **Pesquisa de vídeo** .
2. Clique em **Pesquisa de vídeo do dispositivo** à esquerda.
3. Selecione o tipo de pesquisa como **Evento ATM** .
4. Defina o período de tempo para pesquisa no campo Tempo.

- Selecione o período de tempo predefinido na lista suspensa.
- Selecione **Intervalo de tempo personalizado** para especificar a hora de início e de término da pesquisa.

5. Digite o número do cartão que está contido nas informações do caixa eletrônico.
6. Selecione o dispositivo e a câmera para pesquisar as informações do caixa eletrônico no campo Câmera.
7. Opcional: Selecione uma câmera, mova o cursor e clique nela para alternar o tipo de transmissão e o local de armazenamento entre **Transmissão principal/Armazenamento principal** , **Subtransmissão/Armazenamento principal** , **Transmissão principal/Armazenamento auxiliar** ou **Subtransmissão/Armazenamento auxiliar** .

Observação

Você pode mover o cursor para e alternar em lote a condição de pesquisa, incluindo o tipo de fluxo e o local de armazenamento no site atual/remoto. Se o tipo de fluxo configurado ou o local de armazenamento não for suportado, isso não terá efeito.

8. Clique em **Pesquisar** .
   Os resultados da pesquisa podem ser classificados por câmeras ou tempo. Você pode clicar em ou para exibir os resultados da pesquisa em modo de lista e modo de miniatura.
9. Opcional: clique em um vídeo pesquisado específico para iniciar a reprodução remota e executar mais operações.

Ver detalhes na janela auxiliar	Clique no canto superior direito para exibir a página atual em uma janela auxiliar.
Posicione o segmento de vídeo	Arraste a linha do tempo para frente ou para trás para posicionar o segmento de vídeo de interesse.
Reprodução normal/reversa	Clique em / para executar a reprodução normal/reversa.
Reprodução normal/reversa de quadro único	Clique em / para executar a reprodução normal/reversa de quadro único.
Reprodução lenta/rápida	Clique / para executar a reprodução lenta/rápida.
Ampliando/reduzindo a barra da linha do tempo	Clique em / para aumentar/diminuir o zoom na barra da linha do tempo.
Ir para Monitoramento	Clique em **Ir para Monitoramento** para abrir a página Monitoramento. Para detalhes, consulte ***Live View*** .
Ícones de reprodução	Para obter detalhes sobre os outros ícones na janela de reprodução, consulte ***Personalizar ícones na janela de reprodução*** .

Observação

- Consulte ***Reprodução*** para obter mais detalhes sobre reprodução.
- Na barra de ferramentas de reprodução, clique para entrar no modo de rastreamento

visual. Para obter detalhes, consulte ***Exibir vídeo de rastreamento visual*** .

10. **Opcional**: Baixe a filmagem correspondente para o armazenamento local.
    - Durante a reprodução, clique para baixar a filmagem atual.
    - Selecione a filmagem e clique em **Exportar** para exportar todas as filmagens selecionadas.

6.4.6 Pesquisar VCA/Vídeo Relacionado a Eventos Inteligentes

Você pode pesquisar arquivos de vídeo onde eventos VCA/smart ocorrem. E você pode reproduzir ou baixar os arquivos de vídeo encontrados. Os eventos VCA/smart incluem detecção de movimento e cruzamento de linha.

Passos

Observação

- Esta função deve ser suportada pelo dispositivo.
- Arquivos de vídeo armazenados em uma Rede de Área de Armazenamento Híbrida não suportam VCA/pesquisa de eventos inteligentes.

1. Acesse a página de Pesquisa VCA / Pesquisa Inteligente e três maneiras são selecionáveis.

Acesso pela página Live View	1. Entre na página Live View e inicie a visualização ao vivo da câmera (consulte ***Live View***). 2. Mova o cursor para a janela de exibição e clique para abrir a página de Pesquisa VCA / Pesquisa Inteligente.
Acesso pela página de reprodução	1. Entre na página de reprodução e inicie a reprodução da câmera (consulte ***Reprodução***). 2. Mova o cursor para a janela de exibição e clique para abrir a página de Pesquisa VCA / Pesquisa Inteligente.
Acesso a partir da página de pesquisa VCA / pesquisa inteligente	No canto superior esquerdo do Control Client, selecione → **Investigação** → **Pesquisa de vídeo** → **Pesquisa VCA / Pesquisa inteligente** .

2. Defina o período de tempo para pesquisa no campo Tempo.
    - Selecione o período de tempo predefinido na lista suspensa.
    - Selecione **Intervalo de tempo personalizado** para especificar a hora de início e de término da pesquisa.
3. Selecione a câmera para pesquisar o vídeo onde o evento VCA/inteligente ocorre.

Observação

Execute esta etapa ao acessar a página Pesquisa VCA / Pesquisa Inteligente no módulo Pesquisa de Vídeo.

4. Selecione o tipo de evento e desenhe a região ou linha de detecção para pesquisa.

- **Movimento:** arraste o cursor na imagem de vídeo para definir o retângulo da grade como a região de detecção para pesquisar as imagens de vídeo dos eventos de detecção de movimento que ocorreram na região.
- **Detecção de cruzamento de linha:** arraste o cursor na imagem de vídeo para definir a linha de detecção para pesquisar as imagens de vídeo dos eventos de cruzamento de linha que ocorreram na linha.

5. **Opcional**: clique para excluir a região ou linha desenhada.
6. Clique em **Pesquisar** para encontrar a filmagem relacionada.
   Os resultados da pesquisa podem ser classificados por câmeras ou tempo. Você pode clicar em ou para alternar entre o modo de lista e o modo de miniatura. Além disso, você pode filtrar a filmagem selecionando **Vídeo regular** , **Pessoa detectada** ou **Veículo detectado** .
7. **Opcional**: inicie a reprodução remota do vídeo pesquisado.
   - Para o modo de lista, clique no item na coluna Intervalo de tempo.
   - Para o modo miniatura, clique na imagem do resultado pesquisado.

   Reproduza o vídeo anterior entre os resultados pesquisados.

   Reproduza o próximo vídeo entre os resultados pesquisados.

   Tocar em ordem

   Depois de reproduzir o vídeo atual, continue reproduzindo o próximo automaticamente.

Observação

- Consulte ***Reprodução*** para obter mais detalhes sobre reprodução.
- Na barra de ferramentas de reprodução, clique para entrar no modo de rastreamento visual. Para obter detalhes, consulte ***Exibir vídeo de rastreamento visual*** .

8. **Opcional**: Baixe a filmagem pesquisada para o armazenamento local.
   - Durante a reprodução, clique para exportar a filmagem atual.
   - Selecione a filmagem e clique em **Exportar** para exportar todas as filmagens selecionadas.
9. **Opcional**: Execute mais operações.

Pesquisa rápida por rosto em imagem	Mova o cursor sobre uma imagem específica e clique em → **Busca rápida por rosto na imagem** para procurar os registros de rosto desejados.
Ver estatísticas de resultados	Mova o cursor sobre a linha do tempo para ter uma visão rápida das informações do vídeo e clique nas informações exibidas para reproduzir o vídeo específico.
Barra de linha do tempo com zoom in/out	Clique em / para aumentar/diminuir o zoom na barra da linha do tempo.
Abrir tela auxiliar	Clique no canto superior direito para exibir a página atual em uma tela auxiliar.

Capítulo 7 Personalizar o Conteúdo do Monitoramento Inteligente

O Intelligent Monitoring exibe as imagens capturadas em tempo real (de rostos, corpos humanos e veículos) e os eventos em tempo real acionados por veículos e pessoas. Você pode personalizar o conteúdo a ser exibido nesta página.

Antes de começar

Certifique-se de ter adicionado câmeras inteligentes e servidores de análise inteligentes ao Web Client. Para obter detalhes, consulte o *Manual do Usuário do HikCentral Professional Web Client* .

Passos

1. No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Monitoramento** → **Monitoramento inteligente** para entrar na página Monitoramento inteligente.
2. Clique em **Definir** no canto superior direito para mostrar o Painel de Configurações.
3. Clique em **Configurações de exibição** e configure os parâmetros relacionados.

Objeto Capturado

Selecione **Rosto** e/ou **Humano** e/ou **Veículo** como objeto(s) capturado(s).

Configurações do evento

Eventos desencadeados por pessoas

Ative **Eventos acionados por pessoas** e selecione os tipos de eventos, como **Rosto capturado** e **Rosto correspondente** .

Observação

Ao selecionar **Matched Face** como o tipo de evento, você deve selecionar uma ou mais bibliotecas de imagens faciais da lista abaixo. Para obter detalhes sobre como adicionar bibliotecas de imagens faciais, consulte o *Manual do Usuário do HikCentral Professional Web Client* .

Eventos acionados por veículos

Ative **Eventos acionados por veículos** e selecione os tipos de eventos, incluindo **Veículo compatível** e **Veículo incompatível** .

Observação

Ao selecionar **Vehicle Matched** como o tipo de evento, você deve selecionar uma ou mais listas de veículos. Para obter detalhes sobre como adicionar listas de veículos, consulte o *Manual do Usuário do HikCentral Professional Web Client* .

Janela pop-up

Ative **a Janela pop-up** e selecione a(s) condição(ões) necessária(s) para habilitar notificações pop-up. Por exemplo, se você marcar **Temperatura anormal** , uma janela aparecerá no meio da página Monitoramento inteligente quando o dispositivo detectar uma pessoa com temperatura anormal.

4. Clique em **Exibição de recursos** e configure os parâmetros relacionados.

Características da pessoa

Selecione quais características da pessoa serão exibidas nos detalhes da captura. Você pode selecionar até 6 características (incluindo características de rosto humano e corpo humano).

Características do veículo

Selecione quais características do veículo serão exibidas nos detalhes de captura. Você pode selecionar até 3 características.

5. **Opcional**: clique em **Área de monitoramento** → e selecione a(s) câmera(s) específica(s) na lista para visualizar as imagens e eventos capturados da(s) câmera(s) selecionada(s).

Observação

- Por padrão, todos os recursos são selecionados.
- Você também pode visualizar a visualização ao vivo da(s) câmera(s) correspondente(s) na **Visualização ao vivo** .

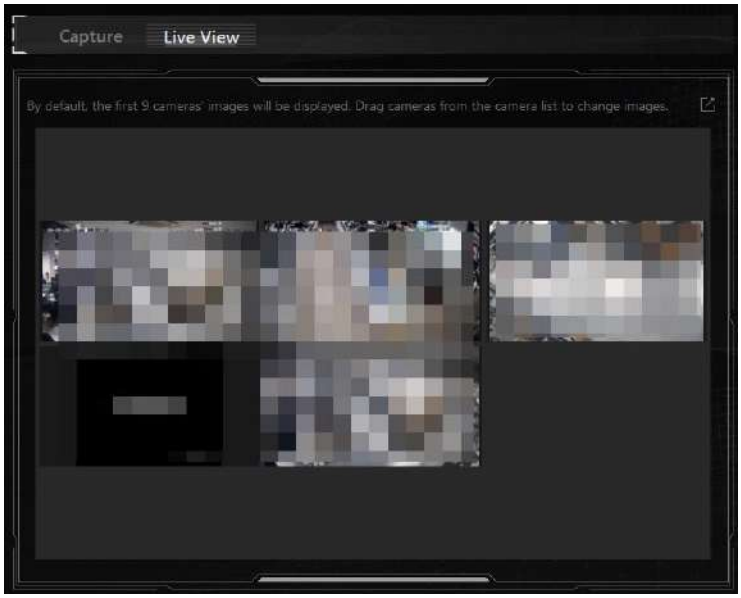


Figura 7-1 Visualização ao vivo

6. Clique em **Salvar** para salvar as configurações acima.
Você pode visualizar as estatísticas de hoje em tempo real na parte superior da página, visualizar as imagens capturadas em tempo real de pessoas e veículos (se configurado) no lado esquerdo da página e visualizar os eventos acionados por pessoas e veículos (se configurado) no lado direito da página.

Observação

A regra de contagem das Estatísticas de Hoje é a seguinte: Uma vez que haja um rosto, um corpo humano ou um veículo capturado pelas câmeras, o número de rostos, corpos humanos e veículos adiciona 1 na plataforma. O mesmo se aplica aos quatro tipos de eventos (Face Match Event, License Plate Matched, Frequently Appeared Persons e Intelligent Cameras). Uma vez que um determinado evento é acionado, seu número adiciona 1 na plataforma.

7. **Opcional**: clique na imagem capturada de uma pessoa ou veículo para visualizar seus detalhes (como nome da câmera e hora da captura) e realizar mais operações.

Tabela 7-1 Detalhes da pessoa

Operação	Função
Adicionar pessoa	Adicione a pessoa à lista de pessoas. Para obter detalhes, consulte ***Adicionar pessoa incompatível ao grupo de pessoas*** .
Pesquisa de imagens	Procure a pessoa nas fotos capturadas. Para detalhes, consulte ***Search Face Pictures by Picture*** .
Capturas relacionadas	Pesquise as capturas e vídeos relacionados. Para detalhes, consulte ***Pesquisar Imagens de Rosto Capturadas por Recurso*** .
Mais → Pesquisa de arquivo	Pesquise o arquivo da foto do rosto atual. Para detalhes, consulte ***Pesquisar Arquivos*** .
Mais → Verificação de identidade → A ser verificado	Verifique a identidade da pessoa. Para detalhes, consulte ***Identity Search*** .
Mais → Verificação de identidade → Alvo	Defina a pessoa como um alvo de comparação. Para detalhes, consulte ***Identity Search*** .
Mais → Baixar	Baixe as fotos e vídeos. Para detalhes, consulte ***Gerenciar tarefas de download/upload*** .

Tabela 7-2 Detalhes do veículo

Operação	Função
Recuperação de Placas de Veículos	Pesquise registros de passagem de veículos por meio do número da placa. Para obter detalhes, consulte ***Search for Passing Vehicles Detected by Cameras and UVSSs (Pesquisar veículos que passam detectados por câmeras e UVSSs)*** .
Download	Baixe as fotos e vídeos. Para detalhes, consulte ***Gerenciar tarefas de download/upload*** .

8. Opcional: clique em um evento acionado por pessoas ou veículos para visualizar seus detalhes (como câmera e hora de captura) e realizar mais operações.

Observação

Consulte a etapa anterior para obter detalhes.

9. **Opcional**: Clique para entrar no módulo de parede inteligente e exibir o conteúdo atual na parede inteligente.

Observação

Para obter detalhes, consulte ***Exibir todo o conteúdo na visualização ao vivo no Smart Wall*** .

10. **Opcional**: clique em no canto superior direito para visualizar as imagens e eventos capturados em tempo real em uma tela auxiliar.

Capítulo 8 Verificar Evento e Alarme

As informações de evento e alarme (por exemplo, informações de alarme de detecção de movimento) recebidas pelo Control Client são exibidas. Você pode verificar as informações detalhadas do evento e alarme, visualizar o vídeo vinculado, gerenciar as informações relacionadas e assim por diante.

Observação

Você deve configurar eventos e alarmes por meio do Web Client antes de poder verificar as informações relacionadas e ações de vinculação por meio do Control Client. Para obter detalhes, consulte o *Manual do Usuário do HikCentral Professional Web Client* .

8.1 Exibir Alarmes em Tempo Real dos Recursos

O módulo Alarm Center exibirá as informações de alarme em tempo real dos recursos gerenciados, como detecção de movimento, perda de vídeo e alarme de violação de vídeo. Você pode verificar os detalhes do alarme e visualizar vídeos e imagens relacionados ao alarme, se configurado.

Observação

Antes de receber alarmes de dispositivos no Control Client, você deve armar os dispositivos. Para obter detalhes, consulte ***Perform Arming Control for Alarms***

No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Monitoramento** → **Central de alarmes** .

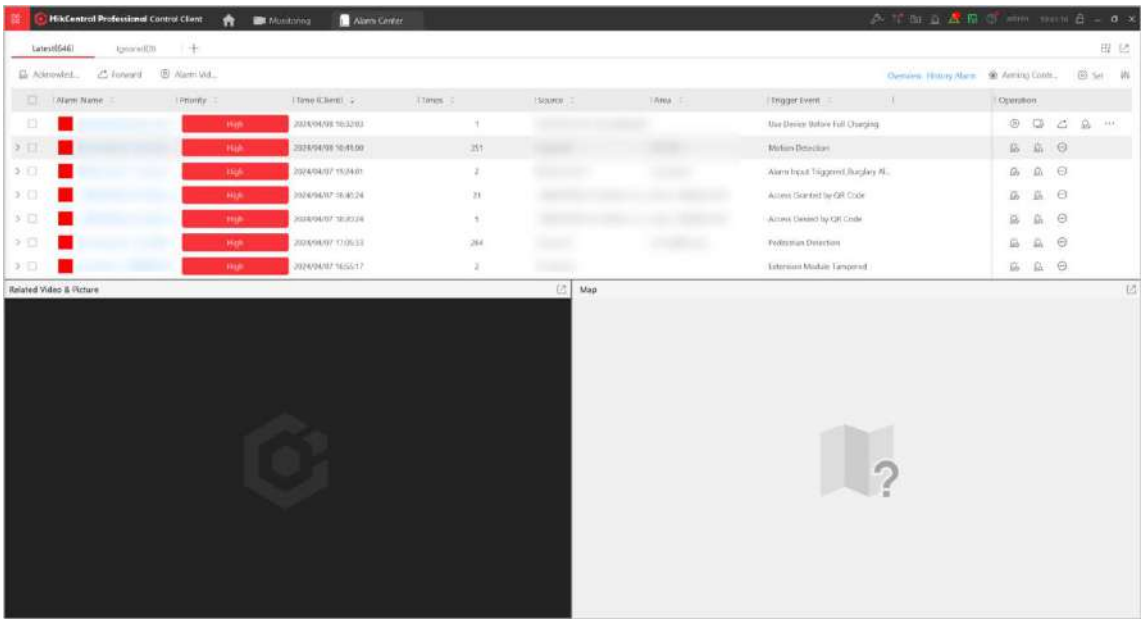


Figura 8-1 Central de alarmes

Clique **em Últimos** ou **Ignorados** para visualizar os últimos alarmes recebidos ou alarmes que não podem ser recebidos pelo Control Client atual.

Clique + para personalizar o filtro (área do site, evento de disparo, status do alarme, etc.) e clique em **Salvar** para salvar o filtro.

Se você tiver habilitado o **Acknowledging Time Limitation** no Web Client, clique em **Timed Out** para visualizar alarmes não reconhecidos após o período de tempo limite configurado. Consulte *o HikCentral Professional Web Client User Manual* para obter detalhes.

Observação

A seleção do site só está disponível para o Sistema Central com o módulo Gerenciamento Remoto do Site.

Tabela 8-1 Operações no Alarm Center

Operação	Descrição
Personalizar colunas exibidas da lista de alarmes	1. Clique para abrir o painel Personalizar nome da coluna. 2. Verifique o(s) nome(s) da(s) coluna(s) a ser(em) exibida(s). **Observação** O **nome do alarme** é exibido por padrão e você não pode desmarcá-lo. 3. Clique em **OK** para salvar as configurações.
Definir parâmetros básicos de alarme	Clique **em Definir** para definir parâmetros básicos de alarme.
Marcar alarme	Clique para marcar alarmes se alguns alarmes forem

Operação	Descrição
	importantes ou precisarem de operações adicionais.
Ver detalhes do alarme	Visualize os detalhes do alarme na tabela da página Central de Alarmes ou clique no nome de um alarme para visualizar os detalhes de um alarme especificado (consulte ***Exibir janela pop-up acionada pelo alarme*** para obter detalhes). **Prioridade de alarme** A prioridade do alarme de acordo com as configurações de prioridade ao adicionar o alarme no Web Client. **Tempo (Cliente)** O horário do Control Client quando o alarme é iniciado. **Horários de alarme** Mostra quantas vezes o alarme foi disparado. **Fonte** O recurso onde o alarme ocorre. **Evento de disparo** Exibe o tipo de evento que disparou o alarme. **Status do alarme** O status atual do alarme, incluindo parado, iniciado e anormal.

Operações de um alarme	**Ir para a página de pesquisa de alarmes** : clique na coluna Operação para ir para a página de pesquisa de eventos e alarmes para pesquisar o alarme atual definindo condições.
	Conteúdo relacionado : Clique na coluna Operação para iniciar a visualização ao vivo ou a reprodução das câmeras relacionadas ao alarme e visualizar as imagens capturadas. Durante a visualização ao vivo, você pode clicar para entrar no modo de rastreamento visual da câmera. Consulte *o Manual do usuário do HikCentral Professional Web Client* para obter detalhes sobre a configuração do rastreamento visual.
	Áudio bidirecional : clique na coluna Operação para iniciar o áudio bidirecional com a fonte de alarme do site atual ou de sites remotos.
	Exibir no Smart Wall : Clique na coluna Operação para exibir o vídeo do alarme no Smart Wall.

	Ignorar : clique na coluna Operação para ignorar o alarme selecionado, para que o Cliente de Controle atual não receba este alarme durante o período de ignorância, mesmo que ele seja acionado. **Aceitar** : Clique na coluna Operação para aceitar o alarme, para que o Cliente de Controle atual possa receber este alarme quando ele for acionado.
	Desabilitar : Clique na coluna Operação para desabilitar o alarme selecionado, para que a plataforma não possa receber e registrar esse alarme durante a duração da desabilitação, mesmo que ele seja acionado. Ao definir os parâmetros de desabilitação, você pode marcar **Desabilitar Alarme do Dispositivo** para alterar o status do alarme do(s) dispositivo(s) exibido(s) na lista de alarmes. **Habilitar** : Clique na coluna Operação para habilitar o alarme, para que a plataforma possa receber este alarme e você possa visualizar as informações do alarme em qualquer cliente.
	Exportar : Clique na coluna Operação para baixar os detalhes do alarme, incluindo informações do alarme, imagem do alarme, vídeo vinculado, mapa vinculado, etc.
	Avançar : Clique na coluna Operação para encaminhar um alarme para outros usuários para confirmação. Marque vários alarmes e clique **em Encaminhar** para encaminhá-los a outros usuários para confirmação.
	Salvar como evidência : clique na coluna Operação de um evento ou alarme selecionado para abrir o painel Salvar como evidência. ● **Adicionar à evidência existente** : insira o nome, a etiqueta, a ID ou a descrição da evidência existente para vincular o arquivo de log de eventos e alarmes à evidência. ● **Criar Evidência** : Defina os parâmetros necessários para criar a nova evidência para vinculação com o arquivo de log de eventos e alarmes. Para saber como criar evidências, consulte ***Adicionar um Caso*** . ● **Only Upload File** : Carregue o arquivo de log de eventos e alarmes do armazenamento local para o pool de recursos. Você pode verificar o progresso do upload no Task Center (veja ***Manage Downloading/Uploading Tasks*** para

	detalhes). **Observação** ● A operação disponível muda de acordo com a ligação de alarme da fonte. Para configuração detalhada, consulte o *Manual do Usuário do HikCentral Professional Web Client* . ● Você pode ir para **Sistema** → **Central de Alarmes** → **Lista de Alarmes** para personalizar os ícones exibidos na coluna Operação.
Classificar alarmes	Clique no nome da coluna da lista de alarmes e selecione uma propriedade para classificar os alarmes pela propriedade selecionada.
Ver vídeo e mapa relacionados ao alarme	Selecione um alarme, o vídeo ou imagem relacionada ao alarme (se houver) será exibido, e o mapa relacionado à fonte do alarme (se houver) também aparecerá nas janelas abaixo. Na janela Vídeo e imagem relacionados, você pode clicar em **Exibir vídeo** ou **imagem** no canto superior direito da janela para alternar o conteúdo de exibição. **Observação** Ao reproduzir os vídeos de alarme gravados na janela Vídeo e Imagem Relacionados, você pode clicar na barra de tempo para reproduzir arquivos de vídeo armazenados no armazenamento principal ou auxiliar.
Reconhecer um alarme	Clique no nome de um alarme para abrir a janela de detalhes do alarme, defina parâmetros (por exemplo, prioridade do alarme, categoria do alarme e observação) e clique em **Reconhecer** para reconhecer o alarme.
Alarmes de reconhecimento em lote	1. Verifique os alarmes na lista de alarmes e clique em **Reconhecer** para abrir a janela Reconhecimento em lote. 2. (Opcional) Defina a prioridade do alarme e a categoria do alarme. 3. (Opcional) Insira uma observação sobre o reconhecimento do alarme. 4. Clique **em OK** . **Observação** Até 100 alarmes podem ser reconhecidos por vez.

Controle de Armar	Clique em **Controle de Armar** no canto superior direito da Central de Alarmes para aceitar/ignorar ou habilitar/desabilitar as regras de alarme configuradas dos recursos selecionados, armar ou desarmar as partições (áreas) dos dispositivos de controle de segurança e radares, e ignorar ou recuperar o desvio para as entradas de alarme (zonas) nas partições (áreas).
Exibir central de alarmes na parede inteligente	Clique no canto superior direito para entrar no módulo Smart Wall e exibir a página da Central de Alarmes na parede inteligente.
Entrar na página de visão geral de eventos e alarmes	Clique em **Visão geral** no canto superior direito da página Central de alarmes para entrar na página Visão geral de alarmes para visualizar o relatório de análise de alarmes, os 5 principais alarmes e as 5 principais zonas de aviso. Consulte ***Visão geral de eventos e alarmes*** para obter detalhes.
Exibir histórico de alarme	Clique em **History Alarm** para entrar no módulo Alarm & Event Search para pesquisar os alarmes do histórico. Veja ***Search for Event and Alarm Logs*** para detalhes.
Visualizar e manipular alarmes relacionados a áreas	Você pode verificar e gerenciar alarmes relacionados a áreas.

8.2 Definir Parâmetros do Centro de Alarme

Vá para **Central de alarmes** → **Definir** para configurar os seguintes parâmetros para a central de alarmes.

- ***Definir parâmetros básicos***
- ***Definir parâmetros de conteúdo relacionado***
- ***Definir som de alarme***
- ***Personalize os ícones no Alarm Center***

Definir Parâmetros Básicos

Você pode definir a posição da janela pop-up do alarme, o modo de exibição da lista de alarmes (alarmes com o mesmo nome podem ser agregados ou alarmes podem ser agrupados por hora), se deseja habilitar o áudio do alarme e a janela pop-up.

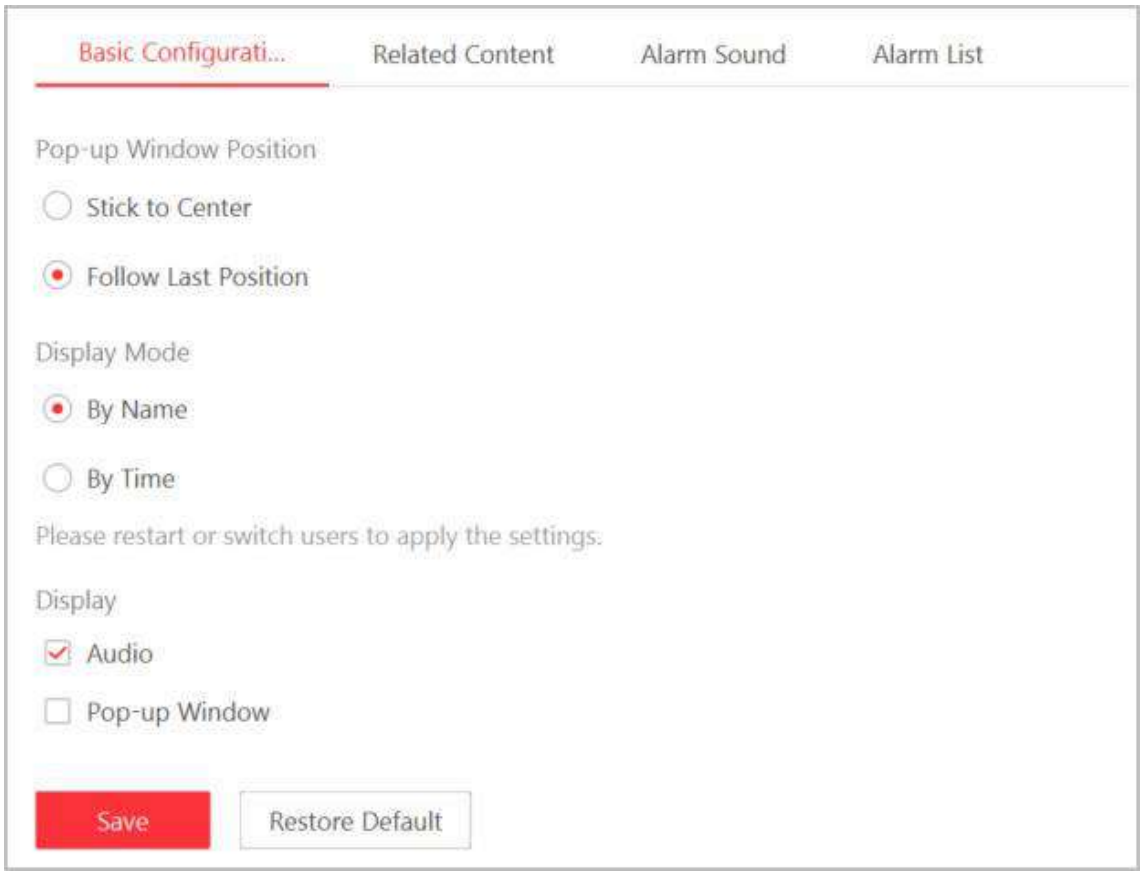


Figura 8-2 Configuração básica do Alarm Center

Definir Parâmetros de Conteúdo Relacionado

Você pode personalizar o conteúdo relacionado exibido na Central de Alarmes definindo os parâmetros, incluindo se deseja exibir o vídeo, a imagem ou o mapa relacionado, qual tipo de conteúdo será exibido com prioridade na janela de vídeo e o tipo de transmissão padrão para visualização ao vivo e reprodução.

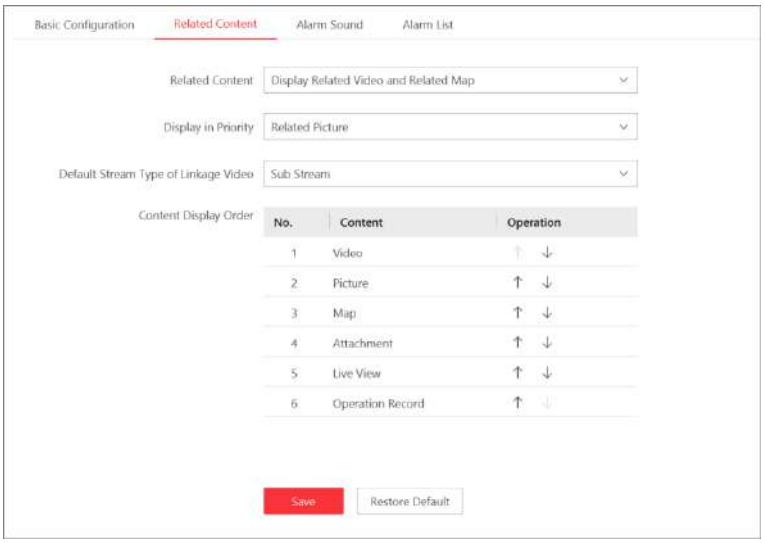


Figura 8-3 Configurações de conteúdo relacionado do Alarm Center

Conteúdo Relacionado

A(s) janela(s) do conteúdo relacionado a ser(em) exibida(s) no Alarm Center. Você pode selecionar para exibir a janela Related Video & Picture, a janela Map ou ambas para visualizar o conteúdo relacionado de um alarme.

Exibir em Prioridade

O tipo de conteúdo prioritário a ser exibido na janela Vídeo e Imagem Relacionados.
Por exemplo, se você definir **a Exibição prioritária da janela de vídeo** como Imagem relacionada, a imagem capturada do alarme será exibida primeiro na janela Vídeo e imagem relacionados na Central de alarmes.

Observação

Este parâmetro é válido somente quando **Exibir conteúdo relacionado** for Exibir vídeo relacionado e mapa relacionado ou Exibir somente vídeo relacionado.

Tipo de fluxo padrão de vídeo de vinculação

O tipo de fluxo padrão para visualização ao vivo e reprodução do alarme na janela Related Video & Picture. Por padrão, é o sub-fluxo.

Ordem de exibição do conteúdo

A ordem de exibição das abas na janela de detalhes do alarme. Clique em ↑/ ↓ na coluna Operation para ajustar a ordem de uma aba conforme necessário.

Definir som de alarme

Quando um alarme (por exemplo, um alarme de detecção de movimento, alarme de exceção de vídeo) é disparado, você pode configurar o cliente para emitir um aviso sonoro e pode configurar o som do aviso sonoro para diferentes níveis de prioridade.

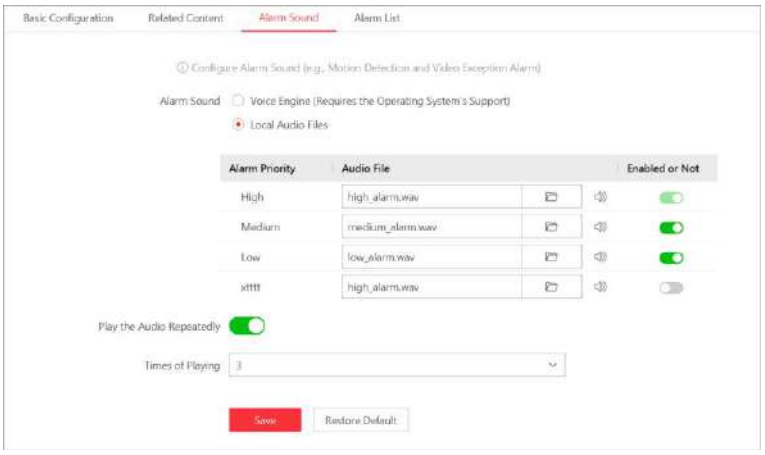


Figura 8-4 Configurações de som de alarme do Alarm Center

Som de alarme

Motor de voz

O computador reproduzirá o texto de voz configurado no Web Client quando o alarme for disparado.

Arquivos de áudio locais

Clique e selecione arquivos de áudio do computador local para diferentes níveis de alarme. Você pode clicar para testar o arquivo de áudio.

Observação

Para configurar o nível de prioridade, consulte o *Manual do Usuário do HikCentral Professional Web Client* .

Reproduzir o áudio repetidamente

Ligue e selecione os horários de reprodução na lista suspensa.

Personalize os ícones no Alarm Center

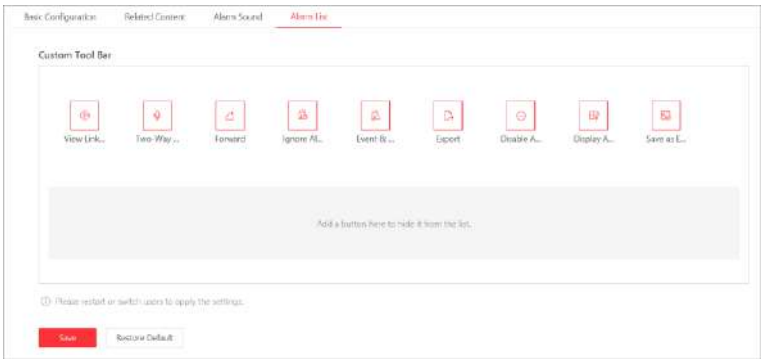


Figura 8-5 Configurações da lista de alarmes do Alarm Center

Tabela 8-2 Ícones na coluna Operação

Ícone	Descrição
Ver conteúdo vinculado	Inicie a visualização ao vivo ou a reprodução das câmeras relacionadas ao alarme e visualize as imagens capturadas.
Áudio bidirecional	Inicie o áudio bidirecional com a fonte de alarme do site atual ou do site remoto.
Avançar	Encaminhe o alarme para outros usuários para confirmação.
Ignorar alarme	Ignore o alarme para que o Control Client não receba o alarme durante o período de ignorância, mesmo que ele seja acionado.
Pesquisa de eventos e alarmes	Pesquise alarmes definindo condições na página Pesquisa de eventos e alarmes.
Exportar	Exporte os detalhes do alarme, incluindo informações do alarme, imagem do alarme, vídeo vinculado, mapa vinculado, etc., para o PC local.
Desativar alarme	Desabilite o alarme para que a plataforma não possa receber e registrar o alarme durante o período de desativação, mesmo que ele seja acionado.
Exibir alarme na parede inteligente	Exiba o vídeo do alarme na parede inteligente.
Salvar como evidência	Salve os recursos como evidência. Veja ***Gerenciamento de Evidências*** para detalhes.

Você pode clicar em um ícone na lista para adicioná-lo ao quadro cinza abaixo para ocultá-lo, ou clicar no ícone no quadro cinza para adicioná-lo novamente e exibi-lo na coluna Operação da Central de Alarmes.
Você também pode arrastar os ícones na lista de ícones para ajustar a ordem dos ícones.

Observação

- Os ícones exibidos na coluna Operação da Central de Alarmes variam de acordo com os recursos do dispositivo.
- Você deve reiniciar o Control Client ou alternar os usuários para aplicar as configurações.

8.3 Exibir Janela Pop-up Acionada por Alarme

Na página Monitoramento em Tempo Real do módulo Controle de Acesso, clique em uma porta que disparou um alarme e, em seguida, selecione **Detalhes do Alarme** para abrir a janela de informações do alarme. Você pode visualizar o horário do alarme, o dispositivo de origem que

disparou o alarme, o evento de disparo e o status do alarme, etc.

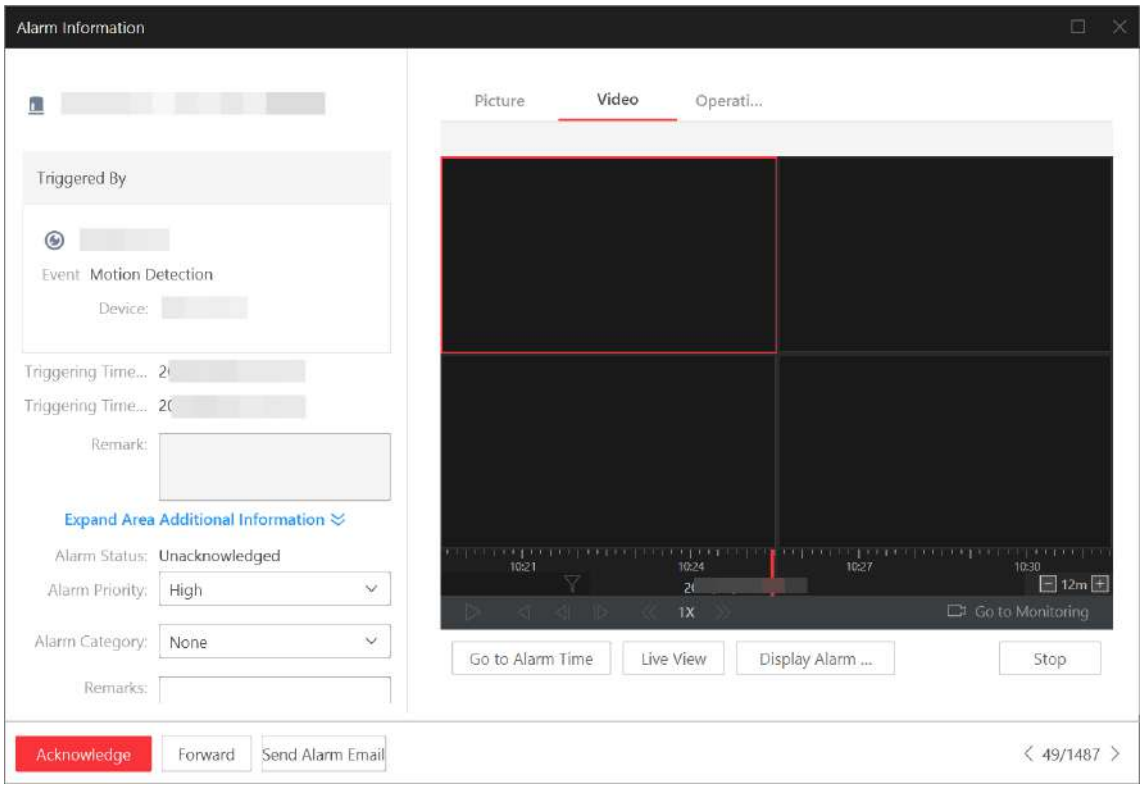


Figura 8-6 Janela pop-up acionada por alarme

Tabela 8-3 Funções e operações suportadas pela janela de alarme pop-up

Função	Operação
Ver área Informações adicionais	Se você tiver definido informações adicionais para a área onde o alarme é disparado, clique em **Expandir informações adicionais da área** para exibi-las.
Editar Alarme	Defina a prioridade do alarme, a categoria do alarme e as observações (por exemplo, insira "alarme falso acionado por folhas" quando tiver verificado os detalhes do alarme e descoberto que é um alarme falso) de acordo com as informações detalhadas do alarme.
Visualizar imagem relacionada ao alarme, áudio, vídeo, visualização ao vivo, mapa, anexo e registro de operação	Clique em **Imagem** / **Áudio** / **Vídeo** / **Visualização ao vivo** / **Mapa** / **Anexo** / **Registro de operação** para visualizar as imagens capturadas relacionadas ao alarme, a reprodução ou o vídeo ao vivo quando o alarme ocorreu, visualizar o local de entrada da câmera/alarme no mapa (se configurado), visualizar os arquivos anexados ao alarme e visualizar os registros de operação (ou seja, encaminhamento, confirmação) do alarme. **Observação** ● Ao visualizar os arquivos de vídeo gravados da câmera relacionada, você pode clicar em **Ir para Hora do Alarme** para reproduzir o vídeo

Função	Operação
	da hora do alarme. Você também pode clicar em **Visualização ao Vivo** para visualizar o vídeo ao vivo das câmeras relacionadas ou clicar em **Exibir no Smart Wall** para reproduzir a reprodução no smart wall. ● Durante a reprodução, você pode clicar na barra de tempo para reproduzir arquivos de vídeo armazenados no armazenamento principal ou auxiliar. ● Se você configurou o rastreamento visual, pode clicar para iniciar o rastreamento visual durante a reprodução.
Iniciar áudio bidirecional	Passe o cursor sobre a imagem de visualização ao vivo e clique para iniciar um áudio bidirecional com pessoas no local monitorado. Você pode ajustar o volume do microfone e do alto-falante e começar a gravar.
Reconhecer alarme	Clique em **Reconhecer** para reconhecer o alarme.
Alarme de avanço	Para alguns alarmes específicos, você pode clicar em **Forward** para encaminhá-los a outros usuários para reconhecimento. E você pode definir a prioridade como High para lembrar outros usuários de reconhecer os alarmes na prioridade mais alta.
Desbloquear porta	Clique em **Destrancar porta** para destrancar a porta que acionou o alarme.
Enviar e-mail de alarme	Clique em **Enviar e-mail de alarme** , selecione um modelo de e-mail e insira o(s) destinatário(s) do alarme e observações para enviar um e-mail contendo as informações sobre este alarme para os destinatários selecionados.
Saída de alarme de controle	Clique em **Controle de Saída de Alarme** para habilitar ou desabilitar as saídas de alarme vinculadas se você tiver definido saídas de alarme vinculadas na regra de alarme. Por exemplo, se um alarme sonoro estiver vinculado à regra de alarme, quando o alarme for disparado, você poderá ligar ou desligar o alarme sonoro.
Transmissão de controle	Clique em **Controle de transmissão** para reproduzir o arquivo de áudio vinculado, executar fala em tempo real ou iniciar o áudio bidirecional. **Observação** Esta função só é suportada pelo Sistema Central com o módulo Gerenciamento de Site Remoto.
Ver alarme anterior ou seguinte	Clique < > para visualizar as informações do alarme anterior ou seguinte.
Habilitar janela pop-up	Desmarque **Janela pop-up** para desativar a janela pop-up quando um novo alarme for acionado.

	Observação Quando a janela pop-up permanecer aberta, o alarme posterior, se a prioridade do alarme for maior, será exibido na janela pop-up e substituirá o anterior.
Exibir janela pop-up em modo de tela cheia	Marque **Tela cheia** para exibir a janela pop-up no modo de tela cheia por padrão.

8.4 Disparar Manualmente um Evento Definido pelo Usuário

A plataforma fornece eventos definidos pelo usuário que são usados se o evento que você precisa não estiver na lista de eventos e alarmes fornecida, ou o evento genérico não puder definir corretamente o evento recebido do sistema de terceiros. No Control Client, você pode disparar um evento definido pelo usuário manualmente e ele ativará uma série de ações de acordo com as configurações no Web Client.

Antes de começar

Adicione o evento definido pelo usuário à plataforma e determine o que acontece quando você o aciona manualmente, como defini-lo como a fonte do alarme, como início/fim do cronograma de armamento do alarme ou como ações de vinculação do alarme. Para obter detalhes, consulte o *Manual do Usuário do HikCentral Professional Web Client* .

Passos

1. No canto superior direito do Control Client, selecione → **Acionar evento** .

Observação

Você também pode clicar em no canto superior direito da página de exibição ao vivo ou de reprodução para abrir a janela Selecionar evento definido pelo usuário.

Os eventos definidos pelo usuário adicionados à plataforma serão exibidos.

2. Selecione o evento que deseja acionar e clique em **OK** .

8.5 Executar Controle de Armar para Alarmes

Você pode aceitar/habilitar e ignorar/desabilitar as regras de alarme configuradas dos recursos selecionados. Após aceitar/habilitar uma regra de alarme, o Control Client/plataforma atual pode receber as informações de alarme disparadas da fonte de alarme. Se você ignorar/desabilitar uma regra de alarme, o Control Client/plataforma atual não poderá receber este alarme da fonte de

alarme.

Passos

Observação

Você também pode executar o controle de armar para dispositivos de controle de segurança (como armar/desarmar partições, ignorar zonas, etc.) e radares. Para detalhes, consulte ***Controle de Segurança*** .

1. No canto superior esquerdo do cliente, selecione → **Todos os módulos** → **Monitoramento** → **Central de alarmes** .
2. No canto superior direito da Central de Alarmes, clique em **Controle de Armar** para abrir a janela Controle de Armar.

Observação

Você também pode selecionar → **Ferramenta** → **Controle de Armar** para abrir a janela Controle de Armar.

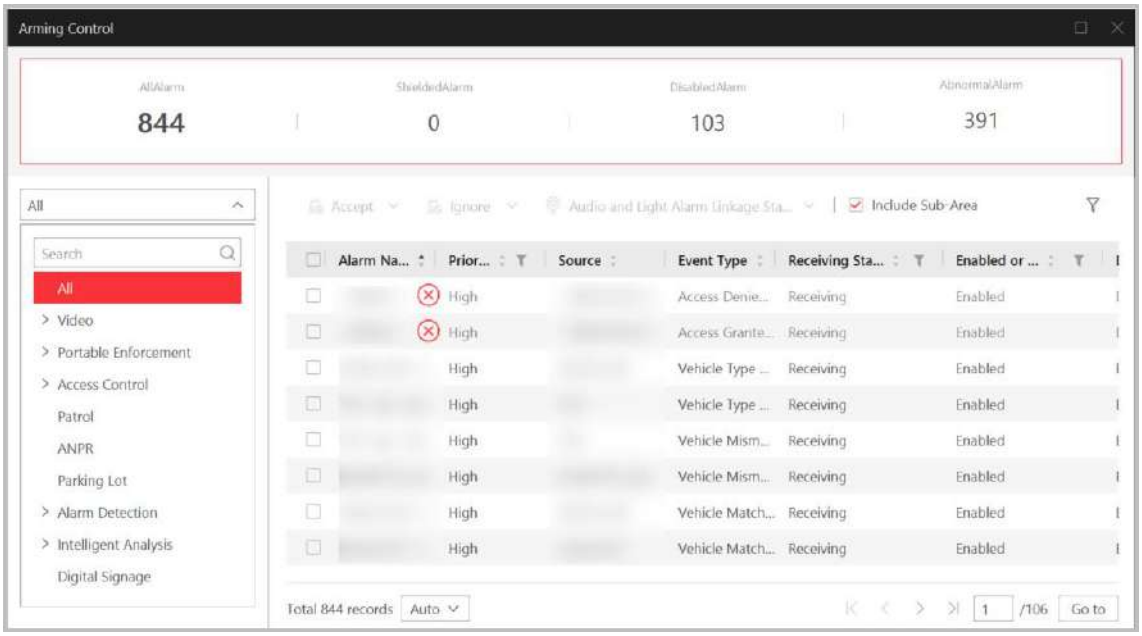


Figura 8-7 Controle de armamento

3. No painel esquerdo, selecione um tipo de fonte.
   Todas as áreas relacionadas serão listadas e todas as regras de alarme configuradas da fonte selecionada serão exibidas. Você pode marcar a opção **Incluir Subárea** para exibir as regras de alarme das fontes nas áreas filhas. Se houver muitas regras de alarme, você pode selecionar um site ou uma área para exibir suas regras de alarme.
4. Opcional: se houver muitas regras de alarme, selecione um site ou uma área para exibir suas regras de alarme ou clique para definir condições para filtrar regras de alarme.

5. Verifique a(s) regra(s) de alarme para executar o controle de armar.

Observação

- Se a fonte for Alarm Input, um ícone será exibido se houver uma exceção. Você pode visualizar os detalhes da exceção movendo o cursor no ícone.
- As configurações de ignorância e aceitação no Alarm Center controlam apenas o recebimento de alarmes no Control Client atual. Mas as configurações de desabilitação e habilitação no Alarm Center controlam o recebimento de alarmes na plataforma.

Ignorar alarme

1. Verifique a(s) regra(s) de alarme no status Aceito.
2. Clique em **Ignorar** → **Ignorar alarme** para abrir o painel de configurações de ignorância.
3. Defina a hora de início, a duração ou o propósito da ignorância.
4. Clique **em Salvar** para ignorar as regras de alarme selecionadas.

Observação

Se você ignorar uma regra de alarme, o Cliente de Controle atual não receberá esse alarme durante o período de ignorância, mesmo que ele seja acionado.
Por exemplo, se você definir a duração da ignorância para uma hora, o alarme não poderá ser recebido pelo Control Client atual, mas será registrado como um log na plataforma dentro de uma hora. O alarme será recebido novamente pelo Control Client atual após uma hora.

Aceitar alarme

1. Verifique a(s) regra(s) de alarme no status Ignorado.
2. Clique em **Aceitar** → **Aceitar alarme** para aceitar as regras de alarme selecionadas.

Observação

Se você aceitar uma regra de alarme, o Control Client atual receberá esse alarme e você poderá visualizar as informações do alarme no Control Client atual.

Desativar alarme

1. Verifique a(s) regra(s) de alarme no status Ativado.
2. Clique em **Ignorar** → **Desativar alarme** para abrir o painel de configurações.
3. Defina a hora de início, a duração ou a finalidade da desativação.
4. Clique **em Salvar** para desabilitar a(s) regra(s) de alarme selecionada(s).

Observação

Se você desabilitar uma regra de alarme, a plataforma não receberá nem registrará esse alarme durante o período de desativação, mesmo que ele seja acionado.
Por exemplo, se você definir a duração da desativação para uma hora, o alarme não poderá ser recebido e registrado pela plataforma dentro de uma hora. O alarme será recebido novamente pela plataforma após uma hora.

Habilitar alarme

1. Verifique a(s) regra(s) de alarme no status Desativado.
2. Clique em **Aceitar** → **Habilitar alarme** para habilitar a(s) regra(s) de alarme

selecionada(s).

Observação

Se você habilitar uma regra de alarme, a plataforma receberá esse alarme e você poderá visualizar as informações do alarme em qualquer cliente.

Habilitar ligação de alarme de áudio e luz

1. Verifique a(s) regra(s) de alarme no status DESLIGADO na coluna Status de vinculação de alarme de áudio e luz.
2. Clique em **Habilitar vinculação de alarme de áudio e luz** para habilitar a(s) regra(s) de alarme selecionada(s).

Observação

A vinculação de alarmes de áudio e luz deve ser suportada pelo dispositivo vinculado aos eventos/alarmes, incluindo cruzamento de linha, intrusão, entrada de região, saída de região e detecção de movimento.

Desativar a ligação de alarme de áudio e luz

1. Verifique a(s) regra(s) de alarme no status LIGADO na coluna Status de vinculação de alarme de áudio e luz.
2. Clique em **Habilitar vinculação de alarme de áudio e luz** para desabilitar a(s) regra(s) de alarme selecionada(s).

Observação

A vinculação de alarmes de áudio e luz deve ser suportada pelo dispositivo vinculado a determinados eventos/alarmes, incluindo cruzamento de linha, intrusão, entrada de região, saída de região e detecção de movimento.

8.6 Pesquisa de Eventos e Alarmes

A plataforma fornece estatísticas e resultados de análise de eventos históricos e alarmes para que você tenha uma visão geral e outras aplicações. Você também pode pesquisar eventos históricos e alarmes definindo diferentes condições para visualizar os detalhes conforme necessário.

8.6.1 Visão Geral de Eventos e Alarmes

No módulo de visão geral de eventos e alarmes, você terá uma visão geral da distribuição de eventos ou alarmes, dos 5 principais tipos de eventos ou categorias de alarmes e das 5 principais áreas de eventos ou alarmes.

No canto superior esquerdo da página inicial, selecione → **Monitoramento de segurança** → **Evento e alarme** .

Selecione **Pesquisar** → **Visão geral** à esquerda.

No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Investigação**

→ **Pesquisa de eventos e alarmes** → **Visão geral** .

Figura 8-8 Análise de eventos e alarmes

Módulo	Descrição
1	● Tendência diária: os números de eventos ou alarmes nos últimos 7 dias ou nos últimos 30 dias são exibidos no gráfico de barras verticais. ● Tendência horária: os números de eventos ou alarmes de 24 horas dos últimos 7 dias, dos últimos 30 dias ou do período personalizado são exibidos no gráfico de linhas.
2	Os dados dos 5 principais tipos de eventos ou categorias de alarmes disparados no dia atual, últimos 7 dias ou últimos 30 dias são exibidos no gráfico de barras horizontais. Você pode clicar no número vermelho de um item para pular para a página Event and Alarm Search.
3	Os dados das 5 principais áreas de eventos ou alarmes no dia atual, nos últimos 7 dias ou nos últimos 30 dias são exibidos no gráfico de barras horizontais.

Você pode clicar em **Configurações** no canto superior direito para personalizar os tipos de eventos ou categorias de alarmes a serem calculados na página de visão geral.

Observação

As informações exibidas em cada área mudarão de acordo com o alvo do relatório no painel Configurações. Por exemplo, se você selecionar **Alarme** no painel Configurações como o alvo do relatório, a área superior exibirá apenas o número de alarmes, a área inferior esquerda exibirá apenas os dados das 5 principais categorias de alarmes e a área inferior direita exibirá apenas os dados das 5 principais áreas de alarmes.

8.6.2 Pesquisar Logs de Eventos e Alarmes

Você pode pesquisar arquivos de log de eventos e alarmes do recurso adicionado definindo condições diferentes.

Antes de começar

Certifique-se de ter configurado eventos e alarmes no Web Client. Veja *o Manual do Usuário do HikCentral Professional Web Client* para detalhes.

Passos

1. No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Investigação** → **Pesquisa de eventos e alarmes** → **Pesquisa de eventos e alarmes** .
2. Defina o intervalo de tempo para pesquisa.
   – Selecione um período de tempo predefinido para pesquisa.
   – Selecione **Personalizado** e especifique a hora de início e término da pesquisa.
3. No campo **Disparar alarme** , selecione o status do evento (se o evento é disparado como alarme).

   Todos

   Eventos e alarmes.

   Desabilitado

   Os eventos aconteceram, mas não foram acionados como alarmes.

   Habilitado

   Os eventos aconteceram e foram disparados como alarmes. Se você selecionar isso, poderá definir condições para filtrar alarmes marcando status, reconhecendo status, prioridade de alarme ou categoria de alarme.
4. Ative **a Área** e clique para selecionar a área do evento ou fonte de alarme.
5. Ative **a Condição de disparo** e clique para selecionar os eventos de disparo e a origem do site atual ou de sites remotos.

Observação

- O site remoto está disponível apenas para o Sistema Central com módulo Gerenciamento de Site Remoto (com base na Licença que você adquiriu).
- Se você selecionar eventos de disparo na categoria Controle de acesso, insira o nome da pessoa que entrou/saiu.
- Se você selecionar eventos de disparo na categoria Integração de recursos de terceiros e tiver inserido informações adicionais sobre o alarme no sistema de terceiros, insira as informações adicionais.

6. Ative **Nome do evento e alarme** para selecionar o nome do evento/alarme na lista suspensa.
7. Clique em **Pesquisar** .
   Os logs de eventos ou alarmes correspondentes serão listados na página da direita.
8. **Opcional**: execute as seguintes operações após pesquisar logs de eventos e alarmes.

Visualizar e editar log de eventos e alarmes	Clique no nome de um evento ou alarme pesquisado para visualizar a imagem ou o vídeo do alarme vinculado e os detalhes dos registros de operação. Se o evento e o alarme não forem reconhecidos, você pode selecionar a categoria do alarme ou inserir as observações e clicar em **Reconhecer** no painel de detalhes. Se o evento e o alarme forem reconhecidos, você pode clicar em **Marcado como não reconhecido** para cancelar o reconhecimento do evento e do alarme, ou **Editar alarme** para editar a prioridade, categoria ou observações do alarme.
Marcar evento e alarme	Clique para marcar o evento ou alarme como desejado. A cor do ícone muda para .
Iniciar áudio bidirecional	Se a fonte de alarme estiver vinculada a uma câmera que suporte áudio bidirecional, você pode clicar na coluna Operation para iniciar o áudio bidirecional com a câmera vinculada. Para saber como executar áudio bidirecional, consulte ***Perform Two-Way Audio*** .
Exportar eventos e alarmes	Clique na coluna Operation para exportar o evento ou alarme especificado para o PC local. E você pode visualizar o processo de exportação no Download Center clicando em no topo da página. Ou clique em **Exportar** no canto superior direito da página de resultados da pesquisa e selecione o formato como **Excel** , **CVS** ou **PDF** para exportar todos os eventos e alarmes pesquisados para o PC local. **Observação** Ao exportar todos os eventos e alarmes no formato Excel, você pode marcar **Incluir informações de imagem** para exportar as imagens relacionadas.
Salvar como evidência	Clique na coluna Operação de um evento e alarme selecionado para abrir o painel Salvar como evidência. ● **Adicionar à evidência existente** : insira o nome, a etiqueta, a ID ou a descrição da evidência existente para vincular o arquivo de log de eventos e alarmes à evidência. ● **Criar Evidência** : Defina os parâmetros necessários para criar a nova evidência para vinculação com o arquivo de log de eventos e alarmes. Para saber como criar evidências, consulte ***Adicionar um Caso*** . ● **Only Upload File** : Carregue o arquivo de log de eventos e alarmes do armazenamento local para o pool de recursos. Você pode verificar o progresso do upload no Task Center (veja ***Manage Downloading/Uploading Tasks*** para detalhes).
Mudar para a tela auxiliar	Clique para abrir a página Event & Alarm Search como uma tela auxiliar. Você pode visualizar eventos e alarmes na tela auxiliar, bem como operar outras páginas do Control Client.

Capítulo 9 Busca de Veículos

Os registros relacionados ao veículo detectados por diferentes dispositivos podem ser pesquisados e analisados no Control Client.
No canto superior esquerdo, selecione → **Todos os módulos** → **Investigação** → **Busca de veículos** .

9.1 Busca por Veículos Que Passam Detectados por Câmeras e UVSSs

Se as câmeras ANPR (Reconhecimento Automático de Placas) e UVSSs (Sistemas de Vigilância Inferior do Veículo) adicionadas estiverem configuradas corretamente e as placas dos veículos forem detectadas e reconhecidas com sucesso, você poderá pesquisar informações relacionadas ao veículo que passa.

Antes de começar

Certifique-se de que a licença adquirida seja compatível com a função ANPR.

Passos

1. No painel de navegação esquerdo, selecione **Pesquisa e análise de veículos que passam** → **Pesquisa de veículos que passam** .
2. Selecione **Câmera** ou **UVSS** como o tipo de fonte que detectou os veículos que passavam.
3. Selecione a(s) fonte(s).
   – Se **Câmera** for selecionada como o tipo de fonte, clique em , selecione o site atual ou um site remoto e especifique a(s) câmera(s) ANPR.
   – Se **UVSS** for selecionado como o tipo de fonte, verifique o(s) UVSS(s).
4. Defina o tempo de duração da pesquisa.
5. Ligue e defina a(s) condição(ões) de busca de acordo com suas necessidades. Aqui, apresentamos apenas algumas condições que podem confundi-lo.

Observação

Para as regiões do Oriente Médio e Norte da África, Country/Region e Plate Category devem ser habilitados. Uma vez habilitados, as informações de país/região e categoria de placa serão incluídas nos resultados da pesquisa.

País/Região

O país/região onde o número da placa do veículo está registrado.

Número da placa do veículo

- **Sem placa** : Pesquise veículos sem placas.
- **Com placa** : digite uma palavra-chave para pesquisar veículos pelo número da placa.

Velocidade de condução

Faixa de velocidade de condução do veículo. Esta condição está disponível somente quando o tipo de fonte é selecionado como **Câmera** .

Direção de condução

- **Para frente** : O veículo se moveu em direção à câmera com o cabeçote voltado para ela.
- **Marcha ré** : O veículo se afastou da câmera com a traseira voltada para ela.
- **Outro** : O veículo se moveu em direção à câmera ou se afastou dela em outras direções.

Lista de veículos

Pesquise veículos que passam na(s) lista(s) de veículos específica(s). Esta condição está disponível somente quando o tipo de fonte é selecionado como **Câmera** .

Informações adicionais

O(s) item(ns) de informações adicionais do veículo que você personalizou. Para saber como personalizar as informações do veículo, consulte o manual do usuário do Web Client.

6. Clique em **Pesquisar** .
   Os veículos que passam correspondentes serão exibidos à direita. Você pode clicar em ou para exibir os resultados no modo de lista e no modo de miniatura.
7. **Opcional**: Execute a(s) seguinte(s) operação(ões) após procurar veículos que passam.

Marcar veículos que passam	Clique na coluna Marcar para marcar o veículo. Os veículos marcados podem ser filtrados na próxima busca.
Ver detalhes do veículo	Clique no número da placa na coluna Número da placa para abrir o painel de detalhes do veículo. Você pode visualizar a imagem capturada do veículo/trem de pouso clicando em , o arquivo de vídeo vinculado do veículo que passa clicando em , as informações básicas (incluindo a imagem capturada da placa, o número da placa reconhecido, as informações do proprietário do veículo, as informações do veículo e as informações da fonte de detecção) e a localização geográfica do veículo no mapa (se o veículo for adicionado ao mapa como um ponto de acesso). Você também pode clicar na aba Informações Básicas para editar o número da placa caso o número reconhecido esteja incorreto. **Observação** Ao visualizar o arquivo de vídeo vinculado de veículos que passam, você pode controlar a reprodução e clicar em **Ir para monitoramento** para entrar na página de monitoramento.
Adicionar à lista de veículos	Se um veículo for reconhecido, você pode adicioná-lo manualmente a uma lista de veículos. Clique na coluna Operation ou clique em **Add to List** no painel de detalhes do veículo e, em seguida, selecione uma lista para adicionar o veículo à lista. Veja ***Add Recognized Vehicle to Vehicle List*** para obter detalhes.
Baixe um veículo que	Clique na coluna Operation ou clique em **Download** no painel de detalhes do

passa	veículo para salvar as informações sobre o veículo que passa como um arquivo CSV no PC local. As imagens capturadas e o arquivo de vídeo vinculado também serão salvos na mesma pasta. Você pode visualizar o progresso do download no Task Center. Para detalhes, consulte ***Gerenciar tarefas de download/upload*** .
Carregar veículos que passam	Clique na coluna Operação de um veículo que passa para vinculá-lo a uma evidência ou enviá-lo ao pool de recursos. ● **Adicionar à evidência existente** : insira o nome, a etiqueta, a ID ou a descrição da evidência existente para vincular o veículo que passa à evidência. ● **Criar Evidência** : Defina os parâmetros necessários para criar uma evidência para vinculá-la ao veículo que passa. ● **Somente Carregar Arquivo** : Carregue as informações do veículo que passa do armazenamento local para o pool de recursos. Você pode verificar o progresso do carregamento no Centro de Tarefas. Para obter detalhes, consulte ***Gerenciar Tarefas de Download/Carregamento*** .
Exportar veículos que passam	Clique em **Exportar** e selecione **Excel** , **CSV** ou **PDF** como o formato de arquivo exportado. ● Se você selecionar **Excel** como formato de arquivo, poderá marcar **Exportar imagem** para salvar as imagens contidas nos resultados da pesquisa no PC local com o arquivo exportado. ● Não é possível exportar mais de 500 veículos que passam no formato PDF ao mesmo tempo. **Observação** As imagens exportadas serão nomeadas e classificadas pelo tempo de captura. ● Não é possível exportar mais de 100.000 veículos que passam sem imagens capturadas ao mesmo tempo. ● Verifique o status e o progresso da tarefa de exportação na **Central de Tarefas** .
Classificar resultados da pesquisa	**lassificar por tempo** Classifique os resultados da pesquisa pelo momento em que os veículos passam pela câmera ou UVSS. **lassificar por tempos de passagem de veículos** Classifique os resultados da pesquisa pelos horários em que os veículos passaram pela câmera

9.2 Busca por Veículos Que Passam Detectados por Entradas e Saídas

Se o número da placa de um veículo for reconhecido por câmeras ou unidades de captura

vinculadas a uma entrada e saída, você pode pesquisar informações de passagem do veículo relacionado.

Passos

1. No painel de navegação esquerdo, selecione **Pesquisa de estacionamento** → **Pesquisa de veículos que passam na entrada e saída** .
2. Selecione uma ou várias entradas e saídas onde você deseja procurar os registros de passagem de veículos.
3. Defina o tempo de duração da pesquisa.
4. Ative e defina a(s) condição(ões) de busca de acordo com suas necessidades. Aqui, apresentamos apenas condições que podem confundi-lo.

   País/Região

   Selecione o país/região onde o número da placa do veículo está registrado.

   Número da placa do veículo.

   - **Sem placa** : Pesquise veículos sem placas.
   - **Com placa** : insira o número da placa do veículo ou parte dele.

   Entrar ou Sair

   Selecione se o veículo está entrando ou saindo.

   Como abrir a barreira

   Selecione como a cancela é aberta quando um veículo entra/sai do estacionamento. **Manual** indica que um guarda de segurança controlou manualmente a cancela para abrir após identificar o proprietário do veículo; **Auto Allow for Entry and Exit** indica que a cancela abriu automaticamente após o número da placa ser reconhecido por uma unidade de captura; **Not Opened** indica que a cancela não abriu mesmo após a unidade de captura reconhecer o número da placa.

   Razão

   Selecione o(s) motivo(s) para permitir ou não a entrada/saída do veículo na lista suspensa.

   Lista de veículos

   Selecione na lista suspensa para pesquisar registros de veículos temporários, veículos de visitantes, veículos registrados ou veículos na lista de bloqueio ou outras listas personalizadas.

   Informações adicionais

   O(s) item(ns) de informações adicionais do veículo que você personalizou. Para saber como personalizar as informações do veículo, consulte o *Manual do Usuário do HikCentral Professional Web Client* .
5. Clique em **Pesquisar** .

   Os resultados correspondentes serão exibidos à direita.

Observação

Você pode clicar em ☰ou ⊞para alternar entre o modo de lista e o modo de miniatura.

6. **Opcional**: execute as seguintes operações conforme necessário.

Marcar veículo Clique na coluna Marcar para marcar o veículo. Os veículos marcados podem ser filtrados na próxima busca.

Ver detalhes do veículo Clique no número da placa na coluna Número da placa para abrir o painel de detalhes do veículo.
Você pode visualizar a imagem capturada clicando em , o arquivo de vídeo vinculado do veículo que passa clicando em , e informações sobre o proprietário do veículo, o veículo e detalhes relacionados à sua entrada/saída.

Observação

Ao visualizar o arquivo de vídeo vinculado de veículos que passam, você pode controlar a reprodução e clicar em **Ir para monitoramento** para entrar na página de monitoramento.
Você pode clicar para alternar entre a câmera vinculada e a câmera ANPR.

Adicionar à lista de veículos Se um veículo não for adicionado a uma lista de veículos, você poderá adicioná-lo manualmente.
Clique na coluna Operação ou clique em **Adicionar veículo** no painel de detalhes do veículo e selecione uma lista de alvos.

Baixe um veículo que passa Clique na coluna Operation ou clique em **Download** no painel de detalhes do veículo para salvar as informações sobre o veículo que passa como um arquivo CSV no PC local. A imagem capturada e o arquivo de vídeo vinculado também serão salvos na mesma pasta.
Você pode ver o progresso do download na Central de Tarefas.

Carregar um veículo que passa Clique na coluna Operação de um veículo que passa para vinculá-lo a uma evidência ou enviá-lo ao pool de recursos.

- **Adicionar à evidência existente** : insira o nome, a etiqueta, a ID ou a descrição da evidência existente para vincular o veículo que passa à evidência.
- **Criar Evidência** : Defina os parâmetros necessários para criar uma evidência para vinculá-la ao veículo que passa.
- **Somente Carregar Arquivo** : Carregue as informações do veículo que passa do armazenamento local para o pool de recursos. Você pode verificar o progresso do carregamento no Centro de Tarefas

Ver foto do proprietário Clique no número da placa e no nome do proprietário do veículo para ver fotos do proprietário, incluindo uma foto de perfil enviada e uma foto tirada na entrada e na saída.

Observação

Esta operação só pode ser realizada se os modos de entrada e saída do estacionamento estiverem definidos como **Person and License Plate Match** . Vá para o módulo Parking Lot no Web Client para definir os modos de entrada/saída.

Exportar um veículo que passa Clique em **Exportar** e selecione **Excel** ou **CSV** como formato do arquivo exportado.

Observação

- Se você selecionar **Excel** como o formato de arquivo, você pode marcar **Exportar Imagem** para salvar as imagens contidas nos resultados da pesquisa no PC local com o arquivo exportado. As imagens exportadas serão nomeadas e classificadas pelo tempo de captura.

- Não é possível exportar mais de 100.000 veículos que passam sem imagens capturadas ao mesmo tempo.

9.3 Pesquisar Registros de Pagamento

Se um veículo pagar a taxa de estacionamento e sair do estacionamento, suas informações de pagamento, como a fonte de pagamento e o tempo de operação, serão registradas na plataforma. Na plataforma, você pode pesquisar os registros de pagamento gerados em um estacionamento específico ou os registros de um veículo específico, definindo condições de pesquisa de acordo com as necessidades reais. Você também pode exportar os registros para seu PC. Com as estatísticas, você pode monitorar algumas das transações feitas nos estacionamentos, o que pode ajudá-lo a gerenciar melhor os estacionamentos.

Passos

1. No painel de navegação esquerdo, selecione **Pesquisa de estacionamento** → **Pesquisa de registro de pagamento** .
2. Defina o tempo de duração da pesquisa.
3. Defina a(s) condição(ões) de busca de acordo com suas necessidades. Aqui, apresentamos apenas condições que podem confundi-lo.

   Operador

   Selecione a pessoa responsável por cobrar a taxa na lista suspensa.

   Método de pagamento

   Selecione como a taxa de estacionamento é paga. **Dinheiro** indica que a taxa é paga em dinheiro; **Conta do Proprietário do Veículo** indica que a taxa é deduzida do saldo da conta do proprietário.

   Fonte de pagamento

   Selecione onde a taxa de estacionamento é paga. **Booth** indica que a taxa de estacionamento é paga no estande; **Toll Center** indica que a taxa de estacionamento é paga no centro de pedágio.
4. Clique em **Pesquisar** .
5. **Opcional**: No canto superior direito, clique em **Exportar** , selecione **Excel** ou **CSV** como o formato do arquivo exportado e clique em **Salvar** para exportar os resultados da pesquisa para o PC local.

9.4 Busca de veículos estacionados

Se o número real de vagas de estacionamento vagas for diferente do número exibido nas telas de orientação, você pode pesquisar os veículos que já saíram, mas ainda estão registrados no estacionamento para editar as informações do veículo. Por exemplo, para estacionamentos que exigem que todos os veículos no local saiam no final do dia, você pode pesquisar os veículos que

ainda estão no estacionamento e exportar as informações dos veículos. Em outra situação, se um veículo for autorizado manualmente a sair do estacionamento, o número de vagas de estacionamento vagas pode não ser atualizado a tempo. Nessa situação, você pode pesquisar o veículo e excluí-lo da lista de veículos do estacionamento para atualizar o número de vagas de estacionamento vagas.

Passos

1. No painel de navegação esquerdo, selecione **Pesquisa de estacionamento** → **Pesquisa de veículos estacionados** .
2. Selecione um estacionamento na lista suspensa.
3. Ative e defina a(s) condição(ões) de busca de acordo com suas necessidades. Aqui, apresentamos apenas condições que podem confundi-lo.

   País/Região

   Selecione o país/região onde o número da placa do veículo está registrado.

   Número da placa do veículo.

   - **Sem placa** : Pesquise veículos sem placas.
   - **Com placa** : insira o número da placa do veículo ou parte dele.

   Como abrir a barreira

   Selecione como a cancela é aberta quando um veículo entra/sai do estacionamento. **Manual** indica que um segurança controlou manualmente a cancela para abrir após identificar o proprietário do veículo; **Automático** indica que a cancela abriu automaticamente após o número da placa ser reconhecido por uma unidade de captura; **Barreira Não Aberta** indica que a cancela não abriu após a unidade de captura reconhecer o número da placa.

   Razão

   Selecione o(s) motivo(s) para permitir ou não a entrada/saída do veículo na lista suspensa.

   Lista de veículos

   Selecione na lista suspensa para pesquisar registros de veículos temporários, veículos de visitantes, veículos registrados ou veículos na lista de bloqueio ou outras listas personalizadas.

   Informações adicionais

   O(s) item(ns) de informações adicionais do veículo que você personalizou. Para saber como personalizar as informações do veículo, consulte o *Manual do Usuário do HikCentral Professional Web Client* .
4. Clique em **Pesquisar** .
   Os resultados correspondentes serão exibidos à direita.

Observação

Você pode clicar em ☰ou ⊞para alternar entre o modo de lista e o modo de miniatura.

5. **Opcional**: execute as seguintes operações conforme necessário.

Marcar veículo Clique na coluna Marcar para marcar o veículo. Os veículos marcados podem ser filtrados na próxima busca.

Ver detalhes do veículo Clique no número da placa na coluna Número da placa para abrir o painel de detalhes do veículo.
Você pode visualizar a imagem capturada clicando em , o arquivo de vídeo vinculado do veículo estacionado clicando em , e informações sobre o proprietário do veículo, o veículo e detalhes relacionados à sua entrada/saída.

Observação

Ao visualizar o arquivo de vídeo vinculado de veículos estacionados, você pode controlar a reprodução e clicar em **Ir para monitoramento** para entrar na página de monitoramento.

Adicionar à lista de veículos Se um veículo não for adicionado a uma lista de veículos, você poderá adicioná-lo manualmente.
Clique em **Adicionar veículo** no painel de detalhes do veículo e selecione uma lista para adicionar o veículo à lista.

Baixar Registro do Veículo Clique na coluna Operation ou clique em **Download** no painel de detalhes do veículo para salvar as informações sobre o veículo estacionado como um arquivo CSV no PC local. A imagem capturada e o arquivo de vídeo vinculado também serão salvos na mesma pasta. Você pode ver o progresso do download na Central de Tarefas.

Ver foto do proprietário Clique no número da placa e no nome do proprietário do veículo para ver fotos do proprietário, incluindo uma foto de perfil enviada e uma foto tirada na entrada e na saída.

Observação

Esta operação só pode ser realizada se os modos de entrada e saída do estacionamento estiverem definidos como **Person and License Plate Match** . Vá para o módulo Parking Lot no Web Client para definir os modos de entrada/saída.

Exportar todos os registros Clique em **Exportar** e selecione **Excel** ou **CSV** como formato do arquivo exportado.

Observação

- Se você selecionar **Excel** como formato de arquivo, poderá marcar **Exportar imagem** para salvar as imagens contidas nos resultados da pesquisa no PC local com o arquivo exportado.
- Não é possível exportar mais de 100.000 registros sem imagens capturadas de uma só vez.

Excluir veículo do estacionamento Clique em **Excluir tudo** para remover todos os veículos exibidos do estacionamento ou clique na coluna Operação de um veículo para removê-lo do estacionamento.

9.5 Busca de Registros de Estacionamento

Na plataforma, você pode pesquisar registros de estacionamento gerados em um estacionamento específico ou registros de um veículo específico, definindo condições de pesquisa relevantes de

acordo com as necessidades reais, e realizar outras operações, como visualizar informações detalhadas dos veículos e exportar os registros para seu PC.

Passos

1. No painel de navegação esquerdo, selecione **Pesquisa de estacionamento** → **Pesquisa de registro de estacionamento** .
2. Defina o tempo de duração da pesquisa.
3. Defina a(s) condição(ões) de busca de acordo com suas necessidades. Aqui, apresentamos apenas condições que podem confundi-lo.

   Vaga de estacionamento nº.

   Digite o número da vaga de estacionamento de um estacionamento específico para pesquisar registros de veículos que estacionam ou estacionaram naquela vaga.

   Status do estacionamento

   Selecione um status de estacionamento. **Parking** indica que o veículo ainda está estacionado no estacionamento, enquanto **Exit** indica que o veículo já saiu do estacionamento.
4. Clique em **Pesquisar** .
   Os resultados correspondentes serão exibidos à direita.

Observação

Você pode clicar em ☰ ou ⊞ para alternar entre o modo de lista e o modo de miniatura.

5. **Opcional**: execute as seguintes operações conforme necessário.

Ver detalhes do veículo	Clique no número da placa na coluna Número da placa para abrir o painel de detalhes do veículo. Você pode visualizar a imagem capturada clicando em , o arquivo de vídeo vinculado do veículo clicando em , e informações sobre o proprietário do veículo, o veículo e detalhes relacionados à sua entrada/saída. **Observação** Ao visualizar o arquivo de vídeo vinculado dos veículos, você pode controlar a reprodução e clicar em **Ir para monitoramento** para entrar na página de monitoramento.
Ver foto do proprietário	Clique no número da placa e no nome do proprietário do veículo para ver fotos do proprietário, incluindo uma foto de perfil enviada e uma foto tirada na entrada e na saída. **Observação** Esta operação só pode ser realizada se os modos de entrada e saída do estacionamento estiverem definidos como **Person and License Plate Match** . Vá para o módulo Parking Lot no Web Client para definir os modos de entrada/saída.
Exportar Registros de Estacionamento de Veículos	Clique em **Exportar** e selecione **Excel** ou **CSV** como formato do arquivo exportado. **Observação** ● Se você selecionar **Excel** como formato de arquivo, poderá marcar **Exportar imagem** para salvar as imagens contidas nos resultados da pesquisa no PC local com o arquivo

exportado.
- Não é possível exportar mais de 100.000 registros de estacionamento sem imagens capturadas de uma só vez.

Ir para Pesquisa de Pessoas	Clique para pular para a página de busca de corpos humanos por características para procurar pessoas que passaram pelo veículo dentro do período de estacionamento do veículo.

9.6 Pesquisar Vários Veículos em Um Único Status de Conta

No Control Client, você pode pesquisar vários veículos sob um status de conta de um estacionamento específico ou de uma conta específica, definindo condições de pesquisa relevantes de acordo com as necessidades reais. Você pode visualizar as informações detalhadas dos resultados da pesquisa, incluindo as informações do proprietário, o número de vagas de estacionamento alocadas a uma conta, a validade do passe de estacionamento de um veículo, o status de estacionamento dos veículos, etc.

Antes de começar

Certifique-se de ter adicionado vários veículos à conta a ser pesquisada e tenha passes de estacionamento relacionados aos veículos, se necessário. Para mais detalhes. Veja o *Manual do Usuário do HikCentral Professional Web Client* .

Passos

1. No painel de navegação esquerdo, selecione **Pesquisa de estacionamento** → **Pesquisa de status de vários veículos em uma conta** .
2. Defina as condições de pesquisa de acordo com as necessidades reais.

   No estacionamento ou não

   Quando **In** for selecionado, os veículos que estão estacionando ou estacionaram no estacionamento serão filtrados; quando **Out** for selecionado, os veículos que saíram do estacionamento serão pesquisados.

   Ocupado ou não

   Quando **Ocupado** for selecionado, os veículos que estiverem ocupando as vagas de estacionamento alocadas à conta serão filtrados; quando **Não Ocupado** for selecionado, os veículos que não estiverem ocupando as vagas de estacionamento alocadas à conta serão pesquisados.
3. Clique em **Pesquisar** .
4. **Opcional**: No canto superior direito, clique em **Exportar** para exportar os resultados para o seu PC no formato Excel.

9.7 Gerar Relatório de Análise de Veículo

Para câmeras ANPR, você pode gerar um relatório para mostrar o número de veículos que passam

detectados por câmeras especificadas durante períodos de tempo especificados.

Passos

1. No painel de navegação esquerdo, selecione **Pesquisa e análise de veículos que passam** → **Análise de veículos** .
2. Selecione a(s) câmera(s) para este relatório.
   1) Clique no campo Câmera para abrir o painel Selecionar Câmera.
   2) No painel, selecione um site na lista suspensa para mostrar suas áreas.
   3) Clique em uma área para mostrar suas câmeras que suportam a função ANPR.

   Observação

   Somente as câmeras ANPN online serão exibidas aqui.

   4) Verifique a(s) câmera(s) para análise.

   Observação

   Não é possível selecionar mais de 20 câmeras ANPR para análise única.

   5) Clique em qualquer lugar fora do painel Selecionar câmera para finalizar a seleção da(s) câmera(s).
3. Selecione o tipo de relatório como relatório diário, relatório semanal, relatório mensal ou relatório anual, ou personalize o intervalo de tempo para um relatório.

   Relatório diário

   O relatório diário mostra dados diariamente. A plataforma calculará o número de veículos em cada hora de um dia.

   Relatório semanal / Relatório mensal / Relatório anual

   Em comparação com o relatório diário, o relatório semanal, o relatório mensal e o relatório anual podem consumir menos tempo, já que não devem ser enviados todos os dias. A plataforma calcula o número de veículos em cada dia da semana, em cada dia de um mês e em cada mês de um ano.

   Intervalo de tempo personalizado

   Personalize os dias no relatório para analisar o número de veículos em cada dia ou em cada mês do intervalo de tempo personalizado.
4. Defina o tempo ou um período de tempo para análise.
5. Clique em **Gerar relatório** .
   As estatísticas de veículos que passam detectados por todas as câmeras selecionadas são exibidas no painel direito.

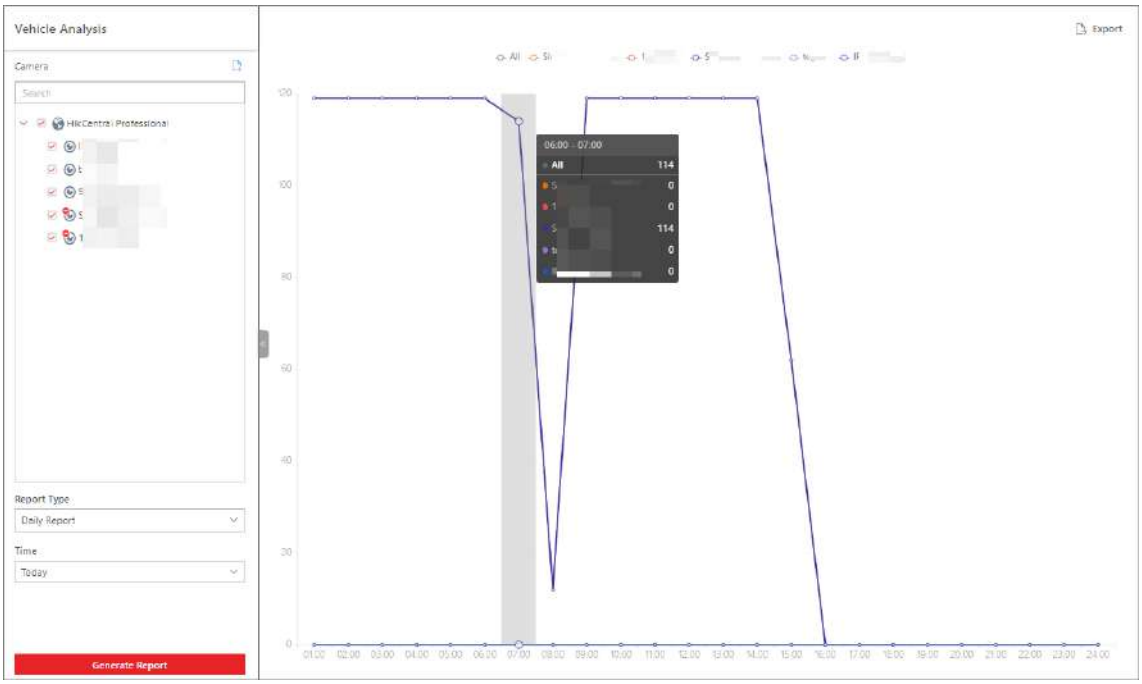


Figura 9-1 Relatório de análise do veículo

6. **Opcional**: Exporte o relatório gerado para o PC local.

Observação

Consulte ***Definir parâmetros gerais*** para obter detalhes sobre como definir o caminho de salvamento para relatórios exportados.

1) Clique em **Exportar** no canto superior direito do painel de relatórios.

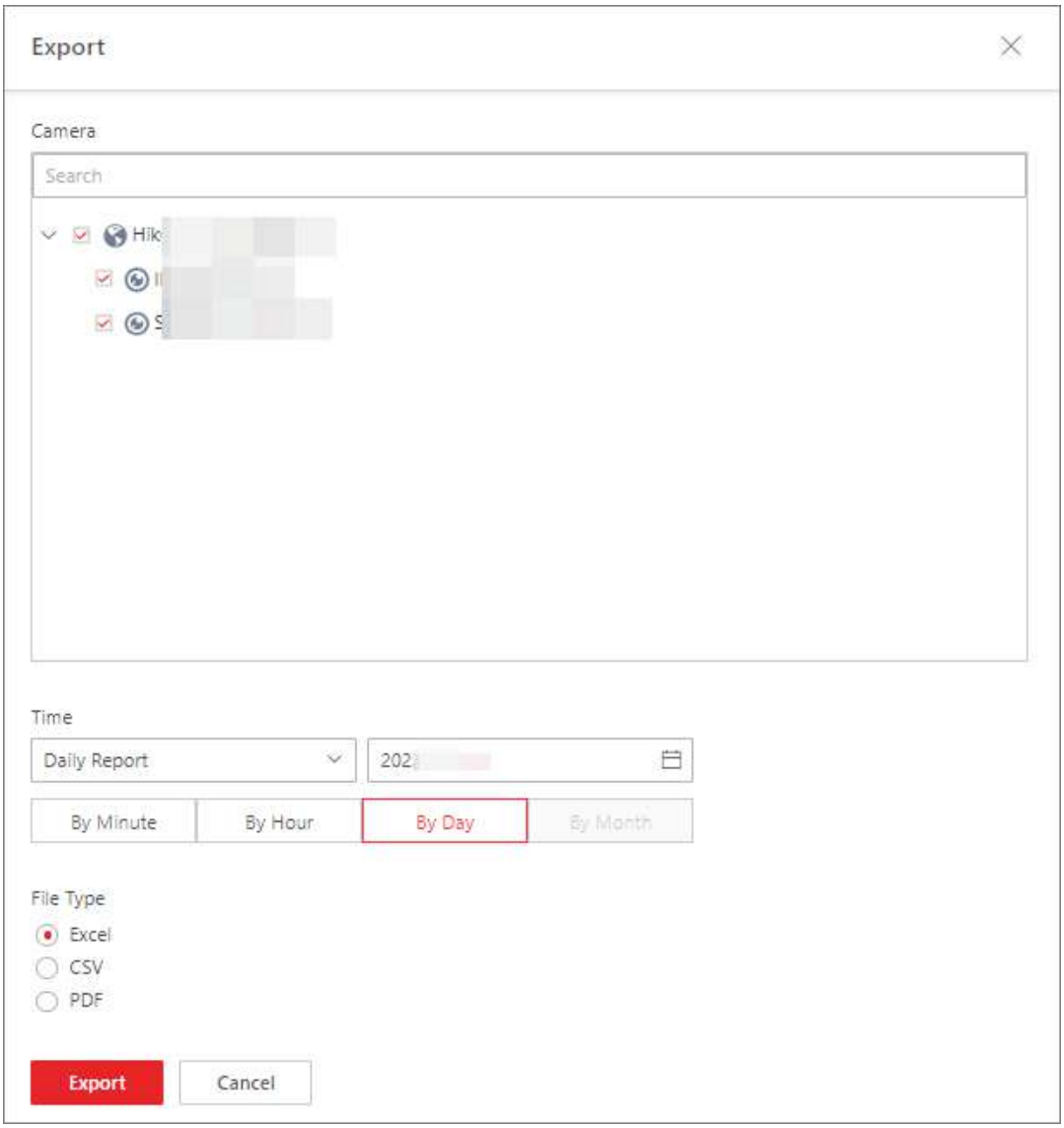


Figura 9-2 Relatório de análise de veículo de exportação

2) **Opcional**: Selecione a(s) câmera(s) contida(s) no relatório e altere o tipo ou a hora do relatório.
3) Selecione um período de tempo mais curto para visualizar dados mais detalhados de cada câmera.

Por minuto

O relatório exportado mostra os dados detalhados de cada minuto para cada câmera (se a câmera tiver sido configurada para relatar dados de análise do veículo para a plataforma a cada minuto). Esta opção está disponível apenas para o relatório diário.

Por hora

O relatório exportado mostra os dados detalhados de cada hora para cada câmera. Esta opção está disponível para o relatório diário/semanal/mensal/de intervalo personalizado.

Por dia

O relatório exportado mostra os dados detalhados de cada dia para cada câmera. Esta opção está disponível para todos os tipos de relatórios.

Por mês

O relatório exportado mostra os dados detalhados de cada mês para cada câmera. Esta opção está disponível para o relatório mensal/anual.

4) Defina o formato do arquivo exportado para **Excel** , **CSV** ou **PDF** .
5) Clique em **Exportar** para iniciar a exportação do relatório.

O progresso da exportação será exibido na Central de Tarefas.

Capítulo 10 Monitoramento de Realidade Aumentada (RA)

Realidade aumentada (RA) é uma experiência interativa de um ambiente do mundo real onde os objetos que residem no mundo real são aprimorados por informações perceptivas geradas por computador, às vezes por meio de múltiplas modalidades sensoriais.

AR fornece agregação das informações coletadas de diferentes câmeras, com base em tecnologias incluindo AR e inteligência artificial. Você pode focar nas informações de forma visual e tridimensional, que combina os alvos de monitoramento, instalações estáticas, vídeos e imagens. O mapa AR também suporta a exibição de vídeo no modo picture-in-picture e fornece conveniência para análise de informações.

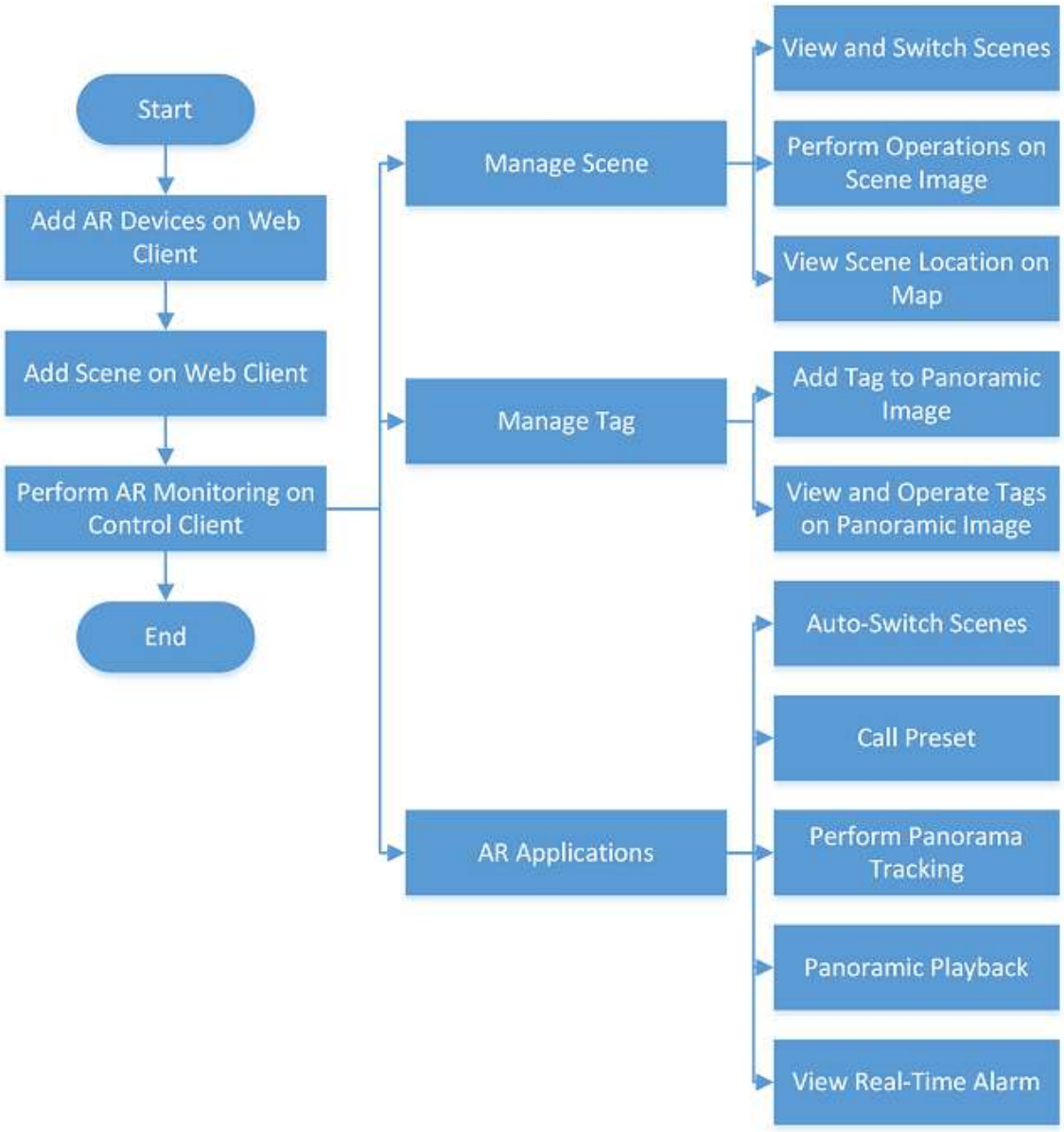


Figura 10-1 Fluxograma de monitoramento de AR

10.1 Introdução à Janela Principal

Depois de configurar cenas no Web Client, você pode executar operações, incluindo gerenciar cenas, gerenciar tags, executar rastreamento panorâmico e visualizar alarmes em tempo real. Nesta seção, você pode executar as seguintes operações.

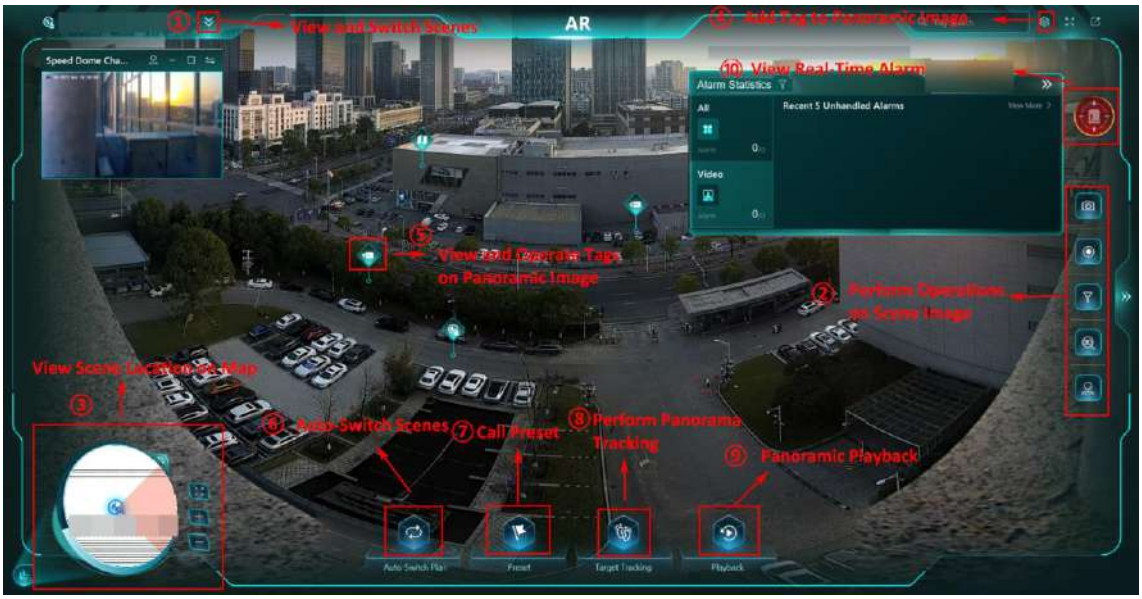


Figura 10-2 Orientação da janela principal

Operação	Descrição
① Ver e alternar cenas	Para obter detalhes, consulte ***Exibir e alternar cenas*** .
② Executar operações na imagem da cena	Você pode executar operações como capturar imagens, gravar vídeos e aplicar zoom 3D. Para obter detalhes, consulte ***Executar operações na imagem da cena*** .
③ Ver localização da cena no mapa	Se você definir locais de cena no mapa no Web Client, poderá visualizar locais de cena no mapa no Control Cent. Para obter detalhes, consulte ***View Scene Location on Map*** .
④ Adicionar tag à imagem panorâmica	Você pode adicionar tags de câmera, tags de cena e tags de mapa à imagem panorâmica. Para obter detalhes, consulte ***Adicionar tag à imagem panorâmica*** .
⑤ Visualizar e operar tags na imagem panorâmica	Se houver alarmes de tags, você pode clicar nas tags para obter detalhes. Para obter detalhes, consulte ***Exibir e operar tags na imagem panorâmica***
⑥ Troca automática de cenas	Você pode adicionar um plano de troca automática, para que as cenas no plano comecem a ser trocadas automaticamente. Para detalhes, consulte ***Cenas de troca automática*** .
⑦ Chamada predefinida	Você pode adicionar predefinições e predefinições de chamada. Para detalhes, consulte ***Predefinição de chamada*** .

Operação	Descrição
⑧ Executar Rastreamento de Panorama	Por meio da câmera AR e da câmera speed dome adicionadas a uma cena, você pode executar o rastreamento panorâmico. Para obter detalhes, consulte ***Executar rastreamento panorâmico*** .
⑨ Reprodução Panorâmica	Você pode executar a reprodução panorâmica. Para detalhes, consulte ***Reprodução Panorâmica*** .
⑩ Ver alarme em tempo real	Para obter detalhes, consulte ***Exibir alarmes em tempo real*** .

10.2 Gerenciamento de Cena

No gerenciamento de cenas, você pode visualizar e alternar cenas, executar operações na imagem da cena, chamar predefinições, visualizar a localização da cena no mapa e alternar cenas automaticamente.
No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Monitoramento** → **AR** para entrar no mapa AR.

10.2.1 Visualizar e Alternar Cenas

Após as cenas serem configuradas no Web Client, você pode visualizá-las no Control Client. Cada cena consiste em uma câmera da série AR PanoVu (obrigatória) e um speed dome (opcional; para rastreamento de panorama).
No canto superior esquerdo, selecione → **Todos os módulos** → **Monitoramento** → **AR** . Clique no canto superior esquerdo para visualizar a lista de cenas.

Observação

- Você só pode visualizar as cenas na área atual. Câmeras em outras áreas não são exibidas.
- Áreas sem recursos adicionais são filtradas automaticamente.
- Clique em / para exibir a lista de cenas no modo lista/miniatura.
- Para cenas que incluem uma câmera AR e speed dome, cada uma delas está no modo de tela dupla. A tela do speed dome será exibida no canto superior esquerdo.

Clique em cenas diferentes. O mapa AR será alternado para o primeiro mapa onde a cena está localizada; se a cena estiver localizada em vários mapas, incluindo o mapa GIS, o mapa GIS será exibido.

Observação

Você também pode clicar em uma cena no mapa ou no canal do speed dome e clicar em **Exibir cena** para alternar para a cena de destino.

10.2.2 Executar Operações na Imagem da Cena

Para cada cena, você pode capturar imagens, gravar vídeos, filtrar tags, executar posicionamento 3D, etc.

No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Monitoramento** → **AR** para entrar no mapa AR.

Clique à direita para exibir o menu de várias operações.

Operação	Descrição
	Capture a imagem atual. A imagem será salva no PC local.
	Clique para iniciar a gravação e clique novamente para parar a gravação. A gravação será salva no PC local.
	Clique e selecione a(s) tag(s) conforme necessário. Clique em **Confirmar** para filtrar as tags a serem exibidas.
	Clique para habilitar o posicionamento 3D. Clique em qualquer ponto na tela para visualizar a imagem ampliada do ponto ou desenhe uma área para visualizar a imagem ampliada da área selecionada no canal do speed dome.
	Clique e use o botão de direção ( ) para ajustar a direção da câmera PTZ e aumentar/diminuir o zoom na cena conforme necessário.

10.2.3 Ver Localização da Cena no Mapa

No painel no canto inferior esquerdo, você pode ver a localização da cena atual no mapa bidimensional.

No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Monitoramento** → **AR** para entrar no mapa AR.

Observação

Se a cena estiver localizada em vários mapas, incluindo o mapa GIS, o mapa GIS será exibido; se a cena estiver localizada em vários mapas, excluindo o mapa GIS, o primeiro mapa onde a cena estiver localizada será exibido; se nenhum mapa tiver sido configurado para a cena, este painel não será expandido por padrão.

Você pode clicar para ocultar este painel; você também pode clicar e arrastar no canto superior direito do painel para ajustar o tamanho do painel.

Observação

- Quando houver várias cenas no mapa, você pode clicar em cenas diferentes para alternar a visualização ao vivo da cena.

- Ao alterar a direção do PTZ, a direção da cena no painel será alterada automaticamente.

Você pode clicar em / para aumentar/diminuir o zoom ou clicar para entrar no modo de tela cheia.

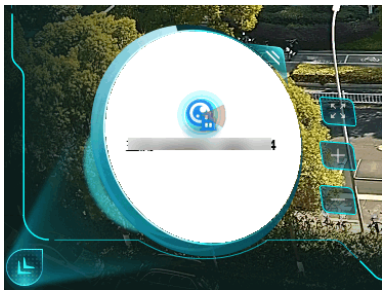


Figura 10-3 Painel de localização de cena

10.3 Gerenciamento de Tags

Para monitorar melhor os eventos e lidar com alarmes prontamente, você pode adicionar tags de recursos, ou seja, recursos, cenas, mapas, partições (áreas) e entradas e saídas, a uma imagem panorâmica. Após configurar essas tags de recursos, você pode visualizá-las e operá-las diretamente na imagem panorâmica.

10.3.1 Adicionar Tag à Imagem Panorâmica

Você pode adicionar tags à imagem panorâmica para recursos, como recursos, cenas, mapas, partições (áreas) e entradas e saídas.

Antes de começar

Certifique-se de que haja uma cena configurada via Web Client.

Passos

1. No canto superior esquerdo, selecione → **Todos os módulos** → **Monitoramento** → **AR** .
2. Clique no canto superior esquerdo e selecione uma cena na lista suspensa.
3. Clique no canto superior direito e clique em **Configuração** ao lado de **Configuração de tag** .
4. Selecione o tipo de recurso a ser adicionado.
5. Selecione a área onde o recurso está localizado na lista suspensa.

Observação

Áreas sem recursos adicionais são filtradas automaticamente.

6. Passe o mouse sobre o recurso e clique em ou arraste-o para a imagem.

Observação

Você pode pesquisar e filtrar recursos inserindo palavras-chave na caixa de pesquisa.

7. Configure as informações relevantes para a tag de recurso, como nome, tipo e grupo, e clique em **OK** para adicionar a tag.
8. Opcional: repita as quatro etapas acima para continuar adicionando mais tags, se necessário.
9. Opcional: se necessário, clique em uma tag na imagem para editar suas informações, excluí-la da imagem panorâmica ou adicioná-la aos favoritos.
10. Clique em **Concluir** abaixo do painel Adicionar tag para finalizar a adição da(s) tag(s).
11. **Opcional**: execute as seguintes operações conforme necessário.

Pesquisar por Tags	No canto superior direito, insira palavra(s)-chave na caixa de pesquisa ao lado de para pesquisar tags adicionadas. Você também pode especificar um tipo de tag para pesquisar apenas tags de um tipo específico.
Visualizar e operar tags	Você pode visualizar e operar uma tag na imagem panorâmica clicando nela. Para obter detalhes, consulte ***View and Operate Tags on Panoramic Image*** .

10.3.2 Visualizar e Operar Tags em Imagem Panorâmica

Depois de adicionar tags de recursos, você pode visualizá-las e operá-las diretamente na imagem panorâmica, como executar operações de controle da câmera, abrir o mapa, visualizar a cena e verificar detalhes do evento.

Observação

Certifique-se de ter adicionado tags de recurso à imagem panorâmica. Para obter detalhes, consulte ***Adicionar tag à imagem panorâmica*** .

Para ir para o módulo AR Map, selecione → **All Modules** → **Monitoring** → **AR** . Clique no canto superior esquerdo e selecione uma cena na lista suspensa. As operações que você pode executar diferem pelo tipo de tag de recurso.

Etiquetas de câmera

Para câmeras adicionadas à imagem panorâmica, você pode clicar em uma tag de câmera e executar operações básicas de controle de câmera na janela de visualização ao vivo, como assistir ao vídeo ao vivo no modo de tela cheia, capturar imagens, gravar vídeo, controlar áudio ligado/desligado, zoom digital, alternar fluxo, controlar PTZ, alternar para reprodução instantânea, iniciar áudio bidirecional e adicionar tags. Se um evento como comparação de imagem de rosto ou comparação de veículo for detectado no momento, você também poderá visualizar os detalhes do evento e os detalhes correspondentes da pessoa/veículo no painel.
Se o status da câmera for Sem alarme no momento, você pode executar controles de armamento para ela, configurá-la para ignorar todos os alarmes a partir de agora e visualizar o histórico de alarmes conforme necessário.
Se um alarme for disparado no momento, a etiqueta da câmera ficará vermelha e você poderá

clicar nela para visualizar informações detalhadas do alarme e a imagem capturada, além de executar operações como confirmar o alarme, encaminhá-lo, enviar e-mails de alarme e executar o controle de saída do alarme.

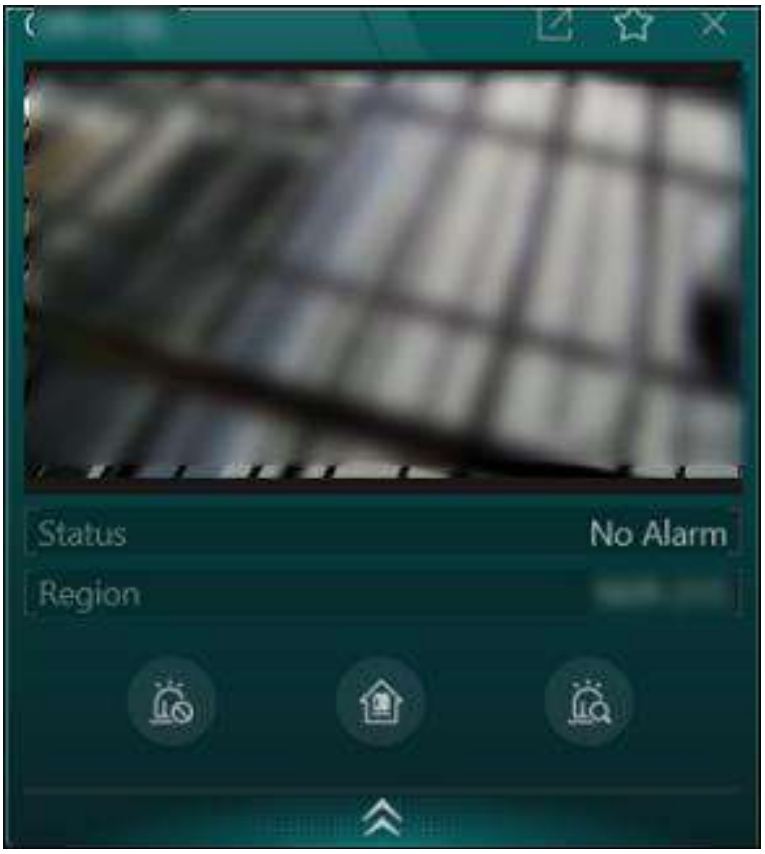


Figura 10-4 Painel de operação da etiqueta da câmera

Tags de cena

Para cenas adicionadas à imagem panorâmica, você pode clicar em uma tag de cena e selecionar **Exibir cena** para abrir a cena correspondente.

Tags do mapa

Para mapas adicionados à imagem panorâmica, você pode clicar em uma tag de mapa para abrir a pré-visualização do mapa e clicar para exibir o mapa em tela cheia, se necessário. No mapa, você pode pesquisar e visualizar detalhes sobre os pontos de acesso que foram adicionados ao mapa por meio do Web Client.

Tags de transmissão

Você pode clicar para transmitir ou iniciar o interfone.

Etiquetas de entrada e saída

Você pode visualizar informações sobre o estacionamento e o número de veículos que entram e saem.

Etiquetas de partição (área)

Você pode armar, desarmar remotamente, armar no modo local e desarmar uma partição (área).
Você pode visualizar zonas e saídas de alarme de uma partição (área).
Você pode passar o mouse sobre a zona para executar operações: ignorar/restaurar desvio e armar/desarmar.
Você pode visualizar os 5 alarmes mais recentes.

Etiquetas de porta

Você pode definir as portas para os seguintes status: permanecer abertas, permanecer fechadas, abertas, fechadas.
Você pode visualizar os 5 alarmes mais recentes.
Se houver um evento de acesso, você poderá visualizar informações pessoais relacionadas ao evento.

10.4 Aplicações RA

Você pode usar vários aplicativos de RA, como rastreamento panorâmico de alvos e monitoramento de alarmes/eventos em tempo real, para entender melhor o que está acontecendo em um local e lidar com situações a tempo.

10.4.1 Troca Automática de Cenas

Você pode gerenciar a troca automática de cenas, incluindo as cenas a serem assistidas, a ordem de troca automática entre diferentes cenas e o intervalo de troca para cada cena.

Passos

1. No canto superior esquerdo, selecione → **Todos os módulos** → **Monitoramento** → **AR** .
2. Clique na parte inferior para abrir o painel de troca automática de plano.
   Você pode ver a lista de cenas.
3. Clique em **Adicionar** para entrar na página Adicionar plano de troca automática.

Figura 10-5 Adicionar plano de troca automática

4. Edite o nome do plano conforme necessário.

Observação

O plano é nomeado com a hora atual por padrão.

5. Selecione a duração de cada cena na lista suspensa.
6. Clique em **Adicionar** em **Cenas no Plano** e selecione cena(s) na área atual. Clique em **Salvar** para adicionar cenas ao plano.

Observação

Clique em / para exibir a lista de cenas no modo lista/miniatura.

7. Clique em **Salvar** para salvar o plano.
8. Após terminar de adicionar o(s) plano(s), você pode executar as seguintes operações.

Inicie a troca automática	Clique para iniciar a troca automática de plano.
Editar a troca automática	Clique para editar o plano de troca automática.
Excluir a troca automática	Clique para excluir o plano de troca automática.

10.4.2 Predefinição de Chamada

Você pode definir predefinições para uma câmera PTZ e chamá-las para realizar tarefas de monitoramento com maior eficiência.

Passos

1. No canto superior esquerdo, selecione → **Todos os módulos** → **Monitoramento** → **AR** .
2. Clique no canto superior esquerdo e selecione uma cena (vinculada a uma câmera PTZ) na lista suspensa para iniciar a visualização ao vivo.
3. Clique para habilitar o controle PTZ e use o botão de direção ( ) para ajustar a direção da câmera PTZ e aumentar/diminuir o zoom na cena conforme necessário.

Figura 10-6 Controle PTZ

4. Clique em **Predefinições** na parte inferior para exibir a lista de predefinições.

Figura 10-7 Painel de predefinições

5. Salve o ângulo de visão atual como uma predefinição.
   - Clique em **Adicionar** para mostrar o painel Adicionar predefinição, insira o nome e o número da predefinição e clique em **OK** .
   - Passe o mouse sobre uma predefinição não configurada, clique em , defina o nome da predefinição e clique em **OK** .
6. Passe o mouse sobre uma predefinição configurada e clique para chamá-la.
7. **Opcional**: Você também pode executar operações em predefinições configuradas.

Operação	Descrição
Editar predefinição	Passe o mouse sobre uma predefinição, clique e edite seu nome.
Excluir predefinição	Passe o mouse sobre uma predefinição e clique para excluí-la.
Pesquisar por Predefinições	Insira palavras-chave na caixa de pesquisa para procurar predefinições de destino.

10.4.3 Executar Rastreamento Panorâmico

Por meio da câmera AR e do domo de velocidade adicionados a uma cena, você pode realizar o rastreamento panorâmico de um alvo em movimento simplesmente clicando na imagem panorâmica.

Antes de começar

Certifique-se de que haja uma cena configurada via Web Client.

Passos

1. No canto superior esquerdo, selecione → **Todos os módulos** → **Monitoramento** → **AR** .
2. Clique no canto superior esquerdo e selecione uma cena na lista suspensa.

Observação

- Por padrão, a visualização da câmera AR é exibida na janela maior (ou seja, tela cheia) e a visualização do speed dome é exibida na janela menor no canto superior esquerdo. Você pode clicar para alternar as visualizações das duas câmeras.
- Por meio da barra de ferramentas da janela de visualização menor, você pode ativar o controle PTZ da janela, aumentar/diminuir a janela ou ocultá-la conforme necessário.

3. Clique em **Rastreamento de Alvo** na parte inferior da página para entrar no modo de rastreamento panorâmico.
4. Na imagem panorâmica, clique em um alvo ou desenhe uma área para iniciar a vinculação inteligente.
   O domo de velocidade começará a rastrear o alvo em movimento e ajustará sua posição adequadamente.

10.4.4 Reprodução Panorâmica

Você pode visualizar as filmagens de vídeo gravadas das câmeras da série PanoVu. Para câmeras AR PanoVu, as tags serão exibidas durante a reprodução e, portanto, você também pode visualizar os vídeos gravados das câmeras vinculadas a essas tags.

Passos

1. No canto superior esquerdo, selecione → **Todos os módulos** → **Monitoramento** → **AR** .
2. Selecione uma cena na lista suspensa.
3. Defina a hora de início e de término e clique em **OK** para começar a procurar as imagens de vídeo da câmera de RA durante esse período.
   A reprodução da cena pela câmera de RA começará se houver filmagem naquele período.
4. Controle a reprodução através da barra de ferramentas de reprodução que aparece na parte inferior, se necessário.

Tabela 10-1 Barra de ferramentas de reprodução

Ícone	Nome	Descrição
/	Reproduzir/Pausar	Iniciar ou pausar a reprodução.

Ícone	Nome	Descrição
	Reprodução de quadro único	Reproduza a filmagem por quadro.
	Controle de velocidade de reprodução	Defina a velocidade de reprodução.
	Linha do tempo de redução/aumento	Encolha ou aumente a linha do tempo para acessar pontos de tempo detalhados em miniatura. Você pode clicar na linha do tempo para reproduzir o vídeo no ponto de tempo preciso.

5. **Opcional**: alterne para reprodução de outras câmeras ou cenas.
   1) Clique na caixa de pesquisa de tags na parte superior da janela.
   2) Selecione uma câmera ou uma cena da lista.
   3) Clique em uma câmera ou cena para iniciar a reprodução.
   A reprodução da câmera/cena selecionada será iniciada.

10.4.5 Exibir Alarmes em Tempo Real

Por meio do painel Estatísticas de alarmes, você pode visualizar as estatísticas gerais de alarmes/eventos de uma determinada cena em tempo real e os detalhes de alarmes não tratados e eventos de correspondência de rosto/veículo, além de localizar onde um alarme/evento ocorre na imagem panorâmica.

Observação

Certifique-se de ter adicionado tags de câmera à imagem panorâmica da cena. Para obter detalhes, consulte ***Adicionar tag à imagem panorâmica*** .

No canto superior esquerdo, selecione → **Todos os módulos** → **Monitoramento** → **AR** .
Clique no canto superior esquerdo e selecione uma cena na lista suspensa.
À direita, clique para abrir o painel Estatísticas de alarme.

Observação

O ícone só ficará vermelho se houver alarmes não tratados no momento.

Para alarmes, você pode verificar os 5 alarmes não manipulados mais recentes em uma lista e visualizar informações detalhadas de um alarme clicando nele. Além de visualizar os detalhes do alarme e a imagem capturada na janela Informações do Alarme, você também pode executar operações como reconhecer o alarme, encaminhá-lo, enviar e-mails de alarme e executar o controle de saída do alarme. Depois que um alarme for reconhecido, ele não aparecerá mais na lista de alarmes não manipulados no painel Estatísticas do Alarme.
Você também pode filtrar esses alarmes por tipo (por exemplo, evento VCA, evento de detecção de rosto, evento de manutenção de câmera, etc.) clicando em , você pode clicar ao lado do número de câmeras com alarmes acionados para mostrar apenas as tags de câmera correspondentes na imagem panorâmica, ou você pode clicar no menu à esquerda do painel para visualizar os alarmes relacionados a cada módulo.
Você pode clicar em **Exibir mais** para visualizar/pesquisar mais alarmes. Para obter detalhes, consulte ***Pesquisar logs de eventos e alarmes*** .

Capítulo 11 Gerenciamento de Mapas

Após configurar corretamente as definições do mapa por meio do Web Client e habilitar a função de mapa no módulo Monitoring, você pode visualizar e gerenciar o mapa, como aumentar ou diminuir o zoom do mapa, localizar os recursos no mapa. Você pode visualizar e operar os recursos adicionados no mapa, como obter a visualização ao vivo e a reprodução das câmeras, UVSSs e portas, definir o controle de armação para câmeras, entradas de alarme, UVSSs e portas, e assim por diante.

Observação

- Se o mapa GIS não for exibido corretamente, todas as miniaturas de E-map do site atual e do Site Remoto serão exibidas. Clique em um E-map para visualizar os detalhes.
- Se você habilitar a função de mapa GIS do Sistema Central via Web Client, você entra no mapa GIS configurado. Todas as miniaturas de E-map do site atual e do Site Remoto são exibidas sob o mapa GIS. Clique em um E-map para visualizar os detalhes.

11.1 Visualizar e Operar o Hot Spot

Você pode visualizar os locais de pontos de acesso, incluindo câmeras, entradas de alarme, saídas de alarme, pontos de acesso, radares, sites, UVSS, etc. no mapa. Além disso, você pode definir o controle de armamento e visualizar os alarmes históricos de cenários de monitoramento por meio dos pontos de acesso. Você pode visualizar informações de latitude e longitude e operações disponíveis de um determinado recurso passando o mouse sobre um recurso no mapa GIS também.

Antes de começar

Configure as configurações do mapa por meio do Web Client. Para obter detalhes, consulte *o Manual do Usuário do HikCentral Professional Web Client* .

Passos

1. No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Monitoramento** → **Monitoramento** .
2. Selecione uma área à esquerda e clique duas vezes em Map.
3. Selecione um mapa para entrar no mapa.
4. Opcional: Execute as seguintes operações no mapa.

Filtrar recurso no mapa	Clique e marque o(s) tipo(s) de recurso conforme desejado.
Selecione vários recursos	Clique e desenhe um retângulo no mapa para selecionar vários recursos.

Arraste o(s) recurso(s) no mapa para exibir	Selecione um ou vários recursos no mapa e arraste-os para a janela de exibição no Live View ou no Playback.
Exibição em tempo real de comparação de imagens faciais/controle de acesso/lista de veículos	Clique em **Visualização ao vivo** e selecione o(s) item(ns) para exibir a imagem do rosto capturada em tempo real, o evento de acesso e a lista de veículos no mapa.
Mais ferramentas	: Adicione um rótulo no mapa. :Capture uma imagem. : Imprima o mapa atual. **2D/3D** : Alterna a dimensão de exibição do mapa. Search : Pesquise um ponto de acesso ou local no mapa.
Exibir mapa no Smart Wall	Clique para exibir o mapa no smart wall. Para detalhes, veja ***Exibir Mapa no Smart Wall*** .

5. Clique no ponto de acesso para abrir a caixa de diálogo que exibe suas funções relacionadas.

Observação

- Se houver um alarme disparado no ponto de acesso, o ícone do ponto de acesso ficará em modo de alarme vermelho . Clique no ícone vermelho e você poderá visualizar as informações detalhadas do alarme.
- Clique em dados do estacionamento, um painel de detalhes do estacionamento aparecerá. Você pode visualizar informações detalhadas do estacionamento, como taxa de ocupação de vagas e detalhes do andar do estacionamento.

6. Opere no diálogo.

Armar ou desarmar ponto de acesso	Você pode armar ou desarmar os pontos quentes por meio da função de controle de armar. Após armar o dispositivo, o Control Client atual pode receber as informações de alarme disparadas do ponto quente. Clique em um ponto de acesso para abrir o diálogo que exibe suas funções relacionadas. No diálogo, clique em **Arm** / **Disarm** para armar/desarmar o ponto de acesso.
Exibir histórico de alarme	Quando um alarme é disparado, ele será registrado no sistema. Você pode verificar o log de histórico relacionado a um alarme, incluindo os detalhes da fonte do alarme, categoria do alarme, hora do alarme disparado, etc. Clique em um ponto de acesso para abrir a caixa de diálogo que exibe suas funções relacionadas. Na caixa de diálogo, clique para entrar na página de pesquisa de eventos e alarmes. Então você pode

pesquisar alarmes históricos do ponto de acesso. Veja ***Pesquisar por Logs de Eventos e Alarmes*** para detalhes.

Transmissão via Hot Spot

Você pode transmitir via hot spot falando em tempo real ou reproduzindo arquivos de áudio salvos.

Observação

Certifique-se de ter adicionado recursos de transmissão no mapa.

1. No mapa, clique no recurso de transmissão para visualizar detalhes como Status, Área e Comentário.
2. Clique em **Transmitir** para selecionar o modo de transmissão.
3. Selecione **Falar** ou **Reproduzir arquivo de áudio** como modo de transmissão.

   Observação

   Falar : Fale em tempo real, e o áudio será gravado e enviado para o servidor.
   Play Audio File : Reproduza os arquivos salvos no servidor. Você pode pesquisar ou selecionar um arquivo de áudio desejado para reproduzir. Você pode clicar em **Download** para baixar um arquivo de áudio selecionado, e a transmissão será mais fluente.

4. Clique em **Iniciar** .
   - Se você selecionar Falar, a transmissão começará imediatamente.
   - Se você selecionar Reproduzir arquivo de áudio, o arquivo de áudio será baixado da nuvem, se você escolher um arquivo da nuvem, ou reproduzido imediatamente, se for um arquivo local.

Figura 11-1 Ponto de acesso do braço / Exibir histórico de alarme

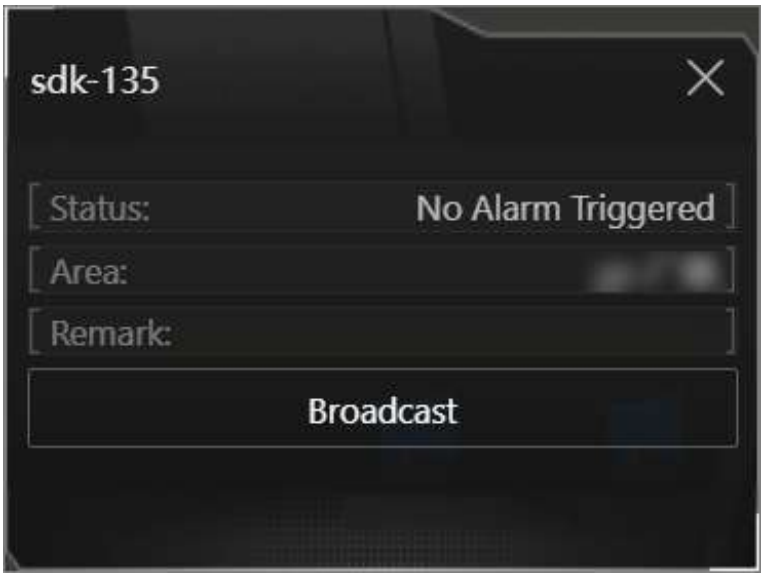


Figura 11-2 Transmissão via Hot Spot

11.2 Pré-visualização da Região Quente

A função de região quente vincula um mapa a outro mapa. Quando você adiciona um mapa a outro mapa como uma região quente, um ícone do link para o mapa adicionado é exibido no mapa principal. O mapa adicionado é chamado de mapa filho, enquanto o mapa ao qual você adiciona a

região quente é o mapa pai.

Antes de começar

Configure as configurações do mapa por meio do Web Client. Para obter detalhes, consulte *o Manual do Usuário do HikCentral Professional Web Client* .

Passos

1. No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Monitoramento** → **Monitoramento** .
2. Clique em **Selecionar mapa** no canto superior esquerdo para exibir o(s) mapa(s) de uma área.
3. Opcional: se uma área tiver vários mapas, clique em um mapa para selecioná-lo.
4. Clique em uma região quente no mapa para entrar no mapa da região quente.

Observação

Se você entrar em um mapa de área de um mapa específico, o caminho completo do mapa da região quente será exibido no canto superior esquerdo. Cada vez que você clicar em **Voltar** , ele retornará apenas ao nível anterior do mapa.

11.3 Pré-visualizar Grupo de Recursos

Durante a exibição do mapa, você pode visualizar locais e regiões dos grupos de recursos, incluindo grupo de contagem de pessoas, grupo de intertravamento de várias portas e grupo anti-passback. Você também pode executar outras operações nos recursos do grupo.

Observação

Certifique-se de ter configurado o grupo de recursos necessário e as configurações de mapa por meio do Web Client. Para obter detalhes, consulte *o Manual do Usuário do HikCentral Professional Web Client* .

- Grupo de contagem de pessoas: você pode visualizar o número em tempo real de pessoas que entraram, saíram da região ou permaneceram na região. Enquanto isso, quando um alarme é disparado na região (como quantidade de pessoas maior/menor que o limite), a região do grupo será destacada no mapa para notificar o usuário no Control Client.
- Grupo de análise de caminho: você pode visualizar o número de pessoas que passam em tempo real no módulo Monitoramento no Control Client.
- Grupo Anti-Passback: Quando um alarme anti-passback é acionado pelas portas do grupo, a região do grupo será destacada no mapa e você poderá visualizar os alarmes em tempo real acionados na região no módulo Monitoramento no Control Client.
- Grupo de intertravamento de várias portas: quando o alarme de intertravamento de várias portas é acionado pelas portas do grupo, a região do grupo será destacada no mapa e você poderá visualizar os alarmes em tempo real acionados na região no módulo de monitoramento no Control Client.

- Grupo de Contagem de Entradas e Saídas: Você pode visualizar o número em tempo real de pessoas que entraram, saíram da região ou permaneceram na região no módulo de Monitoramento no Control Client. Enquanto isso, quando um alarme é disparado na região (como quantidade de pessoas maior/menor que o limite), o cliente notificará o usuário destacando a região no mapa.

11.4 Exibir Alarme de Site Remoto

Se você adicionou um site remoto em um mapa GIS, você pode visualizar as informações de alarmes disparados no site remoto. Mesmo que não haja nenhum alarme disparado no momento, você também pode visualizar os alarmes históricos do site.

Antes de começar

Certifique-se de ter adicionado um site remoto no mapa GIS. Veja *o Manual do Usuário do HikCentral Professional Web Client* para detalhes.

Passos

1. No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Monitoramento** → **Monitoramento** .
2. Opcional: Selecione uma área à esquerda para mostrar seu mapa GIS.
3. Clique no ícone do site para abrir a página de detalhes do site.

Observação

Se houver alarmes não tratados disparados no site remoto, o número de alarmes não tratados será exibido no canto superior direito do ícone do site.

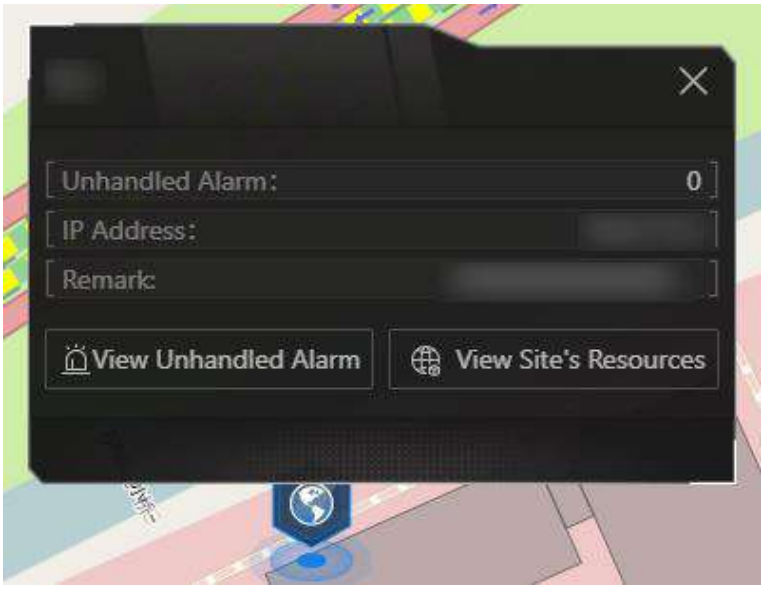


Figura 11-3 Detalhes do site

A cor do ícone do site ficará azul.

4. Clique em **Exibir alarme não tratado** para abrir a janela Alarme não tratado.
   Informações de alarme, incluindo nome do alarme, prioridade do alarme, hora de disparo, fonte do alarme, etc. são exibidas.
5. Opcional: Execute a(s) seguinte(s) operação(ões).

Filtrar alarme por prioridade	Clique na coluna Prioridade de alarme para filtrar alarmes por prioridade de alarme.
Filtrar alarme por status	Clique na coluna Status do alarme para filtrar alarmes por status de alarme.

11.5 Operar Recursos a Partir da Área Geográfica

Depois de adicionar uma área geográfica a um mapa, você pode operar em lote os recursos dentro da área.

No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Monitoramento** → **Monitoramento** .

Clique em **Selecionar mapa** no canto superior esquerdo para exibir o(s) mapa(s) de uma área.

Observação

- Quando várias regiões geográficas se sobrepõem, você pode selecionar a região geográfica na lista primeiro e depois clicar no menu.
- A operação em lote não é suportada quando há mais de 100 recursos em uma área geográfica.

Clique na área geográfica para realizar as seguintes operações.

Bloquear todos os alarmes	Clique em **Ignorar tudo** para bloquear todos os alarmes na área.
Transmissão	Clique em **Transmitir** e todos os alto-falantes IP na área começarão a transmitir e o status do ícone do dispositivo mudará.
Controle de alarme de áudio	Clique em **Controle de alarme de áudio** para iniciar alarmes sonoros.
Controle de alarme de luz estroboscópica	Clique em **Controle de alarme de luz estroboscópica** para iniciar o alarme sonoro e luminoso de todos os dispositivos na área com o recurso.
Iniciar visualização ao vivo	Clique em **Reproduzir vídeo** para iniciar a visualização ao vivo de todas as câmeras na área.

Capítulo 12 Monitoramento de estacionamento

A plataforma fornece serviço de gerenciamento de entrada e saída e pode controlar a entrada e saída dos veículos detectados de acordo com as regras de entrada e saída que você definir. Além disso, a plataforma suporta gerenciamento de taxas de estacionamento, incluindo adicionar cupons e selecionar o método de pagamento antes de abrir o portão de barreira.
Na Entrada e Saída, você pode visualizar as informações dos veículos que entram e saem do estacionamento. A plataforma pode abrir o portão de barreira do estacionamento automaticamente de acordo com as regras de entrada e saída. Se a barreira não abrir, você também pode abri-la manualmente por meio do Control Client para permitir que o veículo entre ou saia.
Na página inicial, selecione **Monitoramento** → **Estacionamento** ou selecione → **Todos os módulos** → **Monitoramento** → **Estacionamento** .

12.1 Controle de Entrada e Saída

O HikCentral Professional fornece serviço de gerenciamento de entrada e saída. Você pode definir regras de entrada e saída para entrada e saída no Web Client para que as cancelas sejam controladas pela plataforma de acordo com as regras que você definir. No Control Client, você pode controlar as cancelas de forma automática e manual, visualizar as informações detalhadas dos veículos que entram e saem do estacionamento e entregar turnos.
Existem dois modos para gerenciamento de entrada e saída: **Monitor at Center** e **Monitor at Booth** . No modo **Monitor at Center** , você pode selecionar um estacionamento para realizar monitoramento e controle; no modo **Monitor at Booth** , você pode selecionar uma entrada/saída para realizar monitoramento e controle. Você também pode visualizar as vagas de estacionamento vagas e exibir o vídeo ao vivo na parede inteligente em ambos os modos.

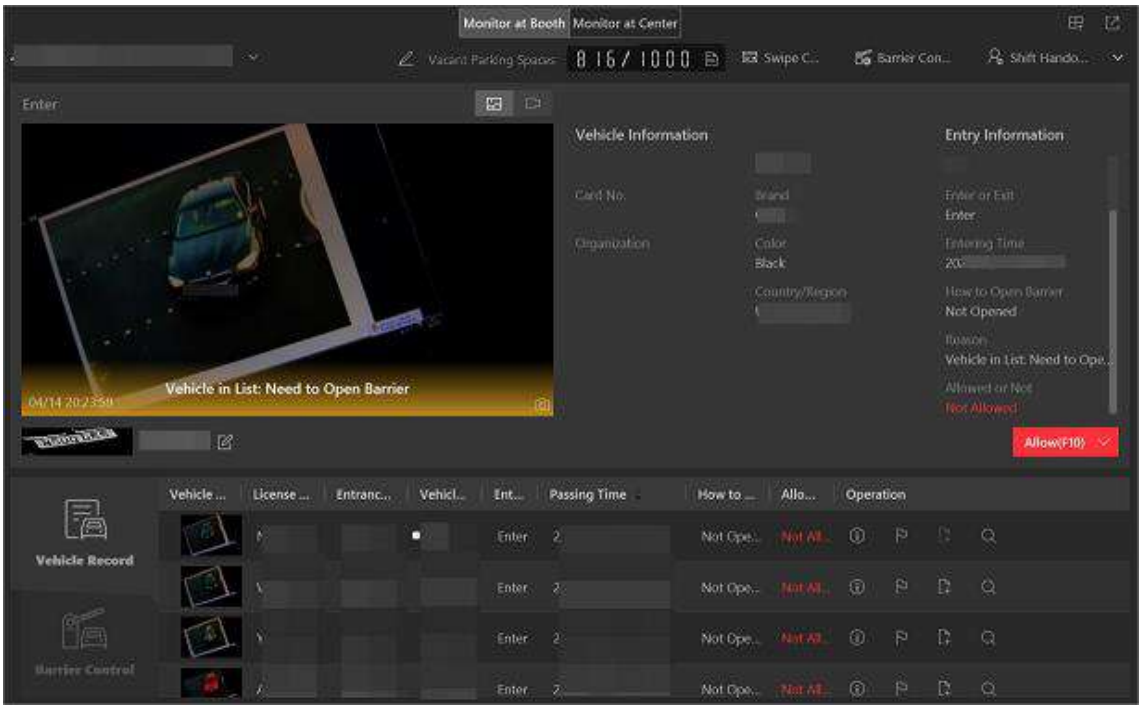


Figura 12-1 Controle de entrada e saída

12.1.1 Abrir Automaticamente a Barreira para Veículos

O veículo pode entrar ou sair do estacionamento com a cancela aberta automaticamente nas seguintes situações:

Barreira aberta automaticamente de acordo com a regra de entrada e saída

Se você tiver definido a regra de entrada e saída para os veículos na lista de veículos e definido **o Método de entrada** ou **Método de saída** como **Automático** no Web Client, e o tempo estiver dentro do período autorizado, quando o sistema detectar um veículo na faixa, a cancela será aberta automaticamente.
Você pode visualizar os detalhes do veículo, como número da placa, marca do veículo, cor, horário de entrada/saída no Control Client.

Observação

Para obter detalhes sobre como definir a regra de entrada e saída, consulte o *Manual do Usuário do HikCentral Professional Web Client* .

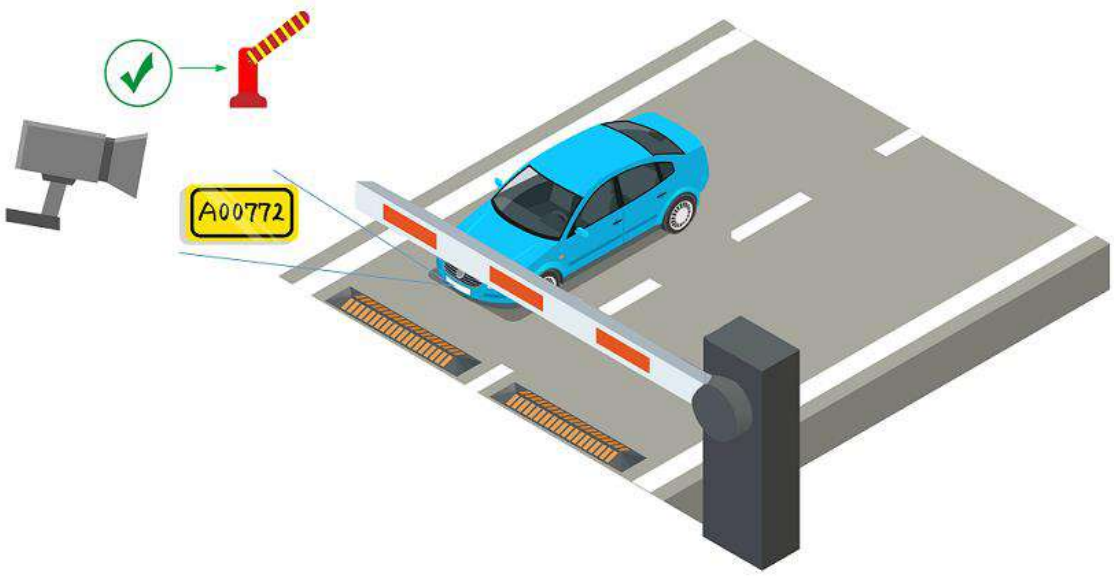


Figura 12-2 Exemplo: Barreira aberta automaticamente para veículo na lista de veículos

Barreira aberta automaticamente após passar o cartão

Se você tiver vinculado um dispositivo de controle de acesso ou dispositivo de interfone com vídeo à faixa, o proprietário do veículo na lista de veículos também poderá passar seu cartão neste dispositivo para verificar sua identidade ao entrar ou sair do estacionamento.
O sistema descobrirá as informações do veículo vinculadas a este cartão e julgará se deve abrir a cancela automaticamente de acordo com a regra de entrada e saída de sua lista de veículos. Se você tiver definido o **Método de entrada** ou **Método de saída** como **Automático** e o tempo estiver dentro do período de tempo autorizado, a cancela será aberta automaticamente.
Nessa situação, você pode usar um dispositivo de controle de acesso ou um dispositivo de vídeo porteiro em vez da câmera ANPR na entrada e na saída para verificar se o cartão está vinculado ao veículo na lista de veículos.

Observação

- Esta função só está disponível para o modo **Monitor at Booth** .
- Antes de habilitar esta função, você precisa clicar em **Passar cartão** na área superior direita e selecionar uma entrada ou saída para habilitar a passagem de cartão para a cancela.
- Certifique-se de já ter vinculado os cartões aos veículos ao adicionar veículos e definir as informações do proprietário do veículo no Web Client.
- Certifique-se de que você já vinculou um dispositivo de controle de acesso ou um dispositivo de interfone com vídeo à faixa no Web Client.
- Para obter detalhes sobre as configurações acima no Web Client, consulte o *Manual do Usuário do HikCentral Professional Web Client* .

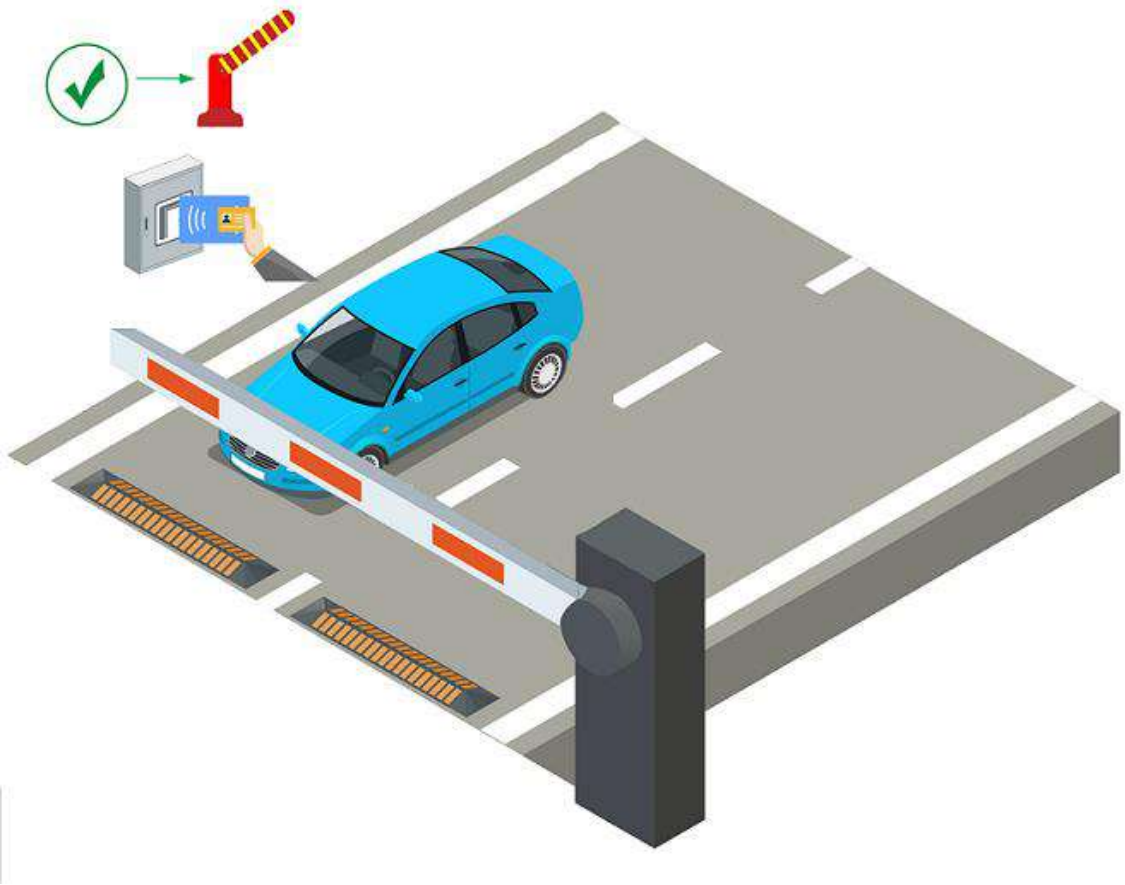


Figura 12-3 Passe o cartão para abrir a barreira

12.1.2 Abrir Manualmente a Barreira para Veículos

No Control Client, as informações dos veículos detectados nas faixas serão exibidas. Se a cancela não for aberta pelo sistema automaticamente, você pode abri-la manualmente pelo Control Client.

No canto superior esquerdo da página inicial, selecione → **Todos os módulos** → **Monitoramento** → **Estacionamento** → **Entrada e saída** para abrir a cancela manualmente nas seguintes situações:

Portão de barreira aberto para entrada

Você pode clicar no botão **Permitir** no painel Entrar para abrir a cancela na entrada.

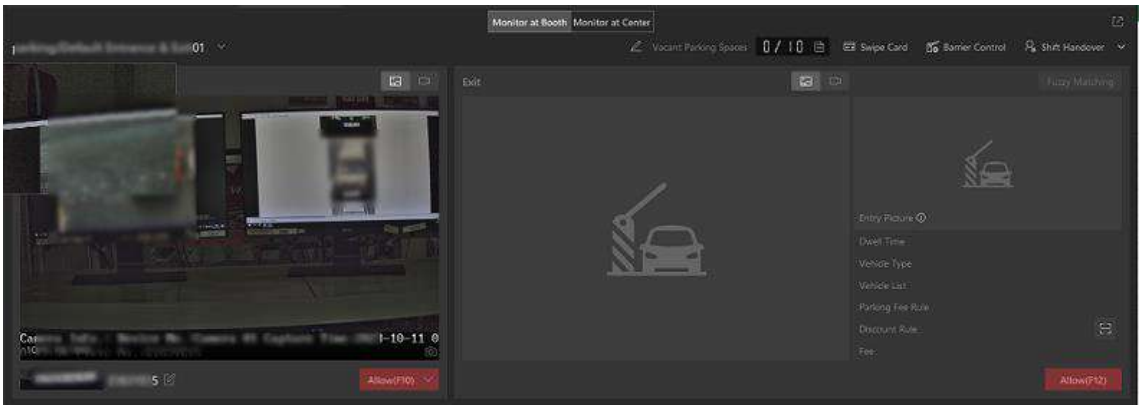


Figura 12-4 Portão de barreira de abertura com um toque

Observação

- A configuração de teclas de atalho não é suportada.
- A imagem de entrada exibida não é capturada em tempo real. É uma imagem de entrada vinculada do veículo existente.

Você também pode clicar em → **Avançado** para inserir observações sobre o veículo, se necessário (por exemplo, o motivo pelo qual você permite que este veículo entre, mesmo que ele não esteja em nenhuma lista de veículos) ou adicionar o veículo a uma lista de veículos que tenha a função **Controle de Vaga de Estacionamento habilitada** , para que este veículo ocupe uma vaga de estacionamento desta lista de veículos.

Observação

Por exemplo, se o estacionamento for compartilhado por três empresas (empresa A, B e C), quando um visitante da empresa C quiser estacionar no estacionamento, o segurança pode abrir a cancela manualmente após verificar sua identidade e selecionar a lista de veículos da empresa C. Para obter detalhes sobre como definir a função **de Controle de Vaga de Estacionamento** da lista de veículos, consulte o *Manual do Usuário do HikCentral Professional Web Client* .

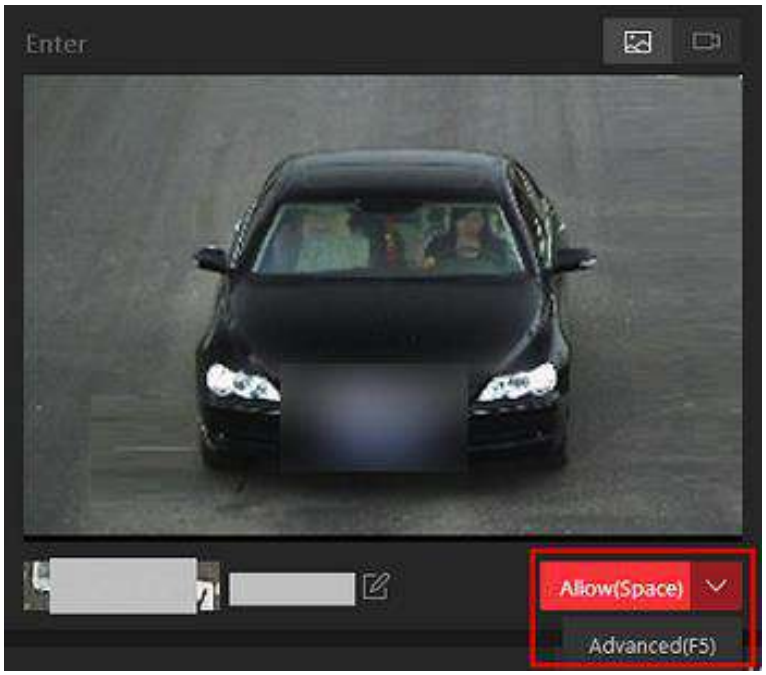


Figura 12-5 Portão de barreira de abertura avançada

Portão de barreira aberto para saída

- Para estacionamento no modo livre, você pode clicar em **Permitir** no painel Saída para abrir a cancela na faixa de saída.
- Para estacionamento no modo pago, você pode clicar em **Pago em dinheiro** ou **Pago por conta** para abrir a cancela na faixa de saída.

Observação

A configuração de teclas de atalho é suportada. Você pode definir as teclas de atalho para abrir o portão de barreira em **Sistema** → **Vídeo** → **Atalho** .

Portão de barreira aberto durante intercomunicação por vídeo

Se você tiver vinculado um dispositivo de controle de acesso ou dispositivo de interfone com vídeo à faixa, o proprietário do veículo pode pressionar um botão no painel frontal do dispositivo para enviar uma solicitação de abertura de barreira ao pessoal de segurança, e o pessoal de segurança pode falar com a pessoa por meio do Control Client, visualizar o vídeo ao vivo da câmera do dispositivo e da unidade de captura (se houver) e abrir a barreira se a identidade da pessoa for confirmada.

Observação

Antes que o Control Client receba a solicitação remota do dispositivo, você deve primeiro adicionar um alarme **do Call Center** para o estacionamento no Web Client. Para obter detalhes sobre como adicionar alarmes, consulte o *Manual do Usuário do HikCentral Professional Web Client* .

Figura 12-6 Iniciar intercomunicador de vídeo para enviar solicitação de abertura de barreira

Após pressionar o botão no painel frontal do dispositivo, uma janela será exibida no Control Client como a seguir:

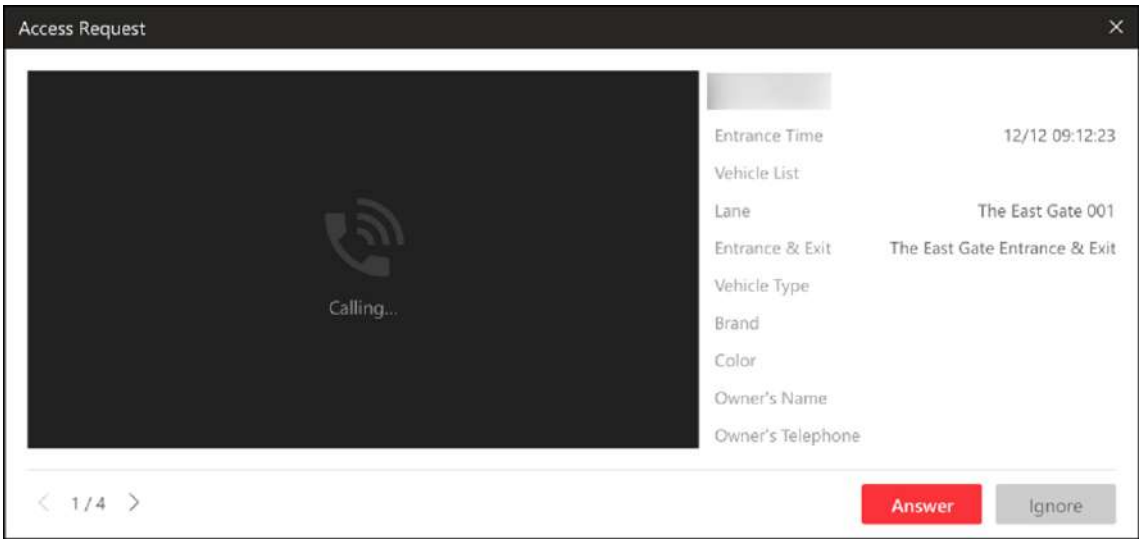


Figura 12-7 Solicitação de acesso recebida pelo cliente de controle

Você pode clicar em **Answer** para visualizar a visualização ao vivo da câmera do dispositivo, bem como a unidade de captura e iniciar uma conversa por voz com a pessoa que inicia esta solicitação. Você também pode clicar em **Ignore** para ignorar esta solicitação e fechar esta janela.

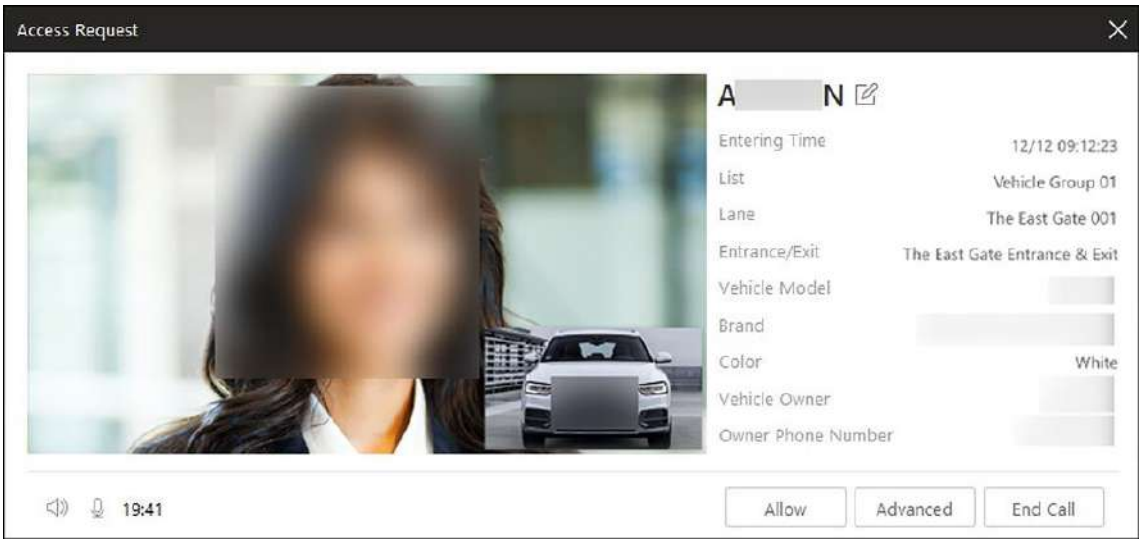


Figura 12-8 Vídeo porteiro

Durante a conversa por voz, clique em **Permitir** para abrir a cancela.
Você também pode clicar em **Avançado para inserir as informações de observação, se necessário, e selecionar uma lista de veículos que tenha a função Controle de Vaga de Estacionamento** habilitada , o que significa que este veículo ocupará uma vaga de estacionamento desta lista de veículos.
Por exemplo, se o estacionamento for compartilhado por três empresas (empresa A, B e C), quando um visitante da empresa C quiser estacionar no estacionamento, o segurança pode abrir a cancela manualmente após verificar sua identidade e selecionar a lista de veículos da empresa C.

Observação

Para obter detalhes sobre como definir a função **de Controle de Vaga de Estacionamento** da lista de veículos, consulte o *Manual do Usuário do HikCentral Professional Web Client* .

Clique em **Encerrar chamada** para encerrar a conversa de voz e fechar esta janela.

12.1.3 Número Correto da Placa

Você pode corrigir os números das placas reconhecidos pelas unidades de captura.
Você pode corrigir o número da placa dos veículos que entram ou saem do estacionamento para **Monitor no Estande** / **Monitor no Centro** .
Clique para editar o número da placa reconhecida.

12.1.4 Ver Informações do Veículo que Passa

Na página Entrada e Saída, você pode visualizar informações sobre veículos (incluindo veículos de visitantes) que entraram ou saíram do estacionamento, incluindo fotos capturadas dos veículos, números de placas, listas de veículos, direções dos veículos, tempo de passagem, permitido ou não, etc. Você também pode visualizar informações detalhadas dos veículos que passaram, marcar

veículos suspeitos, adicionar veículos que passaram a uma lista de veículos, etc.
No painel de navegação esquerdo, clique em **Entrada e Saída** e selecione uma entrada/saída na lista suspensa no canto superior esquerdo da página.

Ver informações de veículos que passam em tempo real

Após entrar na página de Entrada e Saída, o vídeo e a imagem do veículo capturados pela câmera relacionada à faixa são exibidos.

Observação

Você pode alternar entre **Monitor na Cabine** e **Monitor no Centro** .

Passe o mouse sobre a imagem para ampliá-la e clique para ver o vídeo de entrada.

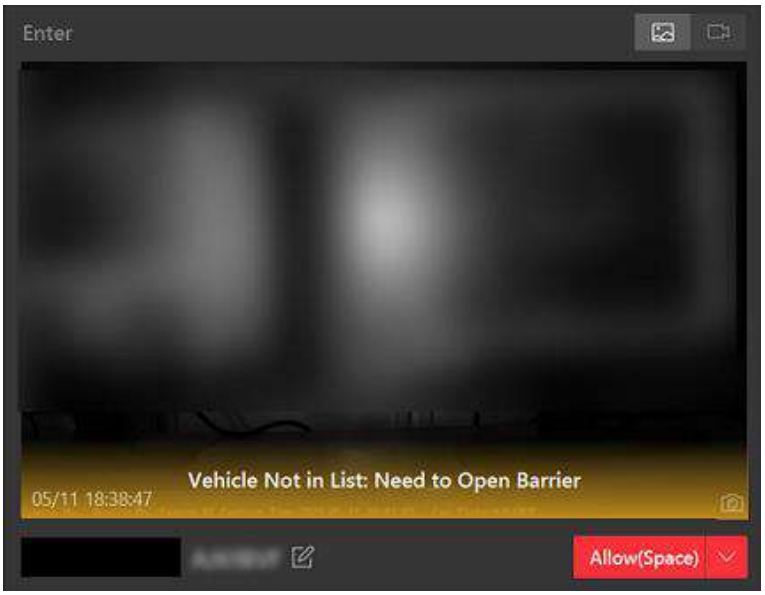


Figura 12-9 Veículo entrando

Na área **Exit** , a imagem e o vídeo do veículo saindo do estacionamento são exibidos, e a imagem correspondente capturada quando ele estava entrando no estacionamento é exibida na área **Enter** com informações relacionadas. Clique para visualizar o vídeo de saída. Se a imagem de entrada correspondente não puder ser encontrada, clique em **Fuzzy Matching** para abrir a janela Matching Result para selecionar um veículo nas imagens de entrada que são consideradas imagens de entrada de veículos semelhantes a este veículo. Depois disso, a imagem selecionada será exibida sob o botão **Fuzzy Matching** como a imagem de entrada do veículo.

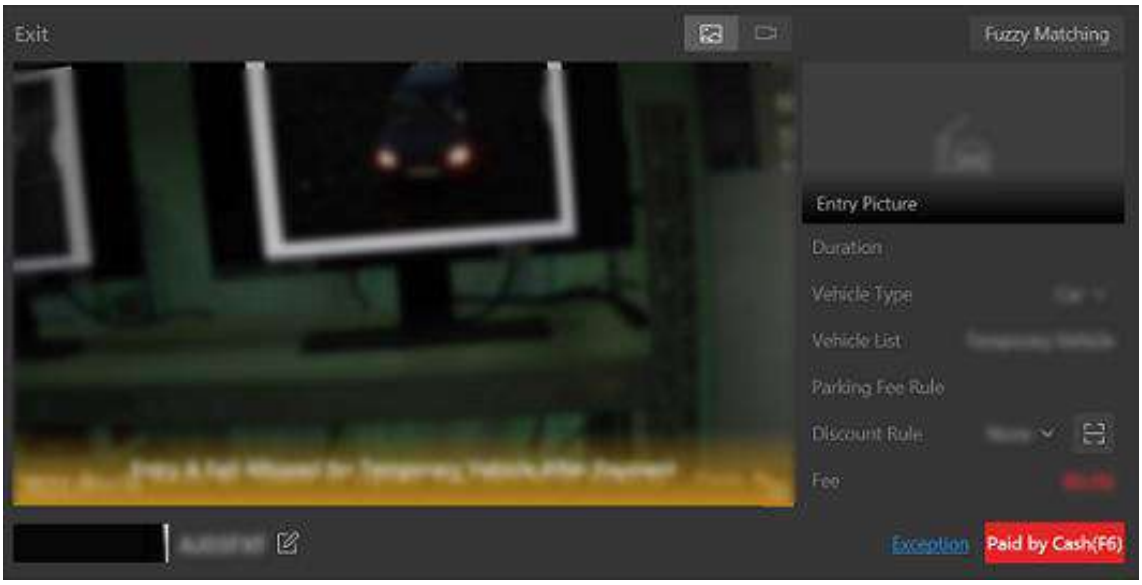


Figura 12-10 Saída do veículo

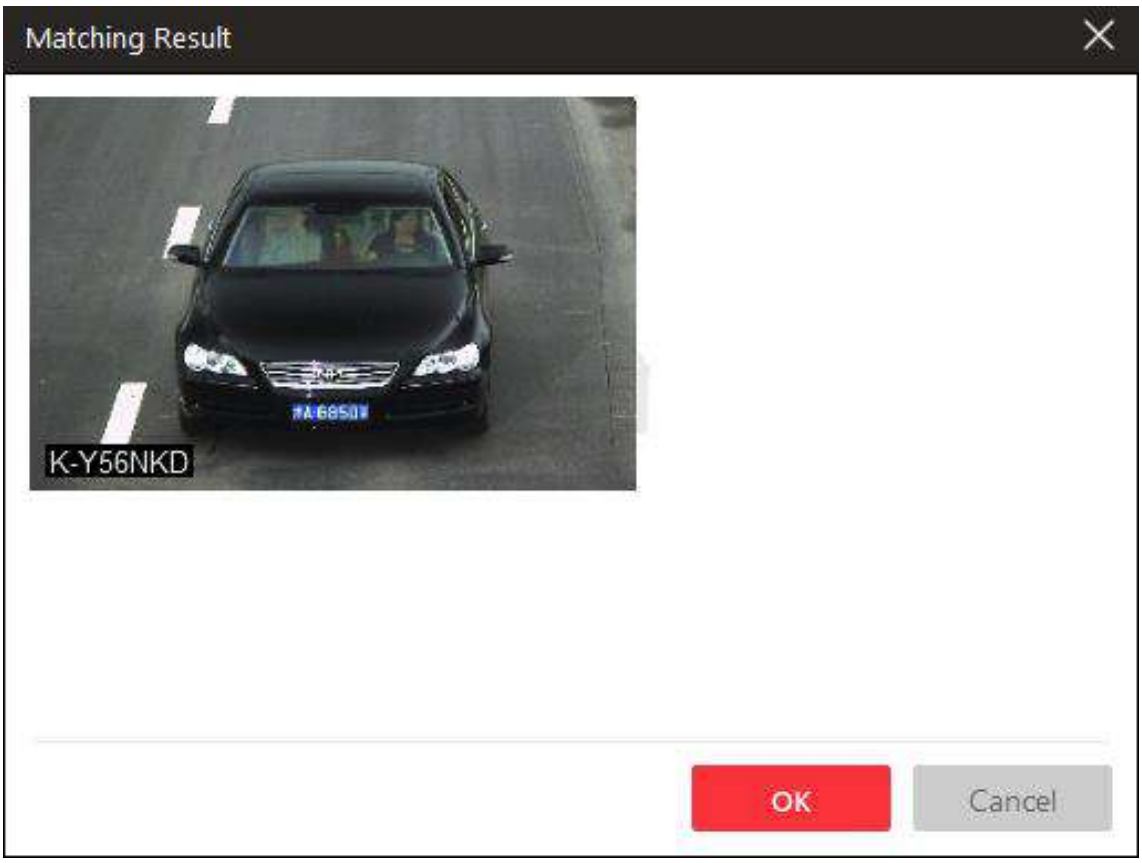


Figura 12-11 Resultado da correspondência

Ver histórico de informações do veículo que passou

Clique em **Vehicle Record** no canto inferior esquerdo para mostrar os veículos passados e suas informações. Você pode executar as seguintes operações, se necessário:

- **Ver detalhes de passagem de veículos**
  Clique para visualizar informações do veículo (informações da organização, características do veículo, etc.) e registro de entrada (faixa, direção, hora de entrada, etc.). Você também pode permitir que o veículo entre ou saia do estacionamento, visualizar o vídeo do veículo e corrigir o número da placa nesta página.
  Quando **a Correspondência de Pessoa e Placa** estiver habilitada no Web Client, uma janela para comparação de captura de rosto que mostra o nome, número de telefone, ID da equipe e organização aparecerá à direita do registro do veículo e do painel de controle da barreira.
  - **O registro mais recente** é marcado por padrão para que esta janela sempre exiba as informações mais recentes sobre o registro do veículo que passou.
  - Quando **a opção Último registro** estiver desmarcada, você poderá alternar entre diferentes registros de veículos.
  - Você também pode clicar para abrir o painel de detalhes do registro e visualizar a imagem carregada à esquerda e a imagem capturada à direita.

Observação

Se o proprietário de um veículo for um visitante, o nome do proprietário do veículo será exibido na cor azul. Clique no nome do proprietário do veículo para mostrar as informações do visitante (incluindo anfitrião, período de validade da visita, tipo de ID, ID No., número de telefone e grupo de visitantes).

- **Marcar veículo**
  Se você acha que um veículo é suspeito, clique para marcá-lo. Os veículos marcados podem ser filtrados mais tarde ao pesquisar as informações de passagem de veículos relacionados no módulo Vehicle Search.
- **Adicionar veículo à lista de veículos**
  Se o Cliente reconhecer um veículo que não foi adicionado à lista de veículos, você pode adicioná-lo à lista de veículos manualmente. Clique para adicionar o veículo a uma lista de veículos.
- **Pesquisar veículo**
  Clique para entrar na página de Pesquisa de Veículos para procurar informações relacionadas à passagem de veículos.

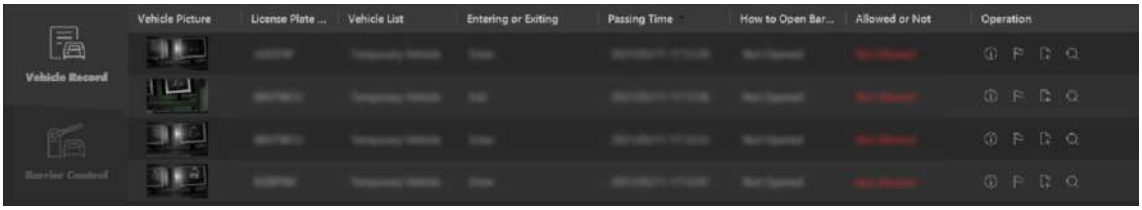


Figura 12-12 Exibir histórico de informações do veículo que passa

Você também pode permitir que veículos entrem/saiam, corrigir número de placa e controlar barreiras manualmente nesta página. Veja ***Manually Open Barrier for Vehicles*** , ***Correct License Plate Number*** e ***Manually Control Barrier*** para detalhes.

12.1.5 Controlar Manualmente a Barreira

Esta função é aplicável para diversas situações. Por exemplo, durante a hora do rush, controlar a barreira por uma unidade de captura ou passagem de cartão consome muito tempo. Nessa circunstância, o guarda pode abrir/fechar a barreira manualmente ou definir o status da barreira como permanecer aberta para que os veículos possam passar rapidamente para economizar tempo. Enquanto isso, se uma unidade de captura não reconhecer um veículo na lista de veículos, ou se não abrir a barreira passando o cartão, o guarda também pode abrir/fechar a barreira manualmente para permitir que o veículo passe.
No painel esquerdo, clique em **Entrada e Saída** para entrar na página Entrada e Saída.

Controle de portão de barreira única

- Clique em **Controle de Barreira** na área inferior esquerda da página.
- Clique em **Abrir** para abrir a barreira uma vez; clique em **Fechar** para fechar a barreira; clique em **Permanecer aberto** para que o portão da barreira permaneça aberto.
- Clique em **Bloquear** para bloquear todos os portões de barreira e clique em **Desbloquear** para desbloquear todos os portões de barreira.
- Clique em **Capturar** para capturar a imagem do veículo passando pela cancela.

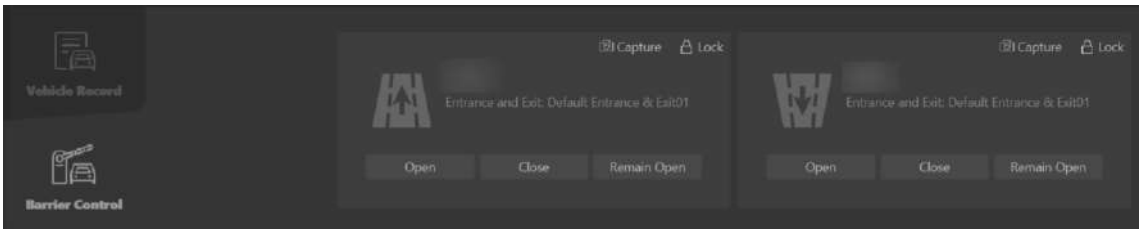


Figura 12-13 Controle manual da barreira

Controle todos os portões de barreira

Clique em **Barrier Control** ao lado de **Vacant Parking Spaces** na área superior direita da página. Você pode escolher bloquear ou desbloquear todos os portões de barreira na entrada e saída atual ou no estacionamento.

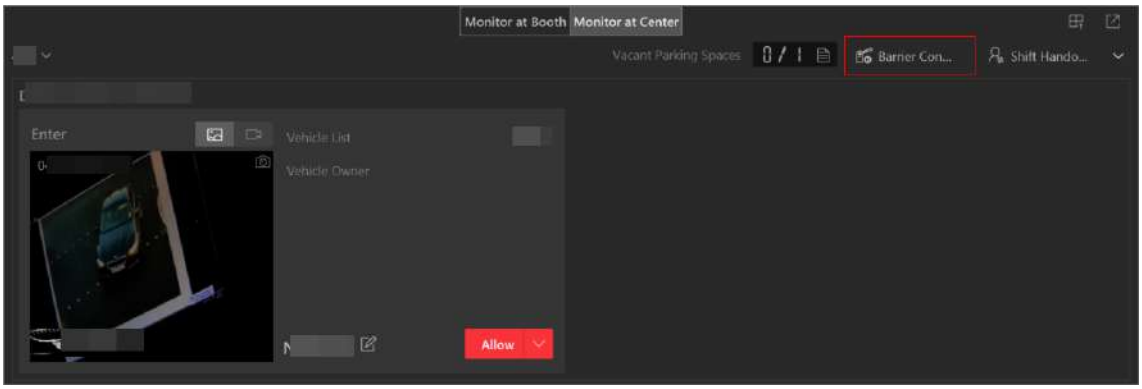


Figura 12-14 Controle todos os portões de barreira

12.1.6 Entrega de Turnos

No Control Client, você pode entregar turnos para outros operadores (ou seja, as pessoas responsáveis pelo gerenciamento de pagamentos). Antes da entrega, você precisa verificar as informações sobre o pagamento que você gerenciou. Além disso, você pode imprimir as informações de pagamento, se necessário.

Passos

1. No painel esquerdo, clique em **Entrada e Saída** para entrar na página Entrada e Saída.
2. Na área superior direita, clique em **Transferência de turno** .
   A janela Visão geral do pagamento será exibida.

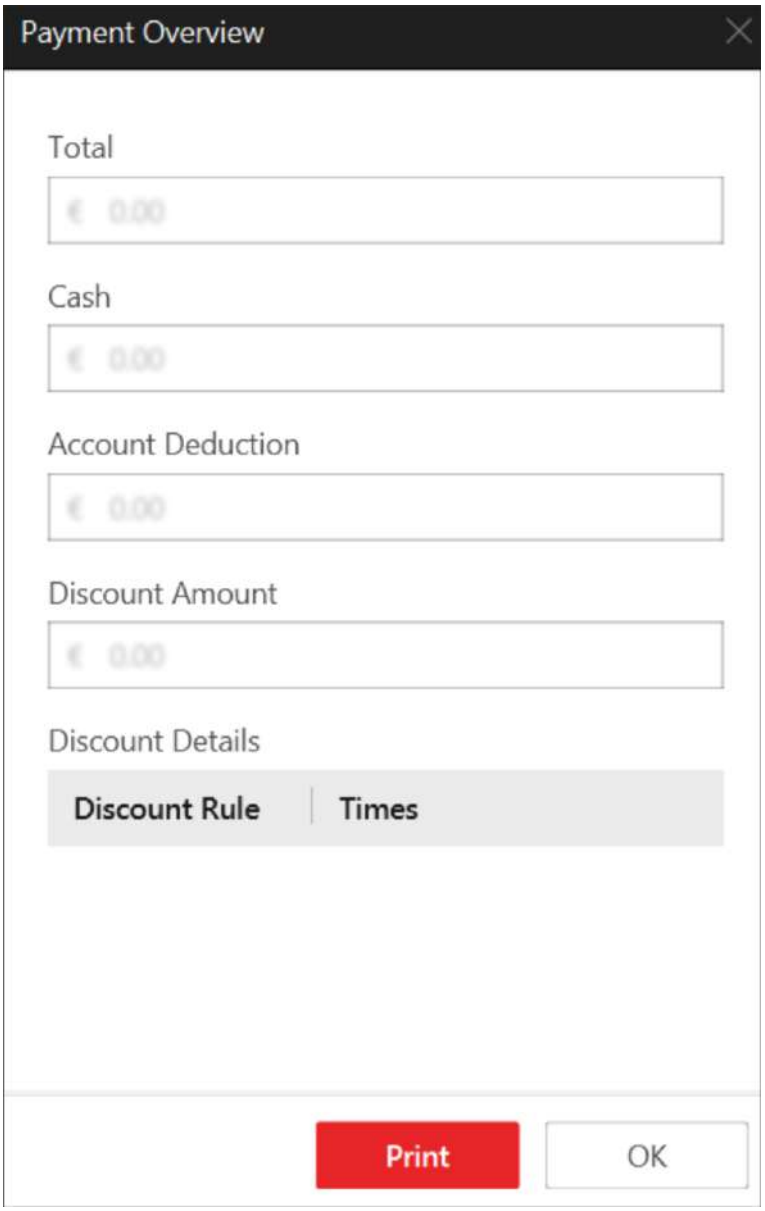


Figura 12-15 Janela Visão geral do pagamento

3. Verifique as informações de pagamento.
4. Opcional: clique em **Imprimir** para imprimir as informações de pagamento.
5. Clique em **OK** .
   A conta atual será desconectada.

12.2 Monitoramento de Vagas de Estacionamento

Na página Visão geral das vagas de estacionamento, você pode visualizar as estatísticas das vagas de estacionamento e pesquisar estatísticas específicas por número da vaga, número da placa e tempo de estacionamento.

A página Visão geral de vagas de estacionamento exibe vários tipos de estatísticas de vagas de estacionamento, incluindo a taxa de ocupação das vagas em um estacionamento, o número de vagas de estacionamento vagas, vagas de estacionamento ocupadas, vagas de estacionamento com status desconhecido e o número de horas extras de estacionamento e violações de estacionamento.

Observação

- Se não houver um mapa adicionado para o estacionamento, as informações sobre as vagas de estacionamento serão sobrepostas diretamente no vídeo de monitoramento.
- Um ícone será exibido em uma vaga de estacionamento para estacionamento de horas extras. Clique no ícone para visualizar os detalhes da vaga de estacionamento e verificar o tipo de veículo que estacionou horas extras.
- Ao selecionar → **Exportar informações de vagas de estacionamento desconhecidas** ao lado do número de vagas de estacionamento com status desconhecido em **Violação** , você pode exportar detalhes como os números das vagas de estacionamento relacionadas e as informações correspondentes do estacionamento e do andar para o PC local como um arquivo XLSX.

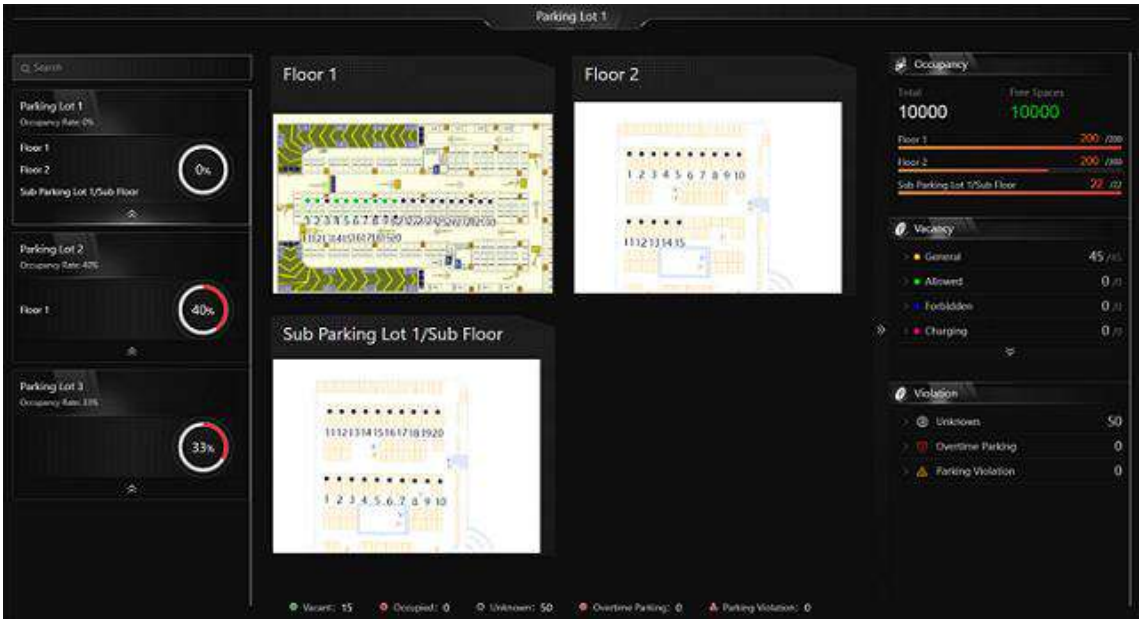


Figura 12-16 Visão geral do espaço de estacionamento

Você pode clicar no nome de um andar para visualizar as estatísticas das vagas de estacionamento deste andar. Na página seguinte, você pode ir para uma vaga de estacionamento específica para

visualizar suas informações detalhadas e pode clicar em uma vaga de estacionamento para visualizar seu status em tempo real e pesquisar registros de estacionamento. Além disso, você pode clicar em **Visão geral do status de ocupação** ou **Visão geral da duração do estacionamento** para visualizar esses dois tipos de estatísticas, respectivamente.

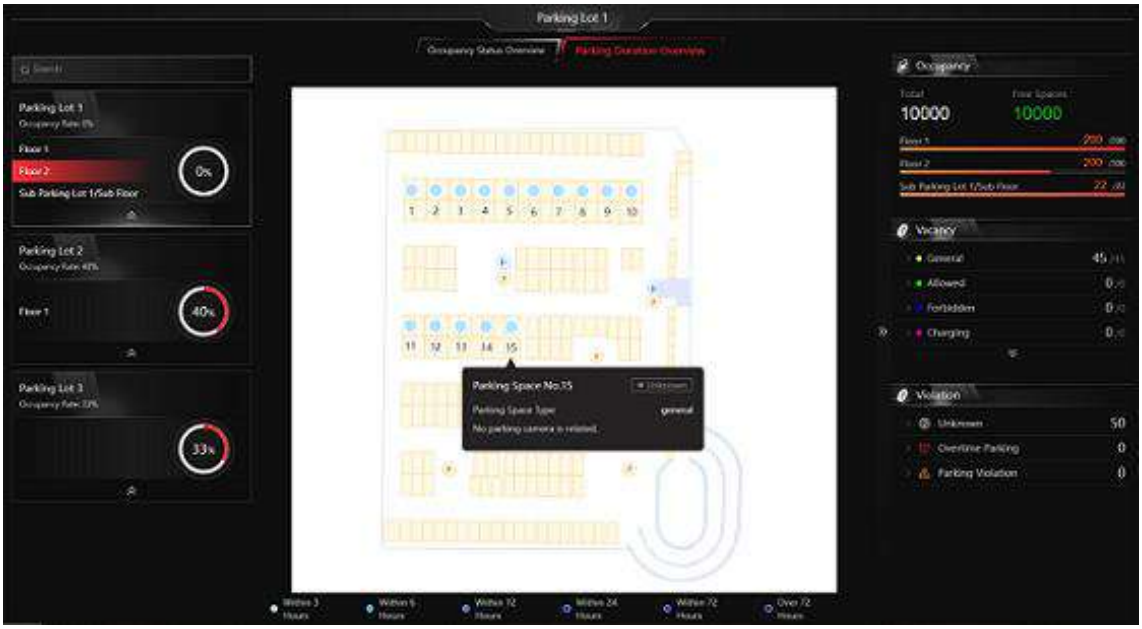


Figura 12-17 Visão geral do espaço de estacionamento no piso

12.3 Pague no Centro de Pedágio

No módulo Toll Center, você pode procurar um veículo específico para visualizar suas informações de estacionamento, como a duração do estacionamento e a taxa total de estacionamento. Depois que todas as informações forem confirmadas, o proprietário do veículo pode pagar a taxa de estacionamento no centro de pedágio.

Passos

1. No painel de navegação esquerdo, clique em **Central de Pedágio** .

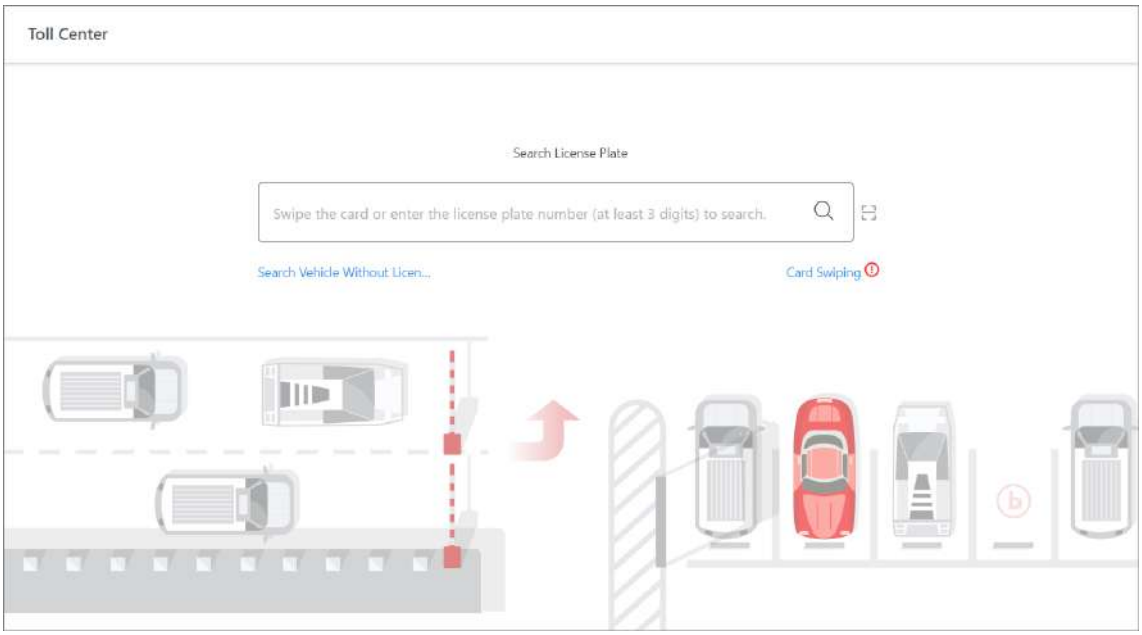


Figura 12-18 Página do Centro de Pedágio

2. Pesquise um veículo específico para obter informações sobre estacionamento.
   - Pesquisar por número de placa: digite pelo menos três dígitos de uma placa para pesquisar o veículo.
   - Pesquisar por imagem do veículo: Se a placa de um veículo não for capturada e registrada, você pode clicar em **Pesquisar veículo sem placa** e selecionar o veículo de destino nas imagens exibidas.
   - Passe o cartão temporário: Passe o cartão temporário que o proprietário do veículo recebeu ao entrar no estacionamento. Após passar o cartão no local, os detalhes do estacionamento serão exibidos. Você pode clicar em **Passar o cartão** para ligar/desligar a criptografia do cartão e ligar/desligar o áudio.
   - Escanear recibo de estacionamento: Clique em ao lado da caixa de pesquisa. Após escanear o código em um recibo de estacionamento, os detalhes do estacionamento serão exibidos para o veículo.

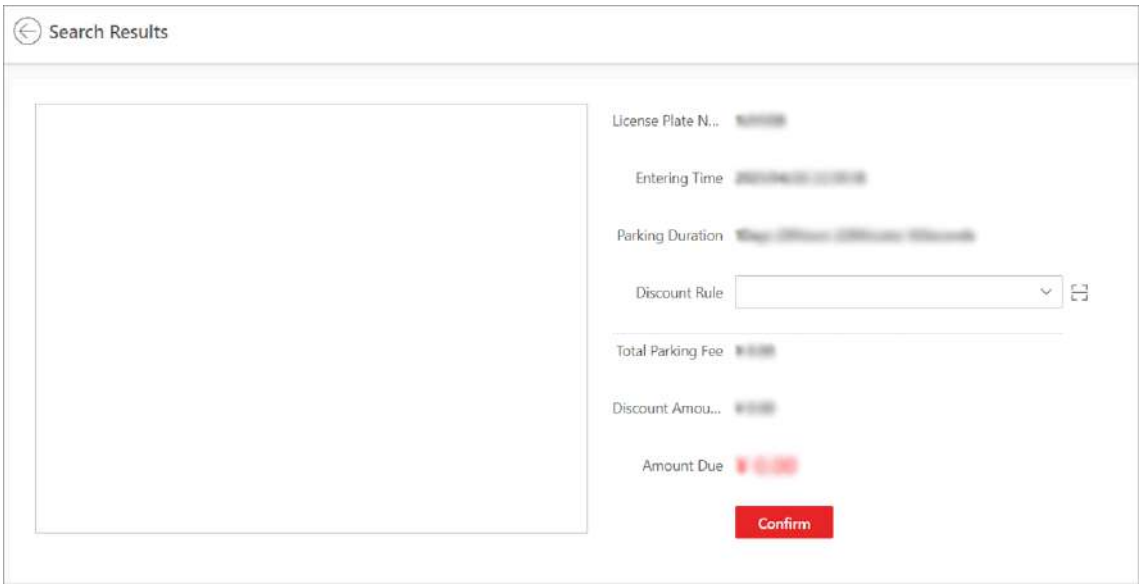


Figura 12-19 Página de resultados da pesquisa

3. Opcional: defina a regra de desconto no painel Resultados da pesquisa.
   – Selecione um cupom na lista suspensa.
   – Clique para adicionar um cupom.
4. Verifique as informações e clique em **Confirmar** .
5. **Opcional**: Na janela pop-up, clique em **Imprimir recibo** para imprimir o recibo ou salvá-lo no PC local em formato PDF.

Capítulo 13 Monitoramento e Pesquisa de Bordo

O módulo de monitoramento de bordo permite que os usuários monitorem os veículos em movimento, incluindo a localização dos veículos para obter informações de GPS em tempo real e velocidade de direção, falar com os motoristas por meio de áudio bidirecional, reproduzir vídeos transmitidos por câmeras montadas no veículo, reproduzir os trajetos percorridos pelos veículos e registrar pesquisas.

13.1 Monitoramento de Direção

Na página Driving Monitoring, você pode monitorar veículos em movimento para obter informações em tempo real, como localizações, velocidades e eventos. Você também pode reproduzir vídeos ao vivo transmitidos por câmeras montadas em veículos, falar com motoristas por áudio bidirecional, rastrear veículos em tempo real, reproduzir os trajetos percorridos pelos veículos e adicionar veículos à lista de Favoritos para gerenciamento rápido e fácil.
No canto superior esquerdo do Cliente, vá para → **Todos os Módulos** → **Monitoramento** → **Monitoramento de Bordo** → **Monitoramento de Condução** .

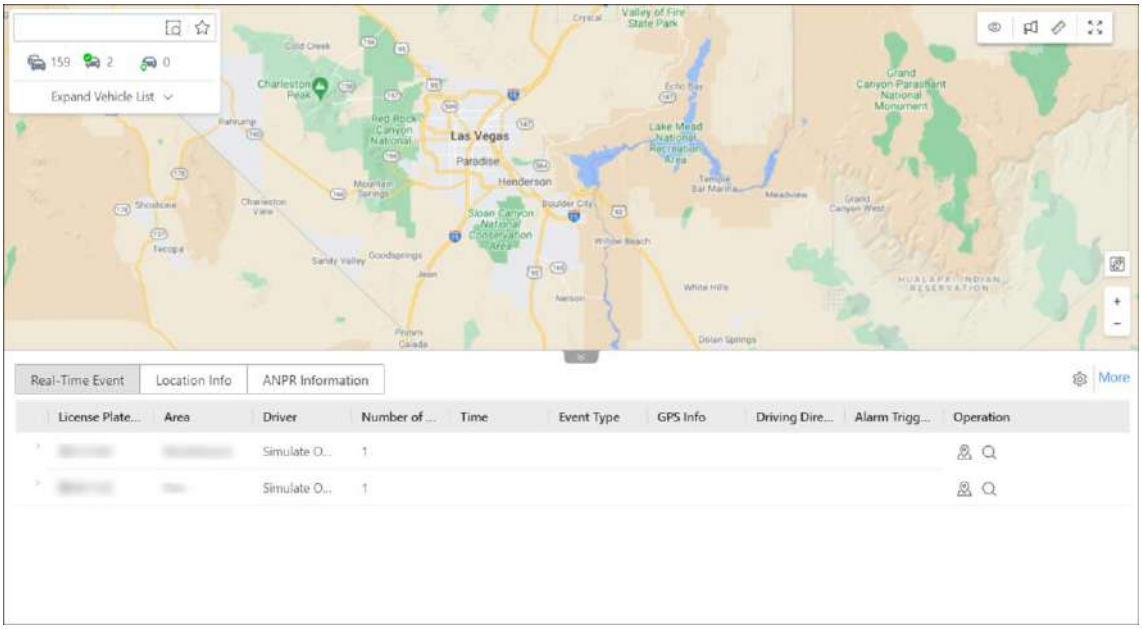


Figura 13-1 Página de monitoramento de direção

Painel de lista de veículos

Execute as seguintes operações conforme necessário:

Operação	Etapa
Pesquisar / Filtrar Veículos	● Insira palavras-chave na caixa de pesquisa para procurar

Operação	Etapa
	veículos de destino. ● Clique para especificar uma área para busca de veículos. ● Clique em / / para visualizar todos os veículos/online/localizados. ● Clique para ver os veículos na lista de favoritos.
Localizar / Transmitir para veículos	Clique em , clique no mapa para selecionar um centro e mova o mouse para desenhar um círculo com base no centro selecionado e, em seguida, clique no mapa novamente para finalizar o desenho. Passe o mouse sobre o círculo desenhado e clique em **Localizar** ou **Transmitir** para localizar ou transmitir para todos os veículos no círculo.
Ver detalhes do veículo	Na lista de veículos, passe o mouse sobre um veículo para ver suas informações em tempo real, incluindo localização, velocidade, etc.
Localizar veículo	Na lista de veículos, passe o mouse sobre um veículo e clique para localizá-lo no mapa e clique novamente para cancelar a localização.
Reproduzir faixa	Na lista de veículos, passe o mouse sobre um veículo e clique para reproduzir o trajeto percorrido pelo veículo.
Iniciar visualização ao vivo	Expanda a lista de câmeras de um veículo específico e clique duas vezes para visualizar os vídeos ao vivo transmitidos pelas câmeras montadas no veículo.
Outro	Na lista de veículos, passe o mouse sobre um veículo e clique para exibir o menu de operação. Você pode escolher reproduzir um vídeo, falar com um motorista por áudio bidirecional, rastrear um veículo em tempo real, reproduzir o trajeto percorrido pelo veículo, controlar saídas de alarme e adicionar/remover um veículo da lista de Favoritos.

Monitoramento de direção no mapa

No mapa GIS, você pode visualizar o número de alarmes não reconhecidos nos veículos. Você pode clicar no ícone de um veículo localizado no mapa para abrir o painel de monitoramento de direção. No painel, você pode visualizar as informações em tempo real do veículo, incluindo sua localização, velocidade, etc., e pode executar as seguintes operações:

Observação

Para um evento que foi inscrito e configurado com gatilho de alarme, apenas um registro será exibido e será marcado como um alarme.

Figura 13-2 Painel de monitoramento de direção

Operação	Etapa
Cancelar localização do veículo	Clique para cancelar a localização do veículo.
Obter localização do veículo	Clique em **Obter localização** para obter a localização do veículo em tempo real.
Reproduzir / Reproduzir vídeo	Clique em **Reproduzir** para reproduzir vídeos ao vivo ou gravados transmitidos por câmeras montadas em veículos. **Observação** Você pode clicar para exportar em lote os vídeos gravados para o PC local e a tarefa de download será exibida no centro de tarefas. A tarefa será pausada se os dispositivos estiverem offline e será retomada automaticamente quando os dispositivos estiverem online novamente.
Fale com o motorista	Clique em **Áudio bidirecional** para falar com o motorista.
Veículo de pista	Clique em **Rastreamento em Tempo Real** para rastrear o veículo em tempo real. Você pode clicar em **Parar** no canto superior esquerdo da página de rastreamento de veículos para parar o rastreamento.
Reproduzir faixa	Clique em **Reprodução de trilha** e selecione um período e uma câmera para reproduzir a trilha gravada pela câmera no período especificado.
Saída de alarme de controle	Clique em **Mais** → **Saída de alarme** e depois clique em / na coluna Operação para habilitar/desabilitar a saída de alarme

Operação	Etapa
	relacionada ao veículo.
Enviar texto	Clique em **Mais** → **Enviar texto** para enviar um texto para o veículo, e o texto será convertido em áudio no veículo.
Exibir histórico de alarmes	Clique em **Mais** → **Exibir histórico de alarmes** para visualizar o histórico de alarmes do veículo.
Ver detalhes do alarme	O número de alarmes disparados é marcado no ícone do veículo no mapa. Você pode clicar no número para visualizar os detalhes do alarme. Você também pode visualizar os vídeos transmitidos das câmeras montadas no veículo.

Evento em tempo real

A tabela Evento em Tempo Real apresenta eventos em tempo real acionados por veículos monitorados online. Cada registro é anexado com informações detalhadas, como número da placa, motorista, tipo de evento e informações de GPS. Você pode executar as seguintes operações:

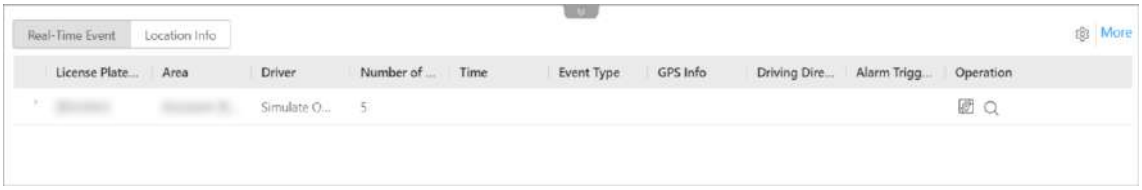


Figura 13-3 Tabela de eventos em tempo real

Operação	Etapa
Localizar veículo	Clique na coluna Operação para localizar um veículo.
Veículo central	Clique na coluna Operação para colocar um veículo localizado no centro do mapa.
Pesquisar por faixa	Clique na coluna Operação para pesquisar o trajeto percorrido por um veículo.
Salvar como evidência	Clique na coluna Operação para salvar o evento como evidência.
Selecione o tipo de evento	Clique para abrir o painel Configurações e selecione os tipos de eventos a serem reportados à plataforma.
Pesquisar por evento de	Clique em **Mais** para acessar a página de Pesquisa de Eventos

Operação	Etapa
condução	de Condução e procurar por eventos de condução acionados no passado.

Informações de localização

A tabela Location Info apresenta as localizações em tempo real dos veículos localizados. Cada registro é anexado com informações detalhadas, como número da placa, informações de GPS e direção de direção. Além disso, você pode executar as seguintes operações:

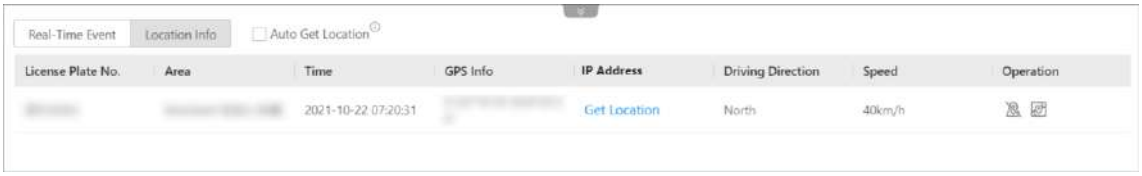


Figura 13-4 Tabela de informações de localização

Operação	Etapa
Obter localização do veículo	Clique em **Obter localização** na coluna Endereço IP para obter a localização em tempo real de um veículo.
Localização de atualização automática	Marque **Obter localização automaticamente** para atualizar os locais com frequência.
Cancelar localização do veículo	Clique na coluna Operação para cancelar a localização de um veículo.
Veículo central	Clique na coluna Operação para colocar um veículo no centro do mapa.

Informações ANPR

A tabela de informações ANPR apresenta os registros de passagem de veículos. Cada registro é anexado com informações detalhadas, como número da placa, informações de GPS e direção de direção.

Clique **em Mais** para ir para **a Pesquisa de veículos que passam** no módulo ANPR; você também pode clicar nos diferentes botões na coluna de operação de cada registro para ir para **a Pesquisa de veículos que passam** com diferentes condições.

Gerenciamento de Mapas

Você pode executar as seguintes operações no mapa:

Operação	Etapa
Exibir regra de direção	Clique e selecione **Regra de cerca** e/ou

Operação	Etapa
	Regra de desvio para exibir as áreas onde os veículos têm ou não permissão para dirigir e as rotas pelas quais os veículos devem dirigir.
Transmitir para o veículo	Clique e selecione o(s) veículo(s) para transmitir para eles.
Medir distância	Clique e especifique o ponto inicial e o ponto final no mapa para medir a distância real entre eles.
Exibição em tela cheia	Clique para exibir o mapa em tela cheia .

13.2 Monitoramento de Rota

Na página de monitoramento de rota, você pode monitorar as rotas de condução dos veículos para obter informações de parada, status da rota, causas de não pontualidade e status de condução dos veículos. Você também pode visualizar as informações detalhadas dos veículos nas rotas, como localizações, velocidades e eventos.
No canto superior esquerdo do Cliente, vá para → **Todos os Módulos** → **Monitoramento** → **Monitoramento de Bordo** → **Monitoramento de Rota** .

Lista de rotas

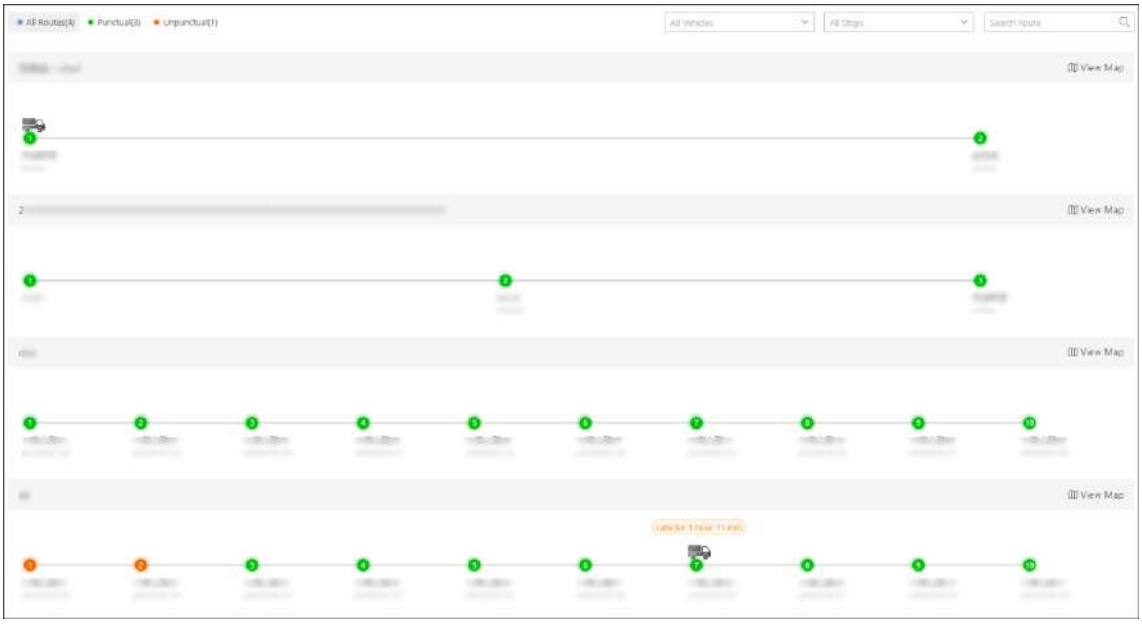


Figura 13-5 Lista de rotas

Execute as seguintes operações conforme necessário:

Operação	Descrição
Filtrar / Pesquisar por Rotas	● No canto superior esquerdo da página, clique em **Todas as rotas** / **Pontuais** / **Não pontuais** para visualizar as rotas correspondentes. ● No canto superior direito, selecione veículos e/ou paradas na lista suspensa e/ou insira palavras-chave na caixa de pesquisa para encontrar rapidamente as rotas de destino.
Ver detalhes da rota	● Você pode visualizar o número total de paradas, os nomes das paradas, o status (pontual/antecipado/atrasado) e a localização atual dos veículos em cada rota. ● Passe o cursor do mouse sobre uma parada para ver seus detalhes, incluindo tarifa pontual, veículo, horário de chegada programado, horário real de chegada, horário de partida programado e horário real de partida.
Adicionar motivo de partida/chegada fora de hora	Passe o cursor do mouse sobre uma parada e clique na coluna Operação para adicionar notas sobre partidas/chegadas fora de hora.

Monitoramento de Rota Única

Clique em **Exibir mapa** para ver os detalhes de uma única rota.

Observação

Os dois painéis à esquerda e na parte inferior da página podem ser exibidos ou ocultados clicando nas setas.

Figura 13-6 Monitoramento de rota única

Execute as seguintes operações conforme necessário:

Operação	Descrição
Ver detalhes da rota	● Você pode visualizar as paradas e os veículos na rota selecionada no mapa GIS. ● Você pode visualizar o horário programado de partida/chegada e o horário real de partida/chegada na tabela na parte inferior, com cores diferentes para diferentes status (normal, partida/chegada antecipada e partida/chegada tardia).
Adicionar motivo de partida/chegada fora de hora	Passe o cursor do mouse sobre o horário real de partida/chegada no horário e clique em **Adicionar observações** para adicionar notas sobre partidas/chegadas fora de hora.
Monitore os veículos na rota	Clique no ícone de um veículo no mapa para abrir seu painel de monitoramento de direção. Para detalhes sobre monitoramento de direção, consulte ***Monitoramento de direção*** .
Ver detalhes do alarme	O número de alarmes disparados é marcado no ícone do veículo no mapa. Você pode clicar no número para visualizar os detalhes do alarme.
Filtrar / Pesquisar por Rotas	● No canto superior esquerdo, você pode filtrar rotas por status (todas/pontuais/impontuais).

Operação	Descrição
	● Clique para selecionar veículos e/ou paradas na lista suspensa e/ou insira palavras-chave na caixa de pesquisa para encontrar rapidamente as rotas de destino.
Mudar para outra rota	Você pode selecionar outra rota no painel esquerdo para visualizar seus detalhes.

13.3 Pesquisa de Registro de Monitoramento de Bordo

Os registros de monitoramento a bordo incluem as trilhas que os veículos percorreram, os eventos acionados por eles em um período especificado, as rotas relacionadas a veículos/grupos de veículos específicos e registros de monitoramento de nível de combustível. Você pode pesquisar registros, visualizar os detalhes de cada registro e exportar registros para seu PC para uso posterior.

13.3.1 Busca por Rastros de Veículos

Você pode pesquisar os trajetos percorridos pelos veículos no período especificado, visualizar informações detalhadas de cada registro, reproduzir trajetos e exportar registros para o PC.

Passos

1. No canto superior esquerdo do Cliente, vá para → **Todos os Módulos** → **Investigação** → **Busca de Veículos** → **Busca de Monitoramento de Bordo** → **Busca de Rastreamento de Veículos** .
2. Defina as condições de pesquisa.
   1) Especifique o período em que você deseja pesquisar rastros de veículos.
   2) Selecione o(s) veículo(s).
   3) Opcional: ative **a Faixa de velocidade** e defina uma faixa de velocidade.
   4) Opcional: ative **Ativado por** e clique para selecionar o(s) tipo(s) de evento(s).

   Observação

   Todos os tipos de eventos foram selecionados por padrão.
3. Clique em **Pesquisar** .

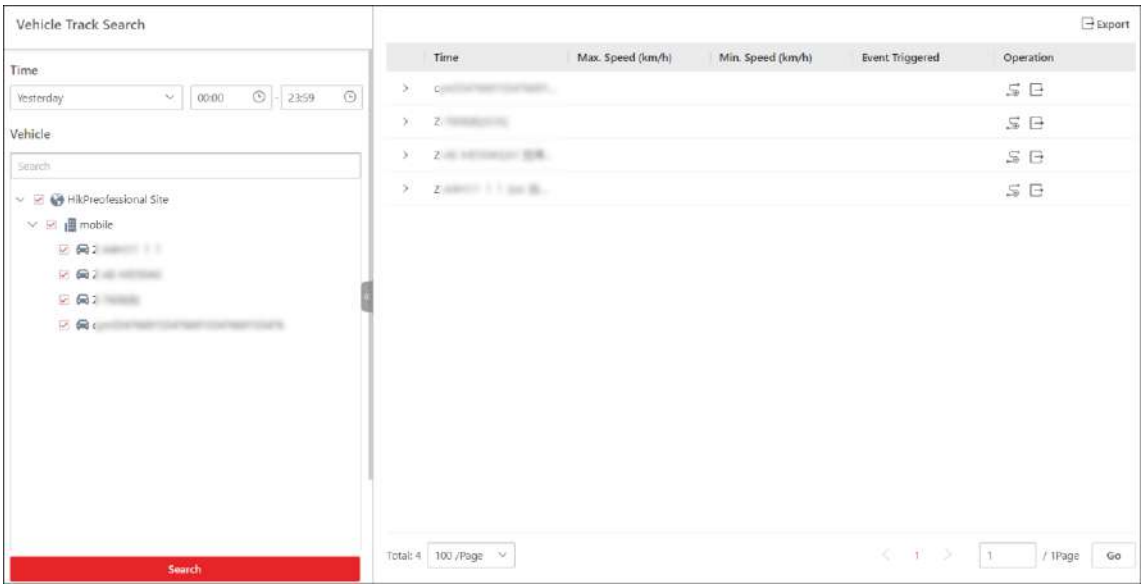


Figura 13-7 Pesquisa de Rastreamento de Veículo

4. Opcional: Execute as seguintes operações.

Reproduzir faixa	Clique para reproduzir uma faixa.
Exportar registro	Clique para exportar um único registro para o PC. Clique em **Exportar** no canto superior direito para exportar todos os registros para o PC.
Outro	Clique e mais registros gerados no período especificado serão exibidos. Você também pode clicar para reproduzir uma trilha e clicar para exportar um registro para o PC.

13.3.2 Pesquisar Eventos de Condução

Você pode pesquisar eventos acionados por veículos, motoristas ou grupos de motoristas, visualizar informações detalhadas de cada registro e exportar registros para o PC.

Passos

1. No canto superior esquerdo do Cliente, vá para → **Todos os Módulos** → **Investigação** → **Pesquisa de Veículos** → **Pesquisa de Monitoramento de Bordo** → **Pesquisa de Eventos de Condução** .
2. Defina as condições de pesquisa.

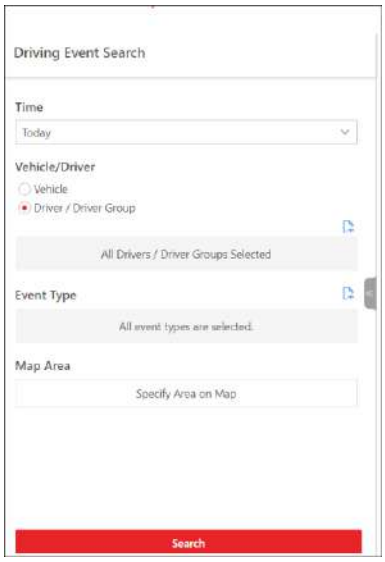


Figura 13-8 Pesquisar eventos de condução

1) Especifique o período em que você deseja pesquisar eventos de direção.
2) Selecione **Veículo** ou **Motorista/Grupo de Motoristas** como o tipo.
3) Clique para selecionar veículo(s), motorista(s) ou grupo(s) de motorista(s).

Observação

Todos os veículos/motoristas/grupos de motoristas foram selecionados por padrão.

4) Na área Tipo de evento, clique para selecionar o(s) tipo(s) de evento.

Observação

Todos os tipos de eventos foram selecionados por padrão.

5) Na área Área do mapa, clique em **Especificar área no mapa** e desenhe uma área no mapa.
A plataforma buscará eventos disparados na área especificada.

3. Clique em **Pesquisar** .
4. Opcional: Execute as seguintes operações.

Reproduzir faixa	Clique para reproduzir uma faixa.
Exportar registro	Clique para exportar um único registro para o PC. Verifique os registros e clique em **Exportar** no canto superior direito para exportá-los para o PC.

13.3.3 Pesquisar Rotas

Você pode pesquisar rotas, visualizar informações detalhadas de cada rota e exportar informações

de rota para o PC local.

Passos

1. No canto superior esquerdo do Cliente, vá para → **Todos os Módulos** → **Investigação** → **Busca de Veículos** → **Busca de Monitoramento de Bordo** → **Busca de Rota** .
2. Defina as condições de pesquisa.

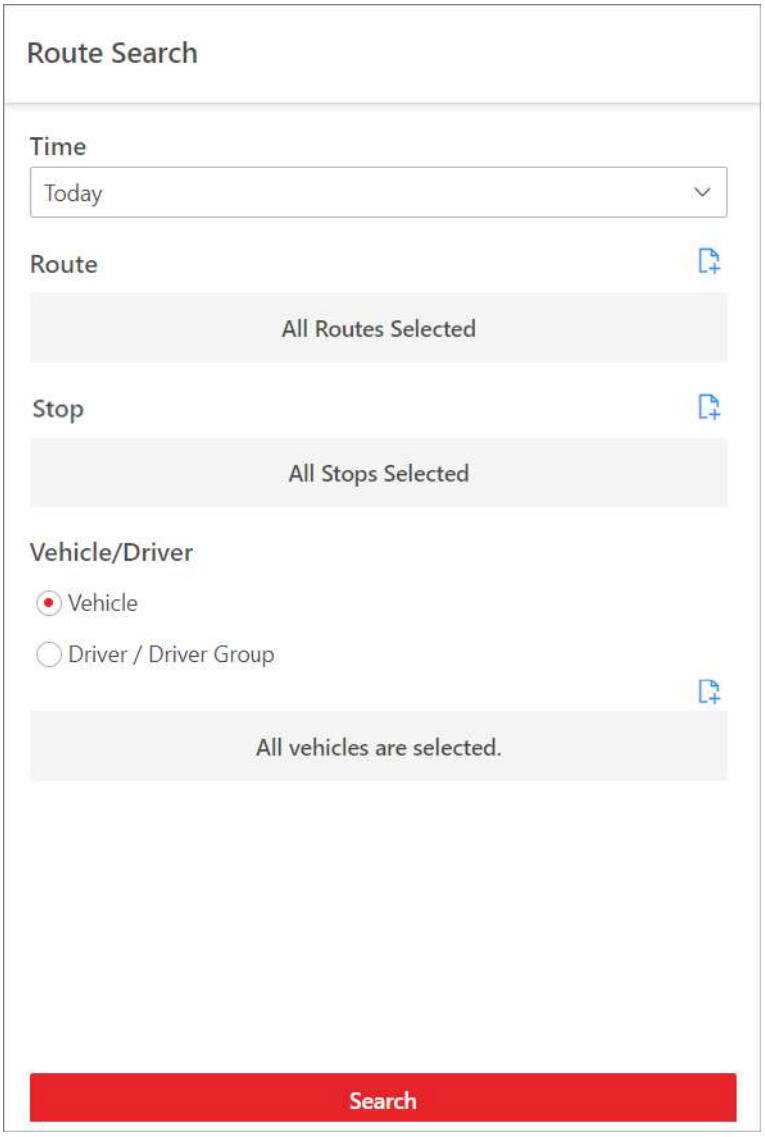


Figura 13-9 Condições de pesquisa

1) Especifique o período em que deseja pesquisar rotas.
2) Clique para selecionar a(s) rota(s).

Observação

Todas as rotas foram selecionadas por padrão.

3) Clique para selecionar parada(s).

Observação

Todas as paradas foram selecionadas por padrão.

4) Selecione **Veículo** ou **Motorista/Grupo de Motoristas** como o tipo.
5) Clique para selecionar veículo(s), motorista(s) ou grupo(s) de motorista(s).

Observação

Todos os veículos/motoristas/grupos de motoristas foram selecionados por padrão.

3. Clique em **Pesquisar** .
As rotas necessárias serão exibidas na lista.

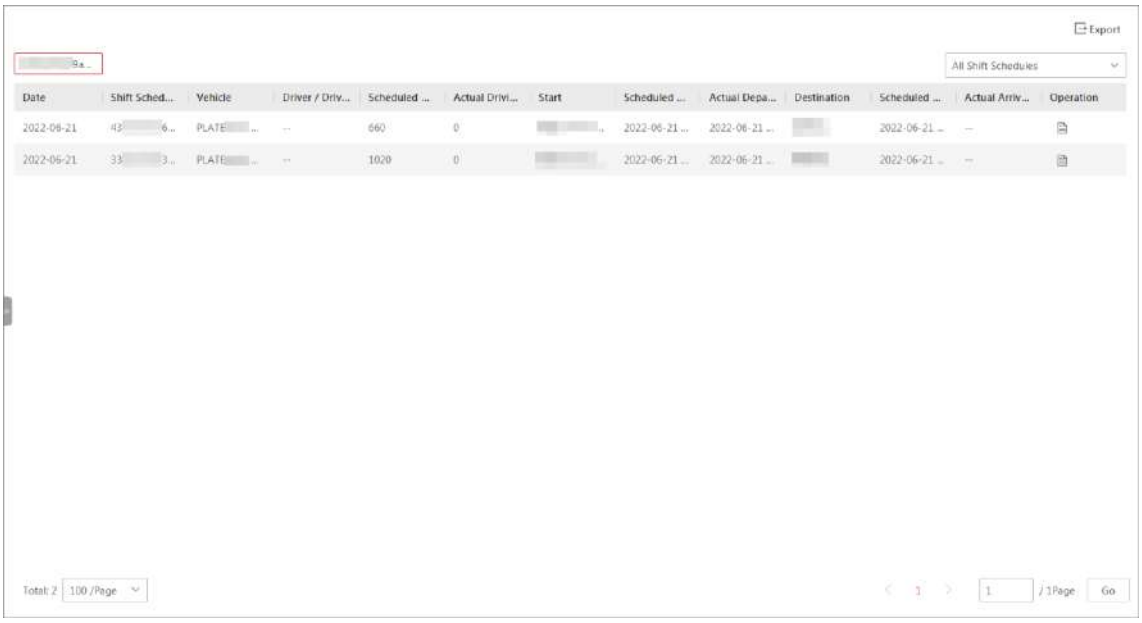


Figura 13-10 Busca por Rotas

4. Opcional: Execute as seguintes operações.

Reproduzir faixa	Na coluna Operação, clique para reproduzir uma faixa.
Exportar registro	Clique para exportar um único registro para o PC. Verifique os registros e clique em **Exportar** no canto superior direito para exportá-los para o PC.

13.3.4 Busca por Registros de Monitoramento de Nível de Combustível

Você pode pesquisar registros de nível de combustível no período especificado e visualizar detalhes como número da placa, área, nome do motorista, modelo do tanque de combustível, quantidade de combustível, nível de combustível no tanque (%), informações de GPS e

abastecimento de combustível ou não.

Passos

1. No canto superior esquerdo do Cliente, vá para → **Todos os Módulos** → **Investigação** → **Busca de Veículos** → **Busca de Monitoramento de Bordo** → **Busca de Registro de Nível de Combustível** .
2. Defina as condições de pesquisa.
   1) Especifique o período em que você deseja pesquisar registros de nível de combustível.
   2) Selecione **Veículo** ou **Motorista/Grupo de Motoristas** , e todos os veículos ou todos os motoristas/grupos de motoristas serão selecionados por padrão.

   Observação

   Clique para especificar determinados veículos ou motoristas/grupos de motoristas.

3. Clique em **Pesquisar** para obter a lista de registros de monitoramento de nível de combustível.

Observação

Você pode clicar em **Exportar** no canto superior direito para exportar os registros para seu PC local.

Capítulo 14 Patrulha

O sistema fornece o serviço para gerenciamento de patrulhas. No Control Client, você pode executar o monitoramento em tempo real de patrulhas (que são configuradas no Web Client) para saber convenientemente se exceções ocorrem durante essas patrulhas, e pesquisar e exportar os registros de eventos relacionados a essas patrulhas.

14.1 Monitoramento de Patrulha em Tempo Real

Você pode monitorar o status da patrulha em tempo real por meio de mapa ou lista, para saber convenientemente se ocorre uma exceção durante a patrulha, o que ajuda a lidar com a exceção a tempo.

Observação

Certifique-se de ter permissão de operação para monitoramento de patrulha.

No canto superior esquerdo do Control Client, selecione → **All Modules** → **Monitoring** → **Patrol Monitoring** . Na página de monitoramento de patrulha, você pode visualizar o status em tempo real das rotas de patrulha e informações sobre eventos em tempo real relacionados às patrulhas.

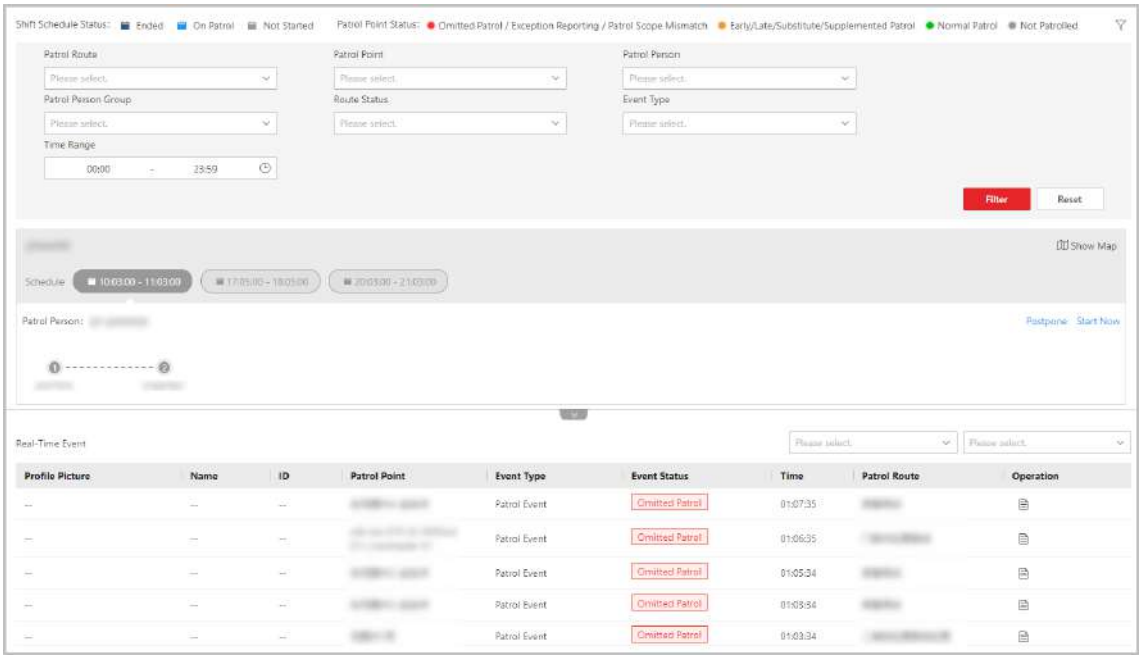


Figura 14-1 Página de monitoramento em tempo real

Status da rota de patrulha

O status em tempo real de todas as rotas de patrulha habilitadas com turnos programados para o

dia atual são exibidos por padrão. Você pode filtrar as rotas clicando no canto superior direito da página e definindo os critérios de filtro (por exemplo, rota de patrulha, ponto de patrulha, pessoa de patrulha/grupo de pessoas de patrulha, status da rota, tipo de evento e intervalo de tempo).
Informações como o nome da rota, patrulheiro/grupo de patrulheiros, período de tempo programado para cada turno e uma lista de pontos de patrulha são exibidas para cada rota de patrulha. O status do cronograma do turno (por exemplo, encerrado, em patrulha e não iniciado) e o status do ponto de patrulha (por exemplo, patrulha omitida/relatório de exceção, incompatibilidade de escopo de patrulha, patrulha antecipada, patrulha tardia, patrulha substituta, patrulha suplementada, patrulha normal e não patrulhada) são indicados com cores diferentes em relação às legendas no topo da página.
Você pode clicar em um ponto de patrulha que já esteja sendo patrulhado para visualizar seu status e as informações relacionadas ao evento de patrulha. Você também pode passar o mouse sobre um turno para visualizar seu status e informações detalhadas. Se necessário, você pode iniciar ou adiar manualmente um turno ainda não iniciado selecionando o cronograma de turno e clicando em **Iniciar agora** ou **Adiar,** respectivamente.
Para rotas de patrulha com pontos de patrulha adicionados aos mapas, você também pode clicar em **Mostrar mapa** para alternar para o monitoramento do status da patrulha em tempo real por meio de mapas.

Evento em tempo real

A página de monitoramento de patrulha também oferece suporte à exibição de informações sobre eventos relacionados à patrulha em tempo real (por exemplo, eventos de patrulha, relatórios de exceção e incompatibilidade de escopo de patrulha), incluindo informações sobre a pessoa da patrulha (por exemplo, foto do perfil, nome, ID), informações do evento (por exemplo, tipo de evento, status do evento), informações da patrulha (por exemplo, ponto de patrulha, escopo de patrulha válido, rota de patrulha, cronograma de turnos, tempo de patrulha programado/real e pessoa da patrulha planejada/real) e arquivos de vídeo/imagem e anexos relacionados.

Observação

As informações reais exibidas podem variar dependendo do tipo de evento e do status da patrulha.

Você pode filtrar os eventos em tempo real por tipo de evento e visualizar detalhes sobre cada evento clicando na coluna Operação.

14.2 Busca por Registros de Eventos Relacionados à Patrulha

Você pode pesquisar e exportar registros de eventos relacionados a patrulhas, incluindo eventos de patrulha e relatórios de exceções.

Antes de começar

Certifique-se de ter permissão de operação para busca de patrulha.

Passos

1. No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Investigação** → **Pesquisa de pessoas** → **Pesquisa de patrulha** .

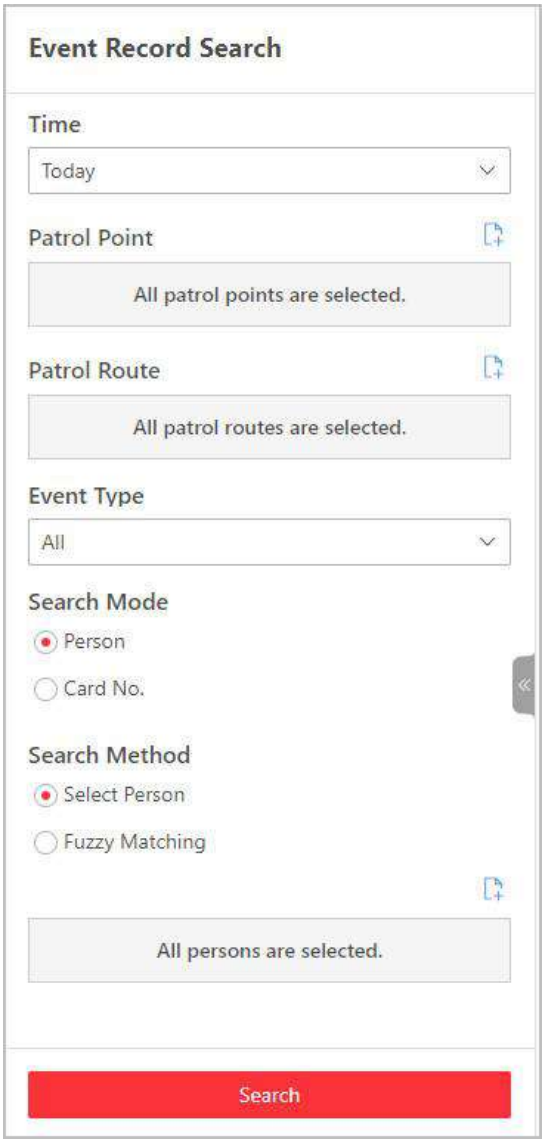


Figura 14-2 Pesquisa de registro de eventos

2. Defina as condições de pesquisa.

Tempo

Selecione entre **Hoje** , **Ontem** , **Semana atual** , **Últimos 7 dias** e **Últimos 30 dias** ou defina um intervalo de tempo personalizado de no máximo 31 dias.

Ponto de patrulha

Por padrão, todos os pontos de patrulha são selecionados. Clique para selecionar certos pontos de patrulha para filtrar os resultados da pesquisa.

Rota de patrulha

Por padrão, todas as rotas de patrulha são selecionadas. Clique para selecionar determinada(s) rota(s) de patrulha para filtrar os resultados da pesquisa.

Tipo de evento

Por padrão, todos os registros de eventos relacionados à patrulha serão pesquisados. Selecione **Patrol Event** , **Exception Reporting** ou **Patrol Scope Mismatch** na lista suspensa para pesquisar apenas o tipo especificado de registros de eventos.

Modo de pesquisa

Escolha se deseja pesquisar os registros de eventos por **Pessoa** ou **Número do Cartão** .

- Pesquisar por pessoa: No campo **Método de pesquisa** , escolha se deseja pesquisar por seleções de pessoas ou por correspondência parcial de nomes de pessoas.
- Pesquisar por número do cartão: digite o número do cartão na caixa de pesquisa.

3. Clique em **Pesquisar** .
   Os registros correspondentes serão exibidos no lado direito da página.
4. Opcional: Execute as seguintes operações de acordo com suas necessidades.

Exibir detalhes de um registro de evento	Na coluna Operação de um registro de evento, clique para visualizar informações detalhadas sobre o registro. ● Para um evento de patrulha, você pode visualizar as informações do evento (por exemplo, status da patrulha), informações da patrulha (por exemplo, ponto de patrulha, escopo de patrulha válido, rota de patrulha, cronograma de turnos, horário de patrulha programado/real e patrulheiro planejado/real) dependendo do status da patrulha e vídeos/fotos relacionados à patrulha. ● Para um relatório de exceção, você pode visualizar as informações do evento (por exemplo, tipo e descrição da exceção), informações de patrulha (por exemplo, ponto de patrulha, rota de patrulha e patrulheiro) e os arquivos anexados a este relatório de exceção.
Exportar um registro de evento	Na coluna Operação de um registro de evento, clique para exportar o registro.
Exportar todos os registros de eventos correspondentes	No canto superior direito da página de resultados, clique em **Exportar** para exportar todos os resultados correspondentes. Você pode escolher se deseja exportar no formato XLSX ou CSV, e se deseja exportar os registros de eventos com imagem.

Capítulo 15 Parede Inteligente

O Smart Wall fornece ao pessoal de segurança uma visão geral maior das regiões que eles querem observar para qualquer movimento ou atividade incomum, pequeno ou grande. Um grande número de recursos de monitoramento (como câmeras, mapas e recursos gerenciados na plataforma) pode ser exibido no Smart Wall para monitoramento contínuo. Com a ajuda do Smart Wall, o pessoal de segurança pode responder aos incidentes de forma eficaz. O Smart Wall também está disponível no Mobile Client.
O HikCentral Professional oferece dois modos de paredes inteligentes: Parede Inteligente (Dispositivo de Decodificação) e Parede Inteligente (Placa Gráfica).
No modo Smart Wall (dispositivo de decodificação), os dispositivos de decodificação podem decodificar os fluxos e exibir as imagens das câmeras nas unidades de exibição conectadas aos dispositivos de decodificação.
No modo Smart Wall (placa gráfica), a placa gráfica do PC que executa o Control Client decodificará as imagens e outros conteúdos (como páginas do Control Client) e os exibirá nas telas conectadas ao PC.

15.1 Gerenciar Smart Wall (Dispositivo de decodificação)

Um Smart Wall (Dispositivo de Decodificação) é uma configuração especial de vários monitores que consiste em vários monitores, telas ou unidades de exibição lado a lado contíguas ou sobrepostas para formar uma tela grande, para que você possa ter uma visão geral completa de grandes centros de monitoramento. Com o smart wall, você pode facilmente criar visualizações definindo a divisão de janelas e o conteúdo para o smart wall gerenciado. Além disso, o vídeo acionado pelo evento também pode ser exibido no smart wall para ajudar o operador a se concentrar rapidamente nos assuntos mais críticos. Por exemplo, se uma porta for aberta, o smart

wall pode ser configurado para exibir o vídeo da câmera mais próxima da porta.

Figura 15-1 Cenário de aplicação: Smart Wall (dispositivo de decodificação)

No Web Client, você precisa adicionar dispositivos de parede inteligente (como controladores e decodificadores de parede de vídeo) ao sistema e criar paredes inteligentes virtuais. Então, você precisa vincular a saída de decodificação dos dispositivos de decodificação às janelas da parede inteligente virtual.

Após a configuração, o Control Client oferece suporte à exibição de vídeos da câmera no smart wall para obter uma visão geral completa e clara desses vídeos.

Figura 15-2 Paredes inteligentes

Clique em / para abrir ou fechar a parede inteligente remotamente.

Os seguintes ícones estão disponíveis na janela do Smart Wall.

Observação

- Os ícones exibidos variam de acordo com a capacidade das paredes inteligentes.
- Você pode selecionar uma janela e pressionar a tecla F2 para definir o número da câmera e clicar em **Confirmar** . O número da câmera será exibido na janela.

Ícone	Descrição
	Defina a janela atual como janela de alarme. Até 4 janelas podem ser definidas como janelas de alarme.
/	Defina o modo de exibição do alarme como bloco ou comutação automática.
	Quando as configurações do smart wall no servidor SYS são alteradas (por exemplo, mais smart walls são adicionadas, saídas de decodificação vinculadas são alteradas, dispositivos de decodificação são excluídos), um ponto vermelho aparecerá neste ícone. Clique nele para sincronizar as informações do smart wall.
	Defina para exibir o número da janela na parede inteligente ou visualizar os detalhes da parede inteligente.
/	Desbloqueie ou bloqueie a janela. Quando você bloqueia a janela, não é possível exibir o vídeo nesta janela ou parar de decodificar e exibir na janela.
	Defina a divisão da janela para a janela de exibição selecionada do smart wall. Clique duas vezes na janela dividida para ampliá-la.
/	Exibir ou ocultar as regras do VCA na janela de exibição do smart wall, como quadros de detecção de alvos configurados para eventos do VCA.
	Pare todas as janelas tocando.
	Salve as configurações atuais na visualização ou em outra visualização. Dessa forma, você pode visualizar facilmente os vídeos ao vivo necessários no smart wall chamando essa visualização. **Observação** Para obter detalhes, consulte ***Criar visualização*** .
	Clique para visualizar o cronograma de visualização do smart wall atual. Você pode alterar o cronograma conforme necessário.
	Crie uma janela de roaming para abrir uma janela virtual na(s) tela(s).
/	Clique e arraste o cursor para selecionar as janelas a serem unidas. Clique e as janelas unidas serão divididas.
	Abra uma janela definindo coordenadas, altura e largura.

Ícone	Descrição
	Monitore previamente o recurso antes de exibi-lo no mural inteligente. **Observação** Certifique-se de ter configurado a permissão do usuário para pré-monitoramento sob a permissão Whole Smart Wall Operation. Para obter detalhes sobre como configurar a permissão do usuário, consulte o *Manual do Usuário do HikCentral Professional Web Client* .
	Adicione uma janela de texto para inserir textos conforme necessário. **Observação** Certifique-se de ter configurado a permissão do usuário para configurar o texto sob a permissão Whole Smart Wall Operation. Para obter detalhes sobre como configurar a permissão do usuário, consulte o *Manual do Usuário do HikCentral Professional Web Client* .
	No canto inferior direito, clique no ícone para mostrar ou ocultar a janela de texto.
	Defina o modelo de layout por meio das seguintes operações e clique em **Salvar** para salvar as configurações. **Observação** Certifique-se de ter configurado a permissão do usuário para configurar o layout em Whole Smart Wall Operation permission. Para obter detalhes sobre como configurar a permissão do usuário, consulte o *Manual do Usuário do HikCentral Professional Web Client* . ● Selecione ou personalize um modo de divisão de janela. ● Selecione a posição do texto e defina o valor de pixel correspondente para ajustar o tamanho do texto. ● Habilite **Abrir Janela** para habilitar a função de abrir janelas.
	● Selecione uma tela para exibir a área de trabalho. ● Exiba o conteúdo de programas (PowerPoint, Google Chrome, Internet Explorer, Microsoft Edge, Microsoft Word, Microsoft Excel e reprodutores de vídeo) no smart wall. **Observação** Esta função está disponível apenas para Windows 10 (versão 1907 e superior).

Ícone	Descrição
/	Coloque a janela no topo ou coloque-a na parte inferior.
	Selecione um logotipo para a janela.
	Alterne o tipo de transmissão do vídeo.
	Amplie a janela.
	Comece a usar o controle PTZ.
	Pare de decodificar.
	Ver reprodução.
	Veja o status da decodificação.
	Abra a janela de visualização.
	Faça a pré-operação antes de exibir na parede inteligente. **Observação** ● Certifique-se de ter a permissão de usuário para pré-operação. Para obter detalhes sobre como configurar a permissão de usuário, consulte o *Manual do Usuário do HikCentral Professional Web Client* . ● Você pode clicar em / para desfazer/refazer operações durante a pré-operação.
	Pause o vídeo ao vivo na janela de visualização ao vivo e o último quadro será exibido.
	Diagnostique o dispositivo remotamente.
	Arraste uma janela para alternar a posição do recurso. **Observação** ● Durante a troca, não há suporte para mover uma janela virtual. ● Esta função não é suportada ao executar a alternância automática em uma janela ou em várias janelas. ● Esta função é suportada para janelas fixas e janelas de roaming, e não é suportada para janelas de reprodução e janelas bloqueadas.
	Controle remotamente o PC que está conectado com a câmera via USB. Você também pode arrastar o recurso para a área de pré-monitoramento e clicar em **KVM** para usar esta função.

15.1.1 Ver Vídeos

Depois de configurar o smart wall no Web Client, os fluxos de vídeo podem ser decodificados pelas saídas de decodificação configuradas e, então, você pode visualizar os vídeos decodificados no smart wall.

Passos

1. Selecione uma parede inteligente.
2. Selecione no canto inferior esquerdo das janelas da parede inteligente para selecionar um modo de divisão de janela.
3. Opcional: antes de exibir na parede inteligente, você pode iniciar a visualização ao vivo da câmera clicando na câmera na árvore de recursos para verificar seu status.

Observação

Você também pode arrastar o recurso para a parte inferior do cliente para visualização ou arrastar o recurso da parte inferior para uma janela de exibição para exibi-lo diretamente no smart wall.

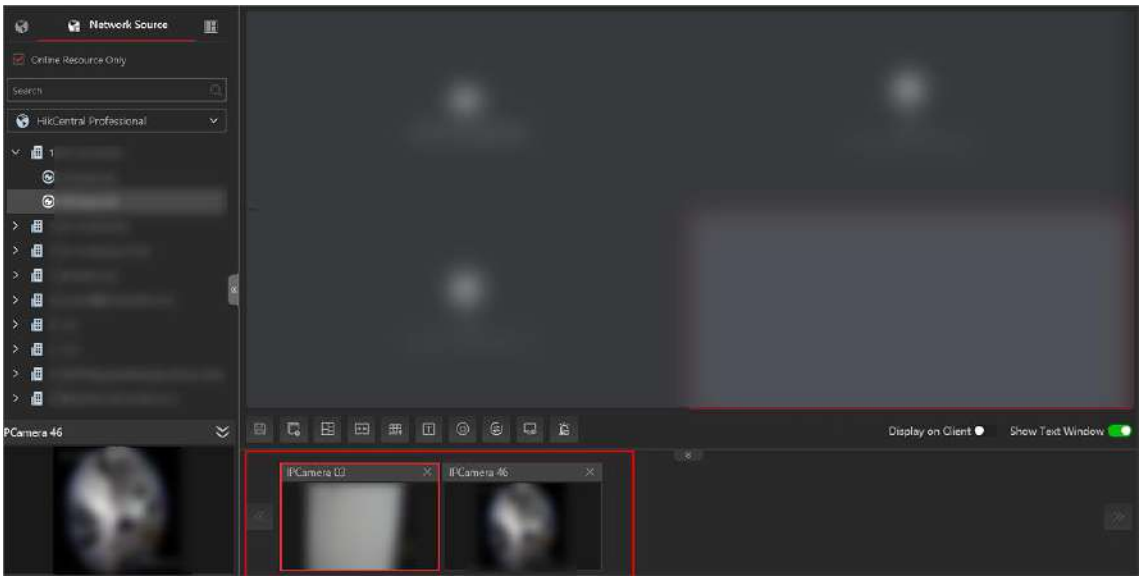


Figura 15-3 Visualizar recurso

4. Exiba recursos locais ou de rede na parede inteligente.

Observação

Há três maneiras de exibir vários recursos na área.

Tabela 15-1 Modo de exibição

Modo	Descrição
Jogo em lote	Selecione vários recursos, arraste-os para uma janela e selecione **Batch Play** . Os vídeos

Modo	Descrição
	serão reproduzidos sequencialmente nas janelas seguintes, começando pela janela selecionada.
Troca automática de tela única	Selecione vários recursos, arraste-os para uma janela e selecione **Single-Screen Auto-Switch** . Os vídeos serão reproduzidos sequencialmente na janela selecionada.
Troca automática de várias janelas	Selecione vários recursos, arraste-os para uma janela e selecione **Multi-Window Auto-Switch** . Os vídeos serão reproduzidos sequencialmente nas janelas selecionadas.

5. Opcional: Você pode executar a(s) seguinte(s) operação(ões).

Habilitar áudio Clique para habilitar o áudio.

Observação

Para reproduzir o áudio do video wall, defina a porta de áudio primeiro no Web Client. Para obter detalhes, consulte Gerenciar Smart Wall no *Manual do Usuário do HikCentral Professional Web Client* .

Ver status da câmera Clique para mostrar a taxa de quadros, a resolução e o formato de transmissão da câmera.

Trocar fluxo No Web Client, você pode definir o tipo de fluxo padrão do vídeo ao vivo das câmeras exibidas na parede inteligente. Se você quiser alterar o fluxo, como alterar para o fluxo principal para obter melhor qualidade de imagem, você pode alternar o fluxo manualmente da seguinte forma.
Clique em ou para alternar a transmissão ao vivo para transmissão principal ou secundária.

Observação

Se você alternar o tipo de transmissão, certifique-se de ter desativado **a opção Troca automática para transmissão secundária** na página de configuração da Web do dispositivo.

Pare de decodificar e exibir Clique em ou para interromper a decodificação e a exibição da janela especificada ou de todas as janelas.

Observação

Para janelas bloqueadas e janelas vinculadas a alarmes, não é possível interromper a decodificação e a exibição.

Exibir nome da saída de decodificação	Para visualizar o nome da saída de decodificação em uma janela, vá para **Sistema** → **Smart Wall** → **Exibir** e ative **Exibir nome da saída** .

15.1.2 Criar Uma Janela de Roaming

Windowing é abrir uma janela virtual na(s) tela(s). A janela pode estar dentro de uma tela ou abranger várias telas. Você pode mover a janela nas telas válidas conforme desejado e essa função é chamada de roaming. Com a função windowing e roaming, você pode criar uma janela personalizada e o tamanho e a posição da janela não serão limitados pela(s) tela(s) real(ais).

Passos

1. Clique e arraste nas telas que estão vinculadas às saídas de decodificação para abrir uma janela.

Observação

- Telas vinculadas a saídas BNC não estão disponíveis para abrir uma janela.
- Você também pode clicar para abrir uma janela definindo coordenadas, altura e largura.

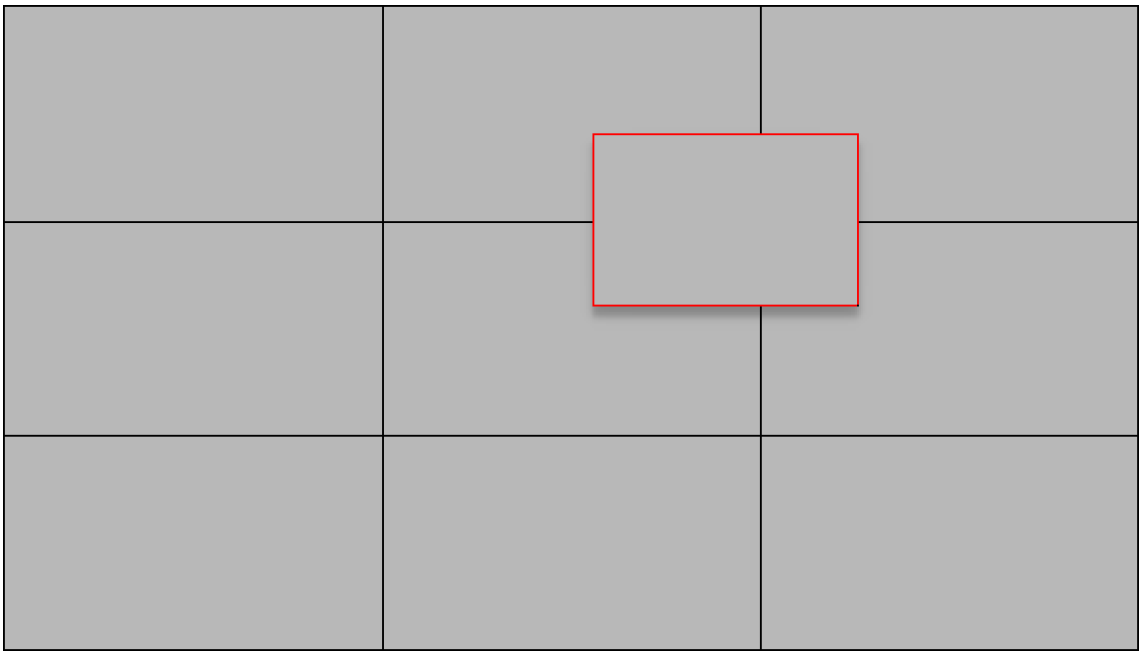


Figura 15-4 Abrir uma janela

2. Opcional: execute a(s) seguinte(s) operação(ões) após abrir uma janela.

Percorrer	Clique na janela e segure o mouse para movê-la dentro do escopo das telas válidas.
Ajustar tamanho da janela	Mova o cursor para as bordas da janela e ajuste o tamanho da janela quando o cursor se transformar em uma seta direcional.
Ampliar janela	Clique duas vezes na janela e ela será ampliada para preencher as telas estendidas e exibir na camada superior. Clique duas vezes novamente para restaurar.
Cole a janela no topo	Clique para exibir a janela na camada superior.
Janela de fixação na parte inferior	Clique em exibir a janela na camada inferior.

15.1.3 Criar Visualização

Uma visualização é um layout de vídeo personalizado dentro de janelas de parede inteligente, adaptado às suas necessidades específicas. Depois de arrastar vídeos para janelas, você pode criar uma visualização para exibição conveniente na parede de vídeo. Dessa forma, você pode acessar rapidamente os recursos usados com frequência na parede inteligente de vídeo para uma excelente visão geral.

Por exemplo, você está configurando uma sala de controle com um video wall que consiste em quatro janelas. Você quer monitorar diferentes seções de uma instalação de produção. Neste caso, você pode criar visualizações que representam áreas específicas de interesse.

Você pode criar uma exibição chamada "Linha de Produção 1", onde a Janela 1 exibe um feed ao vivo da linha de montagem, a Janela 2 mostra dados e análises em tempo real para métricas de produção, a Janela 3 exibe uma visão de câmera em close de um processo crítico e a Janela 4 mostra um painel com indicadores-chave de desempenho.

Outra visualização poderia ser "Controle de Qualidade", onde a Janela 1 exibe uma transmissão ao vivo da estação de controle de qualidade, a Janela 2 mostra relatórios de inspeção detalhados, a Janela 3 exibe gráficos e tabelas mostrando métricas de qualidade e a Janela 4 mostra uma transmissão de câmera da área de teste do produto final.

Ao organizar essas visualizações em grupos, você pode alternar facilmente entre diferentes perspectivas e monitorar aspectos específicos da unidade de produção, permitindo uma exibição de vídeo conveniente e um gerenciamento eficiente das operações na sala de controle.

Criar uma visualização

1. Selecione e arraste vídeos para janelas.
2. Selecione para salvar o layout do vídeo como uma visualização.
   a. Defina o nome da exibição.
   b. Defina a visualização como pública ou privada.

Observação

- Os grupos de exibição e as exibições na exibição pública podem ser vistos por todos os usuários do sistema.
- Os grupos de visualização e as visualizações na visualização privada só podem ser vistos pelo usuário que os adicionou.

c. (Opcional) Ative **a Reprodução Programada** para definir a programação de exibição.
d. (Opcional) Selecione **Mais** para definir o local de armazenamento.

3. Selecione para abrir a janela Exibir, passe o cursor sobre a exibição, selecione e selecione **Aplicar** para aplicar as configurações ao dispositivo.

Criar um grupo de visualização

Depois de criar várias visualizações, você pode criar um grupo de visualizações para gerenciá-las.

1. Selecione para abrir a janela Exibir.
2. Selecione **Exibição Pública** ou **Exibição Privada** para adicionar este grupo de exibição.
3. Selecione , defina o nome do grupo e selecione **Salvar** .
4. Arraste as visualizações selecionadas para o grupo.
5. (Opcional) Passe o cursor sobre uma visualização, selecione e selecione uma duração de exibição para a visualização.
6. (Opcional) Passe o cursor sobre um grupo de visualizações, selecione e selecione **Iniciar troca automática** para iniciar a troca automática de visualizações.

15.1.4 Ver Vídeos Relacionados ao Alarme no Smart Wall

Se você habilitar a ligação de parede inteligente para alarmes, a visualização ao vivo de câmeras, visualizações públicas ou saídas de decodificação relacionadas ao alarme aparecerão na parede inteligente escolhida quando o alarme for disparado. Portanto, você saberá os detalhes do alarme em tempo hábil para operações futuras.

- Quando um alarme vinculado a várias câmeras/saídas de decodificação em uma janela de exibição é acionado, a janela será dividida em um modo de divisão adaptável e mostrará os vídeos de todas as câmeras.
- Quando vários alarmes vinculados a uma janela de exibição são acionados, a janela será dividida em um modo de divisão adaptável e mostrará os vídeos relacionados aos alarmes.
- Quando cada alarme vinculado a várias janelas de exibição é acionado, cada janela mostrará um vídeo relacionado ao alarme. Se os alarmes excederem o limite da janela, a janela será dividida em um modo de divisão adaptável e mostrará os vídeos relacionados a mais alarmes.
  Por exemplo, 18 alarmes são vinculados à janela 1, janela 2 e janela 3 de uma parede inteligente. Quando o alarme 1, o alarme 2 e o alarme 3 são acionados, a janela de exibição da parede inteligente será exibida na Figura 5.1. Quando o alarme 4, o alarme 7 e o alarme 12 são acionados, a janela de exibição será exibida na primeira janela. Para obter detalhes, consulte a figura a seguir.

Observação

Uma janela de alarme pode ser dividida em 16 janelas para exibir alarmes.

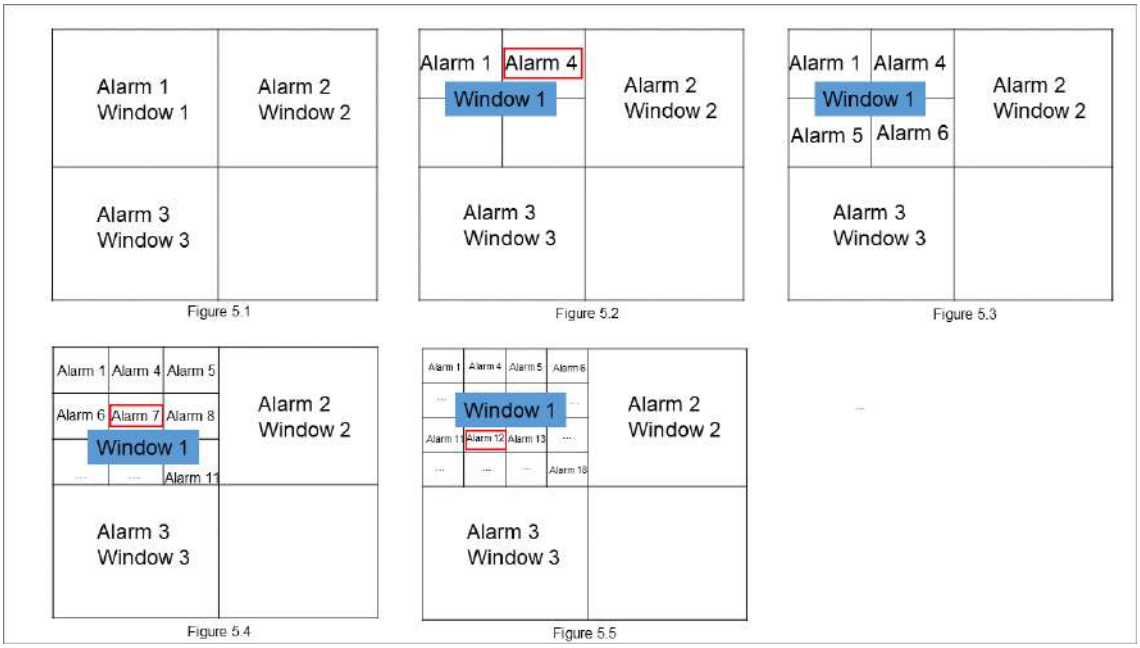


Figura 15-5 Vários alarmes exibidos no Smart Wall

Observação

As regras de alarme dos alarmes exibidos nas janelas não serão alteradas quando o modo de divisão da janela for alterado.

15.1.5 Ver Outros Conteúdos no Smart Wall

Você pode exibir os seguintes conteúdos no smart wall: o painel de controle, a página Estacionamento, a página Monitoramento Inteligente, a página Central de Alarmes, a página Monitoramento, sua área de trabalho e seus programas.

Tabela 15-2 Conteúdo da tela

Contente	Como fazer
Painel de controle	1. No canto superior esquerdo do Control Client, selecione → **Painel de Controle** para entrar na página Meu Painel de Controle. 2. Clique no canto superior direito do cliente e selecione uma parede inteligente para exibir o painel de controle na parede inteligente.

Contente	Como fazer
Estacionamento	1. No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Monitoramento** → **Estacionamento** para entrar no módulo Estacionamento. 2. Clique no canto superior direito do cliente e selecione uma parede inteligente para exibir a página do estacionamento na parede inteligente.
Monitoramento Inteligente	1. No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Monitoramento** → **Monitoramento inteligente** para entrar no módulo Monitoramento inteligente. 2. Clique no canto superior direito do cliente e selecione uma parede inteligente para exibir a página Monitoramento Inteligente na parede inteligente.
Central de Alarmes	1. No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Monitoramento** → **Central de alarmes** para entrar no módulo Central de alarmes. 2. Clique no canto superior direito do cliente e selecione um smart wall para exibir a página da central de alarmes no smart wall.
Monitoramento	1. No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Monitoramento** → **Monitoramento** para entrar no módulo Monitoramento. 2. Clique no canto superior direito do cliente e selecione uma parede inteligente para exibir a página de monitoramento na parede inteligente.
Desktop ou Programas	Selecione para selecionar sua área de trabalho ou determinados programas no mural de vídeo. **Observação** Esta função está disponível apenas para o Windows 10 (versão 1907 e posteriores).

15.1.6 Visualizar e Exportar Janela Nº e ID da Câmera

Ao exibir a visualização ao vivo no smart wall, você pode usar um teclado para operações convenientes, como iniciar a visualização ao vivo no smart wall, controle PTZ, etc. Se você quiser

exibir a visualização ao vivo de determinada câmera em determinada janela no smart wall, você deve pressionar o número do identificador da câmera e o número da janela de destino no teclado, que são chamados de **ID da câmera** e **Nº da janela** .
No Web Client, você pode definir um ID exclusivo para cada câmera adicionada no sistema. Para obter detalhes, consulte o *Manual do Usuário do HikCentral Professional Web Client* .
No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Monitoramento** → **Controle de parede inteligente** e clique em → **Exibir número da janela** para mostrar o número de cada janela.
Se você quiser exportar um documento que contém os IDs de todas as câmeras e informações da parede inteligente (como nome da parede inteligente, linha e coluna, etc.) como referência, clique em → **Exibir nº da janela e ID da câmera** para gerar um documento.
Clique em **Download** para baixar este documento e salvá-lo no PC local. Você pode imprimi-lo se necessário.

Observação

- O arquivo exportado está no formato PDF.
- O documento exportado também contém o número do smart wall, que é usado para selecionar o smart wall por meio do teclado de rede.

15.2 Gerenciar Parede de Tela (Placa Gráfica)

Screen Wall (placa gráfica) é independente de hardware. Não requer nenhum recurso de decodificação, como controladores de video wall ou decodificadores. O PC que executa o cliente pode decodificar os fluxos por sua placa gráfica e, em seguida, exibir o conteúdo nas telas conectadas ao PC. Como resultado, é uma solução econômica e fácil de implementar.
Esse tipo de parede de tela é usado principalmente em pequenos cenários de monitoramento, como supermercados, com menos de quatro unidades de exibição necessárias.

Figura 15-9 Cenário de aplicação: Parede de tela (placa gráfica)

Neste modo de parede de tela, você pode exibir não apenas os vídeos da câmera na parede de tela, mas também outros conteúdos de exibição, como mapas, status de saúde, página de monitoramento, etc.

Observação

Até quatro telas são suportadas como paredes de tela para um Control Client neste modo.
Você precisa primeiro configurar a permissão do usuário no Web Client para exibir os recursos de parede de tela. Para obter detalhes sobre como definir os parâmetros, consulte o *HikCentral Professional Web Client User Manual* .

15.2.1 Exibir Conteúdo no Smart Wall no Modo Smart Wall

Uma variedade de conteúdos (por exemplo, vídeo, mapa) pode ser compartilhada no smart wall para ajudar você a responder de forma rápida e eficaz. O modo smart wall (placa gráfica) fornece uma maneira conveniente de configurar o smart wall inicial, verificar a visão geral completa do layout do smart wall ou ajustar o layout do smart wall. Você pode selecionar a tela inteligente desejada e entrar neste modo para definir a divisão da janela (com suporte de telas de LED e LCD), ajustar o layout, exibir o conteúdo no smart wall ou executar outras operações.

Antes de começar

Certifique-se de ter habilitado a função **de decodificação de hardware da GPU** em → **Vídeo** → **Exibição** .

Passos

1. No canto superior esquerdo, selecione → **Todos os módulos** → **Monitoramento** → **Controle de parede inteligente** .
2. Entre no **Modo Smart Wall** .
   – Clique duas vezes em uma parede inteligente na lista de paredes inteligentes.
   – Arraste uma parede inteligente da lista de paredes inteligentes para a área de layout da parede inteligente.
3. Opcional: clique no canto inferior esquerdo para escolher a divisão de janela predefinida para definir o layout da janela de exibição do smart wall.
4. No modo de parede inteligente, exiba o conteúdo na parede inteligente.
   – Exibir câmera no Smart Wall: clique duas vezes no nome de uma câmera ou arraste a câmera para a área de layout do Smart Wall para exibi-la no Smart Wall.
   – Exibir mapa no Smart Wall: clique duas vezes no mapa ou arraste-o para a área de layout do Smart Wall para exibir o mapa no Smart Wall.
   – Área de exibição no Smart Wall: clique duas vezes na área ou arraste a área para a área de layout do Smart Wall para exibir os recursos na área do Smart Wall.

   Observação

   Se houver vários recursos na área, ao arrastá-los para a área de layout do smart wall, você precisará selecionar **Reproduzir em lote** ou **Troca automática de janela única** / **troca automática de várias janelas** para exibir cada recurso em uma janela de exibição ou troca automática de área de exibição em uma/várias janelas de exibição no smart wall.

   – Exibir visualização no Smart Wall: arraste a visualização para a área de layout do Smart Wall e selecione **Troca automática de tela única** ou **Substituir visualização atual** para exibir a troca automática de visualização em uma janela de exibição ou substituir o conteúdo de exibição atual no Smart Wall.
   – Exibir grupo de visualização no Smart Wall: arraste o grupo de visualização para a área de layout do Smart Wall para exibir a alternância automática de cada visualização em uma janela de exibição no Smart Wall.
   – Exibir comparação de imagens de rosto no Smart Wall: clique duas vezes na biblioteca de imagens de rosto ou arraste-a para a área de layout do Smart Wall para exibir o resultado da comparação de imagens de rosto no Smart Wall.
5. Opcional: No modo de parede inteligente (placa gráfica), execute uma das seguintes operações.

Ver canal de recursos	Você pode visualizar todos os canais de recursos exibidos no smart wall.
Ajustar janela de exibição	Arraste uma janela de exibição para outra para ajustar a ordem do layout no smart wall.
Editar Nome	Clique ··· e selecione **Editar nome** para editar o nome do smart wall.
Mostrar parede inteligente	Clique ··· e selecione **Mostrar parede inteligente** para mostrar o nome na parede inteligente.

Exibir ou não exibir alarme na tela	Clique para desabilitar a exibição do alarme na tela correspondente quando um alarme for disparado. Clique para restaurar a exibição do alarme na tela.
Sair do Modo Smart Wall	Clique **em Sair do Modo Smart Wall** para sair do modo.

15.2.2 Exibir Conteúdo no Smart Wall no Modo Live View

Durante a exibição ao vivo, se você vir algo importante na janela de exibição ao vivo, por exemplo, um suspeito capturado por uma câmera ou um VIP correspondido no painel de comparação de imagens de rosto, você pode exibir esses conteúdos no smart wall para obter uma visão geral completa e maior.
Após exibir o conteúdo ao vivo no smart wall (em outro display) neste modo, você pode continuar a visualizar outro conteúdo ao vivo ou executar outras operações no Control Client no display atual, sem alterar o conteúdo que o smart wall exibe. Esta função permite que você fique de olho no seu smart wall enquanto trabalha no Control Client. Por exemplo, o smart wall continua a mostrar o vídeo atual enquanto você inicia a reprodução desta câmera no Control Client.

Exibir todo o conteúdo em visualização ao vivo no Smart Wall

No módulo Monitoramento, você pode exibir todo o conteúdo que está visualizando nas janelas de exibição na parede inteligente (placa gráfica) para obter uma visão geral maior por meio de uma operação de um toque.

Observação

Certifique-se de ter habilitado a função **de decodificação de hardware da GPU** em → **Vídeo básico** → **Exibição** .

Após iniciar a visualização ao vivo, clique no canto superior direito do Control Client e selecione uma parede inteligente para exibir todas as janelas de exibição na parede inteligente.

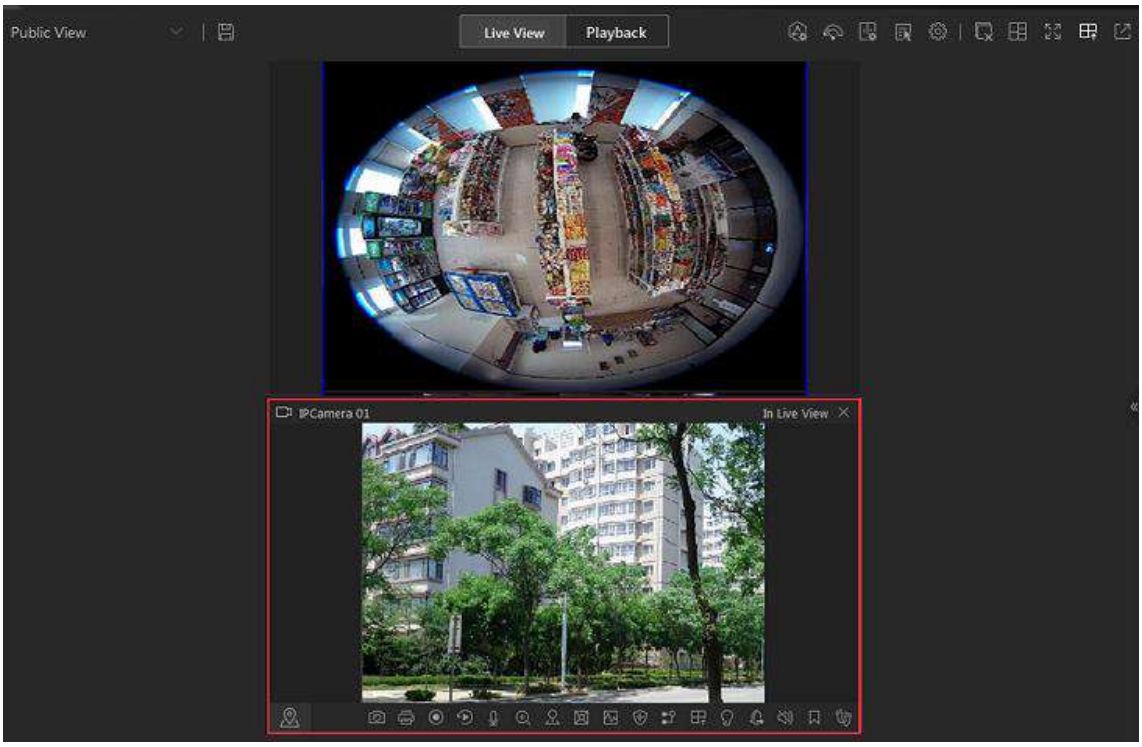


Figura 15-10 Exibir todo o conteúdo em visualização ao vivo no Smart Wall

Observação

O conteúdo inclui todos os recursos exibidos na área de exibição, como vídeos das câmeras, mapas, bibliotecas de imagens de rostos, pontos de acesso, etc.

Passe o cursor na parte superior da tela do smart wall e clique em **Sair do Modo Smart Wall** para parar de exibir o conteúdo no smart wall.

Exibir câmera na parede inteligente

Você pode exibir a visualização ao vivo de uma câmera na parede inteligente sem decodificação, para mostrar detalhes da área monitorada pela câmera em tempo hábil.

Antes de começar

- Conecte seu PC a pelo menos uma parede inteligente.
- Certifique-se de ter habilitado a função **de decodificação de hardware da GPU** em → **Vídeo básico** → **Exibição** .

Passos

1. No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Monitoramento** → **Monitoramento** .
2. Opcional: clique no canto inferior esquerdo para selecionar um modo de divisão de janela.
3. Exiba a visualização ao vivo de uma câmera na parede inteligente.
   – Passe o cursor sobre uma janela de visualização ao vivo, clique na barra de ferramentas da janela e selecione uma parede inteligente.

Observação

Você também pode clicar em **Smart Wall (Dispositivo de decodificação)** para decodificar e exibir esta câmera no Smart Wall.

– Passe o cursor sobre o nome de uma câmera, clique em e depois passe o cursor sobre **Exibir na parede** para selecionar uma parede inteligente.

4. Opcional: Use um teclado USB (como o DS-1005KI) para iniciar a visualização ao vivo de uma determinada câmera na parede inteligente pressionando o número identificador da câmera.

Observação

No Web Client, você pode definir um ID exclusivo para cada câmera adicionada no sistema. Para obter detalhes, consulte o *Manual do Usuário do HikCentral Professional Web Client* .

Área de exibição na parede inteligente

Você pode exibir a visualização ao vivo de todas as câmeras em uma área na parede inteligente para visualizar os detalhes de uma área em tempo hábil e ter uma visão geral da área.

Antes de começar

- Conecte seu PC a pelo menos uma parede inteligente.
- Certifique-se de ter habilitado a função **de decodificação de hardware da GPU** em → **Vídeo básico** → **Exibição** .

Passos

1. No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Monitoramento** → **Monitoramento** .
2. Passe o cursor sobre o nome de uma área, clique em e depois passe o cursor sobre **Exibir na parede** para selecionar uma parede inteligente para exibir todas as câmeras na área na parede inteligente.

Exibir Mapa no Smart Wall

Você pode exibir E-map e mapa GIS no smart wall para mostrar o layout geral e os locais dos dispositivos adicionados, ou dispositivos de um certo tipo. As informações de alarme serão exibidas no smart wall também quando um alarme for disparado.

Antes de começar

- Configure um mapa GIS ou E-map via Web Client antecipadamente. Para detalhes, veja *o Manual do Usuário do HikCentral Professional Web Client* .
- Certifique-se de ter habilitado a função **de decodificação de hardware da GPU** em → **Vídeo básico** → **Exibição** .

Passos

1. No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Monitoramento** → **Monitoramento** .
2. Opcional: clique no canto inferior esquerdo para selecionar um modo de divisão de janela.
3. Exiba um mapa na parede inteligente.
   – Passe o cursor sobre **Mapa** , clique e mova o cursor sobre **Exibir na parede** para selecionar uma parede inteligente.
   – Clique duas vezes **em Map** para exibi-lo no painel direito. Clique no canto superior direito da janela de exibição do mapa e selecione uma parede inteligente.

Observação

Os dispositivos adicionados ao mapa serão exibidos com o mapa.

Exibir visualização e visualizar grupo no Smart Wall

Se você salvou uma visualização, pode exibi-la no smart wall em tempo hábil com a divisão de janelas salva e a correspondência entre câmeras e janelas.

Passos

1. No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Monitoramento** → **Monitoramento** .
2. Clique para abrir o painel Exibir.
3. No canto superior esquerdo da janela de visualização ao vivo, selecione uma visualização ou grupo de visualizações na lista suspensa e passe o cursor em **Exibir no Smart Wall** para selecionar um smart wall.
   A visualização ou grupo de visualizações será exibido na parede inteligente selecionada no modo de divisão de janela salvo.

15.2.3 Exibir Vídeo Relacionado ao Alarme no Smart Wall

Se você habilitou a ligação de parede inteligente para um alarme, a visualização ao vivo de câmeras ou visualizações públicas relacionadas ao alarme aparecerão na parede inteligente escolhida quando o alarme for disparado. Portanto, você saberá os detalhes do alarme em tempo hábil para operações futuras. Você também pode exibir manualmente a visualização ao vivo de uma das câmeras relacionadas ao alarme na parede inteligente.

Antes de começar

- Configure um alarme (e habilite a ligação de parede inteligente para ele) por meio do Web Client de antemão. Para obter detalhes, consulte *o Manual do Usuário do HikCentral Professional Web Client* .
- Certifique-se de ter habilitado a função **de decodificação de hardware da GPU** em → **Vídeo básico** → **Exibição** .

Passos

1. No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Monitoramento** → **Central de alarmes** para entrar no módulo Central de alarmes.
   As informações dos alarmes disparados serão exibidas.
2. Opcional: clique em um alarme para exibir a visualização ao vivo do alarme na janela **Vídeo e imagem relacionados** no canto inferior esquerdo do cliente para uma prévia.
3. Exibir visualização ao vivo de uma câmera relacionada a um alarme na parede inteligente.

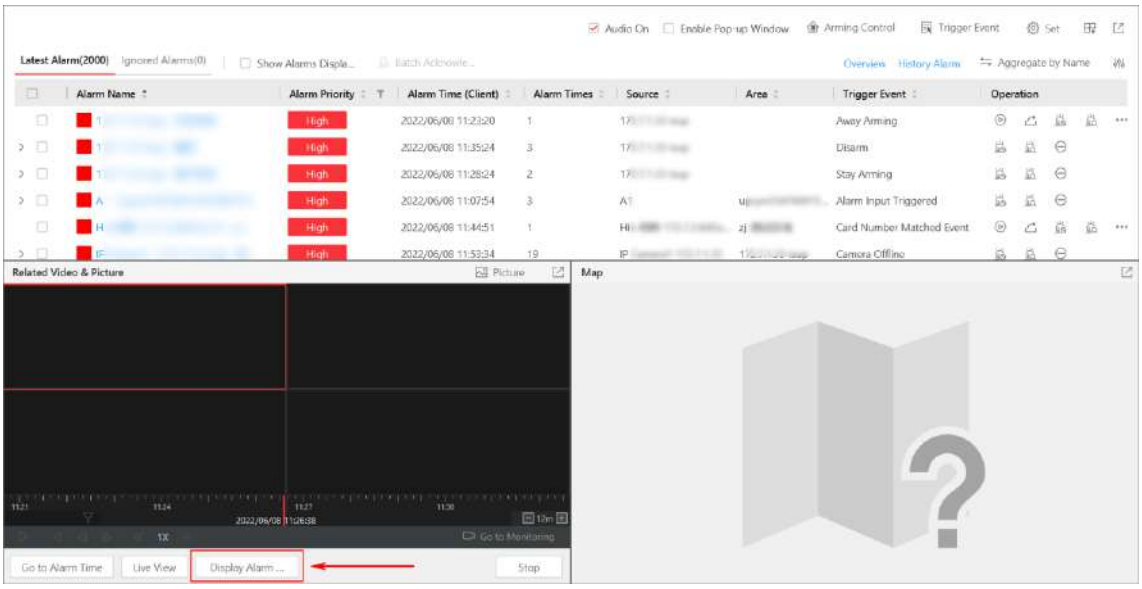


Figura 15-11 Vídeo relacionado ao alarme de exibição no Smart Wall

Se você estiver visualizando o vídeo da câmera na janela Vídeo e imagem relacionados, clique em **Exibir alarme no Smart Wall** abaixo da janela para selecionar um smart wall.

4. Opcional: Passe o cursor na parte superior da parede inteligente em exibição para mostrar a barra Sair do Modo de Parede Inteligente e, em seguida, clique para habilitar a exibição automática de alarme e vídeo na parede atual.
   - O ícone muda para . As câmeras ou visualizações relacionadas dos alarmes configurados com a ligação de parede inteligente podem ser exibidas na parede inteligente automaticamente quando acionadas.

Figura 15-12 Sair da barra do modo Smart Wall

   - Se você tiver desativado a exibição automática de alarme e vídeo na parede atual, o nome da parede inteligente mudará para (Alarme Desativado)Nome da Parede Inteligente.

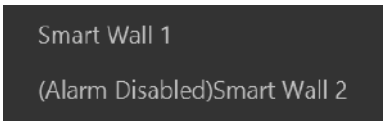


Figura 15-13 Nome do Smart Wall com alarme desabilitado

Observação

Esta configuração não será alterada após reiniciar o Control Client.

5. Selecione → **Todos os módulos** → **Monitoramento** → **Monitoramento** → **Controle de parede inteligente** e clique duas vezes no nome da parede inteligente em funcionamento para entrar no Modo de parede inteligente no cliente.
   - As janelas das câmeras relacionadas ao alarme serão exibidas no painel direito com uma barra de título vermelha em modo de bloco, com o nome de cada câmera sendo exibido nas respectivas janelas.
   - Para visualização relacionada ao alarme, a visualização será exibida no painel direito, cobrindo as imagens que você está visualizando no modo de divisão de janela salvo.
6. Opcional: execute as seguintes operações, se necessário.

Ver detalhes do alarme	Clique na barra de título vermelha no cliente para abrir a janela de informações do alarme para obter detalhes.
Mudar para o modo de comutação automática	Clique para alternar entre o modo de bloco e o modo de troca automática para as câmeras relacionadas ao alarme.

Observação

- No modo de troca automática, você pode passar o cursor sobre a janela de exibição para executar operações, incluindo troca de transmissão, alternância entre reprodução instantânea e visualização ao vivo, gravação, troca de câmera, avanço rápido e avanço lento.
- Até 64 janelas podem ser exibidas na parede inteligente. Você pode executar as tarefas mencionadas acima para controlar a exibição de visualização ao vivo das câmeras e visualizações.
- Se você tiver habilitado o alarme no smart wall, a visualização ao vivo dos alarmes com prioridade mais alta cobrirá a dos alarmes com prioridade mais baixa antes do horário previsto para a exibição no smart wall.
- Você pode configurar o tempo devido da exibição do smart wall por meio do Web Client. Para obter detalhes, consulte *o Manual do Usuário do HikCentral Professional Web Client* .
- Quando vários alarmes com a mesma ligação câmera/visualização são acionados, os alarmes serão exibidos na parede inteligente mostrando o número do alarme. Quando um novo alarme com a ligação câmera/visualização é acionado, o número muda. O título da janela de alarme mostra o nome do alarme com a maior prioridade. Passe o cursor sobre o nome do alarme, você pode visualizar todos os alarmes em ordem de tempo e prioridade e lidar com eles em um lote.

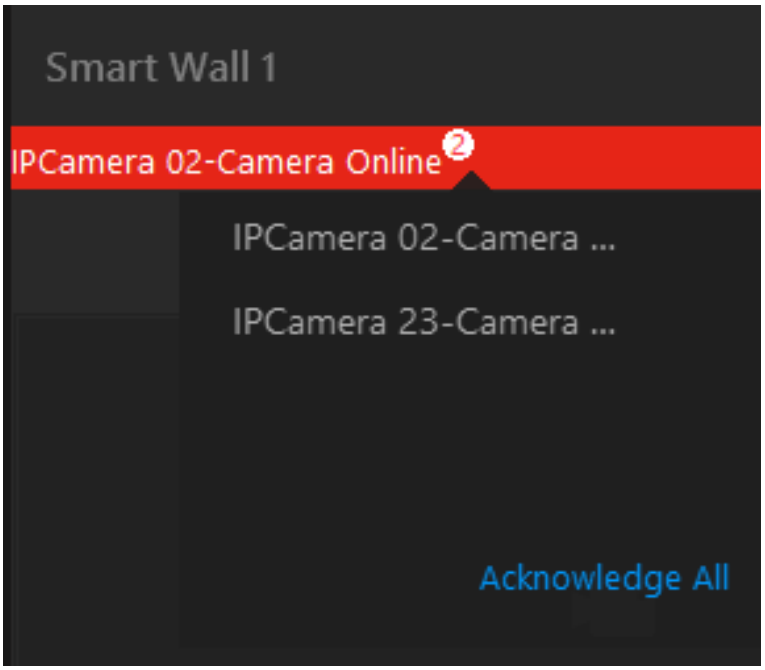


Figura 15-14 Exibir vários alarmes com a mesma ligação de câmera/visualização no Smart Wall

15.2.4 Exibir Página de Monitoramento de Saúde no Smart Wall

Você pode exibir a página de monitoramento de saúde no smart wall para ter uma visão geral do status dos dispositivos adicionados e do HikCentral Professional Service.

Antes de começar

Adicione dispositivos ao HikCentral Professional por meio do Web Client. Para obter detalhes, consulte *o Manual do Usuário do HikCentral Professional Web Client* .

Passos

1. No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Manutenção** → **Monitoramento de integridade** para entrar no módulo Monitoramento de integridade.
   O status geral dos dispositivos adicionados e do HikCentral Professional Service será exibido.
2. Clique no canto superior direito do cliente e selecione um smart wall para exibir a página de monitoramento de saúde no smart wall.

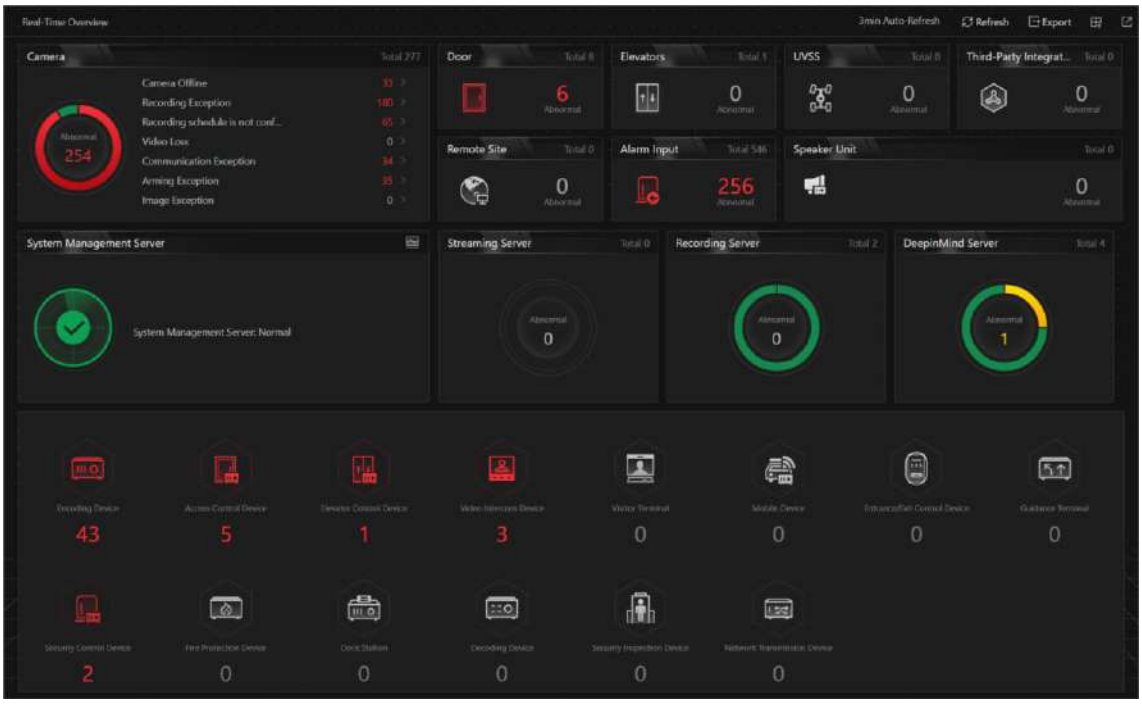


Figura 15-15 Exibir página de monitoramento de saúde no Smart Wall

3. Opcional: clique em **Sair do modo Smart Wall** no Smart Wall para parar de exibir a página de monitoramento de saúde no Smart Wall.

15.2.5 Exibir Área de Trabalho no Smart Wall

Para certos cenários, você pode compartilhar o conteúdo do seu desktop no smart wall para melhor exibição e experiência. Você pode adicionar o PC executando o servidor RSC ao HikCentral Professional e exibi-lo no smart wall como uma câmera normal.

Passos

1. Instale o servidor RSC no PC local e defina a senha para o servidor RSC.

Observação

Você pode entrar em contato com nosso suporte técnico para obter o pacote de instalação do RSC Server.

Cuidado

A força da senha do dispositivo pode ser verificada automaticamente. Recomendamos fortemente que você altere a senha de sua escolha (usando um mínimo de 8 caracteres, incluindo pelo menos três tipos das seguintes categorias: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. E recomendamos que você altere sua senha regularmente, especialmente no sistema de alta segurança, alterar a

senha mensalmente ou semanalmente pode proteger melhor seu produto.
A configuração adequada de todas as senhas e outras configurações de segurança é de responsabilidade do provedor de serviços e/ou usuário final.

2. Entre na página Gerenciamento de dispositivos de codificação do Web Client para adicionar o PC (considerado um dispositivo de codificação) executando o servidor RSC ao HikCentral Professional por endereço IP.

Observação

Ao adicionar o PC ao HikCentral Professional, o número da porta padrão é 8000 e a senha deve ser a mesma configurada no servidor RSC na Etapa 1.

3. Opcional: configure as configurações relacionadas no Web Client, se necessário, como adicionar a câmera virtual do PC à área, configurar a gravação e definir o servidor de streaming.

Observação

- Depois de adicionar a câmera virtual do PC à área, você pode executar operações básicas da mesma forma que com câmeras normais.
- Se você quiser gravar o vídeo para a área de trabalho exibida no smart wall, precisará configurar os parâmetros de gravação para a câmera virtual e não poderá selecionar o dispositivo de codificação como local de armazenamento.
- A câmera virtual do PC não é calculada como o número da câmera da licença que você comprou.

4. No Control Client, selecione → **Todos os módulos** → **Monitoramento** → **Monitoramento** para entrar no módulo Monitoramento.
5. Exiba sua área de trabalho no smart wall.
   – Entre **no Modo Smart Wall** e clique duas vezes no nome da câmera virtual do PC ou arraste a câmera virtual do PC para a área de layout da área do Smart Wall para exibir a área de trabalho no Smart Wall.

   Observação

   Para obter mais detalhes sobre como entrar no **Modo Smart Wall** , consulte ***Exibir conteúdo no Smart Wall no Modo Smart Wall*** .

   – Clique na aba **Recurso Local** e passe o cursor sobre o nome da câmera virtual do PC. Então você pode clicar em → **Exibir na Parede** e selecionar uma parede inteligente para exibir a área de trabalho na parede inteligente.

   O ícone da câmera virtual mudará para , e sua área de trabalho será exibida no smart wall.

Capítulo 16 Busca de Pessoa

O sistema suporta reconhecimento facial, funções de comparação e busca rápida. Após adicionar dispositivos que suportam reconhecimento facial, os dispositivos podem reconhecer rostos e comparar com as pessoas no sistema.
Além do reconhecimento facial, você também pode adicionar servidores de reconhecimento facial ao sistema e definir tarefas de reconhecimento do corpo humano.
No Control Client, o operador pode visualizar as informações de comparação de imagens faciais em tempo real durante a visualização ao vivo e ver se as pessoas detectadas correspondem ou não às informações pessoais na biblioteca de imagens faciais predefinida. O operador também pode visualizar as informações de reconhecimento do corpo humano ao visualizar o vídeo ao vivo das câmeras vinculadas ao servidor de reconhecimento facial e configuradas com reconhecimento do corpo humano.
No canto superior esquerdo, selecione → **Todos os módulos** → **Investigação** → **Pesquisa de pessoas** .

16.1 Pesquisa Rápida de Pessoas

Você pode pesquisar rapidamente rostos e corpos humanos usando recursos e fotos carregadas, pesquisar rapidamente por arquivo de pessoa por fotos carregadas e pesquisar rapidamente por informações de pessoa alvo. Após a pesquisa, você pode visualizar as fotos ou arquivos de vídeo relacionados aos resultados da pesquisa, salvar os resultados da pesquisa no PC local, etc.

Observação

Certifique-se de que sua licença suporta a função de reconhecimento facial, ou vá para a página inicial do Web Client, clique em **License Details** → **Configuration** → **Add** e então selecione as câmeras adicionadas como câmeras de reconhecimento facial. Caso contrário, a função de reconhecimento facial não pode executar normalmente no sistema.

Pesquise rapidamente imagens de destino por recursos

As imagens de rostos e corpos humanos capturados podem ser pesquisadas por características faciais/corporais da pessoa.
No painel de navegação esquerdo, selecione **Pesquisa rápida** → **Recurso** .

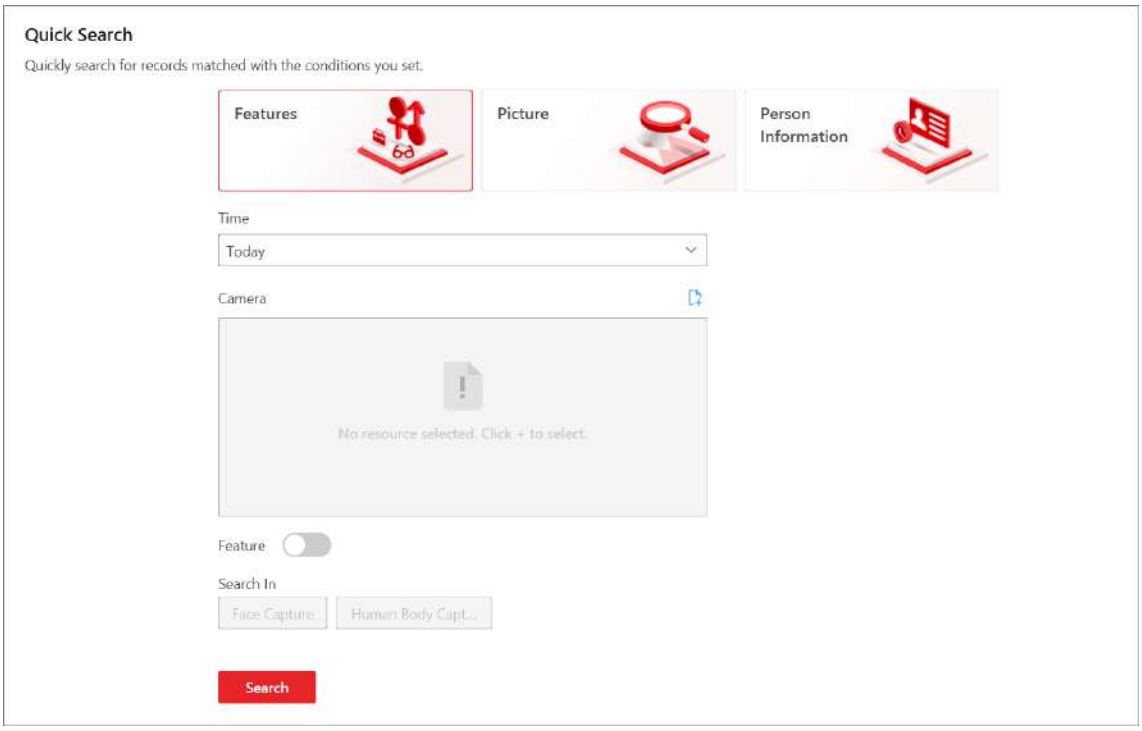


Figura 16-1 Busca rápida de imagens de rosto capturadas por recurso

Após definir as condições de pesquisa, selecione **Captura de rosto** ou **Captura de corpo humano** como alvo da pesquisa. Na página de resultados da pesquisa, você pode executar mais operações. Consulte ***Pesquisar imagens de rosto capturadas por recurso*** e ***Pesquisar imagens de corpo humano capturadas por recursos*** .

Use a imagem para pesquisar rapidamente as imagens de destino

Use imagens para pesquisar rapidamente capturas de rostos e corpos humanos de pessoas-alvo.
No painel de navegação esquerdo, selecione **Pesquisa rápida** → **Imagem** .
Após definir as condições de pesquisa, selecione **Captura de rosto** ou **Captura de corpo humano** como alvo da pesquisa. Na página de resultados da pesquisa, você pode executar mais operações. Consulte ***Pesquisar imagens de rosto por imagem*** e ***Pesquisar imagens de corpo humano por imagem*** .

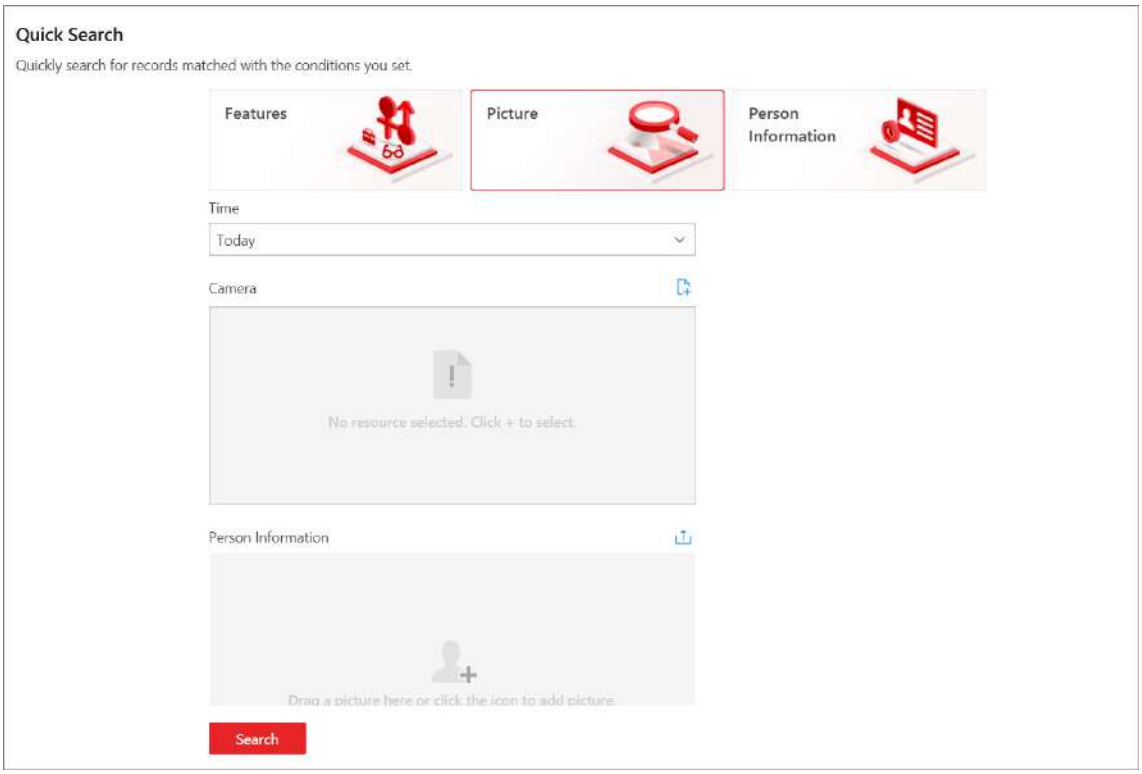


Figura 16-2 Use a imagem para pesquisar rapidamente por imagens e arquivos de rostos e corpos humanos capturados

Use a imagem para pesquisar arquivos rapidamente

Observação

Certifique-se de ter adicionado um servidor de análise inteligente ao sistema e configurado a câmera de captura e a biblioteca de imagens de rosto para ele.

Pesquise rapidamente arquivos de pessoas por uma imagem para verificar as imagens ou vídeos capturados de pessoas semelhantes na biblioteca. Você também pode verificar se uma pessoa é um estranho.

No painel de navegação esquerdo, selecione **Pesquisa rápida** → **Imagem** .

Defina as condições de pesquisa e clique em **Search** . Na página de resultados da pesquisa, você pode executar mais operações. Veja ***Search for Archives*** .

Pesquise rapidamente informações pessoais

Selecionando hora e departamento e inserindo o nome de uma pessoa, faça uma busca rápida por pessoas na plataforma.

No painel de navegação esquerdo, selecione **Pesquisa rápida** → **Informações da pessoa** .

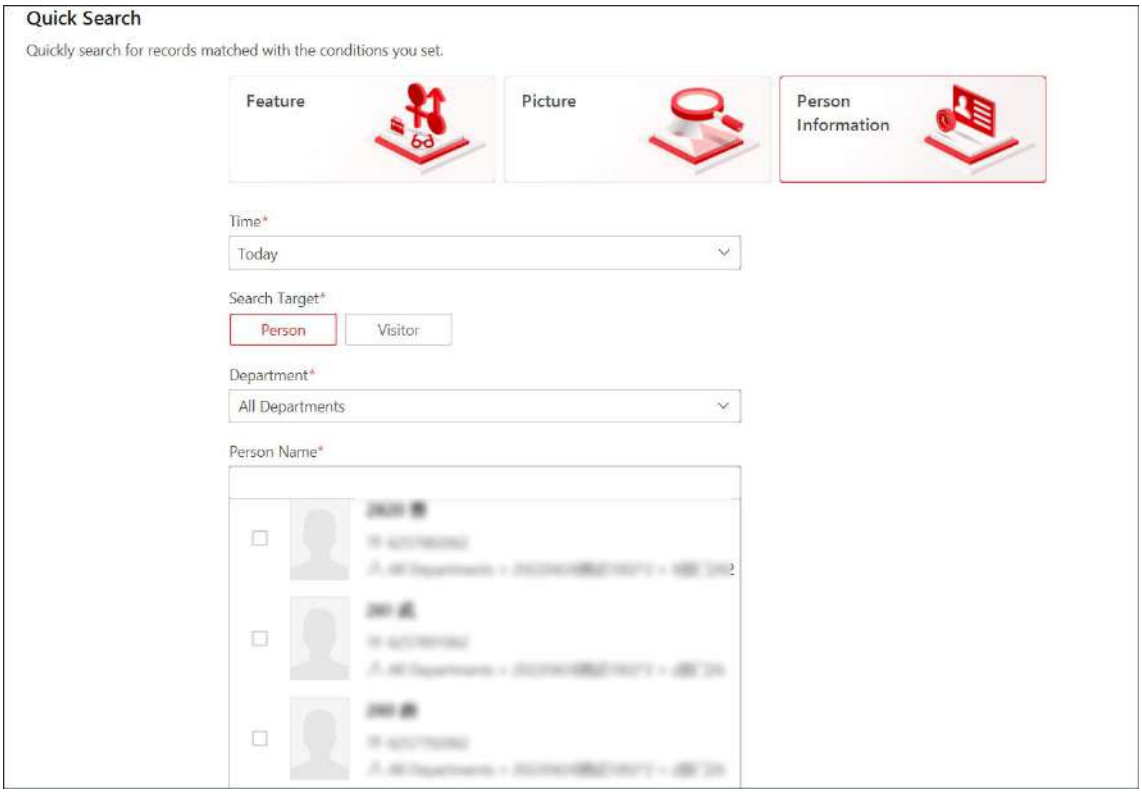


Figura 16-3 Pesquisa rápida de informações pessoais

Defina as condições de pesquisa e clique em **Pesquisar** .
As informações da pessoa, incluindo informações básicas (como tipo de pessoa, departamento e número da placa do veículo), registros de acesso, eventos de patrulha e registros de passagem de veículos são exibidos.

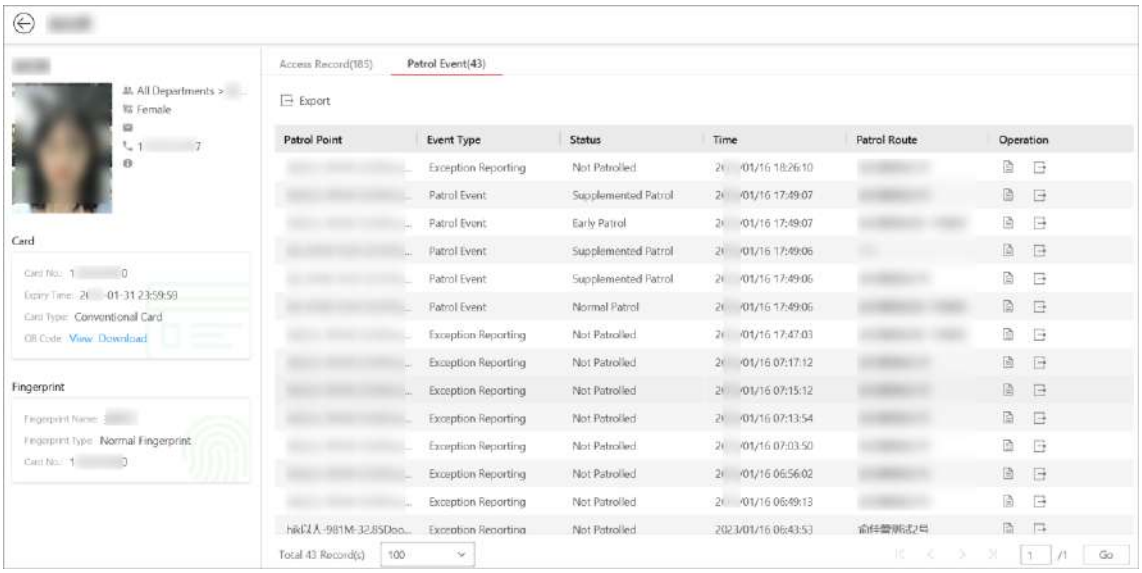


Figura 16-4 Informações da pessoa pesquisada

Execute as seguintes operações para as informações da pessoa pesquisada.

Credenciais	No painel esquerdo, visualize os detalhes do cartão adicionado e a impressão digital da pessoa. Na área do cartão, você pode clicar em **Exibir** para visualizar o código QR do cartão e clicar em **Baixar** para baixar a imagem do código QR para o armazenamento local para operações posteriores. **Observação** Esta operação é suportada somente quando as credenciais foram adicionadas às informações da pessoa. Para obter detalhes sobre o gerenciamento de credenciais de pessoas, consulte o *HikCentral Professional Web Client User Manual* .
Captura de rosto	Clique em **Captura de rosto** para visualizar as imagens de rosto capturadas relacionadas à pessoa e realizar mais operações. ● Alterar a ordem de exibição. ● Clique em / / para visualizar os resultados pesquisados em miniaturas/lista/mapa. ● No modo Mapa, selecione uma ou mais imagens e clique em **Gerar Padrão** para exibir o padrão de uma determinada pessoa no mapa. ● Clique em uma imagem capturada e execute mais operações. ○ Clique em **Adicionar Pessoa** e defina os parâmetros necessários para adicionar a pessoa à lista de pessoas. Para obter detalhes sobre como definir os parâmetros, consulte o *Manual do Usuário do HikCentral Professional Web Client* . ○ Clique em **Picture Search** para ir procurar a pessoa alvo nas fotos capturadas, carregando uma foto do corpo humano. Para informações detalhadas, veja ***Search Face Pictures by Picture*** . ○ Clique em **Mais** → **Pesquisa de arquivo** para ir para a página Pesquisa de arquivo e procurar o arquivo da pessoa. ○ Clique em **Mais** → **Verificação de identidade** → **Para ser verificado** para verificar a identidade da pessoa ou clique em **Mais** → **Verificação de identidade** →

	Alvo para definir a pessoa como alvo de comparação. ○ Clique em **Mais** → **Capturas relacionadas** para exibir imagens capturadas durante 30s antes e depois de capturar a imagem atual. ○ Clique em / para ver a imagem grande e o vídeo relacionado (se disponível). ○ Clique **em Download** para baixar a imagem para o PC local.
Registros de acesso	Clique em **Registro de acesso** para visualizar os registros de acesso relacionados à pessoa e realizar mais operações. ● Clique **em Exportar** e defina o formato do arquivo para exportar a lista de registros de acesso. ● Clique na coluna Operation e defina os parâmetros relacionados para salvar o registro de acesso no Evidence Management Center. Para obter detalhes, consulte ***Evidence Management*** .
Eventos de Patrulha	Clique em **Evento de patrulha** para visualizar os eventos de patrulha relacionados à pessoa e realizar mais operações. ● Clique na coluna Operação para salvar um registro como um arquivo Excel no seu PC, incluindo os detalhes do evento, informações da pessoa, perfil da pessoa, arquivo de vídeo gravado (se configurado), etc. ● Clique para ver os detalhes do evento de patrulha, como ver o vídeo relacionado e o anexo. ● Clique em **Relatório** e defina o formato do arquivo para exportar a lista de eventos de patrulha.

16.2 Busca de Imagens Capturadas

Imagens de rosto ou corpo humano podem ser capturadas e armazenadas na plataforma. Você pode procurar as imagens de rosto ou corpo humano capturadas por características específicas ou carregando uma imagem. Você também pode procurar por imagens de rosto correspondentes com imagens no grupo de comparação e procurar pessoas por frequência.

16.2.1 Pesquisar Imagens de Rosto Capturadas por Recurso

As imagens faciais capturadas podem ser armazenadas no servidor SYS ou no Recording Server. Você pode procurar a pessoa alvo nas imagens capturadas por características faciais da pessoa. Você também pode visualizar os arquivos de vídeo relacionados aos resultados da pesquisa e

salvar os arquivos de vídeo relacionados como evidência.

Passos

Observação

Certifique-se de que sua licença suporta a função de reconhecimento facial, ou vá para a página inicial do Web Client, clique em **License Details** → **Configuration** → **Add** e então selecione as câmeras adicionadas como câmeras de reconhecimento facial. Caso contrário, a função de reconhecimento facial não pode executar normalmente no sistema.

1. No painel de navegação esquerdo, selecione **Pesquisar imagens capturadas** → **Pesquisar rostos capturados** .
2. No campo Pesquisar por, selecione **Pesquisar por recurso** .
3. No campo Tempo, defina o período de tempo.

   Você pode selecionar **Intervalo de tempo personalizado** para especificar a hora de início e de término da pesquisa.
4. Selecione a(s) câmera(s) para pesquisar as fotos do rosto.
   1) Clique para abrir o painel da lista de câmeras.
   2) Selecione o site atual ou um site remoto na lista suspensa de sites para mostrar suas câmeras.
   3) Marque a(s) câmera(s) que você deseja pesquisar.

Observação

Até 200 recursos podem ser selecionados para pesquisa ao mesmo tempo.

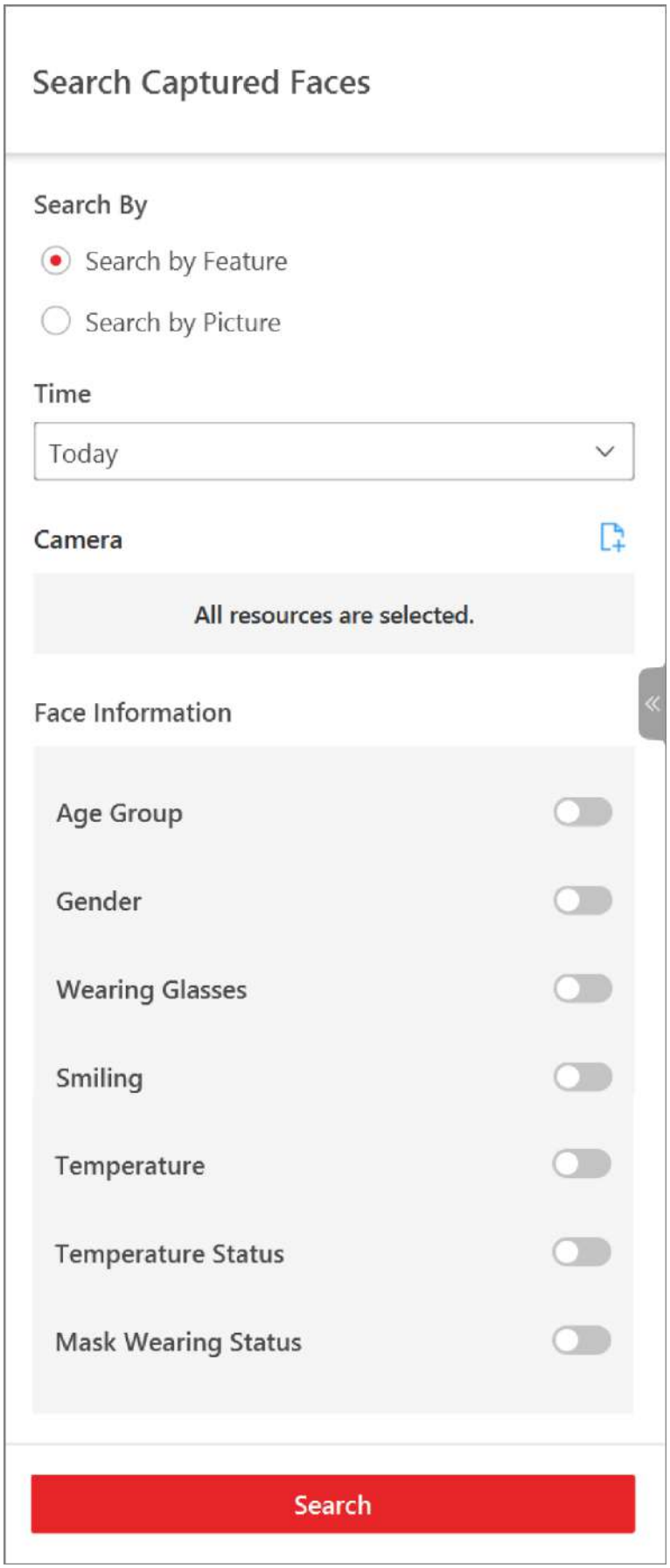

Search Captured Faces
Search By
Search by Feature
Search by Picture
Time
Today
Camera
All resources are selected.
Face Information
Age Group
Gender
Wearing Glasses
Smiling
Temperature
Temperature Status
Mask Wearing Status
Search

Figura 16-5 Pesquisar imagens capturadas

5. Opcional: defina as características do rosto e os parâmetros relacionados na área **Informações do rosto .**

Usando óculos

Após ativar, você pode filtrar fotos de rostos correspondentes, dependendo se a pessoa usa óculos/óculos de sol ou não.

Sorrindo

Após ativar, você pode filtrar fotos de rostos correspondentes, dependendo se a pessoa está sorrindo ou não.

Temperatura

Após a ativação, você pode definir um limite para procurar pessoas correspondentes cuja temperatura da superfície da pele seja igual ou superior ao limite.

Status da temperatura

Após habilitado, você pode filtrar pessoas correspondentes por status de temperatura (normal ou anormal).

Status de uso de máscara

Após ativar, você pode filtrar fotos de rosto correspondentes, dependendo se a pessoa usa máscara ou não.

Observação

Esta função deve ser suportada pelo dispositivo. Você só pode habilitar recursos faciais que são suportados pelo dispositivo.

6. Clique em **Pesquisar** .
   Os resultados da pesquisa serão exibidos.
7. Opcional: Execute as seguintes operações para as imagens pesquisadas.

Selecione o período de tempo	Arraste o controle deslizante para filtrar os resultados definindo um período de tempo em que uma foto de rosto é capturada.
Filtrar dentro dos resultados	Na parte superior da página de resultados, você pode selecionar ou verificar as condições do filtro para filtrar os resultados.
Alterar ordem de exibição	● Selecione **Cronologicamente** para exibir os resultados pesquisados em ordem cronológica. ● Selecione **Reverter cronologicamente** para exibir os resultados pesquisados em ordem cronológica reversa. ● Selecione **Câmera** para exibir os resultados pesquisados por câmeras.

Alternar modo de exibição	Os resultados pesquisados podem ser exibidos em três modos, e você pode alternar entre diferentes modos de exibição. ● Clique para visualizar os resultados da pesquisa em miniaturas. ● Clique para exibir a(s) câmera(s) no mapa e clique em uma câmera para visualizar os resultados pesquisados em miniaturas. ● Clique para visualizar os resultados da pesquisa em forma de lista.
Gerar Padrão	No modo Mapa, selecione uma ou mais imagens e clique em **Gerar Padrão** para exibir o padrão de uma determinada pessoa no mapa. **Observação** Certifique-se de ter adicionado recursos no mapa. Para obter detalhes sobre como definir os parâmetros, consulte o *HikCentral Professional Web Client User Manual* .
Abrir tela auxiliar	Clique no canto superior direito para exibir a página atual em uma tela auxiliar.

8. Opcional: Passe o cursor sobre uma imagem correspondente e execute as seguintes operações.

Adicionar à lista de pessoas	Clique em **Adicionar Pessoa** e defina os parâmetros necessários para adicionar a pessoa à lista de pessoas. Para obter detalhes sobre como definir os parâmetros, consulte o *Manual do Usuário do HikCentral Professional Web Client* .
Pesquisa de imagens	Clique em **Picture Search** para procurar a pessoa alvo nas fotos capturadas carregando uma foto de rosto. Para informações detalhadas, veja ***Search Face Pictures by Picture*** .
Pesquisa de arquivo	Clique em **Pesquisa de arquivo** para ir para a página Pesquisa de arquivo e pesquisar no arquivo da pessoa.
Verificação de identidade	Clique em **Verificação de identidade** → **A ser verificado** para verificar a identidade da pessoa ou clique em **Verificação de identidade** → **Alvo** para definir a pessoa como alvo de comparação.

9. Opcional: clique duas vezes em uma imagem capturada para visualizar informações detalhadas e você pode executar as seguintes operações.

Capturas relacionadas	Clique em **Capturas relacionadas** para exibir imagens capturadas durante 30s antes e depois da captura da imagem atual.
Ver imagem e vídeo	Clique em / para ver a imagem grande e o vídeo relacionado (se disponível).

Observação

Para instruções de controle de reprodução, consulte ***Reprodução*** . Alguns ícones podem não estar disponíveis para reprodução de imagem de rosto.

Baixar imagem Clique **em Download** para baixar a imagem para o PC local.

10. Opcional: exporte as fotos e vídeos correspondentes para o armazenamento local.
    1) Selecione os resultados correspondentes a serem exportados e clique em **Exportar** .
    2) Selecione o conteúdo a ser exportado.
    3) Selecione **Excel** ou **CSV** como formato.
    4) (Opcional) Se o conteúdo a ser exportado contiver vídeo, selecione **MP4** ou **AVI** como formato de vídeo.

    Observação

    O formato MP4 suporta criptografia. Você pode definir uma senha para criptografar o arquivo de vídeo para fins de segurança.

    5) Defina o caminho de salvamento.
    6) Clique em **Salvar** para adicionar a tarefa de download ao centro de downloads.

    Observação

    Para obter detalhes sobre como gerenciar as tarefas de download, consulte ***Gerenciar tarefas de download/upload*** .

16.2.2 Pesquisar Imagens de Rosto por Imagem

Você pode procurar por fotos de rosto carregando uma foto de rosto. Você também pode visualizar os arquivos de vídeo relacionados aos resultados da pesquisa e salvar os arquivos de vídeo relacionados como evidência.

Passos

Observação

Certifique-se de que sua licença suporta a função de reconhecimento facial, ou vá para a página inicial do Web Client, clique em **License Details** → **Configuration** → **Add** e então selecione as câmeras adicionadas como câmeras de reconhecimento facial. Caso contrário, a função de reconhecimento facial não pode executar normalmente no sistema.

1. No painel de navegação esquerdo, selecione **Pesquisar imagens capturadas** → **Pesquisar rostos capturados** .

2. No campo Pesquisar por, selecione **Pesquisa de imagem** .
3. No campo Tempo, defina o período de tempo.

   Você pode selecionar **Intervalo de tempo personalizado** para especificar a hora de início e de término da pesquisa.
4. Selecione a(s) câmera(s).
   1) Clique para abrir o painel da lista de câmeras.
   2) Selecione o site atual ou um site remoto na lista suspensa de sites para mostrar suas câmeras.
   3) Marque a(s) câmera(s) que você deseja pesquisar.

Observação

Até 200 recursos podem ser selecionados para pesquisa ao mesmo tempo.

5. Opcional: defina uma imagem para pesquisa de rosto e você pode enviar uma conforme desejar.
   – Insira uma palavra-chave de nome de pessoa ou ID de pessoa no campo Informações da pessoa para pesquisar nas pessoas adicionadas.
   – Clique em **Carregar imagem** para carregar uma foto de rosto do PC local.

   Observação

   A imagem enviada deve estar no formato JPG e o tamanho da imagem não deve ser maior que 1 GB.

   O rosto reconhecido será marcado na foto do rosto.
6. Opcional: arraste o controle deslizante para definir a similaridade.
7. Clique em **Pesquisar** .
   Os resultados da pesquisa serão exibidos.
8. Opcional: Execute as seguintes operações para as imagens pesquisadas.

Selecione o período de tempo	Arraste o controle deslizante para filtrar os resultados definindo um período de tempo em que uma foto de rosto é capturada.
Filtrar dentro dos resultados	Na parte superior da página de resultados, você pode selecionar ou verificar as condições do filtro para filtrar os resultados.
Alterar ordem de exibição	● Selecione **Cronologicamente** para exibir os resultados pesquisados em ordem cronológica. ● Selecione **Reverter cronologicamente** para exibir os resultados pesquisados em ordem cronológica reversa. ● Selecione **Similaridade** para exibir os resultados pesquisados em ordem de similaridade. ● Selecione **Câmera** para exibir os resultados pesquisados por câmeras.

Alternar modo de exibição Os resultados pesquisados podem ser exibidos em três modos, e você pode alternar entre diferentes modos de exibição.
- Clique para visualizar os resultados da pesquisa em miniaturas.
- Clique para exibir a(s) câmera(s) no mapa e clique em uma câmera para visualizar os resultados pesquisados em miniaturas.
- Clique para visualizar os resultados da pesquisa em forma de lista.

Gerar Padrão No modo Mapa, selecione uma ou mais imagens e clique em **Gerar Padrão** para exibir o padrão de uma determinada pessoa no mapa.

Observação

Certifique-se de ter adicionado recursos no mapa. Para obter detalhes sobre como definir os parâmetros, consulte o *HikCentral Professional Web Client User Manual* .

Abrir tela auxiliar Clique no canto superior direito para abrir a página atual em uma tela auxiliar.

9. Opcional: Passe o cursor sobre uma imagem correspondente e execute as seguintes operações.

Adicionar à lista de pessoas Clique em **Adicionar Pessoa** e defina os parâmetros necessários para adicionar a pessoa à lista de pessoas. Para obter detalhes sobre como definir os parâmetros, consulte o *HikCentral Professional Web Client User Manual* .

Pesquisa de imagens Clique em **Picture Search** para procurar a pessoa alvo nas fotos capturadas carregando uma foto de rosto. Para informações detalhadas, veja ***Search Face Pictures by Picture*** .

Pesquisa de arquivo Clique em **Pesquisa de arquivo** para ir para a página Pesquisa de arquivo e pesquisar no arquivo da pessoa.

Verificação de identidade Clique em **Verificação de identidade** → **A ser verificado** para verificar a identidade da pessoa ou clique em **Verificação de identidade** → **Alvo** para definir a pessoa como alvo de comparação.

10. Opcional: clique duas vezes em uma imagem capturada para visualizar informações detalhadas e você pode executar as seguintes operações.

Capturas relacionadas Clique em **Capturas relacionadas** para exibir imagens capturadas durante 30s antes e depois da imagem capturada.

Ver imagem e vídeo Clique em / para ver a imagem grande e o vídeo relacionado (se disponível).

Observação

Para instruções de controle de reprodução, consulte ***Reprodução*** . Alguns ícones podem não estar disponíveis para reprodução de imagem de rosto.

Baixar imagem Clique **em Download** para baixar a imagem para o PC local.

11. Opcional: exporte as fotos e vídeos correspondentes para o armazenamento local.
    1) Selecione os resultados correspondentes a serem exportados e clique em **Exportar** .
    2) Selecione o conteúdo a ser exportado.
    3) Selecione **Excel** ou **CSV** como formato.
    4) (Opcional) Se o conteúdo a ser exportado contiver vídeo, selecione **MP4** ou **AVI** como formato de vídeo.

Observação

O formato MP4 suporta criptografia. Você pode definir uma senha para criptografar o arquivo de vídeo para fins de segurança.

    5) Defina o caminho de salvamento.
    6) Clique em **Salvar** para adicionar a tarefa de download ao centro de downloads.

Observação

Para obter detalhes sobre como gerenciar as tarefas de download, consulte ***Gerenciar tarefas de download/upload*** .

16.2.3 Pesquisar Imagens Capturadas do Corpo Humano por Características

Você pode pesquisar fotos de pessoas definindo características da pessoa. Para os resultados pesquisados, você pode visualizar os arquivos de vídeo relacionados (se disponíveis) e salvar os arquivos de vídeo no armazenamento local. Pode ajudar a descobrir o suspeito alvo em locais como bancos e joalherias quando você conhece algumas características de um suspeito.

Antes de começar

Certifique-se de ter adicionado servidor(es) de análise inteligente ou servidor(es) de fusão inteligente no cliente web.

Passos

1. No painel de navegação esquerdo, selecione **Pesquisar imagens capturadas** → **Pesquisar capturas de corpos humanos** .
2. No campo Pesquisar por, selecione **Pesquisar por recurso** .

3. No campo Tempo, defina o período de tempo.

Observação

Você pode selecionar **Custom Time Interval** para especificar o horário de início e término da pesquisa. O intervalo de tempo personalizado não deve ser maior que 7 dias.

4. Clique para selecionar a(s) câmera(s) na lista de câmeras pop-up.

Observação

Você pode inserir uma palavra-chave na caixa de pesquisa para encontrar rapidamente a(s) câmera(s) de destino.

5. Opcional: No campo Informações da pessoa, habilite as opções de recursos pessoais correspondentes, conforme desejado, como usar óculos.

Observação

Esta função deve ser suportada pelo dispositivo. Você só pode habilitar recursos pessoais que são suportados pelo dispositivo.

6. Clique em **Pesquisar** .
   Os resultados da pesquisa serão exibidos cronologicamente.
7. Opcional: Para os resultados pesquisados, você pode executar mais operações.

Selecione o período de tempo	Arraste o controle deslizante para filtrar os resultados definindo um período de tempo em que uma foto corporal é capturada.
Alternar modo de exibição	Os resultados pesquisados podem ser exibidos em três modos, e você pode alternar entre diferentes modos de exibição. ● Clique para visualizar os resultados da pesquisa em miniaturas. ● Clique para exibir a(s) câmera(s) no mapa e clique em uma câmera para visualizar os resultados pesquisados em miniaturas. ● Clique para visualizar os resultados da pesquisa em forma de lista.
Alterar ordem de exibição	● Selecione **Cronologicamente** para exibir os resultados pesquisados em ordem cronológica. ● Selecione **Reverter cronologicamente** para exibir os resultados pesquisados em ordem cronológica reversa. ● Selecione **Câmera** para exibir os resultados pesquisados por câmeras.
Pesquisa de imagens	● No modo Grade, passe o cursor sobre o resultado pesquisado e

clique em **Pesquisa de Imagem** para começar a pesquisar imagem por imagem.

Observação

Para mais detalhes, consulte ***Pesquisar imagens do corpo humano por imagem*** .

- No modo de lista, clique para realizar uma pesquisa secundária.

Ver detalhes da pessoa

Coloque o cursor na foto da pessoa e você poderá ver os detalhes da captura, incluindo se a pessoa usa óculos, tipo de cabelo, tipo de blusa, etc.

Observação

Esta função deve ser suportada pelo dispositivo.

Ver imagem e vídeo

Clique na foto da pessoa para vê-la maior e assistir ao vídeo relacionado (se disponível).

Observação

Para obter detalhes sobre as instruções de controle de reprodução, consulte ***Reprodução*** .

Gerar Padrão

Selecione uma ou mais imagens e clique em **Gerar Padrão** para exibir o padrão de uma determinada pessoa no mapa.

Observação

Certifique-se de ter adicionado recursos no mapa. Para obter detalhes sobre como definir os parâmetros, consulte o *HikCentral Professional Web Client User Manual* .

Exportar resultados

Você pode exportar os resultados pesquisados (tanto fotos quanto vídeos) para o armazenamento local. Marque um ou mais resultados pesquisados e clique em **Exportar** no canto superior direito para adicionar os itens selecionados ao centro de download.

Observação

Para obter detalhes sobre como gerenciar as tarefas de download, consulte ***Gerenciar tarefas de download/upload*** .

Abrir tela auxiliar

Clique no canto superior direito para abrir a página atual em uma tela auxiliar.

8. Clique em uma imagem capturada para ver informações detalhadas, como se você está sorrindo, e você pode realizar as seguintes operações.

Download	Clique em **Download** para baixar as fotos ou vídeos.
Ver imagem e vídeo	Clique em / para ver a imagem grande e o vídeo relacionado (se disponível).

Observação

Para obter instruções de controle de reprodução, consulte ***Reprodução*** .

16.2.4 Pesquisar Imagens do Corpo Humano por Imagem

Você pode pesquisar fotos de corpos humanos carregando uma foto de rosto ou corpo humano. Você também pode visualizar os arquivos de vídeo relacionados aos resultados da pesquisa e salvar os arquivos de vídeo relacionados como evidência.

Antes de começar

Você adicionou servidor(es) de análise inteligente ou servidor(es) de fusão inteligente no cliente web.

Passos

1. No painel de navegação esquerdo, selecione **Pesquisar imagens capturadas** → **Pesquisar capturas de corpos humanos** .
2. No campo Pesquisar por, selecione **Pesquisa de imagem** .
3. No campo Tempo, defina o período de tempo.

Observação

Você pode selecionar **Custom Time Interval** para especificar o horário de início e término da pesquisa. O intervalo de tempo personalizado não deve ser maior que 7 dias.

4. Selecione a(s) câmera(s) para pesquisar a foto do rosto.
   1) Clique para abrir o painel da lista de câmeras.
   2) Selecione um site atual ou um site remoto na lista suspensa de sites para mostrar suas câmeras.
   3) Marque a(s) câmera(s) que você deseja pesquisar.

Observação

Até 200 recursos podem ser selecionados para pesquisa ao mesmo tempo.

5. Passe o mouse sobre o painel de informações da pessoa e clique em **Carregar imagem** para carregar uma foto de rosto do PC local para definir uma imagem para pesquisa de imagens.

Observação

A imagem enviada deve estar no formato JPG e o tamanho da imagem não deve ser maior que 1 GB.

6. Opcional: arraste o controle deslizante para definir a similaridade.
7. Clique em **Pesquisar** .
   Os resultados da pesquisa serão exibidos cronologicamente.
8. Opcional: Para os resultados pesquisados, você pode executar mais operações.

Alternar modo de exibição	Os resultados pesquisados podem ser exibidos em três modos, e você pode alternar entre diferentes modos de exibição. ● Clique para visualizar os resultados da pesquisa em miniaturas. ● Clique para exibir a(s) câmera(s) no mapa e clique em uma câmera para visualizar os resultados pesquisados em miniaturas. ● Clique para visualizar os resultados da pesquisa em forma de lista.
Pesquisa de imagens	● No modo Grade, passe o mouse sobre o resultado pesquisado e clique em **Pesquisar imagem** para começar a pesquisar imagem por imagem. ● No modo de lista, clique para realizar uma pesquisa secundária. **Observação** Para mais detalhes, consulte ***Pesquisar imagens do corpo humano por imagem*** .
Ver detalhes da pessoa	Coloque o cursor na foto da pessoa e você poderá ver os detalhes da captura, incluindo se a pessoa usa óculos, tipo de cabelo, tipo de blusa, etc. **Observação** Esta função deve ser suportada pelo dispositivo.
Ver imagem e vídeo	Clique na foto da pessoa para vê-la maior e assistir ao vídeo relacionado (se disponível). **Observação** Para obter detalhes sobre as instruções de controle de reprodução, consulte ***Reprodução*** .
Selecione o período de tempo	Arraste o controle deslizante para filtrar os resultados definindo um período de tempo em que uma foto de rosto é capturada.

Alterar ordem de exibição	● Selecione **Cronologicamente** para exibir os resultados pesquisados em ordem cronológica. ● Selecione **Reverter cronologicamente** para exibir os resultados pesquisados em ordem cronológica reversa. ● Selecione **Câmera** para exibir os resultados pesquisados por câmeras.
Gerar Padrão	Selecione uma ou mais imagens e clique em **Gerar Padrão** para exibir o padrão de uma determinada pessoa no mapa. **Observação** Certifique-se de ter adicionado recursos no mapa. Para obter detalhes sobre como definir os parâmetros, consulte o *HikCentral Professional Web Client User Manual* .
Exportar resultados	Você pode exportar os resultados pesquisados (tanto fotos quanto vídeos) para o armazenamento local. Marque um ou mais resultados pesquisados e clique em **Exportar** no canto superior direito para adicionar os itens selecionados ao centro de download. **Observação** Para obter detalhes sobre como gerenciar as tarefas de download, consulte ***Gerenciar tarefas de download/upload*** .
Abrir tela auxiliar	Clique no canto superior direito para abrir a página atual em uma tela auxiliar.

9. Clique em uma imagem capturada para ver informações detalhadas, como se você está sorrindo, e você pode realizar as seguintes operações.

Capturas relacionadas	Clique em **Download** para baixar as fotos ou vídeos.
Ver imagem e vídeo	Clique em / para ver a imagem grande e o vídeo relacionado (se disponível). **Observação** Para obter instruções de controle de reprodução, consulte ***Reprodução*** .

16.2.5 Pesquisar por Imagens de Rosto Correspondentes

Você pode procurar por imagens de rostos correspondentes com imagens de rostos em bibliotecas de imagens de rostos especificadas. Você também pode filtrar ainda mais os rostos correspondentes por temperatura da superfície da pele e status de uso de máscara para propósitos como prevenção de doenças infecciosas. Exportar a filmagem de vídeo relacionada para o PC local e salvá-la como evidência para o servidor SFTP também são suportados.

Passos

1. No painel de navegação esquerdo, selecione **Pesquisar imagens capturadas** → **Pesquisar rostos correspondentes** .
2. No campo **Tempo** , defina o período de tempo para pesquisa.

Observação

Você pode selecionar **Intervalo de tempo personalizado** para especificar a hora de início e de término da pesquisa.

3. Selecione as bibliotecas de imagens de rostos para procurar as imagens correspondentes.

Observação

Passe o cursor sobre uma biblioteca de imagens de rosto e clique para selecionar as câmeras vinculadas ao grupo.

4. Opcional: insira uma palavra-chave de nome de pessoa ou ID de pessoa para filtrar os resultados.
5. Opcional: Defina as seguintes condições.

Temperatura da superfície da pele

Após a ativação, você pode definir um limite para procurar pessoas correspondentes cuja temperatura da superfície da pele seja igual ou superior ao limite.

Status da temperatura

Após habilitado, você pode filtrar pessoas correspondentes por status de temperatura (normal ou anormal).

6. Clique em **Pesquisar** .
   As pessoas correspondentes serão exibidas e agrupadas por diferentes bibliotecas de imagens de rosto, e você poderá visualizar os detalhes da pessoa.
7. Opcional: Execute as seguintes operações para as imagens pesquisadas.

Alternar modo de exibição	Os resultados pesquisados podem ser exibidos em três modos, e você pode alternar entre diferentes modos de exibição. ● Clique para visualizar os resultados da pesquisa em miniaturas. ● Clique para exibir a(s) câmera(s) no mapa e clique em uma câmera para visualizar os resultados pesquisados em miniaturas.

Gerar Padrão	No modo Mapa, selecione uma ou mais imagens e clique em **Gerar Padrão** para exibir o padrão de uma determinada pessoa no mapa.

Observação

Certifique-se de ter adicionado o recurso no mapa. Para obter detalhes sobre como definir os parâmetros, consulte o *HikCentral Professional Web Client User Manual* .

8. Clique ao lado da imagem original para realizar uma pesquisa secundária.

Pesquisa de imagens	Clique em **Picture Search** para procurar a pessoa alvo nas fotos capturadas carregando uma foto de rosto. Para informações detalhadas, veja ***Search Face Pictures by Picture*** .
Pesquisa de arquivo	Clique em **Pesquisa de arquivo** para ir para a página Pesquisa de arquivo e pesquisar no arquivo da pessoa.
Verificar identidade	Clique em **Verificação de identidade** → **A ser verificado** para verificar a identidade da pessoa ou clique em **Verificação de identidade** → **Alvo** para definir a pessoa como alvo de comparação.
Abrir tela auxiliar	Clique no canto superior direito para abrir a página atual em uma tela auxiliar.

9. Opcional: clique duas vezes em uma imagem capturada para visualizar informações detalhadas e você pode executar as seguintes operações.

Capturas relacionadas	Clique em **Capturas relacionadas** para exibir imagens capturadas durante 30s antes e depois da imagem capturada.
Ver imagem e vídeo	Clique em / para ver a imagem grande e o vídeo relacionado (se disponível).

Observação

Para instruções de controle de reprodução, consulte ***Reprodução*** . Alguns ícones podem não estar disponíveis para reprodução de imagem de rosto.

Baixar imagem	Clique em **Mais** → **Baixar** para baixar a imagem para o PC local.

10. Opcional: exporte as fotos e vídeos correspondentes para o armazenamento local.
    1) Selecione os resultados correspondentes a serem exportados e clique em **Exportar** .
    2) Selecione o conteúdo a ser exportado.
    3) Selecione **Excel** ou **CSV** como formato.

4) (Opcional) Se o conteúdo a ser exportado contiver vídeo, selecione **MP4** ou **AVI** como formato de vídeo.

Observação

O formato MP4 suporta criptografia. Você pode definir uma senha para criptografar o arquivo de vídeo para fins de segurança.

5) Defina o caminho de salvamento.
6) Defina e confirme a senha para o arquivo ZIP.
7) Clique em **Salvar** para adicionar a tarefa de download ao centro de downloads.

Observação

Para obter detalhes sobre como gerenciar as tarefas de download, consulte ***Gerenciar tarefas de download/upload*** .

16.2.6 Pesquisar Pessoas por Frequência

Você pode procurar por fotos de pessoas que aparecem com frequência/raramente capturadas por câmeras específicas em um período de tempo específico. A função pode ser útil para rastrear potenciais clientes VIP no setor de varejo, como lojas de luxo. Também pode ser usada para descobrir suspeitos que podem cometer crimes e, depois, notificar o pessoal de segurança para ficar de guarda em locais como bancos e joalherias.

Antes de começar

Certifique-se de ter configurado o alarme de pessoa que aparece com frequência/raramente no dispositivo. Para detalhes, consulte o manual do usuário do dispositivo.

Passos

1. No painel de navegação esquerdo, clique em **Pesquisar imagens capturadas** → **Pesquisar pessoas por frequência** para entrar na página Pesquisar pessoa por frequência.
2. No campo de tempo, selecione um período de tempo ou selecione **Intervalo de tempo personalizado** para personalizar um período de tempo para pesquisa.
3. Selecione **Pessoas Frequentemente Aparecidas** ou **Pessoas Raramente Aparecidas** como o tipo de pesquisa.
4. Selecione a(s) câmera(s) para pesquisar as fotos das pessoas que aparecem com frequência/raramente.

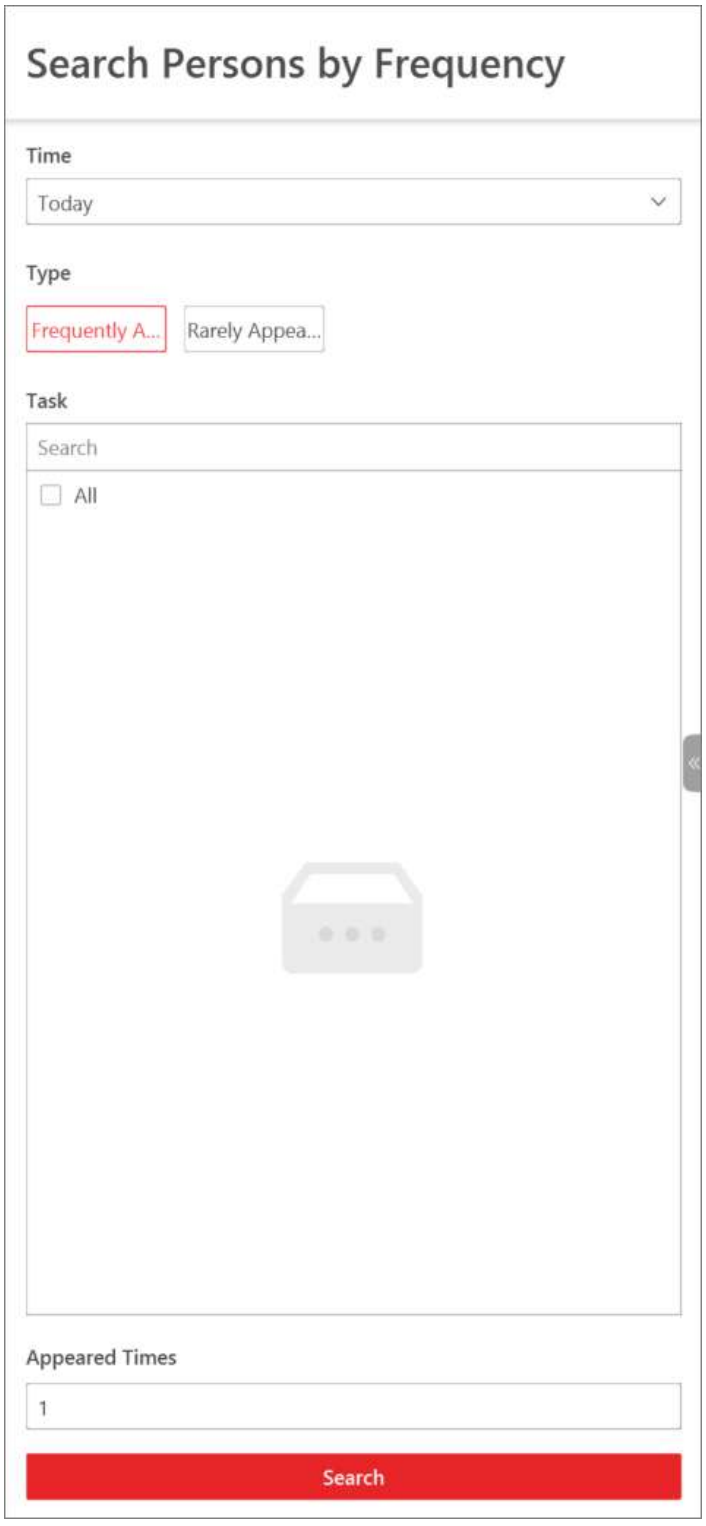


Figura 16-6 Pesquisar pessoas por frequência

1) Opcional: marque **Incluir subárea** para permitir a exibição de câmeras em subáreas.
2) Selecione áreas e depois selecione a(s) câmera(s) nessas áreas.

Observação

Até 200 recursos podem ser selecionados para pesquisa ao mesmo tempo.

5. Insira um número no campo Horários de Aparição.
6. Clique em **Pesquisar** .
   As pessoas que aparecem com frequência/raramente serão listadas à direita. Você pode ver a foto, o horário em que apareceram e os horários em que apareceram de cada pessoa listada.
7. Opcional: Na coluna Operação, clique para adicionar a lista de pessoa para pessoa.
8. Opcional: execute uma pesquisa secundária após clicar na coluna Operação.

Pesquisa de imagens	Clique em **Picture Search** para procurar a pessoa alvo nas fotos capturadas carregando uma foto de rosto. Para informações detalhadas, veja ***Search Face Pictures by Picture*** .
Pesquisar Arquivo	Clique em **Pesquisa de arquivo** para ir para a página Pesquisa de arquivo e pesquisar no arquivo da pessoa.
Verificar identidade	Clique em **Verificação de identidade** → **A ser verificado** para verificar a identidade da pessoa ou clique em **Verificação de identidade** → **Alvo** para definir a pessoa como alvo de comparação.
Abrir tela auxiliar	Clique no canto superior direito para abrir a página atual em uma tela auxiliar.

9. Clique duas vezes em uma imagem capturada para visualizar informações detalhadas e você pode executar as seguintes operações.

Exibir histórico de captura	Clique em **Captura de histórico** para visualizar as capturas de histórico.
Baixar imagem	Clique **em Download** para baixar a imagem para o PC local.

10. Opcional: filtre imagens e vídeos relacionados por câmeras.
    1) Clique em **Filtrar câmeras** para selecionar a(s) câmera(s).
    2) Clique **em OK** .
       As imagens capturadas pelas câmeras selecionadas e os vídeos gravados por elas serão exibidos.
11. Opcional: Você pode executar as seguintes operações depois de filtrar as imagens relacionadas.

Capturas relacionadas	Clique em **Capturas relacionadas** para exibir imagens capturadas 30s antes e depois da imagem capturada.
Ver imagem e vídeo	Clique em / para ver a imagem grande e o vídeo relacionado (se disponível).

12. Opcional: exporte as fotos e vídeos correspondentes para o armazenamento local.

1) Selecione os resultados correspondentes a serem exportados e clique em **Exportar** .
2) Selecione o conteúdo a ser exportado.
3) Selecione **Excel** ou **CSV** como formato.
4) (Opcional) Se o conteúdo a ser exportado contiver vídeo, selecione **MP4** ou **AVI** como formato de vídeo.

Observação

O formato MP4 suporta criptografia. Você pode definir uma senha para criptografar o arquivo de vídeo para fins de segurança.

5) Defina o caminho de salvamento.
6) Clique em **Salvar** para adicionar a tarefa de download ao centro de downloads.

Observação

Para obter detalhes sobre como gerenciar as tarefas de download, consulte ***Gerenciar tarefas de download/upload*** .

16.3 Pesquisa de Identidade

Recursos e informações sobre pessoas capturadas podem ser salvos como arquivos para pesquisa no Control Client. E o Control Client também fornece comparação de imagem para imagem e comparação de imagem para grupo, o que significa que você pode saber a similaridade entre dois rostos em duas imagens diferentes, ou se uma pessoa é membro de uma biblioteca de imagens de rosto existente.

16.3.1 Pesquisar por Arquivos

O sistema salvará as características e informações (incluindo fotos e vídeos capturados) da pessoa capturada como arquivo. Você pode pesquisar os arquivos relacionados de uma foto de rosto para verificar as fotos ou vídeos capturados de pessoas semelhantes na biblioteca. Você também pode verificar se uma pessoa é um estranho.

Antes de começar

Certifique-se de ter adicionado um servidor de análise inteligente ao sistema e configurado a câmera de captura e a biblioteca de imagens de rosto para ele.

Passos

Observação

Por padrão, o arquivo será mantido por 3 meses.

1. No painel de navegação esquerdo, clique em **Pesquisa de identidade** → **Pesquisa de arquivo** para entrar na página Pesquisa de arquivo.
2. Selecione uma biblioteca de imagens faciais no campo Biblioteca de Imagens Faciais. Você também pode verificar o grupo de estranhos.
3. Carregue uma foto do rosto no campo Informações da pessoa.
4. Arraste o controle deslizante de similaridade para definir uma similaridade.
5. Clique em **Pesquisar** .
   Imagens cuja similaridade é maior que a configurada serão exibidas no painel direito. Passe o cursor sobre uma imagem pesquisada e os detalhes (por exemplo, nome do grupo, etc.) da imagem aparecerão, e os detalhes da imagem de estranhos são diferentes dos da biblioteca de imagens de rosto.

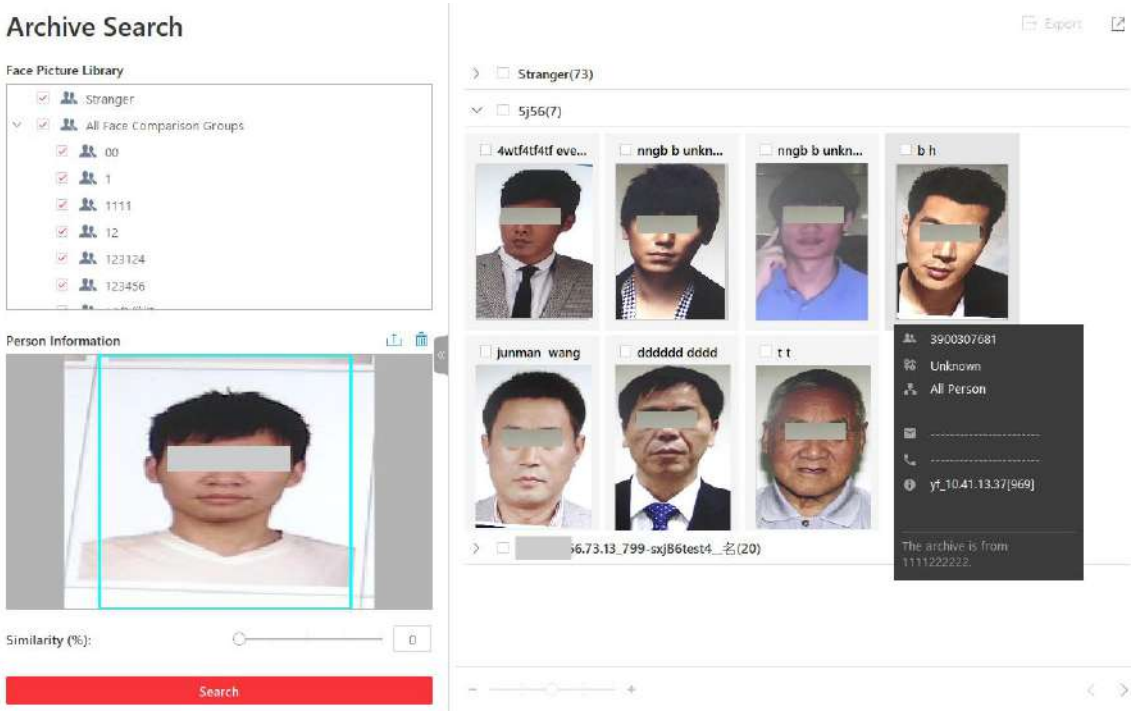


Figura 16-7 Pesquisa de arquivo

6. Opcional: Passe o cursor sobre uma imagem correspondente e clique para realizar uma pesquisa secundária.

Pesquisar imagem capturada	Clique em **Pesquisar imagem capturada** para ir para a página Pesquisa de rosto e pesquisar as imagens capturadas relacionadas à imagem do rosto pesquisada, definindo condições de pesquisa.
Pesquisar Arquivo	Clique em **Pesquisar arquivo** para ir para a página Pesquisar arquivo e pesquisar no arquivo da pessoa pesquisada.
Verificar identidade	Clique em **Verificação de identidade** → **A ser verificado** para verificar a identidade da pessoa ou clique em **Verificação de identidade** → **Alvo** para definir a pessoa como alvo de comparação.

7. Opcional: Execute a(s) seguinte(s) operação(ões).

Ver imagem e vídeo	Clique em uma imagem correspondente para ver mais fotos capturadas e vídeos relacionados.
Exportar relatório de pesquisa de arquivo	Verifique as imagens pesquisadas e clique em **Exportar** para salvar os dados no computador atual. Selecione **Excel** se quiser salvar a imagem ou o vídeo pesquisado.
Tempo de captura do filtro	Clique em uma imagem correspondente e clique em **Filtrar tempo de captura** para definir o período em que a imagem e o vídeo serão capturados.

16.3.2 Verificar Identidade Comparando com Imagem

Quando você não tem certeza sobre a identidade de uma pessoa, você pode comparar a foto do rosto dela com as da biblioteca de fotos de rosto para identificá-la.

Antes de começar

Certifique-se de ter adicionado um servidor de análise inteligente ao sistema e configurado a câmera de captura e a biblioteca de imagens de rosto para ele.

Passos

1. No painel de navegação esquerdo, clique em **Pesquisa de identidade** → **Verificação de identidade** para entrar na página Verificação de identidade.
2. Carregue a foto do rosto que você deseja identificar.
3. Selecione **Biblioteca de imagens de rosto** no campo **Comparar** .
4. Selecione uma biblioteca de imagens de rosto na lista.
5. Opcional: Defina parâmetros relacionados à epidemia.

   Temperatura

   Após a ativação, você pode definir um limite para procurar pessoas correspondentes cuja temperatura da superfície da pele seja igual ou superior ao limite.

   Status da temperatura

   Após habilitado, você pode filtrar pessoas correspondentes por status de temperatura (normal ou anormal).

   Usar máscara ou não

   Após habilitar, você pode filtrar pessoas correspondentes que usam máscara e aquelas que não usam.
6. Arraste o controle deslizante de similaridade para definir uma similaridade.

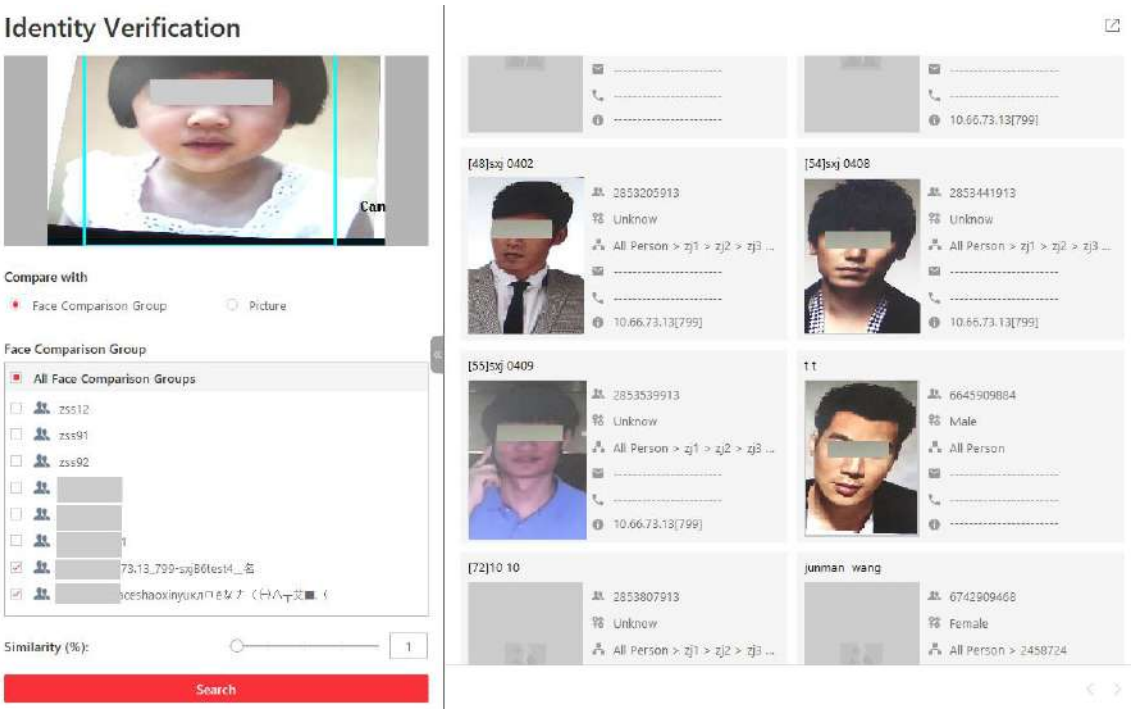


Figura 16-8 Comparar com o grupo de reconhecimento facial

7. Clique em **Pesquisar** .
   Imagens cuja semelhança for maior que a configurada serão exibidas no painel direito.
8. Opcional: clique em **Adicionar pessoa** para adicionar a pessoa à lista de pessoas.
9. Opcional: Passe o cursor sobre uma imagem correspondente e clique para realizar uma pesquisa secundária.

Pesquisar imagem capturada	Clique em **Pesquisar imagem capturada** para ir para a página Pesquisa de rosto e pesquisar as imagens capturadas relacionadas à imagem do rosto pesquisada, definindo condições de pesquisa.
Pesquisar Arquivo	Clique em **Pesquisar arquivo** para ir para a página Pesquisar arquivo e pesquisar no arquivo da pessoa pesquisada.
Verificar identidade	Clique em **Verificação de identidade** → **A ser verificado** para verificar a identidade da pessoa ou clique em **Verificação de identidade** → **Alvo** para definir a pessoa como alvo de comparação.

16.3.3 Verificar Identidade Comparando com Biblioteca de Imagens Faciais

Você também pode comparar duas fotos de rostos para ver se são da mesma pessoa de acordo

com a semelhança.

Antes de começar

Certifique-se de ter adicionado um servidor de análise inteligente ao sistema e configurado a câmera de captura e a biblioteca de imagens de rosto para ele.

Passos

1. No painel de navegação esquerdo, clique em **Pesquisa de identidade** → **Verificação de identidade** para entrar na página Verificação de identidade.
2. Carregue a foto do rosto que você deseja identificar no campo **Informações da Pessoa** na parte superior do painel.
3. Selecione **Imagem** no campo **Comparar** .
4. Carregue uma foto no campo **Informações da pessoa** na parte inferior do painel.

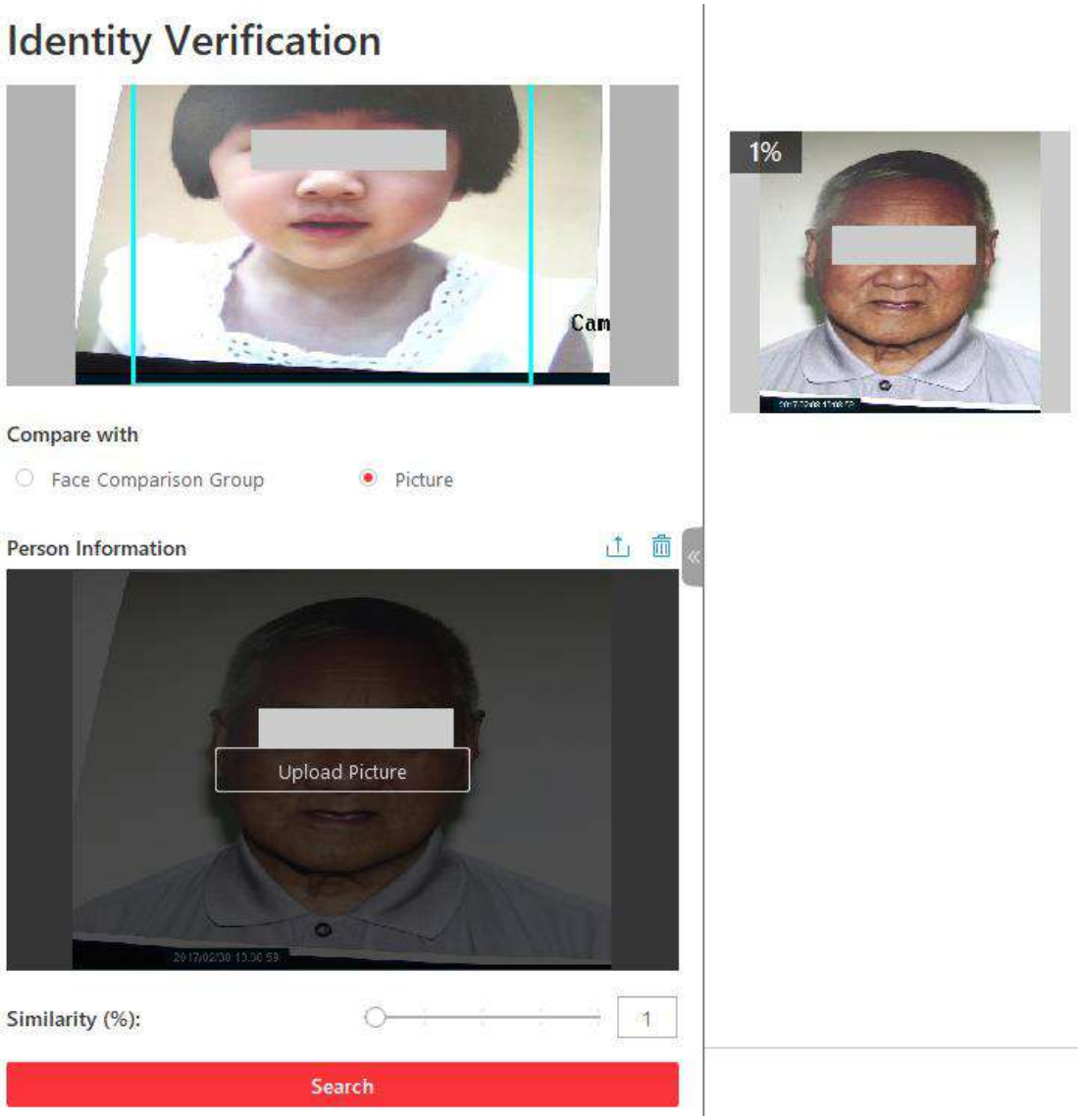


Figura 16-9 Comparar com a imagem especificada

Observação

Você pode enviar uma foto com mais de um rosto, e o cliente notará a semelhança entre a primeira foto e todos os rostos desta foto.

5. Arraste o controle deslizante de similaridade para definir uma similaridade.
6. Clique em **Pesquisar** .
   A(s) foto(s) de rosto na segunda foto carregada será(ão) exibida(s) no painel direito, e a semelhança entre as pessoas na primeira e na segunda foto carregada será exibida.
7. Opcional: clique em **Adicionar pessoa** para adicionar a pessoa à lista de pessoas.
8. Opcional: Passe o cursor sobre uma imagem correspondente e clique para realizar uma pesquisa secundária.

Pesquisar imagem por imagem	Clique em **Search Picture by Picture** para ir para a página Face Search para procurar uma pessoa alvo nas fotos capturadas carregando uma foto de rosto. Para informações detalhadas, veja ***Search Face Pictures by Picture*** .
Pesquisar Arquivo	Clique em **Pesquisar arquivo** para ir para a página Pesquisar arquivo e pesquisar no arquivo da pessoa pesquisada.
Verificar identidade	Clique em **Verificação de identidade** → **A ser verificado** para verificar a identidade da pessoa ou clique em **Verificação de identidade** → **Alvo** para definir a pessoa como alvo de comparação.

Capítulo 17 Gestão de Evidências

No módulo Gerenciamento de Evidências, você pode gerenciar casos e arquivos (incluindo fotos, vídeos, áudios e outros arquivos), que contêm informações importantes sobre incidentes, como acidentes de trânsito e crimes violentos, para resolução de disputas ou processos judiciais.
No canto superior esquerdo do Cliente, selecione → **Todos os Módulos** → **Investigação** → **Coleta de Evidências** .

17.1 Gerenciar Arquivos

Os arquivos se referem a vídeos, fotos e documentos sobre incidentes como acidentes de trânsito e crimes violentos em caso de necessidade de resolução de disputas ou casos legais. Você pode carregar arquivos do PC local, definir agendamentos para obter arquivos de dispositivos e compartilhar arquivos adicionados. Você também pode vincular os arquivos adicionados com os casos específicos.

Observação

- A permissão (como visualização, edição, exportação e compartilhamento) de arquivos especificados (arquivos vinculados a casos ou arquivos carregados por dispositivos portáteis) varia de acordo com as funções do usuário. Na página Permissão do Usuário de um arquivo carregado, são exibidos os detalhes da permissão.
- Se o arquivo for um arquivo de dispositivo portátil enviado por um policial, o policial será o proprietário padrão do arquivo.
- O proprietário do arquivo tem todas as permissões. Usuários de nível superior do proprietário do arquivo têm as mesmas permissões de arquivo que o proprietário do arquivo. Usuários com permissão de super acesso podem visualizar todos os arquivos. Pessoas no mesmo departamento do proprietário do arquivo também podem visualizar os arquivos.

17.1.1 Carregar Um Arquivo Local

Você pode carregar arquivos do seu PC local para o Evidence Management Center. Para os arquivos carregados, você pode executar mais operações, como visualizar os arquivos adicionados por tipo de arquivo e tag de arquivo, e filtrar e exportar os arquivos.

Passos

1. Selecione **Gerenciamento de arquivos** à esquerda.

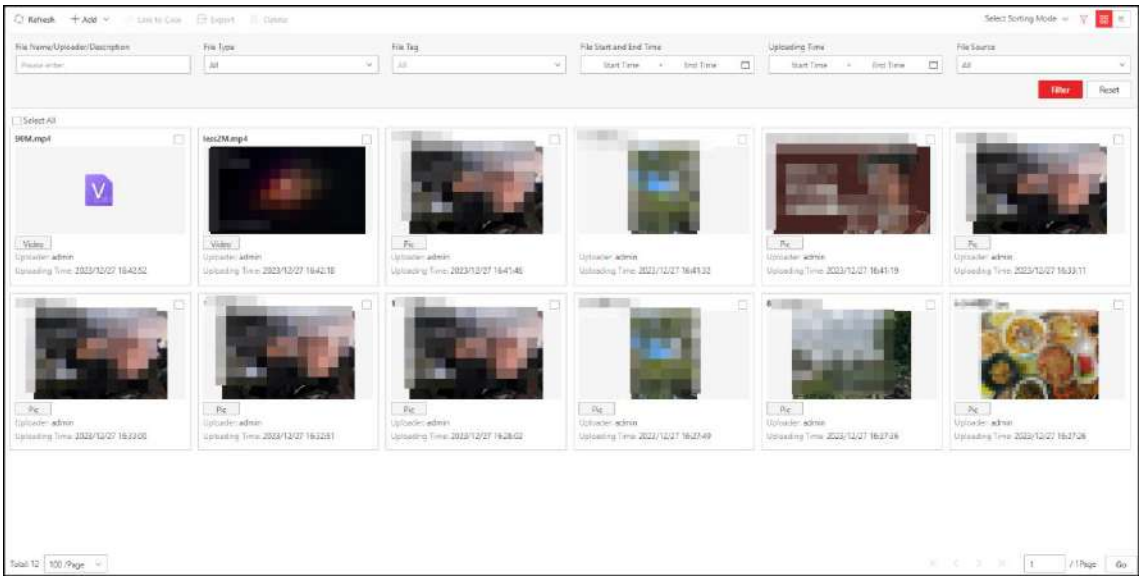


Figura 17-1 Página de gerenciamento de arquivos

2. Clique em **Adicionar** → **Carregar arquivo local** para abrir o painel Carregar arquivo local.
3. Opcional: Selecione uma ou várias tags de arquivo.
4. Opcional: Defina a localização geográfica quando o arquivo foi criado de acordo com as instruções na interface.
5. Clique em **Carregar** e selecione as fotos, vídeos, áudios ou outros arquivos do PC local para adicionar.
6. Clique em **Salvar** .

17.1.2 Carregar Arquivos do Dispositivo

Você pode definir um cronograma para carregar arquivos de câmeras on-board, dispositivos portáteis, etc. para o Evidence Management Center. Para os arquivos adicionados, você pode executar mais operações, como visualizar os arquivos adicionados por tipo de arquivo e tag de arquivo, filtrar e exportar os arquivos.

Antes de começar

Certifique-se de ter adicionado dispositivo(s) à plataforma.

Passos

1. Selecione **Gerenciamento de arquivos** à esquerda.
2. Clique em **Adicionar** → **Carregar do dispositivo** .
3. Opcional: selecione uma ou várias tags de arquivo e insira a descrição do arquivo.
4. Selecione o modo de upload e defina os parâmetros relacionados.

Carregar no horário especificado

Especifique a hora de início e término do upload e da gravação do arquivo.

Carregar quando conectado via Wi-Fi

Os arquivos serão carregados automaticamente assim que o Wi-Fi for detectado e conectado,

então você só precisa especificar o horário de início/término da gravação das câmeras.

Observação

Certifique-se de ter adicionado dispositivos como dispositivos de bordo e dispositivos portáteis que suportem conexão Wi-Fi.

5. Selecione uma ou várias câmeras na lista Câmeras vinculadas.
6. Clique em **Salvar** .

17.1.3 Salvar Arquivos em Outros Módulos

Arquivos gerados de outros módulos podem ser salvos no Evidence Management Center, incluindo o módulo Monitoring, módulo Alarm Center, módulo On-Board Monitoring, módulo Patel Monitoring, módulo Video Search, módulo Person Search, módulo Task Center, módulo Parking Lot. Ao salvar vídeos/áudios/fotos/documentos em outros módulos no Evidence Management Center, você pode especificar o modo de adição e a tag de arquivo dos arquivos para gerenciamento posterior.

Salvar vídeo gravado manualmente no Evidence Management Center

Durante a visualização ao vivo, você pode gravar manualmente imagens de vídeo que contêm informações importantes sobre incidentes, como acidentes de trânsito e crimes violentos, e salvá-las no Centro de Gerenciamento de Evidências.

Antes de começar

Certifique-se de ter definido o local de armazenamento para SFTP ou armazenamento local no Web Client. Para obter detalhes, consulte o capítulo Gerenciamento de evidências no *Manual do usuário do HikCentral Professional Web Client* .

Passos

1. Inicie a visualização ao vivo.
2. Clique na barra de ferramentas da janela de exibição para iniciar a gravação manual.
   O ícone se transforma em
3. Clique para parar a gravação.
   Uma caixa de diálogo será exibida.
4. Clique **em Salvar como** na caixa de diálogo para abrir o painel Salvar como.
5. Marque **Salvar no Centro de Gerenciamento de Evidências** e defina as informações necessárias para a evidência.

Observação

Para obter detalhes sobre as informações necessárias para a evidência, consulte ***Salvar imagens de vídeo encontradas no Centro de gerenciamento de evidências*** .

6. Clique em **Salvar** .
   As imagens de vídeo gravadas salvas serão enviadas para o SFTP ou armazenamento local.

Observação

Você pode pesquisar as evidências salvas. Para obter detalhes, consulte ***Adicionar um caso*** .

Exportar filmagens de vídeo em reprodução para o Evidence Management Center

Durante a reprodução, você pode exportar um vídeo que contém informações importantes sobre incidentes, como acidentes de trânsito e crimes violentos, e salvá-lo no Centro de Gerenciamento de Evidências.

Antes de começar

Certifique-se de ter definido o local de armazenamento para SFTP ou armazenamento local no Web Client. Para obter detalhes, consulte o capítulo Gerenciamento de evidências no *Manual do usuário do HikCentral Professional Web Client* .

Passos

1. Inicie a reprodução.
2. Clique na barra superior para abrir o painel Exportar.
3. Arraste a linha do tempo para especificar o clipe de exportação.
4. Defina o tipo de arquivo.
5. Habilite **Salvar no Centro de Gerenciamento de Evidências** e defina as informações necessárias para a evidência.

Somente Carregar Arquivo

- Defina a tag de arquivo para adicionar o arquivo de vídeo ao módulo Coleta de Evidências sem salvá-lo como caso.
- Defina a localização geográfica onde o arquivo será criado de acordo com as instruções na interface.

Criar novo caso

Defina parâmetros como ID do caso, tipo de caso, status do caso, endereço do caso e conteúdo personalizado para criar um novo caso.

Observação

Você pode adicionar e excluir o tipo de caso, a tag do caso, o status do caso e o conteúdo personalizado no Web Client. Consulte o capítulo Gerenciamento de evidências no *Manual do usuário do HikCentral Professional Web Client* para obter detalhes.

Tipo de caso

Selecione o tipo de acidente ou incidente suspeito registrado no(s) arquivo(s) de vídeo, como furto, assalto ou ataque.

Situação do caso

Selecione **Desativar** se o caso relacionado estiver resolvido e selecione **Ativar** se o caso relacionado estiver pendente.

Hora de início/término do caso

A hora de início e de término do evento de evidência.

Endereço do caso

A localização geográfica onde o caso ocorreu.

Conteúdo personalizado

O texto, como o resultado/conclusão de incidentes com base nas evidências coletadas da organização no local, como presos, advertidos e feridos.

Adicionar ao caso existente

Adicione o(s) arquivo(s) de vídeo ao caso existente, que pode ser pesquisado pelo nome ou ID. Após salvar o(s) arquivo(s) de vídeo como caso, você pode visualizar o arquivo de vídeo na seção Conteúdo do arquivo no painel de detalhes do caso.

6. Defina o caminho de salvamento e clique em **Salvar** .
   As filmagens recortadas serão enviadas para o SFTP ou armazenamento local.

Observação

Você pode pesquisar as evidências salvas. Para detalhes, consulte ***Adicionar um Caso*** .

Salvar vídeo recortado em reprodução no Evidence Management Center

Durante a reprodução, você pode recortar manualmente imagens de vídeo que contenham informações importantes sobre incidentes, como acidentes de trânsito e crimes violentos, e salvá-las no Centro de Gerenciamento de Evidências.

Antes de começar

Certifique-se de ter definido o local de armazenamento para SFTP ou armazenamento local no Web Client. Para obter detalhes, consulte o capítulo Gerenciamento de evidências no *Manual do usuário do HikCentral Professional Web Client* .

Passos

1. Inicie a reprodução.
2. Clique para iniciar o recorte.
   O ícone muda para .
3. Clique para parar o recorte.
   Uma caixa de diálogo será exibida.
4. Clique **em Salvar como** na caixa de diálogo para abrir o painel Salvar como.
5. Marque **Salvar no Centro de Gerenciamento de Evidências** e defina as informações necessárias para a evidência.

Observação

Para obter detalhes sobre as informações necessárias para a evidência, consulte ***Salvar imagens de vídeo encontradas no Centro de gerenciamento de evidências*** .

6. Clique em **Salvar** .
   As filmagens recortadas serão enviadas para o SFTP ou armazenamento local.

Observação

Você pode pesquisar as evidências salvas. Para obter detalhes, consulte ***Adicionar um caso*** .

Salvar imagens de vídeo encontradas no Evidence Management Center

Depois de pesquisar por filmagens em condições específicas, você pode exportar as filmagens correspondentes que contêm informações de incidentes, como acidentes de trânsito e crimes violentos, e salvá-las no Centro de Gerenciamento de Evidências.

Antes de começar

Certifique-se de ter definido o local de armazenamento para SFTP ou armazenamento local no Web Client. Para obter detalhes, consulte o capítulo Gerenciamento de evidências no *Manual do usuário do HikCentral Professional Web Client* .

Passos

1. Pesquise vídeos.
2. Entre no painel Exportar.
   – Na lista de arquivos de vídeo, clique no intervalo de tempo para reproduzir o arquivo de vídeo e, em seguida, clique em .
   – Selecione o(s) arquivo(s) de vídeo na lista de arquivos de vídeo e clique em **Exportar** no canto superior direito.

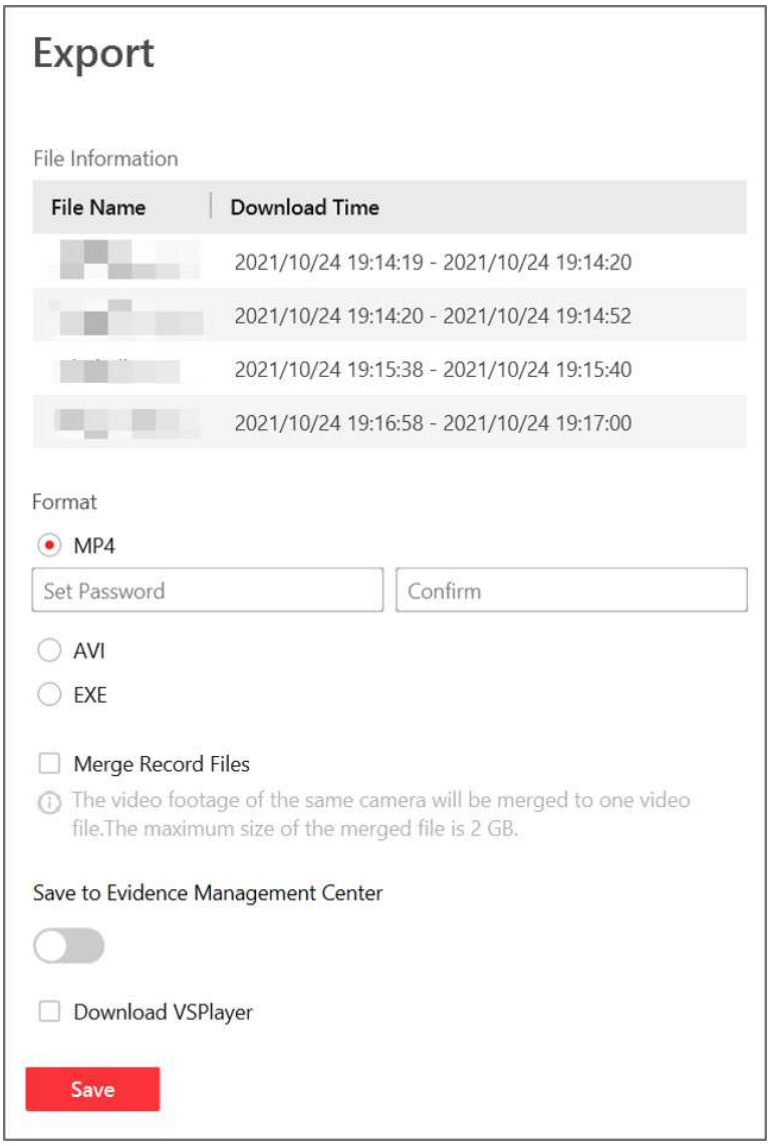


Figura 17-2 O Painel de Exportação

3. Selecione o formato para o vídeo salvo.
4. Opcional: marque **Mesclar arquivos gravados** para mesclar as filmagens de uma câmera em um arquivo de vídeo.
5. Marque **Salvar no Centro de Gerenciamento de Evidências** e defina as informações necessárias para a evidência.

Somente Carregar Arquivo

Defina a tag de arquivo para adicionar o arquivo de vídeo ao módulo Coleta de Evidências sem salvá-lo como caso.

Adicionar ao caso existente

Adicione o(s) arquivo(s) de vídeo ao caso existente, que pode ser pesquisado pelo nome ou ID. Após salvar o(s) arquivo(s) de vídeo como caso, você pode visualizar o arquivo de vídeo na seção Conteúdo do arquivo no painel de detalhes do caso.

Criar novo caso

Defina parâmetros como ID do caso, tipo de caso, status do caso e conteúdo personalizado para criar um novo caso.

Observação

Você pode adicionar e excluir o tipo de caso, a tag do caso, o status do caso e o conteúdo personalizado no Web Client. Consulte o capítulo Gerenciamento de evidências no *Manual do usuário do HikCentral Professional Web Client* para obter detalhes.

Tipo de caso

Selecione o tipo de acidente ou incidente suspeito registrado no(s) arquivo(s) de vídeo, como furto, assalto ou ataque.

Situação do caso

Selecione **Desativar** se o caso relacionado estiver resolvido e selecione **Ativar** se o caso relacionado estiver pendente.

Hora de início/término do caso

A hora de início e de término do evento de evidência.

Conteúdo personalizado

O texto, como o resultado/conclusão de incidentes com base nas evidências coletadas da organização no local, como presos, advertidos e feridos.

6. Opcional: marque **Baixar VSPlayer** para baixar o VSPlayer ao exportar a filmagem.

Observação

Esta opção está disponível quando você seleciona AVI ou MP4 como formato.

7. Clique em **Salvar** para salvar o(s) arquivo(s) de vídeo como evidência.
   Os arquivos de vídeo serão baixados no Centro de Tarefas e depois enviados como evidência para o SFTP ou armazenamento local.

Observação

- Você pode pesquisar as evidências salvas. Para obter detalhes, consulte ***Adicionar um caso*** .

Salvar a filmagem de vídeo baixada no Evidence Management Center

Quando a tarefa de download for concluída no Centro de Tarefas, você pode salvar as imagens de vídeo baixadas, que contêm informações importantes sobre incidentes como acidentes de trânsito e crimes violentos, e salvá-las no Centro de Gerenciamento de Evidências.

Antes de começar

Certifique-se de ter definido o local de armazenamento para SFTP ou armazenamento local no Web Client. Para obter detalhes, consulte o capítulo Gerenciamento de evidências no *Manual do*

usuário do HikCentral Professional Web Client .

Passos

1. No canto superior esquerdo do Cliente, selecione → **Todos os Módulos** → **Gerenciamento** → **Central de Tarefas** .
2. Clique **em Concluir** para visualizar a tarefa concluída.
3. Selecione a filmagem baixada e clique em **Salvar como** para abrir o painel Salvar como.
4. Marque **Salvar no Centro de Gerenciamento de Evidências** e defina as informações necessárias para a evidência.

Observação

Para obter detalhes sobre as informações necessárias para a evidência, consulte ***Salvar imagens de vídeo encontradas no Centro de gerenciamento de evidências*** .

5. Clique em **Salvar** .
   As imagens de vídeo salvas serão enviadas para o SFTP ou armazenamento local.

Observação

Você pode pesquisar as evidências salvas. Para obter detalhes, consulte ***Adicionar um caso*** .

17.1.4 Visualizar e Editar Arquivos

Após adicionar arquivos ao Evidence Management Center, você pode visualizar os detalhes dos arquivos e editar as informações. Por exemplo, você pode reproduzir os arquivos de vídeo, adicionar máscaras e textos, recortar vídeos, habilitar o modo silencioso para vincular arquivos de vídeo com casos correspondentes posteriormente.
Selecione **Gerenciamento de arquivos** à esquerda.

Gerenciar arquivos adicionados

Operação	Descrição
Filtrar os arquivos	Clique no canto superior direito para desdobrar o painel de filtro, defina condições como tipo de arquivo e tag de arquivo e, em seguida, clique em **Filtrar** para filtrar o arquivo de destino.
Atualizar os arquivos	Clique em **Atualizar** para atualizar a lista de arquivos.
Vincular os arquivos ao caso	Selecione arquivos para vincular a casos. Para obter detalhes, consulte ***Vincular arquivos a casos*** .
Exportar os arquivos	Selecione os arquivos e clique em **Exportar** para exportá-los.

Operação	Descrição
	Observação Para visualizar os registros de exportação de arquivos, consulte ***Gerenciar registros de operações*** .
Apagar os arquivos	Selecione os arquivos e clique em **Excluir** para excluí-los.
Alternar modo de exibição	Clique em ou ou para exibir os arquivos adicionados no modo cartão, modo lista ou modo mapa.

Visualizar e editar um arquivo

No modo de cartão ou de lista, você pode clicar no nome do arquivo para abrir o painel de detalhes do arquivo e executar as seguintes operações, se necessário.

Observação

Somente vídeos no formato PS, TS ou MPEG-4 podem ser reproduzidos e editados após serem totalmente carregados.

Formato de arquivo	Operação	Descrição
Comum	Ver detalhes	Veja quem carregou o arquivo, hora do carregamento, tamanho do arquivo e descrição. Pessoas do departamento do proprietário do arquivo têm permissão para ver detalhes do arquivo.
	Editar informações básicas	Edite o nome do arquivo, a tag do arquivo e a descrição.
	Editar Permissão do Usuário	Em Permissão do usuário, clique para editar as permissões de arquivo dos usuários compartilhados.
	Link para o caso	Clique e insira o nome do caso, ID ou descrição para pesquisar os casos a serem vinculados.
	Confirmar valor de verificação de integridade	Clique para copiar o valor de verificação de integridade do caso. Você pode verificar a integridade do arquivo comparando o valor de verificação de integridade da plataforma e o do arquivo exportado.
	Pesquisar arquivo no mapa	Clique para pesquisar arquivos no mapa inserindo uma localização geográfica ou especificando uma área para pesquisa.
Foto	Ampliar a imagem	Clique para ampliar a imagem.

Formato de arquivo	Operação	Descrição
Vídeo	Iniciar/Pausar/Parar reprodução de vídeo	Clique em / / para iniciar/pausar/parar a reprodução do vídeo.
	Reprodução normal/reversa	Clique para executar a reprodução reversa. Clique e para executar a reprodução rápida.
	Tela cheia	Clique para mostrar o vídeo em tela cheia.
	Editar vídeo	Clique para entrar na página Editar vídeo e arraste a linha do tempo para posicionar o segmento de vídeo desejado. ● Clique em **Adicionar texto** para inserir o texto e arraste-o para o local apropriado. ● Clique em **Adicionar Mosaico** e desenhe uma região desejada do mosaico no vídeo. ● Clique em **Recortar** , arraste a linha do tempo para a posição desejada e clique novamente para finalizar o recorte. ● Selecione um ou vários clipes e clique em **Excluir** para excluí-los. ● Selecione o áudio e clique em **Áudio desligado** para definir o vídeo no modo mudo.

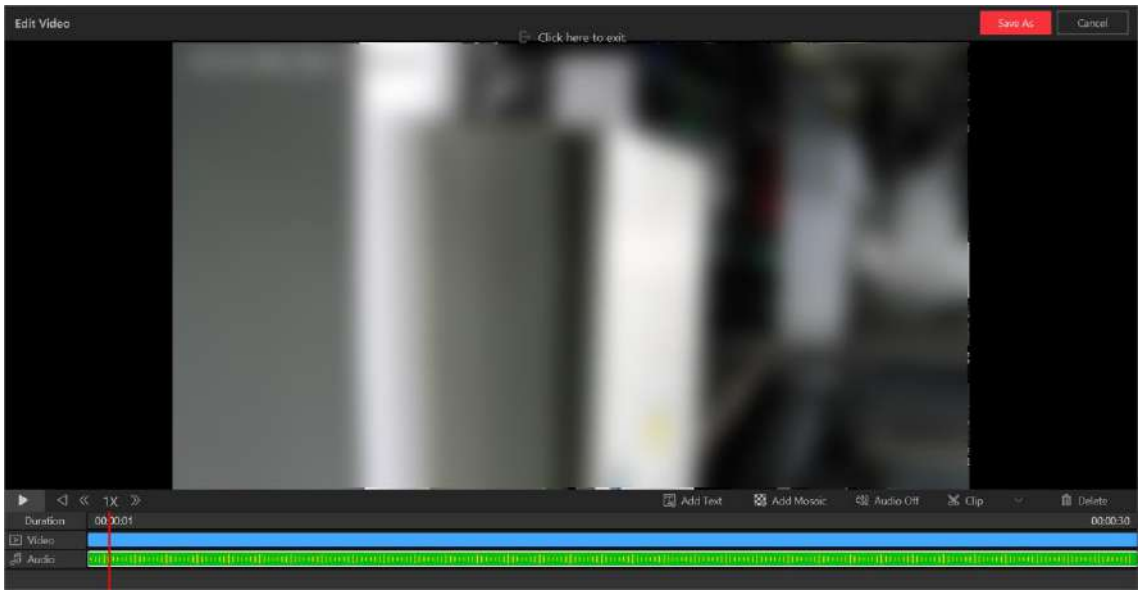


Figura 17-3 Editar um arquivo de vídeo

17.2 Gerenciar Casos

Um caso é sobre incidentes como acidentes de trânsito e crimes violentos. Você pode adicionar, editar e compartilhar casos. Após adicionar casos, você pode vincular arquivos enviados do local/dispositivo aos casos e os arquivos vinculados podem ser usados como materiais para resolver disputas ou casos legais.

Observação

- A permissão do caso (como visualizar, editar, exportar e compartilhar) varia de acordo com as funções do usuário. Na página Permissão do Usuário de um caso adicionado, são exibidos os detalhes da permissão.
- O proprietário do caso tem todas as permissões. Usuários de nível superior do proprietário do arquivo têm as mesmas permissões que o proprietário do arquivo. Usuários com permissão de super acesso podem visualizar todos os casos. Pessoas no mesmo departamento do proprietário do caso também podem visualizar o caso.

17.2.1 Adicionar Um Caso

Você pode adicionar casos sobre incidentes como acidentes de trânsito e crimes violentos para resolver disputas ou casos legais. Você pode definir informações detalhadas para o caso adicionado, incluindo o nome do caso, ID, tipo, tag, organização no local, resultado/conclusão, status e hora. Além disso, você pode carregar o arquivo (incluindo fotos, áudios, vídeos, arquivos Excel, arquivos CSV, arquivos PDF e outros) como o conteúdo do caso de câmeras ou da página Gerenciamento de Arquivos.

Antes de começar

Certifique-se de ter configurado as configurações básicas no Web Client. Para obter detalhes, consulte o capítulo Gerenciamento de evidências no *Manual do usuário do HikCentral Professional Web Client* .

Passos

1. No painel de navegação esquerdo, selecione **Gerenciamento de casos** .
2. Clique em **Adicionar** para entrar na página Adicionar caso.

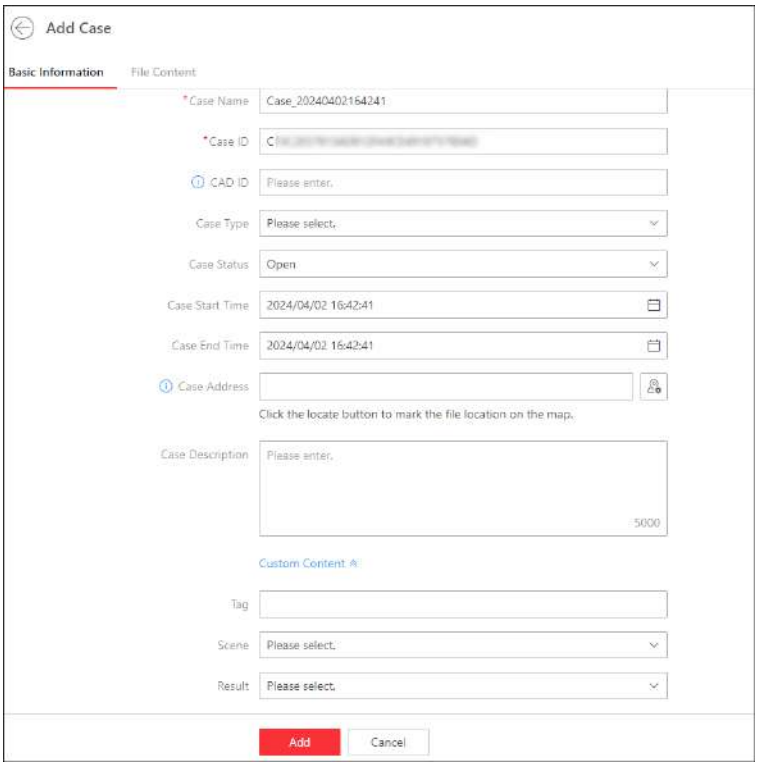


Figura 17-4 Adicionar caso

3. Crie um nome para o caso.
   O ID do caso será gerado automaticamente no Client. Você pode editar o ID do caso, que deve incluir de 1 a 64 letras ou dígitos.
4. Opcional: defina o ID do CAD, tipo, status, hora (hora de início e hora de término do evento do caso), endereço do caso, descrição, etc. para o caso.
5. Clique na aba **Conteúdo do arquivo** para entrar na página Conteúdo do arquivo.
6. Opcional: Defina o modo de adição de arquivos ao caso.
   – Selecione **Adicionar** → **Carregar arquivo local** para carregar arquivos (como fotos, áudios e vídeos) do PC local para o conteúdo do caso.
   – Selecione **Importar do gerenciamento de arquivos** , marque um ou vários arquivos relacionados ao caso e clique em **Confirmar** .
7. Clique em **Adicionar** para adicionar o caso e retornar à página Gerenciamento de evidências.

17.2.2 Visualizar e Editar Casos

Selecione **Gerenciamento de casos** à esquerda.
Você pode visualizar os detalhes dos casos, editar as informações dos casos e exportá-los para seu PC local.

Operação	Descrição
Atualizar caso	Clique em **Atualizar** para atualizar a visualização mais recente das informações do caso.

Operação	Descrição
Alternar modo de exibição	Clique em ou ou para exibir os casos adicionados no modo cartão, modo lista ou modo mapa.
Selecione o modo de classificação	Clique em **Selecionar modo de classificação** para selecionar a ordem de exibição.
Excluir Caso	Selecione o(s) caso(s) e clique em **Excluir** para excluí-lo(s).
Caixa de filtro	Clique no canto superior direito da página Evidence Management, insira uma palavra-chave na caixa de pesquisa ou defina condições de filtro e clique em **Filter** para filtrar o(s) caso(s) de destino. Você também pode clicar em **Save Filtering Condition** para salvar as configurações atuais das condições de filtragem para uso posterior.
Abrir/Fechar Caso	Selecione um ou vários casos e clique em **Fechar caso** para fechá-lo se o caso relacionado estiver resolvido, ou clique em **Abrir caso** para abrir o caso selecionado se o caso relacionado estiver pendente.
Exportar Registro de Caso	Clique em **Exportar** para exportar os registros de caso selecionados em formato Excel, CSV ou PDF. Ou clique em **Exportar tudo** para exportar todos os casos. **Observação** ● Você pode marcar **Incluir arquivo de caso** para exportar o arquivo de caso anexado. ● Você pode visualizar os registros de download na página Registro de Download.
Ver detalhes do caso e editar caso	● No modo de cartão ou de lista, você pode clicar no nome do caso para visualizar as informações básicas do caso, o conteúdo do arquivo e os registros de operação. ● Você pode editar as informações básicas do caso, como tipo, hora e tag. ● Você pode carregar mais arquivos relacionados do PC local para o conteúdo do caso, excluir arquivos desnecessários e procurar arquivos. ● Você pode clicar em **Case Report** para baixar o relatório do caso. O relatório inclui informações básicas do caso, arquivo de evidência vinculado e registro detalhado da operação. Você pode visualizar os registros de download na página Download Record.
Pesquisar caso no mapa	● No modo de mapa, você pode pesquisar casos inserindo uma localização geográfica ou especificando uma área.

17.2.3 Compartilhar Casos

Você pode compartilhar casos com usuários com os quais você tem permissão para compartilhar. Os usuários compartilhados têm as permissões para, como visualizar, compartilhar e editar o caso, conforme você definir.
Selecione os arquivos adicionados e clique em **Compartilhar** .

Compartilhar com o usuário interno do sistema

Clique em **Adicionar** para selecionar usuários como receptores de caso. Defina as permissões dos receptores e clique em **Compartilhar** .

Compartilhar com o sistema Usuário externo

Clique em **Adicionar e-mail** para adicionar os e-mails dos destinatários do arquivo. Defina o título e o conteúdo do e-mail. Defina as permissões dos destinatários e a data de expiração e clique em **Compartilhar** .

17.3 Vincular Arquivos a Casos

Você pode vincular o arquivo adicionado ao caso existente ou ao caso recém-adicionado. Os arquivos vinculados registrados no caso podem ser usados como materiais para resolver disputas ou casos legais.

Observação

Certifique-se de ter adicionado o(s) arquivo(s).

No painel esquerdo, selecione **Gerenciamento de arquivos** .

Vincular um único arquivo a um ou vários casos

1. Clique em um arquivo para abrir o painel de detalhes do arquivo.
2. Na página **Informações básicas** , clique + para adicionar um campo de caso.

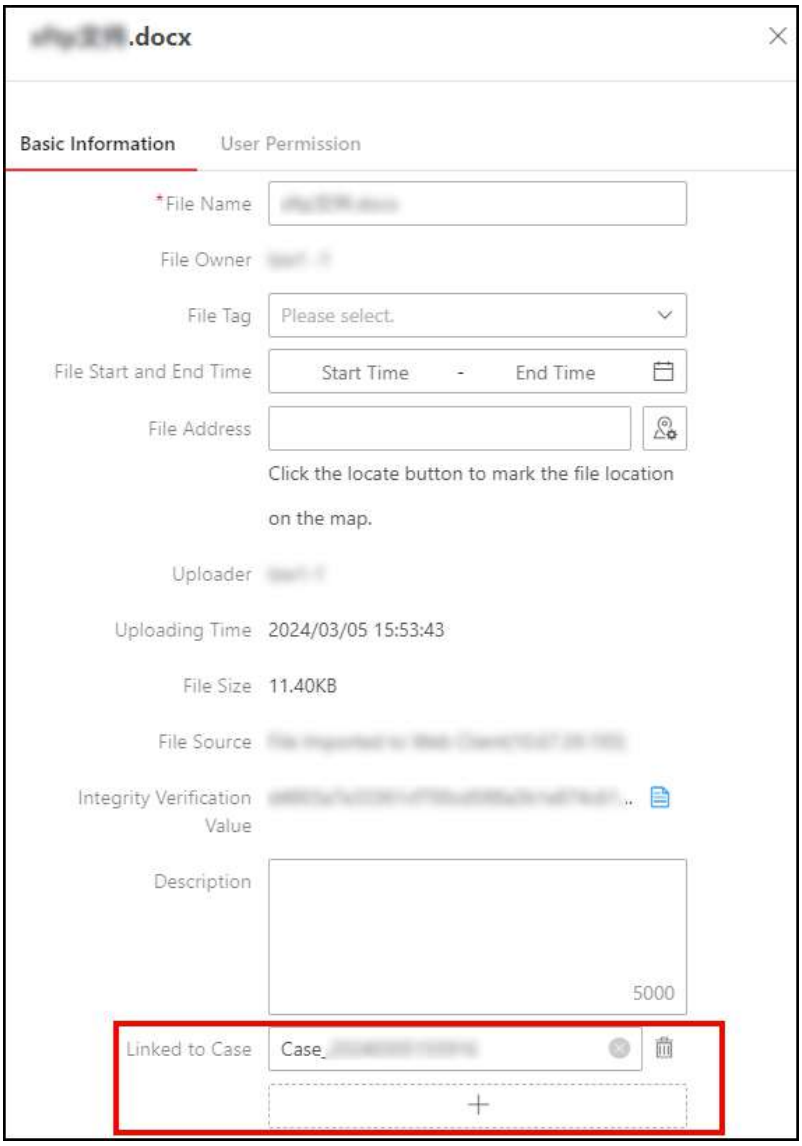


Figura 17-5 Vincular um único arquivo ao caso

3. Pesquise e selecione um caso pelo nome ou ID.
4. Clique **em Salvar** .

Arquivos de link em lote para um caso

1. Selecione vários arquivos.
2. Clique em **Link para caso** para abrir o painel Link para caso.
3. Pesquise e selecione um caso pelo nome ou ID.
4. Clique **em Salvar** .

17.4 Gerenciar Registros de Operação

Você pode gerenciar os registros de operação, incluindo visualizar ou excluir os registros de

upload/download de casos ou arquivos.
Selecione **Registro de operação** → **Carregar registro** ou **Registro de operação** → **Baixar registro** à esquerda.
Na página Upload Record, você pode visualizar os registros (incluindo tamanho do caso ou arquivo e status do upload) do caso ou arquivos enviados do PC local ou câmeras relacionadas. E na página Download Record, você pode visualizar os registros (incluindo tamanho do caso ou arquivo e status do download) do caso ou arquivos exportados na plataforma.
Você também pode procurar registros por nome, verificar um registro e clicar em / / na coluna Operation para pausar/retomar/tentar novamente a tarefa de upload/download. Ou você pode verificar o(s) registro(s) e clicar em **Delete** para excluir o(s) registro(s) selecionado(s).

Capítulo 18 Relatório de Análise Inteligente

Relatórios, criados para um período específico, são documentos essenciais, que são usados para verificar se um negócio funciona bem e efetivamente. No HikCentral Professional, os relatórios podem ser gerados diariamente, semanalmente, mensalmente, anualmente e por período de tempo personalizado. Os relatórios também podem ser adicionados ao painel para navegação rápida. Você pode usar relatórios como base para criar decisões, abordar problemas, verificar tendências e comparações, etc.

No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Análise inteligente** para entrar neste módulo.

18.1 Cenário Varejo/Supermercado

O cenário de varejo/supermercado foi criado para lojas no setor de varejo. Na seção, você pode visualizar relatórios de uma/duas/várias lojas. Você também pode visualizar relatórios inteligentes, como contagem de pessoas na loja e relatórios de análise de calor da loja.

18.1.1 Exibir Painel de Relatórios da Loja

O painel de relatórios fornece uma visão geral das lojas. Você pode selecionar uma loja ou várias lojas para visualizar os relatórios.

Passos

1. No módulo Análise Inteligente, selecione **Painel** .
2. Opcional: Selecione uma loja ou várias lojas e você poderá executar as seguintes operações.

Operação	Descrição
Definir hora do relatório	Clique em **Dia** , **Semana** , **Mês** , **Ano** , **Dia da promoção** ou **Personalizado** para selecionar a hora do relatório.
Ver Painel/Relatório Significado	Passe o cursor sobre ou no canto superior direito de um determinado parâmetro e você verá as explicações do painel/relatório.
Painel de Exportação	Clique **em Exportar** para exportar o painel em formato PDF para o PC local. **Observação** ● Consulte ***Definir parâmetros gerais*** para obter detalhes sobre como definir o caminho de salvamento do relatório exportado.

Operação	Descrição
	● Você pode obter o relatório exportado na Central de Tarefas.
Configurar conteúdo do painel	Clique em **Configurar conteúdo do painel** para selecionar o conteúdo do painel/relatório a ser exibido.
Alternar entre ano após ano e ciclo após ciclo	Clique em **Alternar para ciclo após ciclo** ou **Alternar para ano após ano** para alternar o modo de estatísticas do relatório.
Atualizar painel	Clique em **Atualizar** para atualizar o painel.
Ampliar painel/relatório	Clique para ampliar o painel ou o relatório.
Abrir tela auxiliar	Clique em **Abrir tela auxiliar** para exibir o relatório na tela auxiliar.

18.1.2 Exibir Relatório da Loja

Se você escolher o cenário Varejo/Supermercado, poderá visualizar relatórios de uma única loja, duas lojas e várias lojas.
No módulo Análise Inteligente, selecione **Armazenar Relatório** .

Exibir relatório de loja única

Você pode visualizar relatórios de uma única loja.
Selecione **Relatório de loja única** à esquerda.
No topo da página, o conteúdo definido é exibido. Passe o cursor no canto superior direito de um determinado parâmetro e você verá as explicações dos parâmetros.
Na seção Tendência de contagem de pessoas, você pode visualizar a tendência diária e horária da contagem de pessoas (entrada), contagem de pessoas (entrada + passagem), taxa de entrada, etc.
Na seção Detalhes da contagem de pessoas, você pode visualizar os dados coletados de cada andar e suas classificações.
Você pode executar as seguintes operações.

Operação	Descrição
Selecione a loja	Clique para selecionar uma loja.
Definir hora do relatório	Clique em **Dia/Semana/Mês/Ano/Personalizado** para selecionar a hora do relatório.
Ver Parâmetro Significado	Passe o cursor sobre o canto superior direito de um determinado parâmetro e você verá as explicações do parâmetro.

Operação	Descrição
Alternar entre ano após ano e ciclo após ciclo	Clique em **Alternar para ano a ano** / **Alternar para ciclo a ciclo** para comparar as estatísticas do relatório de diferentes maneiras. **Observação** Para exportar relatórios, estatísticas ano a ano e estatísticas ciclo a ciclo serão exportadas.
Abrir tela auxiliar	Clique em **Abrir tela auxiliar** para exibir o relatório na tela auxiliar.
Relatório de Exportação	● Marque/desmarque **All** para **Statistics Target** . Quando estiver marcado, o conteúdo do relatório será exibido. Marque os itens conforme necessário. ● Clique **em Exportar** para exibir o painel Exportar. ● Selecione Excel, CSV ou PDF como o formato dos relatórios exportados. ● Selecione Por dia, Por hora ou Por mês como a dimensão do relatório. ● Clique **em Exportar** .

Ver relatório de comparação

Você pode visualizar relatórios de comparação de duas lojas.
No canto superior esquerdo do Cliente, selecione → **Todos os Módulos** → **Análise Inteligente** → **Relatório da Loja** → **Relatório de Comparação** .
Clique para selecionar duas lojas.
Você pode executar as seguintes operações.

Operação	Descrição
Definir hora do relatório	Clique em **Dia/Semana/Mês/Ano/Personalizado** para selecionar a hora do relatório.
Ver Parâmetro Significado	Passe o cursor sobre o canto superior direito de um determinado parâmetro e você verá as explicações do parâmetro.
Relatório de Exportação	● Clique **em Exportar** para exibir o painel Exportar. ● Selecione Excel, CSV ou PDF como o formato dos relatórios exportados. ● Selecione Por dia, Por hora ou Por mês como a dimensão do relatório. ● Clique **em Exportar** .

Operação	Descrição
Abrir tela auxiliar	Clique em **Abrir tela auxiliar** para exibir o relatório na tela auxiliar.

Exibir relatórios de várias lojas

Você pode visualizar relatórios de várias lojas.
Selecione **Relatórios de várias lojas** à esquerda.
Você pode executar as seguintes operações.

Operação	Descrição
Selecionar lojas	Clique para selecionar várias lojas.
Definir hora do relatório	Clique em **Dia/Semana/Mês/Ano/Personalizado** para selecionar a hora do relatório.
Ver Parâmetro Significado	Passe o cursor sobre o canto superior direito de um determinado parâmetro e você verá as explicações do parâmetro.
Alternar entre ano após ano e ciclo após ciclo	Clique em **Alternar para ano a ano** / **Alternar para ciclo a ciclo** para comparar as estatísticas do relatório de diferentes maneiras. **Observação** Para exportar relatórios, estatísticas ano a ano e estatísticas ciclo a ciclo serão exportadas.
Relatório de Exportação	● Clique **em Exportar** para exibir o painel Exportar. ● Marque/desmarque **All** para **Statistics Target** . Quando estiver marcado, o conteúdo do relatório será exibido. Marque os itens conforme necessário. ● Selecione Excel, CSV ou PDF como o formato dos relatórios exportados. ● Selecione Por dia, Por hora ou Por mês como a dimensão do relatório. ● Clique **em Exportar** .
Abrir tela auxiliar	Clique em **Abrir tela auxiliar** para exibir o relatório na tela auxiliar.

Ver relatório do dia de promoção da loja

Você pode visualizar o relatório contendo contagem de pessoas, tráfego de pedestres e taxa de entrada em um dia de promoção e obter uma visão direta da tendência de contagem de pessoas e classificações de diferentes lojas.
Selecione **Relatório do Dia de Promoção da Loja** à esquerda.
Você pode executar as seguintes operações.

Operação	Descrição
Selecione a loja e o dia da promoção	Verifique as lojas na lista suspensa. Você também pode digitar o nome da loja no campo de pesquisa para procurá-la. Selecione um dia de promoção para gerar um relatório de lojas naquele dia. O relatório correspondente das lojas selecionadas no dia da promoção é exibido.
Ver Parâmetro Significado	Passe o cursor sobre o canto superior direito de um determinado parâmetro e você verá as explicações do parâmetro.
Alternar entre ano após ano e ciclo após ciclo	Clique em **Alternar para ano a ano** / **Alternar para ciclo a ciclo** para comparar as estatísticas do relatório de diferentes maneiras. **Observação** Para exportar relatórios, estatísticas ano a ano e estatísticas ciclo a ciclo serão exportadas.
Relatório de Exportação	● Clique **em Exportar** para exibir o painel Exportar. ● Marque/desmarque **All** para **Statistics Target** . Quando estiver marcado, o conteúdo do relatório será exibido. Marque os itens conforme necessário. ● Selecione Excel, CSV ou PDF como o formato dos relatórios exportados. ● Selecione Por dia, Por hora ou Por mês como a dimensão do relatório. ● Clique **em Exportar** .
Abrir tela auxiliar	Clique em **Abrir tela auxiliar** para exibir o relatório na tela auxiliar

18.1.3 Exibir Relatório de Análise Inteligente da Loja

No cenário de varejo/supermercado, para visualizar relatórios de análise inteligentes, incluindo análise de contagem de pessoas, características de pessoas, análise de calor, análise de caminho e análise de fila, você deve configurar a(s) loja(s) e adicioná-las à plataforma com antecedência.

- **Relatório de Contagem de Pessoas da Loja** : Você pode gerar um relatório de contagem de pessoas que exibe os dados de período a período e a tendência das estatísticas de contagem de pessoas para ter uma visão direta das pessoas que entram, saem, passam e taxa de entrada. Você também pode exportar o relatório para o PC local.
- **Store Person Feature Analysis Report** : A plataforma suporta salvar características de rostos humanos reconhecidos e gerar relatórios em vários períodos de tempo. Os relatórios informam a porcentagem e o número de pessoas com características diferentes em diferentes períodos de tempo. Ele pode ser usado em lugares como shopping centers para analisar os interesses das pessoas em diferentes características.
- **Relatório de análise de calor da loja** : você pode gerar um relatório de análise de calor para mostrar os movimentos do consumidor, os horários de visita e o tempo de permanência em uma área configurada.

Observação

- Certifique-se de ter adicionado uma câmera de rede de mapa de calor à plataforma e configure corretamente a câmera com a regra de mapa de calor para a área necessária. Para adicionar uma câmera de rede de mapa de calor, consulte o *Manual do Usuário do HikCentral Professional Web Client* . Para configurar a regra de mapa de calor, consulte o manual do usuário da câmera de rede de mapa de calor.
- Certifique-se de ter adicionado a câmera a um mapa estático. Para obter detalhes sobre como adicionar uma câmera ao mapa estático, consulte o *Manual do Usuário do HikCentral Professional Web Client* .

- **Relatório de Análise de Caminho da Loja** : A análise de caminho é usada principalmente para analisar as pessoas que contam nos caminhos nos shoppings. Com a ajuda de câmeras fisheye, a plataforma pode coletar dados dos consumidores (por exemplo, onde os clientes andam mais). Isso ajuda os gerentes a analisar quais áreas/lojas do shopping chamam mais a atenção do comprador e quais são esquecidas. Depois de definir os caminhos da câmera fisheye e suas direções, a plataforma calcula o tempo de permanência das pessoas em cada caminho e o número de pessoas que passam, ajudando-os a tomar decisões.

Observação

- Certifique-se de ter adicionado corretamente a câmera a um mapa estático e definido seus caminhos no mapa por meio do Web Client primeiro. Para obter detalhes sobre como adicionar a câmera ao mapa e definir caminhos, consulte o *Manual do Usuário do HikCentral Professional Web Client* .
- Você deve ter adicionado grupos de análise de caminho. Para detalhes, veja o manual do usuário do Web Client.

- **Relatório de análise de fila de armazenamento** : para câmeras que oferecem suporte ao

gerenciamento de filas, você pode gerar um relatório para mostrar o número de exceções de fila e o número de pessoas em cada fila, além de mostrar o status da fila, incluindo a duração da espera e o comprimento da fila.

Observação

Certifique-se de ter adicionado uma câmera que suporte gerenciamento de filas ao sistema e configure regiões de filas. Para configurar a região de filas, consulte o manual do usuário da câmera.

Veja o processo de exemplo de visualização de um relatório de análise de calor. Algumas configurações de parâmetros específicos podem variar de acordo com os relatórios.

1. No módulo Análise Inteligente, selecione **Centro de Análise** → **Análise de Calor** .
2. Selecione uma loja/câmera para pesquisar dados de fila. Um relatório de análise de fila da câmera/loja selecionada será exibido.
3. (Opcional) Defina o ciclo estatístico como **Dia** , **Semana** , **Mês** , **Ano** , **Dia da promoção** ou **Personalizado** .

   Relatório diário

   O relatório diário mostra dados diariamente. O sistema calculará os dados da fila detectados em cada hora de um dia.

   Relatório semanal, relatório mensal e relatório anual

   Em comparação com o relatório diário, o relatório semanal, o relatório mensal e o relatório anual podem consumir menos tempo, já que não devem ser enviados todos os dias. A plataforma calculará o número de pessoas ou o tempo de permanência das pessoas em cada dia da semana, em cada dia de um mês e em cada mês de um ano.

   Dia da promoção

   O relatório do dia da promoção mostra dados em uma base de dia de promoção. A plataforma enviará um relatório no horário de envio em um dia de promoção, que contém resultados de análise no dia.

   Intervalo de tempo personalizado

   Os usuários podem personalizar os dias no relatório para analisar o número de pessoas ou o tempo de permanência das pessoas em cada dia ou mês do intervalo de tempo personalizado.
4. (Opcional) Defina o tempo ou o período de tempo para estatísticas.

Observação

Para um relatório de intervalo de tempo personalizado, você precisa definir a hora de início e a hora de término para especificar o período de tempo.

5. (Opcional) Execute a(s) seguinte(s) operação(ões).

Operação	Descrição
Definir parâmetros de análise de calor	a. Clique em **Configurações de análise de calor** . b. Defina a **Duração da Permanência** para obter estatísticas dentro do intervalo configurado. **Observação** Por exemplo, se você definir a duração da permanência como > 15s, quando uma pessoa permanecer em uma área por mais de 15 segundos, ela será considerada como se estivesse residindo na área. c. Selecione o **significado da cor do calor** , incluindo o total de pessoas e o tempo de permanência. d. Marque **Mostrar** ou **Ocultar** as áreas de calor divididas. e. Clique **em Salvar** . f. Arraste o controle deslizante de limite no canto superior direito para ajustar o intervalo da dimensão estatística. Os dados de calor fora do intervalo não serão exibidos.
Alternar entre ano após ano e ciclo após ciclo	Clique em **Alternar para ano a ano** / **Alternar para ciclo a ciclo** para comparar as estatísticas do relatório de diferentes maneiras. **Observação** Para exportar relatórios, estatísticas ano a ano e estatísticas ciclo a ciclo serão exportadas.
Relatório de Exportação	g. Clique **em Exportar** . h. Defina o formato do arquivo exportado como Excel, CSV ou PDF. i. Selecione a dimensão de tempo como **Por hora** , **Por dia** ou **Por mês** . j. Clique **em Exportar** . **Observação** ● Consulte ***Definir parâmetros gerais*** para obter detalhes sobre como definir o caminho de salvamento do relatório exportado. ● Você pode obter o relatório exportado na Central de Tarefas.
Abrir tela auxiliar	Clique em **Abrir tela auxiliar** para exibir o relatório na tela auxiliar.

18.2 Cenário Público

O Public Scenario é projetado para situações públicas, como estações e hospitais. Você pode visualizar relatórios como contagem de pessoas e relatórios de análise de calor.

18.2.1 Personalizar Painel de Relatórios

O painel de relatórios fornece uma visão geral dos relatórios de cenário público. Há relatórios de contagem de pessoas, relatórios de análise de calor, relatórios de análise de veículos, relatórios de análise de filas, etc. Você pode personalizar o painel de relatórios conforme necessário.

Passos

1. No módulo Análise Inteligente, selecione **Painel** .
2. Opcional: No canto superior esquerdo, clique em → **Adicionar painel** na página do painel do relatório e crie um nome para adicionar um novo painel.

Observação

- Você pode adicionar até 100 painéis.
- O novo painel aparece e é nomeado por padrão como "Painel + Hora em que foi adicionado". Por exemplo, em "Painel20190916102436", "2019" representa o ano, "09" o mês, "16" a data, "10" a hora, "24" o minuto e "26" o segundo.

Você pode visualizar o painel adicionado clicando para expandir a lista de painéis adicionados.

3. Opcional: Você pode executar as seguintes operações.

Operação	Descrição
Editar nome do painel	No canto superior esquerdo, clique em . Clique para editar o nome do painel.
Excluir painel	No canto superior esquerdo, clique em . Clique para excluir o painel.
Adicionar relatório ao painel	1. Depois de selecionar um painel, clique em **Adicionar relatório** , selecione um tipo de relatório e clique em **Avançar** . 2. Defina o nome do relatório, o tipo de análise, o tipo de relatório e a hora. **Observação** - Se você selecionar a análise para uma câmera, precisará selecionar a câmera já adicionada à plataforma. - Se você selecionar a análise em uma região, precisará selecionar o grupo de análise já adicionado à plataforma.

	3. Clique **em Add** para adicionar o relatório ao dashboard. O relatório aparecerá no dashboard selecionado. 4. Clique em **Adicionar relatório** para adicionar mais relatórios ao painel, conforme necessário.
Editar nome do relatório	No canto superior direito de um relatório, clique em ··· e depois em **Editar** .
Excluir relatório do painel	No canto superior direito de um relatório, clique em ··· e depois em **Excluir** .
Alternar entre ano após ano e ciclo após ciclo	Clique em **Alternar para ano a ano** / **Alternar para ciclo a ciclo** para comparar as estatísticas do relatório de diferentes maneiras.
Trocar hora para visualizar dados do relatório	Selecione um painel e clique em **Alternar hora para exibição** para definir o tipo e a hora do relatório. **Tipo de relatório** Selecione a base de tempo para os relatórios. Por exemplo, o relatório diário mostra dados em uma base diária. **Tempo** Defina o tempo específico para gerar os relatórios. Por exemplo, se você selecionar **Custom Time Interval** como o tipo de relatório, você pode clicar para especificar um intervalo de tempo para gerar dados de relatório. Clique em **Save** (Salvar) para alterar a base de tempo padrão de todos os relatórios no painel para a data que você definiu na subetapa anterior.
Exporte relatórios	Exporte o(s) relatório(s) do painel para o PC local. a. Clique em **Exportar** para exibir o painel Exportar. b. Selecione o(s) relatório(s) na lista de relatórios. c. Selecione **Excel** , **CSV** ou **PDF** como o formato do(s) relatório(s) exportado(s). d. Clique **em Exportar** .

18.2.2 Exibir Relatório de Análise Inteligente

No cenário público, para visualizar relatórios de análise inteligente, incluindo análise de contagem de pessoas, características de pessoas, análise de calor, análise de caminho, análise de fila, análise de densidade de pessoas, análise de temperatura e análise de vários tipos de alvos, você deve

configurar os grupos de análise/câmeras correspondentes com antecedência.

Relatório de contagem de pessoas

O relatório de contagem de pessoas mostra o número de pessoas que cruzaram a linha contadas por câmeras de contagem de pessoas ou obtidas de registros de acesso de dispositivos de controle de acesso em uma região específica e dentro de um determinado período de tempo. O relatório permite que você saiba o número de pessoas que permanecem em uma região específica, o que pode ser usado para determinados cenários comerciais ou de emergência. Por exemplo, para um cenário de emergência, durante uma saída de incêndio, o número de pessoas que permaneceram será exibido no mapa, o que é necessário para o resgate. Para um cenário comercial, o gerente do shopping pode obter o relatório de contagem de pessoas para saber se a loja é atraente e obter o número de pessoas que entram em cada loja para determinar se deve limitar o número de clientes que permanecem no shopping por motivos de segurança durante o horário de pico. Você também pode gerar um relatório de contagem de pessoas para uma única loja ou várias lojas.
Antes de gerar um relatório de contagem de pessoas, você pode adicionar grupo(s) de contagem de pessoas para agrupar as portas e câmeras de contagem de pessoas de uma determinada região para definir a borda da região. Depois disso, você pode definir uma regra de relatório regular para as câmeras especificadas que suportam contagem de pessoas ou grupos de contagem de pessoas, e a plataforma enviará e-mails com relatórios anexados aos destinatários alvo diariamente, semanalmente ou mensalmente. Você também pode gerar manualmente um relatório de contagem de pessoas a qualquer momento para visualizar os dados, se necessário.

Relatório de análise de calor

O relatório de análise de calor mostra dados com um mapa de calor, que é uma representação gráfica de dados representados por cores. A função de mapa de calor da câmera é geralmente usada para rastrear os movimentos dos consumidores (onde os clientes andam e quais itens eles param para tocar e pegar) e analisar os tempos de visita e o tempo de permanência em uma área configurada. Este relatório é usado principalmente para gerentes de loja ou varejistas para ver qual parte da loja recebeu mais atenção dos consumidores e qual recebeu menos. Saber para onde os clientes se movem é útil para os varejistas. Eles podem otimizar os layouts da loja, por exemplo, onde colocar produtos populares e impopulares.
Antes de usar o relatório de análise de calor, você pode adicionar um grupo de análise de calor para definir a região para análise de calor. Depois disso, você pode definir uma regra de relatório regular para as câmeras especificadas ou os grupos de análise de calor especificados, e o sistema enviará e-mails com relatórios de análise de calor anexados aos destinatários alvo diariamente, semanalmente ou mensalmente. Você também pode gerar manualmente um relatório de análise de calor a qualquer momento para visualizar os dados, se necessário.

Relatório de Análise de Características Pessoais

O relatório de análise de características pessoais mostra a proporção de pessoas com diferentes características detectadas por câmeras que suportam reconhecimento facial.
Você pode adicionar um grupo de análise de características de pessoa antes de gerar um relatório para definir a região para análise de características de pessoa agrupando as câmeras que suportam reconhecimento facial e análise de características. Depois disso, você pode definir uma

regra de relatório regular para as câmeras especificadas ou grupos de análise de características de pessoa especificados, e o sistema enviará e-mails com relatórios anexados aos destinatários alvo diariamente, semanalmente ou mensalmente. Você também pode gerar manualmente um relatório de análise de características de pessoa a qualquer momento para visualizar os dados, se necessário.

Relatório de Análise de Fila

O relatório de análise de fila mostra o número de exceções de fila e o número de pessoas em cada fila, e mostra o status da fila, incluindo a duração da espera e o comprimento da fila. É útil para alocar recursos para varejistas.
Você pode definir uma regra de relatório regular para as câmeras especificadas, e o sistema enviará e-mails com relatórios de análise de fila anexados aos destinatários alvo diariamente, semanalmente ou mensalmente. Você também pode gerar manualmente um relatório de análise de fila a qualquer momento para visualizar os dados, se necessário.

Relatório de Análise de Caminho

A análise de caminho é usada principalmente para analisar as pessoas que contam nos caminhos nos shoppings. Com a ajuda de câmeras fisheye, o sistema pode coletar dados dos consumidores (por exemplo, onde os clientes andam mais) e traduzir esses dados em um painel para gerentes de shopping. Isso ajuda os gerentes a analisar quais áreas/lojas do shopping chamam mais a atenção do comprador e quais são esquecidas.
Antes de usar a análise de caminho, você deve adicionar grupos de análise de caminho primeiro, que definem a região para análise de caminho. Depois disso, você pode definir uma regra de relatório regular para o grupo de análise de caminho especificado, e o sistema enviará e-mails com relatórios de análise de caminho anexados aos destinatários alvo diariamente, semanalmente ou mensalmente. Você também pode gerar manualmente um relatório de análise de caminho a qualquer momento para visualizar os dados, se necessário.

Relatório de Análise de Densidade de Pessoas

O relatório de análise de densidade de pessoas mostra a tendência de variação dos dados de densidade de pessoas no gráfico de linhas. Os dados de densidade de pessoas se referem à quantidade máxima de pessoas que apareceram nas imagens de uma câmera específica durante um determinado período de tempo. Os dados são úteis para o gerenciamento e controle da quantidade de pessoas em áreas ou espaços específicos durante períodos de tempo especiais. Por exemplo, suponha que você fosse um gerente de um shopping durante um surto epidêmico, você poderia gerar um relatório de análise de densidade de pessoas para descobrir o(s) período(s) de tempo durante o qual a densidade excessiva de pessoas geralmente ocorre no shopping e, em seguida, organizar com antecedência o pessoal e os trabalhos relacionados de acordo para limitar a aglomeração de pessoas nesses períodos de tempo para evitar a propagação da doença infecciosa.

Relatório de Análise de Temperatura

O relatório de análise de temperatura mostra o número de exceções (temperatura muito alta ou muito baixa) e a temperatura máxima/mínima de diferentes pontos de termometria em diferentes

predefinições.
Você pode definir uma regra de relatório regular para as câmeras térmicas especificadas e o sistema enviará e-mails com relatórios anexados aos destinatários alvo diariamente, semanalmente ou mensalmente. Você também pode gerar manualmente um relatório de análise de temperatura a qualquer momento para visualizar os dados, se necessário.

Relatório de análise de vários tipos de alvos

O relatório de análise do tipo multi-alvo mostra o número de pessoas, veículos motorizados e veículos não motorizados dentro de um período especificado. Você pode definir uma regra de relatório regular para as câmeras especificadas e o sistema enviará e-mails com relatórios anexados aos destinatários alvo diariamente, semanalmente ou mensalmente. Você também pode gerar manualmente um relatório de análise a qualquer momento para visualizar os dados, se necessário.

Gerar Relatório de Análise

Você pode gerar relatórios de contagem de pessoas, relatórios de análise de calor, relatórios de análise de características de pessoas, relatórios de análise de fila, relatórios de análise de caminho, relatórios de densidade de pessoas, relatórios de análise de temperatura e relatórios de análise de tipo multi-alvo. Para relatório de contagem de pessoas, relatório de análise de calor, relatório de análise de caminho e relatório de análise de características de pessoas, certifique-se de ter adicionado os grupos de análise correspondentes.

- **Relatório de Contagem de Pessoas** : Você pode gerar um relatório de contagem de pessoas que exibe os dados de período a período e a tendência das estatísticas de contagem de pessoas para ter uma visão direta das pessoas que entram, saem, passam e taxa de entrada. Você também pode exportar o relatório para o PC local.

Observação

Antes de começar, certifique-se de ter configurado corretamente a câmera com uma regra de contagem de pessoas para a área necessária. Para configurar a regra de contagem de pessoas, consulte o manual do usuário da câmera de contagem de pessoas.

- **Relatório de análise de calor** : você pode gerar um relatório de análise de calor para visualizar os movimentos do consumidor e analisar os tempos de visita e permanência em uma área configurada.

Observação

  - Antes de começar, certifique-se de ter adicionado uma câmera de rede de mapa de calor à plataforma e configurado corretamente a câmera com a regra de mapa de calor para a área necessária. Para adicionar uma câmera de rede de mapa de calor, consulte o *Manual do Usuário do HikCentral Professional Web Client* . Para configurar a regra de mapa de calor, consulte o manual do usuário da câmera de rede de mapa de calor.
  - Antes de começar, certifique-se de ter adicionado a câmera a um mapa estático. Para obter detalhes sobre como adicionar uma câmera ao mapa estático, consulte o *Manual do Usuário*

do HikCentral Professional Web Client .

- **Relatório de Análise de Características Pessoais** : A plataforma suporta salvar características de rostos humanos reconhecidos e gerar relatórios em vários períodos de tempo. Os relatórios informam a porcentagem e o número de pessoas com características diferentes em diferentes períodos de tempo. Pode ser usado em lugares como shopping centers para analisar os interesses das pessoas em diferentes características.

Observação

Antes de começar, certifique-se de ter adicionado um grupo de análise de recursos de pessoa se quiser executar análise de recursos em uma região. Consulte *o Manual do Usuário do HikCentral Professional Web Client* para obter detalhes sobre como adicionar um grupo de análise de recursos de pessoa.

- **Relatório de análise de fila** : para câmeras que suportam gerenciamento de fila, você pode gerar um relatório para mostrar o número de exceções de fila e o número de pessoas em cada fila, além de mostrar o status da fila, incluindo a duração da espera e o comprimento da fila.

Observação

Antes de começar, certifique-se de ter adicionado uma câmera que suporte gerenciamento de filas ao sistema e configure as regiões de fila. Para configurar a região de fila, consulte o manual do usuário da câmera.

- **Relatório de análise de caminho** : a análise de caminho é usada principalmente para analisar as pessoas que contam nos caminhos nos shoppings. Com a ajuda de câmeras fisheye, a plataforma pode coletar dados dos consumidores (por exemplo, onde os clientes andam mais) e traduzir esses dados em um painel para gerentes de shopping. Isso ajuda os gerentes a analisar quais áreas/lojas do shopping chamam mais a atenção do comprador e quais são esquecidas. Depois de definir os caminhos da câmera fisheye e suas direções, a plataforma calcula o tempo de permanência das pessoas em cada caminho e o número de pessoas que passam, ajudando-os a tomar decisões.

Observação

  - Antes de começar, certifique-se de ter adicionado corretamente a câmera a um mapa estático e definido seus caminhos no mapa por meio do Web Client primeiro. Para obter detalhes sobre como adicionar a câmera ao mapa e definir caminhos, consulte o *Manual do Usuário do HikCentral Professional Web Client* .
  - Antes de começar, certifique-se de ter adicionado grupos de análise de caminho. Para detalhes, consulte o manual do usuário do Web Client.

- **People Density Analysis Report** : Você pode gerar manualmente um relatório de densidade de pessoas para visualizar os dados de densidade de pessoas de dois períodos de tempo adjacentes. Você também pode exportar o relatório para o PC local.

Observação

- Antes de começar, certifique-se de ter adquirido a licença que oferece suporte à análise de densidade de pessoas, ou a função não estará disponível.
- Antes de começar, certifique-se de ter adicionado o servidor de detecção de eventos anormais ao HikCentral Professional e vinculado câmeras ao servidor. Para obter detalhes, consulte *o Manual do usuário do HikCentral Professional Web Client* .
- Antes de começar, certifique-se de ter configurado a análise de densidade de pessoas no servidor de detecção de eventos anormais. Para detalhes, consulte o manual do usuário do servidor.

- **Relatório de análise de temperatura** : para câmeras térmicas, você pode gerar um relatório para mostrar o número de exceções (temperatura muito alta ou muito baixa) e a temperatura máxima/mínima de diferentes pontos de triagem de temperatura em diferentes predefinições, e gerar um relatório para mostrar os números correspondentes de uma predefinição especificada do ponto de triagem de temperatura.
- **Relatório de análise de vários tipos de alvos** : você pode gerar um relatório para mostrar o número de pessoas, veículos motorizados e veículos não motorizados dentro de um período especificado.

O processo de geração desses relatórios pode ser geralmente dividido em 4 seções: selecionar o recurso de dados do relatório, definir o ciclo estatístico, definir o tempo ou período de tempo para estatísticas e executar operações subsequentes no relatório conforme necessário. Algumas configurações de parâmetros específicos podem variar de acordo com os relatórios.

Veja o exemplo de processo de geração de um relatório de contagem de pessoas.

1. No módulo Análise Inteligente, selecione **Centro de Análise** → **Análise de Contagem de Pessoas** .
2. Selecione o tipo de recurso de dados do relatório.

   Câmera

   Um relatório de contagem de pessoas com base nos dados das câmeras selecionadas será gerado. Você pode comparar os dados de diferentes câmeras.

   Grupo de Análise

   Um relatório de contagem de pessoas com base nos dados dos grupos de contagem de pessoas que você selecionar será gerado. Você pode comparar os dados de diferentes grupos.

   Observação

   Certifique-se de ter adicionado grupos de contagem de pessoas. Para detalhes, consulte o *Manual do Usuário do HikCentral Professional Web Client* .

3. Selecione câmeras de contagem de pessoas ou grupos de contagem de pessoas com base no tipo de recurso de dados definido na etapa anterior.

Observação

Até 20 câmeras/grupos podem ser selecionados.

O relatório correspondente das câmeras/grupos selecionados será exibido.

4. Defina o ciclo estatístico como **Dia** , **Semana** , **Mês** , **Ano** ou **Personalizado** .

Relatório diário

O relatório diário mostra dados diariamente. A plataforma exibirá os dados de contagem de pessoas detectados em cada hora de dois dias adjacentes.

Relatório semanal, relatório mensal e relatório anual

Em comparação com o relatório diário, o relatório semanal, o relatório mensal e o relatório anual podem consumir menos tempo, já que não devem ser enviados todos os dias. A plataforma exibirá os dados de contagem de pessoas detectados em cada dia de duas semanas adjacentes, em cada dia de dois meses adjacentes e em cada mês de dois anos adjacentes.

5. Selecione um período de tempo predefinido ou personalize um período de tempo para estatísticas.

Observação

Para um relatório de intervalo de tempo personalizado, você precisa definir a hora de início e a hora de término para especificar o período de tempo.

6. Execute a(s) seguinte(s) operação(ões) após gerar o relatório de contagem de pessoas.

Operação	Descrição
Alternar entre ano após ano e ciclo após ciclo	Clique em **Alternar para ano a ano** / **Alternar para ciclo a ciclo** para comparar as estatísticas do relatório de diferentes maneiras. **Observação** Para exportar relatórios, estatísticas ano a ano e estatísticas ciclo a ciclo serão exportadas.
Adicionar ao painel	a. Clique em **Adicionar ao painel** no canto superior direito da página. b. Crie um nome para o relatório. c. Selecione um painel. Ou clique em **Novo** para criar um novo quadro e então selecione-o. d. Clique em **OK** ou **Adicionar e vá para o painel** .
Relatório de Exportação	e. Clique **em Exportar** . f. Marque/desmarque **All** para **Statistics Target** . Quando estiver marcado, somente o Excel estará disponível para o tipo de arquivo na próxima etapa.

Operação	Descrição
	Observação Esta opção está disponível somente para o relatório de análise de contagem de pessoas. g. Defina o formato do arquivo exportado como Excel, CSV ou PDF. h. Selecione a dimensão de tempo como **Por hora** , **Por dia** ou **Por mês** . i. Clique **em Exportar** . **Observação** ● Consulte ***Definir parâmetros gerais*** para obter detalhes sobre como definir o caminho de salvamento do relatório exportado. ● Você pode obter o relatório exportado na Central de Tarefas.
Abrir tela auxiliar	Clique em **Abrir tela auxiliar** para exibir o relatório na tela auxiliar.

Capítulo 19 Controle de Segurança

Um dispositivo de controle de segurança detecta pessoas, veículos, etc., entrando em uma região predefinida, aciona eventos e alarmes e relata informações de eventos/alarmes (como localização) ao pessoal de segurança.
No Control Client, o operador pode visualizar o vídeo das câmeras relacionadas ao radar, armar e desarmar partições, ignorar zonas, etc. Se um alarme de pânico for disparado, o operador pode lidar com a solicitação no Control Client.

19.1 Inicie a Visualização ao Vivo da Câmera Calibrada do Radar

Você pode iniciar a visualização ao vivo da câmera calibrada de um radar para visualizar a imagem da área de detecção do radar.

Antes de começar

Certifique-se de ter configurado pelo menos uma câmera calibrada para o radar. Consulte *o Manual do Usuário do HikCentral Professional Web Client* para obter detalhes sobre a configuração da câmera calibrada.

Passos

1. No canto superior esquerdo do Cliente, vá para → **Todos os Módulos** → **Monitoramento** → **Monitoramento** .
2. Selecione **Visualização ao vivo** .
3. Clique duas vezes no nome de um radar ou arraste um radar da lista de áreas para a área de exibição para iniciar a visualização ao vivo de suas câmeras calibradas.
   A imagem de uma câmera calibrada será exibida na janela de exibição.

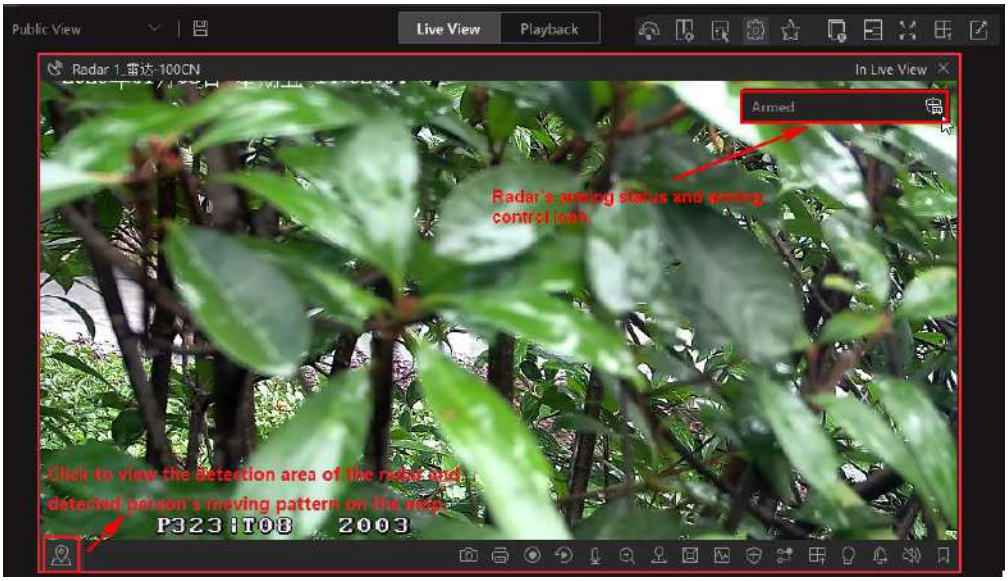


Figura 19-1 Visualização ao vivo das câmeras calibradas do radar

4. Opcional: Execute a(s) seguinte(s) operação(ões).

Controle de Armar	O status de armar do radar será exibido no canto superior direito da janela de visualização ao vivo. Clique para armar o radar; clique para desarmar um radar.
Trocar câmera calibrada	Passe o cursor sobre a miniatura para exibir as miniaturas de outras câmeras calibradas e, em seguida, clique em uma das miniaturas para exibi-la na janela de exibição.
Localizar no mapa	Clique no canto inferior esquerdo da janela de visualização ao vivo para mostrar o mapa onde o radar foi adicionado, para que você veja o padrão de movimento de quem invadiu a área de detecção.

Observação

- Um aviso sobre o status de armamento atual aparecerá se não houver nenhuma câmera calibrada vinculada ao radar quando você armar o radar.
- Um aviso sobre falha de armamento aparecerá se alguém estiver na área de detecção do radar quando você armar o radar.

19.2 Lidar com o Alarme de Pânico da Estação de Alarme de Pânico

Uma estação de alarme de pânico é instalada principalmente em áreas com multidão ou alta incidência de casos, como escolas, atrações turísticas, hospitais, mercados e estacionamentos. Quando a emergência acontece ou alguém pede ajuda, a pessoa pode pressionar o botão de pânico para enviar o alarme para o centro de monitoramento, e o operador no centro tomará as ações apropriadas.

Observação

Você deve primeiro definir um alarme disparado pela entrada de alarme para a estação de alarme de pânico via Web Client. Para detalhes, consulte o *Manual do Usuário do HikCentral Professional Web Client.*

Se alguém pressionar o botão de pânico na estação de alarme de pânico, uma janela aparecerá no Control Client como a seguinte:

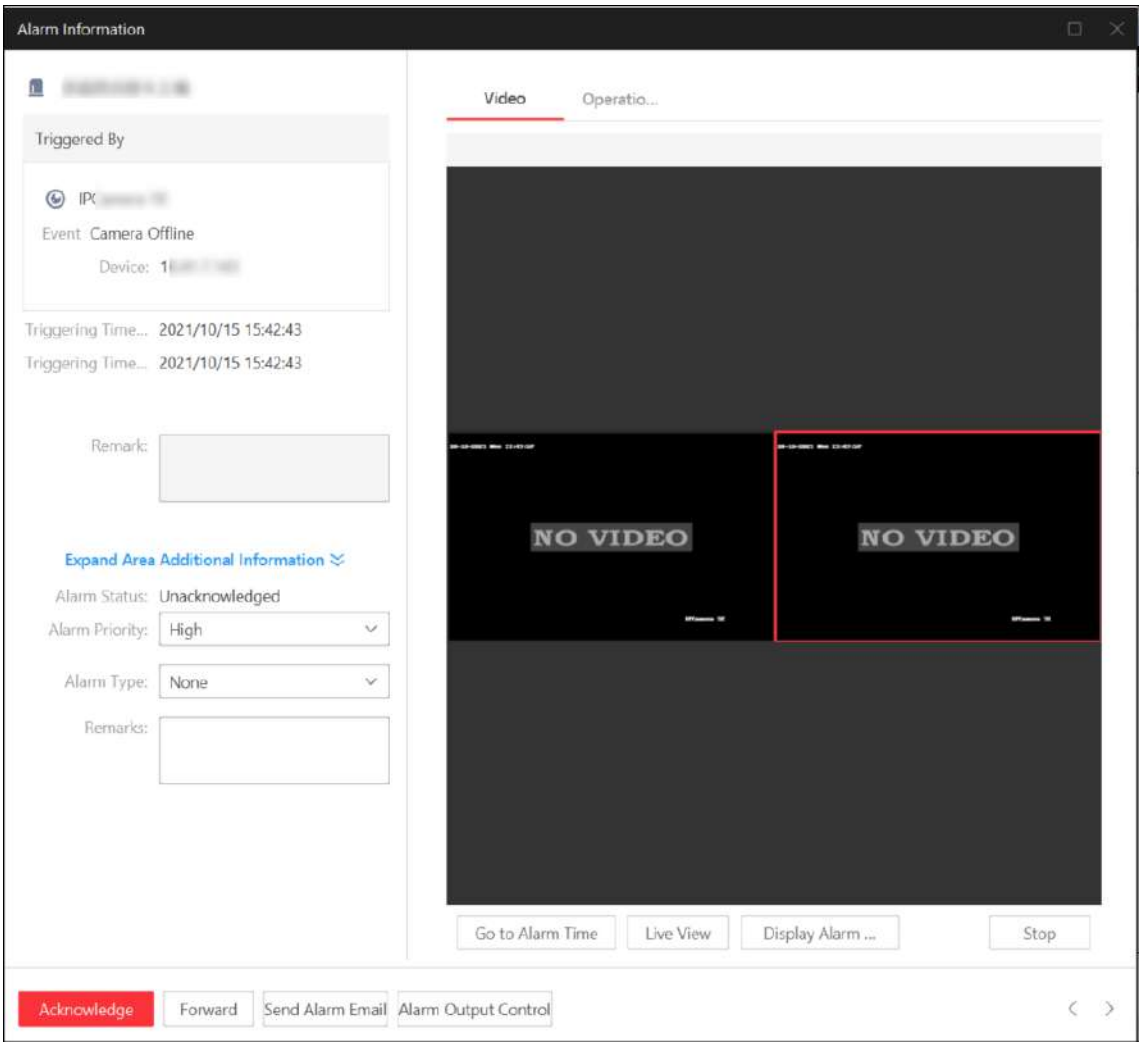


Figura 19-2 Alarme de pânico

Função	Descrição
Reconhecer alarme	Clique em **Reconhecer** para reconhecer este alarme de pânico.
Alarme de avanço	Clique **em Avançar** para encaminhar este alarme para outra pessoa.
Enviar e-mail de alarme	Clique em **Enviar e-mail de alarme** para enviar um e-mail de alarme para um destinatário específico.
Controle de saída de alarme	Clique em **Controle de Saída de Alarme** e ligue/desligue os interruptores para controlar o status das saídas de alarme.
Parar transmissão	Clique em **Parar transmissão** para interromper a transmissão de terminais específicos.

Capítulo 20 Controle de Acesso e Controle de Elevador

O controle de acesso é uma técnica de segurança que pode ser usada para regular quem pode ter acesso às portas especificadas e o controle de elevador pode ser usado para regular quem pode ter acesso aos andares especificados usando o elevador.
Depois de definir as permissões das pessoas para acessar portas e andares específicos, atribuindo níveis de acesso aos grupos de acesso, as pessoas autorizadas podem acessar portas e andares específicos com credenciais.

20.1 Monitoramento em Tempo Real

Com o grupo de operação de emergência, você pode controlar o status do ponto de acesso em um lote quando uma emergência acontece. Por exemplo, depois de agrupar as portas das entradas e saídas principais de uma escola em um grupo de operação de emergência, o pessoal de segurança da escola pode bloquear as portas no grupo, para que ninguém possa entrar ou sair da escola, exceto a manutenção e administradores de alto nível. Esta função também pode bloquear professores, zeladores, alunos, etc.

Observação

Somente usuários com função de Administrador ou Operador podem controlar todos os pontos de acesso em um lote.

- Certifique-se de ter agrupado as portas em um grupo de operação de emergência.
- Somente usuários com função de Administrador ou Operador podem controlar todas as portas em um lote.

Entre na página de monitoramento.
Você pode controlar todos ou parte dos pontos de acesso no site e área selecionados de acordo com sua necessidade. Quando a emergência terminar, você pode restaurar o status para Access with Credential.
No canto superior direito, clique para selecionar um site e uma área.

20.1.1 Iniciar Visualização ao Vivo de Dispositivos de Controle de Acesso/Controle de Elevador

Para dispositivos de controle de acesso com câmeras instaladas internamente ou conectadas externamente, e dispositivos de controle de elevador vinculados a câmeras, você pode iniciar a visualização ao vivo desses dispositivos.

Antes de começar

Certifique-se de ter adicionado os dispositivos à plataforma.

Passos

1. No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Monitoramento** → **Monitoramento** .
2. Clique duas vezes em um dispositivo à esquerda para iniciar a visualização ao vivo.
3. Passe o cursor na janela de visualização ao vivo para mostrar a barra de ferramentas na parte inferior. Você pode clicar em botões diferentes de acordo com sua necessidade.

   Exemplo

   Você pode clicar para iniciar o áudio bidirecional com pessoas próximas ao dispositivo.

20.1.2 Exibir Evento de Acesso em Tempo Real

No módulo Access Control, você pode visualizar eventos acionados por portas e elevadores. Você também pode controlar o status de portas e elevadores de acordo com os detalhes do evento, pesquisar mais informações sobre o evento e assim por diante.
Na página Monitoramento, selecione **Comparação de imagens faciais** .
Selecione uma biblioteca de imagens faciais cujos eventos de acesso você deseja visualizar.
Eventos de acesso em tempo real são exibidos na parte inferior da página.

Pesquisar registros de dispositivos	Clique na coluna Operação para ir para a página Recuperação de dados gravados do dispositivo e pesquisar registros personalizando as condições de pesquisa.
Coluna personalizada	Clique para personalizar as colunas a serem exibidas.
Eventos claros	Clique para limpar todos os eventos na lista.
Ver detalhes do último registro de acesso	No canto inferior direito desta página, marque **Auto Update Record** para exibir as informações da pessoa/visitante contidas no registro de acesso mais recente. Se você desmarcar **Auto Update Record** , a plataforma exibirá as informações da pessoa/visitante contidas nos registros de acesso históricos. A plataforma oferece suporte para ocultar a janela.

20.1.3 Controle de Porta

Você pode alterar o status de todas as portas em um local ou portas em grupos específicos de operações de emergência para trancadas, destrancadas, permanecendo trancadas ou

permanecendo destrancadas.
Acesse a página **Monitoramento** do Control Client.
Controle todas ou parte das portas no site atual.

Desbloquear

Quando uma porta estiver trancada, se você destrancar a porta, ela será destrancada. Quando a duração aberta acabar, a porta será trancada novamente automaticamente.

Trancar

Quando a porta estiver destrancada, se você trancar a porta, ela será fechada e trancada. A pessoa que tem a permissão de acesso pode acessar a porta com credenciais.

Permaneça desbloqueado

As portas serão destrancadas. Todas as pessoas podem acessar a porta sem a necessidade de credenciais. Esta função é usada quando uma emergência acontece e todas as pessoas são obrigadas a sair o mais rápido possível, como em uma escada de incêndio.
Clique na barra de ferramentas superior e selecione **Permanecer desbloqueado** → **Permanecer todas desbloqueadas** e todas as portas permanecerão desbloqueadas.
Clique na barra de ferramentas superior e selecione **Permanecer desbloqueado** → **Permanecer parcialmente desbloqueado** e selecione as portas para configurá-las para permanecer desbloqueadas.

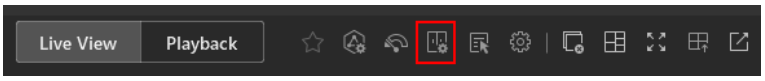


Figura 20-1 Barra de ferramentas na parte superior

Permanecer bloqueado

A porta será fechada e trancada. Nenhuma pessoa, exceto os usuários com permissão de super acesso, pode acessar a porta, mesmo com credenciais autorizadas. Esta função é aplicável para situações como impedir que pessoas indesejadas no prédio fujam.
Clique na barra de ferramentas superior e selecione **Permanecer bloqueado** → **Permanecer bloqueado** e todas as portas permanecerão bloqueadas.
Clique na barra de ferramentas superior e selecione **Permanecer bloqueado** → **Permanecer parcialmente bloqueado** e selecione as portas para configurá-las para permanecerem bloqueadas.

20.1.4 Controle de Piso

Você pode alterar o status de todos os andares em um local ou andares em grupos específicos de operações de emergência para acesso temporário, acesso com credencial, acesso livre ou acesso proibido.

Observação

Certifique-se de ter agrupado os andares em um grupo de operação de emergência.

Acesse a página **Monitoramento** do Control Client.
Controle todos ou parte dos andares no local atual.

Acesso Temporário

Durante o tempo de acesso temporário, as pessoas podem acessar este andar sem a necessidade de credenciais. Após o tempo de acesso, o andar será recuperado para o status Access with Credential.

Acesso com Credencial

A pessoa que possui permissão de acesso pode acessar este andar com credenciais.

Acesso Livre

Todas as pessoas podem acessar este andar sem necessidade de credenciais.
Clique na barra de ferramentas superior e selecione **Permanecer desbloqueado/acesso livre** → **Permanecer todos desbloqueados/acesso livre** e todos os andares permanecerão desbloqueados.
Clique na barra de ferramentas superior e selecione **Permanecer desbloqueado/acesso livre** → **Permanecer parcialmente desbloqueado/acesso livre** e selecione os andares para defini-los como desbloqueados.

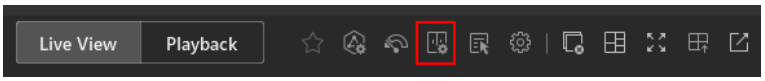


Figura 20-2 Barra de ferramentas na parte superior

Acesso Proibido

Nenhuma pessoa, exceto os usuários com permissão de super acesso, pode acessar este andar, mesmo com credenciais autorizadas. Esta função é aplicável para situações como impedir que pessoas não autorizadas no edifício escapem.
Clique na barra de ferramentas superior e selecione **Permanecer bloqueado/Acesso proibido** → **Permanecer todos bloqueados/Acesso proibido** e todos os andares permanecerão bloqueados.
Clique na barra de ferramentas superior e selecione **Permanecer bloqueado/Acesso proibido** → **Permanecer parcialmente bloqueado/Acesso proibido** e selecione os andares para defini-los como bloqueados.

20.2 Pesquisar Registros de Autenticação de Pessoas

Você pode pesquisar registros de autenticação de pessoas acionados em pontos de acesso especificados definindo condições de pesquisa. Por exemplo, se você selecionar pontos de acesso específicos e definir o tipo de evento como acesso negado por cartão, você pode obter todos os eventos de acesso negado (acesso por passagem de cartão) acionados nos pontos de acesso.

Antes de começar

Certifique-se de ter configurado o evento de ponto de acesso no Web Client. Para obter detalhes, consulte o *Manual do Usuário do HikCentral Professional Web Client* .

Passos

1. Opcional: Na página Registro de autenticação de pessoa, importe registros de autenticação de pessoa para o sistema.
   – Importar do(s) dispositivo(s).
      1. Clique em **Importar evento** → **Importar do dispositivo** para entrar na página Importar do dispositivo.
      2. Selecione o(s) dispositivo(s) na lista de dispositivos.
      3. (Opcional) Ative o **Intervalo de tempo especificado** e defina a hora de início e a hora de término para importar registros gerados no período de tempo especificado.

      Observação

      - Se o dispositivo tiver carregado registros no sistema anteriormente, não será necessário ativar o **Intervalo de tempo especificado** e os registros dos últimos 7 dias do(s) dispositivo(s) selecionado(s) serão importados por padrão se nenhum intervalo de tempo for especificado.
      - Se o dispositivo nunca tiver carregado nenhum registro no sistema antes, você deverá ativar o **Intervalo de tempo especificado** para importar registros dos dispositivos selecionados.

      4. Clique em **OK** para iniciar a importação.

      Uma janela será exibida para exibir o progresso da importação e os detalhes da falha.
   – Importe do arquivo que é exportado do dispositivo.
      1. Clique em **Importar evento** → **Importar do arquivo** para entrar na página Importar do arquivo.
      2. Clique para selecionar o arquivo a ser importado.

      Observação

      Somente o arquivo criptografado pode ser importado.

      3. Digite a senha no campo **Senha** .
      4. Clique **em OK** .
2. Na lista suspensa **Tempo , selecione o tempo durante o qual os registros são gerados.**

   Observação

   A hora aqui pode ser a hora do dispositivo ou a hora do cliente, que é baseada nas configurações de fuso horário em **Sistema** → **Geral** .
3. Selecione um site na lista suspensa Site.
4. Opcional: Na área **Ponto de acesso , clique em** , selecione a área na lista à esquerda e selecione a(s) porta(s) ou elevador(es), ou selecione tudo na lista à direita.
5. Opcional: Na área **Tipo de evento , clique** para selecionar o(s) tipo(s) de evento.
6. Na lista suspensa **Resultado da autenticação , selecione um tipo de resultado de acesso para filtrar rapidamente registros de acesso concedido ou registros de acesso negado.**
7. Defina o modo de pesquisa.

1. Selecione **Pessoa/Visitante** como modo de pesquisa.
2. Selecione **Selecionar pessoa** ou **Correspondência aproximada** como modo de pesquisa.

Selecionar pessoa

Clique para selecionar a(s) pessoa(s)

Correspondência Fuzzy

Insira uma palavra-chave para procurar pessoas cujo nome contenha a palavra-chave.

3. Clique em **Adicionar** para selecionar a(s) pessoa(s) ou insira as palavras-chave do nome da pessoa para correspondência aproximada.

1. Selecione **Nº do cartão** como modo de pesquisa.
2. Digite o número do cartão.

8. Opcional: ative **o Status da temperatura** e selecione **Normal** ou **Anormal** .
9. Opcional: ative **o Status de uso da máscara** e selecione **Usando máscara** ou **Sem máscara** .
10. Clique em **Pesquisar** .

Os registros correspondentes são listados à direita.

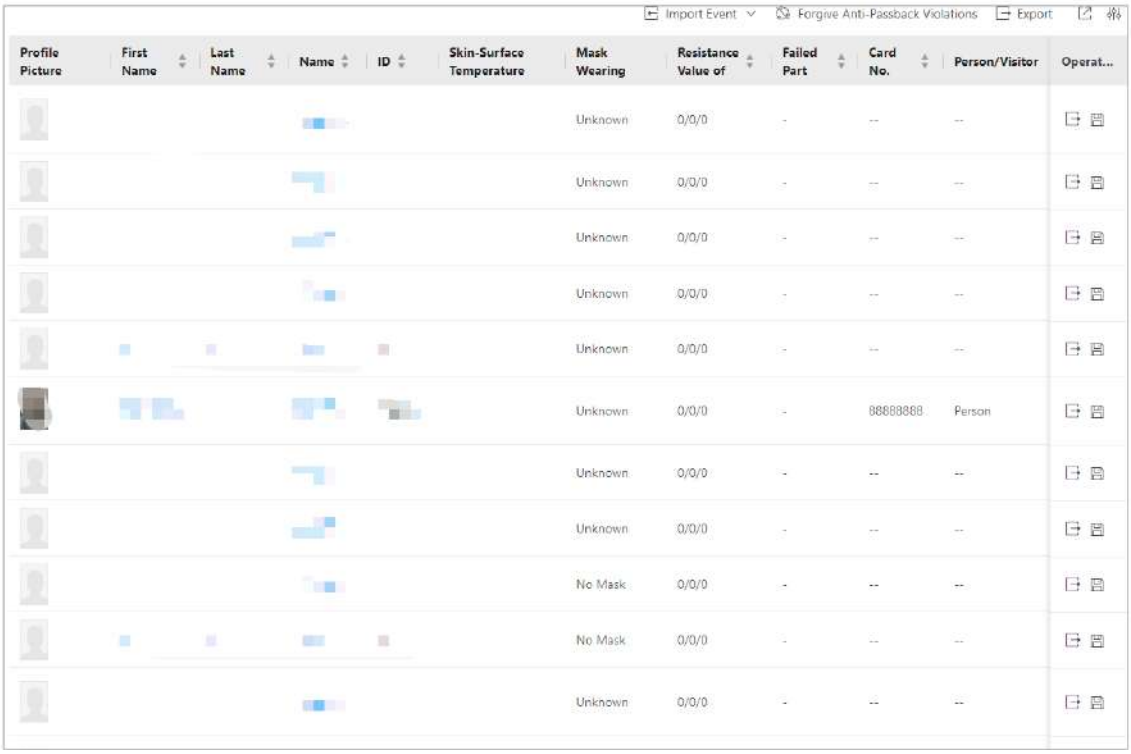


Figura 20-3 Registros de autenticação de pessoa

11. Opcional: execute as seguintes operações após pesquisar registros.

Ver detalhes do registro	Clique no nome da pessoa na coluna Nome completo para visualizar os detalhes do registro, como informações da pessoa e informações de acesso.
Perdoar violação	Quando uma pessoa tenta usar um cartão sem seguir a regra anti-

anti-passback	passback, o acesso será negado. Isso é chamado de "Violação Anti-Passback". Quando a violação anti-passback ocorre, nenhum acesso é permitido a menos que o evento de violação anti-passback seja perdoado. Você pode clicar em **Perdoar Anti-Passback** na parte superior para perdoar todos os eventos de violação de anti-passback nos resultados da pesquisa.
Exportar registro único	Clique na coluna Operação para salvar um registro como um arquivo Excel ou CSV no seu PC, incluindo os detalhes do evento, as informações da pessoa, o perfil da pessoa, o arquivo de vídeo gravado (se configurado), etc.
Exportar todos os registros pesquisados	Clique em **Exportar** no canto superior direito para salvar os detalhes do registro pesquisado no seu PC. Você pode selecionar o formato do arquivo como Excel, PDF ou CSV e selecionar itens para exportar.
Salvar um registro como evidência	Clique para salvar o registro no centro de gerenciamento de evidências.

Observação

- A senha é necessária por questões de segurança.
- Você pode visualizar o progresso do download na Central de Tarefas ao exportar os dados.

20.3 Pesquisar por Logs de Dispositivos

Os logs podem ser eventos/alarmes disparados por eventos anormais detectados por dispositivos e aqueles disparados por dispositivos (como falhas de dispositivos). Você pode procurar os logs em diferentes dimensões de acordo com suas necessidades.

Passos

1. No canto superior esquerdo da página Registro do dispositivo, selecione um intervalo de tempo para pesquisa.
2. Selecione um site na lista suspensa Site.
3. Ative os tipos de recursos nos quais você deseja pesquisar registros.

Ponto(s) de acesso

Os pontos de acesso incluem portas de dispositivos de controle de acesso e dispositivos de intercomunicação de vídeo, e andares de dispositivos de controle de elevador. Os logs podem ser registros de acesso, registros de operação e alarmes disparados por comportamentos humanos.

Dispositivo

Os dispositivos incluem dispositivos de controle de acesso, dispositivos de controle de elevador e dispositivos de intercomunicação de vídeo. Os logs registrados nesses dispositivos podem cobrir todos os eventos acionados pelos dispositivos (como falhas de dispositivos).

Entrada de alarme

As entradas de alarme incluídas nos dispositivos. Os logs estão armando mudanças de status.

4. Selecione a(s) fonte(s) de evento e o(s) tipo(s) de evento para cada tipo de recurso ativado.
5. Clique em **Pesquisar** .

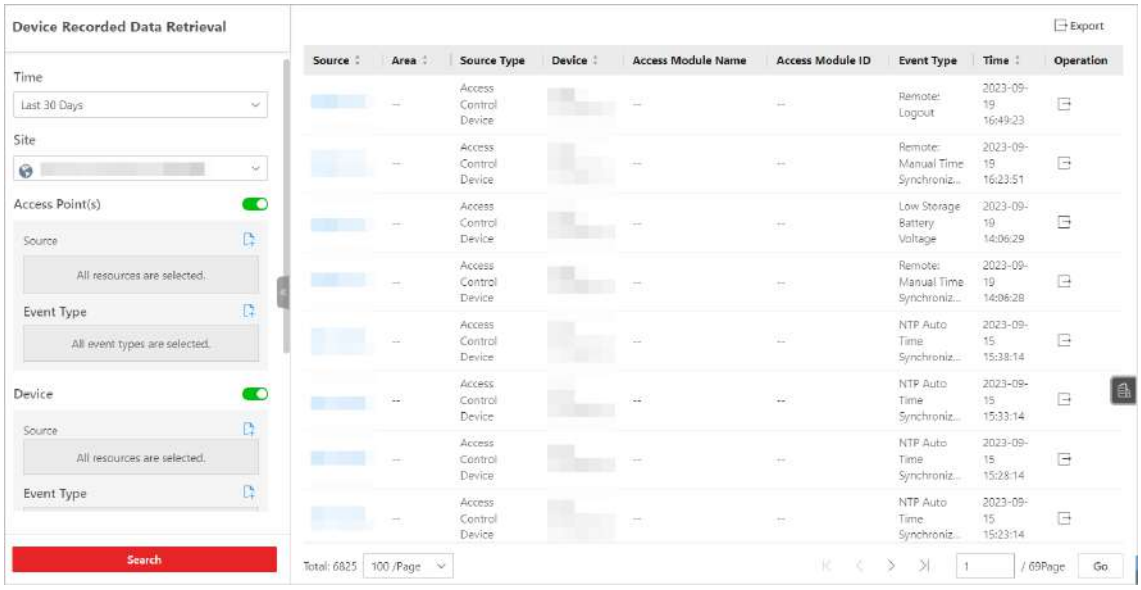


Figura 20-4 Recuperação de dados registrados do dispositivo

6. Opcional: Execute outras operações nos registros pesquisados.

Ver detalhes do registro	Clique no nome do dispositivo na coluna Origem para visualizar os detalhes do registro, como o nome do dispositivo e o tipo de registro.
Exportar registro único	Clique na coluna Operação para salvar o registro no PC local como um arquivo CSV.
Exportar todos os registros pesquisados	Clique em **Exportar** para salvar todos os registros pesquisados no PC local como um arquivo Excel, PDF ou CSV.

Observação

- A senha é necessária por questões de segurança.
- Você pode visualizar o progresso do download na Central de Tarefas ao exportar os dados.

20.4 Porta Aberta para Autenticação Multifator

No controle de acesso, a autenticação multifator é um método de autenticação no qual a porta será destrancada somente após várias pessoas autenticarem várias credenciais por vez. Esse método é usado principalmente para locais com altos requisitos de segurança, como cofres de banco. Com a supervisão mútua das pessoas, a autenticação multifator fornece maior segurança para os ativos nesses locais.
Você pode definir uma regra de autenticação multifator no Web Client. Para obter detalhes, consulte o *Manual do Usuário do HikCentral Professional Web Client* .
Se você definir o modo de acesso como **Desbloqueio Remoto Após Concedido** , quando as pessoas no grupo de acesso forem autenticadas na porta, uma janela aparecerá no Control Client conforme a seguir.
Clique em **Answer** para responder à solicitação e iniciar o áudio bidirecional. Se a porta estiver vinculada a uma câmera, você pode visualizar o vídeo ao vivo da câmera relacionada. Você precisa verificar a identidade das pessoas antes de abrir a porta.

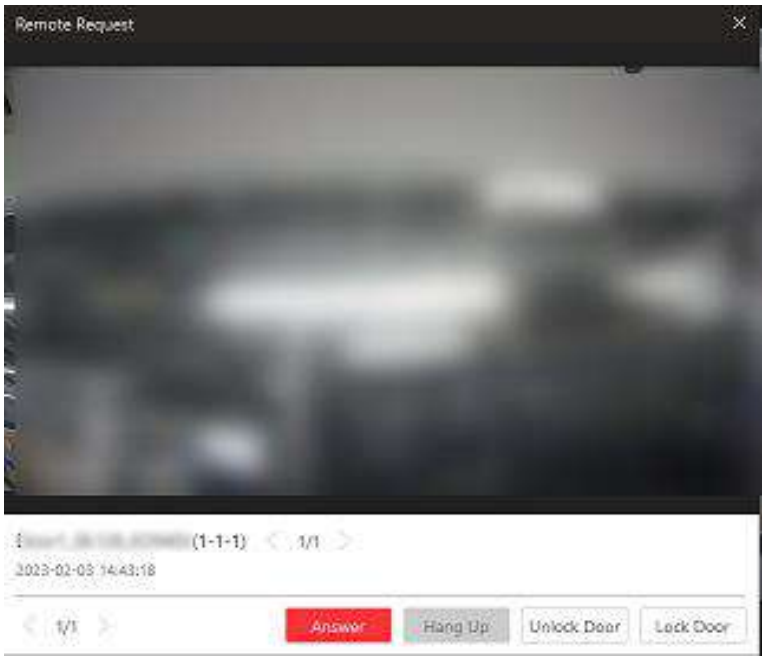


Figura 20-5 Porta aberta remotamente

Clique em **Abrir porta** e a porta será destrancada.

20.5 Solicitação de Abertura de Porta de Alça do Terminal de Controle de Acesso por Vídeo

O terminal de controle de acesso por vídeo suporta conversação por voz com o cliente conectado. A pessoa pode pressionar um botão no painel frontal do dispositivo para enviar uma solicitação de abertura de porta para o pessoal de segurança e o pessoal de segurança pode falar com a

pessoa via Control Client, visualizar o vídeo ao vivo da câmera do terminal de controle de acesso por vídeo e destrancar a porta se a identidade da pessoa for confirmada. Esta função é usada principalmente quando a pessoa esquece de levar suas credenciais ou para visitantes.

Observação

Antes que o Control Client receba a solicitação remota do terminal de controle de acesso de vídeo, você deve primeiro adicionar um alarme **Calling Surveillance Center** para o ponto de acesso deste terminal de controle de acesso de vídeo no Web Client. Para obter detalhes sobre como adicionar alarmes, consulte o *Manual do Usuário do HikCentral Professional Web Client* .

Após pressionar o botão no painel frontal do dispositivo, uma janela aparecerá no Control Client. Você pode visualizar a visualização ao vivo da câmera do terminal de controle de acesso de vídeo e executar as seguintes operações.

- Responder solicitação: clique em **Responder** para iniciar uma conversa de voz com a pessoa que iniciou a solicitação.
- Ignorar solicitação: clique em **Ignorar** para ignorar esta solicitação e fechar esta janela.
- Abrir porta: durante a conversa por voz, clique em **Abrir porta** para permitir que a pessoa entre.
- Encerrar chamada: clique em **Encerrar chamada** para encerrar a conversa de voz e fechar esta janela.

20.6 Exibir Estatísticas Finais de Autenticação

O sistema pode contar indivíduos em uma região agrupando portas e usando registros de autenticação final. Isso permite que você veja quem recebeu acesso e quantas pessoas ainda estão na área. A função é aplicável para certas cenas de emergência. Por exemplo, durante uma saída de incêndio, todas as pessoas são obrigadas a sair da região.

Antes de começar

Certifique-se de ter adicionado grupos de contagem de autenticação final para agrupar as portas no Web Client. Para obter detalhes, consulte o *Manual do Usuário do HikCentral Professional Web Client* .

Passos

1. Na página Contagem de autenticação final, selecione um intervalo de tempo para a contagem.
2. Na lista **Origem** , selecione um grupo de autenticação final.
3. Na lista suspensa **Tipo de contagem de entradas e saídas , selecione o tipo de pessoas que você deseja pesquisar.**

   Todas as pessoas

   Todos os registros de acesso de entrada e saída nas últimas 24 horas serão listados.

   As pessoas ficaram

   Pessoas que ainda estão na região serão listadas. O sistema filtra as pessoas cujo registro de entrada é encontrado, mas o registro de saída não é encontrado.

   Pessoas Sairam

As pessoas que entraram e saíram da região posteriormente serão listadas.

4. Clique em **Pesquisar** .
   Todos os registros correspondentes serão listados, mostrando informações como detalhes da pessoa, local do último acesso, etc.
5. Opcional: Execute outras operações após a pesquisa.

Ver detalhes do evento	Clique no nome da pessoa na coluna Nome para visualizar os detalhes do registro, incluindo o vídeo gravado da câmera relacionada ao ponto de acesso (se configurado), informações da pessoa e informações de acesso.
Exportar registro único	Clique na coluna Operação para baixar o registro, incluindo informações da pessoa, perfil da pessoa, número de telefone, local do último acesso, etc.
Exportar todos os registros pesquisados	Clique em **Exportar** no canto superior direito para exportar os detalhes dos eventos de controle de acesso pesquisados (incluindo informações da pessoa, perfil da pessoa, número de telefone, local do último acesso, etc.).
Imprimir Registro Único	Clique na coluna Operação para imprimir o registro.
Imprimir todos os registros pesquisados	Clique em **Imprimir** no canto superior direito para imprimir todos os registros pesquisados.

Observação

- A senha é necessária por questões de segurança.
- Até 100.000 registros podem ser exportados por vez.
- Você pode visualizar o progresso do download na Central de Tarefas ao exportar os dados.

Capítulo 21 Manutenção

O Control Client permite que você monitore o status de integridade do recurso e pesquise logs de recursos. Os dados de status de integridade do recurso e logs de recursos, que são especialmente importantes para a manutenção do sistema, ajudam a localizar a fonte de exceções e determinar métodos para solução de problemas.
Na página inicial, selecione **Manutenção** ou selecione → **Todos os módulos** → **Manutenção** .

21.1 Visão Feral da Saúde

Health Overview fornece informações quase em tempo real e de histórico sobre o status do SYS e recursos adicionados. É essencial para vários aspectos da operação dos servidores ou dispositivos e é especialmente importante para manutenção. Quando ocorre uma exceção de recurso, você pode entrar neste módulo para verificar o status do recurso e descobrir os dispositivos anormais e visualizar os detalhes da exceção.

21.1.1 Visão Geral do Status de Saúde em Tempo Real

No módulo Health Overview, você pode visualizar o status de saúde em tempo real dos dispositivos, servidores e recursos gerenciados na plataforma. Se não houver dispositivos de transmissão de rede adicionados, a página Real-Time Overview fornece uma visão geral do status de saúde com gráficos e dados básicos do status do recurso.
Selecione **Visão geral em tempo real** .

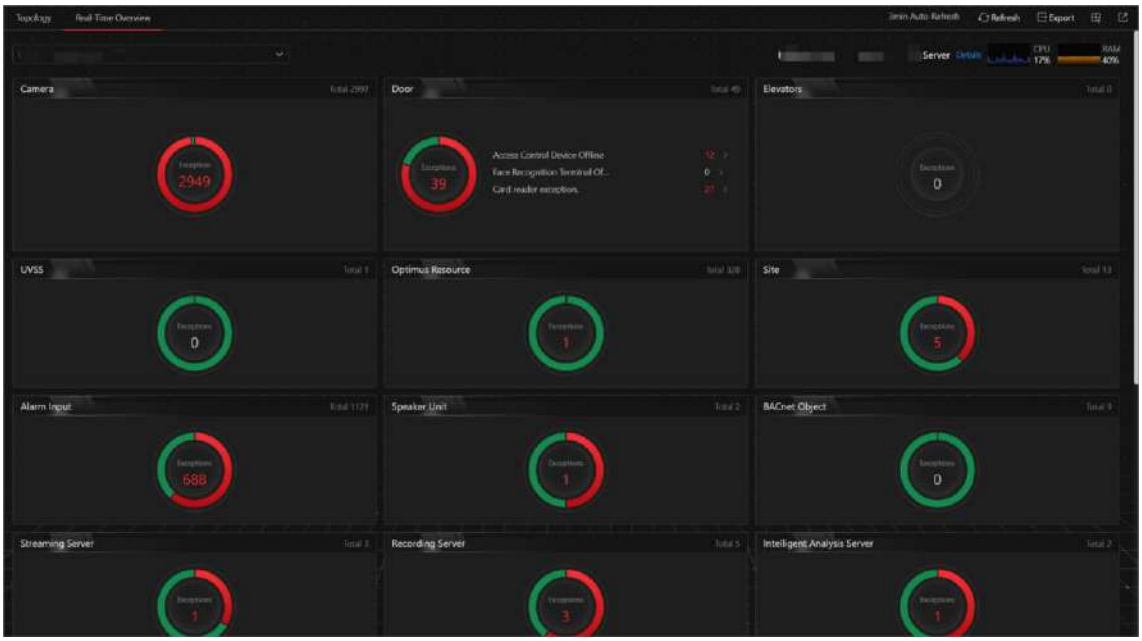
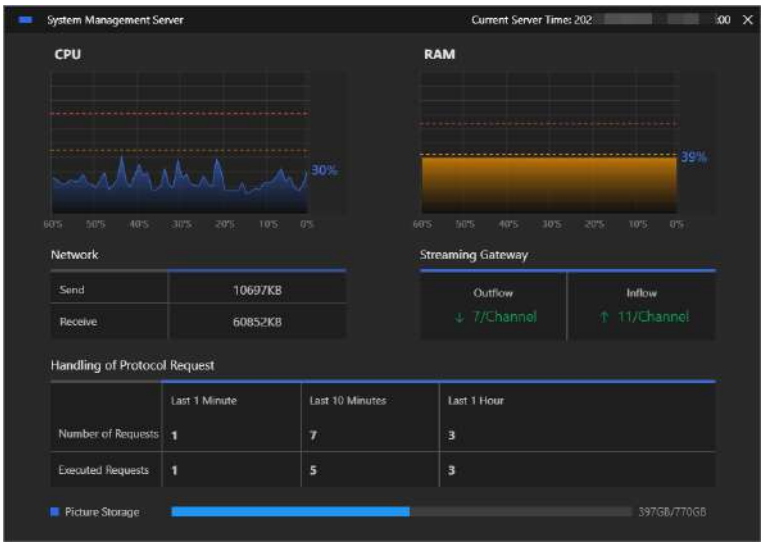


Figura 21-1 Visão geral do status de saúde em tempo real

Tabela 21-1 Página de status de saúde em tempo real

Seção	Descrição
Exibir status do recurso por site	Selecione um site na lista suspensa no canto superior esquerdo para exibir o status dos recursos no site selecionado. Se ocorrer uma exceção em um site, o ícone aparecerá ao lado do nome do site e você poderá mover o cursor sobre ele para visualizar os detalhes da exceção.
Status do servidor de gerenciamento do sistema	Veja o uso de CPU e RAM do servidor do site no canto superior direito da página de visão geral. Clique em **Detalhes** para abrir a janela Servidor de Gerenciamento do Sistema para visualizar o status detalhado, incluindo o horário atual do servidor, uso da CPU, uso da RAM, status da rede, status do gateway de streaming, status de tratamento da solicitação de protocolo e armazenamento de imagens.  **Figura 21-2 Detalhes de status do servidor de gerenciamento do sistema**
Status do recurso	Visualize os dados anormais de diferentes recursos adicionados à plataforma de forma gráfica. Você pode mover o cursor sobre o gráfico para exibir os tipos de exceção e os números correspondentes de dispositivos anormais e, em seguida, clicar em um tipo ou número no gráfico para visualizar os detalhes de status em tempo real dos recursos.
Estatísticas de exceção do dispositivo	Veja o número de dispositivos anormais com diferentes tipos adicionados na plataforma. Você pode clicar em um número sob a imagem do dispositivo para ver os detalhes do status em

Seção	Descrição
	tempo real do dispositivo. Se o ícone aparecer na parte superior da imagem do dispositivo, isso indica que o firmware do dispositivo deve ser atualizado. Para atualizar o firmware, consulte o *HikCentral Professional Web Client User Manual* .
Atualizar página de visão geral	● Atualizar manualmente: clique em **Atualizar** no canto superior direito da página Visão geral em tempo real para atualizar manualmente o status do recurso na página. ● Atualização Automática: **Gerenciamento** → **Sistema** → **Monitoramento de Saúde** para definir o intervalo para atualização automática do status do recurso na página. Veja os detalhes em ***Definir Frequência de Verificação de Saúde*** .
Página de Visão Geral de Exportação ou Dados de Exceção	Clique em **Exportar** no canto superior direito da página Visão geral em tempo real para exportar a página em formato PDF. Ou você pode marcar **Exportar dados de exceção** para exportar os dados de exceção em formato Excel/CSV.  **Figura 21-3 Página de Visão Geral de Exportação ou Dados de Exceção**
Exibir na parede inteligente	Clique para exibir a página de visão geral no smart wall se você tiver adicionado e configurado smart walls na plataforma.

21.1.2 Visão Geral do Status de Saúde em Tempo Real (topologia)

No módulo Health Overview, você pode visualizar o status de saúde em tempo real dos dispositivos, servidores e recursos gerenciados na plataforma. Se houver dispositivos de transmissão de rede gerenciados na plataforma, a página Real-Time Overview fornece uma topologia dos dispositivos gerenciados. Topologia é uma figura que exibe as relações de conexão entre dispositivos de transmissão de rede, dispositivos de segurança, etc. É usada principalmente

para manutenção de rede.

Observação

- Certifique-se de que os dispositivos de transmissão de rede foram adicionados à plataforma.
- Se um dispositivo de transmissão de rede não puder ser reconhecido pela plataforma, ele será exibido como um dispositivo desconhecido.
- A topologia não suporta câmeras corporais, mas suporta dispensadores de tíquetes.

Na área Visão geral da saúde, selecione **Visão geral em tempo real** .
Clique na aba **Topologia** na parte superior para entrar na página Topologia.

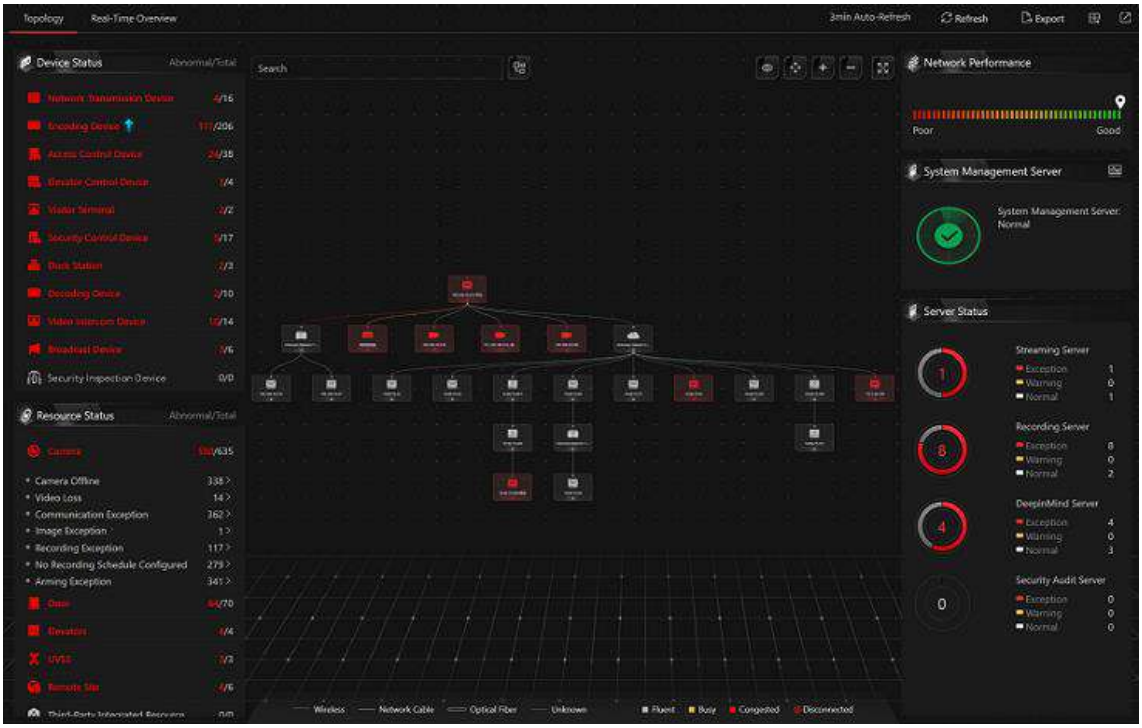
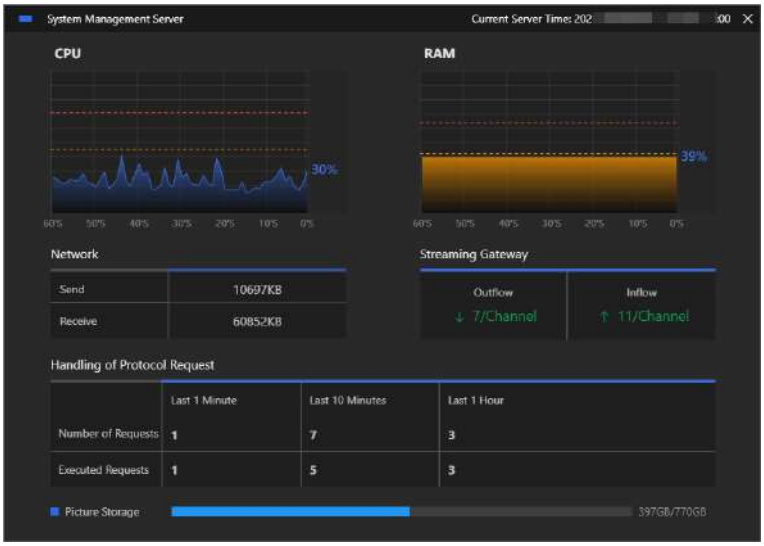


Figura 21-4 Visão geral da topologia

Tabela 21-2 Página Topologia

Seção	Descrição
Status do dispositivo	Visualize os dados anormais de diferentes dispositivos adicionados à plataforma. Você pode clicar no número para localizar o dispositivo anormal na topologia ou visualizar o status em tempo real dos dispositivos. Se o ícone aparecer ao lado do nome do tipo de dispositivo, isso indica que o firmware do dispositivo deve ser atualizado. Para atualizar o firmware, consulte o *HikCentral Professional Web Client User Manual* .
Status do recurso	Visualize os dados anormais de diferentes recursos adicionados

Seção	Descrição
	à plataforma. Você pode clicar em um número para visualizar os detalhes de status em tempo real dos recursos.
Detalhes da topologia	Visualize os relacionamentos entre dispositivos, informações do dispositivo, status do link, informações de alarme, etc. Veja os detalhes em ***Detalhes da topologia*** .
Desempenho da rede	Visualize o desempenho atual da rede (ruim ou bom) do System Management Server.
Status do servidor de gerenciamento do sistema	Clique no canto superior direito da seção Servidor de Gerenciamento do Sistema para visualizar o status detalhado, incluindo o horário atual do servidor, uso da CPU, uso da RAM, status da rede, status do gateway de streaming, status de tratamento da solicitação de protocolo e armazenamento de imagens.  **Figura 21-5 Detalhes de status do System Management Server**
Status do servidor	Visualize o status (ou seja, exceção, aviso, normal) dos servidores adicionados na plataforma.
Gerar Topologia Novamente	Clique em **Atualizar** → **Gerar topologia novamente** para desenhar a topologia de rede novamente.
Atualizar	● Atualização manual: clique em **Atualizar** no canto superior direito da página Visão geral em tempo real para atualizar manualmente o status do recurso na página. ● Atualização Automática: **Gerenciamento** → **Sistema** → **Monitoramento de Saúde** para definir o intervalo para atualização automática do status do recurso na página. Veja os detalhes em ***Definir Frequência de Verificação de Saúde*** .

<table>
<tr><th>Seção</th><th>Descrição</th></tr>
<tr><td>Exportar dados de topologia ou exceção</td><td>Clique em Exportar no canto superior direito da página Topologia e selecione o tipo de exportação como Padrão ou Somente Topologia para exportar a topologia em formato PDF ou os dados de exceção em formato Excel/CSV.

Observação
● Se o tipo de exportação for selecionado como Padrão , todas as informações exibidas (topologia e dados de exceção) na página Monitoramento de integridade serão exportadas.
● Se o tipo de exportação for selecionado como Somente topologia , somente a topologia será exportada no formato PDF.

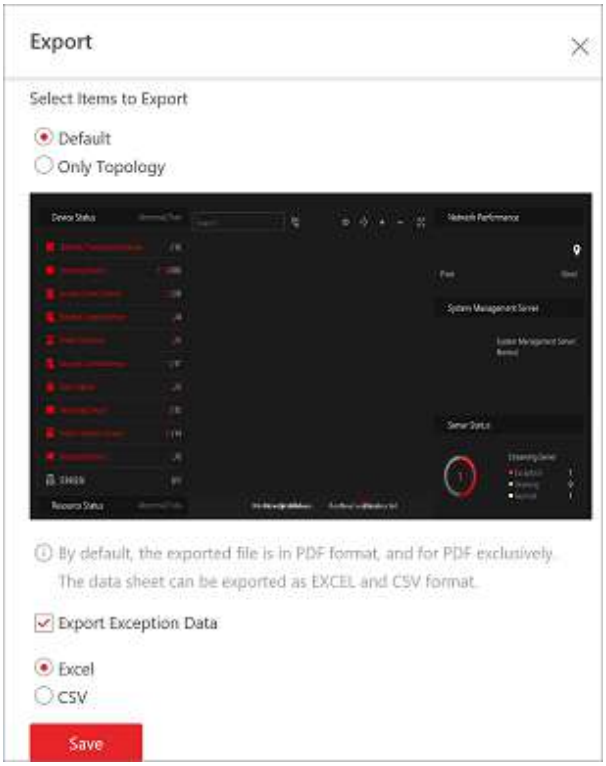
 

Figura 21-6 Topologia de exportação</td></tr>
<tr><td>Exibir na parede inteligente</td><td>Clique para exibir a página de visão geral no smart wall se você tiver adicionado e configurado smart walls na plataforma.</td></tr>
</table>

Detalhes da topologia

A topologia dos dispositivos exibirá os relacionamentos hierárquicos entre os dispositivos,

informações do dispositivo, status do link, informações de alarme, etc.

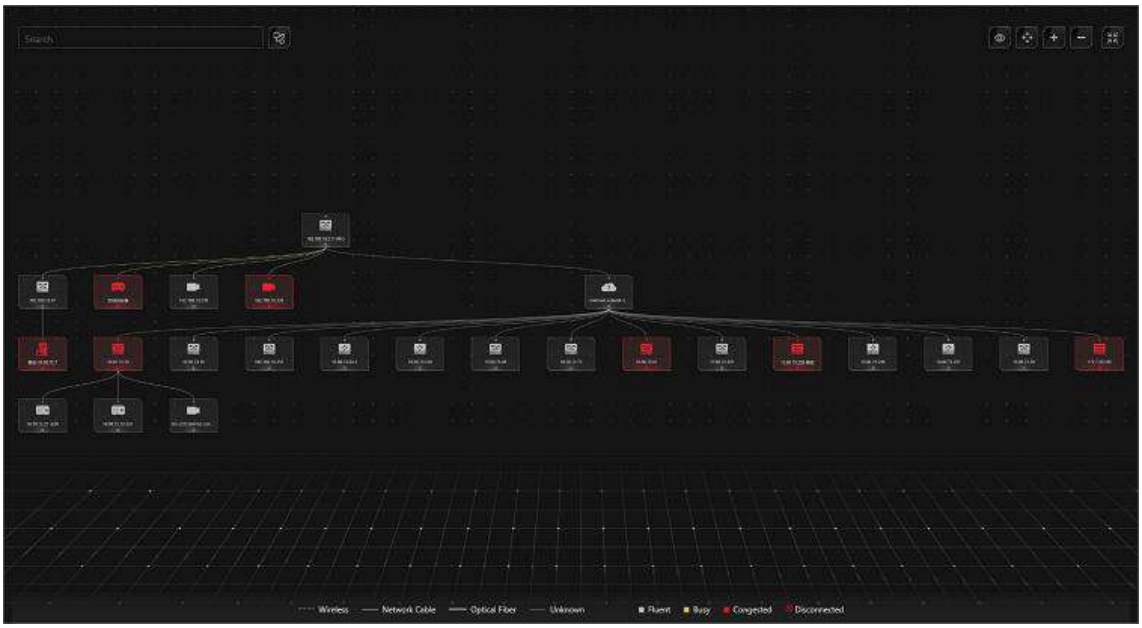


Figura 21-7 Detalhes da topologia

Nó do dispositivo

Os nós do dispositivo são exibidos por ícones, incluindo o Servidor de Gerenciamento do Sistema, Servidor de Gravação, dispositivo de transmissão de rede, dispositivo de codificação, dispositivo de controle de acesso, dispositivo de intercomunicação de vídeo, ponte de rede, conversor de fibra, etc. Cada nó do dispositivo exibe o nome do dispositivo e o endereço IP.

Observação

- Quando as informações do dispositivo (nome do dispositivo, endereço IP, status online/offline) forem alteradas, você deverá atualizar manualmente para gerar a topologia novamente ou definir a atualização automática.
- Quando a hierarquia do dispositivo ou a conexão física mudar, você deverá atualizar manualmente para gerar a topologia novamente.
- Se o ícone do nó for exibido em vermelho, isso indica que o dispositivo está anormal ou que alarmes foram disparados. Você pode visualizar o motivo da exceção do dispositivo ou detalhes do alarme.
- Para os dispositivos on-line adicionados, o alias do dispositivo exibido é o mesmo que o endereço IP do dispositivo.

Ver detalhes do dispositivo

Clique no nó do dispositivo na topologia e clique em **Detalhes** na lista suspensa. Você pode visualizar os detalhes do dispositivo, incluindo as informações básicas (por exemplo, nome do dispositivo, endereço IP e modelo do dispositivo), uso do dispositivo (por exemplo, uso de RAM, uso de CPU, energia PoE), status de armação e matriz de disco (para dispositivo de codificação), vídeo ao vivo (se o dispositivo estiver vinculado a uma câmera), nome da faixa vinculada /

direção de entrada / nome de entrada e saída / status de controle de barreira (se a entrada e a saída estiverem vinculadas a uma câmera), status do painel do dispositivo (por exemplo, portas e uso de portas) e informações da porta (por exemplo, nome da porta e tipo de dispositivo par, endereço IP do dispositivo par e nome do dispositivo par).

Observação

Os detalhes do dispositivo variam de acordo com os diferentes modelos.

Link

A cor do link indica a taxa de utilização da largura de banda da rede (vermelho: congestionado, amarelo: ocupado, cinza: fluente). E o formato do link indica o tipo de link (sem fio, link de rede, fibra óptica).

Ver detalhes do link

Mova o cursor para o link entre os nós para exibir os detalhes do link. Você pode visualizar a taxa upstream e a taxa downstream para determinar se o status da rede é normal ou não. Você também pode visualizar o tipo de dispositivo conectado, endereço IP, nome da porta e status da porta.

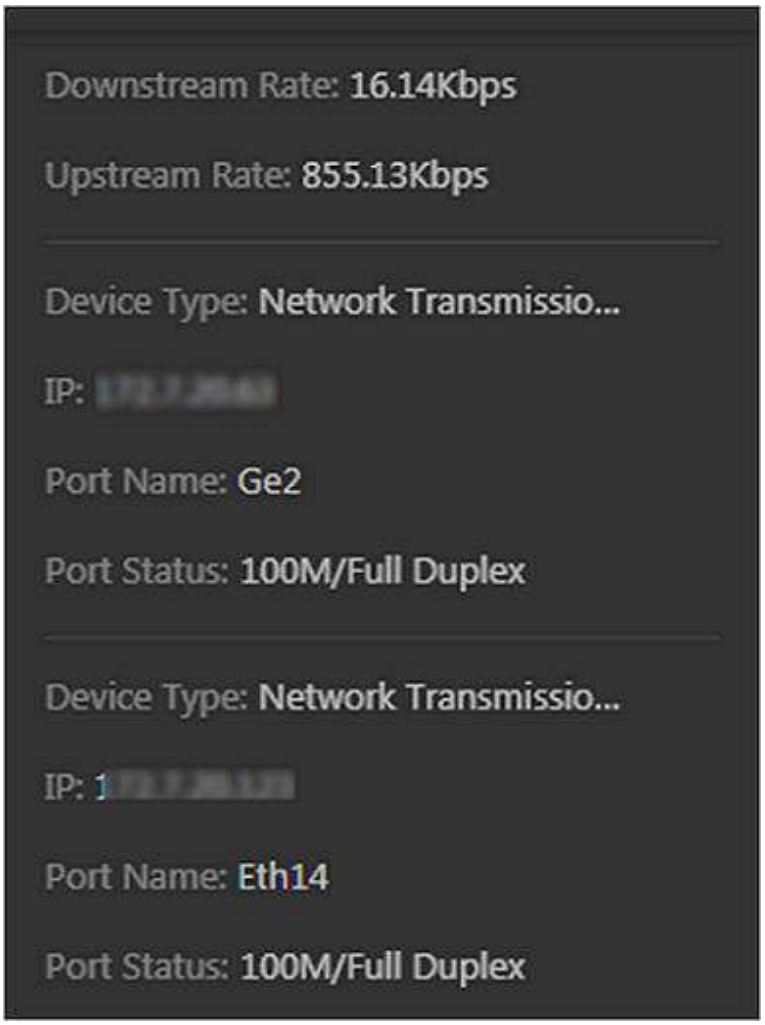


Figura 21-8 Exibir detalhes do link

Exibir caminho de conexão

Se houver uma falha de transmissão de dados entre os dispositivos, você pode visualizar o caminho de conexão para julgar qual link está desconectado, de modo a restaurar o link o mais rápido possível. Clique no nó do dispositivo e na topologia e clique em **Mostrar caminho de conexão** na lista suspensa. De acordo com as informações apresentadas na janela de prompt, clique em **Common Unknown Node** ou **Select Node** para selecionar o nó peer e, em seguida, clique em **OK** . Depois disso, o caminho de conexão entre os dois nós será exibido.

Configuração remota

Clique no nó do dispositivo na topologia e clique em **Configuração Remota** na lista suspensa para configurar os parâmetros do dispositivo, incluindo configurações do sistema, rede e configuração de porta. Você pode configurar os parâmetros de rede e a porta do dispositivo de acordo com o uso da rede. Para obter detalhes, consulte o manual do usuário do dispositivo.

Observação

Esta função deve ser suportada pelo dispositivo.

Exibir logs do dispositivo

Quando ocorre uma falha no dispositivo ou é necessária uma solução de problemas, você pode visualizar os logs do dispositivo para saber os alarmes, notificações, operações e eventos do dispositivo. Clique no nó do dispositivo na topologia e clique em **View Device Logs** na lista suspensa para entrar na página Device Logs, e você pode definir as condições para pesquisar os logs do dispositivo.

Observação

Esta função deve ser suportada pelo dispositivo.

Definir como nó raiz

Quando precisar ajustar a estrutura da topologia, você pode clicar no nó do dispositivo na topologia e clicar em **Definir como nó raiz** na lista suspensa para definir o nó como o nó raiz.

Observação

Somente o switch, a ponte de rede sem fio e o conversor de fibra podem ser definidos como nó raiz.

Aumentar/diminuir o zoom

Clique em ou para ampliar ou reduzir o(s) nó(s) do dispositivo e o(s) nó(s) do dispositivo subsidiário(s). Você pode rolar a roda do mouse para ampliar ou reduzir a topologia.

Ajustar Topologia

Clique no plano de fundo da topologia para movê-la para cima, para baixo, para a direita ou para a esquerda.

Tela cheia

Clique no canto superior direito da topologia para exibi-la em modo de tela cheia.

Visão adaptável

Clique no canto superior direito da topologia para adaptá-la à janela atual, para ajudar você a conhecer toda a hierarquia da topologia rapidamente.

Procurar

Ao inserir o nome do dispositivo ou o endereço IP na caixa de pesquisa, você pode localizar rapidamente o dispositivo na topologia.

21.1.3 Visão Geral de Dados Históricos de Saúde

Você pode visualizar a taxa histórica on-line de recursos e dispositivos ou a taxa de integridade da

gravação.

Na área Visão geral da saúde, selecione **Visão geral do histórico** .

Figura 21-9 Visão geral dos dados históricos de saúde

Tabela 21-3 Página de dados históricos de saúde

Seção	Descrição
Selecione o site	No canto superior esquerdo da página Visão geral do histórico, selecione um Site atual ou remoto na lista suspensa para exibir os dados históricos dos recursos no Site.
Filtrar dados	Selecione um período de tempo na lista suspensa no canto superior direito de cada seção para filtrar dados por dia, semana ou mês.
Taxa de recursos on-line	● No gráfico de linhas, você pode executar as seguintes operações: ○ Mova o cursor no gráfico de linhas para visualizar a taxa de câmeras online e o número de câmeras offline em pontos de tempo específicos. ○ Clique no ponto a na linha para ir para a página Log de Recursos e visualizar o status detalhado da rede das câmeras naquele momento. ● No gráfico de rosca, você pode executar as seguintes operações: ○ Mova o cursor para a parte vermelha do gráfico de rosca para visualizar o número de câmeras que estavam offline e a taxa de offline durante o período de tempo selecionado. ○ Mova o cursor para a parte verde do gráfico de rosca para visualizar o número de câmeras que permanecem online e

Seção	Descrição
	a taxa online durante o período de tempo selecionado. ● Na mesa, você pode fazer uma das seguintes ações: ○ Clique em **Duração total offline** para classificar as câmeras em termos de duração total offline dentro do período de tempo selecionado. ○ Clique **em Tempos offline** para classificar as câmeras em termos de tempo offline dentro do período de tempo selecionado.
Taxa de dispositivo on-line	● No gráfico de linhas, você pode fazer uma das seguintes ações. ○ Mova o cursor no gráfico de linhas para visualizar a taxa de dispositivos on-line e o número de dispositivos off-line em pontos de tempo específicos. ○ Clique no ponto a na linha para ir para a página Log do dispositivo e visualizar o status detalhado da rede dos dispositivos naquele momento. ● No gráfico de rosca, você pode realizar as seguintes operações. ○ Mova o cursor para a parte vermelha do gráfico de rosca para visualizar o número de dispositivos que estavam offline e a taxa de offline durante o período de tempo selecionado. ○ Mova o cursor para a parte verde do gráfico de rosca para visualizar o número de dispositivos que permanecem online e a taxa online durante o período de tempo selecionado. ● Na mesa, você pode fazer uma das seguintes coisas. ○ Clique em **Duração total offline** para classificar os dispositivos em termos de duração total offline dentro do período de tempo selecionado. ○ Clique em **Tempos offline** para classificar os dispositivos em termos de tempo offline dentro do período de tempo selecionado.
Taxa de integridade de gravação	Para obter a taxa de integridade da gravação, divida a duração total do vídeo pela duração da gravação programada e multiplique o resultado por 100%. No gráfico de linhas, você pode mover o cursor para visualizar a taxa de integridade da gravação em pontos de tempo específicos. Clique no ponto a na linha para ir para a página Resource Log para visualizar o status detalhado dos recursos dos dispositivos naquele ponto de tempo.

Seção	Descrição
Taxa de cópia de gravação	No gráfico de linhas, você pode mover o cursor para visualizar a taxa de retorno de chamada de gravação em pontos de tempo específicos. Clique em um ponto na linha para ir para a página Resource Log para visualizar o status detalhado do recurso dos dispositivos naquele ponto de tempo.
Atualizar	● Atualizar manualmente: clique em **Atualizar** no canto superior direito da página Visão geral do histórico para atualizar manualmente os dados na página. ● Atualização Automática: **Gerenciamento** → **Sistema** → **Monitoramento de Saúde** para definir o intervalo para atualização automática dos dados na página. Veja os detalhes em ***Definir Frequência de Verificação de Saúde*** .
Página de Visão Geral de Exportação ou Dados de Exceção	Clique em **Exportar** no canto superior direito da página Visão geral do histórico para exportar a página em formato PDF. Ou você pode marcar **Exportar dados de exceção** para exportar os dados de exceção em formato Excel/CSV.  **Figura 21-10 Página de Visão Geral de Exportação ou Dados de Exceção**

21.2 Verificação de Saúde

Para controlar o status de saúde dos recursos na plataforma, você pode executar uma verificação de saúde manual para escanear rapidamente a plataforma em busca de riscos potenciais por diferentes tipos de verificação, cujos itens de verificação podem ser configurados. Para problemas encontrados durante a verificação de saúde, você pode adicioná-los como tarefas pendentes para tratamento posterior. Você também pode personalizar tarefas pendentes de acordo com a necessidade real.

Na página inicial, selecione **Manutenção** → **Verificação de integridade** ou selecione → **Todos**

os módulos → Manutenção → Verificação de integridade .

21.2.1 Executar Verificação Manual

Você pode iniciar manualmente a verificação de integridade para escanear rapidamente a plataforma em busca de riscos potenciais e configurar itens de verificação para diferentes tipos de verificação.
Selecione **Verificação manual** à esquerda.

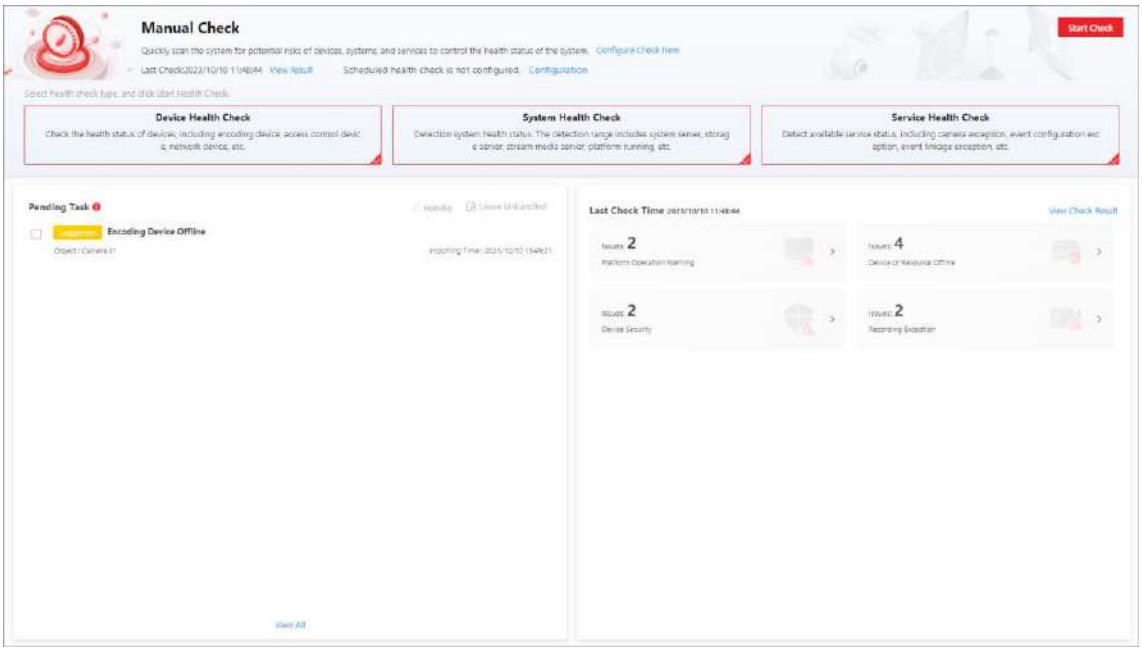


Figura 21-11 Página de verificação manual

Nesta página, você pode realizar as seguintes operações.

- ***Iniciar verificação de integridade manualmente***
- ***Configurar itens de verificação***
- ***Gerenciar tarefas pendentes***
- ***Ver os últimos resultados da verificação***

Iniciar verificação de integridade manualmente

Clique em **Verificação de integridade do dispositivo** , **Verificação de integridade do sistema** ou **Verificação de integridade do serviço** na parte superior da página Verificação de integridade para selecionar os tipos a serem verificados e, em seguida, clique em **Iniciar verificação de integridade** no canto superior direito para entrar na página Verificação.

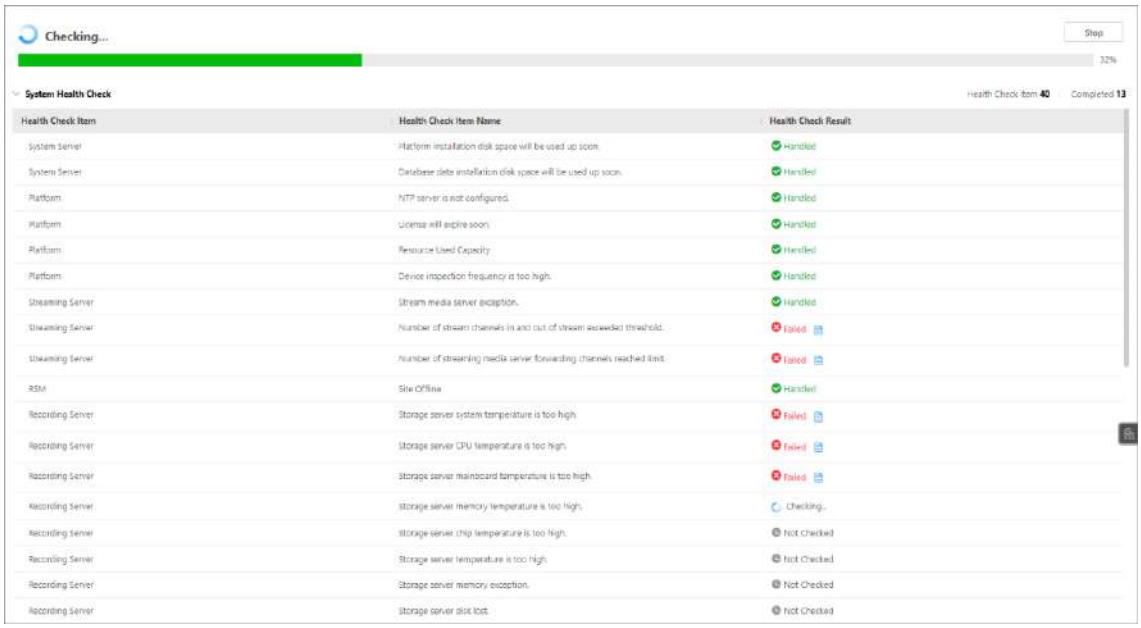


Figura 21-12 Verificando a página

Durante a verificação de saúde, você pode visualizar a porcentagem de progresso, itens de verificação em tempo real e resultado. Para itens com falha, você pode clicar na coluna Resultado da verificação de saúde para visualizar os detalhes da falha. Você também pode clicar em **Parar** no canto superior direito para cancelar a verificação de saúde.

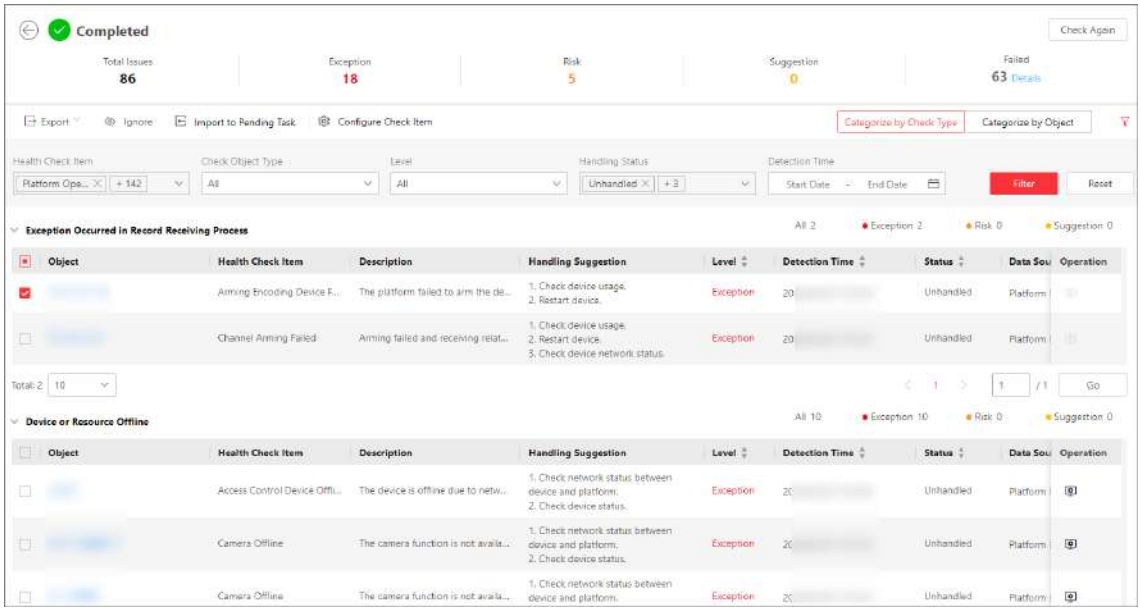


Figura 21-13 Página concluída

Quando a verificação de integridade estiver concluída, você poderá executar as seguintes operações.

- Veja o número total de problemas, exceções, riscos, sugestões e itens com falha ou clique em **Detalhes** ao lado do número de itens com falha para ver os detalhes do item com falha.
- Clique em **Configurar Item de Verificação** para visualizar a lista de itens de verificação de

integridade e itens de verificação ignorados. Para mais operações na página Lista de Itens de Verificação de Integridade, consulte ***Configurar Itens de Verificação*** .

- Clique em **Categorize by Check Type** ou **Categorize by Object** no topo da lista de problemas para exibir e calcular problemas por tipo de verificação de integridade ou objeto. Você pode clicar na frente de um nome de categoria para desdobrá-la e ver mais detalhes.
- Clique no canto superior direito da lista de problemas para abrir o painel de filtro e definir condições para filtrar os problemas.
- Mova o cursor sobre o botão **Exportar** e clique em **Exportar tudo** para exportar todos os problemas para o PC local.
- Verifique o(s) problema(s) na lista e clique em **Exportar** na parte superior da lista para exportar o(s) problema(s) selecionado(s) para o PC local.
- Verifique o(s) problema(s) na lista e clique em **Importar para Tarefa Pendente** para mover o(s) problema(s) selecionado(s) para a tarefa pendente para gerenciamento posterior. Consulte ***Gerenciar Tarefas Pendentes*** para obter detalhes.
- Clique no nome do objeto para visualizar os detalhes e informações do dispositivo e clique para ir para a página de configuração do dispositivo.
- Verifique o(s) problema(s) na lista e clique em **Ignorar** para ignorar os problemas selecionados.
- Clique em **Verificar novamente** para iniciar a verificação de integridade novamente.

Observação

Se você quiser iniciar a verificação de integridade regularmente, clique em **Configurar** na parte superior da página Verificação Manual para habilitar a verificação de integridade agendada. Para operações detalhadas, consulte ***Configurar Verificação de integridade agendada*** .

Configurar itens de verificação

Na parte superior da página Verificação manual, clique em **Configurar item de verificação** para entrar na página Lista de itens de verificação de integridade.

- Na guia **Configurar item de verificação**
  - Clique na frente do nome da categoria para exibir os itens de verificação disponíveis.
  - Clique na coluna Operation de um item que não seja ignorado e selecione o objeto para entrar em vigor. Uma vez que o item de verificação for ignorado, os problemas do objeto selecionado verificado por este item não serão relatados.
- Na guia **Item de verificação ignorado**
  - Clique em **Categorizar por tipo de verificação** ou **Categorizar por objeto** para exibir os itens de verificação ignorados por tipo de verificação ou objeto.
  - Marque os itens ignorados e clique em **Restaurar** para cancelar a opção de ignorá-los.

Gerenciar tarefas pendentes

Na seção Tarefa Pendente, os problemas importados para a tarefa pendente serão listados.
Clique no nome de uma tarefa pendente para editar seu nome, nível, notas e configurações de notificação por e-mail no painel direito.
Mova o cursor sobre uma tarefa pendente e clique em **Gerenciar** ou **Deixar sem tratamento** para gerenciar uma única tarefa.

Verifique as tarefas pendentes e clique em **Gerenciar** ou **Deixar sem tratamento** no canto superior direito da seção para processar em lote as tarefas selecionadas.
As tarefas pendentes manipuladas desaparecerão da seção Pending Task e serão exibidas na página Maintenance Log. Para obter detalhes, consulte ***Search for Maintenance Logs*** .
Clique em **View All** na parte inferior desta seção para entrar na página Pending Task. Para obter detalhes, consulte ***Add Custom Pending Tasks*** .

Ver os últimos resultados da verificação

Na seção Última hora de verificação, a última hora de verificação e a visão geral do problema correspondente serão exibidas.
Clique > em uma categoria de problema para entrar na página Resultado da verificação de integridade e localizar a lista de detalhes correspondente.
Clique em **Exibir resultado da verificação** no canto superior direito da seção Última hora da verificação ou clique em **Exibir resultado** na parte superior da página Verificação manual para entrar na página Resultado da verificação de integridade.

21.2.2 Adicionar Tarefas Pendentes Personalizadas

A página Tarefa Pendente lista as tarefas pendentes personalizadas, além das tarefas pendentes importadas da página Verificação Manual. Você pode adicionar tarefas pendentes personalizadas para acomodar suas necessidades, manipular, ignorar, excluir e exportar tarefas pendentes e notificações de conjuntos em lote. Esta seção o guiará pela adição de tarefas pendentes personalizadas.

Passos

1. Selecione **Tarefa Pendente** à esquerda.
2. Selecione **Adicionar tarefa pendente personalizada** . Esta parte apresentará parâmetros-chave.

Nível

Selecione um dos três níveis a seguir:

- **Exceção** : refere-se a um erro ou a uma situação excepcional. Por exemplo, se um dispositivo ficar offline devido a problemas de rede, seria considerado uma exceção.
- **Risco** : refere-se ao comprometimento potencial de uma função ou sistema devido a certos fatores. Por exemplo, se você definir uma senha fraca, as informações do dispositivo correm o risco de vazar.
- **Sugestão** : Refere-se a uma recomendação ou conselho que melhora o desempenho ou a funcionalidade de um sistema. Por exemplo, configurar o servidor NTP ou ajustar a frequência de inspeção do dispositivo são sugestões para melhorar o desempenho do sistema.

Notificação por e-mail

Para receber e-mails de notificações de tarefas pendentes em um horário agendado, ative **Notificação por e-mail** . Você pode adicionar um novo modelo de e-mail ou selecionar um modelo de e-mail para definir as informações e o conteúdo do destinatário.

3. Clique em **OK** para salvar as configurações.

4. Opcional: Após adicionar tarefas pendentes, você pode editá-las, manipulá-las, deixá-las sem manipulação, excluí-las, definir notificações em lote, desabilitar notificações em lote, exportar essas tarefas, filtrá-las de acordo com várias condições, definir a largura da coluna adaptável e personalizar itens da coluna.

21.2.3 Configurar Verificação de Integridade Agendada

Você pode configurar uma verificação de integridade agendada para detectar e resolver proativamente possíveis problemas e manter a estabilidade e a confiabilidade dos seus dispositivos, serviços e sistemas.

Antes de começar

- Você definiu um modelo de e-mail com informações do destinatário, assunto e conteúdo.
- Você configurou as configurações de e-mail, como endereço do remetente, endereço do servidor SMTP e porta.

Passos

1. Selecione **Verificação manual** à esquerda para abrir a página Verificação manual.
2. Na parte superior, clique em **Configurar** para entrar na página Verificação de integridade agendada.
3. Ative **a Verificação de integridade agendada** .
4. Selecione **Item de verificação de integridade** .

   Verificação de integridade do dispositivo

   Os itens de verificação do dispositivo incluem senha, exceção de gravação, temperatura do HDD e incompatibilidade de resolução.

   Verificação de integridade do sistema

   Os itens de verificação do sistema incluem espaço em disco, frequência de inspeção do dispositivo e temperatura da CPU do servidor de armazenamento.

   Verificação de saúde do serviço

   Os itens de verificação de serviço incluem o tempo limite de operação e a perda de vídeo.
5. Defina o período de verificação de integridade.

Observação

Você pode agendar verificações de saúde diariamente, semanalmente ou mensalmente. Para uma verificação de saúde automática no último dia de cada mês, defina o período de verificação de saúde como Por mês e o horário da verificação de saúde como Último dia. Evite definir o horário da verificação de saúde como 31 para meses com menos de 31 dias.

6. Configure as configurações avançadas. Esta parte apresentará os parâmetros-chave.

   Importação automática de resultados para tarefa pendente

   Se você ativar **a Importação Automática de Resultados para Tarefa Pendente** e marcar a opção **Substituir Pendentes Duplicados** , a nova tarefa pendente substituirá

automaticamente a antiga quando os itens marcados e os objetos das tarefas pendentes forem os mesmos.

Exportar automaticamente os resultados como relatório

Ative para enviar ou salvar os relatórios de verificação de integridade.

Enviar relatório por e-mail

Se você tiver ativado **Enviar Relatório por Email** , selecione um modelo de email para definir as informações e o conteúdo do destinatário. Você pode clicar em **Adicionar** para adicionar um novo modelo de email.

Carregar para SFTP

Para garantir uma transferência de arquivos segura, confiável e eficiente, carregue o relatório no SFTP.

Observação

Você pode clicar em **Configurar** para definir o SFTP.

7. Clique em **Salvar** .

21.3 Status do Recurso

Você pode monitorar o status dos recursos adicionados, como dispositivos de controle de acesso e servidores de gravação, o que ajuda a descobrir e manter os recursos anormais a tempo, garantindo o bom funcionamento da plataforma ao máximo.
Na página inicial, selecione **Manutenção** → **Status do recurso** ou selecione → **Todos os módulos** → **Manutenção** → **Status do recurso** .
Selecione um tipo de recurso para executar as seguintes operações.

Operações comuns

Operação	Descrição
Filtrar status do recurso	Marque a caixa de seleção no canto superior direito da página de exibição de status para selecionar os tipos de exceção na lista suspensa para filtrar o status do recurso.
Exibir status do dispositivo	Clique no nome do dispositivo para visualizar os detalhes de status e informações básicas do dispositivo.
Configurar dispositivo	Clique na coluna Operação para ir para a página Área e configurar os parâmetros do dispositivo especificado.
Dispositivo de filtro	Selecione o(s) tipo(s) de dispositivo na primeira lista suspensa na parte superior para filtrar o status do dispositivo por tipo de dispositivo.
Exportar dados de	Clique em **Exportar** para exportar os dados de status como CSV ou Excel

Operação	Descrição
status	para o PC local.
Atualizar status do recurso	Clique na coluna Operação para atualizar o status do recurso especificado ou clique em **Atualizar** para atualizar o status de todos os recursos exibidos na página. **Observação** O status do recurso será atualizado automaticamente em um intervalo especificado.
Editar Valor Atual	Clique na coluna Valor atual para editar o valor atual do dispositivo.

Status da câmera

Operação	Descrição
Ver status da câmera relacionada	Clique no endereço IP para visualizar o status do dispositivo ao qual a câmera está relacionada.
Ver registros online/offline	Clique na coluna Operação para visualizar os registros online/offline da câmera especificada. **Observação** Esta operação não está disponível para câmeras adicionadas em Sites Remotos.
Ver o status da gravação	Clique na coluna Operação para visualizar o status de gravação da câmera. **Observação** Esta operação não está disponível para câmeras adicionadas em Sites Remotos.
Ver câmera com imagem anormal	Clique em **View Camera with Abnormal Image** para visualizar os vídeos de câmeras com imagens anormais. E você também pode exportar os resultados do diagnóstico de imagem de câmeras selecionadas ou de todas as câmeras em formato PDF.

Status da porta

Operação	Descrição
Status da porta de controle	Clique na coluna Operação e selecione um tipo de controle na lista suspensa para controlar o status da porta. ● **Desbloquear** : Quando a porta estiver trancada, destranque a porta e ela será aberta. Após a duração aberta (configurada via Web Client), a porta será fechada e trancada novamente automaticamente. ● **Lock** : Quando a porta estiver destrancada, tranque a porta e ela será fechada. A pessoa que tem permissão de acesso pode acessar a porta com credenciais. ● **Permanecer destrancado** : A porta será destrancada (não importa se fechada ou aberta). Todas as pessoas podem acessar a porta sem credenciais necessárias (acesso livre). **Observação** Para a porta vinculada ao dispositivo de interfone com vídeo, não está disponível a configuração de seu status para permanecer destrancada. ● **Permanecer Trancado** : A porta será fechada e trancada. Nenhuma pessoa pode acessar a porta mesmo que tenha as credenciais autorizadas, exceto o usuário com permissão de super acesso.
Ignorar status do dispositivo	Clique na parte superior para ignorar o status do leitor de cartão RS-485.

Status do site remoto

Operação	Descrição
Modo de acesso de comutação	Clique em ou na coluna Operação para alternar o modo de acesso aos recursos no Site Remoto entre o modo **Julgamento Automático** e o modo **Proxy** . ● **Julgamento automático** : o sistema julgará automaticamente a condição da conexão de rede e, em seguida, definirá o modo de acesso do dispositivo de acordo, como acesso direto ou acesso via Streaming Gateway e Management Service. ● **Proxy** : O sistema acessará o dispositivo via Streaming Gateway e Management Service.
Restaurar modo de	Clique em **Restaurar todas as conexões de rede** para restaurar o modo de conexão de todos os recursos do site remoto adicionado

Operação	Descrição
conexão	para o modo **Julgar automaticamente** .
Mudar tipo de fluxo	Selecione o(s) Remote Site(s) e clique em **Switch Stream** para alternar o tipo de stream. Ao iniciar a visualização ao vivo dos recursos do Remote Site no Central System, o Control Client obterá esse stream padrão para iniciar a visualização ao vivo. ● **Main Stream:** O Main Stream fornece vídeo de maior qualidade e resolução, mas acarreta maior uso de largura de banda. ● **Sub-Stream:** O sub-stream pode economizar largura de banda, mas a qualidade do vídeo é inferior à do stream principal. ● **Smooth Stream:** Este tipo de fluxo é geralmente usado em situações de baixa largura de banda. Após alternar para smooth stream, a visualização ao vivo e a reprodução serão mais suaves em desempenho de rede lento, mas a qualidade da imagem será menor de acordo. ● **Tipo de fluxo padrão:** se você selecionar **Tipo de fluxo padrão** , o tipo de fluxo para acessar os recursos do Site remoto selecionado será restaurado para o tipo de fluxo global definido em **Sistema** → **Vídeo** → **Rede** .

Status do dispositivo de codificação

Operação	Descrição
Exibir detalhes do erro	Na coluna **Status do disco** , visualize os detalhes do erro se um disco estiver anormal.
Ver status de gravação dos canais	Clique no status na coluna **Status de Gravação** para visualizar o status de gravação dos canais configurados para armazenar os arquivos de vídeo neste dispositivo de codificação. Se as configurações de gravação estiverem anormais, você pode clicar em **Exceção** na coluna **Status de Gravação** para visualizar os detalhes da exceção no painel pop-up.
Câmera de energia solar Wake Up	Clique para ativar uma câmera alimentada por energia solar se ela estiver no modo de espera.
Ver registros online/offline	Clique na coluna Operação para visualizar os registros online/offline do dispositivo de codificação.
Modo de acesso de comutação	Clique em **Alternar modo de acesso do dispositivo** para alternar o modo de acesso do Control Client para acessar os dispositivos. ● **Restaurar padrão** : restaura o modo de acesso do dispositivo conforme configurado em **Sistema** → **Modo de acesso do dispositivo** no Web Client.

Operação	Descrição
	● **Julgar automaticamente** : Julgue o modo de acesso do dispositivo de acordo com a rede atual. ● **Acesso direto** : acesse o dispositivo diretamente, não pelo HikCentral Professional Streaming Service. **Observação** O modo de acesso direto está disponível quando o dispositivo de codificação e o cliente estão na mesma LAN com o servidor SYS. ● **Proxy** : Acesse o dispositivo via HikCentral Professional Streaming Gateway e HikCentral Professional Management Service. É menos eficaz e menos eficiente do que acessar diretamente.
Mudar tipo de fluxo	Selecione o(s) dispositivo(s) de codificação e clique em **Switch Stream** para alternar o tipo de fluxo. Ao iniciar a visualização ao vivo, o Control Client obterá esse fluxo padrão para iniciar a visualização ao vivo dos recursos do dispositivo de codificação. ● **Main Stream:** O Main Stream fornece vídeo de maior qualidade e resolução, mas acarreta maior uso de largura de banda. ● **Sub-Stream:** O sub-stream pode economizar largura de banda, mas a qualidade do vídeo é inferior à do stream principal. ● **Smooth Stream:** Este tipo de fluxo é geralmente usado em situações de baixa largura de banda. Após alternar para smooth stream, a visualização ao vivo e a reprodução serão mais suaves em desempenho de rede lento, mas a qualidade da imagem será menor de acordo. ● **Tipo de fluxo padrão:** se você selecionar **Tipo de fluxo padrão** , o tipo de fluxo para acessar o(s) dispositivo(s) de codificação selecionado(s) será restaurado para o tipo de fluxo global definido em **Sistema** → **Vídeo** → **Rede** .

Status do dispositivo de bordo

Operação	Descrição
Comando de Log de Depuração de Impressão	Clique na coluna Operação para imprimir o comando de log de depuração.
Exportar Logs do Dispositivo	Clique na coluna Operação para exportar logs de um dispositivo.

21.4 Pesquisa de Log

Três tipos de arquivos de log são fornecidos: logs de servidor, logs de dispositivo e logs de recurso. Os logs de servidor referem-se aos arquivos de log armazenados no servidor SYS no site atual e sites remotos; Os logs de dispositivo referem-se aos arquivos de log armazenados nos dispositivos conectados, como dispositivo de codificação e dispositivo de controle de segurança; Os logs de recurso referem-se aos logs sobre status de gravação da câmera, status online e status de retorno de chamada. Você pode pesquisar os arquivos de log, visualizar os detalhes do log e fazer backup dos arquivos de log.

21.4.1 Pesquisar Logs do Servidor

Você pode pesquisar logs de servidor do site atual ou Remote Sites, que contêm logs de erro, logs de aviso e logs de informação. Os logs de servidor contêm atividades históricas de usuário e servidor. Você pode pesquisar os logs e então verificar os detalhes.

Passos

1. Selecione **Log do sistema** → **Logs do servidor** .
2. Na área **Site** , selecione o site atual ou um Site Remoto.
3. Na área **Evento** , selecione um ou vários tipos de log e subtipos.

Observação

Os logs de erro registram falhas ou erros. Os logs de aviso registram eventos de expiração de licença. Os logs de informação referem-se a outros logs gerais que registram resultados de operações bem-sucedidas ou desconhecidas.

4. Na área **Origem** , defina a origem dos logs que você deseja pesquisar.
5. Opcional: Na área **Nome do recurso** , insira o nome de um recurso para pesquisar os logs do recurso.
6. Defina o intervalo de tempo para pesquisa.

Observação

Você pode selecionar **Personalizado** para definir uma hora de início e término precisas.

7. Clique em **Pesquisar** .
   Todos os logs correspondentes são listados com detalhes à direita.
8. Opcional: marque todos os logs ou logs específicos, clique em **Exportar** e selecione um formato de arquivo (por exemplo, Excel ou CSV) para baixar os logs pesquisados como um único arquivo para o seu PC local.

21.4.2 Pesquisar Registros On-line/Off-line do Dispositivo

Você pode pesquisar os logs online/offline de todos os dispositivos. Os logs online/offline

fornecem informações sobre o status atual do dispositivo (online ou offline), último tempo offline, duração total offline, etc.

Passos

1. Selecione **Log do sistema** → **Log do dispositivo** .
2. Em **Tipo** , selecione **Log Online/Offline** como o tipo de log.
3. Selecione um tipo de dispositivo e marque os dispositivos que deseja pesquisar.
4. Defina o intervalo de tempo para pesquisa.

Observação

Você pode selecionar **Personalizado** para definir uma hora de início e término precisas.

5. Opcional: se houver um grande número de dispositivos, ative o **Intervalo de estatísticas** para definir um intervalo de tempo total offline durante o intervalo de tempo especificado para filtrar os dispositivos ou defina uma duração total offline para filtrar os dispositivos.
6. Clique em **Pesquisar** .
   O log offline/online de cada dispositivo está listado à direita. Você pode verificar o nome, endereço IP, status atual (online/offline), último tempo offline, tempos offline totais e duração offline total de cada dispositivo.
7. Opcional: execute outras operações após pesquisar os logs do dispositivo.

Ver histórico offline	Clique no nome do dispositivo para visualizar o histórico on-line, a duração (exibido como um gráfico de linhas) e o status (exibido como uma lista) do dispositivo. Você pode executar as seguintes operações. ● Filtrar dados: selecione um período de tempo e um status (online, offline ou todos) nas listas suspensas, respectivamente, para filtrar os dados. ● Exibir detalhes: mova o cursor para o gráfico de linhas para visualizar a duração detalhada offline e online em cada ponto de tempo.
Exibir logs do dispositivo	Clique na coluna Operação para visualizar os logs armazenados no dispositivo.
Exportar Logs	Clique em **Exportar** e selecione um formato de arquivo e um tipo de relatório para baixar os logs pesquisados como um único arquivo para seu PC local.

21.4.3 Pesquisar Logs Armazenados no Dispositivo

Você pode pesquisar os logs armazenados em dispositivos de codificação, dispositivos de controle de segurança, dispositivos de decodificação, dispositivos de transmissão de rede, dispositivos de controle de acesso, dispositivos de controle de elevador, dispositivos de bordo e dispositivos de

proteção contra incêndio.

Passos

1. Selecione **Log do sistema** → **Log do dispositivo** .
2. Selecione **Log on Device** como o tipo de log.
3. Selecione um tipo de dispositivo e selecione o dispositivo que deseja pesquisar.
4. Selecione o evento principal como **Normal** ou **Informações da bateria** e marque o(s) subevento(s) a serem pesquisados.
5. Especifique o intervalo de tempo desta pesquisa.

Observação

Você pode selecionar **Intervalo de tempo personalizado** para definir um horário de início e término precisos.

6. Clique em **Pesquisar** .
   Todos os logs correspondentes são listados com detalhes à direita.
7. Opcional: execute outras operações após pesquisar os logs do dispositivo.

Ver histórico offline	Clique no nome do dispositivo para visualizar o histórico on-line, a duração (exibido como um gráfico de linhas) e o status (exibido como uma lista) do dispositivo. Você pode executar as seguintes operações. ● Filtrar dados: selecione um período de tempo e um status (online, offline ou todos) nas listas suspensas, respectivamente, para filtrar os dados. ● Exibir detalhes: mova o cursor para o gráfico de linhas para visualizar a duração detalhada offline e online em cada ponto de tempo.
Exibir logs do dispositivo	Clique na coluna Operação para visualizar os logs armazenados no dispositivo.
Exportar Logs	Clique em **Exportar** e selecione um formato de arquivo e um tipo de relatório para baixar os logs pesquisados como um único arquivo para seu PC local.

21.4.4 Pesquisar por Logs Online/Offline de Recursos

Você pode pesquisar os logs online/offline de câmeras no site atual. Os logs online/offline fornecem informações sobre o status atual do dispositivo (online ou offline), último tempo offline, duração total offline, etc.

Passos

1. Selecione **Log do sistema** → **Logs de recursos** .
2. Em **Tipo** , selecione **Log Online/Offline** .

3. Clique para mostrar a lista de áreas no site atual e então selecione as câmeras cujos registros devem ser pesquisados.
4. Opcional: modifique sua seleção na lista de câmeras selecionadas.

Remover uma câmera	Clique para remover a câmera da lista.
Remover todas as câmeras	Clique para remover todas as câmeras da lista.

5. Em **Tempo** , especifique o intervalo de tempo desta pesquisa.

Observação

Você pode selecionar **Intervalo de tempo personalizado** para definir um horário de início e término precisos.

6. Opcional: se houver um grande número de dispositivos, ative **o Tempo de filtragem** para definir um intervalo de tempo total offline durante o intervalo de tempo especificado para filtrar os dispositivos ou defina uma duração total offline para filtrar os dispositivos.
7. Clique em **Pesquisar** .
   O log offline/online de cada recurso é listado à direita. Você pode visualizar o nome, endereço IP, status atual (online/offline), último tempo offline, tempos offline totais e duração offline total de cada recurso.
8. Opcional: execute outras operações após pesquisar nos logs de recursos.

Ver histórico offline	Clique no nome do recurso para visualizar o histórico on-line, a duração (exibido como um gráfico de linhas) e o status (exibido como uma lista) do recurso. Você pode executar as seguintes operações. ● Filtrar dados: selecione um período de tempo e um status (online, offline ou todos) nas listas suspensas, respectivamente, para filtrar os dados. ● Exibir detalhes: mova o cursor para o gráfico de linhas para visualizar a duração detalhada offline e online em cada ponto de tempo.
Exibir registros do dispositivo on-line/off-line	Clique no endereço IP para visualizar os logs online/offline do dispositivo onde o recurso está vinculado.
Exportar Logs	Clique em **Exportar** e selecione um formato de arquivo e um tipo de relatório para baixar os logs pesquisados como um único arquivo para seu PC local.

21.4.5 Pesquisar Status de Gravação do Recurso

Você pode pesquisar o status de gravação de câmeras no site atual. O status de gravação inclui a

taxa de integridade da gravação, duração total da gravação anormal, tempos de interrupções de gravação, etc.

Passos

1. Selecione **Log do sistema** → **Logs de recursos** .
2. Em **Tipo** , selecione **Status da gravação** .
3. Clique para mostrar a lista de áreas do site atual e então selecione as câmeras cujos registros devem ser pesquisados.
4. Opcional: modifique sua seleção na lista de câmeras selecionadas.

Remover uma câmera	Clique e depois clique para remover uma câmera da lista.
Remover todas as câmeras	Clique e depois clique para remover todas as câmeras da lista.

5. Em **Tempo** , especifique o intervalo de tempo desta pesquisa.

Observação

Você pode selecionar **Intervalo de tempo personalizado** para definir um horário de início e término precisos.

6. Opcional: se houver um grande número de recursos, marque **Condição do filtro** e defina as condições do filtro.

Duração da retenção (dias)

Defina um intervalo de duração de retenção da filmagem gravada para filtrar as câmeras.

Taxa de integridade de gravação

Defina um intervalo da taxa de integridade de gravação para filtrar câmeras. A taxa de integridade de gravação se refere à porcentagem obtida da divisão da duração real da gravação pelo tempo de gravação agendado.

Observação

Para obter detalhes sobre o cronograma de gravação, consulte o *Manual do usuário do HikCentral Professional Web Client* .

7. Clique em **Pesquisar** .
O status de gravação de cada câmera é listado à direita, incluindo nome da câmera, endereço IP da câmera, área onde a câmera pertence, tipo de armazenamento de vídeo, etc.

Hora de início

O momento em que a câmera começou a gravar.

Fim dos tempos

A última hora em que a câmera estava gravando.

Duração da retenção (dias)

A duração da retenção (unidade: dia) da filmagem gravada refere-se à duração entre a **Hora de Início** e **a Hora de Término** .

Comprimento total

O tempo total de armazenamento do vídeo.

Comprimento total anormal

A duração total da perda do vídeo dentro do tempo programado.

Interrupção de gravação

O total de vezes de interrupção da gravação dentro do tempo programado.

8. Opcional: Verifique o status da gravação histórica.
   1) Opcional: clique em **Regra** no canto superior direito para visualizar as regras analíticas para vídeos históricos.

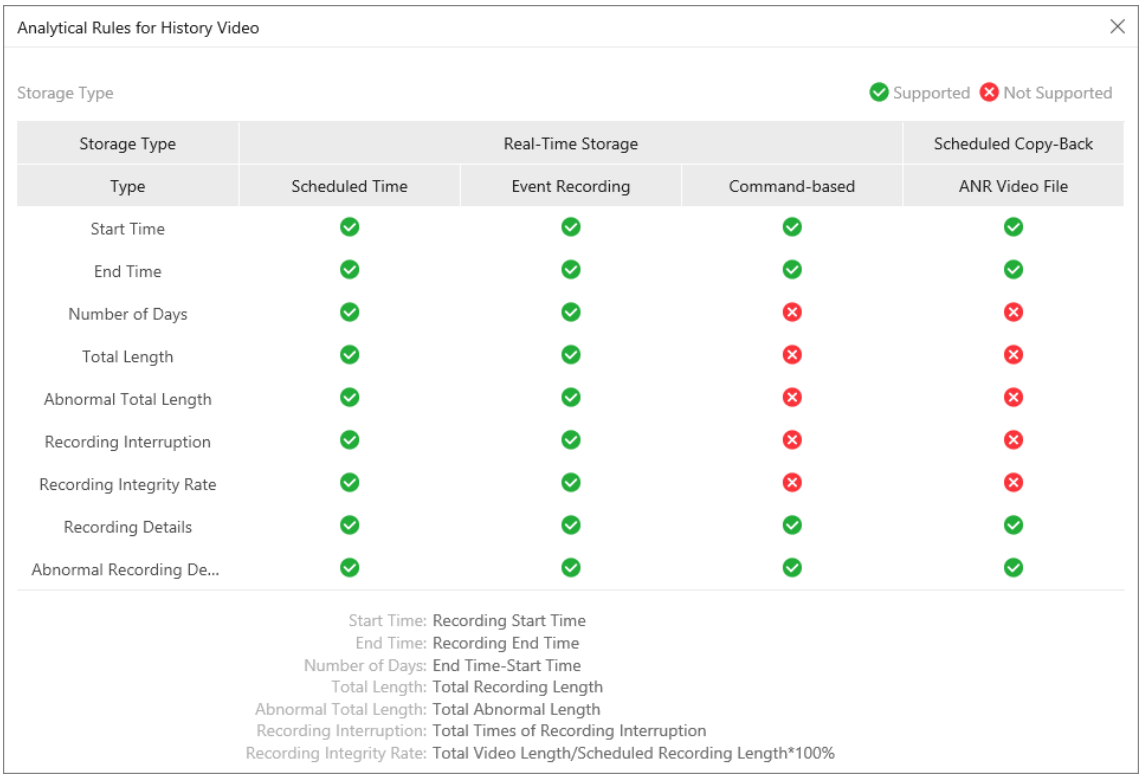


Figura 21-14 Regras analíticas para o vídeo de história

   2) Clique no nome de uma câmera para abrir o painel Status de gravação do histórico.

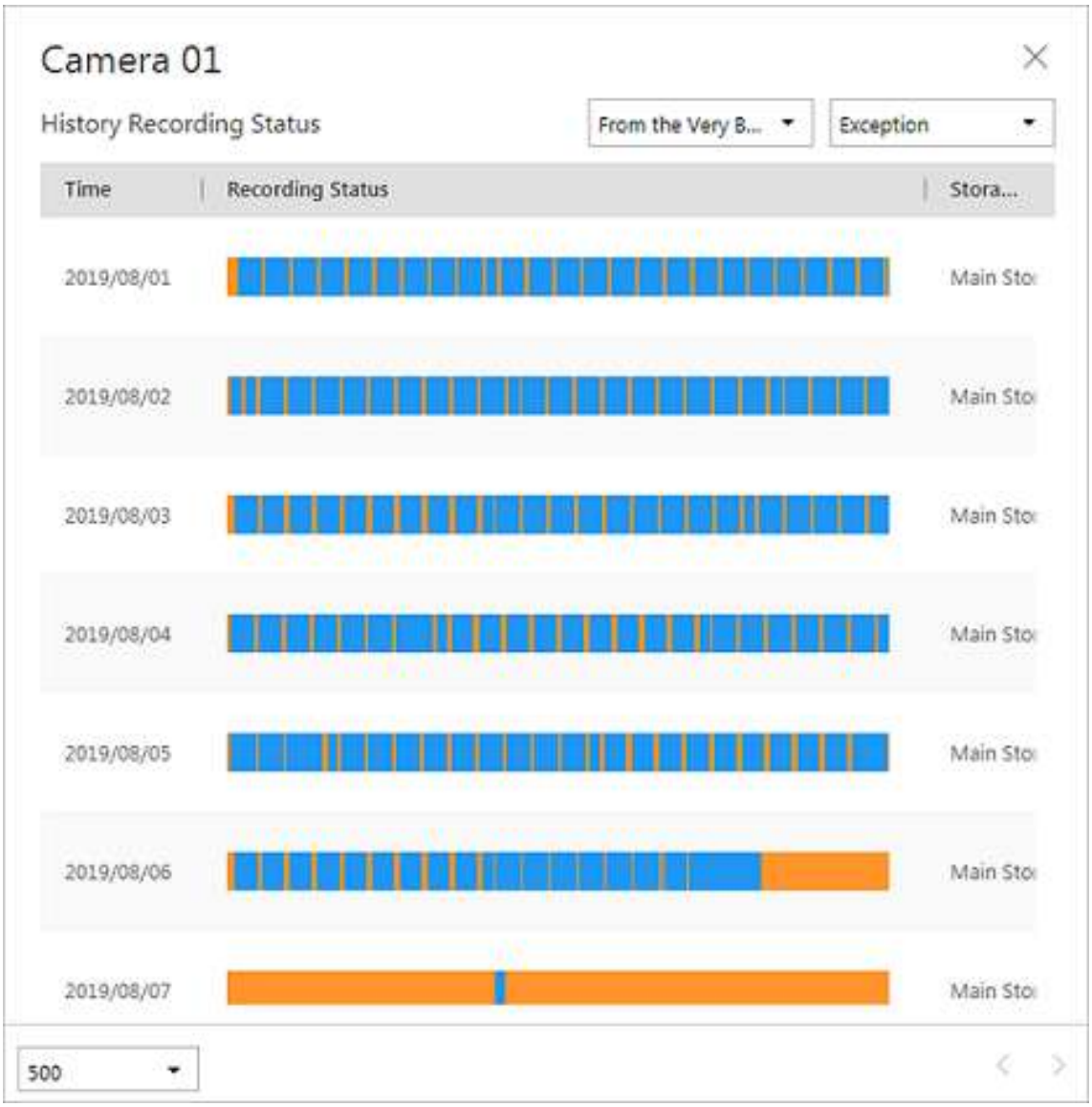


Figura 21-15 Status de gravação do histórico

Observação

As partes azuis nas barras de tempo representam os períodos de tempo durante os quais as filmagens de vídeo foram gravadas. As partes laranja nas barras de tempo representam os períodos de tempo durante os quais a perda de vídeo ocorreu ou os períodos de tempo durante os quais não havia programação de gravação.

3) Selecione um período de tempo e um status (anormal ou todos) nas listas suspensas, respectivamente, para filtrar os dados.
4) Opcional: selecione o número de registros exibidos em cada página do painel Status de gravação do histórico na lista suspensa no canto inferior esquerdo do painel.
5) Opcional: mova o cursor para a barra de tempo para mostrar as 24 horas e clique em uma hora para ver os detalhes do status da gravação dentro da hora.

9. Opcional: clique em **Exportar** e selecione um formato de arquivo e um tipo de relatório para baixar os logs pesquisados como um único arquivo para seu PC local.

21.4.6 Pesquisar Status de Retorno de Chamada do Recurso

Você pode pesquisar o status de retorno de chamada de câmeras no site atual. Nos resultados da pesquisa, você pode visualizar o nome da câmera, tipo de armazenamento, taxa de cópia de retorno de gravação, etc.

Passos

1. Selecione **Log do sistema** → **Logs de recursos** .
2. Em **Tipo** , selecione **Status de retorno de chamada** .
3. Clique para mostrar a lista de áreas do site atual e então selecione as câmeras cujos registros devem ser pesquisados.
4. Opcional: modifique sua seleção na lista de câmeras selecionadas.

Remover uma câmera	Clique e depois clique para remover uma câmera da lista.
Remover todas as câmeras	Clique e depois clique para remover todas as câmeras da lista.

5. Em **Tempo** , especifique o intervalo de tempo desta pesquisa.

Observação

Você pode selecionar **Intervalo de tempo personalizado** para definir um horário de início e término precisos.

6. Clique em **Pesquisar** .
   O status de retorno de cada câmera é listado à direita.
7. Opcional: clique em **Exportar** e selecione um formato de arquivo (por exemplo, Excel ou CSV) para baixar o status de retorno de chamada para o seu PC local.

21.4.7 Pesquisar por Logs de Manutenção

Os logs de manutenção servem como referência para solução de problemas e análise do histórico de eventos de manutenção para melhorar a eficiência e a confiabilidade. Você pode pesquisar logs de manutenção com base no manipulador, tempo de manuseio, status de manuseio e outras condições.

Passos

1. Na barra de navegação, selecione → **Gerenciamento básico** → **Manutenção** → **Log do sistema** .
2. Selecione **Registro de manutenção** à esquerda.

3. Edite os parâmetros de pesquisa, a saber, o nome da tarefa pendente, objeto, nível, manipulador, tempo de manipulação e status de manipulação. Esta parte apresentará os parâmetros-chave.

   Objeto

   Os objetos que estão passando pela verificação de integridade.

   Nível

   Selecione um dos três níveis a seguir:
   - Exceção: Refere-se a um erro ou a uma situação excepcional. Por exemplo, se um dispositivo ficar offline devido a problemas de rede, seria considerado uma exceção.
   - Risco: Refere-se ao comprometimento potencial de uma função ou sistema devido a certos fatores. Por exemplo, se você definir uma senha fraca, as informações do dispositivo correm o risco de vazar.
   - Sugestão: Refere-se a uma recomendação ou conselho que melhora o desempenho ou a funcionalidade de um sistema. Por exemplo, configurar o servidor NTP ou ajustar a frequência de inspeção do dispositivo são sugestões para melhorar o desempenho do sistema.
4. Clique em **Pesquisar** .
   Todos os logs correspondentes são listados com detalhes à direita.
5. Opcional: selecione logs específicos, clique em **Exportar** ou clique em **Exportar** → **Exportar tudo** no menu suspenso no canto superior direito da página e selecione um formato de arquivo (Excel ou CSV) para baixar os logs pesquisados como um único arquivo para seu PC local.

Capítulo 22 Ferramentas

22.1 Iniciar Uma Chamada

Após configurar as soluções de emergência, você pode iniciar uma chamada para verificar se todo o pessoal foi evacuado com segurança de uma área perigosa ou está presente no ponto de reunião designado. Durante emergências, é essencial gerenciar informações de forma eficaz. A chamada fornece uma maneira sistemática de reunir e retransmitir informações sobre o paradeiro dos indivíduos.

Siga os seguintes passos para iniciar uma chamada.

1. Na parte superior do Control Client, selecione **Ferramenta** → **Chamada** → **Selecionar área para acionar emergência** .
2. Veja as informações detalhadas de pessoal de todas as áreas selecionadas para garantir a segurança e a responsabilização de todos os indivíduos.
3. (Opcional) Clique em um cartão para visualizar informações pessoais detalhadas de uma única área, incluindo informações gerais, foto do perfil, nome, número de telefone e status.

Observação

Clique para fazer o check-in de uma pessoa que aparece no ponto de concentração, mas o status da pessoa não é Check-in no ponto de concentração.

4. (Opcional) Você pode executar as seguintes operações conforme necessário.

Operação	Descrição
Acabar com o estado de emergência.	● Selecione **Desligar emergência de todas as áreas** para encerrar o status de emergência de todas as áreas. ● Selecione **Turn Off Emergency** para encerrar o status de emergência da área selecionada. Antes de editar a solução de emergência, encerre o status de emergência.
Selecione os status das pessoas.	Selecione **Definir tipo de estatística** no canto superior direito.
Enviar relatório de reunião de emergência.	Selecione **Enviar relatório** para selecionar áreas/grupos, definir regras de classificação, selecionar o modo de exportação de relatório e confirmar sua senha.

22.2 Vídeo Porteiro

O sistema suporta funções de intercomunicação de vídeo. Intercomunicação de vídeo é uma

técnica de comunicação audiovisual e segurança usada em um edifício ou uma pequena coleção de edifícios. Com microfones e dispositivos de câmera de vídeo em ambos os lados, ele permite a intercomunicação por meio de sinais de vídeo e áudio.
Após adicionar o dispositivo e a pessoa ao sistema e configurar os parâmetros relacionados, o operador pode verificar os eventos e alarmes em tempo real, visualizar o vídeo ao vivo das câmeras relacionadas, controlar o status da porta (como manter a porta trancada), chamar a estação interna e atender chamadas, etc.

22.2.1 Status da Porta de Controle na Visualização ao Vivo

Para dispositivo de interfone de vídeo, você pode visualizar o vídeo ao vivo das câmeras relacionadas à sua porta. Durante a visualização ao vivo, você pode controlar o status da porta, se necessário, e visualizar os eventos de acesso em tempo real.

Passos

1. No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Monitoramento** → **Monitoramento** para entrar na página Monitoramento.
2. Clique em **Visualização ao vivo** na parte superior para entrar na página de visualização ao vivo.
3. Arraste a porta para a janela de exibição ou clique duas vezes no nome da porta depois de selecionar a janela de exibição.
   Se a porta estiver relacionada com câmera(s), a visualização ao vivo dessas câmeras será exibida. Se duas câmeras estiverem relacionadas, o vídeo ao vivo será exibido no modo Picture-in-Picture, o que significa que uma está na parte inferior esquerda da outra.
   Se a porta não estiver relacionada a nenhuma câmera, o status da porta será exibido na janela de exibição.
   O registro de acesso se sobreporá à janela de exibição em tempo real, caso ocorra um evento de acesso.

   Observação

   Para relacionar câmeras com porta, consulte o *Manual do Usuário do HikCentral Professional Web Client* .

4. Opcional: No modo Picture-in-Picture, clique na visualização de vídeo menor para alternar a posição de visualização das duas câmeras.

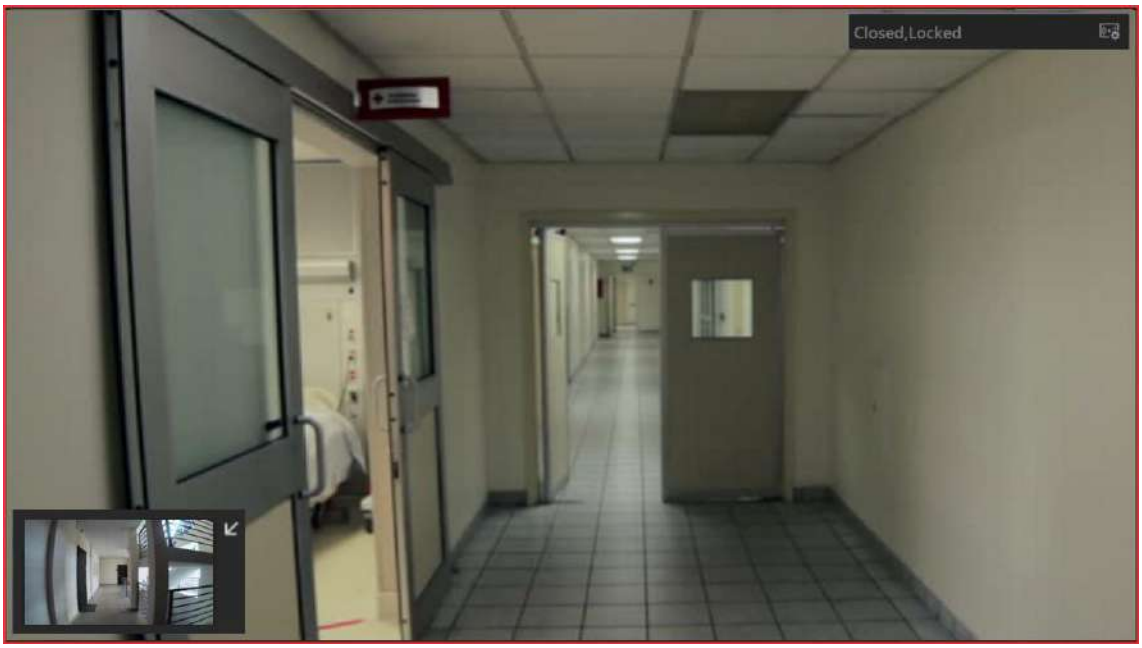


Figura 22-1 Modo Picture-in-Picture

5. Clique nos ícones no meio da janela ou clique no canto superior direito da janela para alternar o status da porta entre **Destrancada** , **Trancada** e **Permanecer destrancada** .

Desbloquear

Quando a porta estiver trancada, destranque-a e ela será aberta. Após o período de porta aberta, a porta será fechada e trancada novamente automaticamente.

Observação

Para definir a duração da abertura da porta, consulte o *Manual do Usuário do HikCentral Professional Web Client* .

Trancar

Quando a porta estiver destrancada, tranque a porta e ela será fechada. A pessoa que tem a permissão de acesso pode acessar a porta com credenciais.

Permaneça desbloqueado

A porta estará destrancada (não importa se fechada ou aberta). Todas as pessoas podem acessar a porta sem credenciais necessárias (acesso livre).

Observação

Para definir o privilégio de superusuário de uma pessoa, consulte o *Manual do Usuário do HikCentral Professional Web Client* .

6. Opcional: Execute as seguintes operações após iniciar o vídeo ao vivo da porta.

Controle o status da porta em um lote	Clique na parte superior da área de exibição para alternar o status de todas as portas no local atual para permanecer

	trancadas/permanecer destrancadas.
Coloque a porta no mapa	Clique no canto inferior esquerdo da janela de exibição para mostrar o mapa e a localização da porta no mapa.

22.2.2 Chamada de Estação Interna

Se a pessoa estiver vinculada a uma estação interna, você pode ligar para a estação interna adicionada por meio do Control Client para iniciar uma conversa de voz com o residente, visualizar o vídeo da câmera da estação interna, etc.

Observação

Certifique-se de ter adicionado a pessoa e vinculado a ela a uma estação interna via Web Client.

1. Acesse a página do Videoporteiro de uma das duas maneiras a seguir:
   - No canto superior direito da barra de navegação superior, selecione → **Videoporteiro** .
   - No painel direito da página inicial, selecione **Ferramenta** → **Videoporteiro** .
2. Selecione um grupo de pessoas para filtrar as pessoas no grupo ou em seus subgrupos de pessoas (configurável) ou insira as palavras-chave para filtrar a pessoa ou estação interna.
3. Clique na coluna Operação para chamar a estação interna.

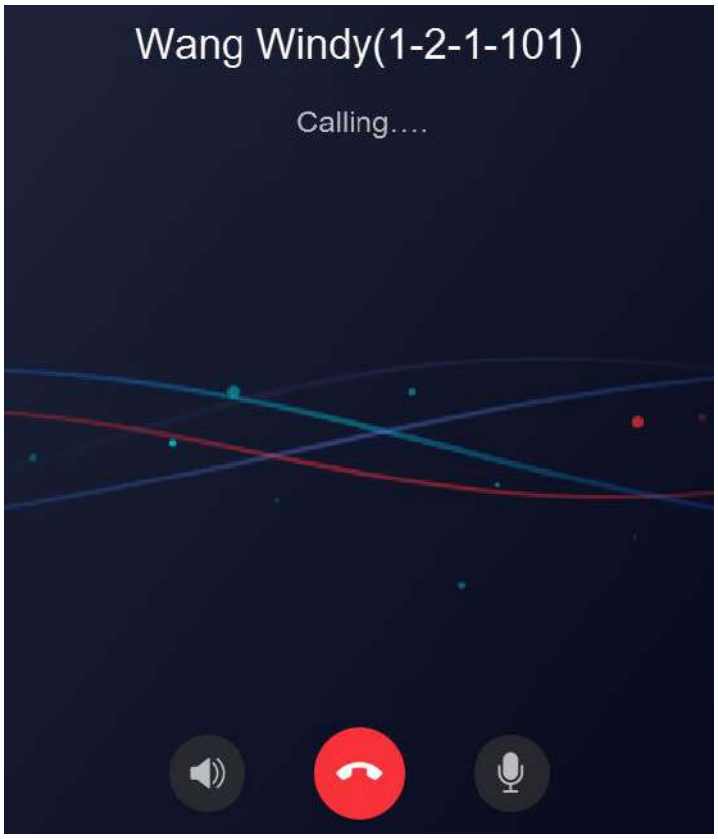


Figura 22-2 Estação interna de chamada

Depois que a chamada for atendida, você pode falar com a pessoa, assistir ao vídeo ou realizar outras operações da seguinte maneira.

- Clique para ajustar o volume do alto-falante.
- Clique para encerrar a fala.
- Clique para ajustar o volume do microfone.
- Clique para iniciar a gravação do áudio durante o interfone de vídeo e clique para finalizar a gravação. O arquivo gravado será salvo no caminho padrão no PC local, e você pode clicar em **Abrir pasta** na janela pop-up para visualizar o arquivo.

22.2.3 Atender Chamada

Você pode atender a chamada da estação de porta e da estação interna adicionadas por meio do Control Client.

Quando o Control Client recebe uma chamada da estação de porta ou estação interna, uma janela aparecerá. Você pode clicar em **Answer** para atender a chamada ou clicar em **Refuse** para recusar a chamada.

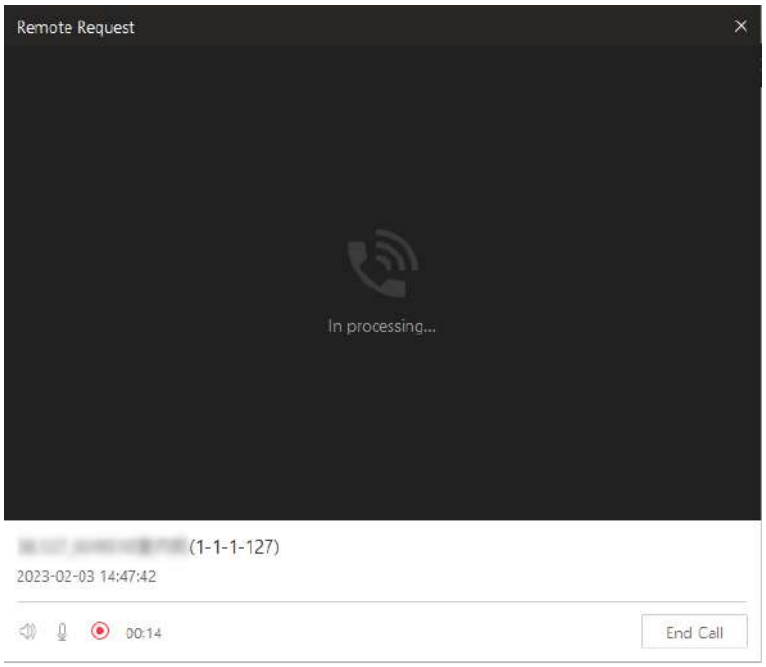


Figura 22-3 Atender chamada

Após a chamada ser atendida, você pode executar as seguintes operações.

- Clique em **Abrir porta** para abrir a porta vinculada remotamente.
- Clique para ajustar o volume do alto-falante.
- Clique para ajustar o volume do microfone.
- Clique para iniciar a gravação do áudio durante o interfone de vídeo e clique para finalizar a gravação. O arquivo gravado será salvo no caminho padrão no PC local, e você pode clicar em **Abrir pasta** na janela pop-up para visualizar o arquivo.
- Clique em **Encerrar chamada** para encerrar a chamada.

Observação

Você só pode atender uma chamada de um dispositivo de interfone de vídeo por meio do Control Client ao mesmo tempo.

22.3 Reproduzir Vídeo via VSPlayer

Você pode executar o software VSPlayer e reproduzir os arquivos de vídeo armazenados no PC local por meio do software.

Passos

1. Acesse a página do VSPlayer de uma das seguintes maneiras.
   - No canto superior direito da barra de navegação superior, selecione → **VSPlayer** .
   - No painel direito da página inicial, selecione **Ferramenta** → **VSPlayer** .
2. Clique duas vezes no vídeo para reproduzi-lo.
3. Opcional: clique no canto superior direito da página do VSPlayer e selecione **Manual do usuário** para visualizar o manual do usuário do VSPlayer para operações mais detalhadas.

22.4 Executar Áudio Bidirecional

A função de áudio bidirecional permite a conversa de voz entre o Control Client e os dispositivos. Você pode obter e reproduzir não apenas o vídeo ao vivo, mas também o áudio em tempo real do dispositivo no Control Client, e o dispositivo também pode obter e reproduzir o áudio em tempo real do Control Client.

Esta função não é suportada pelos dispositivos adicionados em um site remoto.

Passos

1. Acesse a página Áudio bidirecional de uma das seguintes maneiras.
   - No canto superior direito da barra de navegação superior, selecione → **Áudio bidirecional** .
   - No painel direito da página inicial, selecione **Ferramenta** → **Áudio bidirecional** .
2. Selecione uma câmera na área.
3. Selecione **Falar com o dispositivo NVR** ou **Falar com a câmera** .

Fale com o dispositivo NVR

Inicie o áudio bidirecional com um dispositivo NVR.

Observação

- Quando a câmera selecionada está conectada diretamente ao sistema, o áudio vai entre o sistema e a câmera.
- Quando a câmera está conectada ao sistema por meio de um NVR e você seleciona **Device Talk** , o áudio bidirecional vai entre o sistema e o dispositivo NVR.

Falar com a câmera

Inicie o áudio bidirecional com uma câmera.

Observação

- Quando a câmera está conectada diretamente ao sistema, **Falar com a Câmera** não pode ser selecionado.
- Quando a câmera está conectada ao sistema por meio de um NVR, DVR ou estação de entrada/saída, e você seleciona **Falar com a câmera** , o áudio bidirecional vai entre a câmera e o sistema.

4. Clique em **Iniciar** para iniciar o áudio bidirecional.
5. Opcional: clique para ajustar o volume do microfone, clique para ajustar o volume do alto-falante e clique para iniciar a gravação.

22.5 Transmissão

No Control Client, você pode transmitir para os dispositivos ou unidades de alto-falante que foram adicionados ao Web Client. Após a transmissão, você pode pesquisar os registros de transmissão. Acesse a página de transmissão de uma das seguintes maneiras:

- No canto superior direito da barra de navegação superior, selecione → **Transmitir** .
- No painel direito da página inicial, selecione **Ferramenta** → **Transmitir** .

22.5.1 Transmissão para Unidade de Alto-falante Conectada

Você pode transmitir para a(s) unidade(s) de alto-falante conectada(s) selecionando a(s) unidade(s) de alto-falante específica(s) e o modo de transmissão. O arquivo de áudio correspondente ou a voz do usuário será transmitido na(s) unidade(s) de alto-falante em tempo real.

Antes de começar

- Certifique-se de ter agrupado as unidades de alto-falante no Web Client.
- Certifique-se de ter adicionado unidade(s) de alto-falante à(s) área(s) no Web Client.
- Certifique-se de ter adicionado arquivo(s) de mídia à biblioteca de mídia no Web Client.
- Para obter detalhes sobre as operações acima, consulte o *Manual do Usuário do HikCentral Professional Web Client* .

Passos

1. Selecione **Por unidade de alto-falante** na parte superior.
2. Selecione a(s) unidade(s) de alto-falante online para transmissão.
   – Marque **Grupo** e selecione uma ou mais unidades de alto-falante do(s) grupo(s) de unidades de alto-falante.

Observação

Você pode clicar em **Exibir unidade de alto-falante não agrupada** para exibir a(s) unidade(s) de alto-falante que não estão agrupadas.

– Marque **Área** e selecione uma ou mais unidades de alto-falante da(s) área(s) onde as unidades de alto-falante foram adicionadas.

Observação

Você pode passar o mouse sobre uma unidade de alto-falante e clicar para ouvir o conteúdo da transmissão ao vivo. Durante a audição, você pode clicar para ajustar o volume e clicar para parar de ouvir. Esta função deve ser suportada pelo dispositivo.

3. Selecione o modo de transmissão.
   – Verifique **Falar** .
   – Marque **Reproduzir áudio** e selecione um arquivo de áudio da biblioteca de mídia.

   Observação

   Você pode clicar em **Download** para baixar e reproduzir o arquivo de áudio selecionado com antecedência para garantir que o áudio será transmitido fluente e corretamente.

   – Marque **Conteúdo de transmissão personalizado** e insira o conteúdo de transmissão conforme necessário.
   Selecione **Uma vez** ou **Duração especificada** como o modo de reprodução.
4. Clique em **Iniciar** .

Observação

Após iniciar a transmissão, você pode clicar na coluna Operation para ouvir o conteúdo da transmissão; clicar para ajustar o volume; e clicar para parar de ouvir. Esta função deve ser suportada pelo dispositivo.

O que fazer a seguir

Fale no microfone do PC ou reproduza o arquivo de áudio.

22.5.2 Transmissão para Dispositivos Conectados

Execute a função de transmissão para distribuir conteúdo de áudio para o dispositivo adicionado, caso o dispositivo tenha uma saída de áudio.

Observação

- Certifique-se de que o PC tenha um microfone disponível para transmitir áudio para o dispositivo.
- Se o cliente estiver executando áudio bidirecional com a câmera do dispositivo, você não

poderá iniciar a transmissão com o dispositivo e vice-versa.
- O dispositivo Cloud P2P suporta transmissão se habilitar DDNS.

1. Selecione **Por dispositivo** na parte superior.
2. Selecione um grupo de dispositivos existente ou clique para adicionar um grupo de dispositivos, se necessário, e depois clique em **Adicionar** para selecionar o(s) dispositivo(s) para o(s) qual(is) transmitir.
3. Iniciar ou parar a transmissão.

Começar tudo	Clique **em Iniciar tudo** para iniciar a transmissão para o(s) dispositivo(s) selecionado(s). **Observação** Você pode visualizar o status da transmissão em tempo real.
Pare tudo	Clique em **Parar tudo** para interromper a transmissão para o(s) dispositivo(s) selecionado(s).

22.5.3 Pesquisar Registros de Transmissão ao Vivo

Você pode definir condições de pesquisa, incluindo o horário de início, o horário de término e a emissora para pesquisar registros de transmissão ao vivo.

Antes de começar

- Certifique-se de que você terminou a transmissão ao vivo. Consulte ***Transmissão para a unidade de alto-falante conectada*** para obter detalhes.

Passos

1. Selecione **Speaker Unit Records** na parte superior.
2. Defina a hora de início.
3. Defina o horário de término.
4. Selecione uma emissora na lista suspensa.
5. Clique em **Pesquisar** .
   Você pode visualizar os resultados da pesquisa no lado direito e ver os detalhes de cada registro, incluindo a emissora, o número de unidades de alto-falante, a hora de início, o modo de transmissão e o tamanho do arquivo.
6. Opcional: Execute as seguintes operações.

Download	Clique na coluna Operação para baixar o áudio transmitido.
Ver unidade de alto-falante	Clique para visualizar a unidade do alto-falante.

Ver conteúdo de transmissão personalizado	Se o modo de transmissão for **Conteúdo de transmissão personalizado** , passe o cursor do mouse sobre a coluna Operação para visualizar o conteúdo de transmissão personalizado.

22.6 Entrada/Saída de Alarme de Controle

Uma saída de alarme é uma saída no dispositivo que pode ser conectada a um dispositivo periférico, como uma luz, uma barreira, etc. O dispositivo pode enviar sinal para controlar o dispositivo externo conectado, por exemplo, acender a luz, abrir o portão da barreira. O dispositivo periférico conectado pode ser controlado automaticamente por eventos ou alarmes, ou manualmente pelo cliente, e aqui apresentamos o processo para controlar a saída de alarme remotamente pelo cliente.

1. Acesse a página Controle de Saída de Alarme de uma das seguintes maneiras:
   - No canto superior direito da barra de navegação superior, selecione → **Controle de saída de alarme** .
   - No painel direito da página inicial, selecione **Ferramenta** → **Controle de saída de alarme** .
2. Selecione a(s) saída(s) de alarme que você quer habilitar/desabilitar e clique em **Open** / **Close** , uma por uma. Você também pode clicar em **Open All** / **Close All** para habilitar/desabilitar todas as saídas de alarme.

Entrada de alarme de controle

Você pode visualizar o número de painéis de controle de segurança, radares e dispositivos de controle de acesso, armar/desarmar esses dispositivos e ignorar a zona.

1. Acesse a página Controle de Saída de Alarme de uma das seguintes maneiras:
   - No canto superior direito da barra de navegação superior, selecione → **Controle de entrada de alarme** .
   - No painel direito da página inicial, selecione **Ferramenta** → **Controle de entrada de alarme** .
2. (Opcional)Selecione dispositivos para executar as seguintes operações.

Operações	Descrição
Fique de braço	Selecione áreas e selecione **Armar Ficar** para armar áreas no modo Armar Ficar quando você estiver em casa.
Armando	Selecione áreas e selecione **Armar** para armar o sistema quando estiver fora de casa.
Desarmar	Selecione áreas e selecione **Desarmar** para desarmá-las.
Armar Instantâneo	Selecione áreas e selecione **Instant Arming** . Quando as funções estiverem habilitadas, as zonas serão armadas imediatamente, sem atraso, quando as pessoas saírem da área de detecção.

Operações	Descrição
Limpar alarme	Selecione **Limpar alarme** para silenciar os alarmes de uma área.
Ignorar	Selecione **Por Área** . Se você quiser armar intencionalmente sua área com uma ou mais zonas desprotegidas, selecione uma zona e habilite **Bypass** . Se você ignorar uma zona, a zona NÃO será armada (nenhum alarme da zona será disparado), mesmo se outras zonas em uma área estiverem armadas.

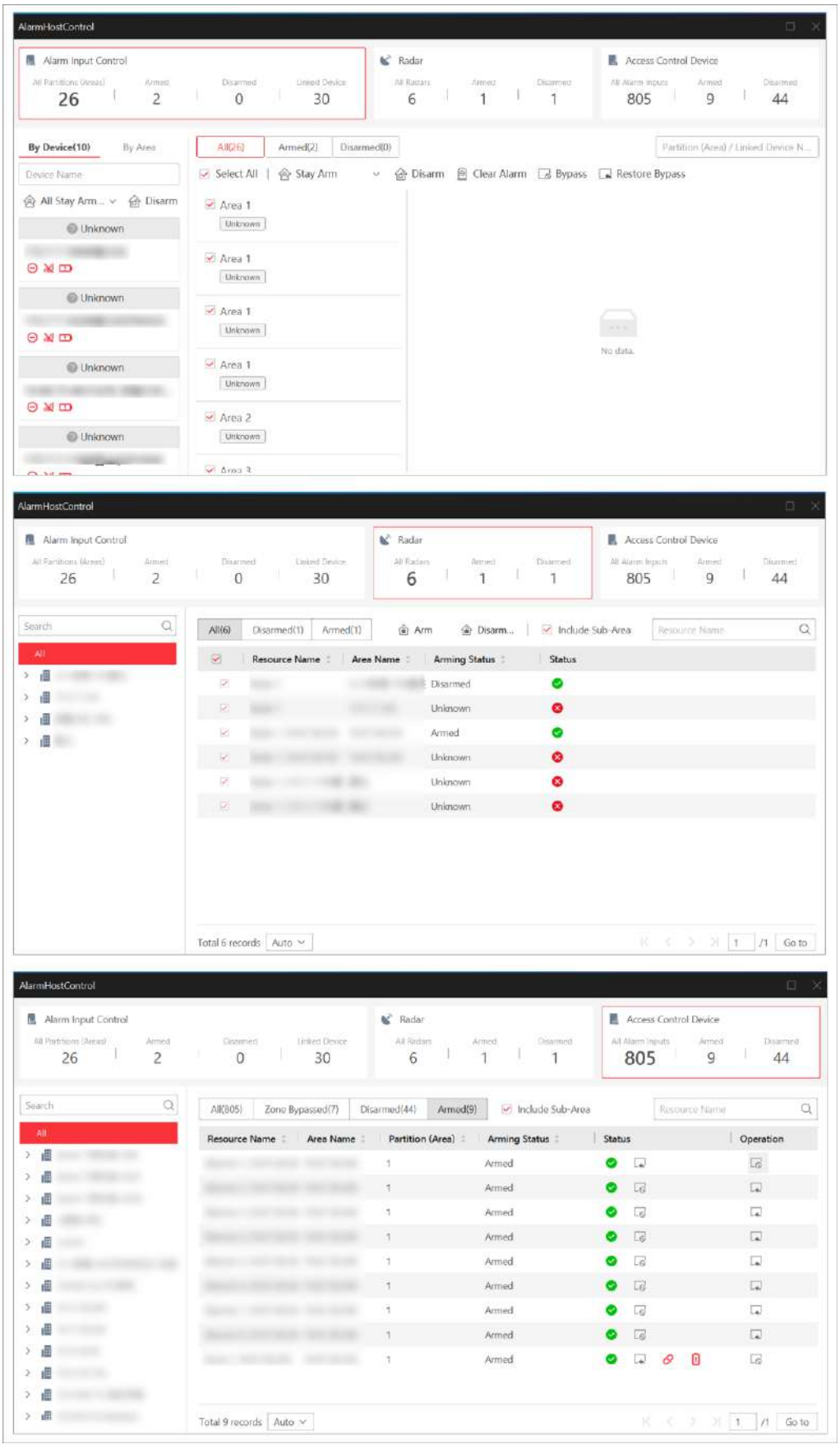

AlarmHostControl
Alarm Input Control
All Partitions (Areas) 26
Armed 2
Disarmed 0
Linked Device 30
Radar
All Radars 6
Armed 1
Disarmed 1
Access Control Device
All Alarm Inputs 805
Armed 9
Disarmed 44
By Device(10)
By Area
Device Name
All Stay Arm...
Disarm
Unknown
All(26)
Armed(2)
Disarmed(0)
Partition (Area) / Linked Device N...
Select All
Stay Arm
Disarm
Clear Alarm
Bypass
Restore Bypass
Area 1
Area 2
No data.
AlarmHostControl
Search
All
All(6)
Disarmed(1)
Armed(1)
Arm
Disarm...
Include Sub-Area
Resource Name
Resource Name
Area Name
Arming Status
Status
Disarmed
Unknown
Armed
Total 6 records
Auto
Go to
AlarmHostControl
All(805)
Zone Bypassed(7)
Disarmed(44)
Armed(9)
Include Sub-Area
Resource Name
Area Name
Partition (Area)
Arming Status
Status
Operation
Armed
Total 9 records
Auto
Go to

Figura 22-4 Controle de entrada de alarme

Saída de alarme de controle

Uma saída de alarme é uma saída no dispositivo que pode ser conectada a um dispositivo periférico, como uma luz, uma barreira, etc. O dispositivo pode enviar sinal para controlar o dispositivo externo conectado, por exemplo, acender a luz, abrir o portão da barreira. O dispositivo periférico conectado pode ser controlado automaticamente por eventos ou alarmes, ou manualmente pelo cliente, e aqui apresentamos o processo para controlar a saída de alarme remotamente pelo cliente.

1. Acesse a página Controle de Saída de Alarme de uma das seguintes maneiras:
   - No canto superior direito da barra de navegação superior, selecione → **Controle de saída de alarme** .
   - No painel direito da página inicial, selecione **Ferramenta** → **Controle de saída de alarme** .
2. Selecione a(s) saída(s) de alarme que você quer habilitar/desabilitar e clique em **Open** / **Close** , uma por uma. Você também pode clicar em **Open All** / **Close All** para habilitar/desabilitar todas as saídas de alarme.

22.7 Outras Ferramentas

Acesse a página Gravação de tela / Evento de disparo / Limpador / Controle de armação de uma das seguintes maneiras:

- No canto superior direito da barra de navegação superior, selecione .
- No painel direito da página inicial, selecione **Ferramenta** .

Controle de Armar

Para obter detalhes, consulte ***Executar controle de armamento para alarmes*** .

Gravação de tela

Observação

Para obter detalhes sobre como definir as informações necessárias para evidências, consulte ***Salvar filmagens de vídeo encontradas no Centro de gerenciamento de evidências*** .

Limpador

Selecione câmeras para iniciar os limpadores em lote.

Observação

Os limpadores pararão automaticamente.

Evento de gatilho

Selecione um evento definido pelo usuário. Veja ***Manually Trigger User-Defined Event*** para detalhes.

Capítulo 23 Gerenciar Tarefas de Download/Upload

Você pode visualizar as tarefas de download/upload em andamento ou concluídas e gerenciar todas as tarefas (por exemplo, download/upload de vídeo, download/upload de informações do veículo), como iniciar, parar, excluir e assim por diante, no Centro de Downloads.

Passos

1. No canto superior esquerdo do Control Client, selecione → **Todos os módulos** → **Gerenciamento** → **Central de tarefas** .

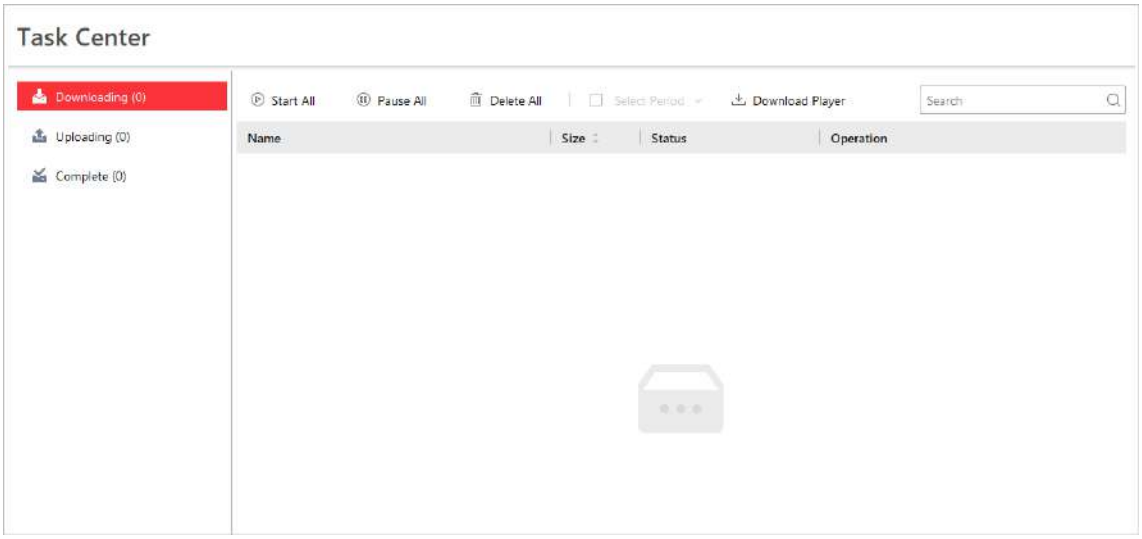


Figura 23-1 Centro de Tarefas

2. Verifique as tarefas de diferentes tipos.

Verifique as tarefas de download em andamento	Clique na aba **Baixando** para verificar as tarefas de download em andamento.
Verificar tarefa de upload	Clique na aba **Upload** para verificar as evidências que estão sendo carregadas do PC local para o pool de recursos.

Observação

Para obter detalhes sobre como salvar filmagens de vídeo como evidência, consulte ***Gerenciamento de evidências*** .

Verificar tarefa concluída	Clique na aba **Concluído** para verificar as tarefas concluídas.

3. Opcional: Execute a(s) seguinte(s) operação(ões) para as tarefas.

Pausar download	Clique para interromper uma tarefa de download em andamento

	ou clique em **Parar tudo** para interromper todas as tarefas.
Continuar o download	Clique para retomar o download ou clique em **Iniciar tudo** para retomar todas as tarefas pausadas.
Organizar tempo para download automático	1. Você pode programar um período de menor movimento para baixar arquivos automaticamente e evitar congestionamento de rede em ambientes com baixa largura de banda. Clique na aba **Download** . 2. Marque **Selecionar período** para selecionar um ou mais períodos de tempo e personalizar o período de tempo correspondente para download automático.
Excluir tarefa de download	Selecione uma tarefa e clique para remover a tarefa de download ou clique em **Excluir tudo** para excluir todos os registros de download. Para concluir a tarefa de download, você também pode optar por excluir os arquivos de vídeo baixados.
Ver vídeo baixado	Para concluir a tarefa de download, clique na coluna Operação para visualizar os arquivos de vídeo baixados.
Selecione o caminho para salvar o arquivo de vídeo	Para concluir a tarefa de download, selecione uma ou várias tarefas e clique em **Salvar como** e selecione o caminho para salvar os arquivos de vídeo.

4. Opcional: clique em **Baixar Player** para baixar o player no seu PC e reproduzir os arquivos de vídeo baixados.

Capítulo 24 Configurações do Sistema

A página Sistema contém configurações gerais, configurações básicas de vídeo, configurações de som de alarme, configurações de monitoramento de saúde, gerenciamento de posição de tela, configurações de impressão de recibos, configurações do modo de página inicial e configurações de chamada.
Selecione **Gerenciamento** → **Sistema** na página inicial ou selecione → **Gerenciamento** → **Sistema** no canto superior esquerdo para entrar na página Sistema.

24.1 Definir Parâmetros Gerais

Você pode definir os parâmetros usados com frequência, incluindo o desempenho da rede, o modo de exibição e o caminho para salvar os arquivos.

Passos

1. Na página Geral, selecione a guia **Parâmetros gerais** .
2. Configure os parâmetros gerais.

Tempo limite da rede

O tempo de espera padrão para o Control Client. As operações serão consideradas falhas se não houver resposta dentro do tempo configurado.
O tempo mínimo de espera padrão das interações entre o Control Client e o servidor SYS é de 30s, o tempo mínimo entre o servidor SYS e os dispositivos é de 5s, e o tempo mínimo entre o Control Client e os dispositivos é de 5s.

Modo Máximo

Selecione **Maximize** ou **Full Screen** como o modo máximo. Para selecionar Maximize, o cliente será maximizado e a barra de tarefas será exibida. Para selecionar Full Screen, o cliente será exibido no modo de tela cheia.

Fuso horário

Hora do dispositivo

O Control Client adotará o horário do fuso horário onde o dispositivo está localizado.

Tempo do cliente

O Control Client (exceto os módulos de Análise de Vídeo) adotará o horário do fuso horário onde o PC que executa o Control Client está localizado.

Diferença de tempo

Se habilitado, as informações de fuso horário serão exibidas na hora. Por exemplo, 2018-12-12 12:12:12 +8:00.

Login automático

O sistema lembrará o nome de usuário e a senha e efetuará login no Control Client

automaticamente quando você iniciar o PC executando o Control Client.

Após iniciar o cliente, abra

Abra automaticamente a página inicial, a última interface ou a visualização após iniciar o cliente.

Página inicial

Exibir automaticamente a página inicial após iniciar o cliente.

Módulo de Função Especificada

Insira automaticamente o módulo de função especificado após iniciar o cliente.

Última Interface

Restaure a última interface aberta quando você executar o cliente na próxima vez.

Vista Especificada

Exiba automaticamente a visualização especificada que você definiu após iniciar o cliente.

- Você pode clicar em **Show Screen No.** para mostrar o número da tela do PC atual executando o Control Client. E você pode selecionar a(s) visualização(ões) especificada(s) de acordo com sua necessidade.
- Suporta a exibição da visualização especificada na tela auxiliar ou na parede inteligente (placa gráfica).
- Para exibir na parede inteligente (placa gráfica), você deve configurar a exibição de conteúdo na parede inteligente (placa gráfica) no modo parede inteligente.
- Para exibição na parede inteligente (placa gráfica), quando você seleciona a visualização especificada, a visualização deve ser exibida na parede inteligente (placa gráfica) ao mesmo tempo e, em seguida, a visualização será exibida na parede inteligente (placa gráfica) após iniciar o cliente na próxima vez, caso contrário, a visualização será exibida na tela auxiliar após iniciar o cliente na próxima vez.

Modo de exibição em larga escala

Para melhorar a eficiência da operação de recursos, se houver um tipo de recurso com mais de 512 recursos, você pode alternar para o **Modo de Exibição em Grande Escala** . Neste modo, os recursos no sistema não serão carregados ao iniciar o Control Client por motivos de economia de tempo, então isso levará tempo ao pesquisar um dispositivo na lista de recursos.

Observação

- Para o Sistema Central na versão gratuita ou com módulo RSM (Remote Site Management), você não pode ligar o Modo de Exibição em Grande Escala. Por padrão, o Sistema Central na versão gratuita está no modo de exibição em grande escala, e o Sistema Central com módulo RSM está no modo de exibição em pequena escala.
- Áreas sem recursos serão exibidas e não há suporte para selecionar todos os recursos de uma vez.
- Por padrão, o modo de exibição em grande escala está desabilitado.

Caminho para salvar arquivo

Defina os caminhos de salvamento para os arquivos que você baixou para o seu computador (arquivos de vídeo gravados ou baixados manualmente, imagens capturadas e arquivos de pacote).

Notificação de Resolução Indevida

Habilita ou desabilita a janela pop-out que notifica que a resolução atual da tela de exibição é inadequada para o Control Client.

3. Clique em **Salvar** .

24.2 Definir Atalho

Você pode definir teclas de atalho do teclado do PC para operações básicas usadas com frequência e operações PTZ ao visualizar vídeos, e configurar atalhos que podem acionar os mesmos recursos em joysticks USB e teclados USB.

Na página Geral, selecione a aba **Atalho** . Na coluna Teclado do PC, insira as teclas e selecione atalhos de joysticks USB e teclados USB na lista suspensa.

Observação

indica que o recurso não oferece suporte à configuração de nenhuma tecla ou atalho.

24.3 Definir Parâmetros de Vídeo

Você pode definir parâmetros de rede, formato de arquivo de imagem, parâmetros de exibição, etc.

Na página Sistema, selecione **Vídeo básico** à esquerda.

Tabela 24-1 Definir parâmetros de vídeo

Área	Parâmetros	Descrição
Definir parâmetros de rede	Fluxo global	Selecione o tipo de fluxo padrão para uso global.
	Visualização ao vivo do fluxo principal/reprodução: Divisões de janela	Quando o número de janelas divididas for menor que o número definido, os vídeos ao vivo ou gravados serão exibidos pelo fluxo principal.
	Largura de banda	Defina o limite superior de largura de banda para baixar vídeos do servidor pStor, que é usado como um servidor de gravação para armazenar arquivos de vídeo e imagens.
Definir	Formato de imagem	Selecione o formato de arquivo para imagens

Área	Parâmetros	Descrição
parâmetros de arquivo		capturadas durante a visualização ao vivo ou reprodução.
	Vídeo de rastreamento visual	Ative **o Rastreamento Visual de Vídeo** para gravar automaticamente o vídeo durante o rastreamento visual.
Definir parâmetros de exibição	Tamanho da fonte	O tamanho da fonte do conteúdo em recursos, visualizações e favoritos.
	Escala de visualização	O modo de exibição de imagem em cada janela de exibição em visualização ao vivo ou reprodução.
	Escala de janela	A escala do vídeo em visualização ao vivo ou reprodução. Você pode defini-lo como 4:3 ou 16:9 (padrão).
	Divisão de Janelas	O número de divisões de janelas.
	Janela de exibição nº.	Exibir o número da janela no módulo Monitoramento.
	Exibir regra VCA	Quando ativado, a regra VCA na visualização ao vivo e na reprodução será exibida.
	Cache de vídeo	Um cache de quadros maior resultará em melhor desempenho de vídeo. Ele é determinado com base no desempenho da rede, desempenho do computador e taxa de bits.
	Pare de transmitir quando a conta estiver bloqueada	Quando habilitado, o streaming será interrompido quando a conta for bloqueada. Após desbloquear a conta, o streaming será restaurado.
	Decodificação Contínua	Decodifique continuamente ao alternar a divisão de janelas entre uma janela e várias janelas.
	Habilitar destaque	Ative esta função para marcar os objetos detectados com retângulos verdes na visualização ao vivo e na reprodução.
	Aguarde o prompt para reprodução síncrona	Habilite esta função para mostrar um prompt de espera pela reprodução síncrona.
	Sobreposição de	Quando ativado, exibe as informações da transação na visualização ao vivo e na imagem

Área	Parâmetros	Descrição
	informações de transação	de reprodução.
	Informações de temperatura de sobreposição	Quando ativado, exibe as informações de temperatura na visualização ao vivo e na imagem reproduzida.
	Decodificação de hardware de GPU	Quando ativado, ativa a decodificação da GPU para visualização ao vivo e reprodução para economizar recursos da CPU.
	Compensação de quadro baixo	Defina o limite de quadros baixo e, quando o valor for atingido, a compensação de quadros baixo será ativada.
	Exibição padrão/Grupo de exibição para exibição ao vivo	Defina as visualizações/grupos de visualizações padrão, que serão reproduzidos automaticamente quando você iniciar a visualização ao vivo.
	Configuração de exibição de contagem de pessoas em tempo real	Você pode ativar **o modo bilíngue** para que os dados sejam exibidos de forma bilíngue.
Definir parâmetros de imagem	Qualidade do vídeo	Defina a qualidade do vídeo ao exibir a área de trabalho no smart wall.
	Modo de codificação	Escolha entre **Codificação de GPU** e **Codificação de CPU** .
	Taxa de quadros de vídeo	Escolha entre 2, 5, 15, 25 e 30.
Definir parâmetros de áudio	Ligar áudio automaticamente	Se ativado, quando você reproduzir um vídeo, o áudio será ligado automaticamente.
	Comando de voz para não usar máscara	Se ativado, haverá um aviso de voz caso a pessoa não esteja usando máscara.
	Comando de voz para temperatura normal	Se ativado, haverá um aviso de voz se a temperatura da pessoa estiver normal.
	Aviso de voz para temperatura anormal	Se ativado, haverá um aviso de voz se a temperatura da pessoa estiver anormal.
Definir barra de ferramentas	Personalize os ícones mostrados durante a visualização ao vivo ou reprodução conforme necessário. Se você marcar **Always Display Toolbar** , a barra de ferramentas sempre será exibida na parte inferior da janela de visualização ao vivo ou reprodução.	

24.4 Habilitar Impressão de Recibos de Estacionamento Gratuito

Você pode habilitar a impressão de recibos de estacionamento quando a cobrança final for 0.
No canto superior esquerdo do Control Client, selecione → **Gerenciamento** → **Sistema** → **Veículo** para entrar na página de configurações de impressão de recibos.
Ative a opção **Imprimir recibo** .
No campo Imprimir recibo de estacionamento gratuito, você pode selecionar **Imprimir** ou **Não imprimir,** de acordo com a necessidade real.
Clique **em Salvar** .

24.5 Definir Parâmetros de Parede Inteligente

Você pode definir a qualidade, o modo de codificação e a taxa de quadros para exibir vídeos em paredes inteligentes, personalizar ícones na barra de operação de paredes inteligentes e definir parâmetros de exibição.
Na página Sistema, selecione **Smart Wall** na barra de navegação esquerda.

Definir parâmetros de imagem

Qualidade do vídeo

Defina a qualidade do vídeo ao exibir vídeos no smart wall.

Modo de codificação

Selecione **Codificação GPU** ou **Codificação CPU** como o modo de codificação. O desempenho da codificação CPU é melhor do que o da codificação GPU, mas a codificação CPU causará grande ocupação da CPU, o que pode afetar outros processos.

Taxa de quadros de vídeo

Defina a taxa de quadros do vídeo exibido no smart wall como 2, 5, 15, 25 ou 30. Quanto maior a taxa de quadros, mais suave será a reprodução do vídeo.

Personalizar ícones na barra de operações

Clique em um ícone na lista para adicioná-lo ao quadro cinza abaixo para ocultá-lo, ou clique no ícone no quadro cinza para adicioná-lo novamente e exibi-lo na barra de operação do smart wall.
Ative **Mostrar somente ícones** para exibir ícones sem descrições na barra de operação.

Observação

Você deve reiniciar o Control Client ou alternar os usuários para aplicar as configurações.

Definir parâmetros de exibição

Mostrar janela nº.

Após habilitado, o número da janela será exibido na parede inteligente.

Nome da saída de exibição

Após habilitado, o nome da saída será exibido na parede inteligente.

24.6 Definir Frequência de Atualização Automática para Painel de Controle Digital

Você pode configurar o intervalo de tempo para atualização automática dos dados e informações no painel de controle digital.
Na página Sistema, selecione **Painel de Controle Digital** na barra de navegação esquerda.
Defina o intervalo de atualização automática para 30s, 1min, 3min, 5min, 10min ou 15min, ou desative **a Atualização Automática** para desabilitar a atualização automática do painel de controle digital.
Clique em **Salvar** para salvar as configurações ou clique **em Padrão** para restaurar as configurações padrão.

Observação

Você deve reiniciar o Control Client ou alternar os usuários para aplicar as configurações.

24.7 Definir Toque para Chamadas

Você pode definir um toque para chamadas de dispositivos de controle de acesso, dispositivos de interfone com vídeo e cancelas no estacionamento.
No canto superior esquerdo do Control Client, selecione → **Gerenciamento** → **Sistema** → **Chamadas** para entrar na página de configurações de toque.
Ative o **toque para chamadas** .
Você pode clicar para selecionar um arquivo de áudio do PC local e clicar para começar a reproduzir o toque.
Clique **em Salvar** .

24.8 Definir Frequência de Verificação de Integridade

Você pode configurar o intervalo de tempo para iniciar automaticamente a verificação de integridade e atualizar o status do recurso.
Na página Sistema, selecione **Status de integridade** na barra de navegação esquerda.
Selecione 30s, 1min, 3min, 5min, 10min ou 15min na lista suspensa para definir o intervalo de atualização automática.
Clique em **Salvar** para salvar as configurações ou clique **em Padrão** para restaurar as configurações padrão.

24.9 Definir Posição da Tela

Para usuários que adotam tela expandida durante a exibição/reprodução ao vivo ou parede inteligente (placa gráfica), é necessário definir a posição da tela de acordo com o layout real para alternar a tela por um teclado de rede convenientemente.

No canto superior esquerdo do Control Client, selecione → **Management** → **System** → **Screen Position** para exibir a posição atual da tela no painel direito. Você pode passar o cursor sobre uma tela para certificar-se das telas correspondentes das janelas exibidas. Arraste uma janela para outra janela para alterar a posição relativa das janelas para que a direção de controle pelo joystick também mude.


See Far, Go Further

DS-K1T673TDX-M
Face Recognition Terminal

Face recognition terminal is a kind of access control device. It can bewidely applied in multiple scenarios, such as enterprises, stations, dwellings, factories, schools, campus and so on.

- 7-inch LCD touch screen,2 Mega pixel wide-anglelens
- Recognition distance: 0.3 to 3 m
- Face recognition duration < 0.2 s/User
- Face recognition accuracy rate ≥ 99%
- Built-in M1 card, reading module (Presents card on thescreen to authenticate)
- Face mask detection
- 50,000 face capacity, 10,000 fingerprint or palm print capacity (With fingerprint or palm module), 50,000 card capacity, 150,000 event capacity, and 50,000 numericpassword.
- Supports ISAPI, ISUP 5.0, TCP/IP (IPv4 and IPv6)
- Supports singleperson and multiple people (Up to 5 people) recognition

▪ Specification

System	
Operation system	Linux
Processor	Dual Core 1000Mhz
RAM Memory	1 GB
Flash Capacity	8 GB
Display	
Size	7-inch
Type	Touch screen
Video	
FOV	HFOV= 75.5°; VFOV= 70°; DFOV= 87°
Pixel	2 MP
Lens	Dual-lens
Video standard	PAL (Default)/NTSC
WDR / Supplement Light type	Yes / IR 850nm
Network	
Wired network	Support 10/100/1000 Mbps self-adaptive
Protocols	TCP/IP, UDP, HTTP, HTTPS, DNS, IPV4, IPV6, RTSP, RTP, P2P, OSDP, ISAPI, ISUP 5.0.
Interface	
Alarm input	1
Alarm output	1
USB	1 (For Module)
Audio Output Interface	1 (3.5 mm)
Network interface	1
RS-485	1
Wiegand	1
Lock output	2
Exit button	1
Door contact input	1
Tamper	1
Capacity	
Card capacity	50,000
Face capacity	50,000
Fingerprint or palm print capacity	10,000
Event capacity	250,000
Numeric Password	50,000
Authentication	
Face recognition accuracy rate	≥ 99%
Card type	M1 card 13,56 MHz (ISO14443A)
Card reading distance	0 to 3 cm
Authentication 1:1	Yes
Authentication 1:N	Yes
Card reading duration	< 1 s
Face recognition duration	< 0.2 s per person

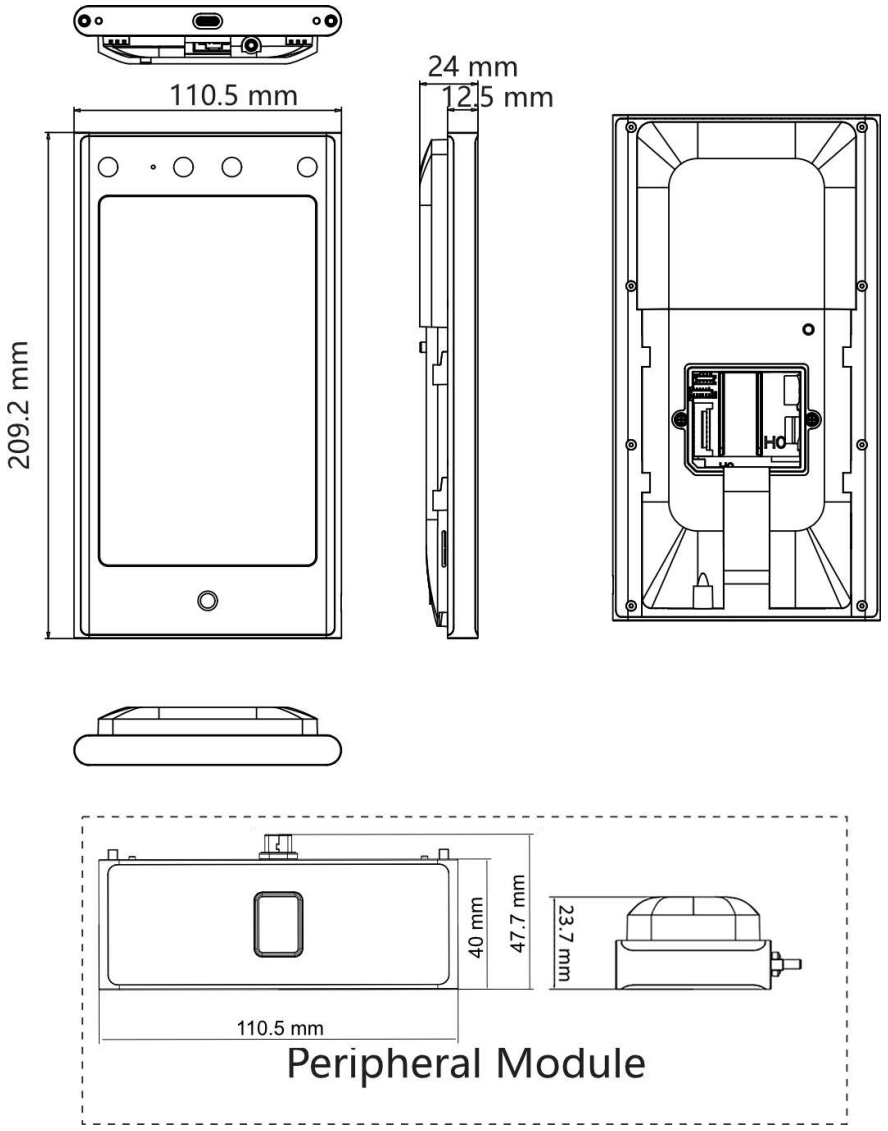
Face recognition distance	0.3 to 3 m
Face registration time	< 10s
Fingerprint duration	< 0,5 s
Fingerprint registration time	< 10s
QR codereading	Yes
ID Numerical Registration Limit	8 Digits
General	
Power supply	12 VDC to 24 VDC/2 A
Working temperature	-30 °C to 60 °C (-22 °F to 140 °F)
Working humidity	0 to 90% (no condensing)
Protective level	IP65
Dimensions	110.5 mm × 209.2 mm × 24 mm (4.35" × 8.24" × 0.94")
Language	English, Spanish (South America), Arabic, Thai, Indonesian, Russian, Vietnamese, Portuguese (Brazil), Japanese, Korean
Weight	Gross Weight：1.06 kg (2.34 lb) Net Weight：0.57 kg (1.26 lb)
MTBF	5 years
Languages (audio and text)	English and Portuguese
Function	
Two-way audio	Support
Time synchronization	Support
Access Level and Access Group	Yes
LED System Status	Yes
GUI	Yes
Backup database	Yes
Template Replication and Comparison	Yes
Anti-pass back	Support
Operation	Online and Standalone
DST / Holidays	Support
HTTPS	Support
Face anti-spoofing	Support
Live view	Support
Audio prompt	Support

▪ Available Model

DS-K1T673TDX

DS-K1T673TDX-M

▪ Dimension



▪ Accessory

▪ Optional

DS-KAB6-D1	DS-KAB6-ZU1	DS-KAB673-FB	DS-KAB673-FBQR	DS-KAB673-BQR
				
DS-KAB673-B	**DS-KAB6-W1**	**DS-KAB673-P**		

Headquaders
0o.55b Oianmo Poad, BinJ rang Dist net,
Han gzhon S10051, 0hina
I +86-b71- 8807-5998
www.hikvis +on.com

Follow us on social media to get the latest product and solution information.

H kvi8 00 0 0 0 0 - Hikvision totporate Channel hik'is onh q

MF1 IC S50

Functional specification

Rev. 5.2 — 15 January 2007
001052

Product data sheet
PUBLIC

1. General description

NXP has developed the Mifare MF1 IC S50 to be used in contactess smart cards according to ISO/IEC 14443A. The communication layer (Mifare RF Interface) complies to parts 2 and 3 of the ISO/IEC 14443A standard. The security layer sports the field proven CRYPTO1 stream cipher for secure data exchange of the Mifare Classic family.

1.1 Contactless Energy and Data Transfer

In the Mifare system, the MF1 IC S50 is connected to a coil with a few turns and then embedded in plastic to form the passive contactless smart card. No battery is needed. When the card is positioned in the proximity of the Read Write Device (RWD) antenna, the high speed RF communication interface allows to transmit data with 106 kBit/s.

1.2 Anticollision

An intelligent anticollision function allows to operate more than one card in the field simultaneously. The anticollision algorithm selects each card individually and ensures that the execution of a transaction with a selected card is performed correctly without data corruption resulting from other cards in the field.

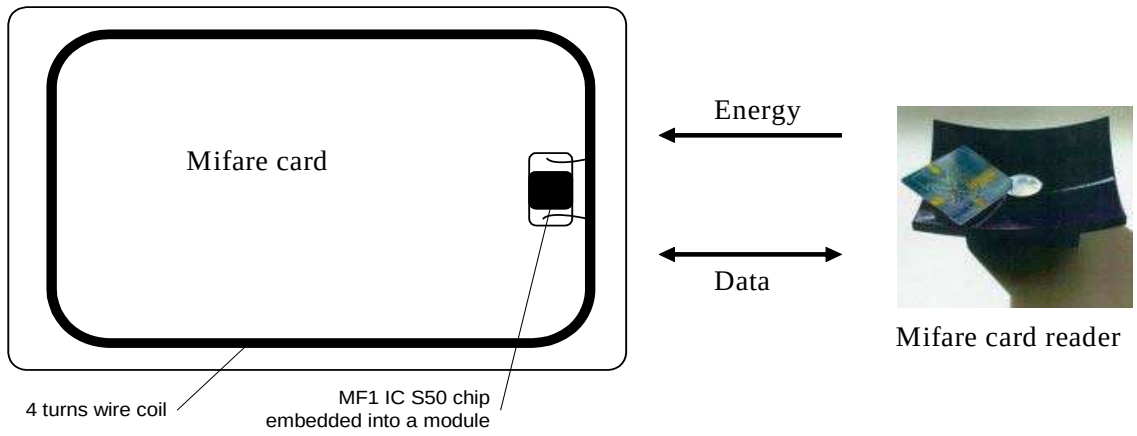


Fig 1. Mifare card reader

1.3 User Convenience

The Mifare system is designed for optimal user convenience. The high data transmission rate for example allows complete ticketing transactions to be handled in less than 100 ms. Thus, the Mifare, card user is not forced to stop at the RWD antenna leading to a high throughput at gates and reduced boarding times onto busses. The Mifare card may also remain in the wallet during the transaction, even if there are coins in it.

1.4 Security

Special emphasis has been placed on security against fraud. Mutual challenge and response authentication, data ciphering and message authentication checks protect the system from any kind of tampering and thus make it attractive for ticketing applications. Serial numbers, which can not be altered, guarantee the uniqueness of each card.

1.5 Multi-application Functionality

The Mifare system offers real multi-application functionality comparable to the features of a processor card. Two different keys for each sector support systems using key hierarchies.

1.6 Delivery Options

- Die on wafer
- Bumped die on wafer
- Chip Card Module
- Flip Chip Package

2. Features

2.1 MIFARE, RF Interface (ISO/IEC 14443 A)

- Contactless transmission of data and supply energy (no battery needed)
- Operating distance: Up to 100mm (depending on antenna geometry)
- Operating frequency: 13.56 MHz
- Fast data transfer: 106 kbit/s
- High data integrity: 16 Bit CRC, parity, bit coding, bit counting
- True anticollision
- Typical ticketing transaction: < 100 ms (including backup management)

2.2 EEPROM

- 1 Kbyte, organized in 16 sectors with 4 blocks of 16 bytes each (one block consists of 16 byte)
- User definable access conditions for each memory block
- Data retention of 10 years.
- Write endurance 100.000 cycles

2.3 Security

- Mutual three pass authentication (ISO/IEC DIS 9798-2)
- Data encryption on RF-channel with replay attack protection
- Individual set of two keys per sector (per application) to support multi-application with key hierarchy
- Unique serial number for each device
- Transport key protects access to EEPROM on chip delivery

3. Ordering information

See Delivery Type Addendum of Device

4. Block diagram

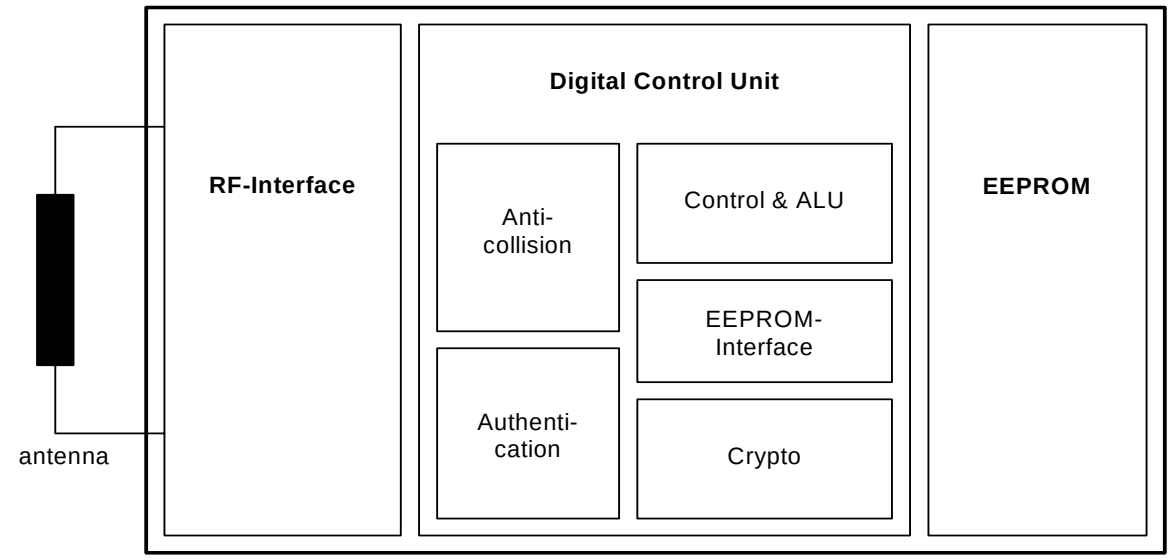


Fig 2. Block diagram

5. Pinning information

5.1 Pinning

See Delivery Type Addendum of Device

6. Functional description

6.1 Block description

The MF1 IC S50 chip consists of the 1 Kbyte EEPROM, the RF-Interface and the Digital Control Unit. Energy and data are transferred via an antenna, which consists of a coil with a few turns directly connected to the MF1 IC S50. No further external components are necessary. (For details on antenna design please refer to the document Mifare, Card IC Coil Design Guide.)

- RF-Interface:
  - Modulator/Demodulator
  - Rectifier
  - Clock Regenerator
  - Power On Reset
  - Voltage Regulator
- Anticollision: Several cards in the field may be selected and operated in sequence
- Authentication: Preceding any memory operation the authentication procedure ensures that access to a block is only possible via the two keys specified for each block
- Control & Arithmetic Logic Unit: Values are stored in a special redundant format and can be incremented and decremented
- EEPROM-Interface
- Crypto unit: The field proven CRYPTO1 stream cipher of the Mifare Classic family ensures a secure data exchange
- EEPROM: 1 Kbyte are organized in 16 sectors with 4 blocks each. A block contains 16 bytes. The last block of each sector is called “trailer”, which contains two secret keys and programmable access conditions for each block in this sector.

6.2 Communication principle

The commands are initiated by the RWD and controlled by the Digital Control Unit of the MF1 IC S50 according to the access conditions valid for the corresponding sector.

6.2.1 Request standard/ all

After Power On Reset (POR) of a card it can answer to a request command - sent by the RWD to all cards in the antenna field - by sending the answer to request code (ATQA according to ISO/IEC 14443A).

6.2.2 Anticollision loop

In the anticollision loop the serial number of a card is read. If there are several cards in the operating range of the RWD, they can be distinguished by their unique serial numbers and one can be selected (select card) for further transactions. The unselected cards return to the standby mode and wait for a new request command.

6.2.3 Select card

With the select card command the RWD selects one individual card for authentication and memory related operations. The card returns the Answer To Select (ATS) code (= 08h), which determines the type of the selected card. Please refer to the document MIFARE, Standardized Card Type Identification Procedure for further details.

6.2.4 Three pass authentication

After selection of a card the RWD specifies the memory location of the following memory access and uses the corresponding key for the three pass authentication procedure. After a successful authentication all memory operations are encrypted.

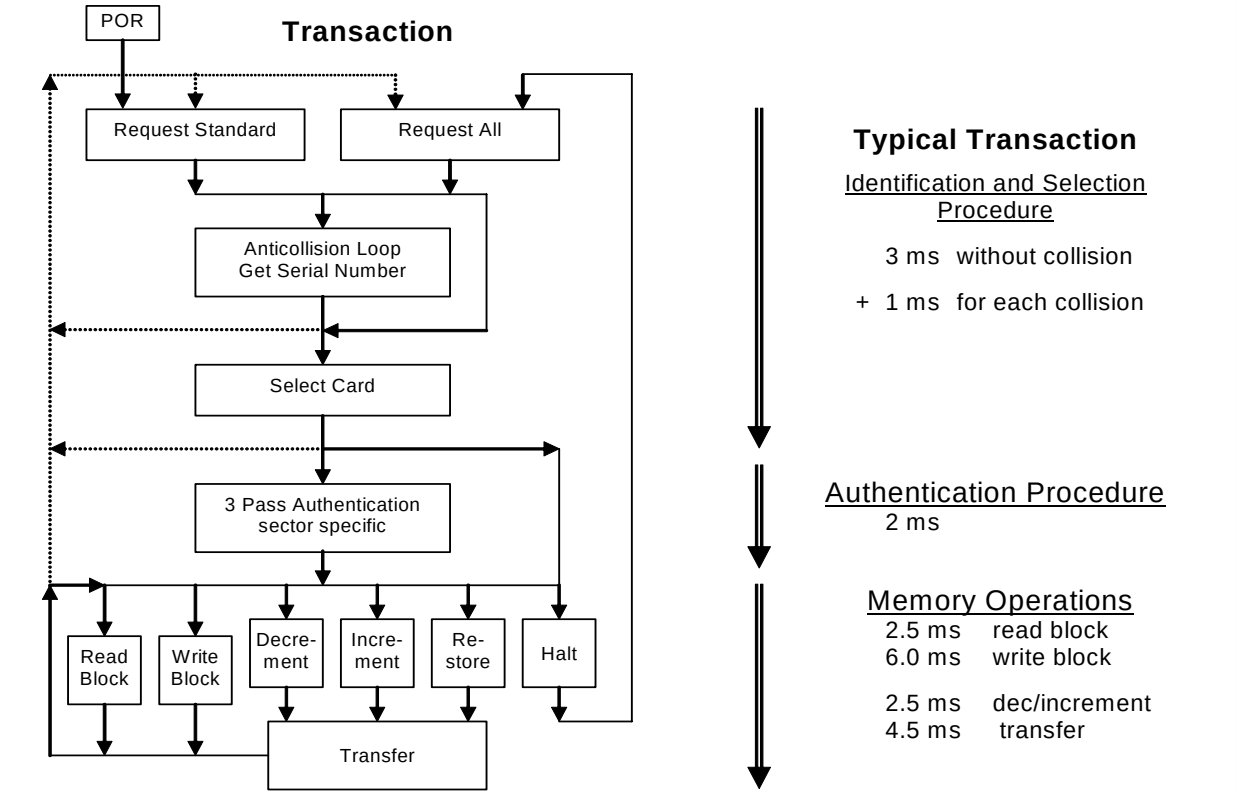


Fig 3. Three pass authentication

6.2.5 Memory operations

After authentication any of the following operations may be performed:

- Read block
- Write block
- Decrement:Decrements the contents of a block and stores the result in a temporary internal data-register
- Increment: Increments the contents of a block and stores the result in the data-register
- Restore: Moves the contents of a block into the data-register
- Transfer: Writes the contents of the temporary internal data-register to a value block

6.3 Data integrity

Following mechanisms are implemented in the contactless communication link between RWD and card to ensure very reliable data transmission:

- 16 bits CRC per block
- Parity bits for each byte
- Bit count checking
- Bit coding to distinguish between "1", "0", and no information
- Channel monitoring (protocol sequence and bit stream analysis)

6.4 Security

To provide a very high security level a three pass authentication according to ISO/IEC DIS 9798-2 is used.

6.4.1 Three pass authentication sequence

1. The RWD specifies the sector to be accessed and chooses key A or B.
2. The card reads the secret key and the access conditions from the sector trailer. Then the card sends a random number as the challenge to the RWD (pass one).
3. The RWD calculates the response using the secret key and additional input. The response, together with a random challenge from the RWD, is then transmitted to the card (pass two).
4. The card verifies the response of the RWD by comparing it with its own challenge and then it calculates the response to the challenge and transmits it (pass three).
5. The RWD verifies the response of the card by comparing it to its own challenge.

After transmission of the first random challenge the communication between card and RWD is encrypted.

6.5 RF interface

The RF-interface is according to the standard for contactless smart cards ISO/IEC 14443A.

The carrier field from the RWD is always present (with short pauses when transmitting), because it is used for the power supply of the card.

For both directions of data communication there is only one start bit at the beginning of each frame. Each byte is transmitted with a parity bit (odd parity) at the end. The LSB of the byte with the lowest address of the selected block is transmitted first. The maximum frame length is 163 bits (16 data bytes + 2 CRC bytes = 16 * 9 + 2 * 9 + 1 start bit).

6.6 Memory organization

The 1024 x 8 bit EEPROM memory is organized in 16 sectors with 4 blocks of 16 bytes each. In the erased state the EEPROM cells are read as a logical “0”, in the written state as a logical “1”.

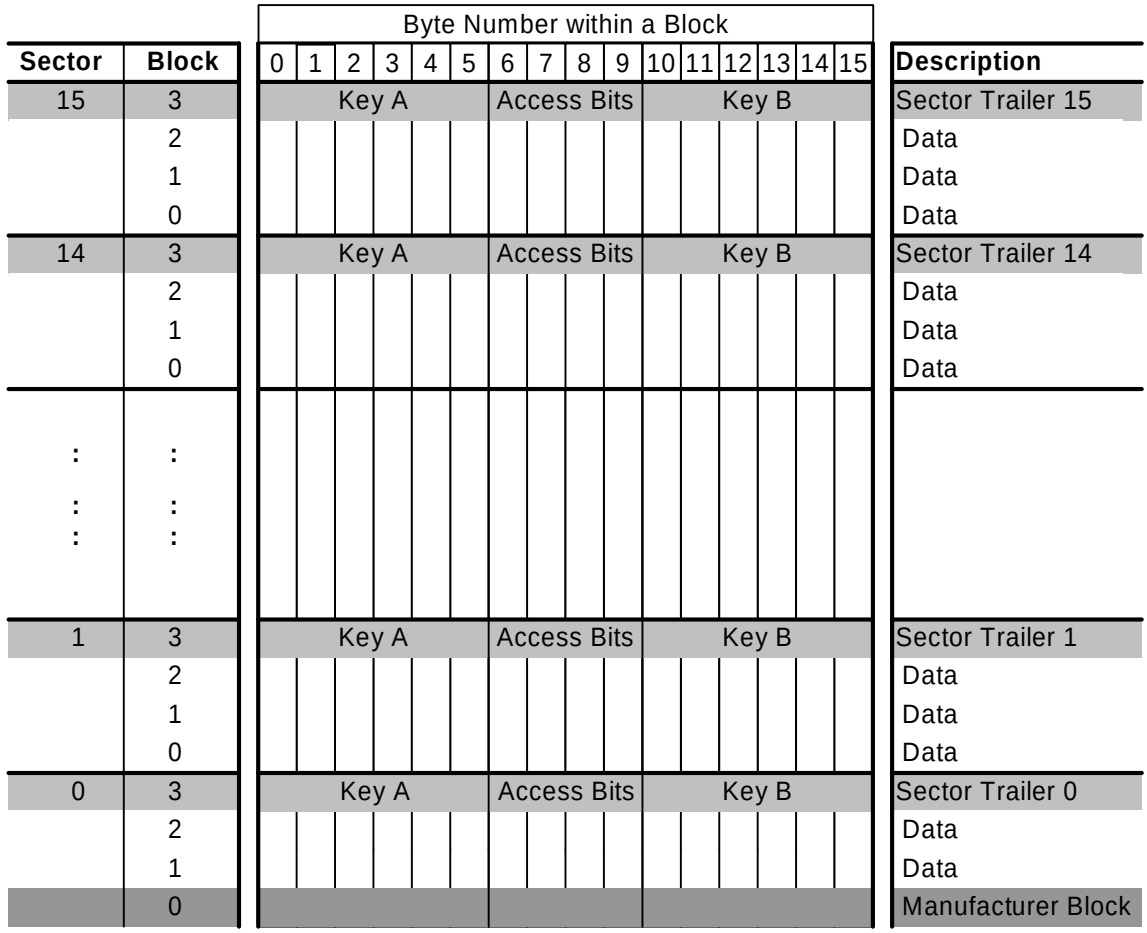


Fig 4. Memory organization

6.6.1 Manufacturer block

This is the first data block (block 0) of the first sector (sector 0). It contains the IC manufacturer data. Due to security and system requirements this block is write protected after having been programmed by the IC manufacturer at production.

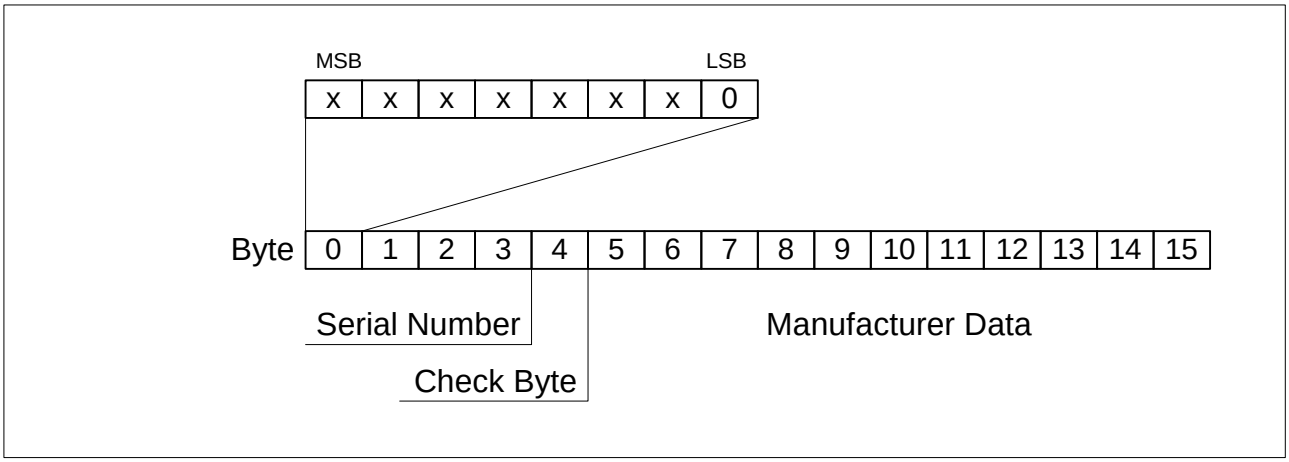


Fig 5. Manufacturer block

6.6.2 Data blocks

All sectors contain 3 blocks of 16 bytes for storing data (Sector 0 contains only two data blocks and the read-only manufacturer block).

The data blocks can be configured by the access bits as

- read/write blocks for e.g. contactless access control or
- value blocks for e.g. electronic purse applications, where additional commands like increment and decrement for direct control of the stored value are provided.

An authentication command has to be carried out before any memory operation in order to allow further commands.

6.6.2.1 Value Blocks

The value blocks allow to perform electronic purse functions (valid commands: read, write, increment, decrement, restore, transfer).The value blocks have a fixed data format which permits error detection and correction and a backup management.

A value block can only be generated through a write operation in the value block format:

- Value: Signifies a signed 4-byte value. The lowest significant byte of a value is stored in the lowest address byte. Negative values are stored in standard 2´s complement format. For reasons of data integrity and security, a value is stored three times, twice non-inverted and once inverted.

- Adr: Signifies a 1-byte address, which can be used to save the storage address of a block, when implementing a powerful backup management. The address byte is stored four times, twice inverted and non-inverted. During increment, decrement, restore and transfer operations the address remains unchanged. It can only be altered via a write command.

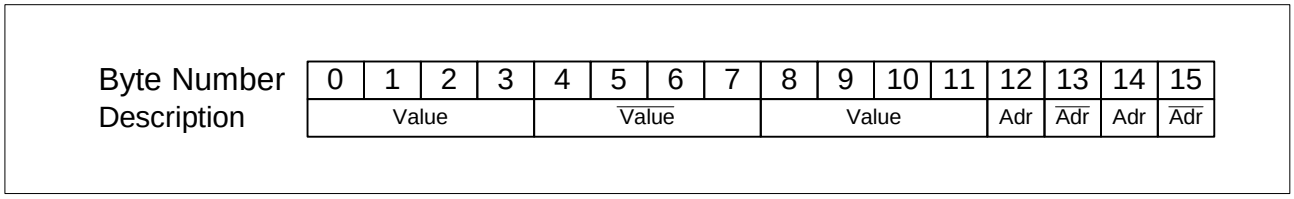


Fig 6. Value blocks

6.6.3 Sector trailer (block 3)

Each sector has a sector trailer containing the

- secret keys A and B (optional), which return logical “0”s when read and
- the access conditions for the four blocks of that sector, which are stored in bytes 6...9. The access bits also specify the type (read/write or value) of the data blocks.

If key B is not needed, the last 6 bytes of block 3 can be used as data bytes.

Byte 9 of the sector trailer is available for user data. For this byte apply the same access rights as for byte 6, 7 and 8.

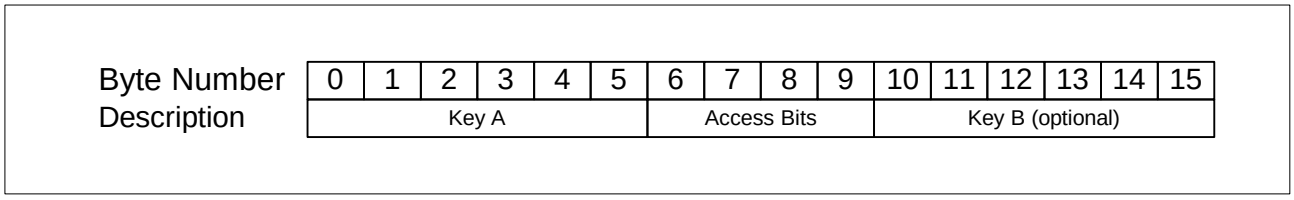


Fig 7. Sector trailer

6.7 Memory access

Before any memory operation can be carried out, the card has to be selected and authenticated as described previously.The possible memory operations for an addressed block depend on the key used and the access conditions stored in the associated sector trailer.

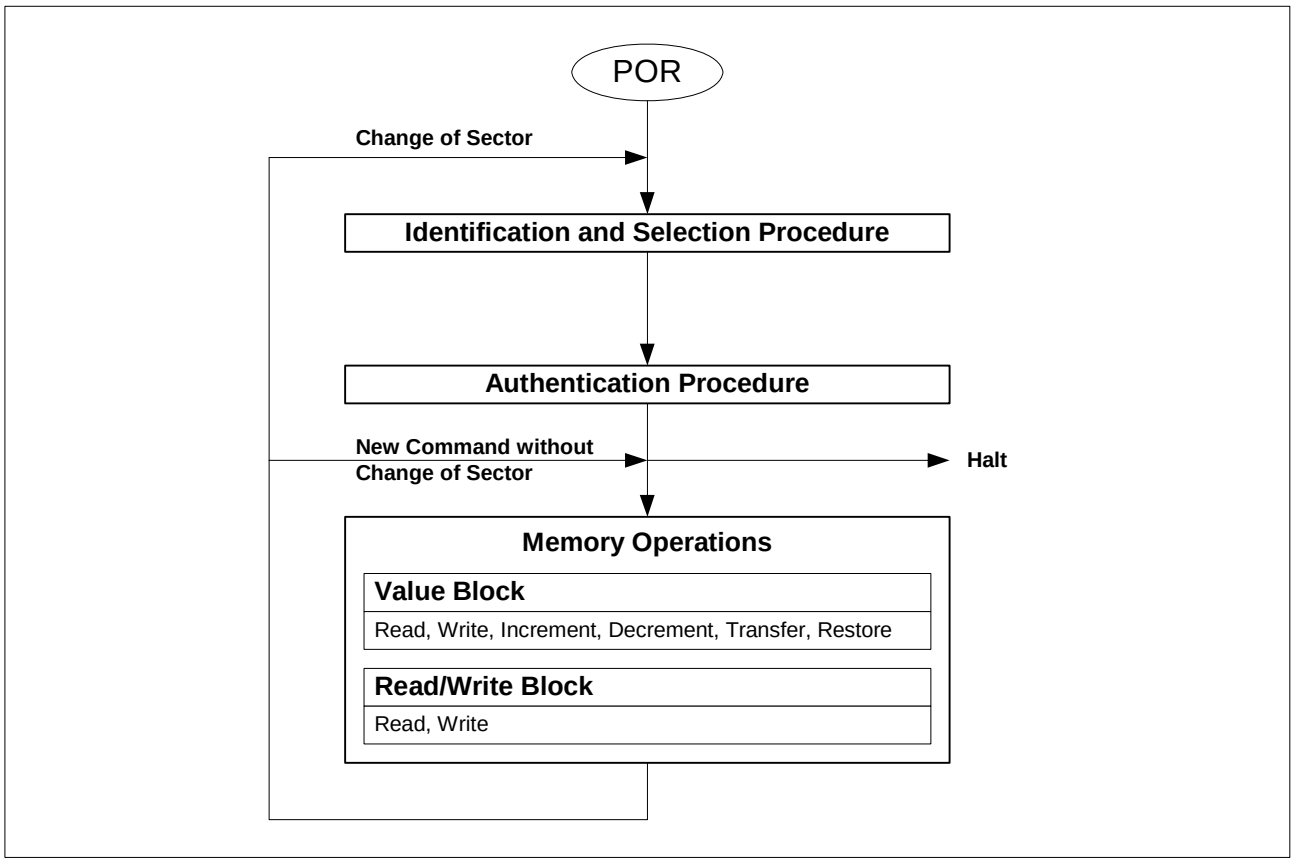


Fig 8. Memory access

Table 1. Memory Operations

Operation	Description	Valid for Block Type
Read	reads one memory block	read/write, value and sector trailer
Write	writes one memory block	read/write, value and sector trailer
Increment	increments the contents of a block and stores the result in the internal data register	value
Decrement	decrements the contents of a block and stores the result in the internal data register	value
Transfer	writes the contents of the internal data register to a block	value
Restore	reads the contents of a block into the internal data register	value

6.7.1 Access conditions

The access conditions for every data block and sector trailer are defined by 3 bits, which are stored non-inverted and inverted in the sector trailer of the specified sector.

The access bits control the rights of memory access using the secret keys A and B. The access conditions may be altered, provided one knows the relevant key and the current access condition allows this operation.

Remark: With each memory access the internal logic verifies the format of the access conditions. If it detects a format violation the whole sector is irreversible blocked.

Remark: In the following description the access bits are mentioned in the non-inverted mode only.

The internal logic of the MF1 IC S50 ensures that the commands are executed only after an authentication procedure or never.

Table 2. Access conditions

Access Bits	Valid Commands		Block	Description
$C1_3$ $C2_3$ $C3_3$	read, write	→	3	sector trailer
$C1_2$ $C2_2$ $C3_2$	read, write, increment, decrement, transfer, restore	→	2	data block
$C1_1$ $C2_1$ $C3_1$	read, write, increment, decrement, transfer, restore	→	1	data block
$C1_0$ $C2_0$ $C3_0$	read, write, increment, decrement, transfer, restore	→	0	data block

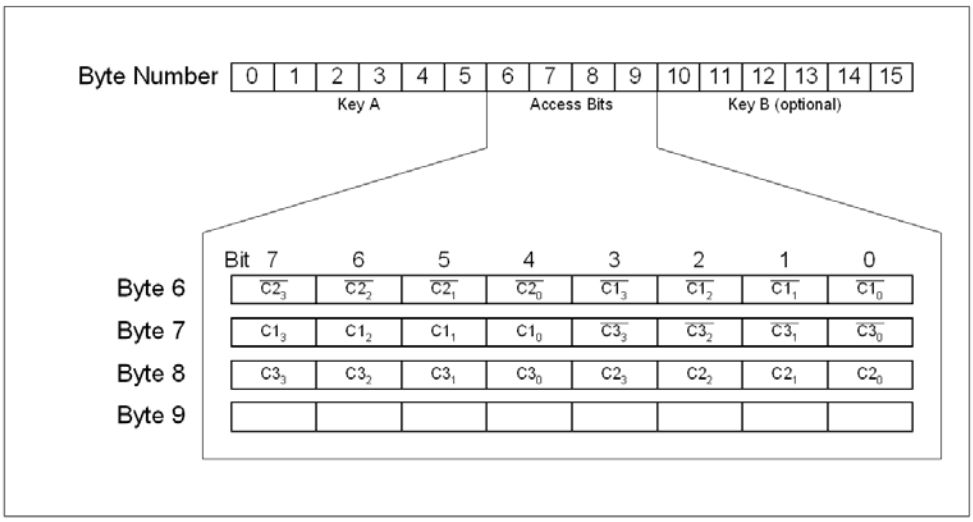


Fig 9. Access conditions

6.7.2 Access conditions for the sector trailer

Depending on the access bits for the sector trailer (block 3) the read/write access to the keys and the access bits is specified as ‘never’, ‘key A’, ‘key B’ or key A|B’ (key A or key B).

On chip delivery the access conditions for the sector trailers and key A are predefined as transport configuration. Since key B may be read in transport configuration, new cards must be authenticated with key A. Since the access bits themselves can also be blocked, special care should be taken during personalization of cards.

Table 3. Access conditions for the sector trailer

Access bits			Access condition for						Remark
			KEYA		Access bits		KEYB		
C1	C2	C3	read	write	read	write	read	write	
0	0	0	never	key A	key A	never	key A	key A	Key B may be read
0	1	0	never	never	key A	never	key A	never	Key B may be read
1	0	0	never	key B	key A|B	never	never	key B	
1	1	0	never	never	key A|B	never	never	never	
0	0	1	never	key A	key A	key A	key A	key A	Key B may be read, transport configuration
0	1	1	never	key B	key A|B	key B	never	key B	
1	0	1	never	never	key A|B	key B	never	never	
1	1	1	never	never	key A|B	never	never	never	

Remark: the grey marked lines are access conditions where key B is readable and may be used for data.

6.7.3 Access conditions for data blocks

Depending on the access bits for data blocks (blocks 0...2) the read/write access is specified as ‘never’, ‘key A’, ‘key B’ or ‘key A|B’ (key A or key B). The setting of the relevant access bits defines the application and the corresponding applicable commands.

- Read/write block: The operations read and write are allowed.
- Value block: Allows the additional value operations increment, decrement, transfer and restore. In one case (‘001’) only read and decrement are possible for a non-rechargeable card. In the other case (‘110’) recharging is possible by using key B.
- Manufacturer block: The read-only condition is not affected by the access bits setting!
- Key management: In transport configuration key A must be used for authentication[1]

1.If Key B may be read in the corresponding Sector Trailer it cannot serve for authentication (all grey marked lines in previous table). Consequences: If the RDW tries to authenticate any block of a sector with key B using grey marked access conditions, the card will refuse any subsequent access after authentication.

Table 4. Access conditions for data blocks

Access bits			Access condition for				Application
C1	C2	C3	read	write	increment	decrement, transfer, restore	
0	0	0	key A|B[1]	key A|B1	key A|B1	key A|B1	transport configuration
0	1	0	key A|B[1]	never	never	never	read/write block
1	0	0	key A|B[1]	key B[1]	never	never	read/write block
1	1	0	key A|B[1]	key B[1]	key B[1]	key A|B[1]	value block
0	0	1	key A|B[1]	never	never	key A|B[1]	value block
0	1	1	key B[1]	key B[1]	never	never	read/write block
1	0	1	key B[1]	never	never	never	read/write block
1	1	1	never	never	never	never	read/write block

[1] if Key B may be read in the corresponding Sector Trailer it cannot serve for authentication (all grey marked lines in previous table). Consequences: If the RWD tries to authenticate any block of a sector with key B using grey marked access conditions, the card will refuse any subsequent memory access after authentication.

7. Limiting values

See Delivery Type Addendum of Device

8. Recommended operating conditions

See Delivery Type Addendum of Device

9. Characteristics

See Delivery Type Addendum of Device

10. Support information

For additional information, please visit: **http://www.nxp.com**

11. Package outline

See Delivery Type Addendum of Device

12. Revision history

Table 5. Revision history

Document ID	Release date	Data sheet status	Change notice	Supersedes
	15 January 2007	Product data sheet		5.1
Modifications:	• The format of this data sheet has been redesigned to comply with the new identity guidelines of NXP Semiconductors. • Legal texts have been adapted to the new company name.			

13. Legal information

13.1 Data sheet status

Document status[1][2]	Product status[3]	Definition
Objective [short] data sheet	Development	This document contains data from the objective specification for product development.
Preliminary [short] data sheet	Qualification	This document contains data from the preliminary specification.
Product [short] data sheet	Production	This document contains the product specification.

[1] Please consult the most recently issued document before initiating or completing a design.

[2] The term 'short data sheet' is explained in section "Definitions".

[3] The product status of device(s) described in this document may have changed since this document was published and may differ in case of multiple devices. The latest product status information is available on the Internet at URL http://www.nxp.com.

13.2 Definitions

Draft — The document is a draft version only. The content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included herein and shall have no liability for the consequences of use of such information.

Short data sheet — A short data sheet is an extract from a full data sheet with the same product type number(s) and title. A short data sheet is intended for quick reference only and should not be relied upon to contain detailed and full information. For detailed and full information see the relevant full data sheet, which is available on request via the local NXP Semiconductors sales office. In case of any inconsistency or conflict with the short data sheet, the full data sheet shall prevail.

13.3 Disclaimers

General — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in medical, military, aircraft, space or life support equipment, nor in applications where failure or malfunction of a NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors accepts no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Limiting values — Stress above one or more limiting values (as defined in the Absolute Maximum Ratings System of IEC 60134) may cause permanent damage to the device. Limiting values are stress ratings only and operation of the device at these or any other conditions above those given in the Characteristics sections of this document is not implied. Exposure to limiting values for extended periods may affect device reliability.

Terms and conditions of sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at http://www.nxp.com/profile/terms, including those pertaining to warranty, intellectual property rights infringement and limitation of liability, unless explicitly otherwise agreed to in writing by NXP Semiconductors. In case of any inconsistency or conflict between information in this document and such terms and conditions, the latter will prevail.

No offer to sell or license — Nothing in this document may be interpreted or construed as an offer to sell products that is open for acceptance or the grant, conveyance or implication of any license under any copyrights, patents or other industrial or intellectual property rights.

13.4 Trademarks

Notice: All referenced brands, product names, service names and trademarks are the property of their respective owners.

Mifare — is a trademark of NXP B.V.

14. Contact information

For additional information, please visit: **http://www.nxp.com**

For sales office addresses, send an email to: **salesaddresses@nxp.com**

15. Tables

16. Figures

17. Contents

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 15 January 2007
Document identifier: 001052

DS-K3B530X Series Swing Barrier

User Manual

Legal Information

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (***https://www.hikvision.com***). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

- This product can only enjoy the after-sales service support in the country or region where the purchase is made.
- If the product you choose is a video product, please scan the following QR code to obtain the "Initiatives on the Use of Video Products", and read it carefully.

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR

IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Data Protection

- To protect data, the development of Hikvision Products incorporates privacy by design principles. For example, for Products with facial recognition features, biometrics data is stored in your Products with encryption method; for fingerprint Products, only fingerprint template will be saved, which is impossible to reconstruct a fingerprint image.
- As a data controller/processor, you may process personal data, including collection, storage, use, processing, disclosure, deletion, etc. You are advised to pay attention to and comply with applicable laws and regulations related to the protection of personal data, including without limitation, conducting security controls to safeguard personal data, such as, implementing reasonable administrative and physical security controls, conduct periodic reviews and the assessments of the effectiveness of your security controls.

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
FCC compliance: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
—Reorient or relocate the receiving antenna.
—Increase the separation between the equipment and receiver.
—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
—Consult the dealer or an experienced radio/TV technician for help
This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.
FCC Conditions
This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:
1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement

CE

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed

under the EMC Directive 2014/30/EU, RE Directive 2014/53/EU,the RoHS Directive 2011/65/EU

2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info

2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see:www.recyclethis.info

Safety Instruction

These instructions are intended to ensure that user can use the product correctly to avoid danger or property loss.

The precaution measure is divided into Dangers and Cautions:

Dangers: Neglecting any of the warnings may cause serious injury or death.

Cautions: Neglecting any of the cautions may cause injury or equipment damage.

⚠	⚠
Dangers: Follow these safeguards to prevent serious injury or death.	**Cautions:** Follow these precautions to prevent potential injury or material damage.

⚠ Danger:

- All the electronic operation should be strictly compliance with the electrical safety regulations, fire prevention regulations and other related regulations in your local region.
- Please use the power adapter, which is provided by normal company. The power consumption cannot be less than the required value.
- Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.
  If the top caps should be open and the device should be powered on for maintenance, make sure:
  1. Power off the fan to prevent the operator from getting injured accidentally.
  2. Do not touch bare high-voltage components.
  3. Make sure the switch's wiring sequence is correct after maintenance.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.
- When the product is installed on wall or ceiling, the device shall be firmly fixed.
- If smoke, odors or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.
- Do not ingest battery, Chemical Burn Hazard.
  This product contains a coin/button cell battery. If the coin/button cell battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death.
  Keep new and used batteries away from children. If the battery compartment does not close securely, stop using the product and keep it away from children. If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the device yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)

⚠ Cautions:

- Stainless steel may be corroded in some circumstances. You need to clean and care the device by using the stainless steel cleaner. It is suggested to clean the device every month.
- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).
- Do not place the device in extremely hot (refer to the specification of the device for the detailed operating temperature), cold, dusty or damp locations, and do not expose it to high electromagnetic radiation.
- The device cover for indoor use shall be kept from rain and moisture.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- Do not aim the device at the sun or extra bright places. A blooming or smear may occur otherwise (which is not a malfunction however), and affecting the endurance of sensor at the same time.
- Please use the provided glove when open up the device cover, avoid direct contact with the device cover, because the acidic sweat of the fingers may erode the surface coating of the device cover.
- Please use a soft and dry cloth when clean inside and outside surfaces of the device cover, do not use alkaline detergents.
- Please keep all wrappers after unpack them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage on the device and lead to additional costs.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.
- Biometric recognition products are not completely applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.
- Do not stay in the lane when the device is rebooting.
- RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS.
- SUITABLE FOR MOUNTING ON CONCRETE OR OTHER NON-COMBUSTIBLE SURFACE ONLY.
- The instructions shall require connection of the equipment protective earthing conductor to the installation protective earthing conductor.

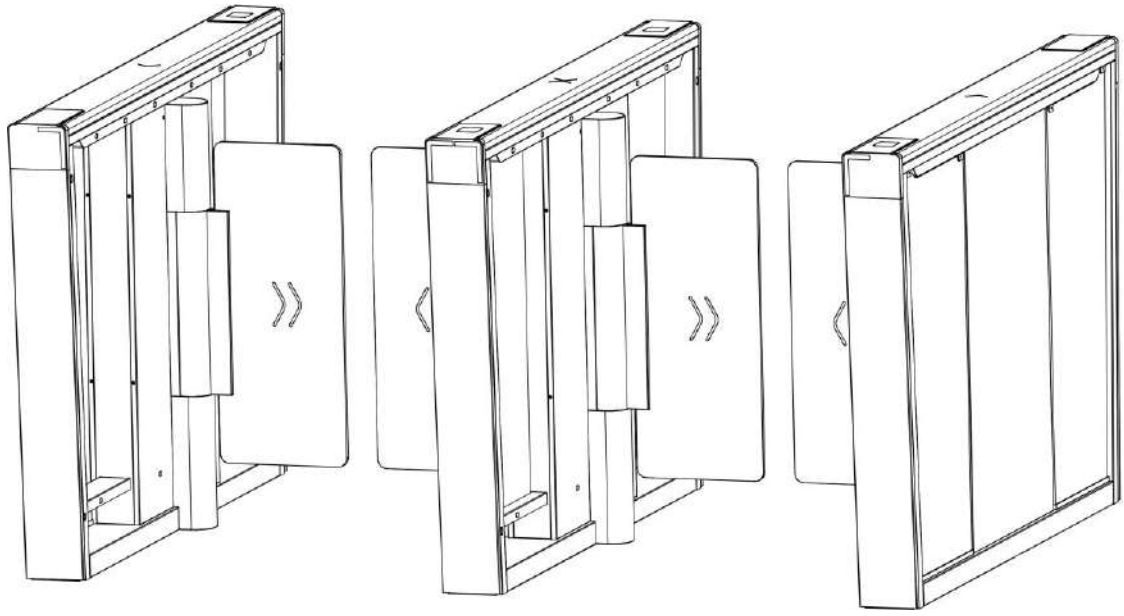
Available Models

Product Name	Model	Description
Swing Barrier	DS-K3B530LX-L/ DS-K3B530X-L DS-K3B530XM-L	Left Pedestal
	DS-K3B530LX-M/ DS-K3B530X-M DS-K3B530XM-M	Middle Pedestal
	DS-K3B530LX-R/ DS-K3B530X-R DS-K3B530XM-R	Right Pedestal

Contents

Chapter 1 Overview

1.1 Introduction



The Swing barrier with 14 IR lights is designed to detect unauthorized entrance or exit. By adopting the swing barrier integratedly with the access control system, person should authenticate to pass through the lane via swiping IC or ID card, scanning QR code, etc. It is widely used in attractions, stadiums, construction sites, residences, etc.

1.2 Main Features

- Supports control mode, inductive mode, free passing mode, remain open mode and remain closed mode in both entrance and exit direction.
- Anti-forced-accessing
  The barrier will react according to soft mode or guarding mode when confronting forced-accessing.
- Self-detection, self-diagnostics, and automatic alarm
- Audible and visual alarm will be triggered when detecting intrusion, tailgating, reverse passing, and climbing over barrier.
- LED indicates the entrance/exit and passing status
- Fire alarm passing
  When the fire alarm is triggered, the barrier will be open automatically for emergency evacuation.
- Valid passing duration settings

System will cancel the passing permission if a person does not pass through the lane within the valid passing duration.

- Bidirectional (Entrance/Exit) lane
  The barrier opening and closing speed can be configured according to the visitor flow.
- TCP/IP network communication
  The communication data is specially encrypted to relieve the concern of privacy leak.
- Permissions validation and anti-tailgating
- Remote barrier opening via keyfob and broadcasting via loudspeaker (custom broadcasting context is supported when installed with access control board).

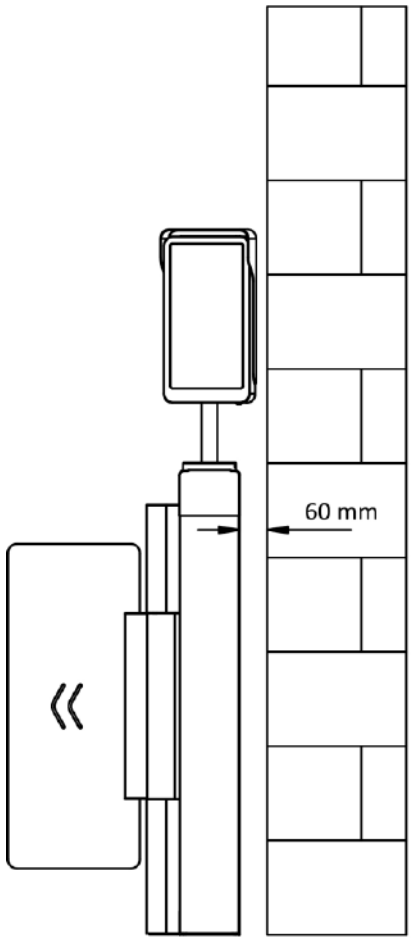
Chapter 2 System Wiring

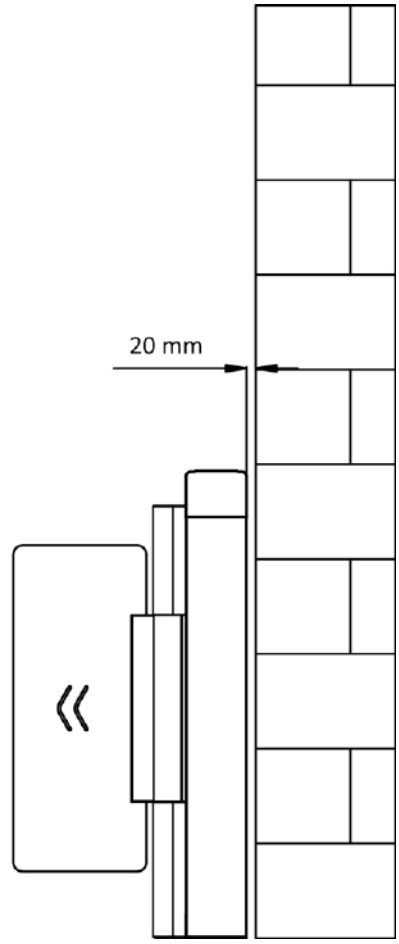
The preparation before installation and general wiring.

Steps

Note

- The device should be installed concrete surface or other flat non-flammable surface.
- If the installation area is too close to the wall, make sure the distance between the pedestal and the wall should be no less than 20 mm (60 mm if with face recognition terminals), or you cannot open the pedestal's top panel or might cause damage to devices.





- The dimension is as follows.

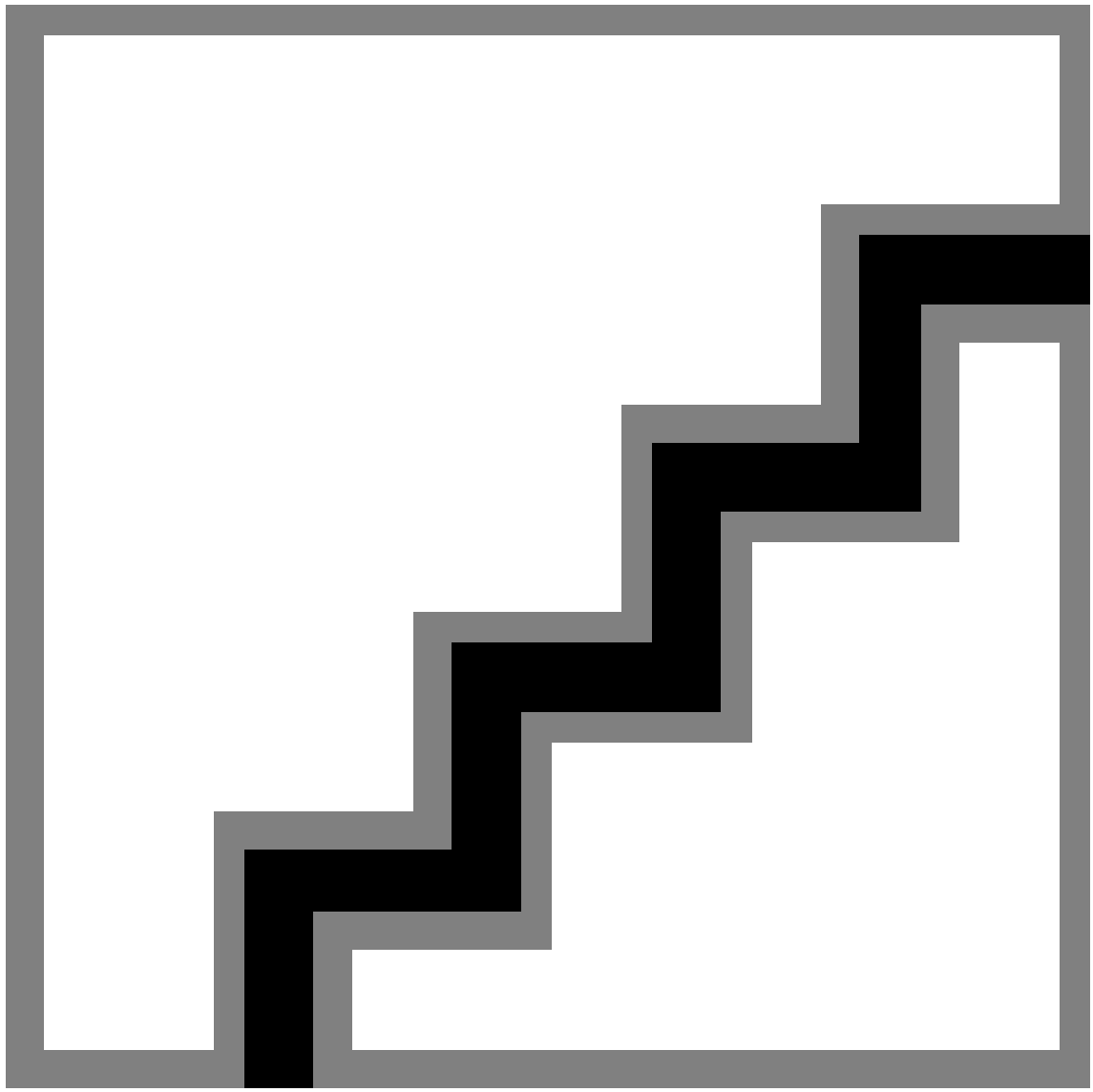


Figure 2-1 Dimension

1. Draw a central line on the installation surface of the left or right pedestal.
2. Draw other parallel lines for installing the other pedestals.

Note

The distance between the nearest two line is L + 272 mm. L represents the lane width.

3. Slot on the installation surface and dig installation holes. Put 4 expansion bolts of M12*120 for each pedestal.

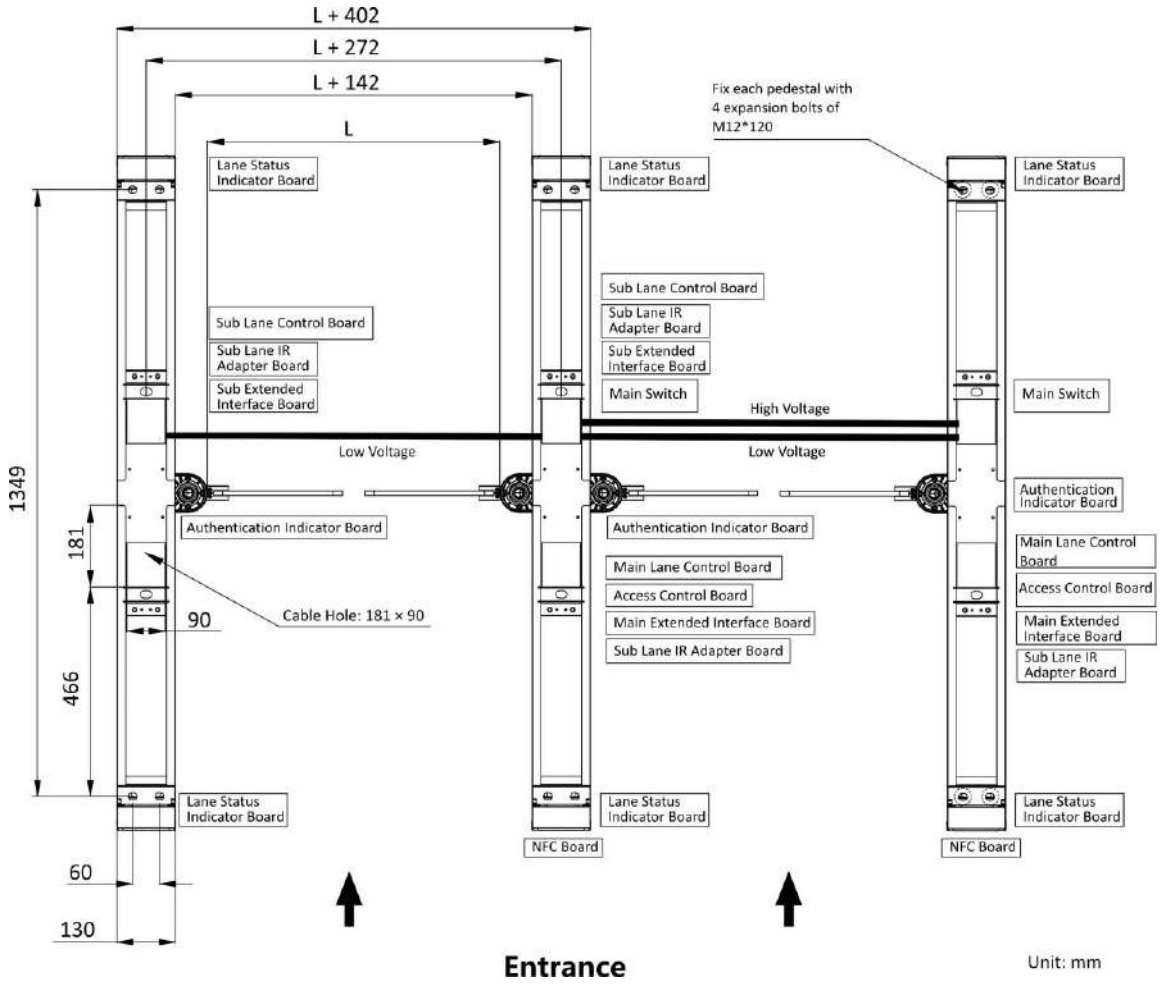


Figure 2-2 Hole Position and System Wiring

4. Bury cables. Each lane buries 1 high voltage cable and 1 low voltage cable. For details, see the system wiring diagram of step 3.

Note

- High voltage: AC power input
  Low voltage: interconnecting cable (communication cable and 24 V power cable) and network communication cable
- The supplied 24 V power cable length is 5 m and the communication cable length is 3 m.
- The suggested inner diameter of the low voltage conduit is larger than 30 mm.
- If you want to bury both of the AC power cord and the low voltage cable, the two cables should be in separated conduits to avoid interference.
- If more peripherals are required to connect, you should increase the conduit diameter or bury another conduit for the external cables.
- The external AC power cord should be double-insulated.
- The network cable must be CAT5e or the network cable has better performance.

Chapter 3 Install Pedestals

Before You Start

Prepare for the installation tools, check the device and the accessories, and clear the installation base.

Steps

Note

- The device should be installed on the concrete surface or other flat non-flammable surfaces.
- Make sure the device is powered off during installation and other operations.
- The installation tools are put inside the package of the pedestal.

1. Prepare for the installation tools, check the components, and prepare for the installation base.
2. Remove 4 screws of each pedestal that fix the 2 side panels.

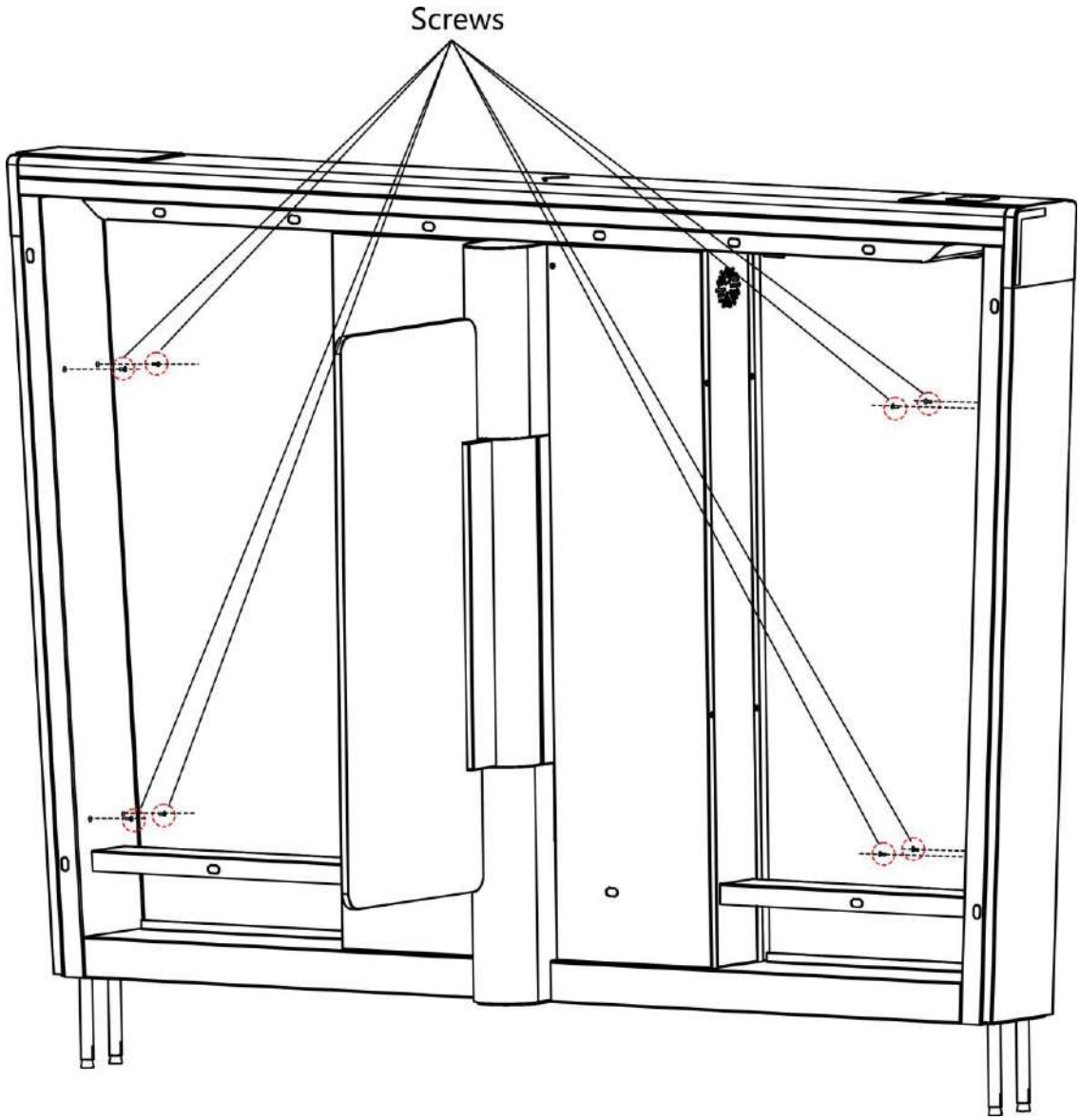


Figure 3-1 Remove Side Panel Screws

3. Remove the side panels and move the pedestals to the corresponded positions according to the entrance and exit marks on the pedestals.

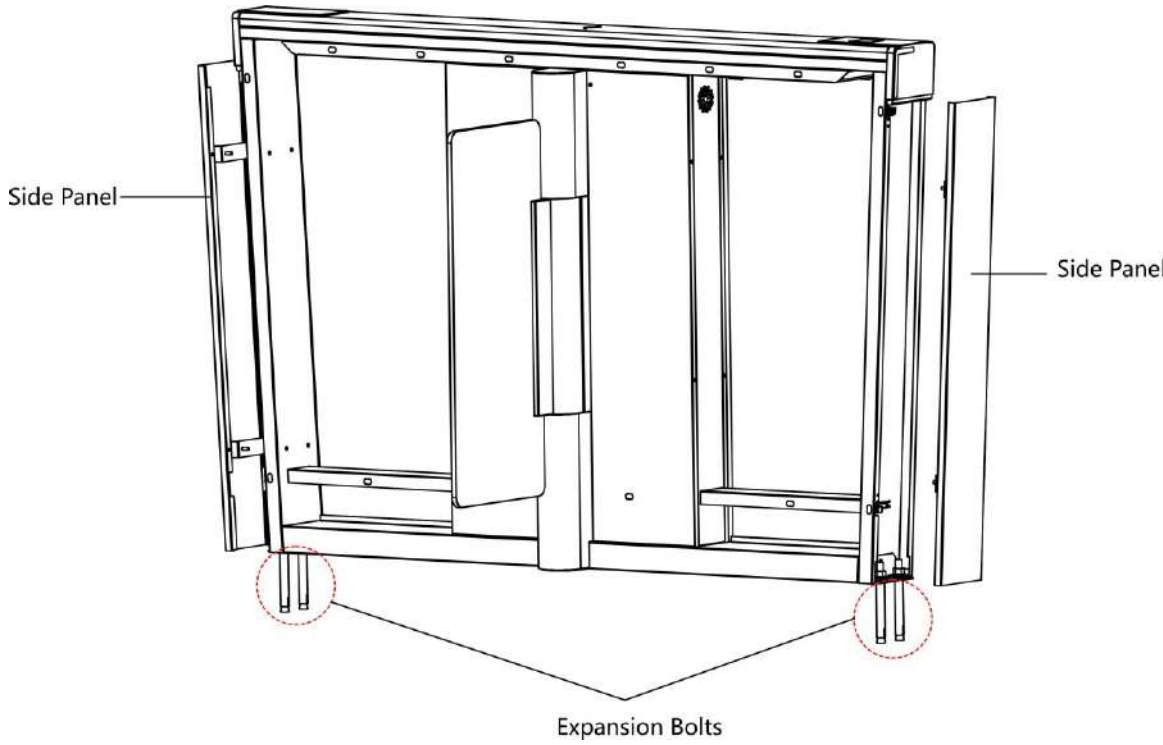


Figure 3-2 Remove Side Panel Screws

Note

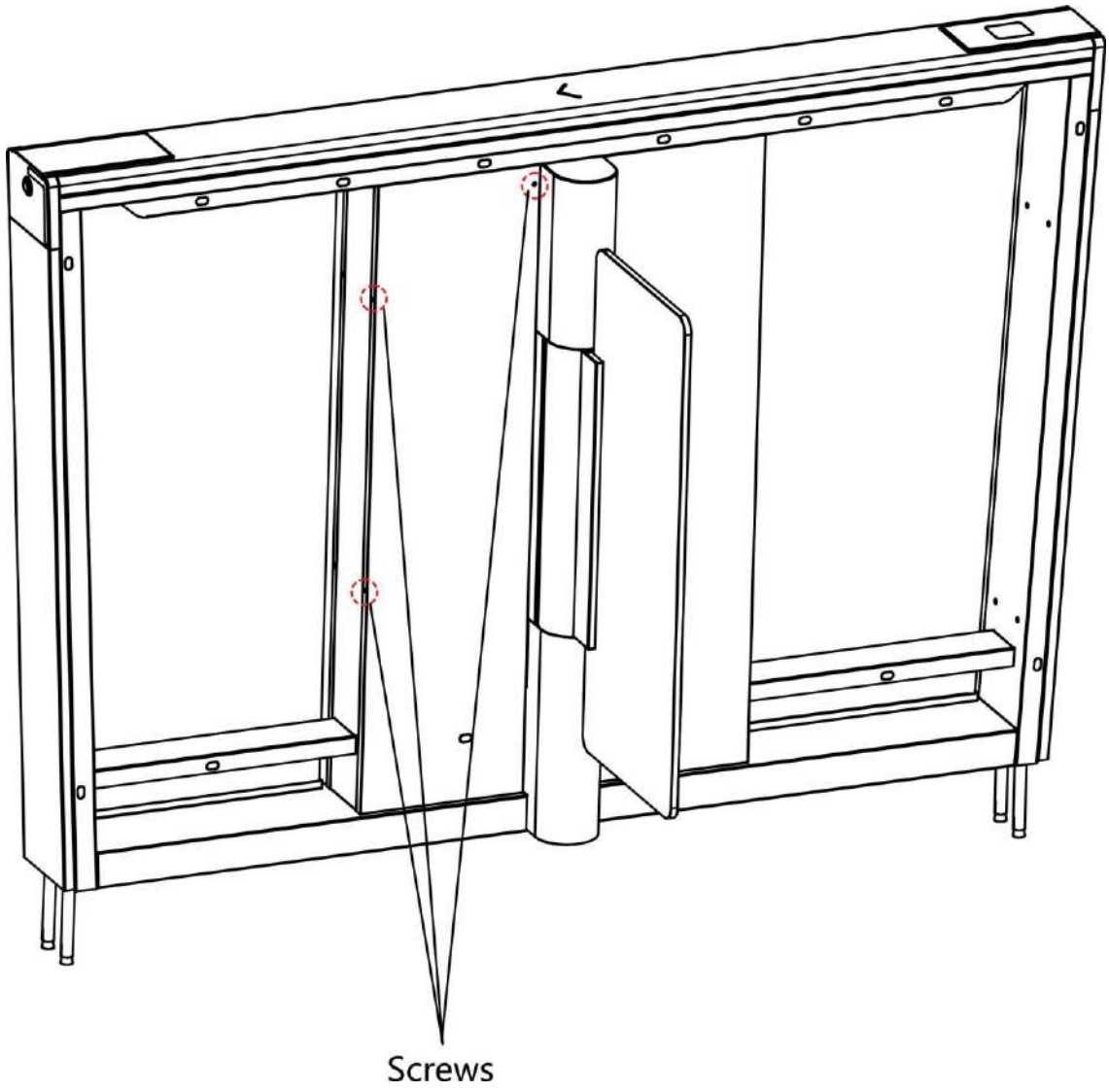
For detailed information about system wiring, see ***System Wiring*** .

4. Secure the pedestals with expansion bolts and fix the side panels to its original position with screws.

Note

- Do not immerse the pedestal in the water. In special circumstances, the immersed height should be no more than 150 mm.

5. Remove 3 screws to open each maintenance door for cable wiring.


Screws

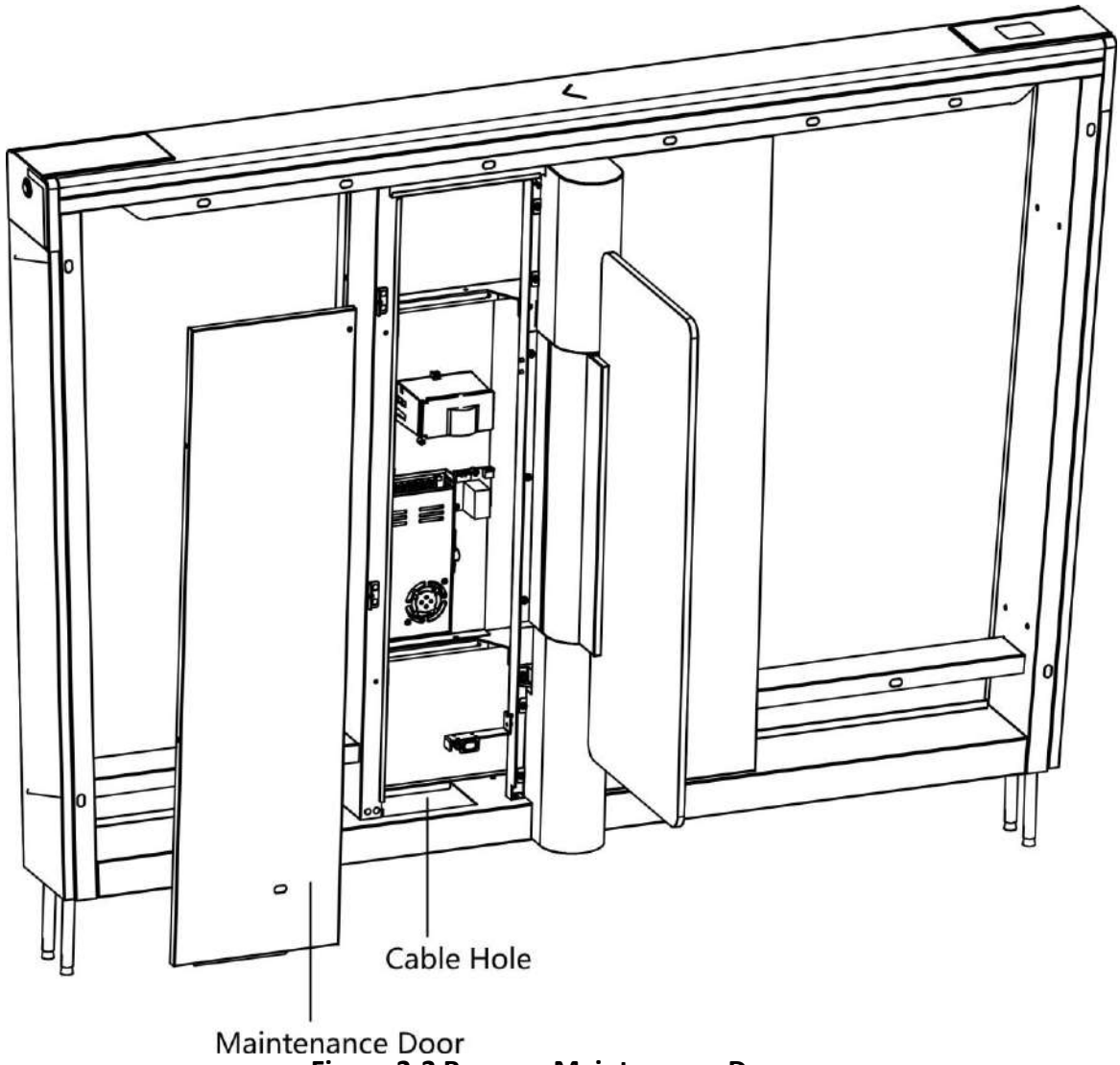


Figure 3-3 Remove Maintenance Door

Note

For detailed information about cables, see ***General Wiring*** .

Chapter 4 General Wiring

Note

- When you should maintain or disassemble the high voltage modules, you should remove the entire high voltage modules and maintain it outside the turnstile. You should unplug the cables that connected to the peripherals before maintenance to avoid destroy of the device.
- When disassembling the high voltage module, you should disconnect the power to avoid injury.
- If only wiring is needed without maintenance, do not remove the high voltage modules.
- The switch and the main lane control board are already connected. The 14 AWG cable to connect between the AC electric supply and the switch should be purchased separately.
- 2 interconnecting cables are supplied: 24 V Power Cable and Communication Cable.
  24 V Power Cable: 5 m long, which is in the middle and right pedestal.
  Communication Cable: 4 m long, CAT5e, which is in the package of middle and right pedestal.

4.1 Components Introduction

By default, basic components of the turnstile are connected well. The pedestals can communicate by wiring the interconnecting cables. And the turnstile supports wiring the AC electric supply for the whole system's power supply.

Note

The voltage fluctuation of the electric supply is between 100 VAC and 240 VAC, 50 to 60 Hz.

The picture displayed below describes the serial port on the entrance and exit direction.

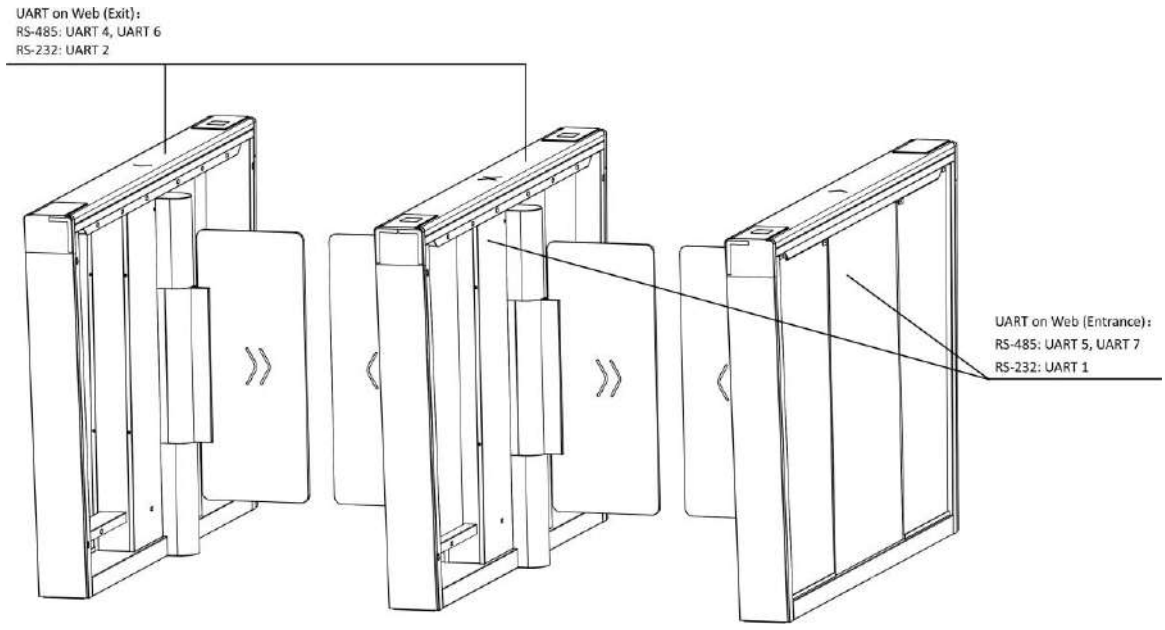


Figure 4-1 Serial Port

The picture displayed below describes the IR sending/receiving module and their corresponding number on the pedestal.

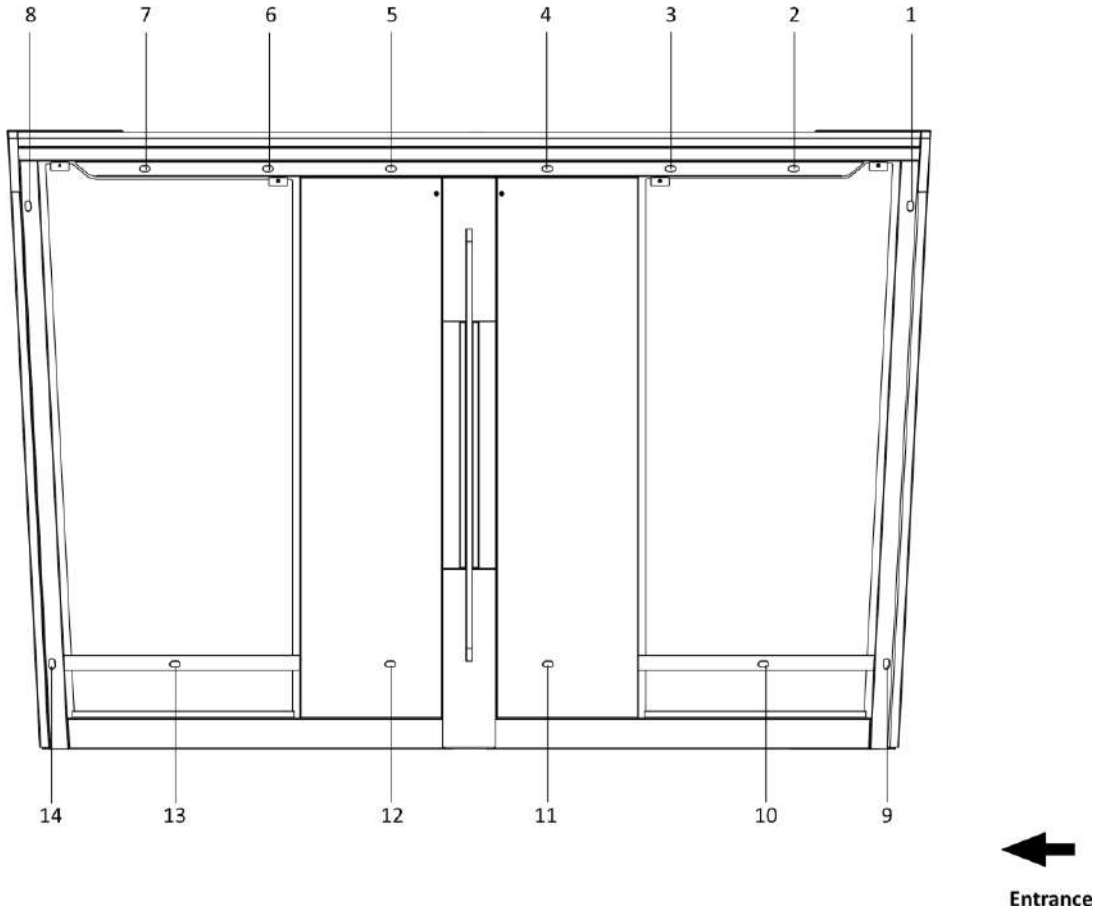


Figure 4-2 IR Sending/Receiving Module Position

Note

Standing at the entrance position in the lane, the IR modules on your left are the IR sending modules, the ones on your right are the IR receiving modules.

4.2 Wiring

Scan the QR code to watch the guide video.

4.3 Terminal Description

4.3.1 General Wiring

The general wiring of lane control board, access control board and extended interface board.

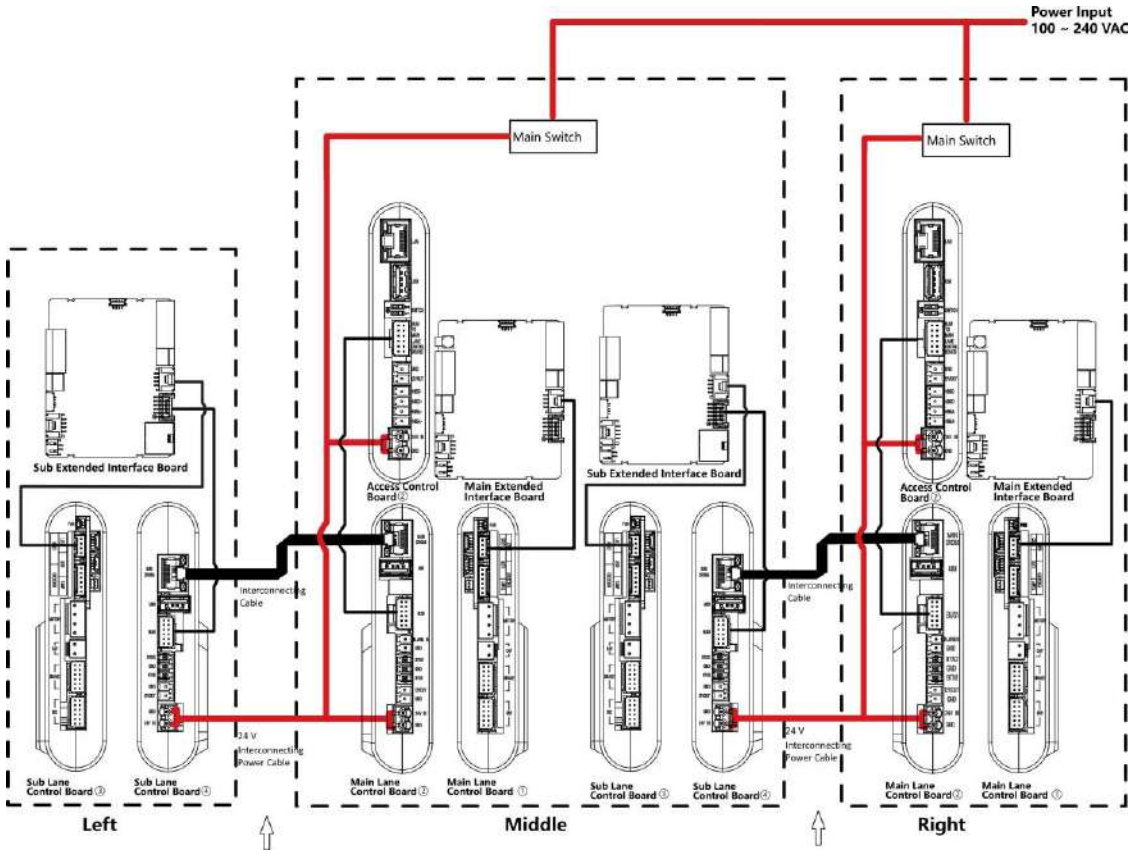


Figure 4-3 General Wiring

Note

- The power cable from power supply to the main lane control board has been connected. You will need to prepare the 14AWG power cable to connect the AC power input to power supply.
- The supplied 2 interconnecting cables need connecting on-site:
  1. 24 V power cable of 14 AWG. The cable is 5 m in length and put inside the right/middle pedestal at the exit.
  2. CAT5e Communication cable. The cable is 3 m in length and put inside the package of the right/middle pedestal.
- The ① and ② or ③ and ④ refer to the two sides of a same board.
- Barrier opens at the entrance/exit: connect to BTN1/BTN2 and GND.

4.3.2 Main Lane Control Board Terminal Description

The main lane control board contains interconnecting interface, access control board interface, fire input interface, exit button interface, 12 VDC output interface, 24 VDC input interface, fan interface, communication interface, encoder interface, power supply interface for motor, supercapacitor interface, main brake interface, adaptor interface and tamper interface.

The picture displayed below is the main lane control board diagram.

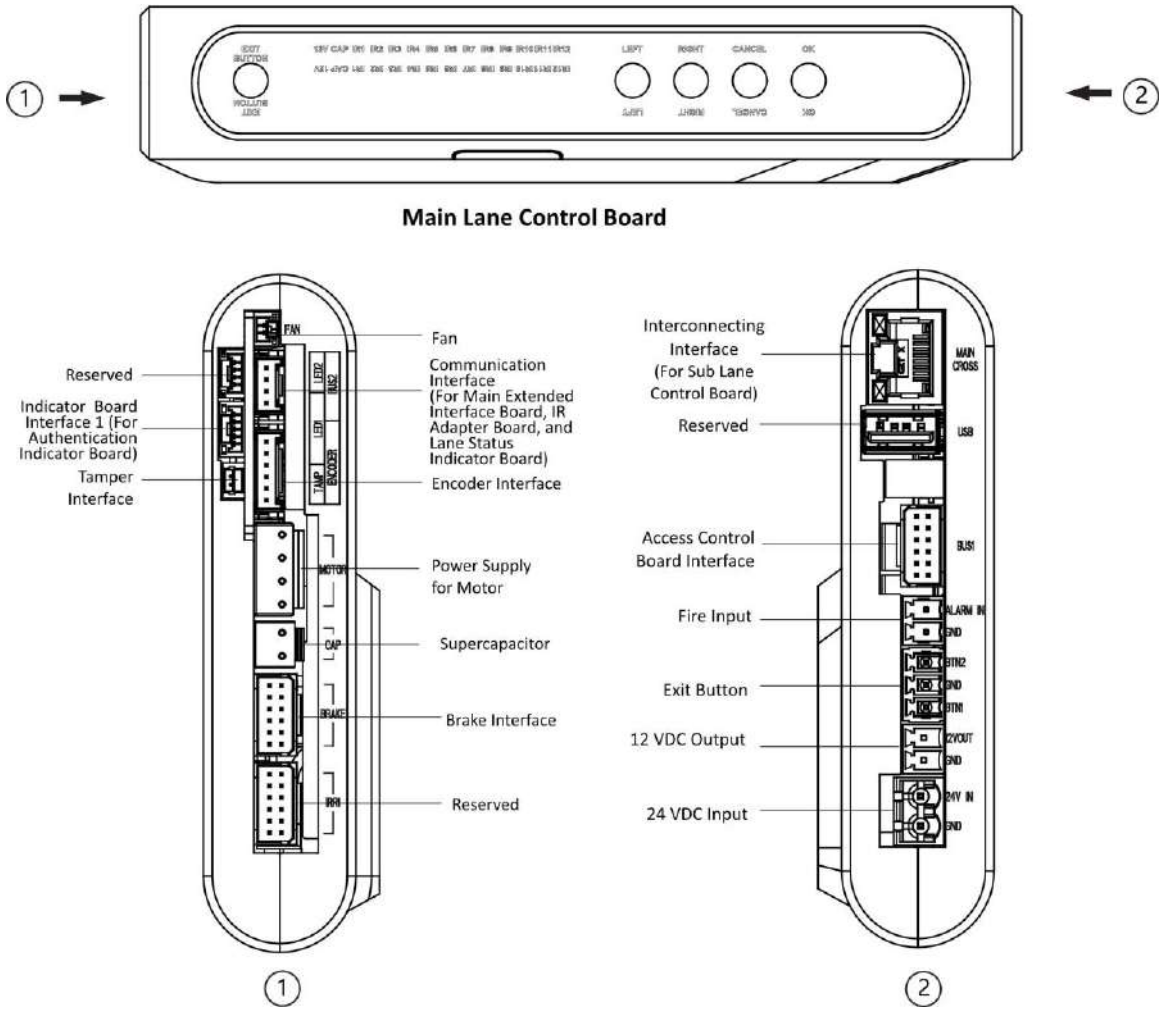


Figure 4-4 Main Lane Control Board Terminals

4.3.3 Sub Lane Control Board Terminal Description

The sub lane control board contains interconnecting interface, BUS interface, exit button interface, 12 VDC output interface, 24 VDC input interface, fan interface, communication interface, encoder interface, power supply interface for motor, supercapacitor interface, sub brake interface, adaptor interface and tamper interface.

The picture displayed below is the sub lane control board diagram.

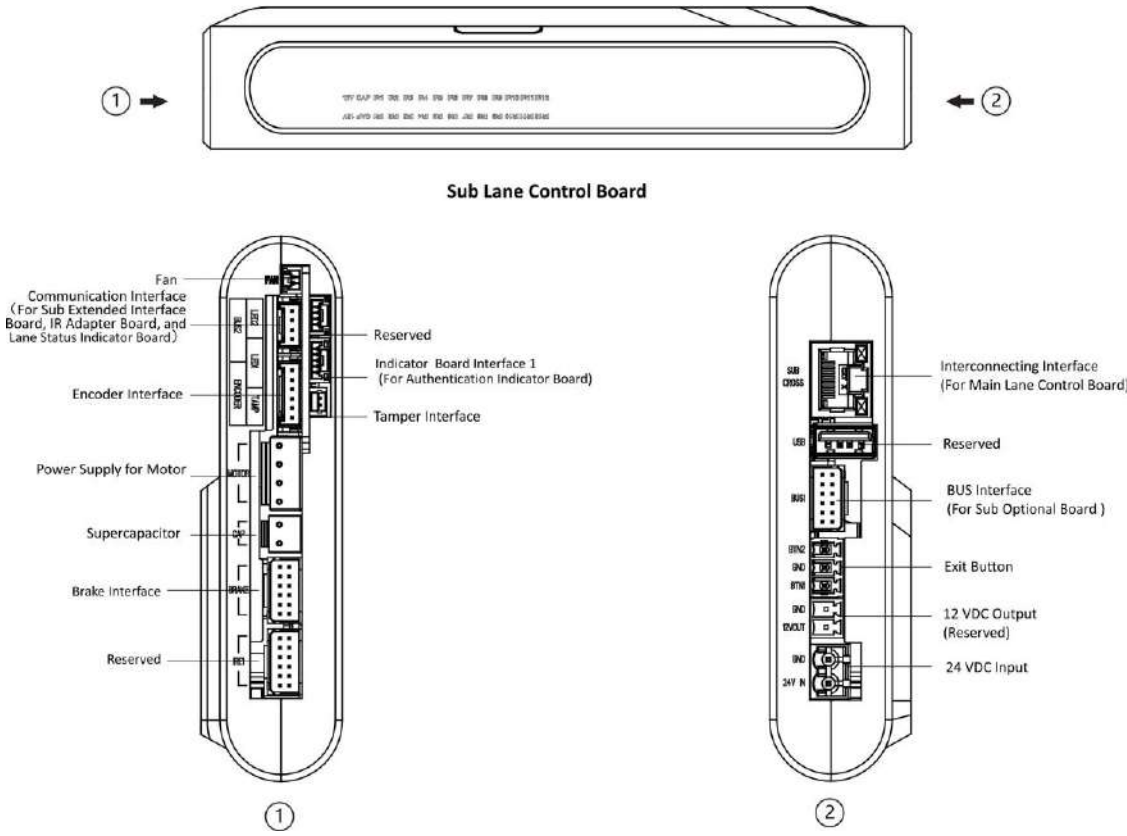


Figure 4-5 Sub Lane Control Board Terminals

4.3.4 Access Control Board Terminal Description (Optional)

Access control board is mainly used for authority identification in places with high security levels such as public security or judicial place, external device accessing, and communication with the upper platform and lane controller.

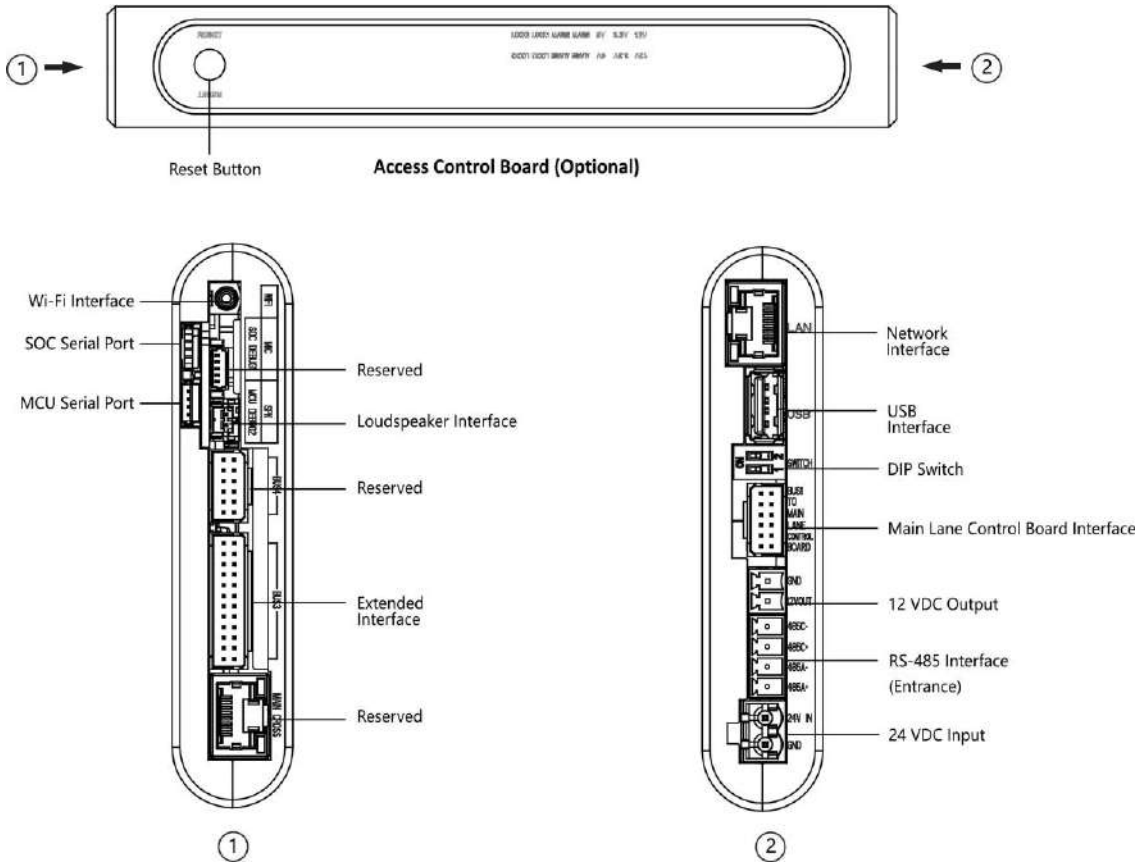


Figure 4-6 Access Control Board

Note

- RS-485A corresponds to port 5 on web and is for QR code scanner connection at entrance by default; RS-485C corresponds to port 7 on web and is for card reader connection at entrance by default.
- The SOC and MCU serial port are for maintenance and debugging use only.
- Press the Reset button for 5 s and the device will start to restore to factory settings.
- The DIP switch is for study mode setting and keyfob paring. For detailed information about the DIP switch, see *DIP Switch Description*.

The wiring diagram of extended interface of access control board is shown as follows.

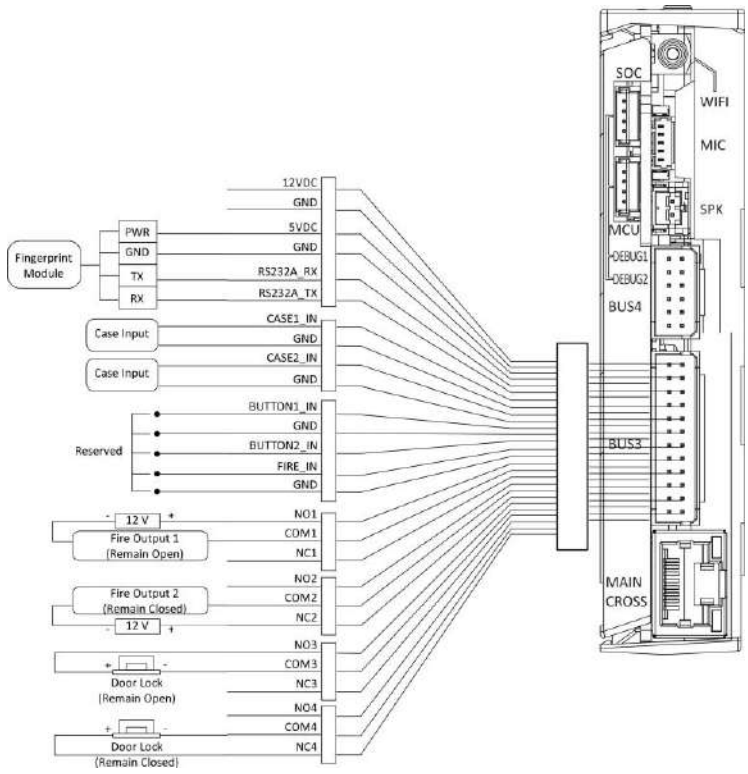


Figure 4-7 Wring Diagram of BUS3 Interface

Note

RS-232A corresponds to port 1 on web.

4.3.5 Main Extended Interface Board Terminal Description

The main extended interface board contains the sub-1G antenna interface, barrier light interface, loudspeaker interface, debugging port, Wiegand/exit button interface, 5 VDC output and communication interface.

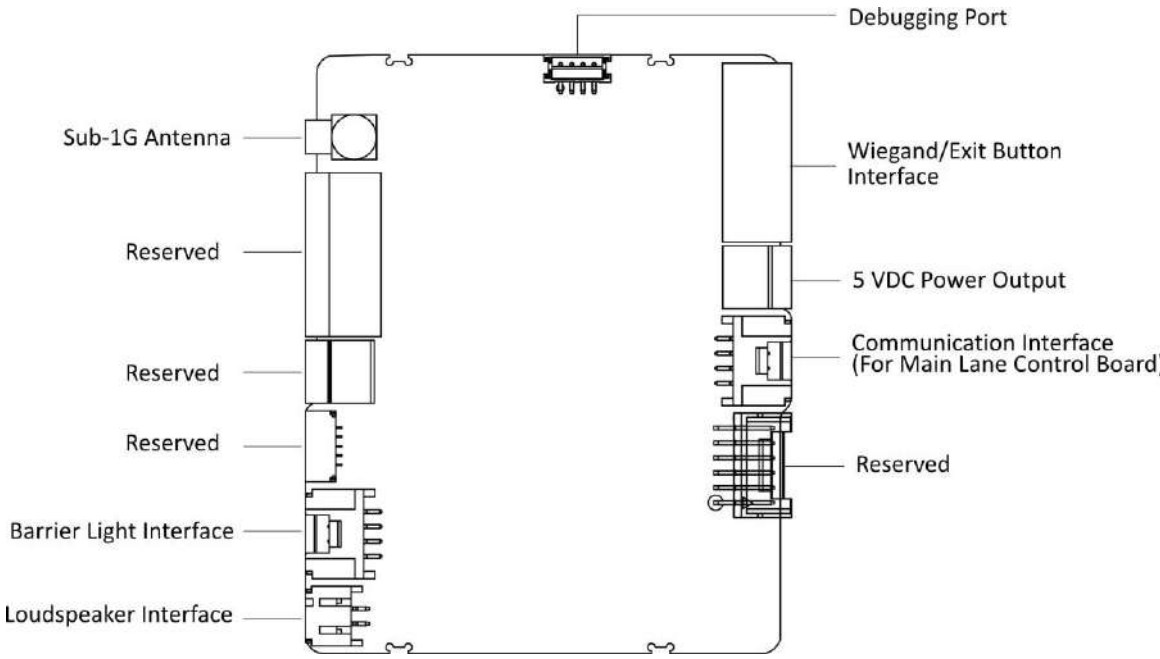


Figure 4-8 Main Extended Interface Board Terminal

Note

When the device is installed with access control board, the loudspeaker shall be connected to the access control board. If not, the loudspeaker shall be connected to the main extended interface board.

4.3.6 Card Reader Board Terminal Description

The card reader board can be connected to the access control board via RS-485 interface.

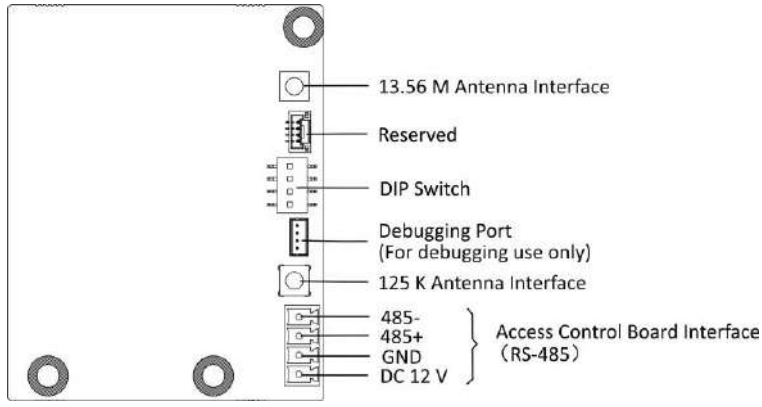


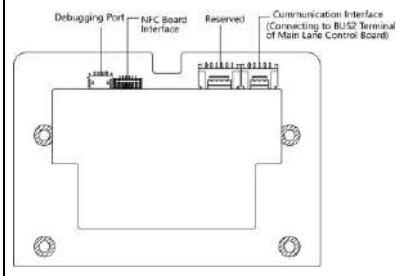
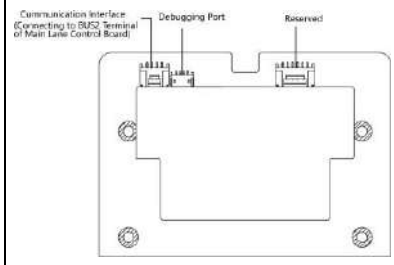
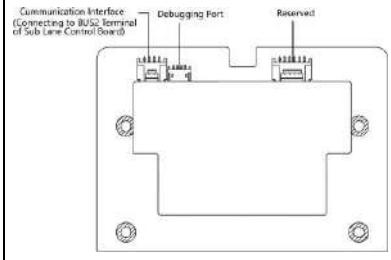
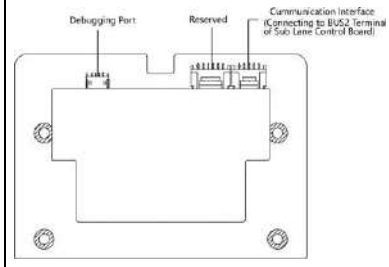
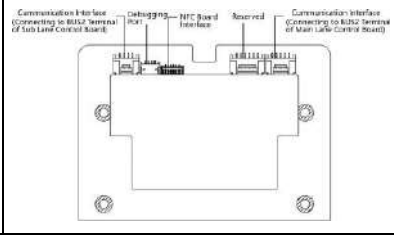
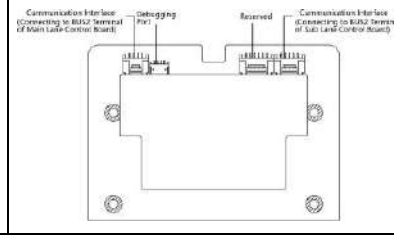
Figure 4-9 Card Reader Board

4.3.7 Lane Status Indicator Board

For details about lane status indicator position, see .

Lane status indicator board in different pedestals are shown as follows.

Table 4-1 Lane Status Indicator Board

Pedestal	Entrance	Exit
Right Pedestal		
Left Pedestal		
Middle Pedestal		

4.3.8 Authentication Indicator Board Terminal Description

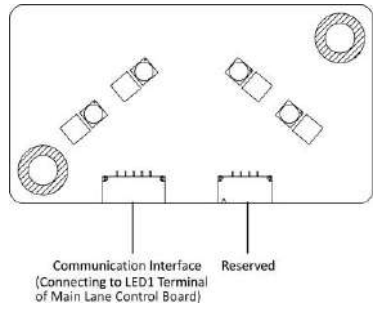


Figure 4-10 Authentication Indicator Board

The authentication indicator board is connected to the LED1 terminal of main lane control board.

4.3.9 RS-485 Wiring

The RS-485 interfaces on the access control board and sub extended interface board are suggested to connect with the face recognition module or the card reader. Here takes connecting with a card reader as an example.

Note

- There are 2 RS-485 interfaces on the access control board for entrance. Refer to ***Access Control Board Terminal Description (Optional)*** for details.
  There are 2 RS-485 interfaces on the sub extended interface board for exit. Refer to for details.
- If connecting the RS-485 with a card reader, by default, the DIP switch of the card reader should be set as follows:
  - For entrance, set the No.1 of the 4-digit DIP switch to ON side.
  - For exit, set the No.3 of the 4-digit DIP switch to ON side.
- If there are other RS-485 devices connecting, the ID of the RS-485 cannot be conflicted.
- The connected 12 V power interface for the face recognition terminal cannot be connected with other 12 V devices.

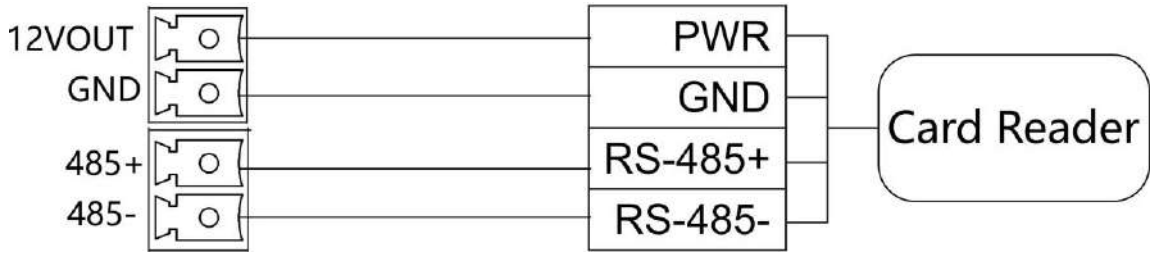


Figure 4-11 Wiring RS-485

4.3.10 RS-232 Wiring

Note

- There is 1 RS-232 interface on the extended interface of access control board, see ***Access Control Board Terminal Description (Optional)*** . The RS-232A corresponds to UART 1 on web.
- There is 1 RS-232 interface on the sub extended interface board, see . The RS-232B corresponds to UART 2 on web.
  The RS-232C interface is reserved.

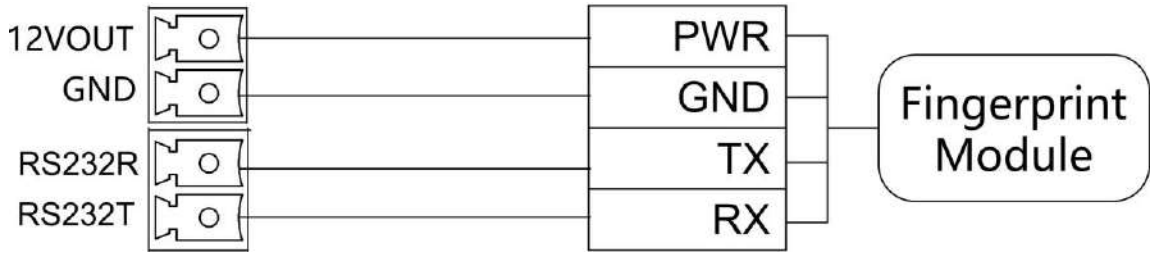


Figure 4-12 RS-232 Wiring

4.3.11 Alarm Input Wiring

On the main lane control board, you can wire the fire alarm input interface.

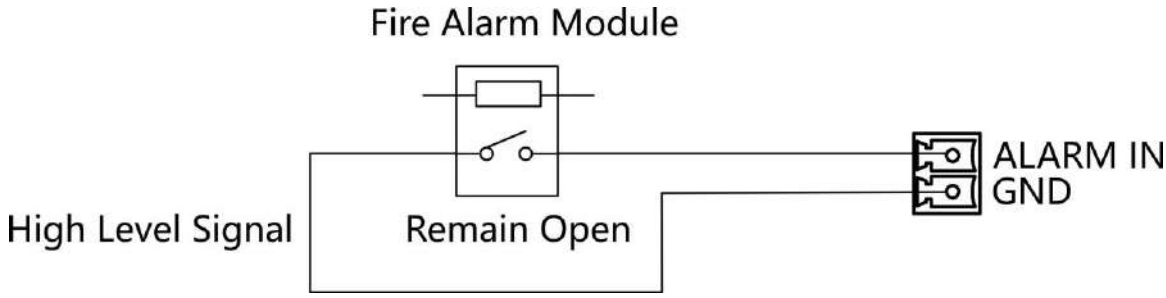


Figure 4-13 Remaining Open

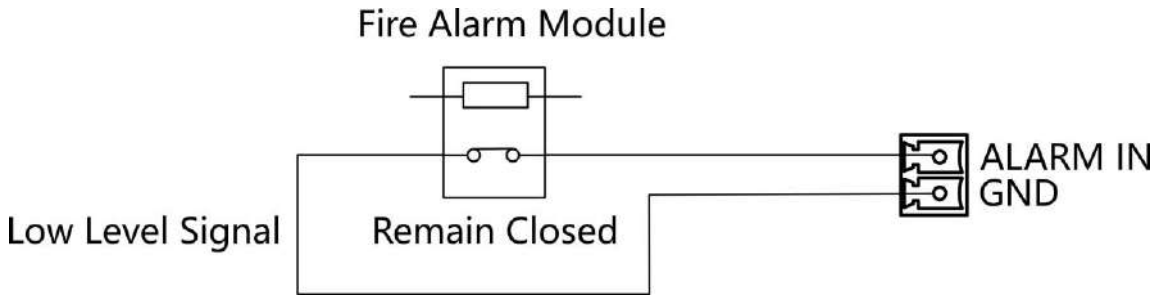


Figure 4-14 Remaining Closed

4.3.12 Exit Button Wiring

The main and sub lane control board each has 1 button interface, which can be connected to exit button or face recognition device.

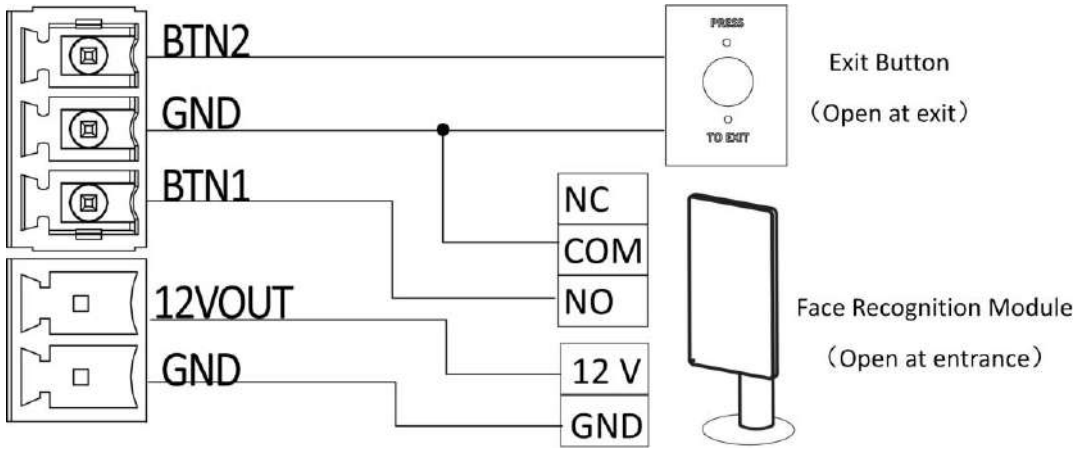


Figure 4-15 Exit Button Wiring

Note

- The face recognition devices are powered via 12 VDC power output interface of the main and sub lane control board.
- Barrier open at the entrance: connect to BTN1 and GND.
- Barrier open at the exit: connect to BTN2 and GND.

4.4 Device Settings via Button

You can configure the device via button on the main lane control board or the DIP switch on the access control board.

Function	Main Lane Control Board & Loudspeaker (Connected to Main Extended Interface Board)	Main Lane Control Board & Access Control Board & Loudspeaker (Connected to Access Control Board)
Working Mode		
Normal/Study Mode	Configure via button (refer to ***Set Study Mode via Button***)	Configure via DIP switch (refer to ***Set Study Mode via DIP Switch (Optional)***)
keyfob Pairing	Configure via button (refer to ***Pair Keyfob via Button***)	Configure via DIP switch (refer to ***Pair Keyfob via DIP Switch (Optional)***)
Passing Mode	Configure via button	Configure via button/web

Function	Main Lane Control Board & Loudspeaker (Connected to Main Extended Interface Board)	Main Lane Control Board & Access Control Board & Loudspeaker (Connected to Access Control Board)
Memory Mode	Configure via button	Configure via button/web
Control Mode	Configure via button	Configure via button/web
Application Mode	Configure via button	Configure via button
Parameter Settings		
Barrier Opening Speed	Configure via button	Configure via button/web
Barrier Closing Speed	Configure via button	Configure via button/web
Card Reading on the Alarm Area	Configure via button	Configure via button/web
Enter Duration	Configure via button	Configure via button/web
Exit Duration	Configure via button	Configure via button/web
IR Sensing Duration	Configure via button	Configure via button/web
Intrusion Duration	Configure via button	Configure via button/web
Overstay Duration	Configure via button	Configure via button/web
Delay Time for Barrier Closing	Configure via button	Configure via button/web
Barrier Recover Duration	Configure via button	Configure via button
Volume Adjustment	Configure via button	Configure via button
Barrier Material	Configure via button	Configure via button/web
Barrier Length	Configure via button	Configure via button/web
Barrier Height	Configure via button	Configure via button/web
Brake	Configure via button	Configure via button
Brake Angle	Configure via button	Configure via button
IR Sensing	Configure via button	Configure via button/web
Fan	Configure via button	Configure via button
Light Brightness	Configure via button	Configure via button/web
Restore to Default	Configure via button	Configure via button/web
Voice Prompt		

Function	Main Lane Control Board & Loudspeaker (Connected to Main Extended Interface Board)	Main Lane Control Board & Access Control Board & Loudspeaker (Connected to Access Control Board)
Climbing over Barrier	Enable or disable via button	Enable or disable via button
Reverse Passing	Enable or disable via button	Enable or disable via button
Exceeding Passing Duration	Enable or disable via button	Enable or disable via button
Intrusion Alarm	Enable or disable via button	Enable or disable via button
Tailgating Alarm	Enable or disable via button	Enable or disable via button
Overstaying Alarm	Enable or disable via button	Enable or disable via button
Motor Inspection	Configure via button	Configure via button
Self-check Voice Prompt	Enable or disable via button	Enable or disable via button
Study Mode Voice Prompt	Enable or disable via button	Enable or disable via button

Note

- Refer to ***Button Configuration Description*** for detailed information.
- If the device is not equipped with access control board, the loudspeaker shall be connected to the main extended interface board.
- If the device is equipped with access control board, the loudspeaker shall be connected to the access control board. You can set custom broadcasting context via web. For details, see ***Prompt Schedule*** .

4.4.1 Configuration via Button

Button Description

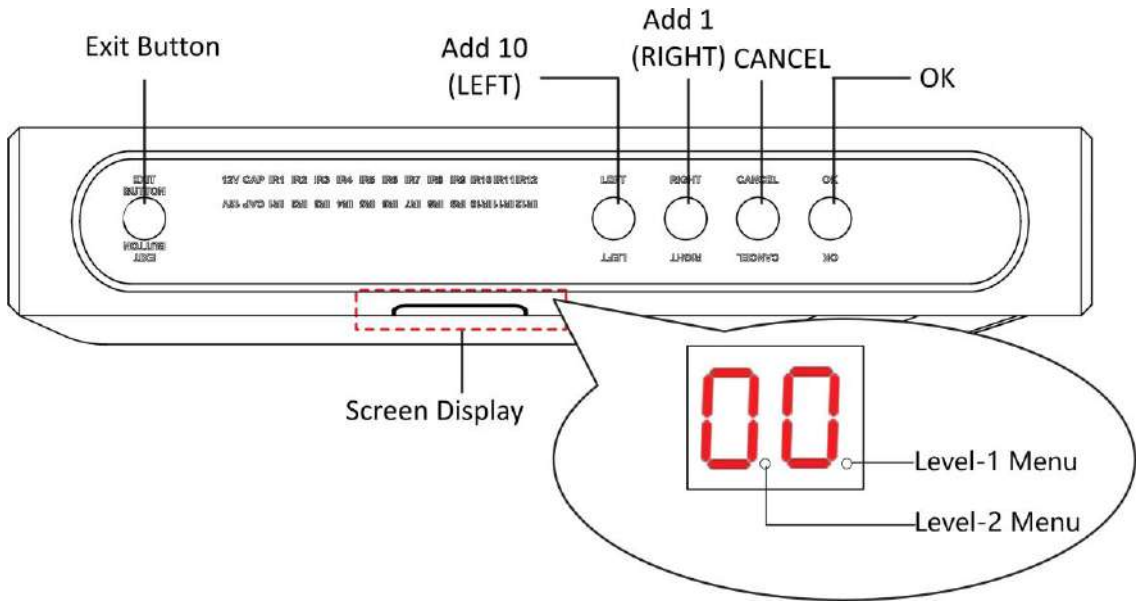


Figure 4-16 Button

Exit Button

- Press to open the barrier from the entrance position.
- Double press to open the barrier from the exit position.

Parameter Configuration Button

- LEFT: Press to add 10 to configuration data.
- RIGHT: Press to add 1 configuration data.
- CANCEL: Return to the Level-1 menu, or exit Level-1 menu.
- OK: Confirm the settings, or enter configuration mode, or enter the Level-2 menu.

Note

- Configuration No. is displayed by two digital tubes.
- Level-1 Menu: If the decimal point on the right is on, it indicates the Level-1 menu. The number represents the configuration No.
- Level-2 Menu: If the decimal point in the middle is on, it indicates the level-2 menu. The number represents the configuration No.

Button Configuration Procedure

Here takes setting intrusion duration to 12 s as example:

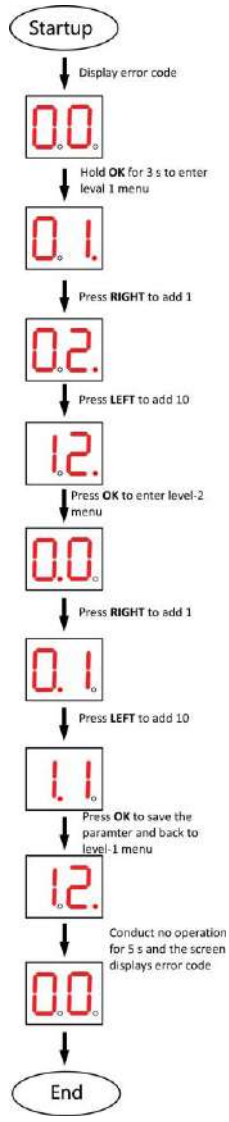


Figure 4-17 Procedure

Steps:

1. Hold **OK** button for 3 s until one beep occurs. The device enter the configuration mode. Level 1 menu lights up. The display screen displays the configuration No. **1**.
2. In the Level-1 menu, press **LEFT** (plus 10) once and press **RIGHT** (plus 1) twice to set the configuration No. to 12. Press **OK** to save settings and the enter the level-2 menu. Or you can press **CANCEL** to exit the current menu, or conduct no operation for 5 s to cancel configuration and exit the current menu.
3. After enter the level 2 menu, press **LEFT** (plus 10) once and **RIGHT** (plus 1) twice to set the configuration No. to 12. Press **OK** to save the settings. Or you can press **CANCEL** to exit the current menu, or conduct no operation for 5 s to cancel configuration and exit the current menu.

Note

- The configuration No. will display in a cycle.
- Each configuration No. refers to a function. For details about the configuration No. and its related function, see ***Button Configuration Description*** .

4.4.2 Study Mode Settings

Set the closed position of the device barrier.

Set Study Mode via Button

Enter the study mode through button configuration to set the closed position of the device barrier.

Steps

Note

- If the device is equipped with access control board, you can set study mode via DIP switch on the access control board only.
- For details about button's operation, see ***Configuration via Button*** .
- For details about the configuration No. and its related function, see ***Button Configuration Description*** .

1. Enter the study mode.
   1) Enter the configuration mode.
   2) Set the configuration No. in Level-1 to **1**. The device will enter the study mode.
   3) Set the configuration No. in the Level-2 menu to **2**. The device will enter the study mode.
2. Power off the device and swing the barrier until it is vertical to the pedestal.
3. Power on the device.
   The device will remember the current position automatically.
4. Reboot the device when you hear **Study accomplished. Please reboot.**

Set Study Mode via DIP Switch (Optional)

Enter the study mode through DIP switching to set the closed position of the device barrier.

Steps

1. Set the No.1 of the 2-digit DIP switch on the access control board to ON by referring the following figure to enter the study mode.

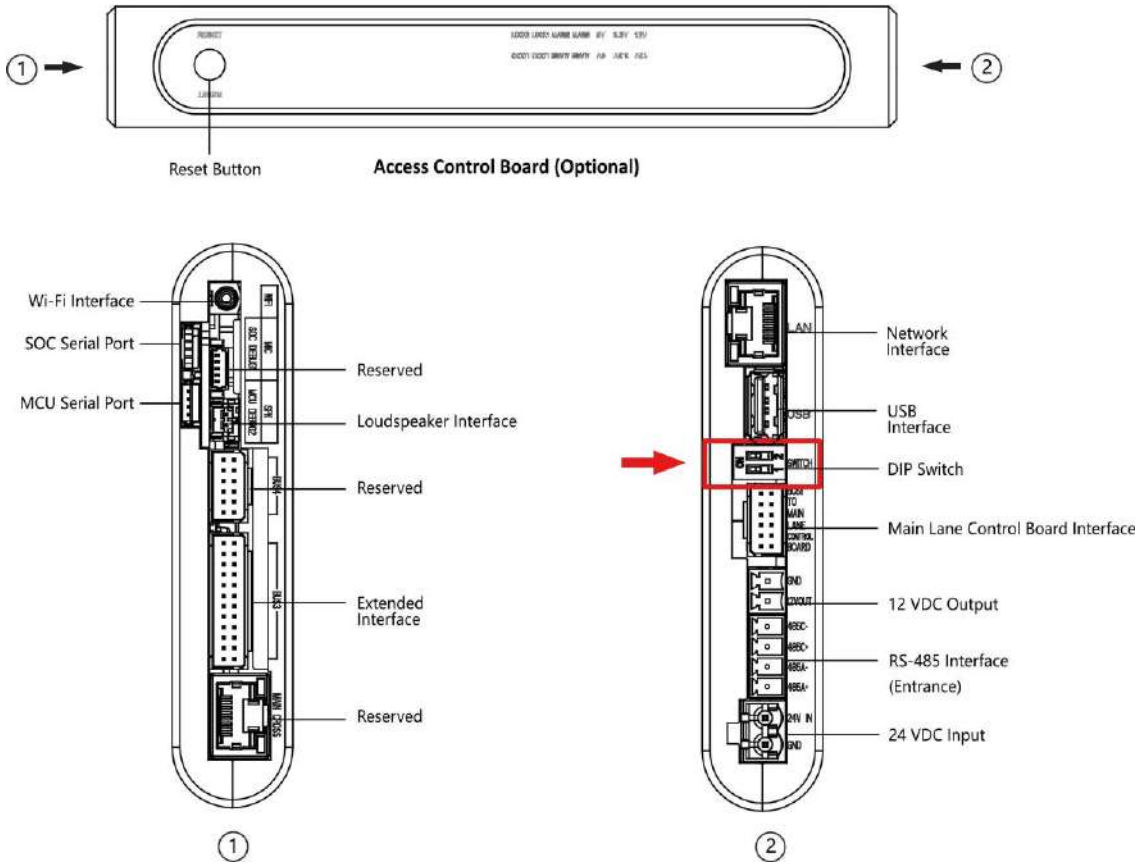


Figure 4-18 DIP Switch Location

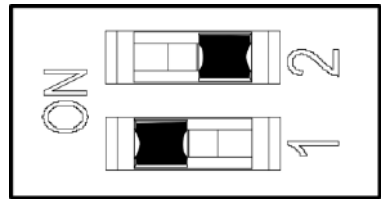


Figure 4-19 Study Mode

2. Adjust the closed position of the barrier.

3. Power on the device.

The device will remember the current position (closed position) automatically.

4. Power off the device.

5. Set the No.1 switches of the 2-digit DIP Switch on the main user extended interface board by referring to the following figure.

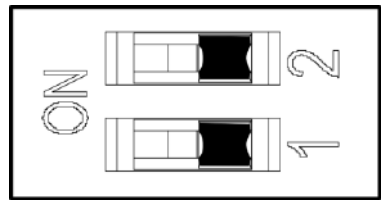


Figure 4-20 Normal Mode

6. Power on the device again.

Note

For details about the DIP switch value and meaning, see *DIP Switch Description*.

The barrier will open automatically and turns back to the closed position. At this circumstance, the device enters the normal mode.

4.4.3 Keyfob Pairing

Pair keyfob via button or DIP switch.

Pair Keyfob via Button

Pair the keyfob to the device via button to open/close the barrier remotely.

Before You Start

Ask our technique supports or sales and purchase the keyfob.

Steps

Note

- If the device is equipped with access control board, you can pair keyfob via DIP switch on the access control board only.
- For details about button's operation, see ***Configuration via Button*** .
- For details about the configuration No. and its related function, see ***Button Configuration Description*** .
- For details about the keyfob operation instructions, see the keyfob's user manual.

1. Enter the keyfob pairing mode.
   1) Enter the configuration mode.
   2) Set the configuration No. in Level-1 to **2**. The device will enter the keyfob pairing mode.
   3) Set the configuration No. in the Level-2 menu to **2**. The device will enter the keyfob pairing mode.

2. Hold the **Close** button for more than 10 seconds.

The keyfob's indicator will flash if the pairing is completed.

3. Exit the keyfob pairing mode.
1) Enter the configuration mode.
2) Set the configuration No. in Level-1 to **2**. The device will enter the keyfob pairing mode.
3) Set the configuration No. in the Level-2 menu to **1**. The device will exit the keyfob pairing mode.

4. Reboot the device to take effect.

Pair Keyfob via DIP Switch (Optional)

Pair the remote control to the device through DIP switch to open/close the barrier remotely.

Before You Start

Ask our technique supports or sales and purchase the keyfob.

Steps

1. Power off the turnstile.

2. Set the No.2 switch of the DIP Switch on the access control board to the ON side.

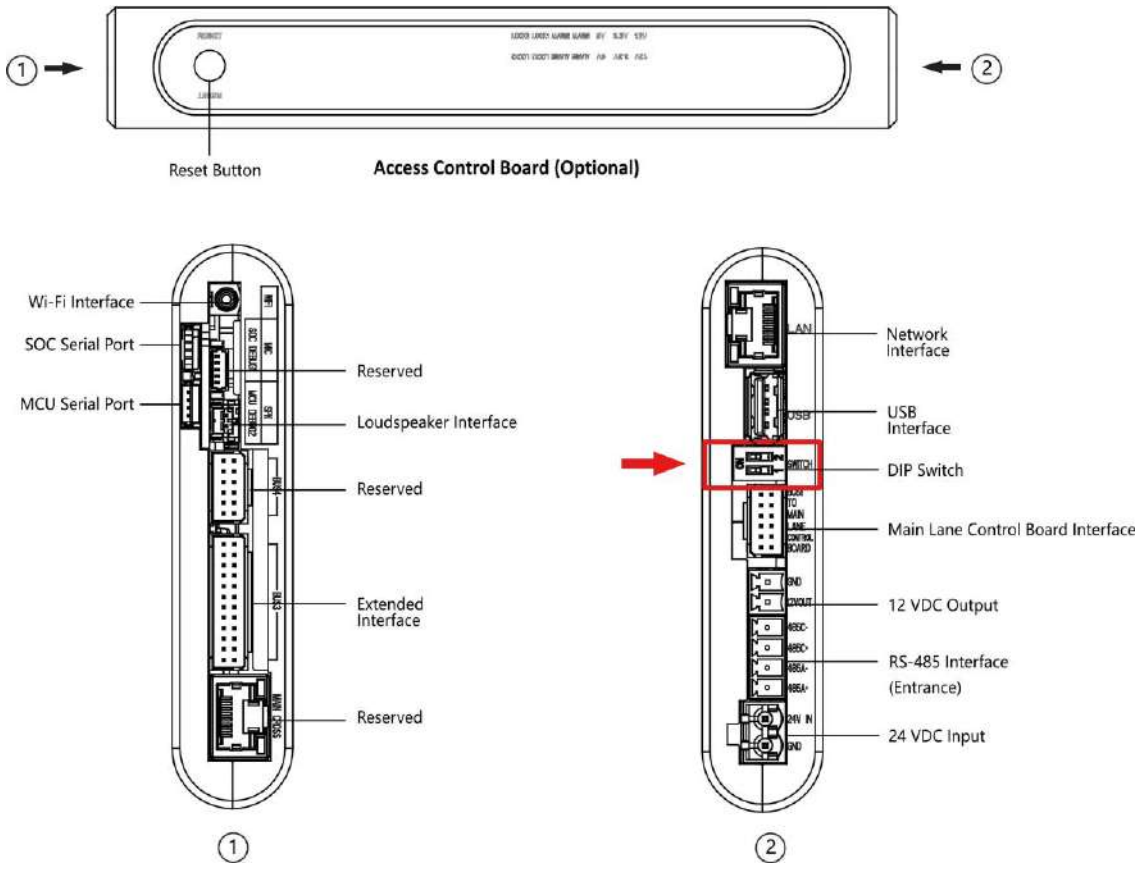


Figure 4-21 DIP Switch Location

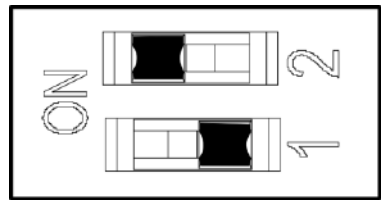


Figure 4-22 Enable Keyfob Paring Mode

3. Power on the turnstile and it will enter the keyfob pairing mode.
4. Hold the **Close** button for more than 10 seconds.
   The keyfob's indicator of the will flash twice if the pairing is completed.
5. Set the No.2 switch to the OFF side, and reboot the turnstile to take effect.

Note

- Only one turnstile can pair the keyfob. If multiple turnstiles are in the pairing mode, the keyfob will select only one of them to pair.
- For details about DIP switch value and meaning, see ***DIP Switch Description*** .

6. **Optional:** Go to **System → User → Keyfob User** on the remote control page of the client software to delete the keyfob.

4.4.4 Initialize Device

Steps

1. Hold the initialization button on the access control board for 5 s.

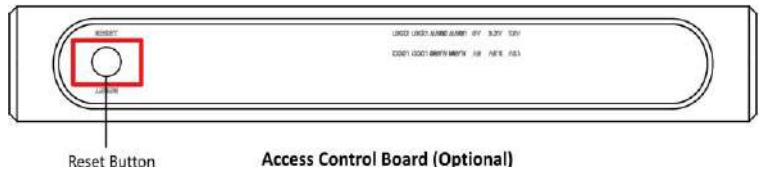


Figure 4-23 Initialization Button Position

2. The device will start restoring to factory settings.
3. When the process is finished, the device will beep for 3 s.

Caution

The initialization of the device will restore all the parameters to the default setting and all the device events are deleted.

Note

Make sure no persons are in the lane when powering on the device.

Chapter 5 Activation

You should activate the device before the first login. After powering on the device, the system will switch to Device Activation page.

Activation via the device, SADP tool and the client software are supported.

The default values of the device are as follows:

- The default IP address: 192.0.0.64
- The default port No.: 80
- The default user name: admin

5.1 Activate via Web Browser

You can activate the device via the web browser.

Steps

1. Enter the device default IP address (192.0.0.64) in the address bar of the web browser, and press **Enter**.

   Note

   Make sure the device IP address and the computer's should be in the same IP segment.

2. Create a new password (admin password) and confirm the password.

   Caution

   STRONG PASSWORD RECOMMENDED-We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

   Note

   Characters containing admin and nimda are not supported to be set as activation password.

3. Click **Activate**.
4. Edit the device IP address. You can edit the IP address via the SADP tool, the device, and the client software.

5.2 Activate via Mobile Web

You can activate the device via mobile web.

Steps

1. Connect to the device hotspot with your mobile phone by entering the hotspot password.

   Note

   - For inactive devices, hotspot is enabled by default.
   - The default hotspot password is the device serial number.

   The login page will pop up.
2. Create a new password (admin password) and confirm the password.

   Caution

   STRONG PASSWORD RECOMMENDED-We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

   Note

   Characters containing admin and nimda are not supported to be set as activation password.
3. Click **Activate**.
4. Edit the device IP address. You can edit the IP address via the SADP tool, the device, and the client software.

5.3 Activate via SADP

SADP is a tool to detect, activate and modify the IP address of the device over the LAN.

Before You Start

- Get the SADP software from the supplied disk or the official website ***http://www.hikvision.com/en/*** , and install the SADP according to the prompts.
- The device and the PC that runs the SADP tool should be within the same subnet.

The following steps show how to activate a device and modify its IP address. For batch activation and IP addresses modification, refer to *User Manual of SADP* for details.

Steps

1. Run the SADP software and search the online devices.
2. Find and select your device in online device list.
3. Input new password (admin password) and confirm the password.

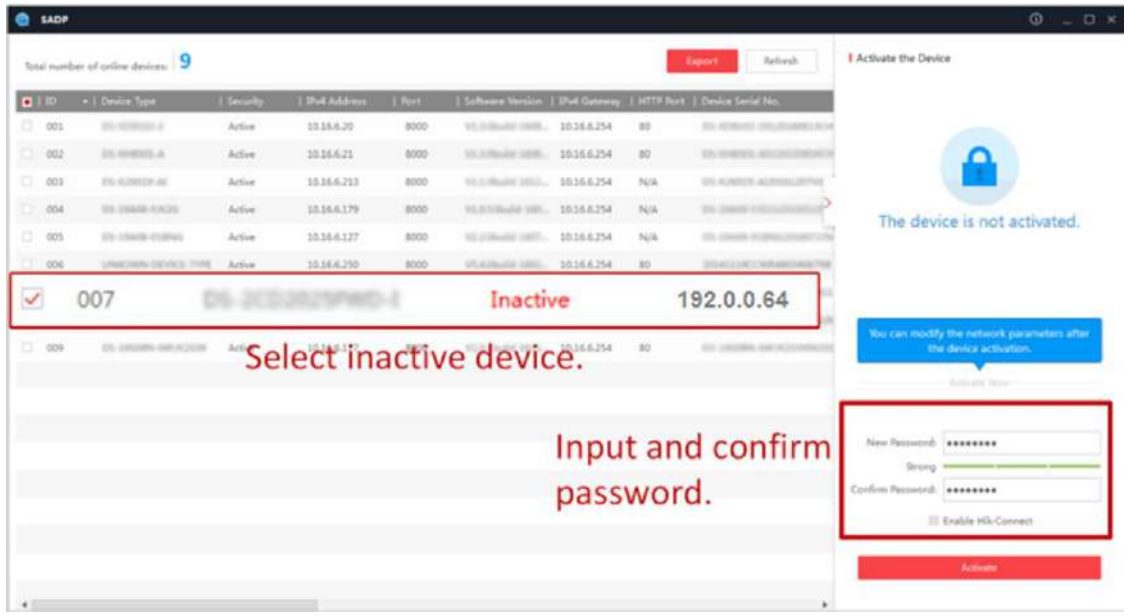
Caution

STRONG PASSWORD RECOMMENDED-We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Note

Characters containing admin and nimda are not supported to be set as activation password.

4. Click **Activate** to start activation.



Status of the device becomes **Active** after successful activation.

5. Modify IP address of the device.
   1) Select the device.
   2) Change the device IP address to the same subnet as your computer by either modifying the IP address manually or checking **Enable DHCP**.
   3) Input the admin password and click **Modify** to activate your IP address modification.

5.4 Activate Device via iVMS-4200 Client Software

For some devices, you are required to create the password to activate them before they can be added to the iVMS-4200 software and work properly.

Steps

Note

This function should be supported by the device.

1. Enter the Device Management page.
2. Click on the right of **Device Management** and select **Device**.
3. Click **Online Device** to show the online device area.
   The searched online devices are displayed in the list.
4. Check the device status (shown on **Security Level** column) and select an inactive device.
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

   Characters containing admin and nimda are not supported to be set as activation password.
7. Click **OK** to activate the device.

Chapter 6 Operation via Web Browser

6.1 Login

You can login via the web browser or the remote configuration of the client software.

Note

Make sure the device is activated. For detailed information about activation, see ***Activation*** .

Login via Web Browser

Enter the device IP address in the address bar of the web browser and press **Enter** to enter the login page.

Enter the device user name and the password. Click **Login**.

Login via Remote Configuration of Client Software

Download and open the client software. After adding the device, click to enter the Configuration page.

6.2 Overview

You can view the device component status, real-time event, person information, network status, basic information, and device capacity. You can also control the barrier remotely.

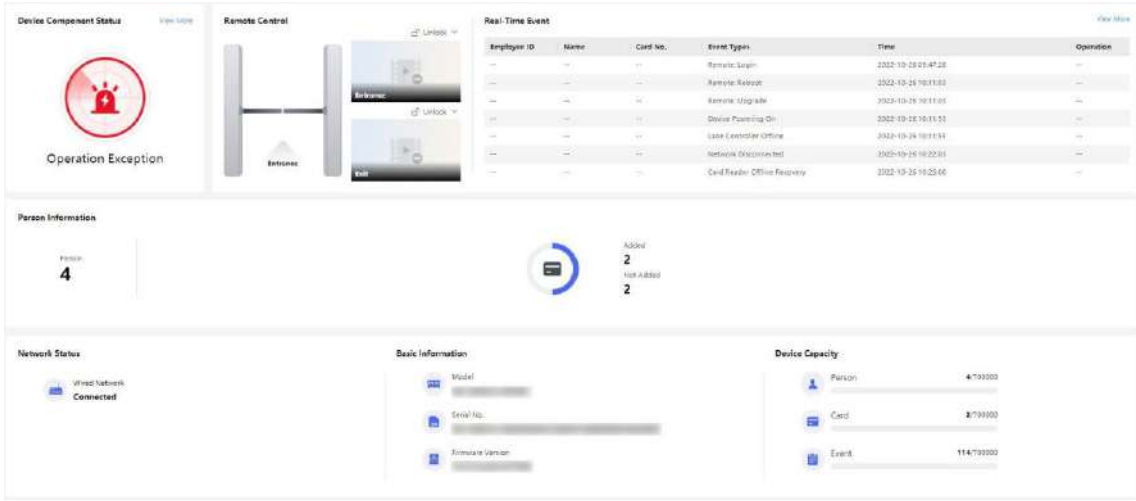


Figure 6-1 Overview

Function Descriptions:

Device Component Status

You can check if the device is working properly. Click **View More** to view the detailed component status.

Remote Control

/ / /

The door is opened/closed/remaining open/remaining closed.

Real-Time Event

You can view the event Employee ID, Name, Card No., Event Type, Time, and Operation. You can also click **View More** to enter the search conditions, including the event type, employee ID, the name, the card No., the start time, and the end time, and click **Search**. The results will be displayed on the right panel.

Person Information

You can view the added and not added information of person and card.

Network Status

You can view the network connection status.

Basic Information

You can view the model, serial No. and firmware version.

Device Capacity

You can view the person, card and event capacity.

6.3 Person Management

Click **Add** to add the person's information, including the basic information, certificate, authentication and settings.

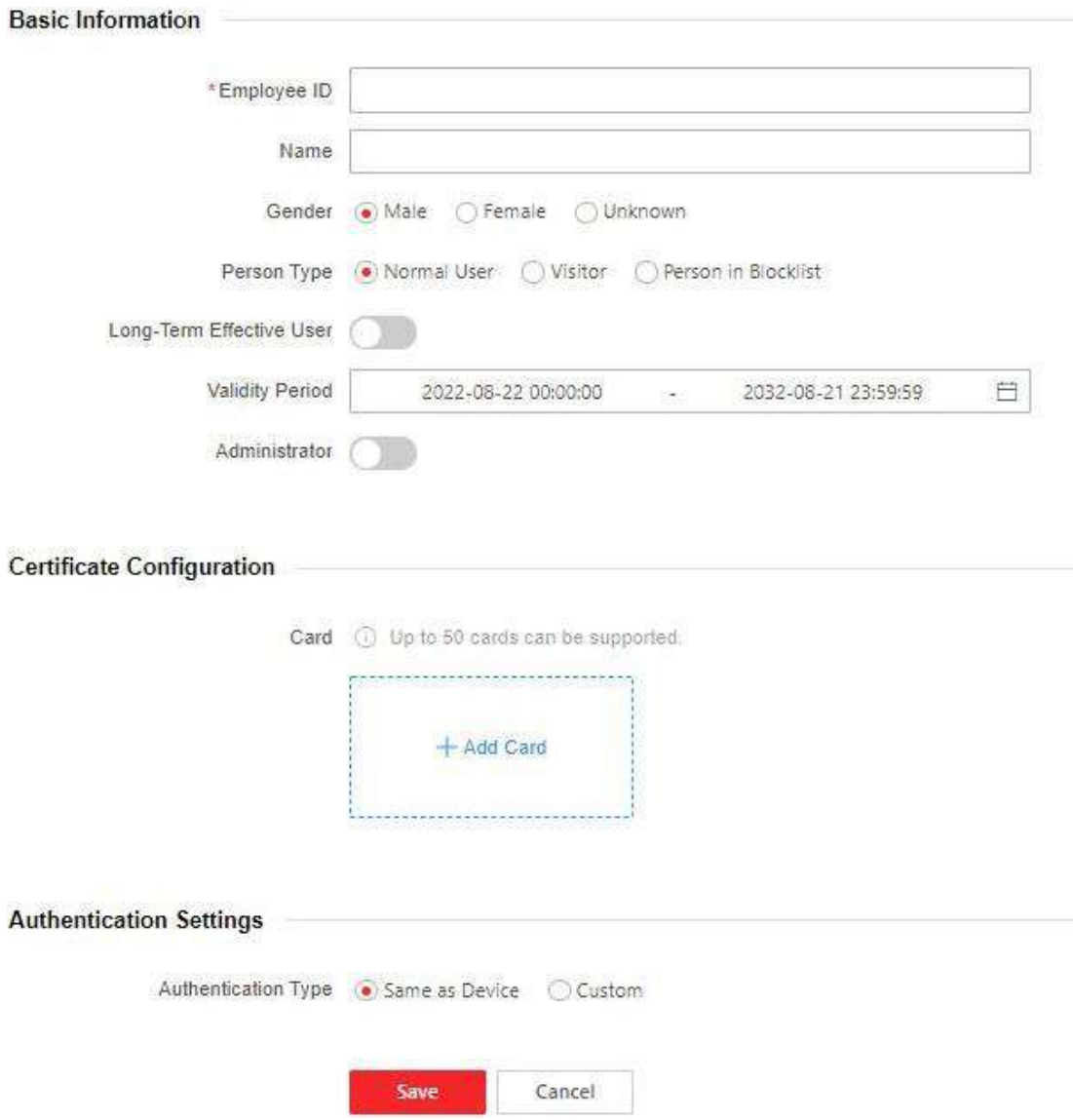


Figure 6-2 Add Person

Add Basic Information

Click **Person Management → Add** to enter the Add Person page.
Add the person's basic information, including the employee ID, the person's name, and person type.
If you select **Visitor** as the person type, you can set the visit times.
Click **Save** to save the settings.

Set Permission Time

Click **Person Management → Add** to enter the Add Person page.

Enable **Long-Term Effective User**, or set **Validity Period** and the person can only has the permission within the configured time period according to your actual needs.
Click **Save** to save the settings.

Add Card

Click **Person Management → Add** to enter the Add Person page.
Click **Add Card**, enter the **Card No.** and select the **Property**, and click **OK** to add the card.

Note
Up to 50 cards can be added.

Click **Save** to save the settings.

Authentication Settings

Click **Person Management → Add** to enter the Add Person page.
Set **Authentication Type** as **Same as Device** or **Custom**.
Click **Save** to save the settings.

Import/Export Person Data

Export Person Data

You can export added person data for back-up or importing to other devices.

Click **Export Person Data**, set an encryption password and confirm it. Click **OK**.

Note
- The person data will be downloaded to your PC.
- The password you set will be required for importing the data file.

Importing Person Data

Click **Importing Person Data** and select the file. Click **Import**.

Enter the encryption password to import and synchronize the person data to devices.

6.4 Search Event

Click **Event Search** to enter the Search page.

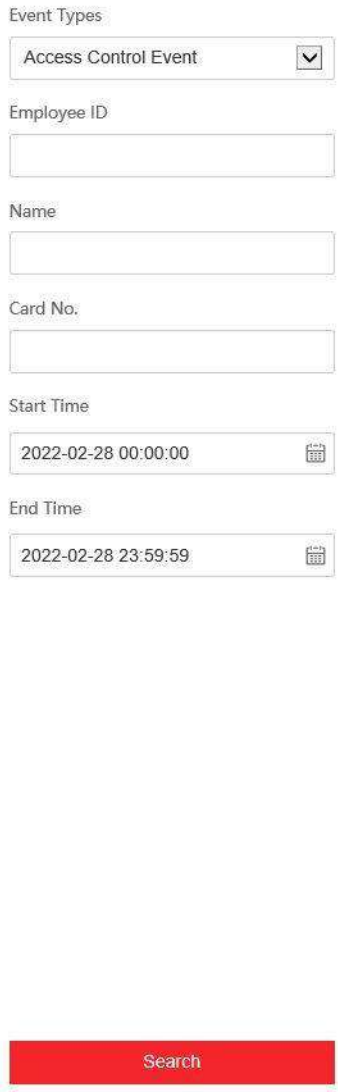


Figure 6-3 Search Event

Enter the search conditions, including the event type, the employee ID, the name, the card No., the start time, and the end time, and click **Search**.

The event types contain access control event and ID card event. If you choose to search for ID card event, you will not need to enter the employee ID, the name, or the card No.

The results will be displayed on the right panel.

6.5 Configuration

6.5.1 View Device Information

Click **Configuration → System → System Settings → Basic Information** to enter the configuration page.

You can view the device name, language, model, serial No., version, IO input, IO output, and local RS-485 number.

You can change **Device Name** and click **Save**.

You can view the device capacity, including person, card and event.

6.5.2 Set Time

Set the device's time.

Click **Configuration → System → System Settings → Time Settings** .

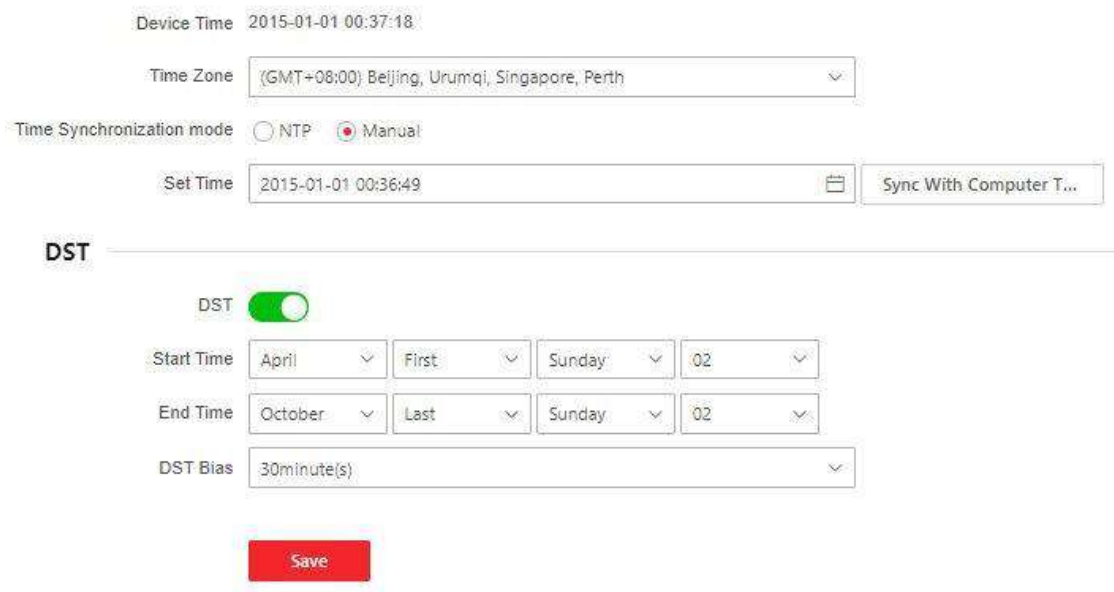


Figure 6-4 Time Settings

Click **Save** to save the settings after the configuration.

Time Zone

Select the device located time zone from the drop-down list.

Time Sync.

NTP

You should set the NTP server's IP address, port No., and interval.

Manual

By default, the device time should be synchronized manually. You can set the device time manually or check **Sync. with Computer Time** to synchronize the device time with the computer's time.

Server Address Type/Server Address/NTP Port/Interval

You can set the server address type, server address, NTP port, and interval.

6.5.3 Set DST

Steps

1. Click **Configuration → System → System Settings → Time Settings** .
2. Enable **DST**.
3. Set the DST start time, end time and bias time.
4. Click **Save** to save the settings.

6.5.4 Change Administrator's Password

Steps

1. Click **Configuration → User Management** .
2. Click .
3. Enter the old password and create a new password.
4. Confirm the new password.
5. Click **OK**.

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.

6.5.5 Online Users

The information of users logging into the device is shown.

Go to **Configuration → System → User Management → Online Users** to view the list of online users.

6.5.6 View Device Arming/Disarming Information

View device arming type and arming IP address.

Go to **Configuration → User Management → Arming/Disarming Information** .

You can view the device arming/disarming information. Click **Refresh** to refresh the page.

6.5.7 Network Settings

Set TCP/IP, hotspot and HTTP(S) parameters.

Set Basic Network Parameters

Click **Configuration → Network → Network Settings → TCP/IP** .

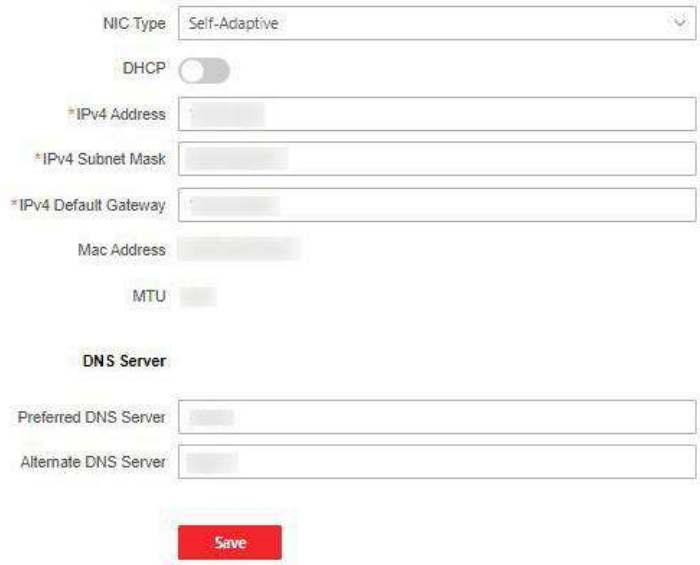


Figure 6-5 TCP/IP Settings Page

Set the parameters and click **Save** to save the settings.

NIC Type

Select a NIC type from the drop-down list. By default, it is **Auto**.

DHCP

If you uncheck the function, you should set the IPv4 address, IPv4 subnet mask, IPv4 default gateway, Mac address, and MTU.

If you check the function, the system will allocate the IPv4 address, IPv4 subnet mask, the IPv4 default gateway automatically.

DNS Server

Set the preferred DNS server and the Alternate DNS server according to your actual need.

Device Hotspot

Set the device hotspot.

Click **Configuration → Network → Network Settings → Device Hotspot** .

Click to **Enable Device Hotspot**. Set hotspot **Name** and **Password**.

Click **Save**.

Set Port Parameters

Set the HTTP, HTTPS, and HTTP Listening parameters.

Click **Configuration → Network → Network Service → HTTP(S)** .

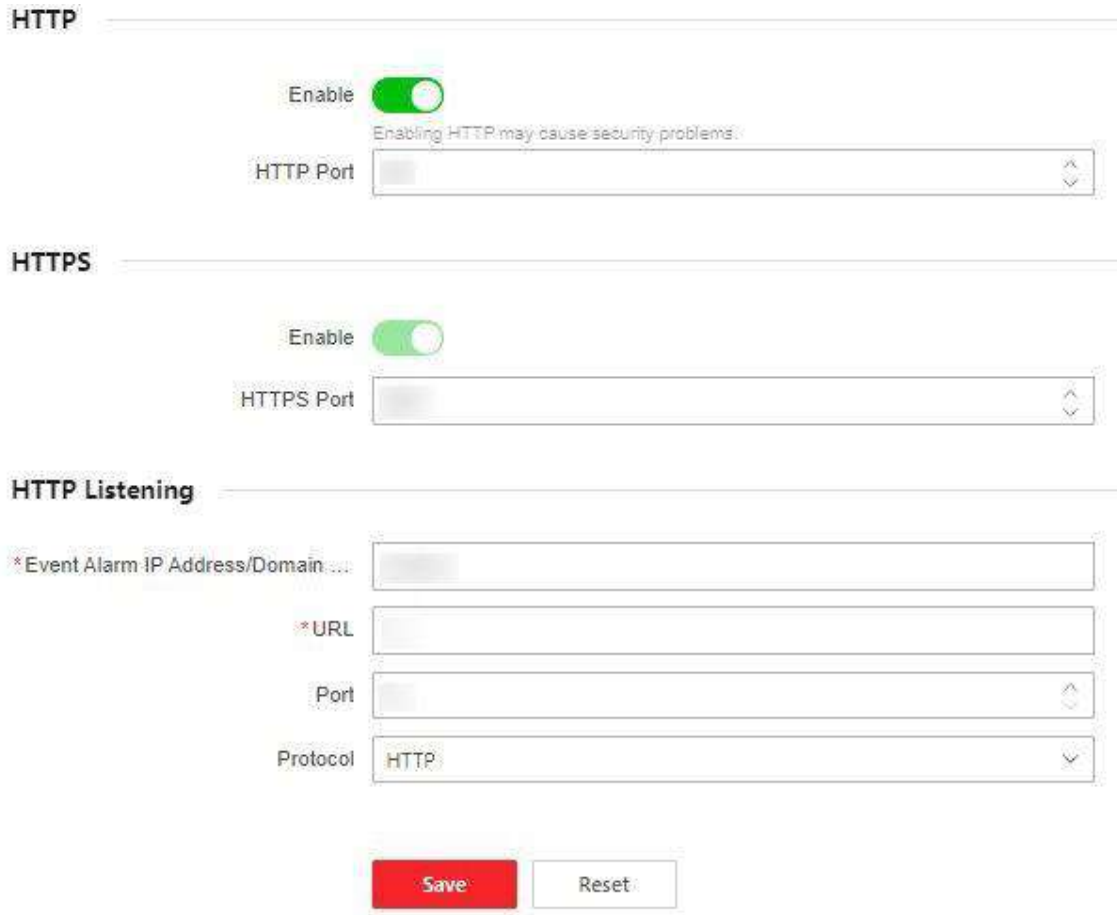


Figure 6-6 Network Service

HTTP

It refers to the port through which the browser accesses the device. For example, when the HTTP Port is modified to 81, you need to enter ***http://192.0.0.65:81*** in the browser for login.

HTTPS

Set the HTTPS for accessing the browser. Certificate is required when accessing.

HTTP Listening

The device can send alarm information to the event alarm IP address or domain name via HTTP protocol/HTTPS protocol. Edit the event alarm IP address or domain name, URL, port, and protocol.

Note

The event alarm IP address or domain name should support the HTTP protocol/HTTPS protocol to receive the alarm information.

.

6.5.8 Set Audio Parameters

Set the image quality, resolution, and the device volume.

Set Audio Parameters

Click **Configuration → Video/Audio → Audio** .

Figure 6-7 Set Audio Parameters

Drag the block to adjust the output volume.
Click **Save** to save the settings after the configuration.
You can also enable **Voice Prompt**.

Note
The functions vary according to different models. Refers to the actual device for details.

6.5.9 Event Linkage

Set linked actions for events.

Steps
1. Click **Configuration → Event → Event Detection → Linkage Settings** to enter the page.

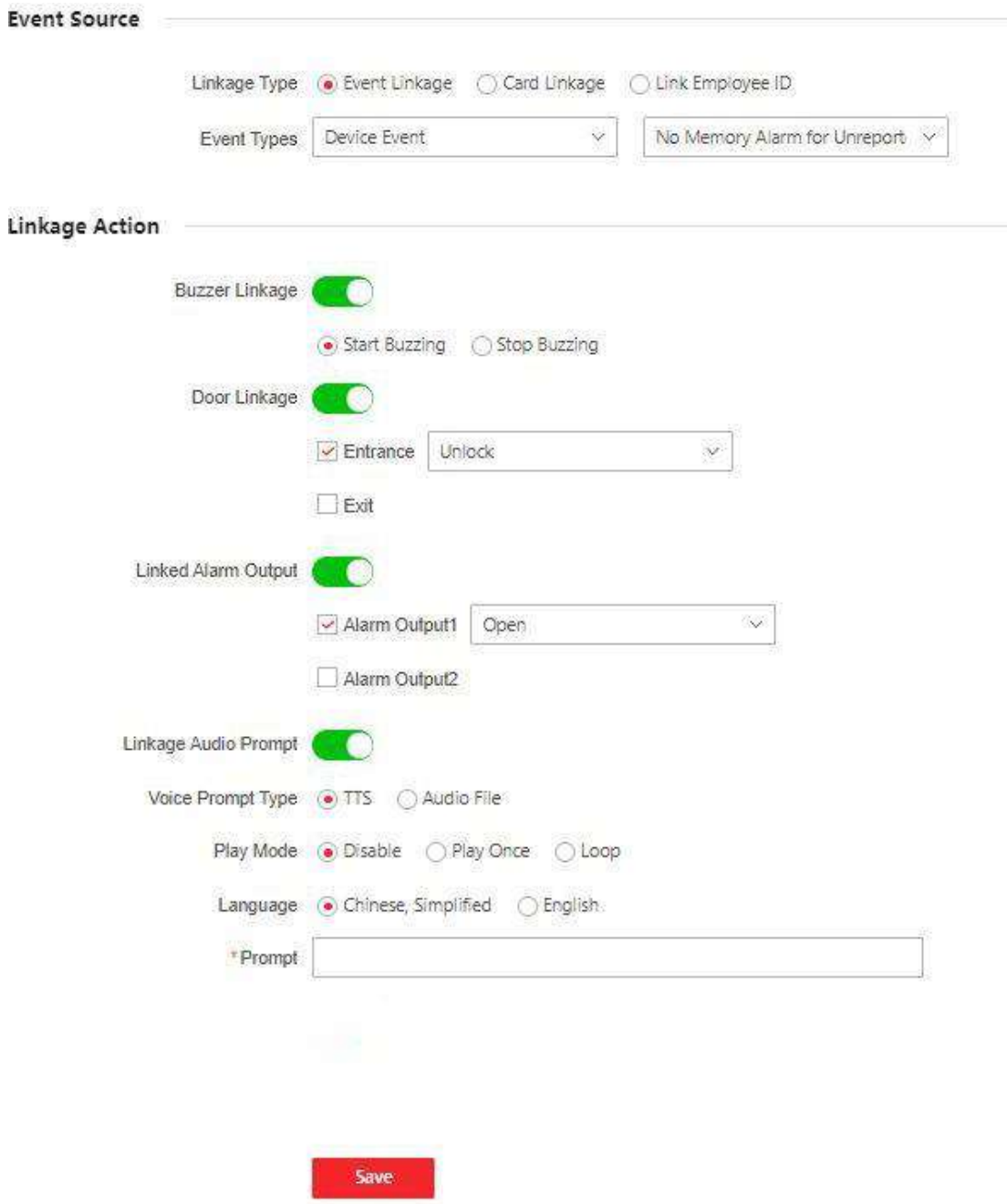


Figure 6-8 Event Linkage

2. Set event source.

- If you choose **Linkage Type** as **Event Linkage**, you need to select event types from the drop-down list.
- If you choose **Linkage Type** as **Card Linkage**, you need to enter the card No. and select the card reader.

- If you choose **Linkage Type** as **Employee ID Linkage**, you need to enter the employee ID and select the card reader.

3. Set linked action.

Linked Buzzer

Enable **Linked Buzzer** and select **Start Buzzing** or **Stop Buzzing** for the target event.

Linked Door

Enable **Linked Door**, check **Entrance** or **Exit**, and set the door status for the target event.

Linked Alarm Output

Enable **Linked Alarm Output**, check **Alarm Output 1** or **Alarm Output 2**, and set the alarm output status for the target event.

Linked Audio Prompt

Enable **Linked Audio Prompt** and select the play mode.

- If you choose **TTS**, you need to set language and enter the prompt content.
- If you choose **Audio File**, you need to select an available audio file from the drop-down list or click **General Linkage Settings** to add a new audio file.

6.5.10 Access Control Settings

Set Authentication Parameters

Click **Configuration → Access Control → Authentication Settings** .

Note

The functions vary according to different models. Refers to the actual device for details.

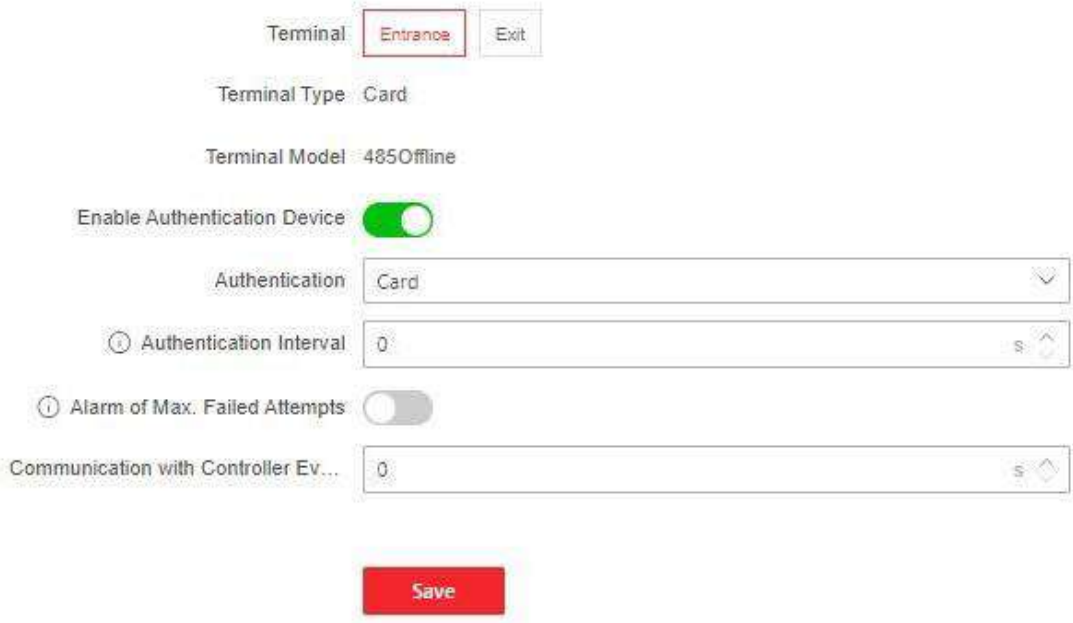


Figure 6-9 Set Authentication Parameters

Click **Save** to save the settings after the configuration.

Terminal

Choose **Entrance** or **Exit** for settings.

Terminal Type/Terminal Model

Get terminal description. They are read-only.

Enable Authentication Device

Enable the authentication function.

Authentication

Select an authentication mode according to your actual needs from the drop-down list.

Authentication Interval

You can set the authentication interval of the same person when authenticating. The same person can only authenticate once in the configured interval. A second authentication will be failed.

Alarm of Max. Failed Attempts

Enable to report alarm when the card reading attempts reach the set value.

Max. Authentication Failed Attempts

Enable to report alarm when the card reading attempts reach the set value.

Communication 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.

Note

The authentication interval value ranges from 2 s to 255 s.

Set Door Parameters

Click **Configuration → Access Control → Door Parameters** .

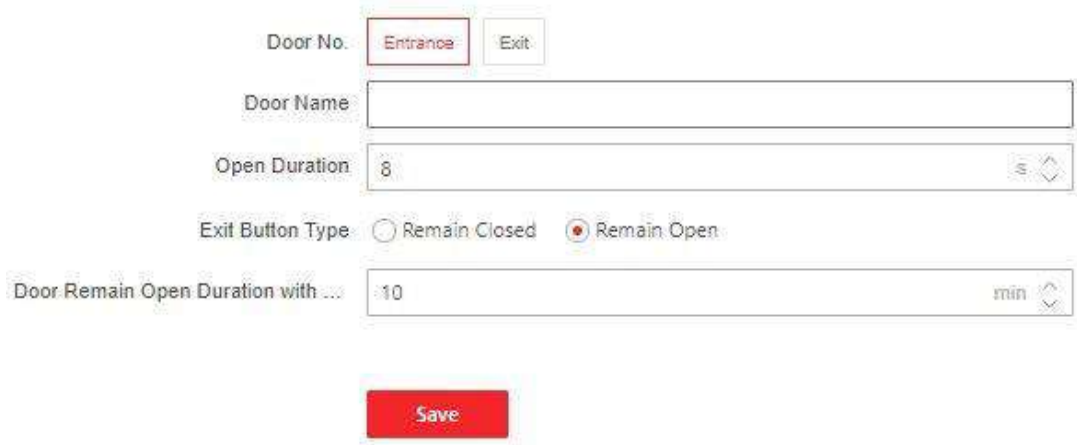


Figure 6-10 Door Parameters Settings Page

Click **Save** to save the settings after the configuration.

Door No.

Select **Entrance** or **Exit** for settings.

Door Name

You can create a name for the door.

Open Duration

Set the door unlocking duration. If the door is not opened for the set time, the door will be locked.

Note

The open duration ranges from 5 s to 60 s.

Exit Button Type

You can set the exit button as **Remain Open** or **Remain Closed** according to your actual needs. By default, it is **Remain Open**.

Door Remain Open Duration with First Person

Set the door open duration when first person is in. After the first person is authorized, it allows multiple persons access the door or other authentication actions.

Note

The duration ranges from 1 s to 1440 s.

Serial Port Settings

Set serial port parameters.

Steps

1. Click **Configuration → Access Control → Serial Port Configuration** .

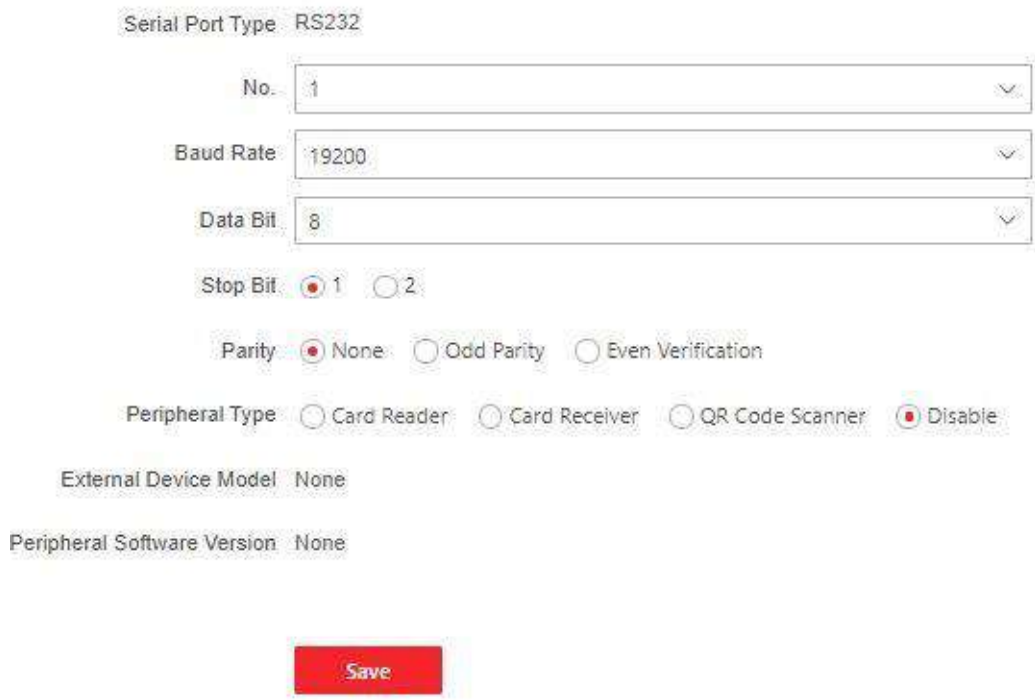


Figure 6-11 Serial Port Settings

2. Set the **No.**, **Baud Rate**, **Data Bit**, **Stop Bit** and **Parity**.
3. Set the **Peripheral Type** as **Card Reader**, **QR Code Scanner** or **Disable**.
4. You can view the serial port type, connected device model and peripheral software version.
5. Click **Save**.

Set Wiegand Parameters

You can set the Wiegand transmission direction.

Steps

Note

Some device models do not support this function. Refer to the actual products when configuration.

1. Click **Configuration → Access Control → Wiegand Settings** .
2. Select **Entrance** or **Exit**.
3. Enable **Wiegand** function.
4. The wiegand transmission direction is set **Input** by default.

   Note

   Input: the device can connect a Wiegand card reader.
5. Click **Save** to save the settings.

   Note

   If you change the peripheral, and after you save the device parameters, the device will reboot automatically.

Host Parameters

Set door contact settings and RS-485 protocol.

Steps

1. Click **Configuration → Access Control → Host Parameter** to enter the page.
2. Set door contact.

   Note

   You can set the door contact as **Door Open Status** or **Door Closed Status** according to your actual needs. By default, it is **Door Open Status**.
3. Set RS-485 protocol.
4. Click **Save**.

Set Terminal Parameters

Set the working mode and remote verification.

Steps

1. Click **Configuration → Access Control → Terminal Parameters** to enter the page.

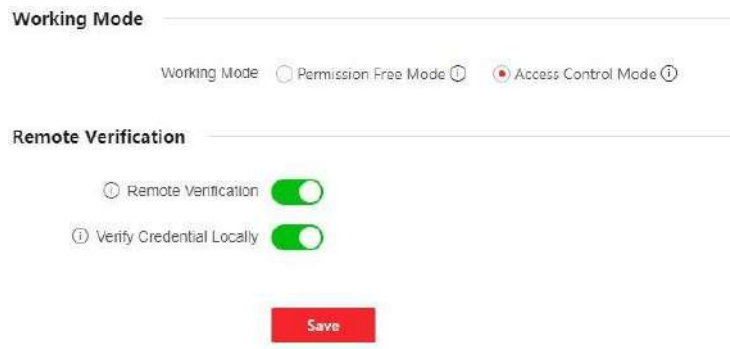


Figure 6-12 Terminal Parameters

2. Set the device working mode.

Permission Free Mode

The device will not verify the person's permission, but only the person's validity period. If the person is in the validity period, the barrier will open.

You can enable **Verify Credential Locally**. After enabling the function, the device will only verify the person's permission without the schedule template, etc.

Access Control Mode

The device works normally and will verify the person's permission to open the barrier.

3. Set remote verification.

1) Enable **Remote Verification**.

Note

The device will upload the person's authentication information to the platform. The platform will judge to open the barrier or not.

2) **Optional:** Enable **Verify Credential Locally**.

Note

After enabling the function, the device will only verify the person's permission without the schedule template, etc.

4. Click **Save** to complete terminal parameter settings.

6.5.11 Turnstile

Basic Parameters

Set turnstile basic parameters.

Steps

1. Click **Configuration → Turnstile → Basic Settings** to enter the page.
2. View the **Device Type**, **Device Model** and **Working Status**.
3. Set **Barrier Material**, **Lane Width**, **Barrier Height**, **Barrier Opening Speed** and **Barrier Closing Speed**.
4. Set the passing mode.
   - If you choose **General Passing**, you can select the barrier status for the entrance and exit from the drop-down list.

     Note

     If you set barrier-free mode, the barrier remains open and will close when authentication fails.
   - If you choose **Weekly Schedule**, you can set a weekly schedule for entrance and exit barriers.
5. Click **Save**.

keyfob

Set keyfob patameters.

Steps

1. Click **Configuration → Turnstile → Keyfob** to enter the page.

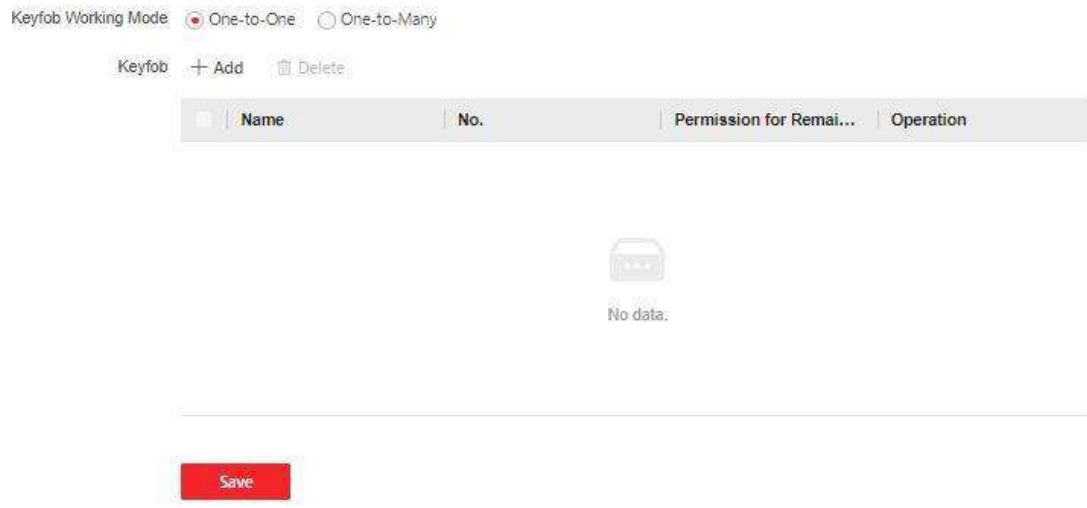


Figure 6-13 keyfob

2. Set **Working Mode** as **One-to-One** or **One-to-Many**.
3. Add keyfob.
   1) Click **Add** and the keyfob adding window will pop up.
   2) Enter the **Name** and **Serial No.**.
   3) Check to enable **Remain Open Permission** at your actual needs.
   4) Click **OK** to add the keyfob.

4. **Optional:** Select a keyfob and click **Delete** to delete the keyfob.
5. Click **Save**.

IR Detector

Set IR detector.

Steps

1. Click **Configuration → Turnstile → IR Detector** to enter the page.

Figure 6-14 IR Detector

2. Set the entrance and exit inductive mode as **Single Triggered** or **Triggered Simultaneously**.
3. Set custom IR detector mode.

   Enable IR Emergency Mode

   If some IR beams do not work properly, you can shield those IR beams to restore the lane. But this action may hit person and cause injury.

   Enable Custom Anti-pinch for Door Closing

   Anti-pinch for door closing refers that the barrier will not close if the device has detected person in the lane. Only after the person walks out of the lane, the barrier will close. If you enable the function, you can shield parts of the IR beams for closing barrier in advance. But this action may hit person and cause injury.
4. Click **Save**.

People Counting

Set people counting .

Steps

1. Click **Configuration → Turnstile → People Counting** to enter the page.

Figure 6-15 People Counting

2. Check to enable **People Counting**.
3. Enable **Device Offline People Counting** at your actual needs.
4. Select **People Counting Type** as **Invalid**, **Passing Detection** or **Authentication Number**.
5. **Optional:** Click **clear** to clear all the people counting information.

Set Indicator Color

Set the color for the indicators.

Steps

1. Click **Configuration → Turnstile → Light Settings** to enter the page.
2. Set light color for lane status indicator.
   1) Set **Light Brightness** as **Auto** or **Fixed Brightness**. If you choose **Fixed Brightness**, you can drag the block or enter the value to adjust the light brightness manually.
   2) Set inductive, prohibited and Auth. passing light color.
3. Set barrier light color.
   1) Check to enable **Light on When on Standby** at your actual needs.
   2) Set the barrier light color.
4. Click **Save**.

Other Settings

Set other parameters.

Steps

1. Click **Configuration → Turnstile → Other Settings** to enter the page.
2. Set **Alarm Output Duration**.

Note

The alarm output duration ranges from 0 s to 3599 s.

3. Set **Temperature Unit**.
4. Check to enable **Do Not Open Barrier When Lane is Not Clear**.
5. Drag the block or enter the value to adjust the light board brightness.
6. Set the alarm buzzer beeping duration, door closing delay time, intrusion duration, overstaying duration and IR obstructed duration.
7. Check to enable **Memory Mode** at your actual needs.

Note

Multiple cards presenting for multiple person passing is allowable when enabling the memory mode. When the passing person's number exceeds the card presenting number, or after the latest person passing with no other person passing within the door open duration, the door will close automatically.

8. Choose the control mode.

Soft Mode

The barrier will be closed after the person has passed through the barrier when there are tailing, forced accessing, etc.

Guard Mode

The barrier will be closed immediately when there are tailgating, forced accessing, etc.

9. Set the fire input type.
10. Click to enable **Motor Self-Test** and choose the main lane or sub lane to start motor self-testing.
11. Click **Save**.

6.5.12 Card Settings

Set Card Security

Click **Configuration → Card Settings → Card Type** to enter the settings page.

Set the parameters and click **Save**.

Enable NFC Card

In order to prevent the mobile phone from getting the data of the access control, you can disable NFC card to increase the security level of the data.

Enable M1 Card

Enable M1 card and authenticating by presenting M1 card is available.

M1 Card Encryption

Sector

M1 card encryption can improve the security level of authentication.

Enable the function and set the encryption sector. By default, Sector 13 is encrypted. It is recommended to encrypt sector 13.

Enable EM Card

Enable EM card and authenticating by presenting EM card is available.

Note

If the peripheral card reader supports presenting EM card, the function is also supported to enable/disable the EM card function.

Enable CPU Card

Enable CPU card and authenticating by presenting CPU card is available.

CPU Card Read Content

After enable the CPU card content reading function, the device can read the CPU card content.

Enable FeliCa Card

The device can read the data from FeliCa card when enabling the FeliCa card function.

Set Card Authentication Parameters

Set the card reading content when authenticate via card on the device.

Go to **Configuration → Card Settings → Card NO. Authentication Settings** .

Select a card authentication mode and enable reversed card No. at your actual needs. Click **Save**.

6.5.13 Set Privacy Parameters

Set the event storage type.

Go to **Configuration → Security → Privacy Settings**

The event storage type is overwriting by default. The earliest 5% events will be deleted when the system detects the stored events has been over 95% of the full space.

6.5.14 Prompt Schedule

Customize the output audio content when authentication succeeded and failed.

Steps

1. Click **Configuration → Preference → Prompt Schedule** .

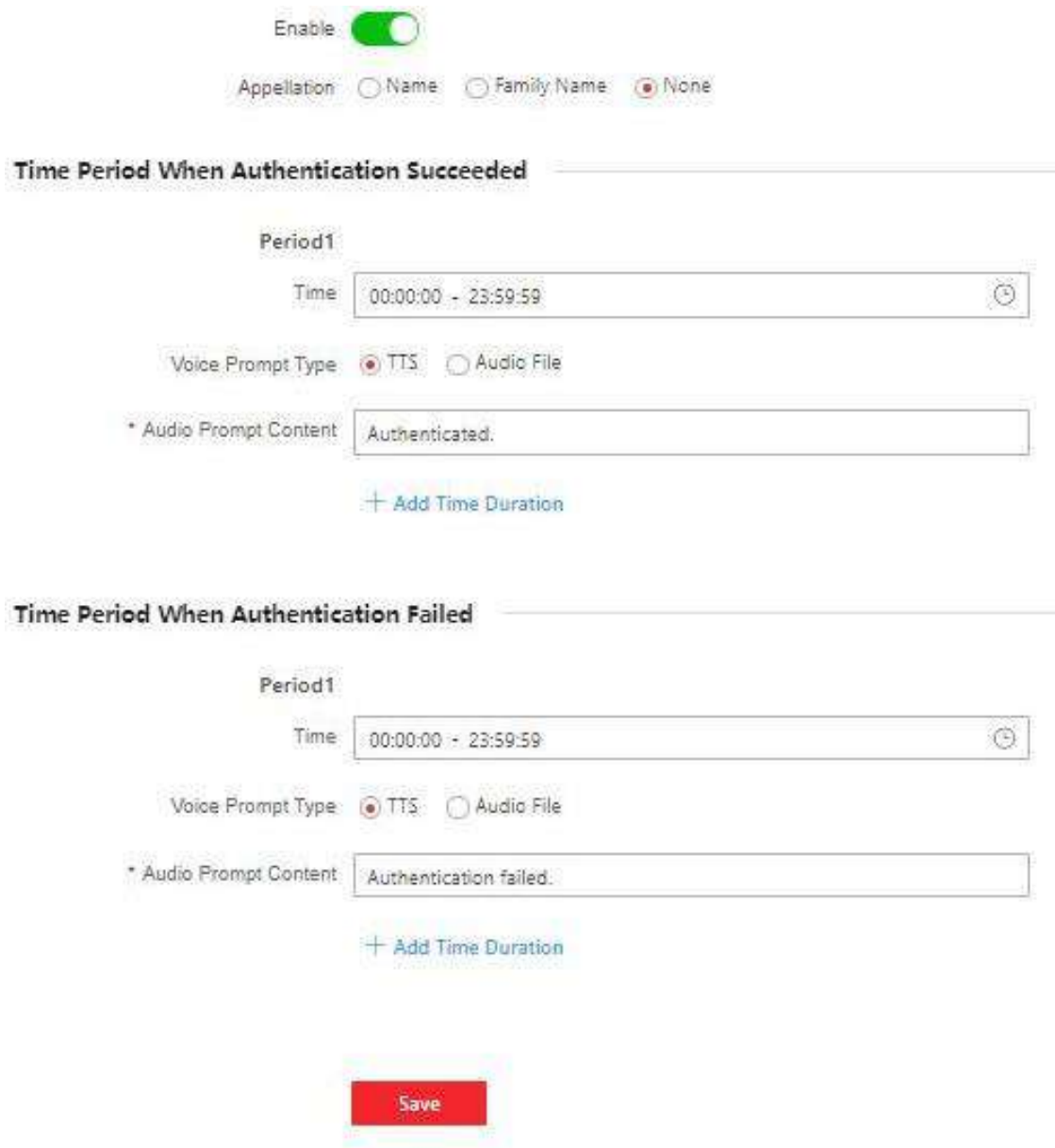


Figure 6-16 Customize Audio Content

2. Select time schedule.

3. Enable the function.

4. Set the appellation.

5. Set the time period when authentication succeeded.

1) Click **Add Time Duration**.

2) Set the time duration.

Note

If authentication is succeeded in the configured time duration, the device will broadcast the configured content.

3) Set the audio content.

TTS

If you choose TTS, you need to set the language and enter the prompt content of authentication success.

Audio File

If you choose audio file, you need to select an available audio file from the drop-down list or click **Audio File Management** to add a new file.

Note

The audio file's format should be wav, and the size should be within 200 KB.

4) **Optional:** Repeat substep 1 to 3.

5) **Optional:** Click to delete the configured time duration.

6. Set the time duration when authentication failed.

1) Click **Add**.

2) Set the time duration.

Note

If authentication is failed in the configured time duration, the device will broadcast the configured content.

3) Set the audio content.

TTS

If you choose TTS, you need to set the language and enter the prompt content of authentication failure.

Audio File

If you choose audio file, you need to select an available audio file from the drop-down list or click **Audio File Management** to add a new file.

Note

The audio file's format should be wav, and the size should be within 200 KB.

4) **Optional:** Repeat substep 1 to 3.

5) **Optional:** Click to delete the configured time duration.

7. Click **Save** to save the settings.

6.5.15 Upgrade and Maintenance

Reboot device, restore device parameters, and upgrade device version.

Reboot Device

Click **Maintenance and Security → Maintenance → Restart** .
Click **Restart** to reboot the device.

Upgrade

Click **Maintenance and Security → Maintenance → Upgrade** .
Select an upgrade type from the drop-down list. Click and select the upgrade file from your local PC. Click **Upgrade** to start upgrading.

Note
Do not power off during the upgrading.

Restore Parameters

Click **Maintenance and Security → Maintenance → Backup and Reset** .

Restore All

All parameters will be restored to the factory settings. You should activate the device before usage.

Restore

The device will restore to the default settings, except for the network parameters and the user information.

Import and Export Parameters

Click **Maintenance and Security → Maintenance → Backup and Reset** .

Export

Click **Export** to export the device parameters.

Note
You can import the exported device parameters to another device.

Import

Click and select the file to import. Click **Import** to start import configuration file.

6.5.16 Device Debugging

You can set device debugging parameters.

Steps

1. Click **Maintenance and Security → Maintenance → Device Debugging** .
2. You can set the following parameters.

Enable SSH

To raise network security, disable SSH service. The configuration is only used to debug the device for the professionals.

Print Log

You can click **Export** to export log.

6.5.17 Component Status

You can view the main lane and sub lane status.

Main Lane Status

Device Component

You can view the status of the access control board, lane control board, user extended interface board, and passing mode indicator board.

Peripheral

You can view the status of the RS-485 card reader and tamper input.

Temperature

You can view the pedestal temperature.

Movement

You can view the working status of motor encoder.

Sub Lane Status

Device Component

You can view the status of the lane control board, passing mode indicator board and upper IR adaptor.

Peripheral

You can view the status of the RS-485 card reader, RS-232 card receiver and tamper input.

Movement

You can view the working status of motor encoder.

Others

Passing Mode

You can view the entrance and exit mode.

IR Detector Status

You can view the status of each pair of the IR beam sensors.

Input and Output Status

You can view the status of the event input/output, alarm input/output and fire alarm.

Other Status

You can view the status of the barrier and the keyfob receiving module.

6.5.18 Log Query

You can search and view the device logs.

Go to **Maintenance and Security → Maintenance → Log** .

Set the major and minor type of the log type. Set the start time and end time for searching, and click **Search**.

The results will be displayed below, which including the No., time, the major type the minor type, the channel No., the local/remote user information, the remote host IP, etc.

6.5.19 Certificate Management

It helps to manage the server/client certificates and CA certificate.

Note

The function is only supported by certain device models.

Create and Install Self-signed Certificate

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. In the **Certificate Files** area, select a **Certificate Type** from the drop-down list.
3. Click **Create**.
4. Input certificate information.
5. Click **OK** to save and install the certificate.

   The created certificate is displayed in the **Certificate Details** area.

   The certificate will be saved automatically.
6. Download the certificate and save it to an asking file in the local computer.
7. Send the asking file to a certification authority for signature.
8. Import the signed certificate.
   1) Select a certificate type in the **Import Passwords** area, and select a certificate from the local, and click **Install**.
   2) Select a certificate type in the **Import Communication Certificate** area, and select a certificate from the local, and click **Install**.

Install Other Authorized Certificate

If you already has an authorized certificate (not created by the device), you can import it to the device directly.

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. In the **Import Passwords** and **Import Communication Certificate** areas, select certificate type and upload certificate.
3. Click **Install**.

Install CA Certificate

Before You Start

Prepare a CA certificate in advance.

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. Create an ID in the **Import CA Certificate** area.

   Note

   The input certificate ID cannot be the same as the existing ones.
3. Upload a certificate file from the local.
4. Click **Install**.

Chapter 7 Configure the Device via the Mobile Browser

7.1 Login

You can log in via mobile browser.

Note

Make sure the device is activated.

You can log in via the following methods:

- If device hotspot is disabled, make sure your mobile phone and the device are connected to the same network. Place your phone to the NFC area and the login page will pop up. If device hotspot is enabled, place your phone to the NFC area and the name and pass
- When the device hotspot is enabled, you can connect to the device hotspot and the loginpage will pop up.
  Enter the device user name and the password. Click **Login**.
- When the device hotspot is enabled, place your phone to the NFC area and the name and passwordof the device hotspot will be obtained automatically.

Note

Android system supporting NFC function is recommended. IOS system is not supported.

7.2 Overview

You can view the device status, conduct remote control, etc.

You can view the device status. If there is exception, you can tap to view the component details.

You can remotely control barrier by tap the icons.

Figure 7-1 Shortcut Entry and Network Status

You can tap to fast enter the basic settings page, user page, keyfob page, light page and network page.

7.3 Configuration

7.3.1 Turnstile Basic Parameters

You can set the basic parameters of the turnstile.

Tap **Basic Settings** of the shortcut entry on the overview page.

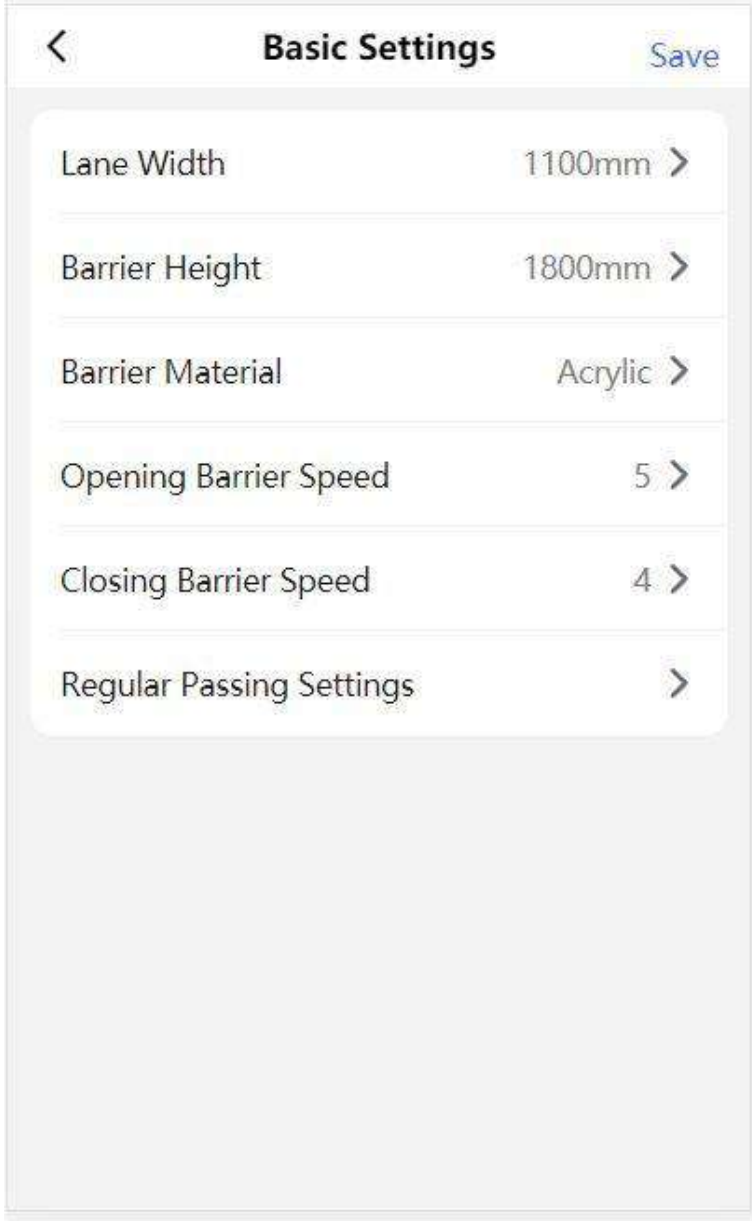


Figure 7-2 Turnstile Basic Parameters

Set **Lane Width**, **Barrier Height**, **Barrier Height**, **Barrier Opening Speed** and **Barrier Closing Speed**.
Set the regular passing mode for the entrance and exit.
Tap **Save**.

7.3.2 User Management

You can add, edit, delete, and search users via mobile Web browser.

Steps

1. Tap **User** to enter the settings page.

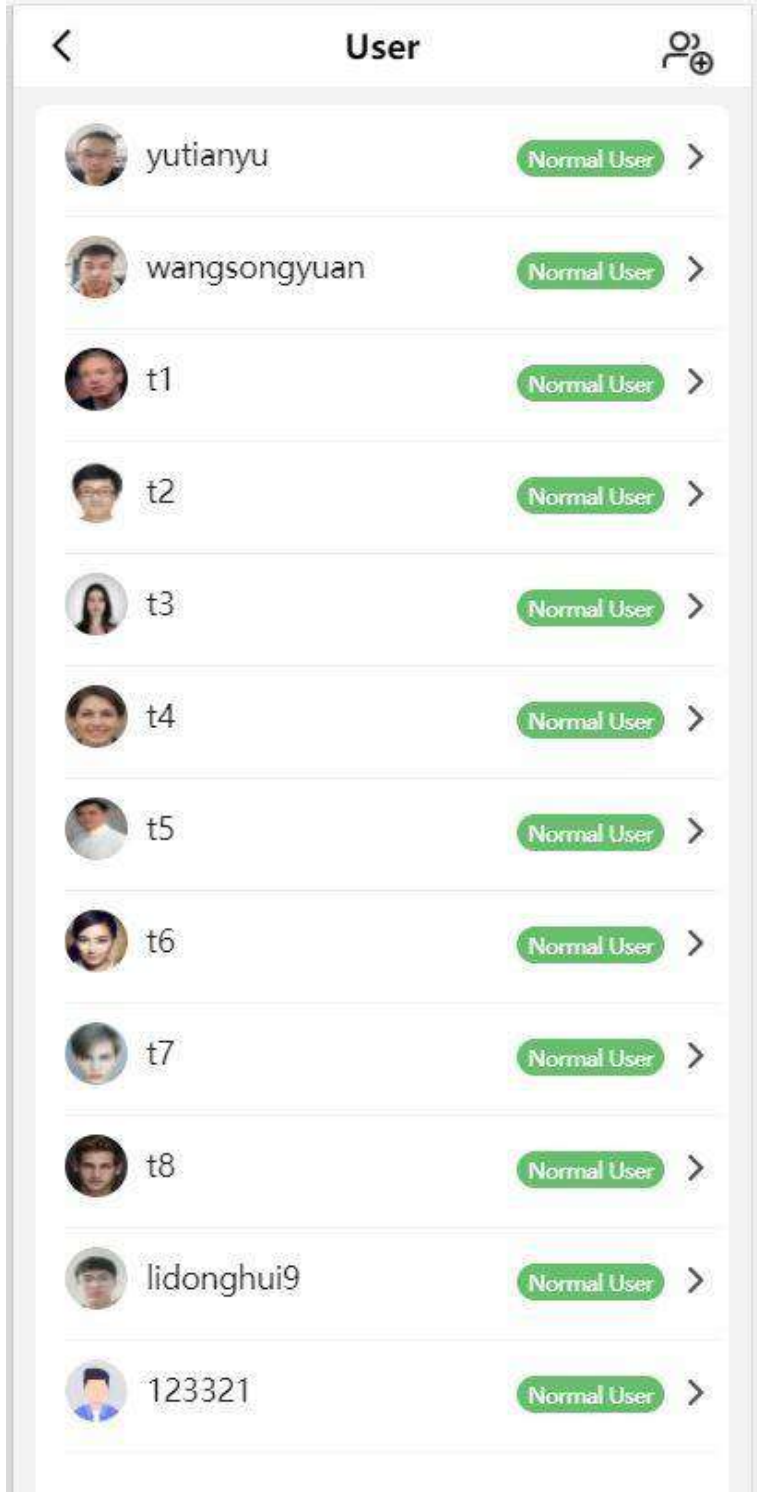


Figure 7-3 Add User

2. Add user.

1) Tap .

2) Set the following parameters.

Employee ID

Enter the employee ID. The Employee ID cannot be 0 or exceed 32 characters. It can be a combination of uppercase, lowercase letters and numbers.

Name

Enter your name. The name supports numbers, uppercase and lowercase English, and characters. The name is recommended to be within 32 characters.

User Role

Select your user role.

Card

Add card. Tap **Card → Add Card** , enter the card No. and select the card type.

3) Tap **Save**.

3. Tap the user that needs to be edited in the user list to edit the information.

7.3.3 Keyfob Settings

Tap **Keyfob** of the shortcut entry on the overview page.

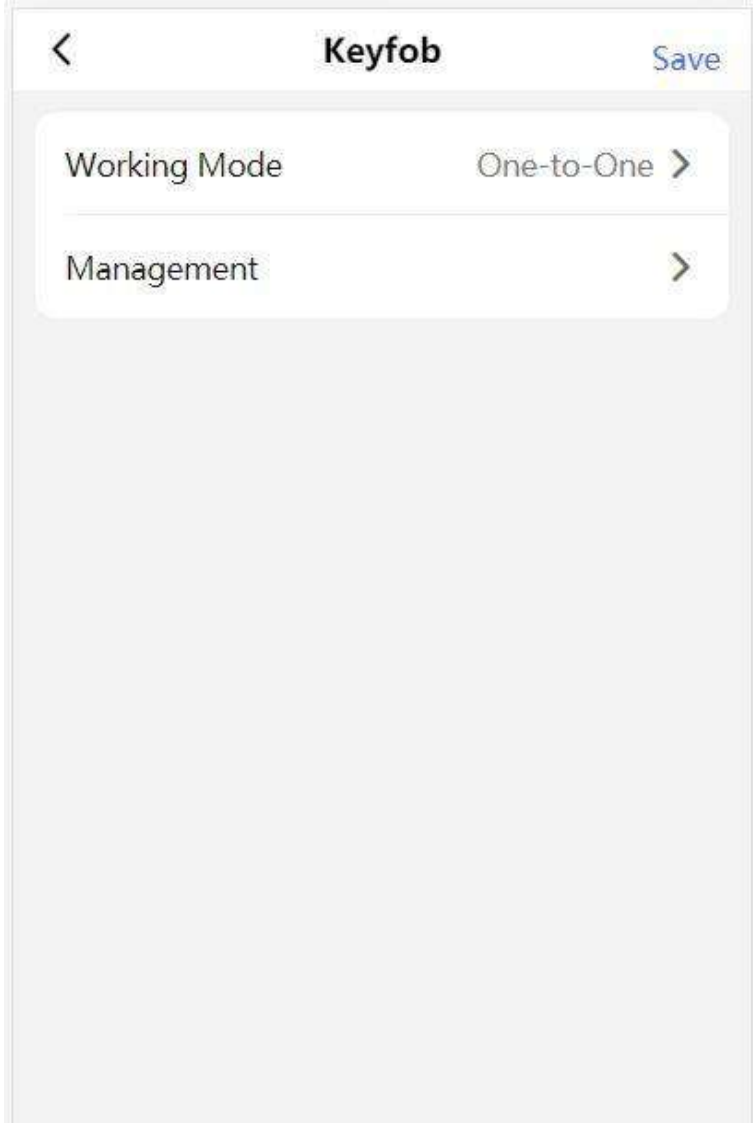


Figure 7-4 Keyfob Settings

Set **Working Mode** as **One-to-One** or **One-to-Many**.

Tap **Management** to enter the page. Tap **+** to add keyfob. Set keyfob name, serial No. and remain open permission.

7.3.4 Light Settings

Tap **Light** of the shortcut entry on the overview page.

Lane Status Indicator

Figure 7-5 Lane Status Indicator Settings

Light Brightness is set **Manual** by default. Enter the value to adjust the light brightness manually. Set light color for inductive/remain open, remain closed and controlled/barrier-free mode respectively.

Barrier Light

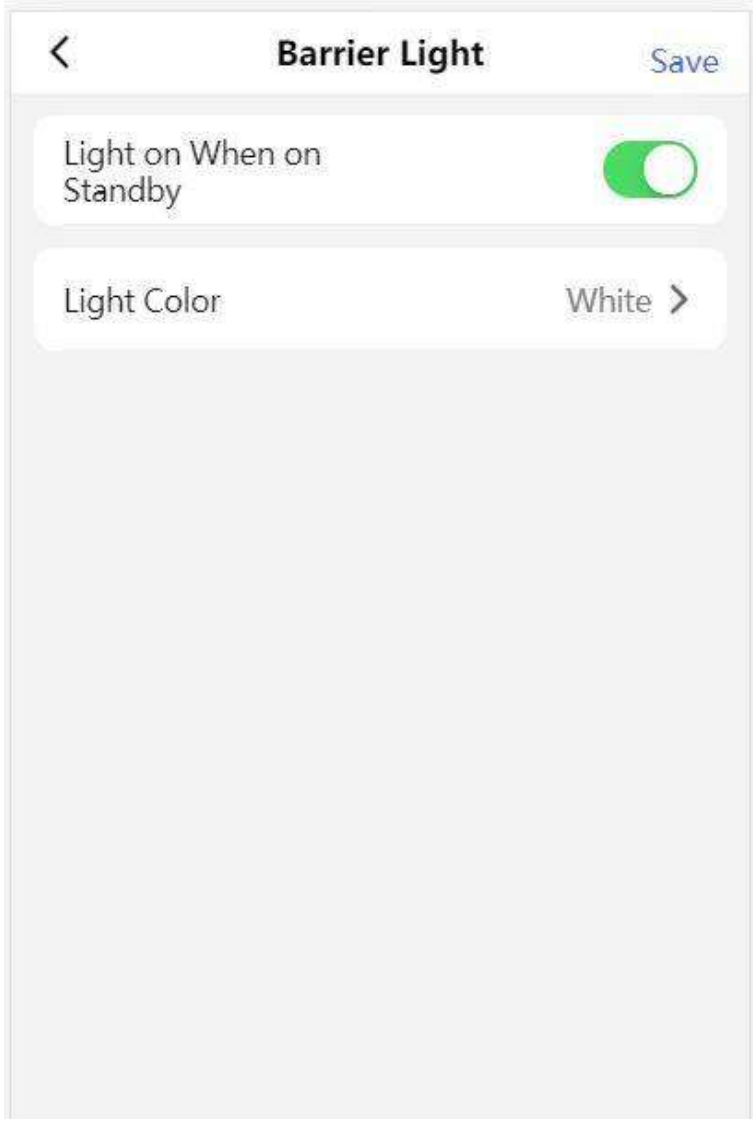


Figure 7-6 Barrier Light Settings

Tap to enable **Light on When on Standby** at your actual needs and set the barrier light color.

7.3.5 Network Settings

You can set the wired network, device hotspot and port.

Wired Network

Set wired network.

Tap **Configuration → Communication Settings → Wired Network** to enter the configuration page.

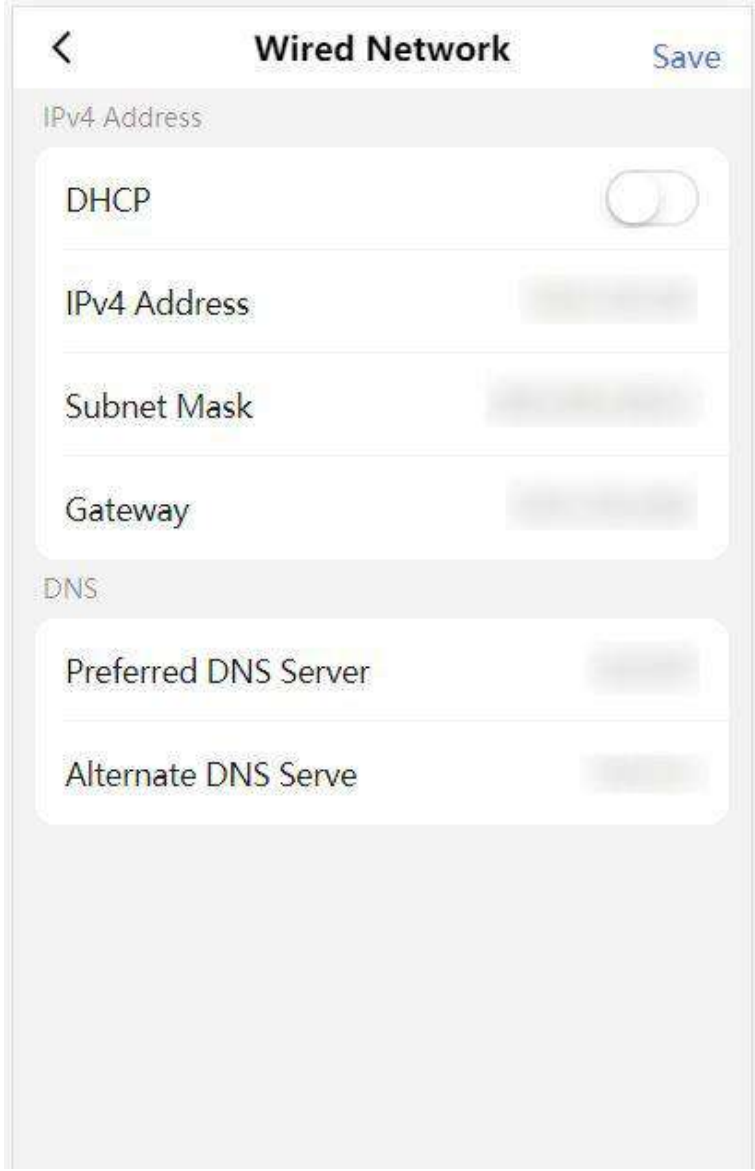


Figure 7-7 Wired Network

DHCP

If you disable the function, you should set the IPv4 address, IPv4 subnet mask, and IPv4 default gateway.

If you enable the function, the system will allocate the IPv4 address, IPv4 subnet mask, and IPv4 default gateway automatically.

DNS Server

Set the preferred DNS server and the Alternate DNS server according to your actual need.

Device Hotspot

Set device hotspot.

Tap **Configuration → Communication Settings → Device Hotspot** to enter the configuration page.

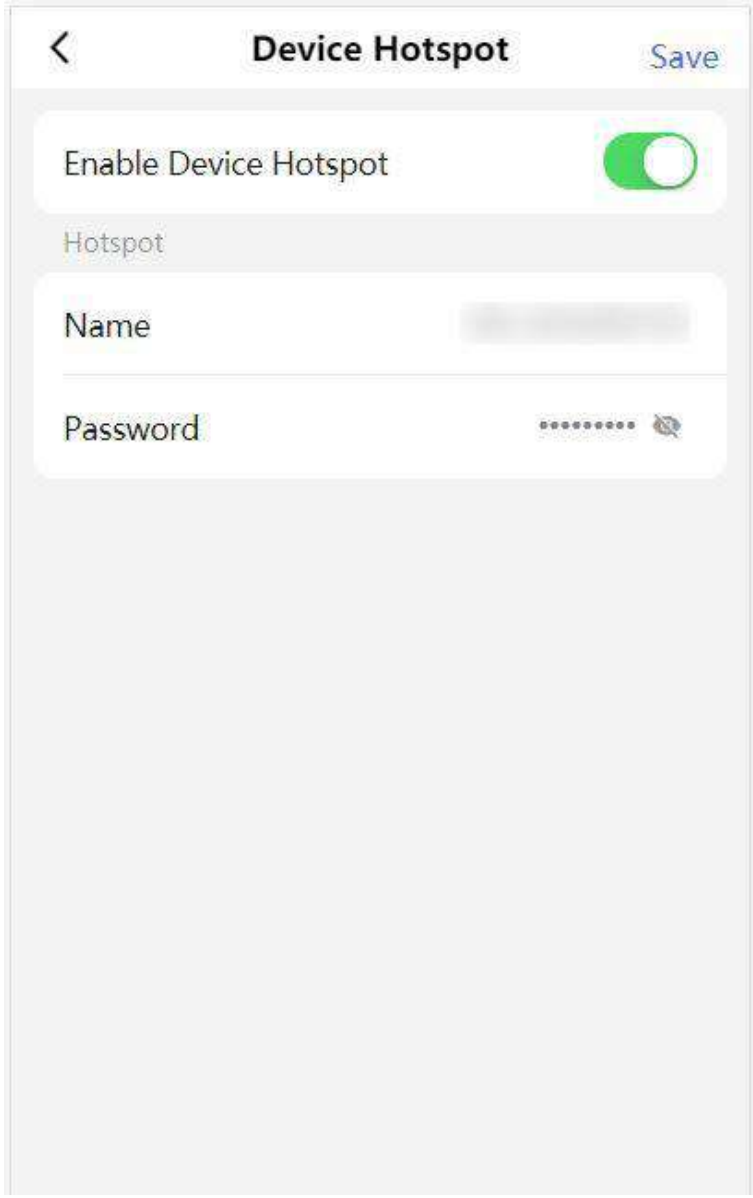


Figure 7-8 Device Hotspot

Tap to **Enable Device Hotspot**. Set hotspot **Name** and **Password**.

Click **Save**.

Serial Port Configuration

Set serial port.

Tap **Configuration → Communication Settings → Serial Port Configuration** to enter the configuration page.

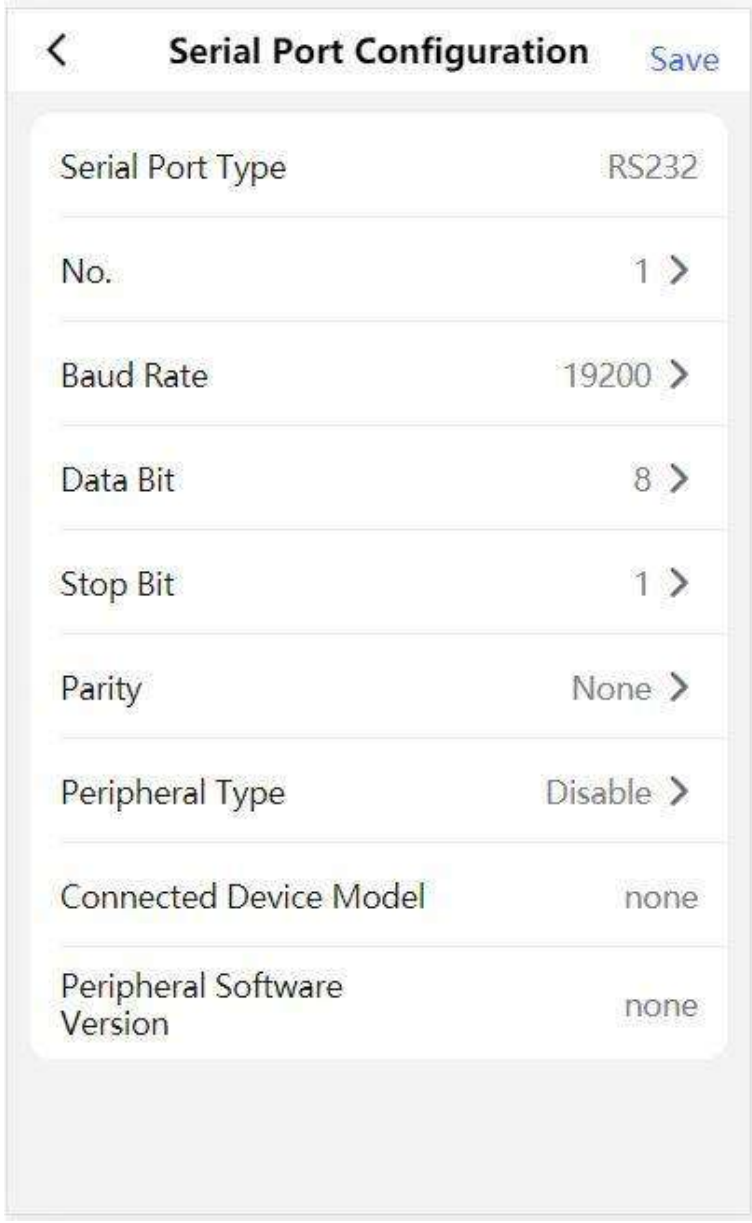


Figure 7-9 Serial Port Configuration

Select the port **No.**, and set **Baud Rate**, **Data Bit**, **Stop Bit** and **Parity**.

Set the **Peripheral Type** as **Card Reader**, **Card Receiver**, **QR Code Scanner** or **Disable**.

Tap **Save**.

7.3.6 Device Basic Settings

Set audio, time, sleep time and privacy.

Tap **Configuration → Basic Settings** to enter the configuration page.

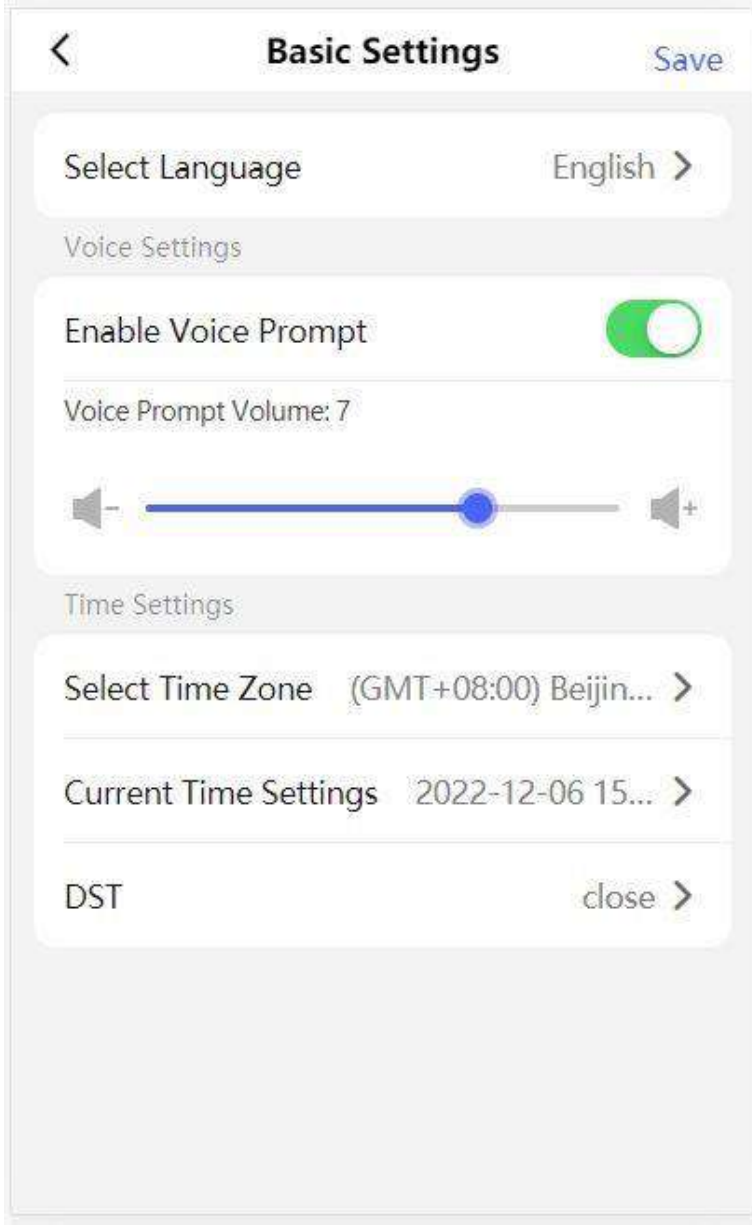


Figure 7-10 Basic Configuration

Language

The language is set English by default.

Voice Settings

Tap to **Enable Voice Prompt**, select entrance or exit to set voice prompt and drag to set the volume.

Time Settings

Tap to select the time zone and the device time.

Tap **DST** to enter the DST setting page. Enable DST and set the DST start time, end time and bias time

7.3.7 Access Control Settings

Set Door Parameters

Tap **Configuration → Access Control → Door Parameters** .

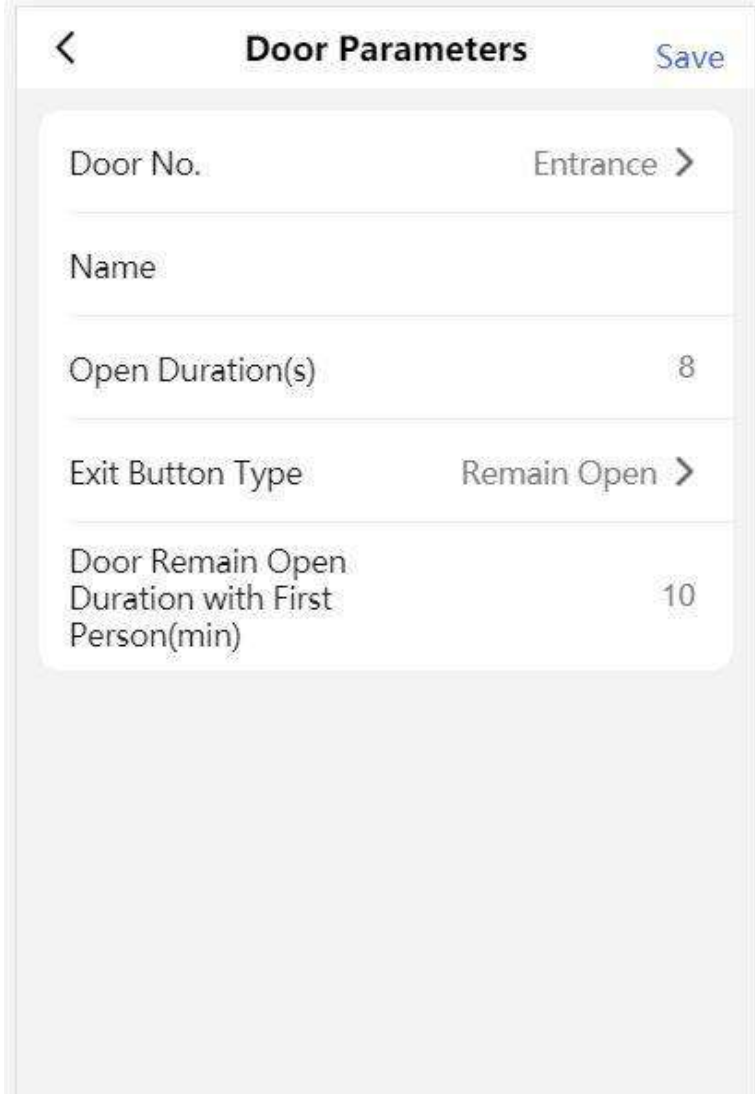


Figure 7-11 Door Parameters Settings Page

Click **Save** to save the settings after the configuration.

Door No.

Select the device corresponded door No.

Name

You can create a name for the door.

Open Duration

Set the door unlocking duration. If the door is not opened for the set time, the door will be locked.

Exit Button Type

You can set the exit button as **Remain Open** or **Remain Closed** according to your actual needs. By default, it is **Remain Open**.

Door Remain Open Duration with First Person

Set the door open duration when first person is in. After the first person is authorized, it allows multiple persons access the door or other authentication actions.

Set Authentication Parameters

Set Authentication Parameters.

Steps

1. Tap **Configuration → Access Control → Authentication Settings** .

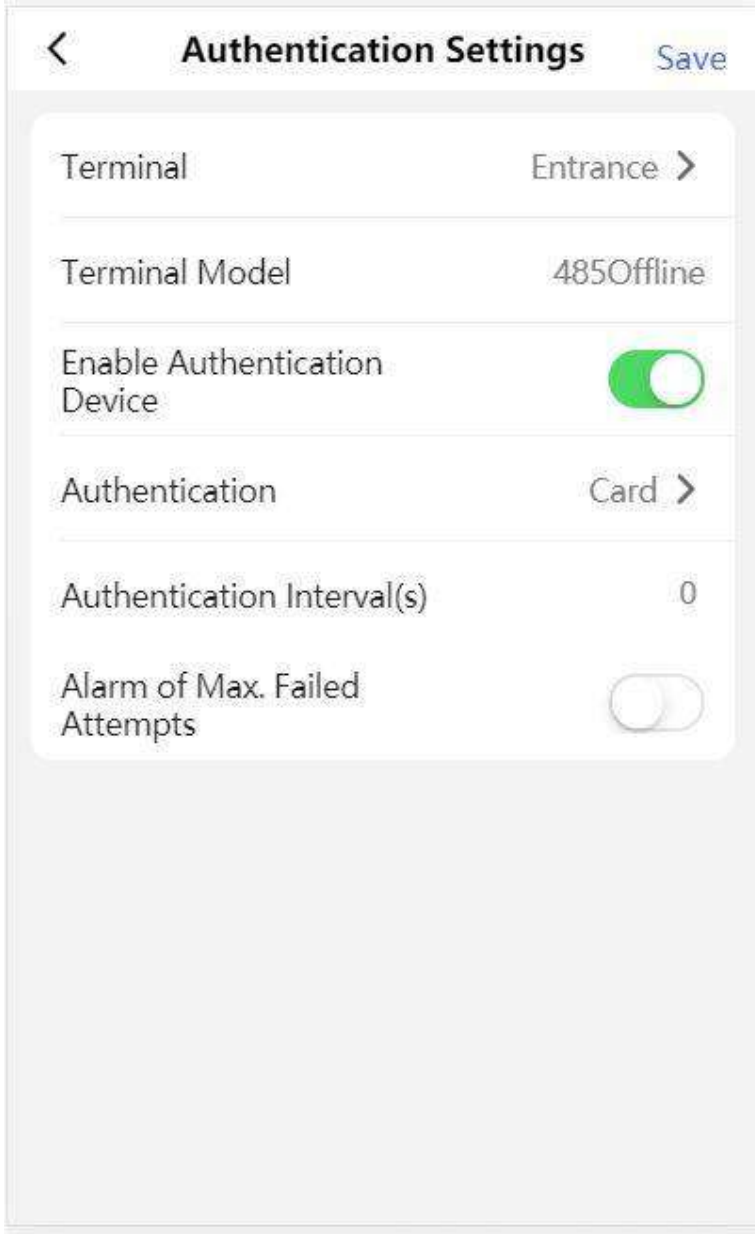


Figure 7-12 Authentication Settings

2. Tap **Save**.

Terminal

Choose **Entrance** or **Exit** for settings.

Terminal Model

Terminal model is read-only.

Enable Authentication Device

Enable the authentication function.

Authentication

Authentication via card by default.

Authentication Interval

You can set the authentication interval of the same person when authenticating. The same person can only authenticate once in the configured interval. A second authentication will be failed.

Alarm of Max. Failed Attempts

Enable to report alarm when the card reading attempts reach the set value.

Set Card Security

Tap **Configuration → Access Control → Card Security** to enter the settings page.

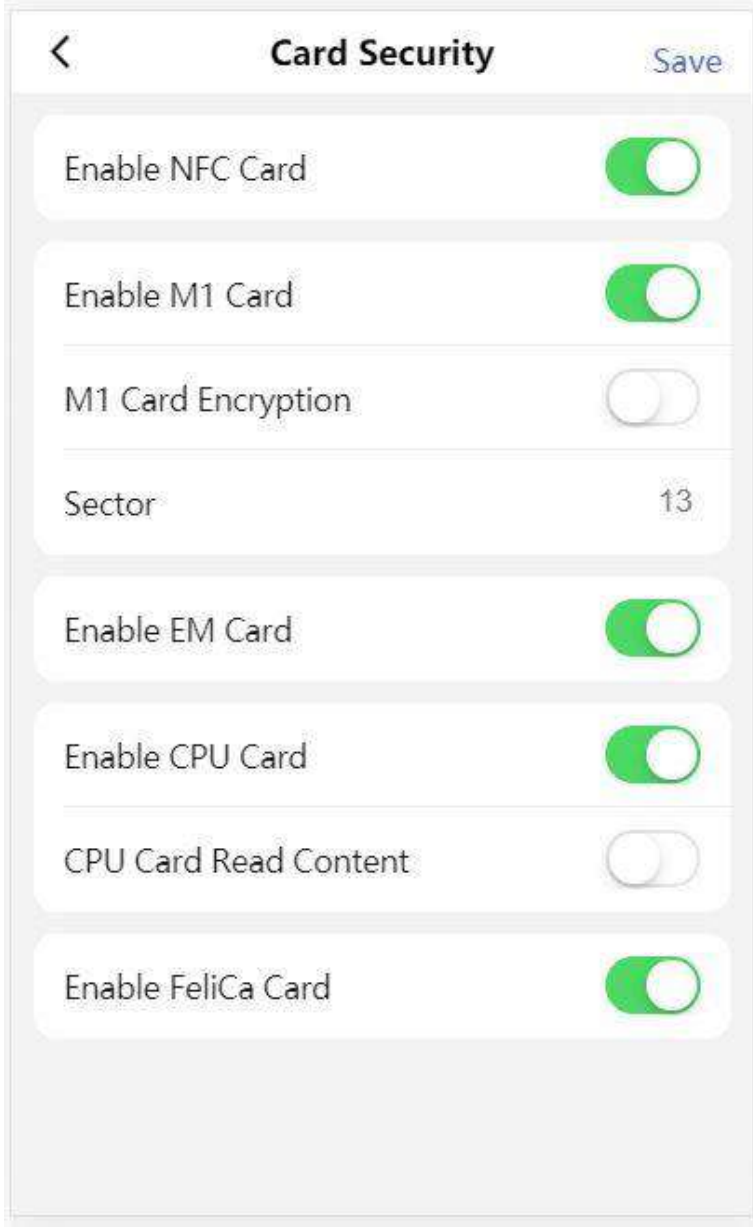


Figure 7-13 Card Security

Set the parameters and click **Save**.

Enable NFC Card

In order to prevent the mobile phone from getting the data of the access control, you can disable NFC card to increase the security level of the data.

Enable M1 Card

Enable M1 card and authenticating by presenting M1 card is available.

M1 Card Encryption

M1 card encryption can improve the security level of authentication.

Sector

Enable the function and set the encryption sector. By default, Sector 13 is encrypted. It is recommended to encrypt sector 13.

Enable EM Card

Enable EM card and authenticating by presenting EM card is available.

Note

If the peripheral card reader supports presenting EM card, the function is also supported to enable/disable the EM card function.

Enable CPU Card

The device can read the data from CPU card when enabling the CPU card function.

CPU Card Read Content

After enable the CPU card content reading function, the device can read the CPU card content.

Enable FeliCa Card

The device can read the data from FeliCa card when enabling the FeliCa card function.

Terminal Settings

Set the working mode.

Tap **Configuration → Access Control → Terminal Parameters** to enter the settings page.

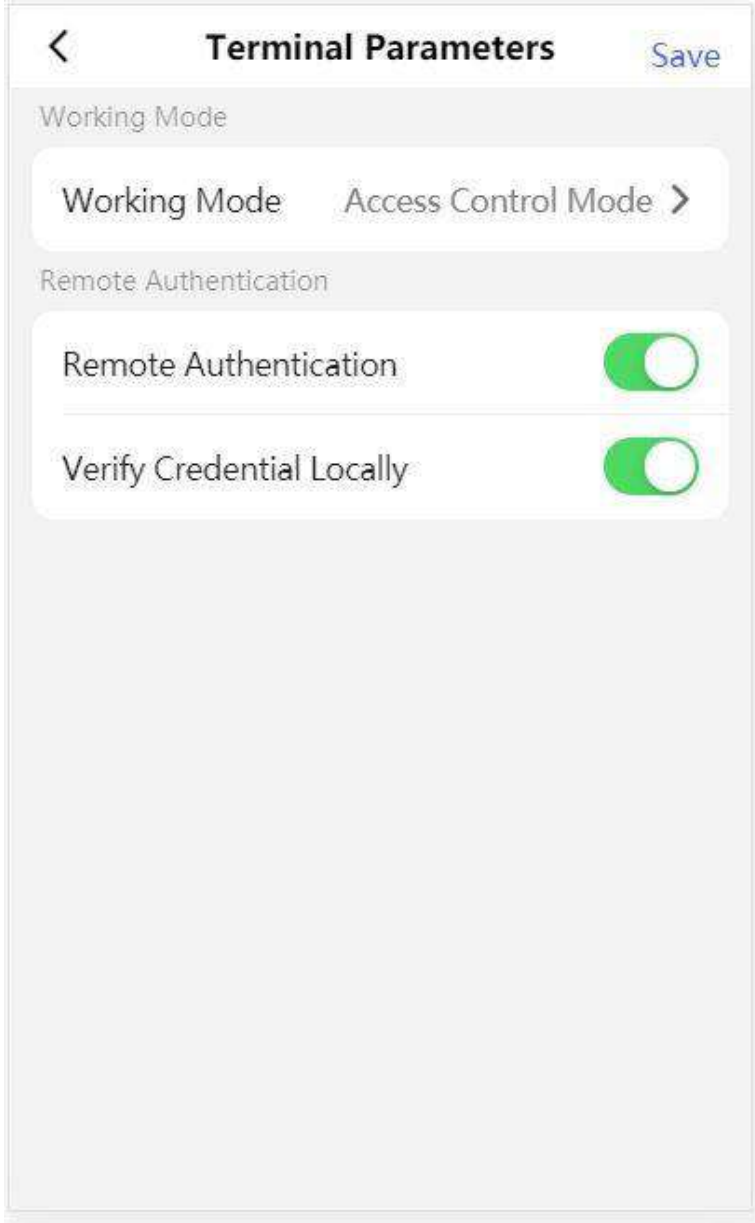


Figure 7-14 Terminal Parameters

Permission Free Mode

The device will not verify the person's permission, but only the person's validity period. If the person is in the validity period, the barrier will open.

You can enable **Verify Credential Locally**. After enabling the function, the device will only verify the person's permission without the schedule template, etc.

Access Control Mode

The device works normally and will verify the person's permission to open the barrier.

Remote Authentication

The device will upload the person's authentication information to the platform. The platform will judge to open the barrier or not.

Verify Credential Locally

The device will only verify the person's permission without the schedule template, etc.

7.3.8 View Device Information

View the device name, language, model, serial No., version, etc.

Tap **Configuration → System Information** to enter the configuration page.

You can view the language, model, serial No., version, IO input and output number, local RS-485 number, MAC address and open source license.

You can change the device name. Tap **Save**.

7.3.9 Device Capacity

Tap **Configuration → Device Capacity** to enter the page.

You can view the quantity of user, card and event.

7.3.10 Log Export

Tap **Configuration → Log Export** to enter the page.

Select a log type and tap **Export**.

7.3.11 Restore and Reboot

Reboot device and restore device parameters.

Restore

Tap **Configuration → Restore** .
All parameters will be restored to the factory settings.

Restart Devices

Tap **Configuration → Restart Devices** .
Tap **Reboot** to reboot the device.

Chapter 8 Client Software Configuration

You can call the hotline to get the iVMS-4200 client software installation package.

8.1 Configuration Flow of Client Software

Follow the flow diagram below to configure on the client software.

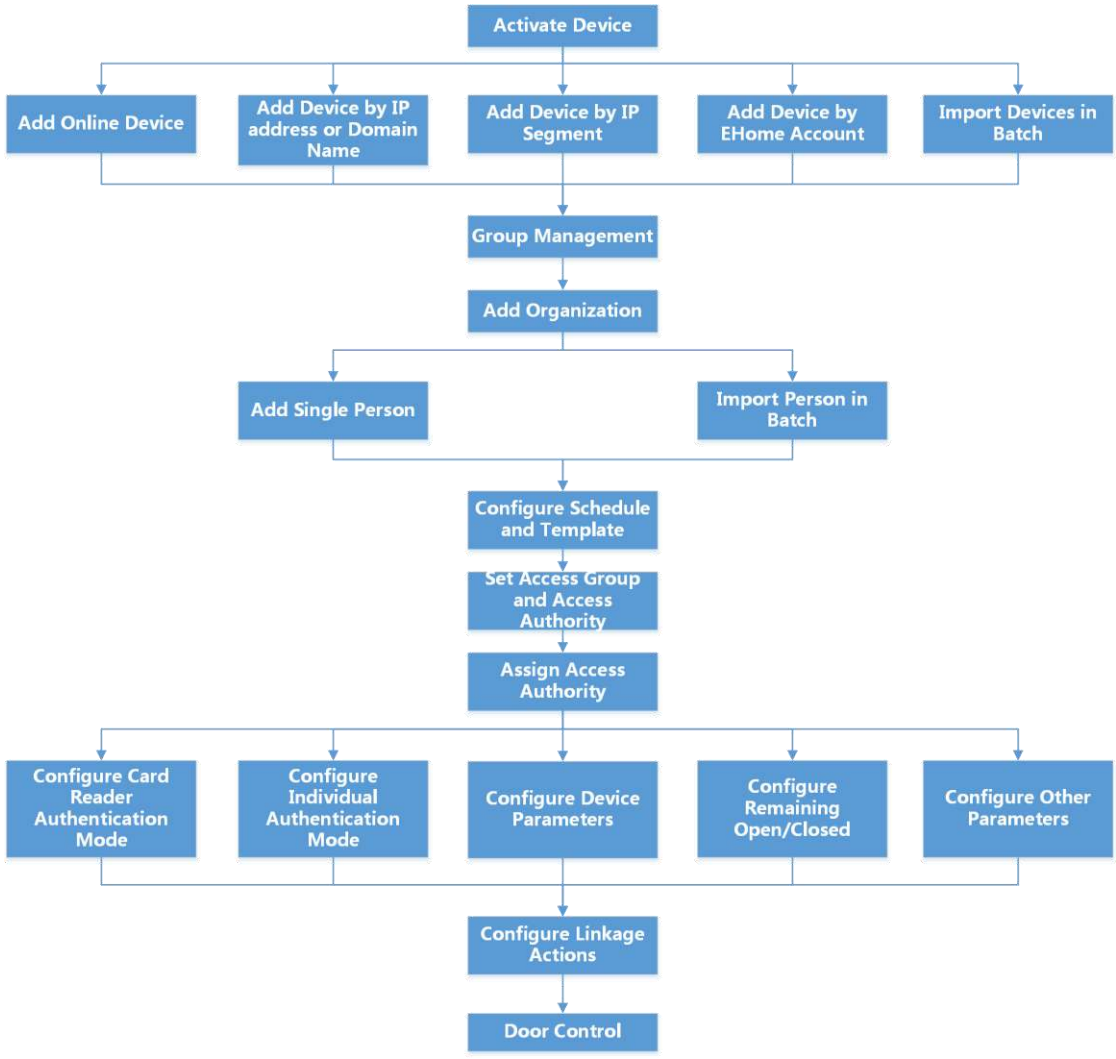


Figure 8-1 Flow Diagram of Configuration on Client Software

8.2 Device Management

The client supports managing access control devices and video intercom devices.

Example
You can control entrance & exit and manage attendance after adding access control devices to the client; you can perform video intercom with the indoor stations and door stations.

8.2.1 Add Device

The client provides three device adding modes including by IP/domain, IP segment, and ISUP protocol. The client also supports importing multiple devices in a batch when there are large amount of devices to be added.

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.
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:** 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 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 access control device, its access points, alarm inputs/outputs, and encoding channels (if exist) will be imported to this group.
8. 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.

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.
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.

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.

6. Click ··· and select the template file.

7. Click **Add** to import the devices.

8.2.2 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 **Online Device** to show the online device area.

All the online devices sharing the same subnet will be displayed in the list.

3. Select the device from the list and click on the Operation column.
4. Reset the device password.
   - 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.

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.

8.2.3 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 8-1 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	Click to set remote configuration of the corresponding device. For details, refer to the user manual of device.
View Device Status	Click to view device status, including door No., door status, etc. **Note** For different devices, you will view different information about device status.

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.

8.3 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 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 control door status, and do some other operations of the devices after managing the resources by groups.

8.3.1 Add Group

You can add group to organize the added device for convenient management.

Steps
1. Enter the Device Management module.
2. Click **Device Management → Group** to enter the group management page.
3. Create a group.
   - Click **Add Group** and enter a group name as you want.
   - Click **Create Group by Device Name** and select an added device to create a new group by the name of the selected device.

Note
The resources (such as alarm inputs/outputs, access points, etc.) of this device will be imported to the group by default.

8.3.2 Import Resources to Group

You can import the device resources (such as alarm inputs/outputs, access points, etc.) to the added group in a batch.

Before You Start
Add a group for managing devices. Refer to ***Add Group*** .

Steps
1. Enter the Device Management module.

2. Click **Device Management → Group** to enter the group management page.
3. Select a group from the group list and select the resource type as **Access Point**, **Alarm Input**, **Alarm Output**, etc.
4. Click **Import**.
5. Select the thumbnails/names of the resources in the thumbnail/list view.

Note

You can click or to switch the resource display mode to thumbnail view or to list view.

6. Click **Import** to import the selected resources to the group.

8.4 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.

8.4.1 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 surbodinate 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.

8.4.2 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.

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.

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.

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 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.

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 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).

8.4.3 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.

8.4.4 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 .
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).

8.4.5 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.

8.4.6 Set Card Issuing Parameters

The client provides two modes for reading a card's number: via card enrollment station or via the card reader of the access control device. If a card enrollment station is available, connect it to the PC running the client by USB interface or COM, and place the card on the card enrollment to read the card number. If not, you can also swipe the card on the card reader of the added access control device to get the card number. As a result, before issuing a card to one person, you need to set the card issuing parameters including the issuing mode and related parameters.

When adding a card to one person, click **Settings** to open the Card Issuing Settings window.

Local Mode: Issue Card by Card Enrollment Station

Connect a card enrollment station to the PC running the client. You can place the card on the card enrollment station to get the card number.

Card Enrollment Station

Select the model of the connected card enrollment station

Note

Currently, the supported card enrollment station models include DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E, and DS-K1F180-D8E.

Card Type

This field is only available when the model is DS-K1F100-D8E or DS-K1F180-D8E.

Select the card type as EM card or IC card according to the actual card type.

Serial Port

It is only available when the model is DS-K1F100-M.

Select the COM the card enrollment station connects to.

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

This field is only available when the model is DS-K1F100-D8, DS-K1F100-D8E, or DS-K1F180-D8E.

If the card is M1 card, and if you need to enable the M1 Card Encryption function, you should enable this function and select the sector of the card to encrypt.

Remote Mode: Issue Card by Card Reader

Select an access control device added in the client and swipe the card on its card reader to read the card number.

8.5 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*** .

8.5.1 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**.

8.5.2 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.

8.6 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.

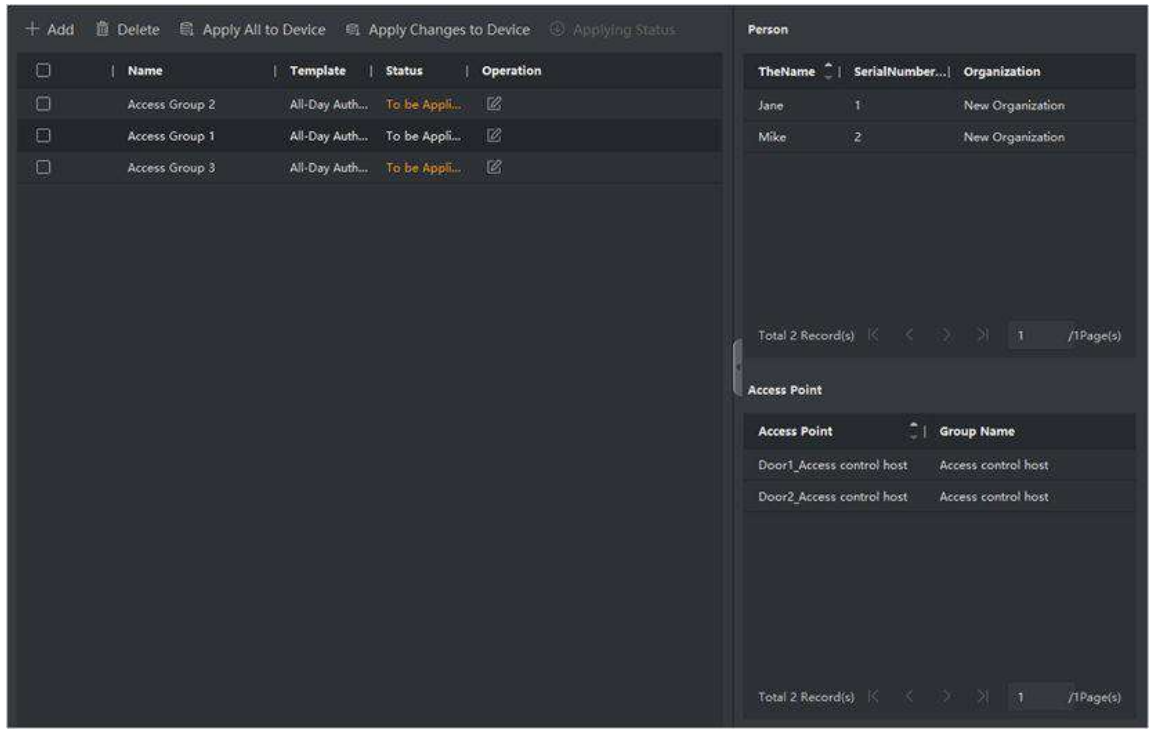


Figure 8-2 Display the Selected Person(s) and Access Point(s)

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**.

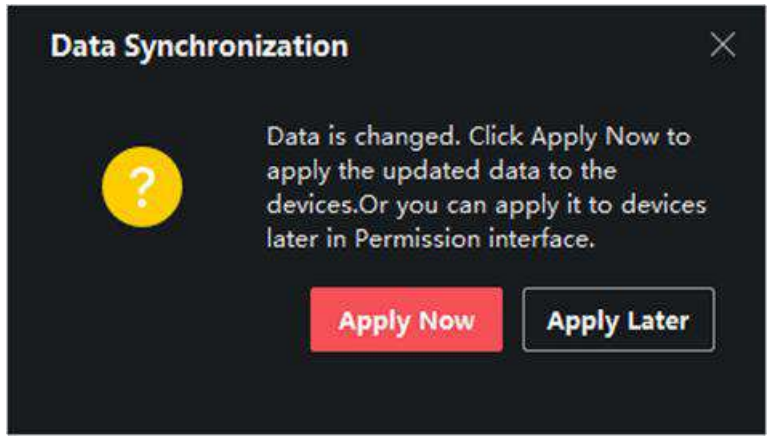


Figure 8-3 Data Synchronization

8.7 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.

8.7.1 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 accesss 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 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**.

8.7.2 Configure Other Parameters

After adding the access control device, you can set its parameters such as network parameters, capture parameters, RS-485 parameters, Wiegand parameters, etc.

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**.

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.

Note

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.

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.

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.

8.8 Door/Elevator Control

In Monitoring module, you can view the real-time status of the doors or elevators managed by the added access control device. You can also control the doors and elevators such as open/close the door, or remain the door open/closed via the client remotely. The real-time access event are displayed in this module. You can view the access details and person details.

Note

For the user with door/elevator control permission, the user can enter the Monitoring module and control the door/elevator. Or the icons used for control will not show. For setting the user permission, refer to .

8.8.1 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 .

Steps

1. Click **Monitoring** to enter the status monitoring page.
2. Select an access point group on the upper-right corner.

   Note

   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.

   Note

   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 .

Result

The icon of the doors will change in real-time according to the operation if the operation is succeeded.

8.8.2 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 8-4 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.

Appendix A. DIP Switch

A.1 DIP Switch Description

The DIP switch is on the access control board. No.1 and No 2 is from the low bit to the high bit.

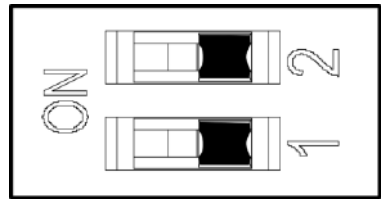


Figure A-1 DIP Switch

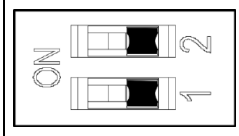
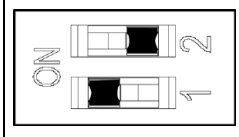
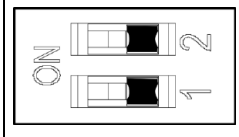
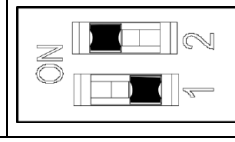
When the switch is towards ON, it means the switch is enabled, otherwise, the switch is off.

A.2 DIP Switch Corresponded Functions

Note

After setting the DIP switch, you should reboot the device, or the function cannot take effect.

The 2-bit DIP switch corresponded functions on the access control board are as follows:

Bit	Device Mode	Function	Decimal Value	DIP Switch Address Diagram
1	Work Mode	Normal Mode	0	
		Study Mode	1	
2	Keyfob Paring Mode	Disable Keyfob Paring Mode	0	
		Enable Keyfob Paring Mode	1	

Appendix B. Button Configuration Description

Refer to the table below for device configuration via button on the main lane control board.

Level-1 Configuration No.	Description	Level-1 Configuration No. and Functions	Notes
1	Study Mode	1-Exit Study Mode/ Normal Mode 2-Study Mode **Note** By default, 1 will be displayed on the display screen.	If the device is equipped with access control board, you can only set via DIP switch.
2	keyfob Pairing Mode	1-Normal Mode 2-Pairing Mode **Note** By default, 1 will be displayed on the display screen.	If the device is equipped with access control board, you can only set via DIP switch.
3	Passing Mode	1-Both sides under control **Note** By default, 1 will be displayed on the display screen. 2-Entrance under control; exit prohibited 3-Entrance under control; exit on inductive mode 4-Both sides on inductive mode	

Level-1 Configuration No.	Description	Level-1 Configuration No. and Functions	Notes
		5-Entrance on inductive mode; exit under control 6-Entrance on inductive mode; exit prohibited 7-Both sides prohibited 8-Entrance prohibited; exit under control 9-Entrance prohibited; exit on inductive mode 10-Entrance under control; exit remaining open 11-Entrance under control; exit on free mode 12-Entrance on inductive mode; exit remaining open 13-Entrance on inductive mode; exit on free mode 14-Entrance prohibited; exit remaining open 15-Entrance prohibited; exit on free mode 16-Entrance remaining open; exit under control 17-Entrance remaining open; exit on inductive mode	

Level-1 Configuration No.	Description	Level-1 Configuration No. and Functions	Notes
		18- Entrance remaining open; exit remaining open 19- Entrance remaining open; exit on free mode 20- Entrance remaining open; exit prohibited 21- Entrance on free mode; exit under control 22- Entrance on free mode; exit on inductive mode 23- Entrance on free mode; exit remaining open 24- Entrance on free mode; exit on free mode 25- Entrance on free mode; exit prohibited	
4	Memory Mode	1-Disable 2-Enable **Note** By default, 2 will be displayed on the display screen.	
5	keyfob Remote Control	1-one to one 2-one to multiple **Note** By default, 1 will be displayed on the display screen.	

Level-1 Configuration No.	Description	Level-1 Configuration No. and Functions	Notes
6	Barrier Opening Speed	1-1, 2-2, …10-10 **Note** By default, 5 will be displayed on the display screen.	
7	Barrier Closing Speed	1-1, 2-2, …10-10 **Note** By default, 5 will be displayed on the display screen.	
8	Card Reading on the Alarm Area	1-Do not open 2-Open **Note** By default, 2 will be displayed on the display screen.	
9	Enter Duration	5-5s, 6-6s, 7-7s, …, 60-60s **Note** By default, 5 will be displayed on the display screen.	
10	Exit Duration	5-5s, 6-6s, 7-7s, …, 60-60s **Note** By default, 5 will be displayed on the display screen.	
11	IR Sensing Duration	0-0s, 1-1s, 2-2s,..., 25-25s	

Level-1 Configuration No.	Description	Level-1 Configuration No. and Functions	Notes
		Note By default, 0 will be displayed on the display screen.	
12	Intrusion Duration	0-0s, 1-1s, 2-2s,..., 20-20s **Note** By default, 0 will be displayed on the display screen.	
13	Overstay Duration	0-0s, 1-1s, 2-2s,..., 20-20s **Note** By default, 0 will be displayed on the display screen.	
14	Delay Time for Barrier Closing	0-0s, 1-1s, 2-2s, 3-3s, 4-4s, 5-5s **Note** By default, 0 will be displayed on the display screen.	
15	Control Mode	1-Button Configuration 2-DIP Switch on Access Control Board **Note** By default, 1 will be displayed on the display screen.	
18	Lane Number	1-Dual Lanes	Unable to change

Level-1 Configuration No.	Description	Level-1 Configuration No. and Functions	Notes
		2-Single Lane **Note** By default, 1 will be displayed on the display screen.	
19	Motor Rotation	1-Clockwise 2-Anticlockwise **Note** By default, 1 will be displayed on the display screen.	Unable to change
21	Volume	1-0, 2-1, 3-2, 4-3, 5-4 **Note** By default, 2 will be displayed on the display screen.	The device will be muted when set to "1".
22	Authenticated Passing	1-Disable 2-Enable **Note** By default, 1 will be displayed on the display screen.	Unable to change via button
23	Invalid Card No.	1-Disable 2-Enable **Note** By default, 1 will be displayed on the display screen.	Unable to change via button

Level-1 Configuration No.	Description	Level-1 Configuration No. and Functions	Notes
24	Fingerprint Unmatched	1-Disable 2-Enable **Note** By default, 1 will be displayed on the display screen.	Unable to change via button
25	Climbing over Barrier	1-Disable 2-Enable **Note** By default, 1 will be displayed on the display screen.	
26	Reverse Passing	1-Disable 2-Enable **Note** By default, 1 will be displayed on the display screen.	
27	Exceeding Passing Duration	1-Disable 2-Enable **Note** By default, 1 will be displayed on the display screen.	
28	Intrusion Alarm	1-Disable 2-Enable **Note** By default, 1 will be displayed on the display screen.	

Level-1 Configuration No.	Description	Level-1 Configuration No. and Functions	Notes
29	Forced Passing	1-Disable 2-Enable **Note** By default, 1 will be displayed on the display screen.	Unable to change via button
30	Tailgating Alarm	1-Disable 2-Enable **Note** By default, 1 will be displayed on the display screen.	
31	Unauthorized Passing	1-Disable 2-Enable **Note** By default, 1 will be displayed on the display screen.	Unable to change via button
32	Exceeding Authentication Duration	1-Disable 2-Enable **Note** By default, 1 will be displayed on the display screen.	Unable to change via button
33	Failed Authentication	1-Disable 2-Enable **Note** By default, 1 will be displayed on the display screen.	Unable to change via button

Level-1 Configuration No.	Description	Level-1 Configuration No. and Functions	Notes
34	Expired Credential	1-Disable 2-Enable **Note** By default, 1 will be displayed on the display screen.	Unable to change via button
35	Overstaying Alarm	1-Disable 2-Enable **Note** By default, 1 will be displayed on the display screen.	
36	Barrier Material	1-Acrylic 2-Stainless Steel 3-Glass	
37	Barrier Length	1-550 2-600 3-650 4-700 5-750 6-800 7-850 8-900 9-950 10-1000 11-1100 12-1200 13-1300 14-1400	

Level-1 Configuration No.	Description	Level-1 Configuration No. and Functions	Notes
		Note By default, 8 will be displayed on the display screen.	
38	Motor Inspection	1-Disable 2-Enable on Main Lane 3-Enable on Sub Lane **Note** By default, 1 will be displayed on the display screen.	
39	Brightness of Light	0-0, 1-1, 2-2, … , 10-10 **Note** By default, 3 will be displayed on the display screen.	The higher the value is, the brighter the light will be.
40	Self-check Voice Prompt	1-Disable 2-Enable **Note** By default, 2 will be displayed on the display screen.	
41	Study Mode Voice Prompt	1-Disable 2-Enable **Note** By default, 2 will be displayed on the display screen.	

Level-1 Configuration No.	Description	Level-1 Configuration No. and Functions	Notes
42	c	4-4, 6-6, 8-8, **Note** By default, 4 will be displayed on the display screen.	Unable to change via button
43	Application Mode	1-Wind-proof 2-Indoor By default, 1 will be displayed on the display screen.	
44	Barrier Recover Duration	1-Normal Speed 2-Fast Recover By default, 1 will be displayed on the display screen.	
45	Brake	1-Disable 2-Barrier Position Exception 3-Intrusion By default, 2 will be displayed on the display screen.	
46	Brake Angle	1-5° 2-10° 3-15° By default, 1 will be displayed on the display screen.	
47	IR Sensing	1-Single Triggered 2-Triggered Simultaneously	

Level-1 Configuration No.	Description	Level-1 Configuration No. and Functions	Notes
		By default, 1 will be displayed on the display screen.	
48	Fan	1-Disabled 2-Enabled By default, 2 will be displayed on the display screen.	
49	Barrier Height	1-700 2-1200 3-1400 4-1600 5-1800 By default, 5 will be displayed on the display screen.	
99	Restore to Default	1- Default 2- Start **Note** By default, 1 will be displayed on the display screen.	

Appendix C. Event and Alarm Type

Event	Alarm Type
Tailgating	Visual and Audible
Reverse Passing	Visual and Audible
Force Accessing	None
Climb over Barrier	Visual and Audible
Overstay	Visual and Audible
Passing Timeout	None
Intrusion	Visual and Audible
Free Passing Authentication Failed	Visual and Audible
Barrier Obstructed	None

Appendix D. Table of Audio Index Related Content

Note

- If the device is not equipped with access control board, the loudspeaker shall be connected to the main extended interface board.
- If the device is equipped with access control board, the loudspeaker shall be connected to the access control board. You can set custom broadcasting context via web.

Content
Climbing over the barrier.
Reverse passing.
Passing timeout.
Intrusion.
Tailgating.
Overstay.

Appendix E. Error Code Description

The swing barrier will display the error code on the seven-segment display if error occurred. Refer to the table below to find the description of each number.

Error Reason	Code	Error Reason	Code
The First IR Beam Triggered	01	The Thirteenth IR Beam Triggered	13
The Second IR Beam Triggered	02	The Fourteenth IR Beam Triggered	14
The Third IR Beam Triggered	03	Authentication Indicator Board (Entrance) Offline	49
The Fourth IR Beam Triggered	04	Authentication Indicator Board (Exit) Offline	50
The Fifth IR Beam Triggered	05	IR Adapter Board Offline	51
The Sixth IR Beam Triggered	06	Interconnecting Exception	53
The Seventh IR Beam Triggered	07	Not Studying	54
The Eighth IR Beam Triggered	08	Obstruction	55
The Ninth IR Beam Triggered	09	Exceeding Studying Range	56
The Tenth IR Beam Triggered	10	Encoder Exception	57
The Eleventh IR Beam Triggered	11	Motor Exception	58
The Twelfth IR Beam Triggered	12	Extended Interface Board Offline (If the board is not installed, the error code of "49" will appear but the device functions normally)	59

Appendix F. Communication Matrix and Device Command

Communication Matrix

Scan the following QR code to get the device communication matrix.
Note that the matrix contains all communication ports of Hikvision access control and video intercom devices.

Figure F-1 QR Code of Communication Matrix

Device Command

Scan the following QR code to get the device common serial port commands.
Note that the command list contains all commonly used serial ports commands for all Hikvision access control and video intercom devices.

Figure F-2 Device Command


See Far, Go Further

São Paulo, 29 de Outubro de 2024.

Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro
CNPJ: 30.121.578/0001-67
Ref.: PREGÃO ELETRÔNICO PARA REGISTRO DE PREÇOS nº 003/2024
Processo nº SEI-430002/000130/2024

DECLARAÇÃO

A HIKVISION DO BRASIL COMÉRCIO DE EQUIPAMENTOS DE SEGURANÇA LTDA, estabelecida na Praça Professor José Lannes, 40, 15º andar - Cidade Monções, São Paulo - SP, 04.571-100, inscrita no CNPJ Nº 15.431.830/0001-40, como fabricante líder em soluções tecnológicas e sistemas de segurança, vem por meio desta atestar que a Catraca IP Hikvision **DS-K3BC411X-RS-M1** atende todos os itens do termo de referencia onde está sendo licitada.

Atenciosamente,

Mario Ma

_____

Jie Ma
President of Hikvision Brazil
mario.ma@hikvision.com

DS-K4H255S
Single Door Magnetic Lock

The DS-K4H255S Single-Door magnetic lock is designed for wooden door, glass door, and metal door. Aluminum is the main material .The maximum thrust of the lock is 272 kg (600 Lbs). It can be used for controlling door opening/closing. Special anti-residual magnetism designed makes the access control automation safer and electric lock more durable.

- Magnetic lock supports up to 272 kg (600 Lbs) of thrust
- Power supply can be 12 VDC or 24 VDC, (default voltage is 12 VDC)
- Suitable for wooden door, glass door, metal door
- High strength material , anodized aluminum housing
- Magnetic lock , completely using electromagnetic suction work
- Abrasion-proof materials

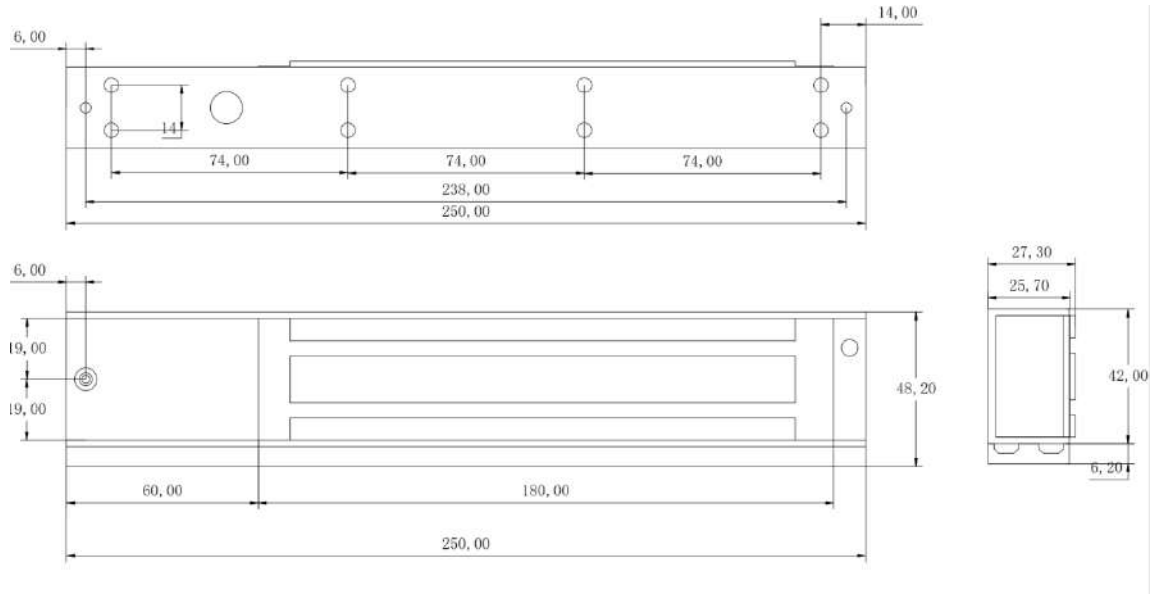
▪ Specification

General	
Power supply	12 VDC to 24 VDC, 470 mA to 235 mA
Working temperature	-10 °C to 55 °C (14 °F to 131 °F)
Working humidity	0 to 95 % (relative humidity)
Dimensions	Lock Body: 250 mm × 28 mm × 48 mm (9.8" × 1.1" × 1.9") Armature Plate: 180 mm × 38 mm × 12 mm (7.1" × 1.5" × 0.5")
Weight	1.9 kg (4.2 lb)
Material	Shell: hard Anodizing Electroplating Operated Lock Body: eco-friendly Zinc Electroplating Operated Armature Plate: eco-friendly Zinc Electroplating Operated
Door type	Glass door, wooden door, and metal door
Thrust	Max. 272 kg (600 Lbs)
Magnetic Lock	
Unlock method	Current Interruption

▪ Available Model

DS-K4H255S

▪ Dimension



Headquarters
No.555 Qianmo Road, Binjiang District,
Hangzhou 310051, China
T +86-571-8807-5998
www.hikvision.com

Follow us on social media to get the latest product and solution information.

Hikvision HikvisionHQ HikvisionHQ Hikvision_Global Hikvision Corporate Channel hikvisionhq

▪ Accessory

▪ Included

DS-K4H255-LZ Value Magnetic Locks	DS-K4H255-U Value Magnetic Locks
	

Headquarters
No.555 Qianmo Road, Binjiang District,
Hangzhou 310051, China
T +86-571-8807-5998
www.hikvision.com

Follow us on social media to get the latest product and solution information.

Hikvision HikvisionHQ HikvisionHQ Hikvision_Global Hikvision Corporate Channel hikvisionhq

DS-TMG023

Coil

Feature

- FVN49/0.26
- Adopts waterproof design
- Design of the cap enables convenient wring

Available Model

DS-TMG023

Parameter

Model / Parameters	DS-TMG023
	Coil
Appearance	Blue
Material	FVN
Dimension	Φ 26 mm (Φ 0.1")
Conductors' number	49

DS-K3B530X Series Swing Barrier

User Manual

Legal Information

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (***https://www.hikvision.com***). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

- This product can only enjoy the after-sales service support in the country or region where the purchase is made.
- If the product you choose is a video product, please scan the following QR code to obtain the "Initiatives on the Use of Video Products", and read it carefully.

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR

IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Data Protection

- To protect data, the development of Hikvision Products incorporates privacy by design principles. For example, for Products with facial recognition features, biometrics data is stored in your Products with encryption method; for fingerprint Products, only fingerprint template will be saved, which is impossible to reconstruct a fingerprint image.
- As a data controller/processor, you may process personal data, including collection, storage, use, processing, disclosure, deletion, etc. You are advised to pay attention to and comply with applicable laws and regulations related to the protection of personal data, including without limitation, conducting security controls to safeguard personal data, such as, implementing reasonable administrative and physical security controls, conduct periodic reviews and the assessments of the effectiveness of your security controls.

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
FCC compliance: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
—Reorient or relocate the receiving antenna.
—Increase the separation between the equipment and receiver.
—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
—Consult the dealer or an experienced radio/TV technician for help
This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.
FCC Conditions
This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:
1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement

CE

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed

under the EMC Directive 2014/30/EU, RE Directive 2014/53/EU,the RoHS Directive 2011/65/EU

2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info

2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see:www.recyclethis.info

Safety Instruction

These instructions are intended to ensure that user can use the product correctly to avoid danger or property loss.

The precaution measure is divided into Dangers and Cautions:

Dangers: Neglecting any of the warnings may cause serious injury or death.

Cautions: Neglecting any of the cautions may cause injury or equipment damage.

⚠	⚠
Dangers: Follow these safeguards to prevent serious injury or death.	**Cautions:** Follow these precautions to prevent potential injury or material damage.

⚠ Danger:

- All the electronic operation should be strictly compliance with the electrical safety regulations, fire prevention regulations and other related regulations in your local region.
- Please use the power adapter, which is provided by normal company. The power consumption cannot be less than the required value.
- Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.
  If the top caps should be open and the device should be powered on for maintenance, make sure:
  1. Power off the fan to prevent the operator from getting injured accidentally.
  2. Do not touch bare high-voltage components.
  3. Make sure the switch's wiring sequence is correct after maintenance.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.
- When the product is installed on wall or ceiling, the device shall be firmly fixed.
- If smoke, odors or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.
- Do not ingest battery, Chemical Burn Hazard.
  This product contains a coin/button cell battery. If the coin/button cell battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death.
  Keep new and used batteries away from children. If the battery compartment does not close securely, stop using the product and keep it away from children. If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the device yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)

⚠ Cautions:

- Stainless steel may be corroded in some circumstances. You need to clean and care the device by using the stainless steel cleaner. It is suggested to clean the device every month.
- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).
- Do not place the device in extremely hot (refer to the specification of the device for the detailed operating temperature), cold, dusty or damp locations, and do not expose it to high electromagnetic radiation.
- The device cover for indoor use shall be kept from rain and moisture.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- Do not aim the device at the sun or extra bright places. A blooming or smear may occur otherwise (which is not a malfunction however), and affecting the endurance of sensor at the same time.
- Please use the provided glove when open up the device cover, avoid direct contact with the device cover, because the acidic sweat of the fingers may erode the surface coating of the device cover.
- Please use a soft and dry cloth when clean inside and outside surfaces of the device cover, do not use alkaline detergents.
- Please keep all wrappers after unpack them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage on the device and lead to additional costs.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.
- Biometric recognition products are not completely applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.
- Do not stay in the lane when the device is rebooting.
- RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS.
- SUITABLE FOR MOUNTING ON CONCRETE OR OTHER NON-COMBUSTIBLE SURFACE ONLY.
- The instructions shall require connection of the equipment protective earthing conductor to the installation protective earthing conductor.

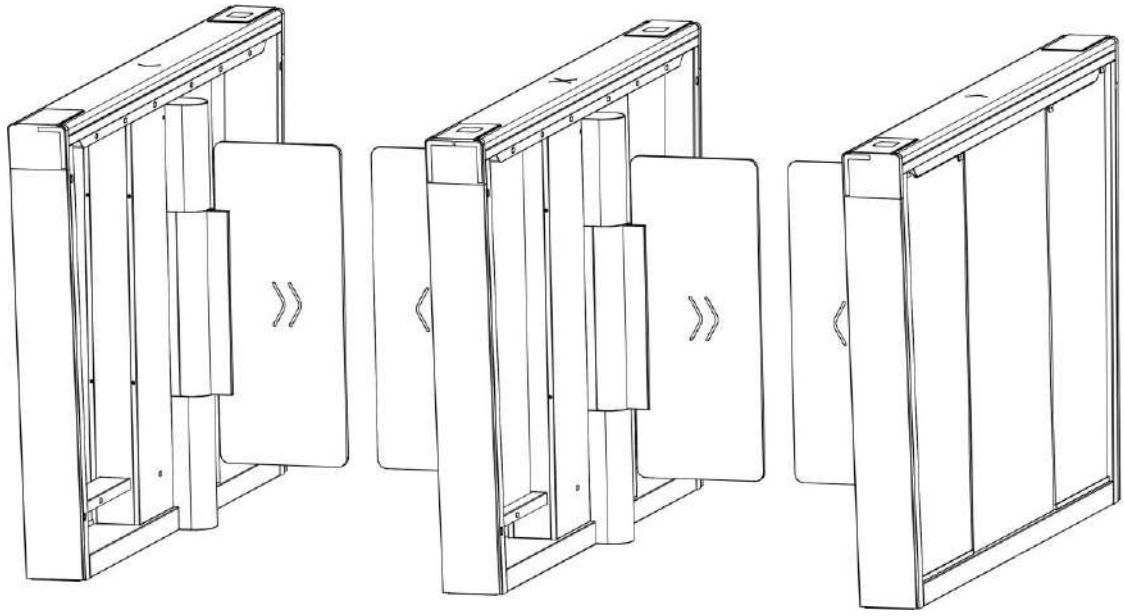
Available Models

Product Name	Model	Description
Swing Barrier	DS-K3B530LX-L/ DS-K3B530X-L DS-K3B530XM-L	Left Pedestal
	DS-K3B530LX-M/ DS-K3B530X-M DS-K3B530XM-M	Middle Pedestal
	DS-K3B530LX-R/ DS-K3B530X-R DS-K3B530XM-R	Right Pedestal

Contents

Chapter 1 Overview

1.1 Introduction



The Swing barrier with 14 IR lights is designed to detect unauthorized entrance or exit. By adopting the swing barrier integratedly with the access control system, person should authenticate to pass through the lane via swiping IC or ID card, scanning QR code, etc. It is widely used in attractions, stadiums, construction sites, residences, etc.

1.2 Main Features

- Supports control mode, inductive mode, free passing mode, remain open mode and remain closed mode in both entrance and exit direction.
- Anti-forced-accessing
  The barrier will react according to soft mode or guarding mode when confronting forced-accessing.
- Self-detection, self-diagnostics, and automatic alarm
- Audible and visual alarm will be triggered when detecting intrusion, tailgating, reverse passing, and climbing over barrier.
- LED indicates the entrance/exit and passing status
- Fire alarm passing
  When the fire alarm is triggered, the barrier will be open automatically for emergency evacuation.
- Valid passing duration settings

System will cancel the passing permission if a person does not pass through the lane within the valid passing duration.

- Bidirectional (Entrance/Exit) lane
  The barrier opening and closing speed can be configured according to the visitor flow.
- TCP/IP network communication
  The communication data is specially encrypted to relieve the concern of privacy leak.
- Permissions validation and anti-tailgating
- Remote barrier opening via keyfob and broadcasting via loudspeaker (custom broadcasting context is supported when installed with access control board).

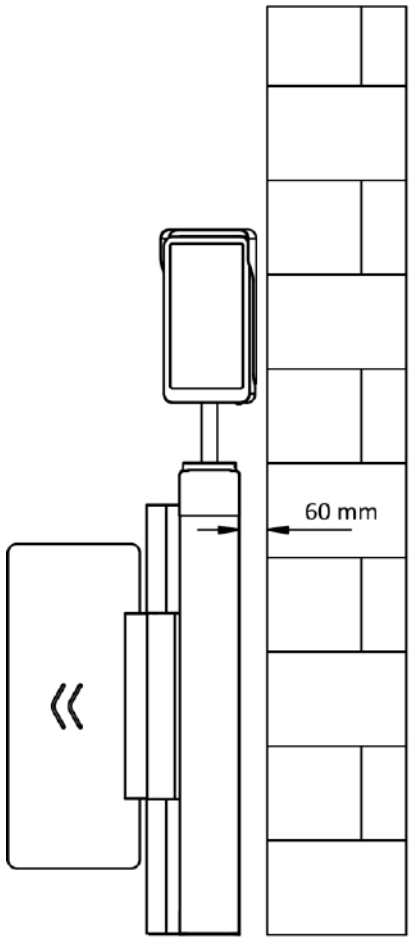
Chapter 2 System Wiring

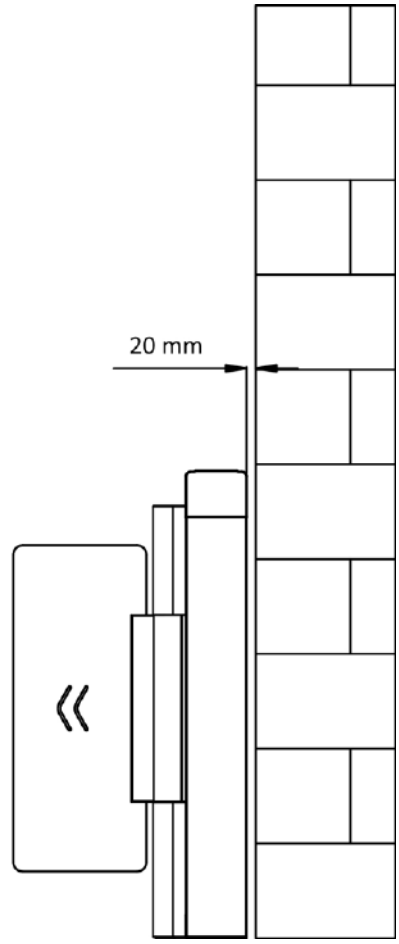
The preparation before installation and general wiring.

Steps

Note

- The device should be installed concrete surface or other flat non-flammable surface.
- If the installation area is too close to the wall, make sure the distance between the pedestal and the wall should be no less than 20 mm (60 mm if with face recognition terminals), or you cannot open the pedestal's top panel or might cause damage to devices.





- The dimension is as follows.

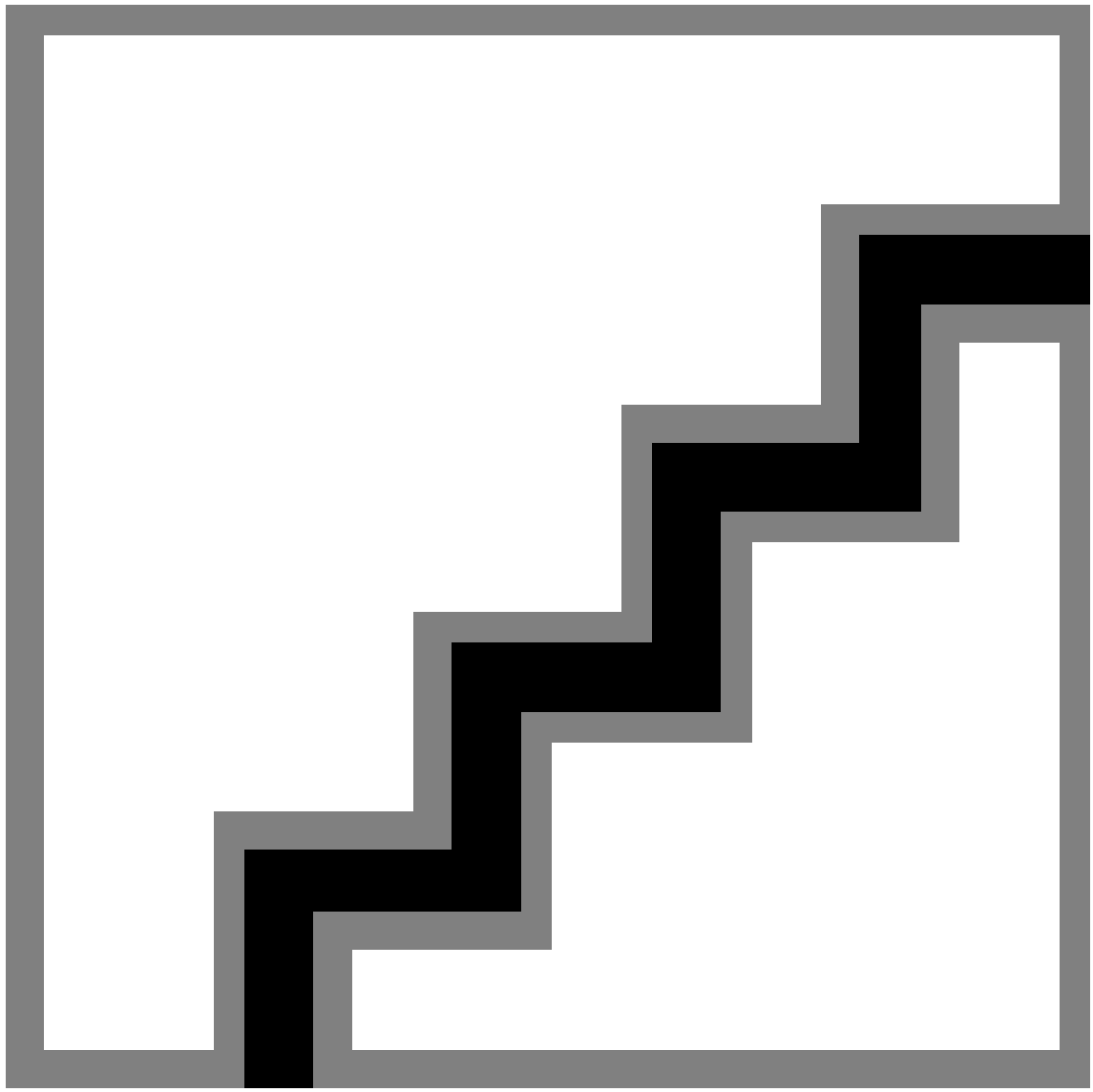


Figure 2-1 Dimension

1. Draw a central line on the installation surface of the left or right pedestal.
2. Draw other parallel lines for installing the other pedestals.

Note

The distance between the nearest two line is L + 272 mm. L represents the lane width.

3. Slot on the installation surface and dig installation holes. Put 4 expansion bolts of M12*120 for each pedestal.

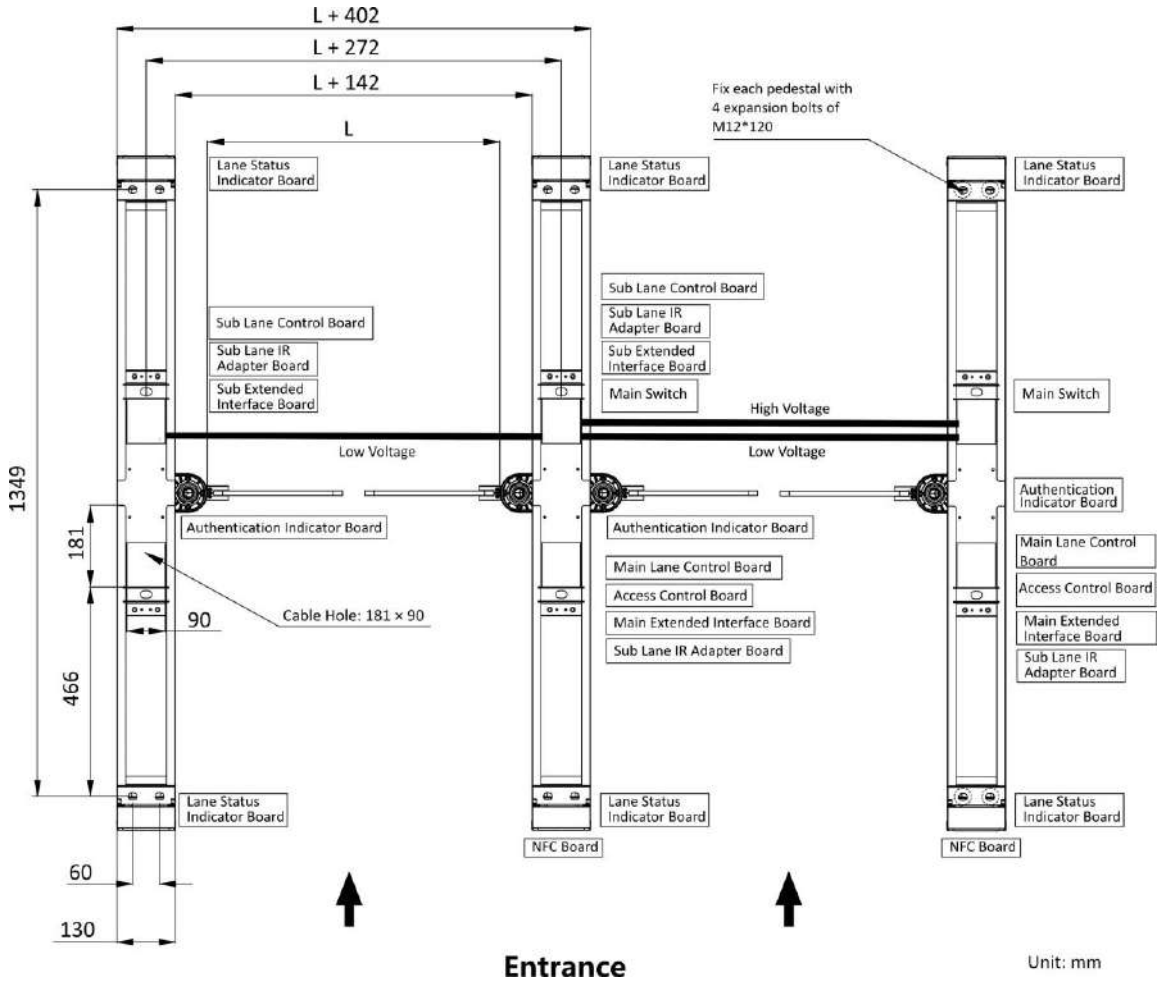


Figure 2-2 Hole Position and System Wiring

4. Bury cables. Each lane buries 1 high voltage cable and 1 low voltage cable. For details, see the system wiring diagram of step 3.

Note

- High voltage: AC power input
  Low voltage: interconnecting cable (communication cable and 24 V power cable) and network communication cable
- The supplied 24 V power cable length is 5 m and the communication cable length is 3 m.
- The suggested inner diameter of the low voltage conduit is larger than 30 mm.
- If you want to bury both of the AC power cord and the low voltage cable, the two cables should be in separated conduits to avoid interference.
- If more peripherals are required to connect, you should increase the conduit diameter or bury another conduit for the external cables.
- The external AC power cord should be double-insulated.
- The network cable must be CAT5e or the network cable has better performance.

Chapter 3 Install Pedestals

Before You Start

Prepare for the installation tools, check the device and the accessories, and clear the installation base.

Steps

Note

- The device should be installed on the concrete surface or other flat non-flammable surfaces.
- Make sure the device is powered off during installation and other operations.
- The installation tools are put inside the package of the pedestal.

1. Prepare for the installation tools, check the components, and prepare for the installation base.
2. Remove 4 screws of each pedestal that fix the 2 side panels.

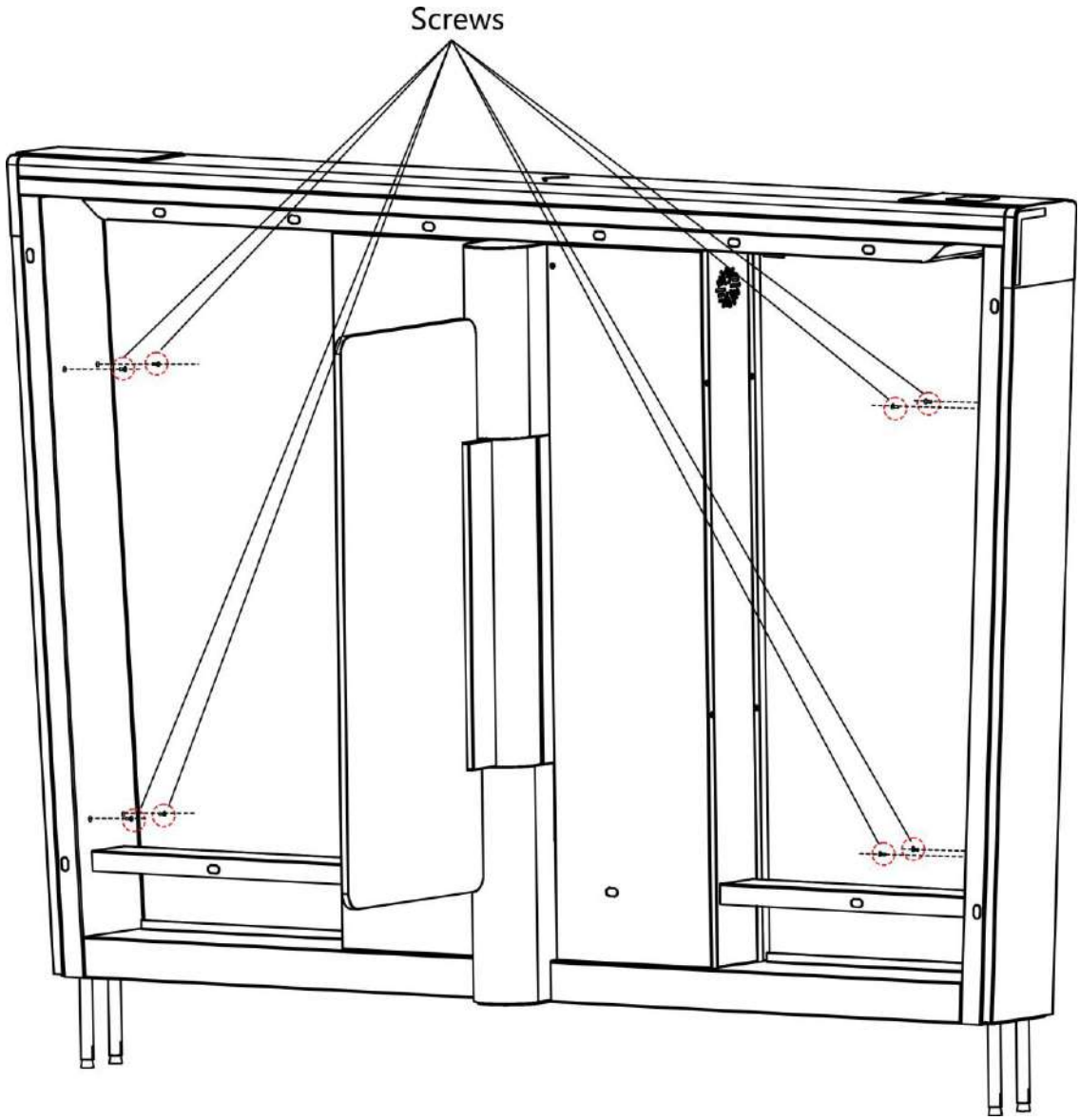


Figure 3-1 Remove Side Panel Screws

3. Remove the side panels and move the pedestals to the corresponded positions according to the entrance and exit marks on the pedestals.

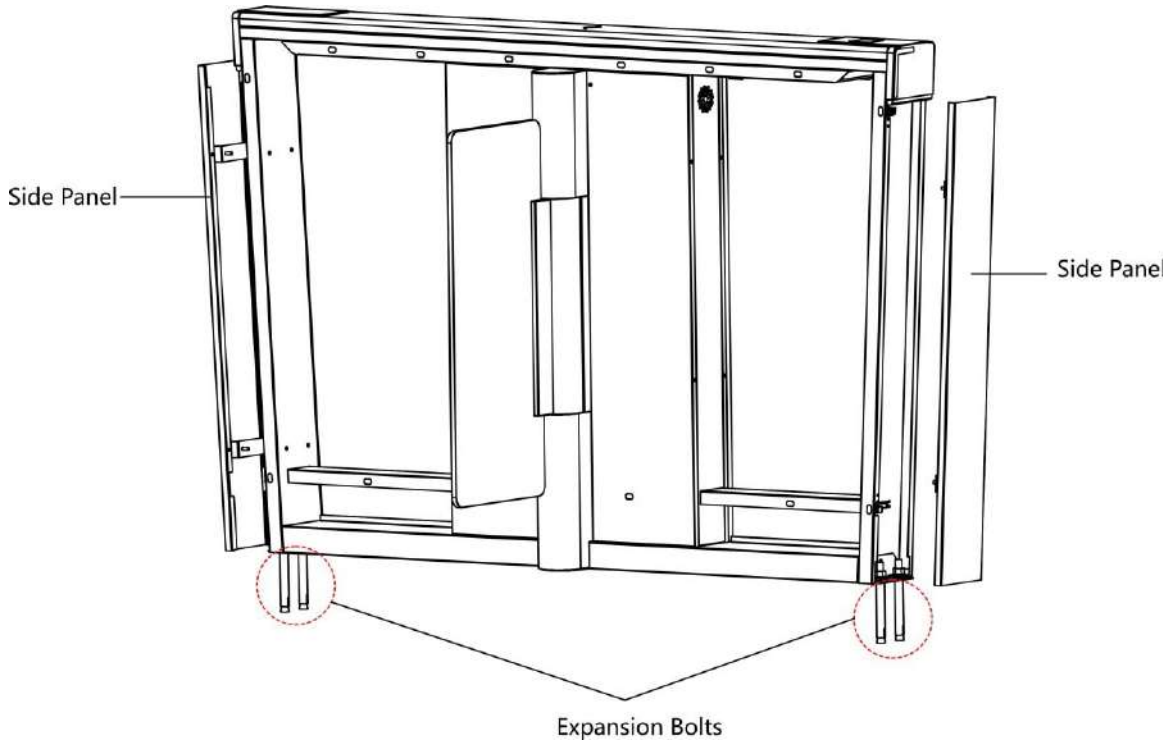


Figure 3-2 Remove Side Panel Screws

Note

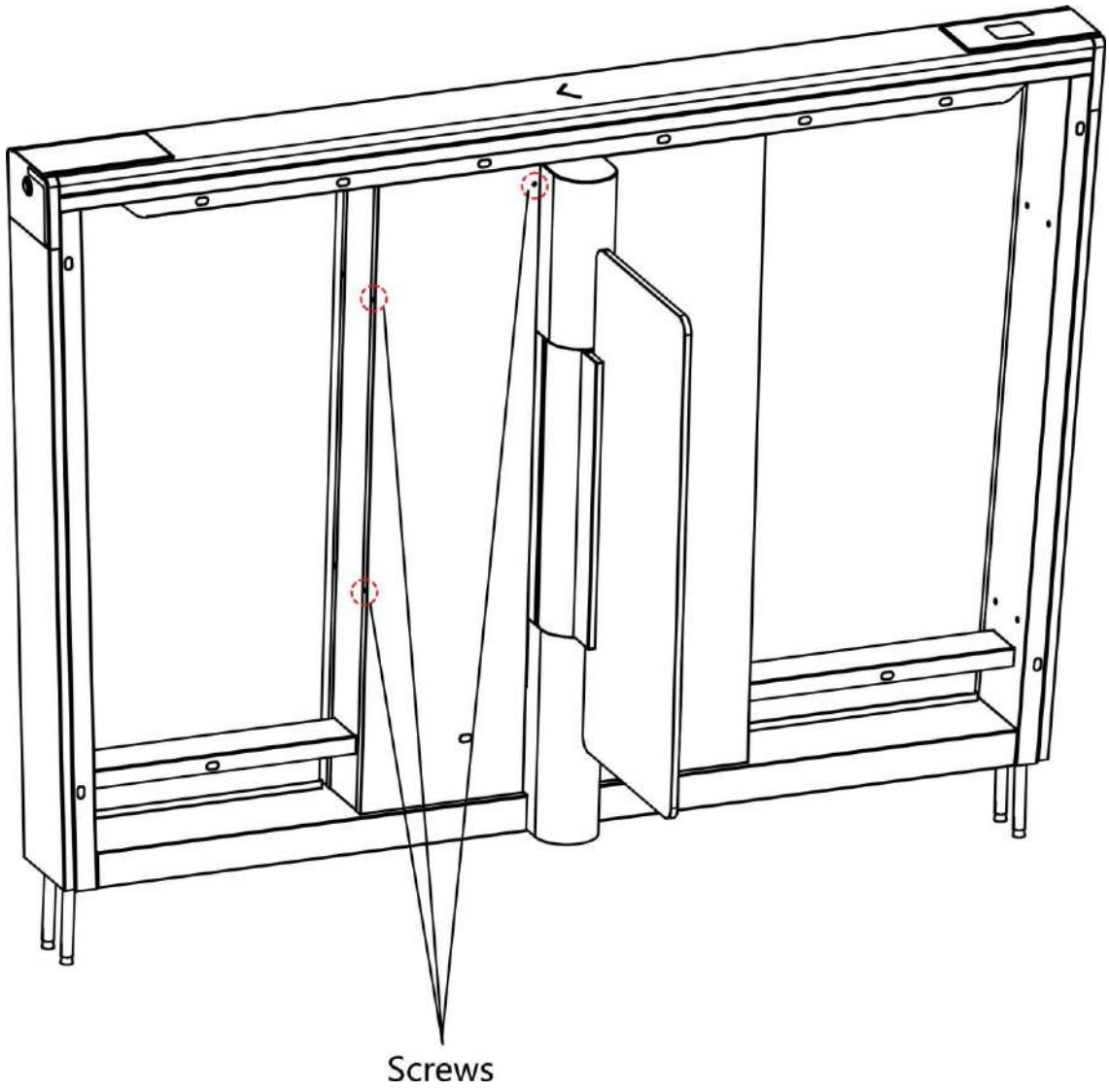
For detailed information about system wiring, see ***System Wiring*** .

4. Secure the pedestals with expansion bolts and fix the side panels to its original position with screws.

Note

- Do not immerse the pedestal in the water. In special circumstances, the immersed height should be no more than 150 mm.

5. Remove 3 screws to open each maintenance door for cable wiring.


Screws

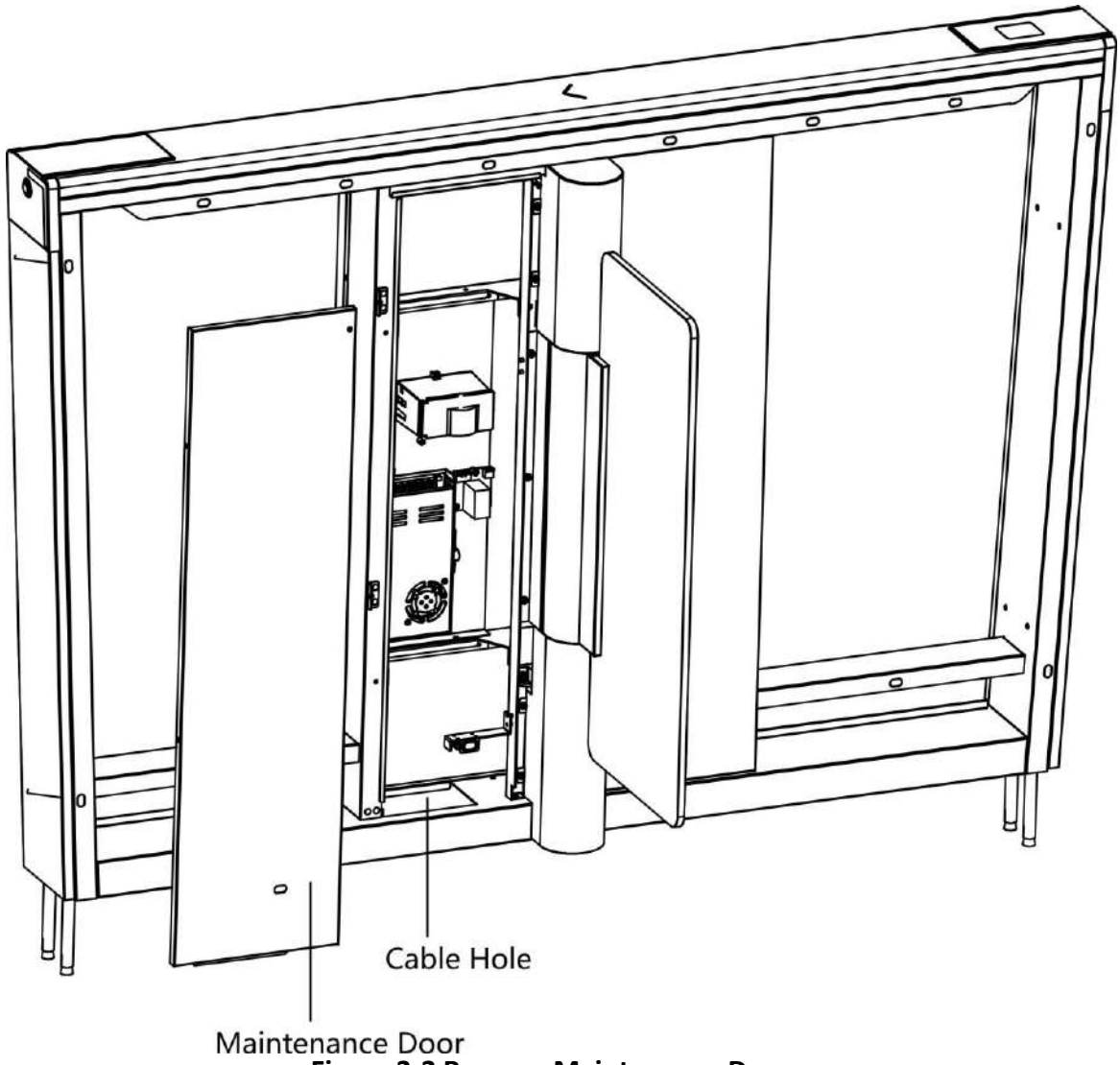


Figure 3-3 Remove Maintenance Door

Note

For detailed information about cables, see ***General Wiring*** .

Chapter 4 General Wiring

Note

- When you should maintain or disassemble the high voltage modules, you should remove the entire high voltage modules and maintain it outside the turnstile. You should unplug the cables that connected to the peripherals before maintenance to avoid destroy of the device.
- When disassembling the high voltage module, you should disconnect the power to avoid injury.
- If only wiring is needed without maintenance, do not remove the high voltage modules.
- The switch and the main lane control board are already connected. The 14 AWG cable to connect between the AC electric supply and the switch should be purchased separately.
- 2 interconnecting cables are supplied: 24 V Power Cable and Communication Cable.
  24 V Power Cable: 5 m long, which is in the middle and right pedestal.
  Communication Cable: 4 m long, CAT5e, which is in the package of middle and right pedestal.

4.1 Components Introduction

By default, basic components of the turnstile are connected well. The pedestals can communicate by wiring the interconnecting cables. And the turnstile supports wiring the AC electric supply for the whole system's power supply.

Note

The voltage fluctuation of the electric supply is between 100 VAC and 240 VAC, 50 to 60 Hz.

The picture displayed below describes the serial port on the entrance and exit direction.

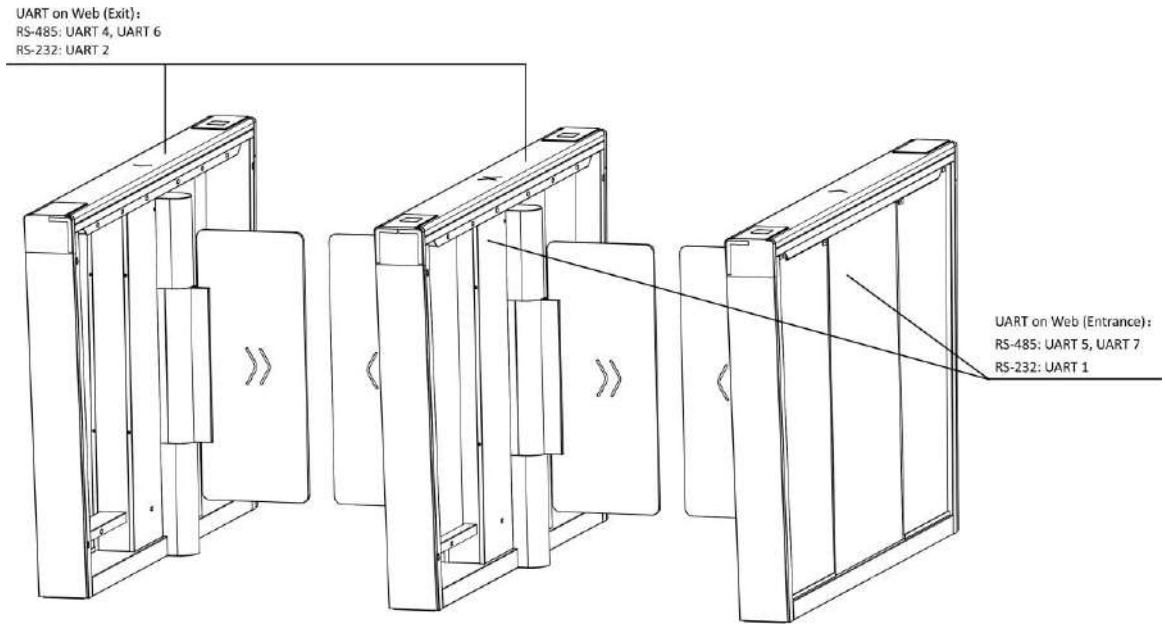


Figure 4-1 Serial Port

The picture displayed below describes the IR sending/receiving module and their corresponding number on the pedestal.

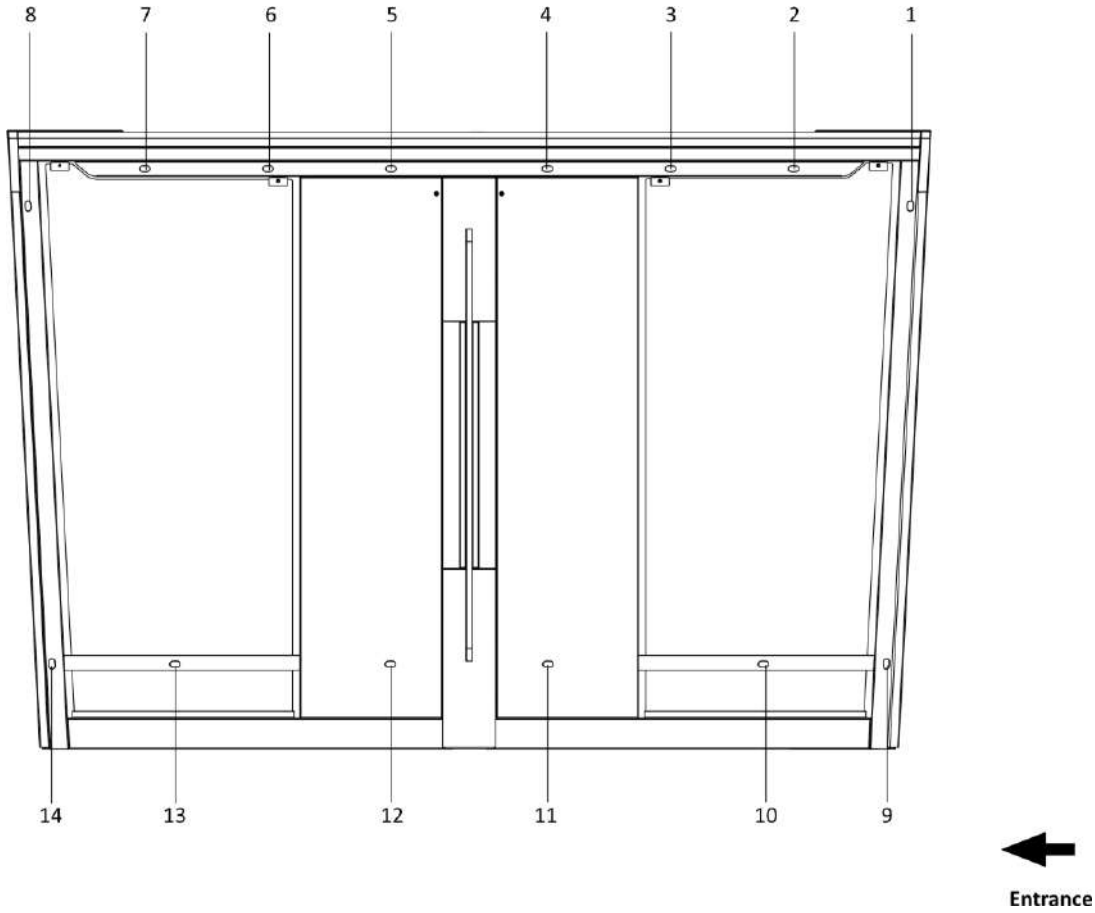


Figure 4-2 IR Sending/Receiving Module Position

Note

Standing at the entrance position in the lane, the IR modules on your left are the IR sending modules, the ones on your right are the IR receiving modules.

4.2 Wiring

Scan the QR code to watch the guide video.

4.3 Terminal Description

4.3.1 General Wiring

The general wiring of lane control board, access control board and extended interface board.

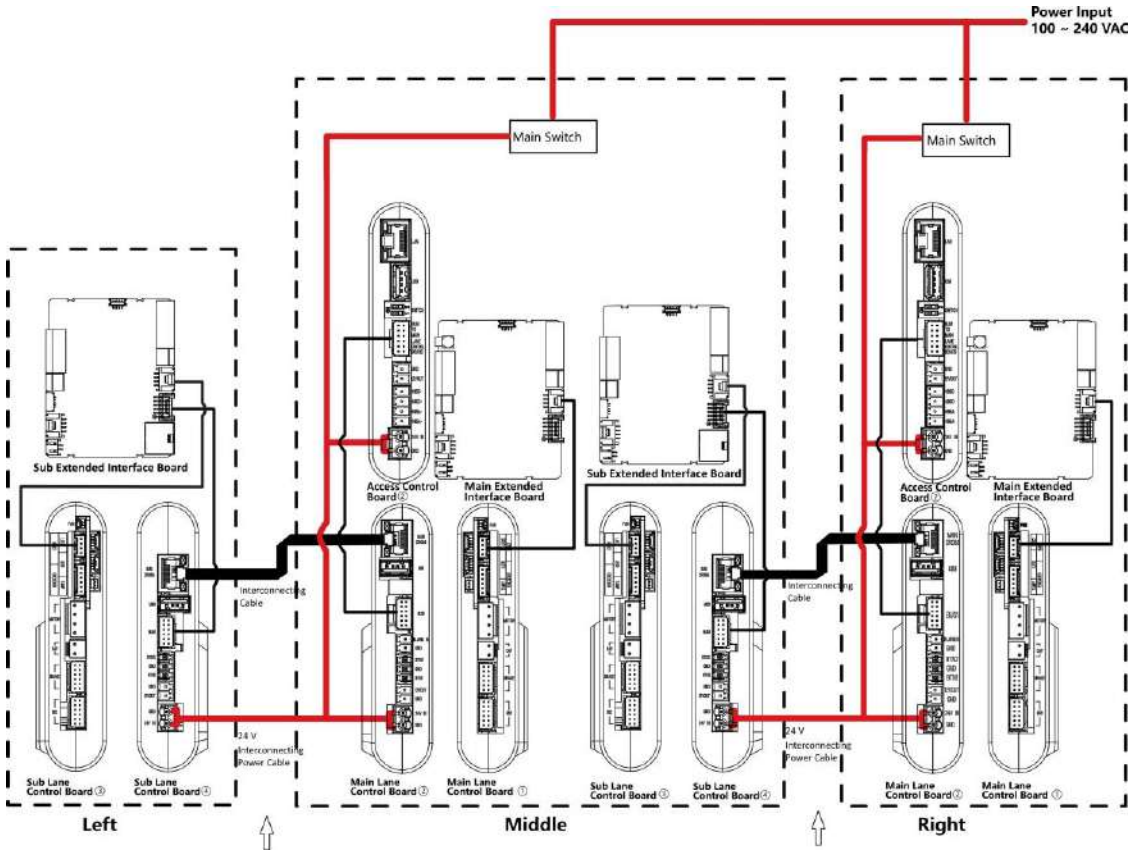


Figure 4-3 General Wiring

Note

- The power cable from power supply to the main lane control board has been connected. You will need to prepare the 14AWG power cable to connect the AC power input to power supply.
- The supplied 2 interconnecting cables need connecting on-site:
  1. 24 V power cable of 14 AWG. The cable is 5 m in length and put inside the right/middle pedestal at the exit.
  2. CAT5e Communication cable. The cable is 3 m in length and put inside the package of the right/middle pedestal.
- The ① and ② or ③ and ④ refer to the two sides of a same board.
- Barrier opens at the entrance/exit: connect to BTN1/BTN2 and GND.

4.3.2 Main Lane Control Board Terminal Description

The main lane control board contains interconnecting interface, access control board interface, fire input interface, exit button interface, 12 VDC output interface, 24 VDC input interface, fan interface, communication interface, encoder interface, power supply interface for motor, supercapacitor interface, main brake interface, adaptor interface and tamper interface.

The picture displayed below is the main lane control board diagram.

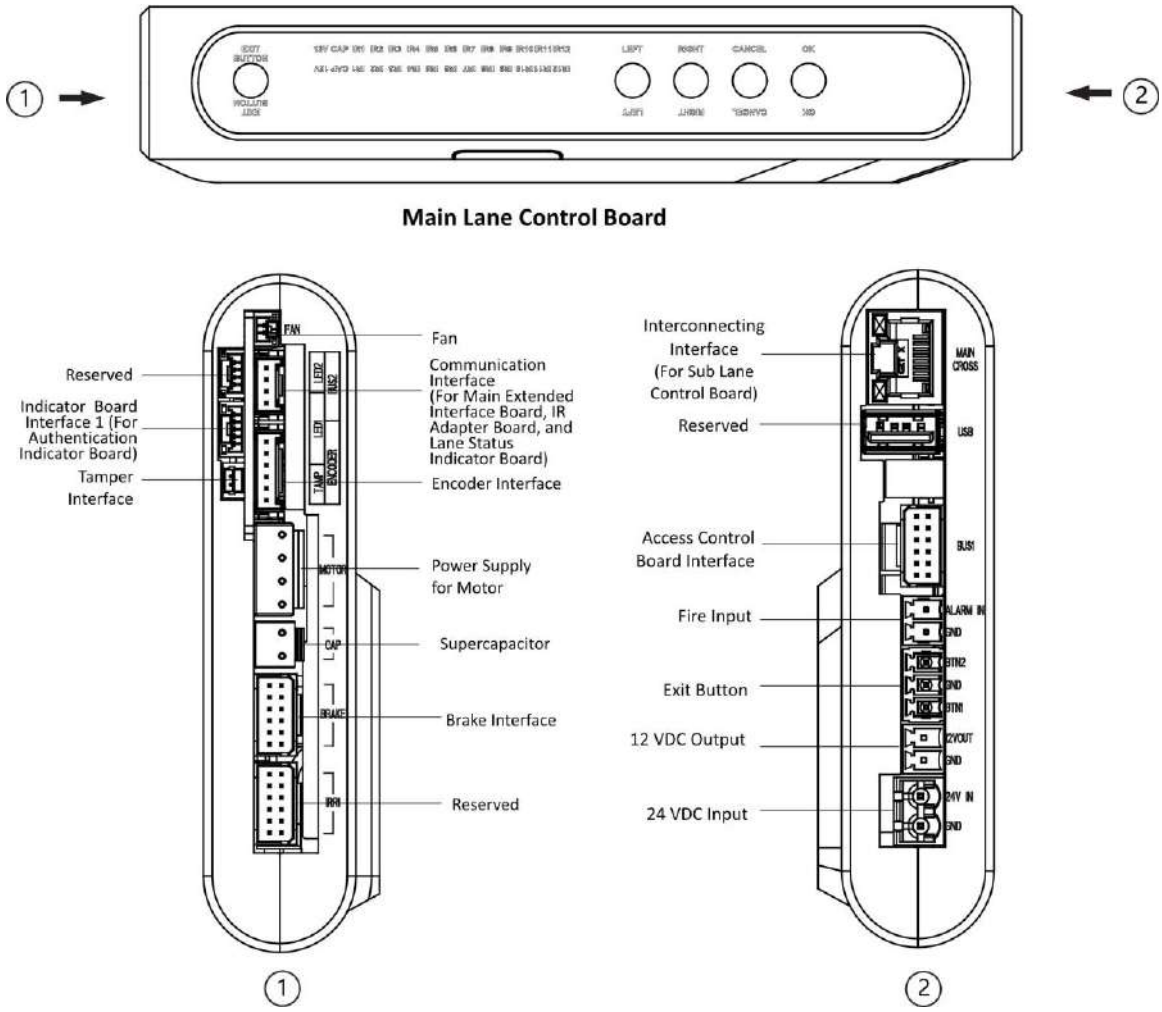


Figure 4-4 Main Lane Control Board Terminals

4.3.3 Sub Lane Control Board Terminal Description

The sub lane control board contains interconnecting interface, BUS interface, exit button interface, 12 VDC output interface, 24 VDC input interface, fan interface, communication interface, encoder interface, power supply interface for motor, supercapacitor interface, sub brake interface, adaptor interface and tamper interface.

The picture displayed below is the sub lane control board diagram.

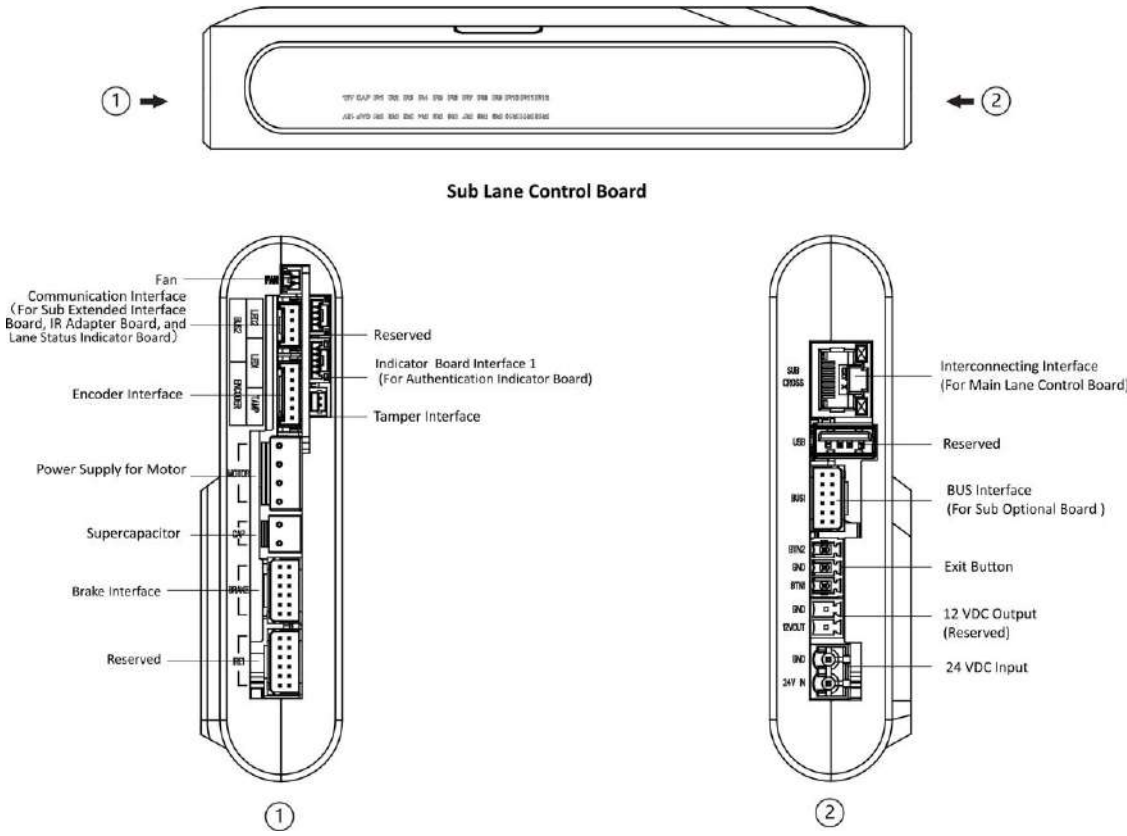


Figure 4-5 Sub Lane Control Board Terminals

4.3.4 Access Control Board Terminal Description (Optional)

Access control board is mainly used for authority identification in places with high security levels such as public security or judicial place, external device accessing, and communication with the upper platform and lane controller.

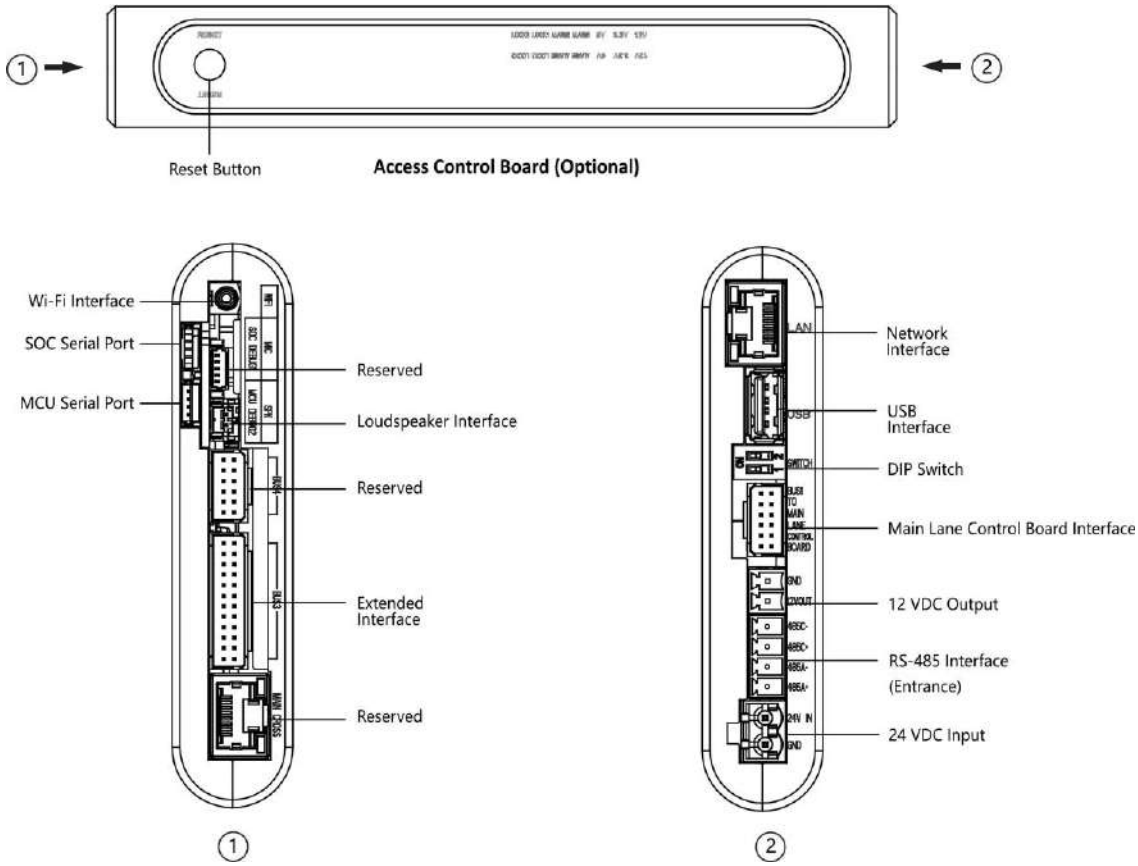


Figure 4-6 Access Control Board

Note

- RS-485A corresponds to port 5 on web and is for QR code scanner connection at entrance by default; RS-485C corresponds to port 7 on web and is for card reader connection at entrance by default.
- The SOC and MCU serial port are for maintenance and debugging use only.
- Press the Reset button for 5 s and the device will start to restore to factory settings.
- The DIP switch is for study mode setting and keyfob paring. For detailed information about the DIP switch, see *DIP Switch Description*.

The wiring diagram of extended interface of access control board is shown as follows.

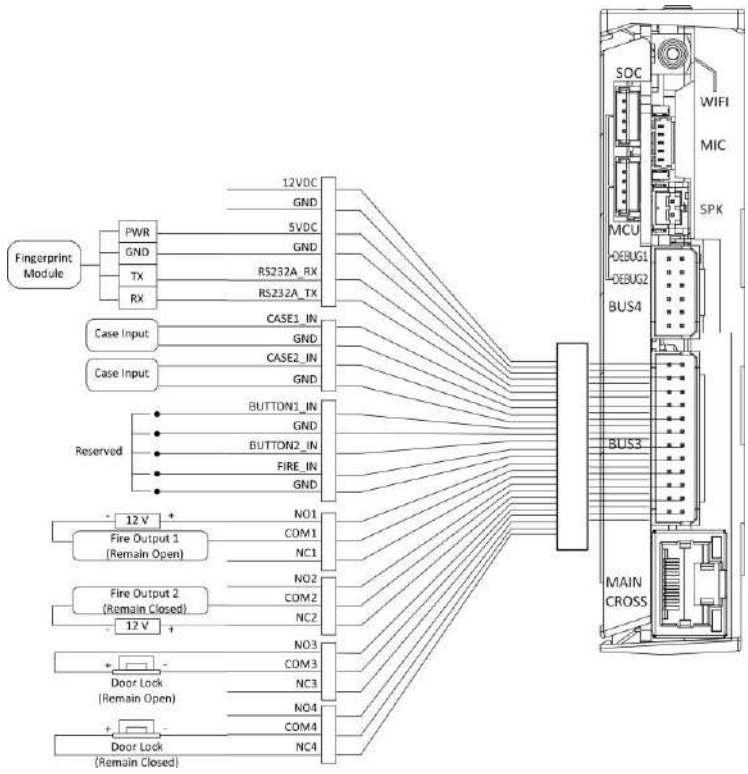


Figure 4-7 Wring Diagram of BUS3 Interface

Note

RS-232A corresponds to port 1 on web.

4.3.5 Main Extended Interface Board Terminal Description

The main extended interface board contains the sub-1G antenna interface, barrier light interface, loudspeaker interface, debugging port, Wiegand/exit button interface, 5 VDC output and communication interface.

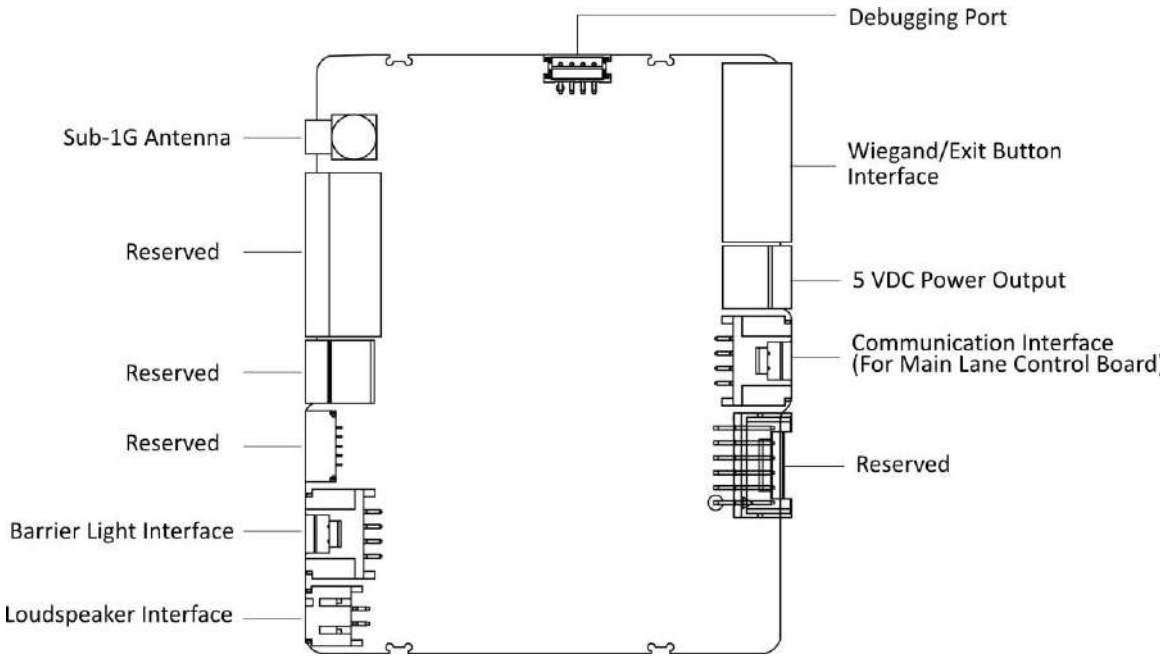


Figure 4-8 Main Extended Interface Board Terminal

Note

When the device is installed with access control board, the loudspeaker shall be connected to the access control board. If not, the loudspeaker shall be connected to the main extended interface board.

4.3.6 Card Reader Board Terminal Description

The card reader board can be connected to the access control board via RS-485 interface.

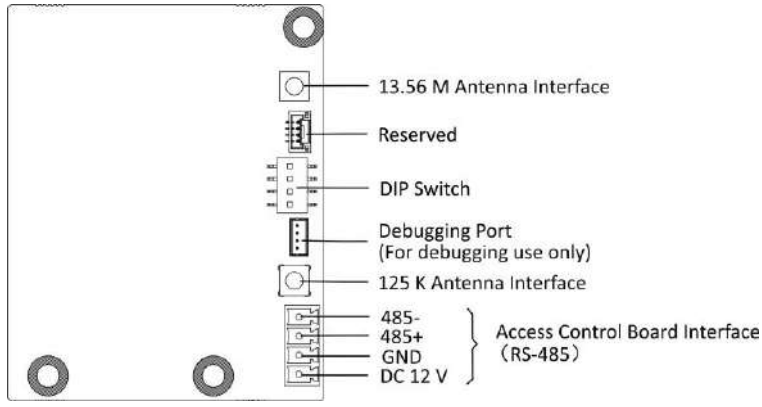


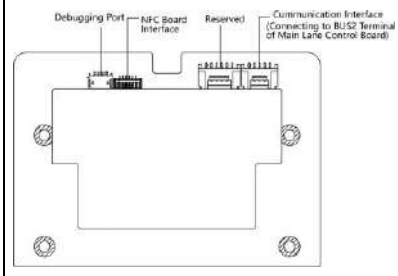
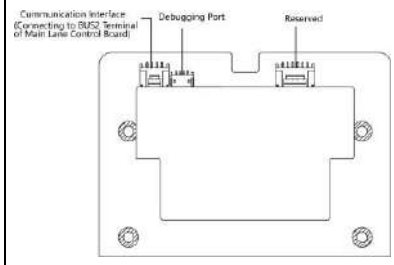
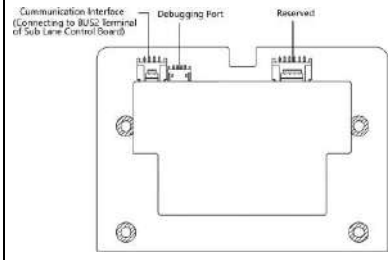
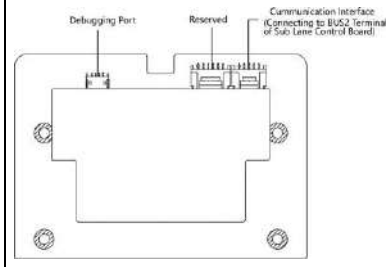
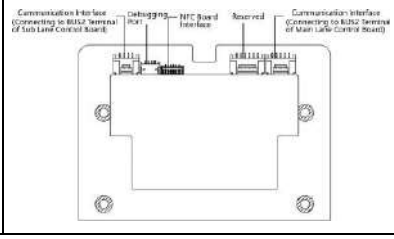
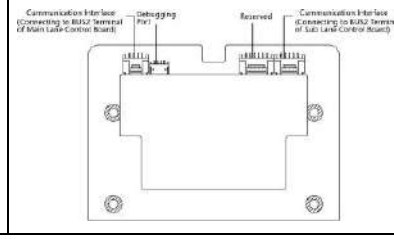
Figure 4-9 Card Reader Board

4.3.7 Lane Status Indicator Board

For details about lane status indicator position, see .

Lane status indicator board in different pedestals are shown as follows.

Table 4-1 Lane Status Indicator Board

Pedestal	Entrance	Exit
Right Pedestal		
Left Pedestal		
Middle Pedestal		

4.3.8 Authentication Indicator Board Terminal Description

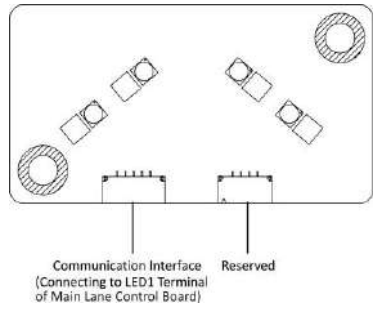


Figure 4-10 Authentication Indicator Board

The authentication indicator board is connected to the LED1 terminal of main lane control board.

4.3.9 RS-485 Wiring

The RS-485 interfaces on the access control board and sub extended interface board are suggested to connect with the face recognition module or the card reader. Here takes connecting with a card reader as an example.

Note

- There are 2 RS-485 interfaces on the access control board for entrance. Refer to ***Access Control Board Terminal Description (Optional)*** for details.
  There are 2 RS-485 interfaces on the sub extended interface board for exit. Refer to for details.
- If connecting the RS-485 with a card reader, by default, the DIP switch of the card reader should be set as follows:
  - For entrance, set the No.1 of the 4-digit DIP switch to ON side.
  - For exit, set the No.3 of the 4-digit DIP switch to ON side.
- If there are other RS-485 devices connecting, the ID of the RS-485 cannot be conflicted.
- The connected 12 V power interface for the face recognition terminal cannot be connected with other 12 V devices.

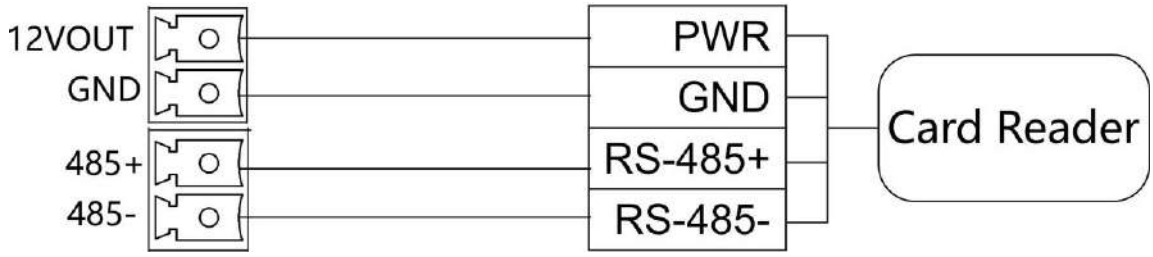


Figure 4-11 Wiring RS-485

4.3.10 RS-232 Wiring

Note

- There is 1 RS-232 interface on the extended interface of access control board, see ***Access Control Board Terminal Description (Optional)*** . The RS-232A corresponds to UART 1 on web.
- There is 1 RS-232 interface on the sub extended interface board, see . The RS-232B corresponds to UART 2 on web.
  The RS-232C interface is reserved.

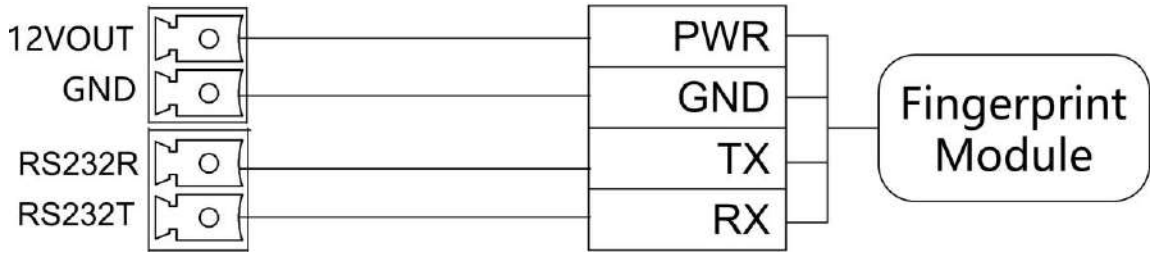


Figure 4-12 RS-232 Wiring

4.3.11 Alarm Input Wiring

On the main lane control board, you can wire the fire alarm input interface.

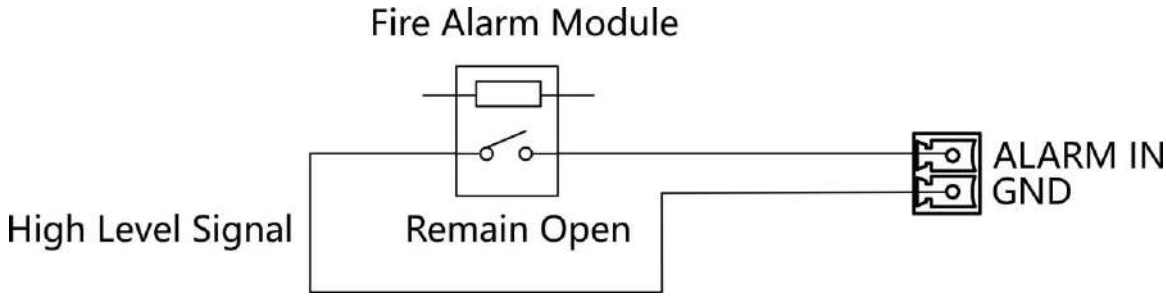


Figure 4-13 Remaining Open

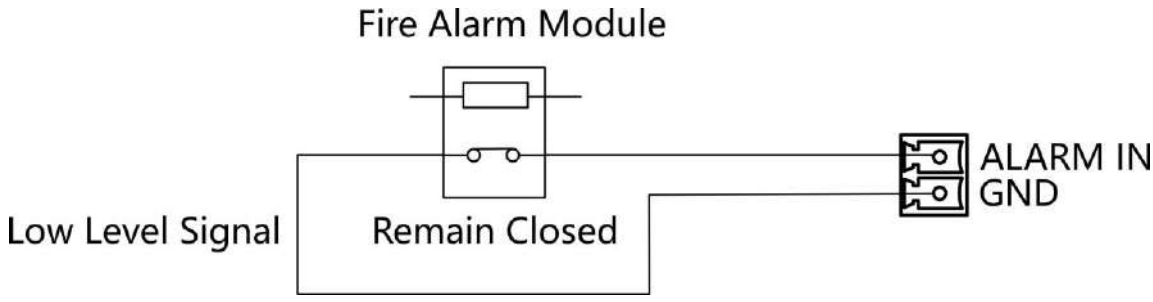


Figure 4-14 Remaining Closed

4.3.12 Exit Button Wiring

The main and sub lane control board each has 1 button interface, which can be connected to exit button or face recognition device.

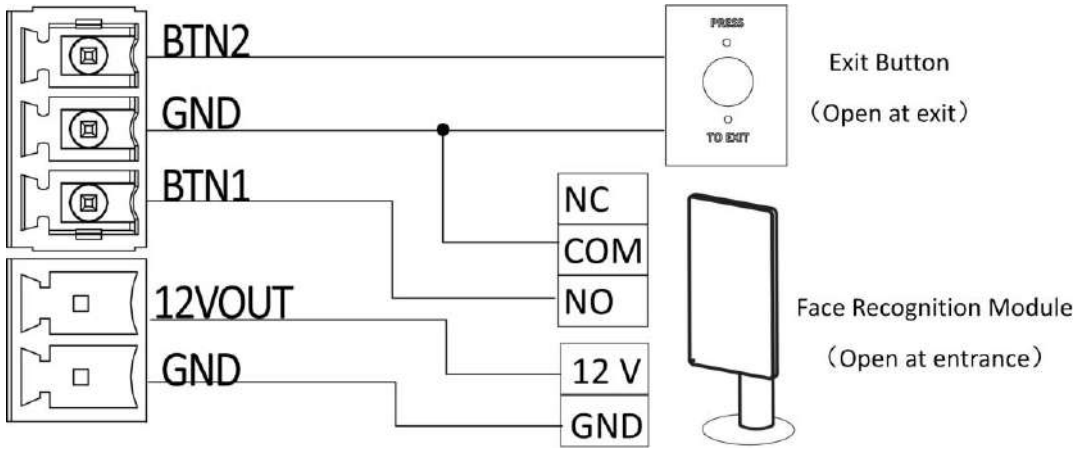


Figure 4-15 Exit Button Wiring

Note

- The face recognition devices are powered via 12 VDC power output interface of the main and sub lane control board.
- Barrier open at the entrance: connect to BTN1 and GND.
- Barrier open at the exit: connect to BTN2 and GND.

4.4 Device Settings via Button

You can configure the device via button on the main lane control board or the DIP switch on the access control board.

Function	Main Lane Control Board & Loudspeaker (Connected to Main Extended Interface Board)	Main Lane Control Board & Access Control Board & Loudspeaker (Connected to Access Control Board)
Working Mode		
Normal/Study Mode	Configure via button (refer to ***Set Study Mode via Button***)	Configure via DIP switch (refer to ***Set Study Mode via DIP Switch (Optional)***)
keyfob Pairing	Configure via button (refer to ***Pair Keyfob via Button***)	Configure via DIP switch (refer to ***Pair Keyfob via DIP Switch (Optional)***)
Passing Mode	Configure via button	Configure via button/web

Function	Main Lane Control Board & Loudspeaker (Connected to Main Extended Interface Board)	Main Lane Control Board & Access Control Board & Loudspeaker (Connected to Access Control Board)
Memory Mode	Configure via button	Configure via button/web
Control Mode	Configure via button	Configure via button/web
Application Mode	Configure via button	Configure via button
Parameter Settings		
Barrier Opening Speed	Configure via button	Configure via button/web
Barrier Closing Speed	Configure via button	Configure via button/web
Card Reading on the Alarm Area	Configure via button	Configure via button/web
Enter Duration	Configure via button	Configure via button/web
Exit Duration	Configure via button	Configure via button/web
IR Sensing Duration	Configure via button	Configure via button/web
Intrusion Duration	Configure via button	Configure via button/web
Overstay Duration	Configure via button	Configure via button/web
Delay Time for Barrier Closing	Configure via button	Configure via button/web
Barrier Recover Duration	Configure via button	Configure via button
Volume Adjustment	Configure via button	Configure via button
Barrier Material	Configure via button	Configure via button/web
Barrier Length	Configure via button	Configure via button/web
Barrier Height	Configure via button	Configure via button/web
Brake	Configure via button	Configure via button
Brake Angle	Configure via button	Configure via button
IR Sensing	Configure via button	Configure via button/web
Fan	Configure via button	Configure via button
Light Brightness	Configure via button	Configure via button/web
Restore to Default	Configure via button	Configure via button/web
Voice Prompt		

Function	Main Lane Control Board & Loudspeaker (Connected to Main Extended Interface Board)	Main Lane Control Board & Access Control Board & Loudspeaker (Connected to Access Control Board)
Climbing over Barrier	Enable or disable via button	Enable or disable via button
Reverse Passing	Enable or disable via button	Enable or disable via button
Exceeding Passing Duration	Enable or disable via button	Enable or disable via button
Intrusion Alarm	Enable or disable via button	Enable or disable via button
Tailgating Alarm	Enable or disable via button	Enable or disable via button
Overstaying Alarm	Enable or disable via button	Enable or disable via button
Motor Inspection	Configure via button	Configure via button
Self-check Voice Prompt	Enable or disable via button	Enable or disable via button
Study Mode Voice Prompt	Enable or disable via button	Enable or disable via button

Note

- Refer to ***Button Configuration Description*** for detailed information.
- If the device is not equipped with access control board, the loudspeaker shall be connected to the main extended interface board.
- If the device is equipped with access control board, the loudspeaker shall be connected to the access control board. You can set custom broadcasting context via web. For details, see ***Prompt Schedule*** .

4.4.1 Configuration via Button

Button Description

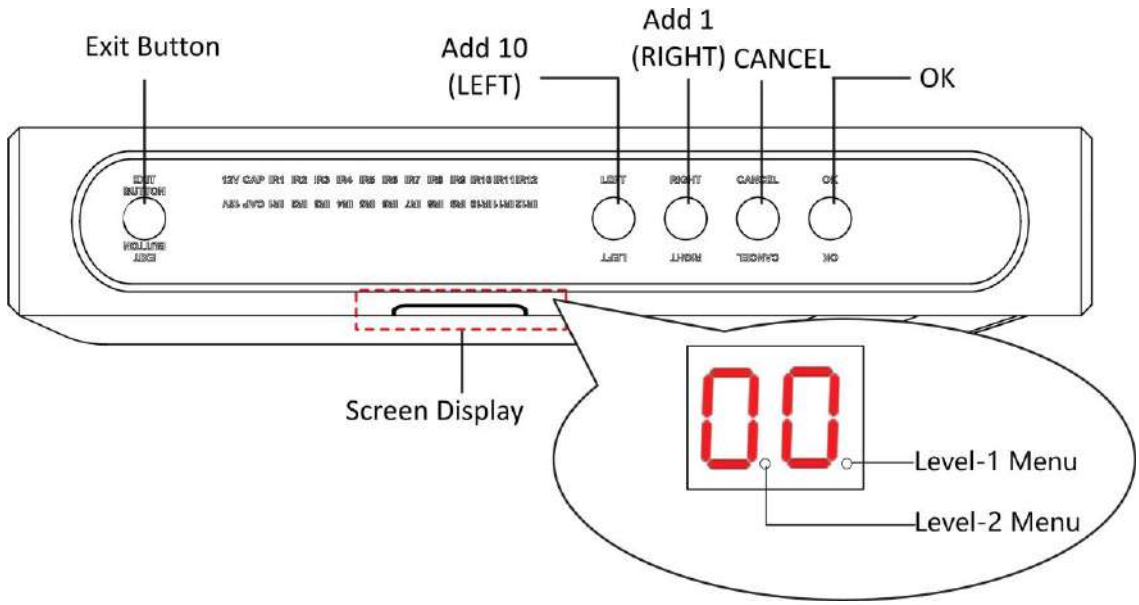


Figure 4-16 Button

Exit Button

- Press to open the barrier from the entrance position.
- Double press to open the barrier from the exit position.

Parameter Configuration Button

- LEFT: Press to add 10 to configuration data.
- RIGHT: Press to add 1 configuration data.
- CANCEL: Return to the Level-1 menu, or exit Level-1 menu.
- OK: Confirm the settings, or enter configuration mode, or enter the Level-2 menu.

Note

- Configuration No. is displayed by two digital tubes.
- Level-1 Menu: If the decimal point on the right is on, it indicates the Level-1 menu. The number represents the configuration No.
- Level-2 Menu: If the decimal point in the middle is on, it indicates the level-2 menu. The number represents the configuration No.

Button Configuration Procedure

Here takes setting intrusion duration to 12 s as example:

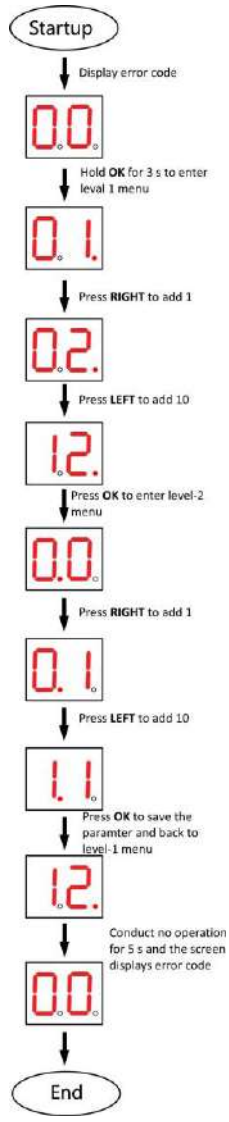


Figure 4-17 Procedure

Steps:

1. Hold **OK** button for 3 s until one beep occurs. The device enter the configuration mode. Level 1 menu lights up. The display screen displays the configuration No. **1**.
2. In the Level-1 menu, press **LEFT** (plus 10) once and press **RIGHT** (plus 1) twice to set the configuration No. to 12. Press **OK** to save settings and the enter the level-2 menu. Or you can press **CANCEL** to exit the current menu, or conduct no operation for 5 s to cancel configuration and exit the current menu.
3. After enter the level 2 menu, press **LEFT** (plus 10) once and **RIGHT** (plus 1) twice to set the configuration No. to 12. Press **OK** to save the settings. Or you can press **CANCEL** to exit the current menu, or conduct no operation for 5 s to cancel configuration and exit the current menu.

Note

- The configuration No. will display in a cycle.
- Each configuration No. refers to a function. For details about the configuration No. and its related function, see ***Button Configuration Description*** .

4.4.2 Study Mode Settings

Set the closed position of the device barrier.

Set Study Mode via Button

Enter the study mode through button configuration to set the closed position of the device barrier.

Steps

Note

- If the device is equipped with access control board, you can set study mode via DIP switch on the access control board only.
- For details about button's operation, see ***Configuration via Button*** .
- For details about the configuration No. and its related function, see ***Button Configuration Description*** .

1. Enter the study mode.
   1) Enter the configuration mode.
   2) Set the configuration No. in Level-1 to **1**. The device will enter the study mode.
   3) Set the configuration No. in the Level-2 menu to **2**. The device will enter the study mode.
2. Power off the device and swing the barrier until it is vertical to the pedestal.
3. Power on the device.
   The device will remember the current position automatically.
4. Reboot the device when you hear **Study accomplished. Please reboot.**

Set Study Mode via DIP Switch (Optional)

Enter the study mode through DIP switching to set the closed position of the device barrier.

Steps

1. Set the No.1 of the 2-digit DIP switch on the access control board to ON by referring the following figure to enter the study mode.

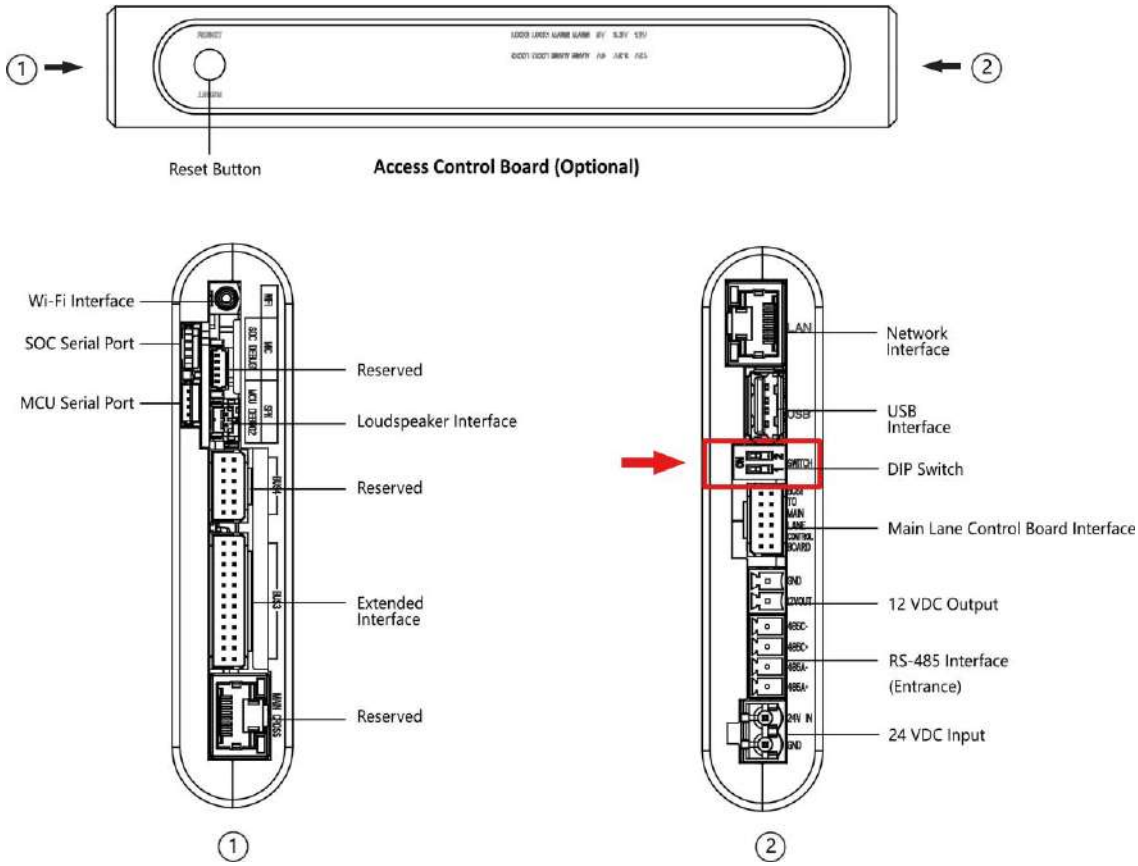


Figure 4-18 DIP Switch Location

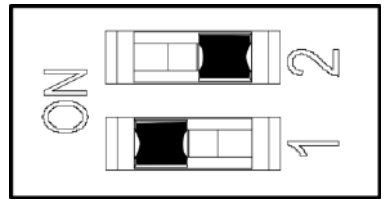


Figure 4-19 Study Mode

2. Adjust the closed position of the barrier.

3. Power on the device.

The device will remember the current position (closed position) automatically.

4. Power off the device.

5. Set the No.1 switches of the 2-digit DIP Switch on the main user extended interface board by referring to the following figure.

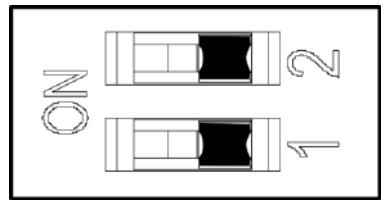


Figure 4-20 Normal Mode

6. Power on the device again.

Note

For details about the DIP switch value and meaning, see *DIP Switch Description*.

The barrier will open automatically and turns back to the closed position. At this circumstance, the device enters the normal mode.

4.4.3 Keyfob Pairing

Pair keyfob via button or DIP switch.

Pair Keyfob via Button

Pair the keyfob to the device via button to open/close the barrier remotely.

Before You Start

Ask our technique supports or sales and purchase the keyfob.

Steps

Note

- If the device is equipped with access control board, you can pair keyfob via DIP switch on the access control board only.
- For details about button's operation, see ***Configuration via Button*** .
- For details about the configuration No. and its related function, see ***Button Configuration Description*** .
- For details about the keyfob operation instructions, see the keyfob's user manual.

1. Enter the keyfob pairing mode.
   1) Enter the configuration mode.
   2) Set the configuration No. in Level-1 to **2**. The device will enter the keyfob pairing mode.
   3) Set the configuration No. in the Level-2 menu to **2**. The device will enter the keyfob pairing mode.

2. Hold the **Close** button for more than 10 seconds.

The keyfob's indicator will flash if the pairing is completed.

3. Exit the keyfob pairing mode.
1) Enter the configuration mode.
2) Set the configuration No. in Level-1 to **2**. The device will enter the keyfob pairing mode.
3) Set the configuration No. in the Level-2 menu to **1**. The device will exit the keyfob pairing mode.

4. Reboot the device to take effect.

Pair Keyfob via DIP Switch (Optional)

Pair the remote control to the device through DIP switch to open/close the barrier remotely.

Before You Start

Ask our technique supports or sales and purchase the keyfob.

Steps

1. Power off the turnstile.

2. Set the No.2 switch of the DIP Switch on the access control board to the ON side.

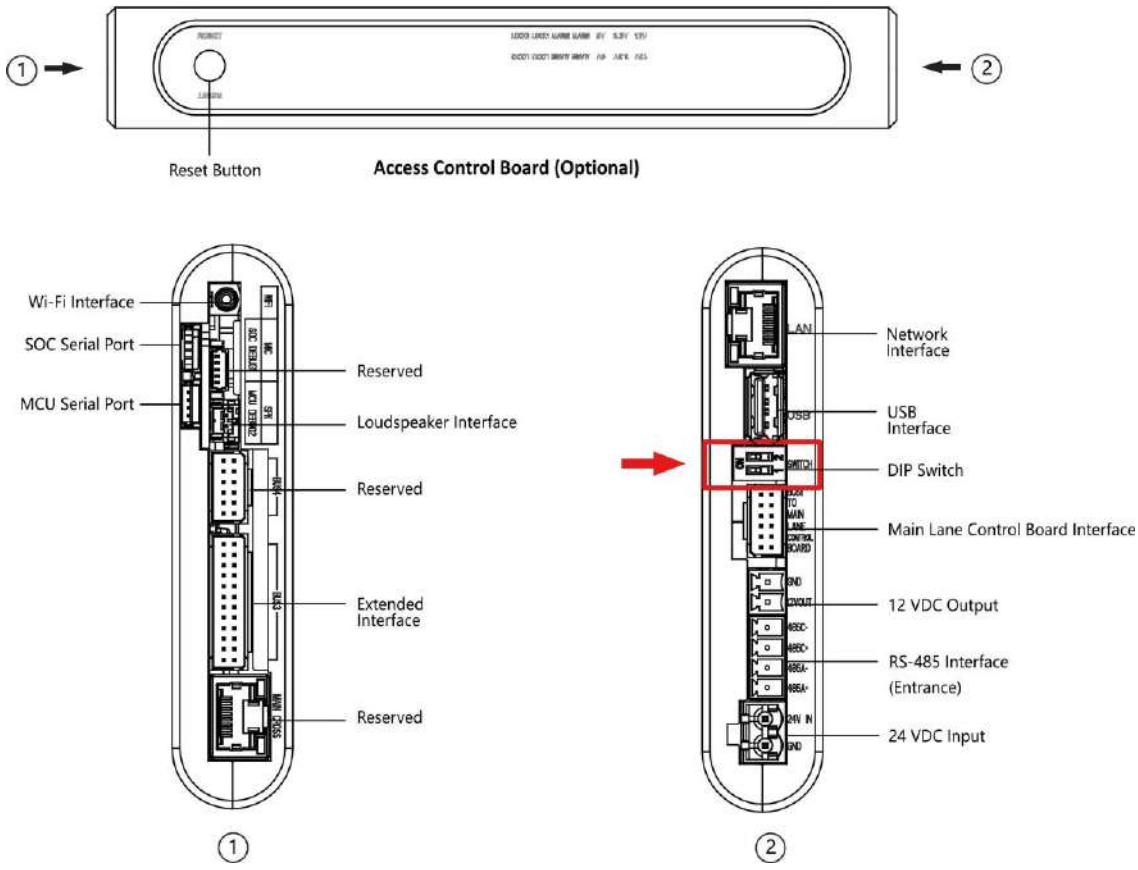


Figure 4-21 DIP Switch Location

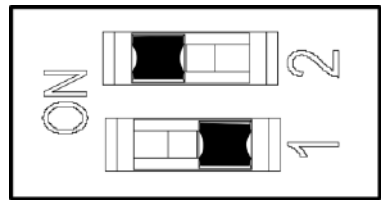


Figure 4-22 Enable Keyfob Paring Mode

3. Power on the turnstile and it will enter the keyfob pairing mode.
4. Hold the **Close** button for more than 10 seconds.
   The keyfob's indicator of the will flash twice if the pairing is completed.
5. Set the No.2 switch to the OFF side, and reboot the turnstile to take effect.

Note

- Only one turnstile can pair the keyfob. If multiple turnstiles are in the pairing mode, the keyfob will select only one of them to pair.
- For details about DIP switch value and meaning, see ***DIP Switch Description*** .

6. **Optional:** Go to **System → User → Keyfob User** on the remote control page of the client software to delete the keyfob.

4.4.4 Initialize Device

Steps

1. Hold the initialization button on the access control board for 5 s.

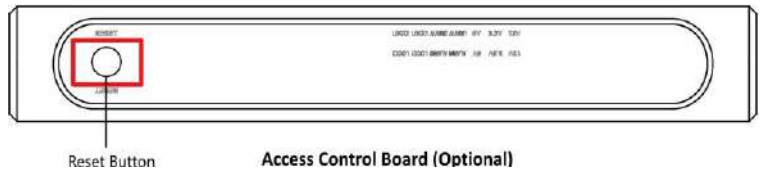


Figure 4-23 Initialization Button Position

2. The device will start restoring to factory settings.
3. When the process is finished, the device will beep for 3 s.

Caution

The initialization of the device will restore all the parameters to the default setting and all the device events are deleted.

Note

Make sure no persons are in the lane when powering on the device.

Chapter 5 Activation

You should activate the device before the first login. After powering on the device, the system will switch to Device Activation page.

Activation via the device, SADP tool and the client software are supported.

The default values of the device are as follows:

- The default IP address: 192.0.0.64
- The default port No.: 80
- The default user name: admin

5.1 Activate via Web Browser

You can activate the device via the web browser.

Steps

1. Enter the device default IP address (192.0.0.64) in the address bar of the web browser, and press **Enter**.

   Note

   Make sure the device IP address and the computer's should be in the same IP segment.

2. Create a new password (admin password) and confirm the password.

   Caution

   STRONG PASSWORD RECOMMENDED-We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

   Note

   Characters containing admin and nimda are not supported to be set as activation password.

3. Click **Activate**.
4. Edit the device IP address. You can edit the IP address via the SADP tool, the device, and the client software.

5.2 Activate via Mobile Web

You can activate the device via mobile web.

Steps

1. Connect to the device hotspot with your mobile phone by entering the hotspot password.

   Note

   - For inactive devices, hotspot is enabled by default.
   - The default hotspot password is the device serial number.

   The login page will pop up.
2. Create a new password (admin password) and confirm the password.

   Caution

   STRONG PASSWORD RECOMMENDED-We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

   Note

   Characters containing admin and nimda are not supported to be set as activation password.
3. Click **Activate**.
4. Edit the device IP address. You can edit the IP address via the SADP tool, the device, and the client software.

5.3 Activate via SADP

SADP is a tool to detect, activate and modify the IP address of the device over the LAN.

Before You Start

- Get the SADP software from the supplied disk or the official website ***http://www.hikvision.com/en/*** , and install the SADP according to the prompts.
- The device and the PC that runs the SADP tool should be within the same subnet.

The following steps show how to activate a device and modify its IP address. For batch activation and IP addresses modification, refer to *User Manual of SADP* for details.

Steps

1. Run the SADP software and search the online devices.
2. Find and select your device in online device list.
3. Input new password (admin password) and confirm the password.

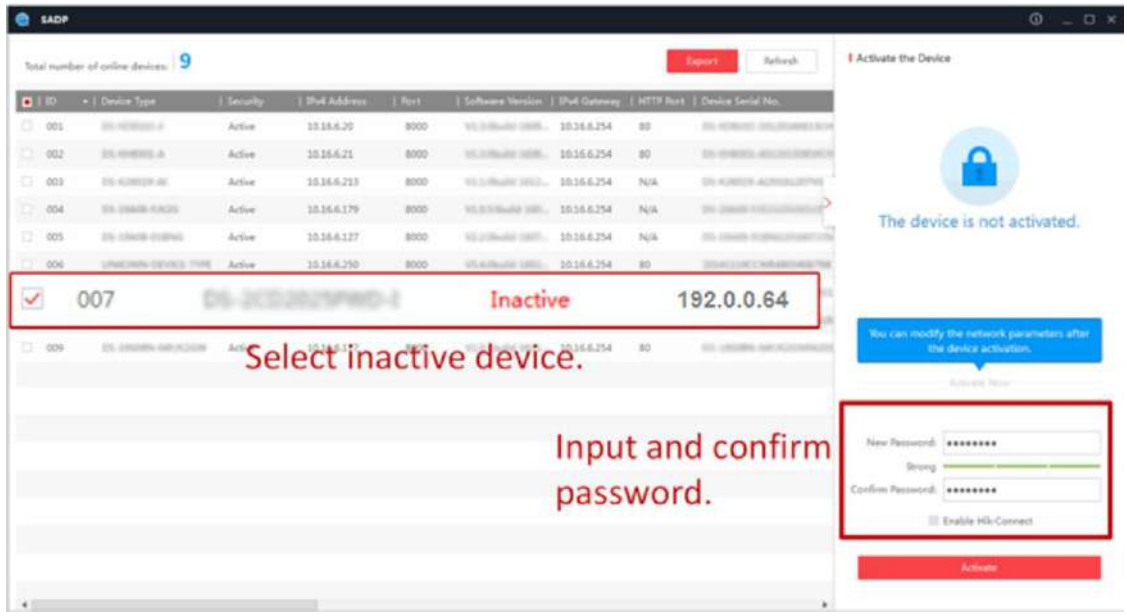
Caution

STRONG PASSWORD RECOMMENDED-We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Note

Characters containing admin and nimda are not supported to be set as activation password.

4. Click **Activate** to start activation.



Status of the device becomes **Active** after successful activation.

5. Modify IP address of the device.
   1) Select the device.
   2) Change the device IP address to the same subnet as your computer by either modifying the IP address manually or checking **Enable DHCP**.
   3) Input the admin password and click **Modify** to activate your IP address modification.

5.4 Activate Device via iVMS-4200 Client Software

For some devices, you are required to create the password to activate them before they can be added to the iVMS-4200 software and work properly.

Steps

Note

This function should be supported by the device.

1. Enter the Device Management page.
2. Click on the right of **Device Management** and select **Device**.
3. Click **Online Device** to show the online device area.
   The searched online devices are displayed in the list.
4. Check the device status (shown on **Security Level** column) and select an inactive device.
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

   Characters containing admin and nimda are not supported to be set as activation password.
7. Click **OK** to activate the device.

Chapter 6 Operation via Web Browser

6.1 Login

You can login via the web browser or the remote configuration of the client software.

Note

Make sure the device is activated. For detailed information about activation, see ***Activation*** .

Login via Web Browser

Enter the device IP address in the address bar of the web browser and press **Enter** to enter the login page.

Enter the device user name and the password. Click **Login**.

Login via Remote Configuration of Client Software

Download and open the client software. After adding the device, click to enter the Configuration page.

6.2 Overview

You can view the device component status, real-time event, person information, network status, basic information, and device capacity. You can also control the barrier remotely.

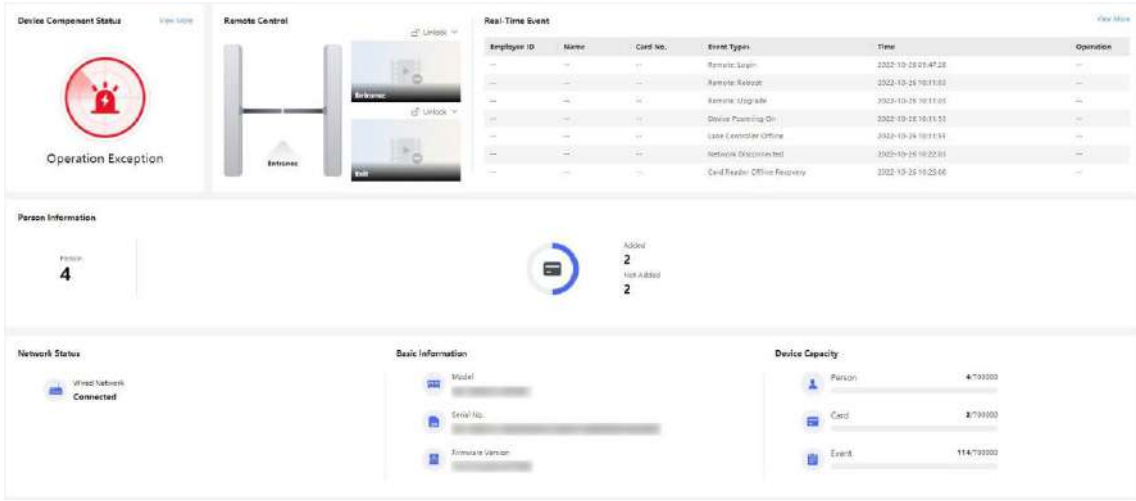


Figure 6-1 Overview

Function Descriptions:

Device Component Status

You can check if the device is working properly. Click **View More** to view the detailed component status.

Remote Control

/ / /

The door is opened/closed/remaining open/remaining closed.

Real-Time Event

You can view the event Employee ID, Name, Card No., Event Type, Time, and Operation. You can also click **View More** to enter the search conditions, including the event type, employee ID, the name, the card No., the start time, and the end time, and click **Search**. The results will be displayed on the right panel.

Person Information

You can view the added and not added information of person and card.

Network Status

You can view the network connection status.

Basic Information

You can view the model, serial No. and firmware version.

Device Capacity

You can view the person, card and event capacity.

6.3 Person Management

Click **Add** to add the person's information, including the basic information, certificate, authentication and settings.

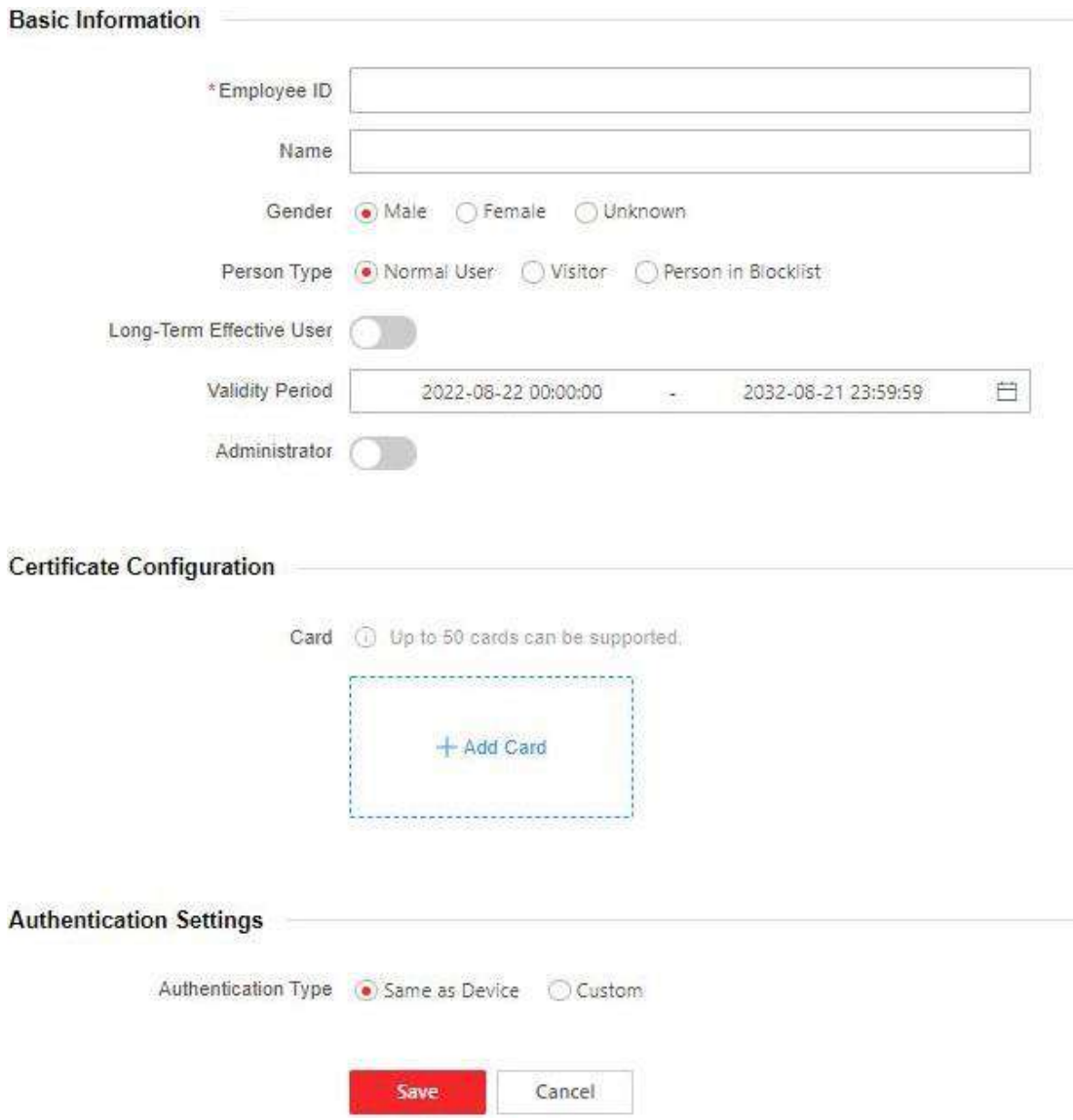


Figure 6-2 Add Person

Add Basic Information

Click **Person Management → Add** to enter the Add Person page.
Add the person's basic information, including the employee ID, the person's name, and person type.
If you select **Visitor** as the person type, you can set the visit times.
Click **Save** to save the settings.

Set Permission Time

Click **Person Management → Add** to enter the Add Person page.

Enable **Long-Term Effective User**, or set **Validity Period** and the person can only has the permission within the configured time period according to your actual needs.
Click **Save** to save the settings.

Add Card

Click **Person Management → Add** to enter the Add Person page.
Click **Add Card**, enter the **Card No.** and select the **Property**, and click **OK** to add the card.

Note
Up to 50 cards can be added.

Click **Save** to save the settings.

Authentication Settings

Click **Person Management → Add** to enter the Add Person page.
Set **Authentication Type** as **Same as Device** or **Custom**.
Click **Save** to save the settings.

Import/Export Person Data

Export Person Data

You can export added person data for back-up or importing to other devices.

Click **Export Person Data**, set an encryption password and confirm it. Click **OK**.

Note
- The person data will be downloaded to your PC.
- The password you set will be required for importing the data file.

Importing Person Data

Click **Importing Person Data** and select the file. Click **Import**.

Enter the encryption password to import and synchronize the person data to devices.

6.4 Search Event

Click **Event Search** to enter the Search page.

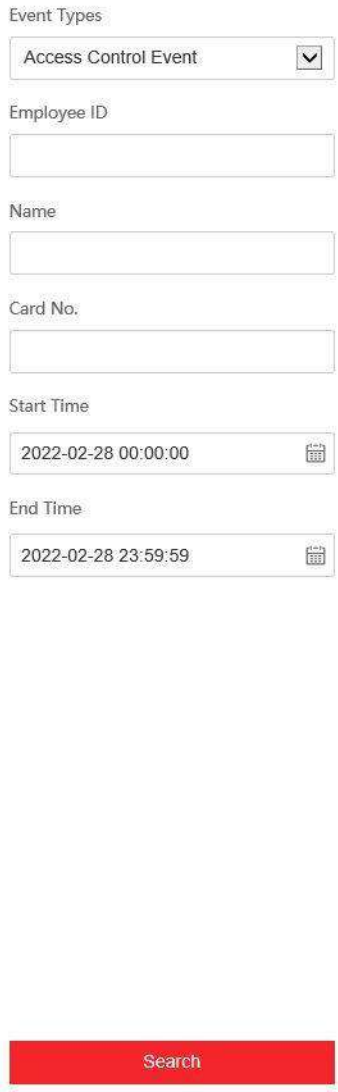


Figure 6-3 Search Event

Enter the search conditions, including the event type, the employee ID, the name, the card No., the start time, and the end time, and click **Search**.

The event types contain access control event and ID card event. If you choose to search for ID card event, you will not need to enter the employee ID, the name, or the card No.

The results will be displayed on the right panel.

6.5 Configuration

6.5.1 View Device Information

Click **Configuration → System → System Settings → Basic Information** to enter the configuration page.

You can view the device name, language, model, serial No., version, IO input, IO output, and local RS-485 number.

You can change **Device Name** and click **Save**.

You can view the device capacity, including person, card and event.

6.5.2 Set Time

Set the device's time.

Click **Configuration → System → System Settings → Time Settings** .

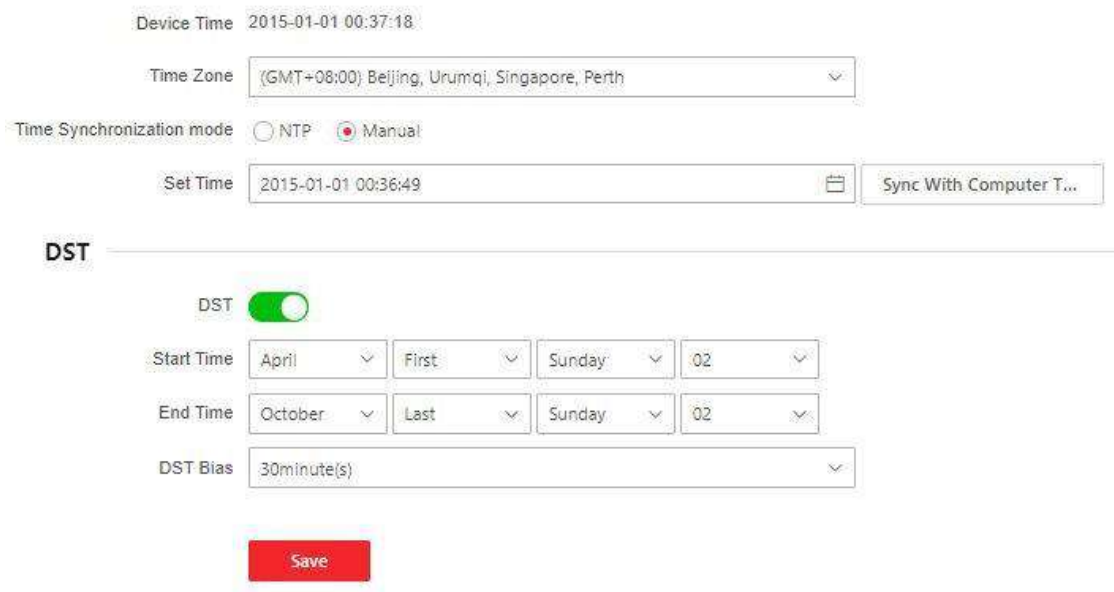


Figure 6-4 Time Settings

Click **Save** to save the settings after the configuration.

Time Zone

Select the device located time zone from the drop-down list.

Time Sync.

NTP

You should set the NTP server's IP address, port No., and interval.

Manual

By default, the device time should be synchronized manually. You can set the device time manually or check **Sync. with Computer Time** to synchronize the device time with the computer's time.

Server Address Type/Server Address/NTP Port/Interval

You can set the server address type, server address, NTP port, and interval.

6.5.3 Set DST

Steps

1. Click **Configuration → System → System Settings → Time Settings** .
2. Enable **DST**.
3. Set the DST start time, end time and bias time.
4. Click **Save** to save the settings.

6.5.4 Change Administrator's Password

Steps

1. Click **Configuration → User Management** .
2. Click .
3. Enter the old password and create a new password.
4. Confirm the new password.
5. Click **OK**.

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.

6.5.5 Online Users

The information of users logging into the device is shown.

Go to **Configuration → System → User Management → Online Users** to view the list of online users.

6.5.6 View Device Arming/Disarming Information

View device arming type and arming IP address.

Go to **Configuration → User Management → Arming/Disarming Information** .

You can view the device arming/disarming information. Click **Refresh** to refresh the page.

6.5.7 Network Settings

Set TCP/IP, hotspot and HTTP(S) parameters.

Set Basic Network Parameters

Click **Configuration → Network → Network Settings → TCP/IP** .

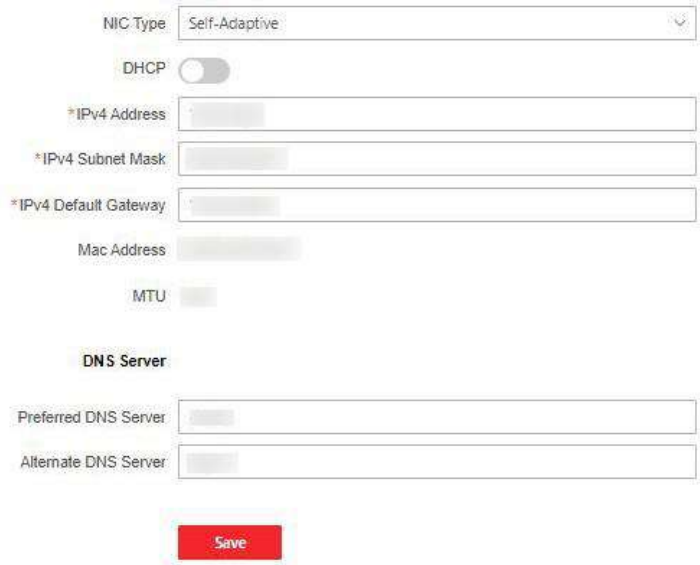


Figure 6-5 TCP/IP Settings Page

Set the parameters and click **Save** to save the settings.

NIC Type

Select a NIC type from the drop-down list. By default, it is **Auto**.

DHCP

If you uncheck the function, you should set the IPv4 address, IPv4 subnet mask, IPv4 default gateway, Mac address, and MTU.

If you check the function, the system will allocate the IPv4 address, IPv4 subnet mask, the IPv4 default gateway automatically.

DNS Server

Set the preferred DNS server and the Alternate DNS server according to your actual need.

Device Hotspot

Set the device hotspot.

Click **Configuration → Network → Network Settings → Device Hotspot** .

Click to **Enable Device Hotspot**. Set hotspot **Name** and **Password**.

Click **Save**.

Set Port Parameters

Set the HTTP, HTTPS, and HTTP Listening parameters.

Click **Configuration → Network → Network Service → HTTP(S)** .

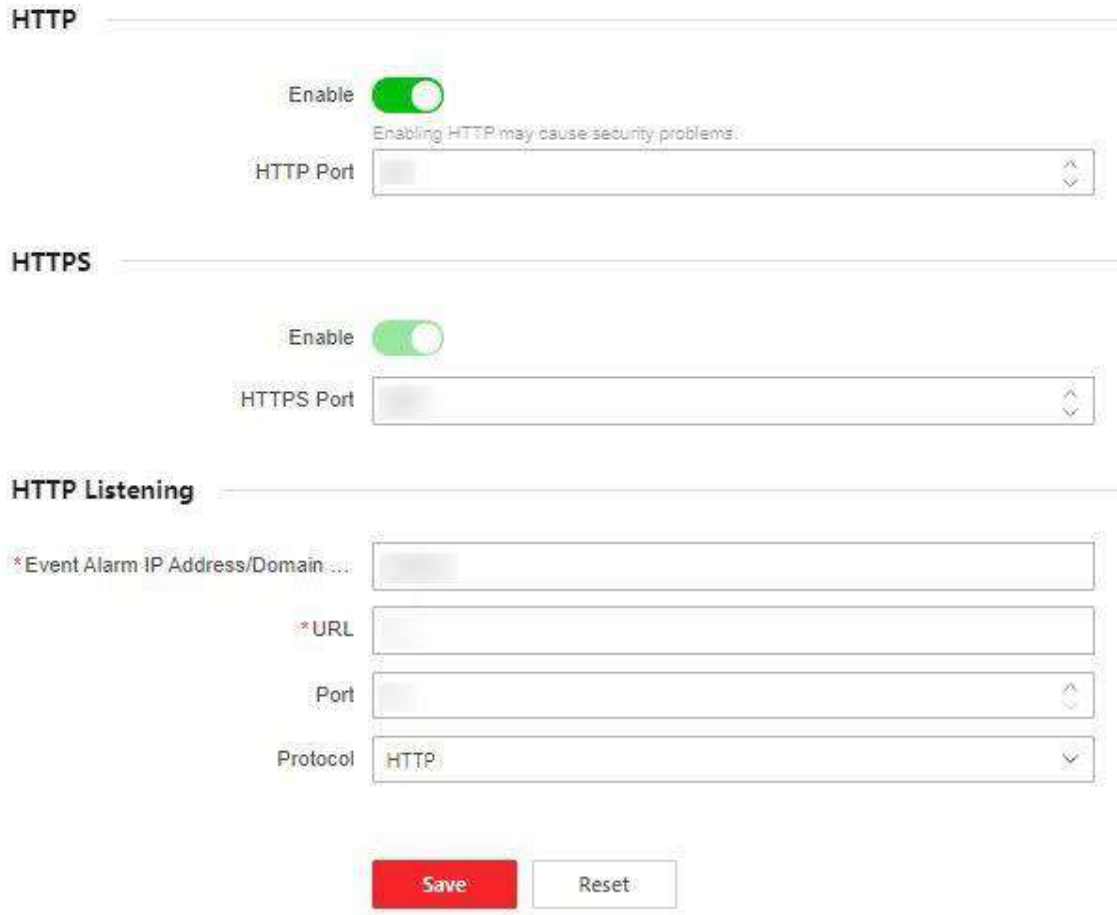


Figure 6-6 Network Service

HTTP

It refers to the port through which the browser accesses the device. For example, when the HTTP Port is modified to 81, you need to enter ***http://192.0.0.65:81*** in the browser for login.

HTTPS

Set the HTTPS for accessing the browser. Certificate is required when accessing.

HTTP Listening

The device can send alarm information to the event alarm IP address or domain name via HTTP protocol/HTTPS protocol. Edit the event alarm IP address or domain name, URL, port, and protocol.

Note

The event alarm IP address or domain name should support the HTTP protocol/HTTPS protocol to receive the alarm information.

.

6.5.8 Set Audio Parameters

Set the image quality, resolution, and the device volume.

Set Audio Parameters

Click **Configuration → Video/Audio → Audio** .

Figure 6-7 Set Audio Parameters

Drag the block to adjust the output volume.
Click **Save** to save the settings after the configuration.
You can also enable **Voice Prompt**.

Note
The functions vary according to different models. Refers to the actual device for details.

6.5.9 Event Linkage

Set linked actions for events.

Steps
1. Click **Configuration → Event → Event Detection → Linkage Settings** to enter the page.

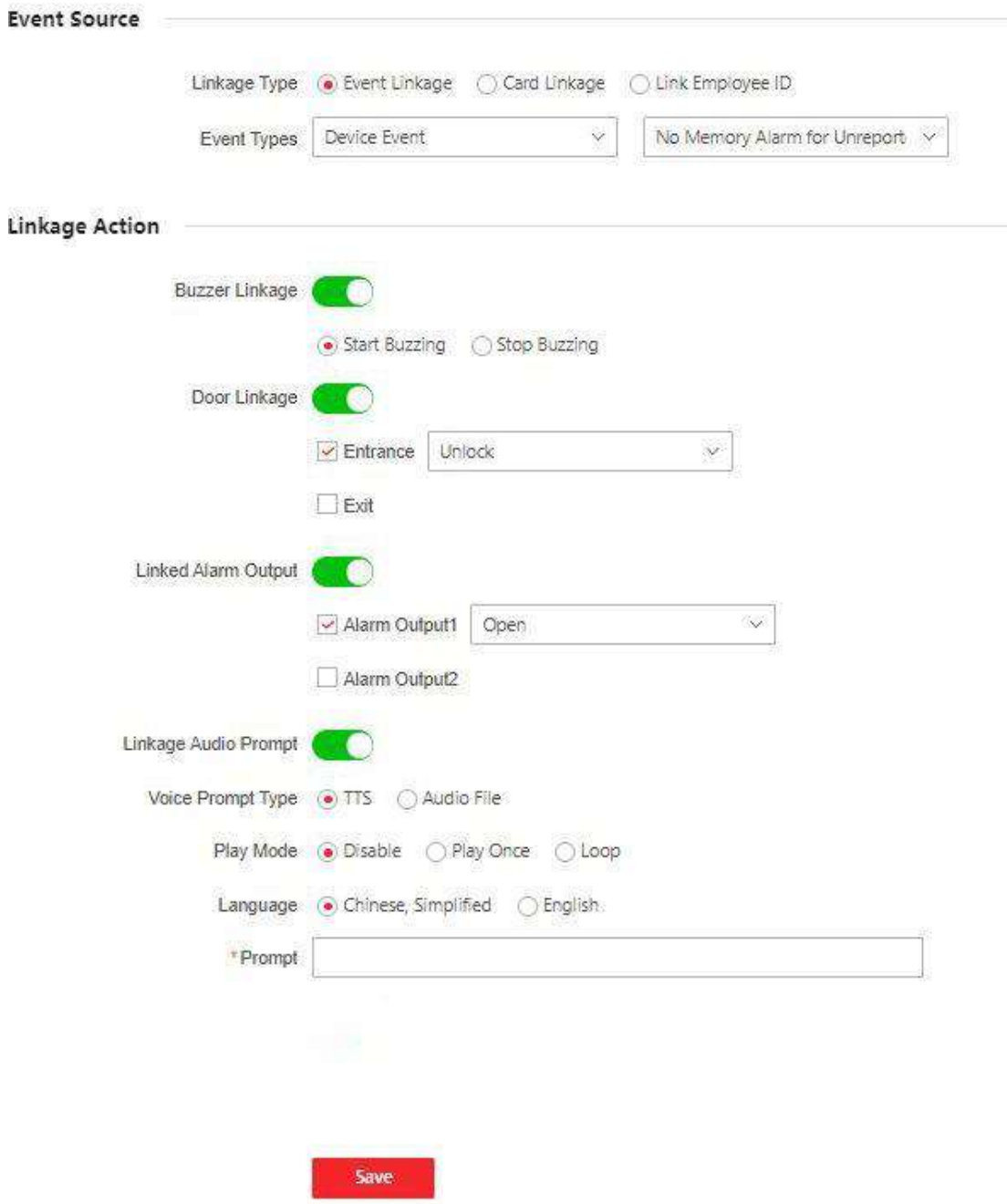


Figure 6-8 Event Linkage

2. Set event source.

- If you choose **Linkage Type** as **Event Linkage**, you need to select event types from the drop-down list.
- If you choose **Linkage Type** as **Card Linkage**, you need to enter the card No. and select the card reader.

- If you choose **Linkage Type** as **Employee ID Linkage**, you need to enter the employee ID and select the card reader.

3. Set linked action.

Linked Buzzer

Enable **Linked Buzzer** and select **Start Buzzing** or **Stop Buzzing** for the target event.

Linked Door

Enable **Linked Door**, check **Entrance** or **Exit**, and set the door status for the target event.

Linked Alarm Output

Enable **Linked Alarm Output**, check **Alarm Output 1** or **Alarm Output 2**, and set the alarm output status for the target event.

Linked Audio Prompt

Enable **Linked Audio Prompt** and select the play mode.

- If you choose **TTS**, you need to set language and enter the prompt content.
- If you choose **Audio File**, you need to select an available audio file from the drop-down list or click **General Linkage Settings** to add a new audio file.

6.5.10 Access Control Settings

Set Authentication Parameters

Click **Configuration → Access Control → Authentication Settings** .

Note

The functions vary according to different models. Refers to the actual device for details.

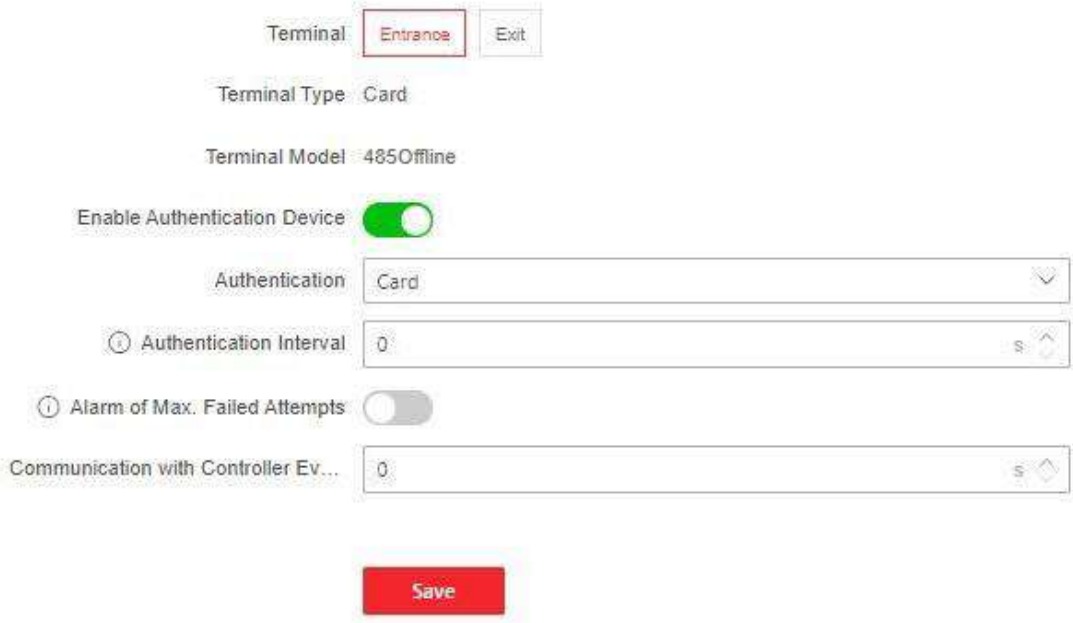


Figure 6-9 Set Authentication Parameters

Click **Save** to save the settings after the configuration.

Terminal

Choose **Entrance** or **Exit** for settings.

Terminal Type/Terminal Model

Get terminal description. They are read-only.

Enable Authentication Device

Enable the authentication function.

Authentication

Select an authentication mode according to your actual needs from the drop-down list.

Authentication Interval

You can set the authentication interval of the same person when authenticating. The same person can only authenticate once in the configured interval. A second authentication will be failed.

Alarm of Max. Failed Attempts

Enable to report alarm when the card reading attempts reach the set value.

Max. Authentication Failed Attempts

Enable to report alarm when the card reading attempts reach the set value.

Communication 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.

Note

The authentication interval value ranges from 2 s to 255 s.

Set Door Parameters

Click **Configuration → Access Control → Door Parameters** .

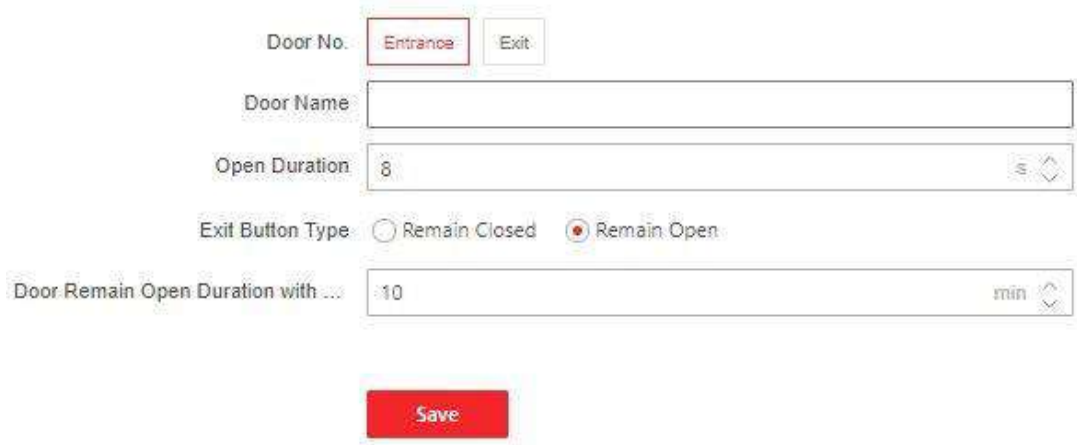


Figure 6-10 Door Parameters Settings Page

Click **Save** to save the settings after the configuration.

Door No.

Select **Entrance** or **Exit** for settings.

Door Name

You can create a name for the door.

Open Duration

Set the door unlocking duration. If the door is not opened for the set time, the door will be locked.

Note

The open duration ranges from 5 s to 60 s.

Exit Button Type

You can set the exit button as **Remain Open** or **Remain Closed** according to your actual needs. By default, it is **Remain Open**.

Door Remain Open Duration with First Person

Set the door open duration when first person is in. After the first person is authorized, it allows multiple persons access the door or other authentication actions.

Note

The duration ranges from 1 s to 1440 s.

Serial Port Settings

Set serial port parameters.

Steps

1. Click **Configuration → Access Control → Serial Port Configuration** .

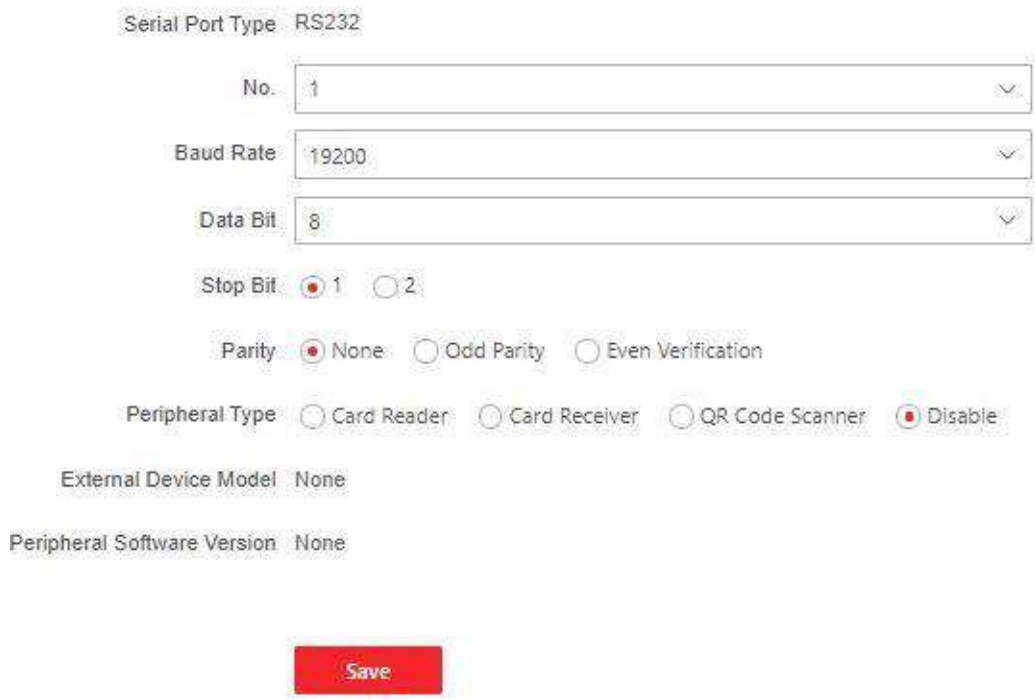


Figure 6-11 Serial Port Settings

2. Set the **No.**, **Baud Rate**, **Data Bit**, **Stop Bit** and **Parity**.
3. Set the **Peripheral Type** as **Card Reader**, **QR Code Scanner** or **Disable**.
4. You can view the serial port type, connected device model and peripheral software version.
5. Click **Save**.

Set Wiegand Parameters

You can set the Wiegand transmission direction.

Steps

Note

Some device models do not support this function. Refer to the actual products when configuration.

1. Click **Configuration → Access Control → Wiegand Settings** .
2. Select **Entrance** or **Exit**.
3. Enable **Wiegand** function.
4. The wiegand transmission direction is set **Input** by default.

   Note

   Input: the device can connect a Wiegand card reader.
5. Click **Save** to save the settings.

   Note

   If you change the peripheral, and after you save the device parameters, the device will reboot automatically.

Host Parameters

Set door contact settings and RS-485 protocol.

Steps

1. Click **Configuration → Access Control → Host Parameter** to enter the page.
2. Set door contact.

   Note

   You can set the door contact as **Door Open Status** or **Door Closed Status** according to your actual needs. By default, it is **Door Open Status**.
3. Set RS-485 protocol.
4. Click **Save**.

Set Terminal Parameters

Set the working mode and remote verification.

Steps

1. Click **Configuration → Access Control → Terminal Parameters** to enter the page.

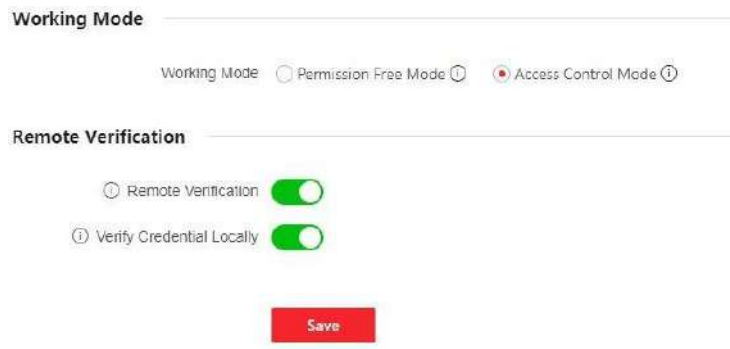


Figure 6-12 Terminal Parameters

2. Set the device working mode.

Permission Free Mode

The device will not verify the person's permission, but only the person's validity period. If the person is in the validity period, the barrier will open.

You can enable **Verify Credential Locally**. After enabling the function, the device will only verify the person's permission without the schedule template, etc.

Access Control Mode

The device works normally and will verify the person's permission to open the barrier.

3. Set remote verification.

1) Enable **Remote Verification**.

Note

The device will upload the person's authentication information to the platform. The platform will judge to open the barrier or not.

2) **Optional:** Enable **Verify Credential Locally**.

Note

After enabling the function, the device will only verify the person's permission without the schedule template, etc.

4. Click **Save** to complete terminal parameter settings.

6.5.11 Turnstile

Basic Parameters

Set turnstile basic parameters.

Steps

1. Click **Configuration → Turnstile → Basic Settings** to enter the page.
2. View the **Device Type**, **Device Model** and **Working Status**.
3. Set **Barrier Material**, **Lane Width**, **Barrier Height**, **Barrier Opening Speed** and **Barrier Closing Speed**.
4. Set the passing mode.
   - If you choose **General Passing**, you can select the barrier status for the entrance and exit from the drop-down list.

     Note

     If you set barrier-free mode, the barrier remains open and will close when authentication fails.
   - If you choose **Weekly Schedule**, you can set a weekly schedule for entrance and exit barriers.
5. Click **Save**.

keyfob

Set keyfob patameters.

Steps

1. Click **Configuration → Turnstile → Keyfob** to enter the page.

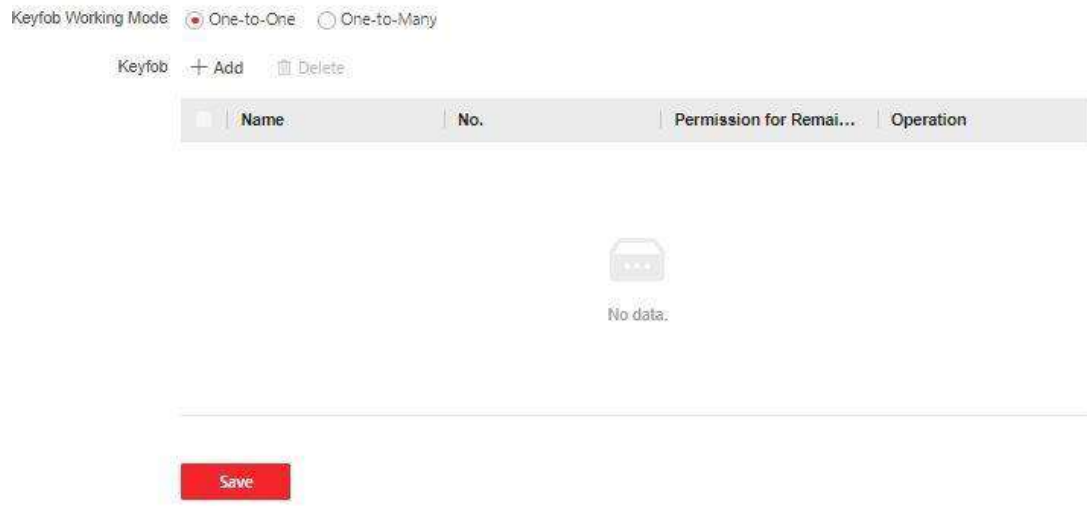


Figure 6-13 keyfob

2. Set **Working Mode** as **One-to-One** or **One-to-Many**.
3. Add keyfob.
   1) Click **Add** and the keyfob adding window will pop up.
   2) Enter the **Name** and **Serial No.**.
   3) Check to enable **Remain Open Permission** at your actual needs.
   4) Click **OK** to add the keyfob.

4. **Optional:** Select a keyfob and click **Delete** to delete the keyfob.
5. Click **Save**.

IR Detector

Set IR detector.

Steps

1. Click **Configuration → Turnstile → IR Detector** to enter the page.

Figure 6-14 IR Detector

2. Set the entrance and exit inductive mode as **Single Triggered** or **Triggered Simultaneously**.
3. Set custom IR detector mode.

   Enable IR Emergency Mode

   If some IR beams do not work properly, you can shield those IR beams to restore the lane. But this action may hit person and cause injury.

   Enable Custom Anti-pinch for Door Closing

   Anti-pinch for door closing refers that the barrier will not close if the device has detected person in the lane. Only after the person walks out of the lane, the barrier will close. If you enable the function, you can shield parts of the IR beams for closing barrier in advance. But this action may hit person and cause injury.
4. Click **Save**.

People Counting

Set people counting .

Steps

1. Click **Configuration → Turnstile → People Counting** to enter the page.

Figure 6-15 People Counting

2. Check to enable **People Counting**.
3. Enable **Device Offline People Counting** at your actual needs.
4. Select **People Counting Type** as **Invalid**, **Passing Detection** or **Authentication Number**.
5. **Optional:** Click **clear** to clear all the people counting information.

Set Indicator Color

Set the color for the indicators.

Steps

1. Click **Configuration → Turnstile → Light Settings** to enter the page.
2. Set light color for lane status indicator.
   1) Set **Light Brightness** as **Auto** or **Fixed Brightness**. If you choose **Fixed Brightness**, you can drag the block or enter the value to adjust the light brightness manually.
   2) Set inductive, prohibited and Auth. passing light color.
3. Set barrier light color.
   1) Check to enable **Light on When on Standby** at your actual needs.
   2) Set the barrier light color.
4. Click **Save**.

Other Settings

Set other parameters.

Steps

1. Click **Configuration → Turnstile → Other Settings** to enter the page.
2. Set **Alarm Output Duration**.

Note

The alarm output duration ranges from 0 s to 3599 s.

3. Set **Temperature Unit**.
4. Check to enable **Do Not Open Barrier When Lane is Not Clear**.
5. Drag the block or enter the value to adjust the light board brightness.
6. Set the alarm buzzer beeping duration, door closing delay time, intrusion duration, overstaying duration and IR obstructed duration.
7. Check to enable **Memory Mode** at your actual needs.

Note

Multiple cards presenting for multiple person passing is allowable when enabling the memory mode. When the passing person's number exceeds the card presenting number, or after the latest person passing with no other person passing within the door open duration, the door will close automatically.

8. Choose the control mode.

Soft Mode

The barrier will be closed after the person has passed through the barrier when there are tailing, forced accessing, etc.

Guard Mode

The barrier will be closed immediately when there are tailgating, forced accessing, etc.

9. Set the fire input type.
10. Click to enable **Motor Self-Test** and choose the main lane or sub lane to start motor self-testing.
11. Click **Save**.

6.5.12 Card Settings

Set Card Security

Click **Configuration → Card Settings → Card Type** to enter the settings page.

Set the parameters and click **Save**.

Enable NFC Card

In order to prevent the mobile phone from getting the data of the access control, you can disable NFC card to increase the security level of the data.

Enable M1 Card

Enable M1 card and authenticating by presenting M1 card is available.

M1 Card Encryption

Sector

M1 card encryption can improve the security level of authentication.

Enable the function and set the encryption sector. By default, Sector 13 is encrypted. It is recommended to encrypt sector 13.

Enable EM Card

Enable EM card and authenticating by presenting EM card is available.

Note

If the peripheral card reader supports presenting EM card, the function is also supported to enable/disable the EM card function.

Enable CPU Card

Enable CPU card and authenticating by presenting CPU card is available.

CPU Card Read Content

After enable the CPU card content reading function, the device can read the CPU card content.

Enable FeliCa Card

The device can read the data from FeliCa card when enabling the FeliCa card function.

Set Card Authentication Parameters

Set the card reading content when authenticate via card on the device.

Go to **Configuration → Card Settings → Card NO. Authentication Settings** .

Select a card authentication mode and enable reversed card No. at your actual needs. Click **Save**.

6.5.13 Set Privacy Parameters

Set the event storage type.

Go to **Configuration → Security → Privacy Settings**

The event storage type is overwriting by default. The earliest 5% events will be deleted when the system detects the stored events has been over 95% of the full space.

6.5.14 Prompt Schedule

Customize the output audio content when authentication succeeded and failed.

Steps

1. Click **Configuration → Preference → Prompt Schedule** .

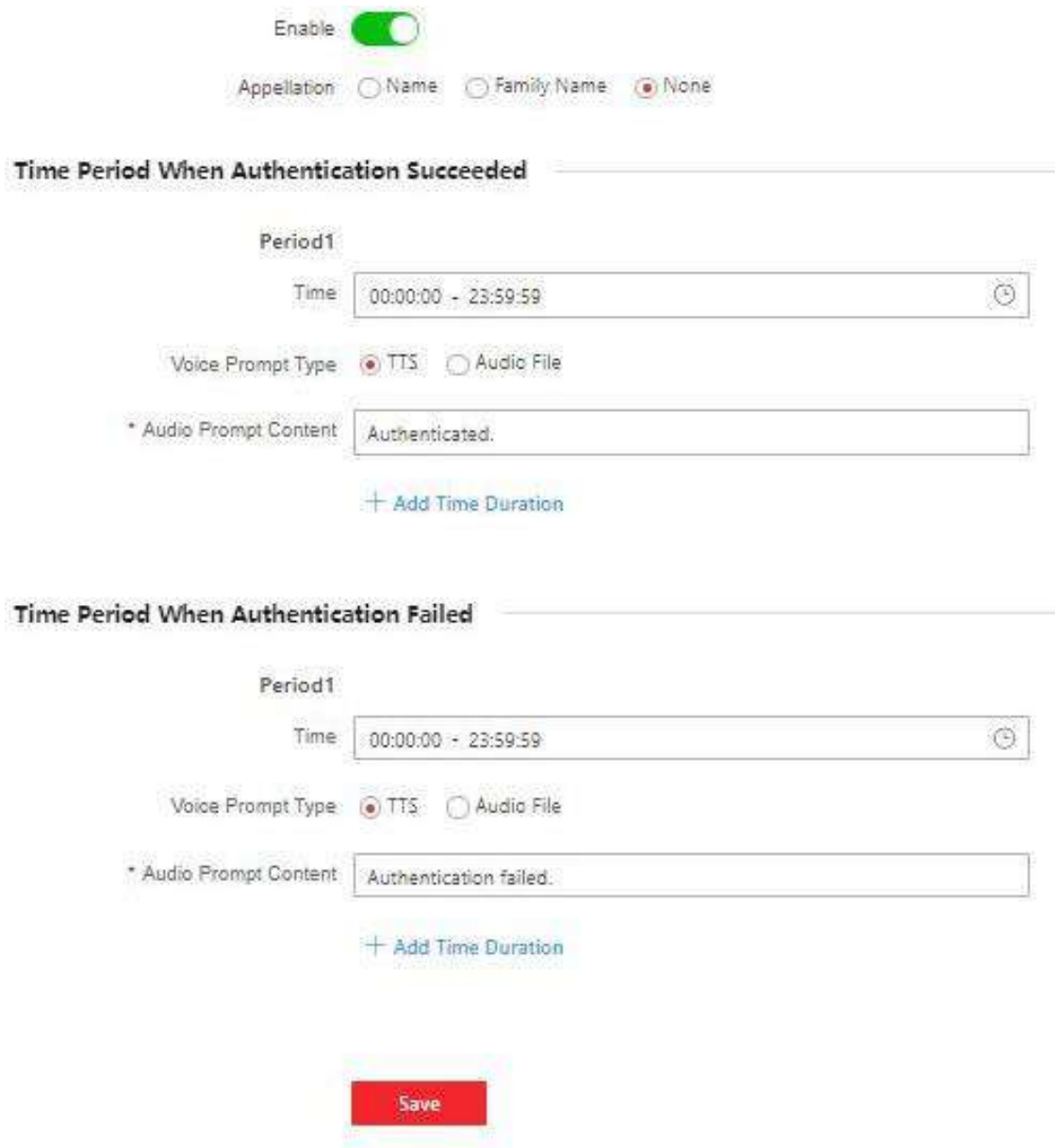


Figure 6-16 Customize Audio Content

2. Select time schedule.

3. Enable the function.

4. Set the appellation.

5. Set the time period when authentication succeeded.

1) Click **Add Time Duration**.

2) Set the time duration.

Note

If authentication is succeeded in the configured time duration, the device will broadcast the configured content.

3) Set the audio content.

TTS

If you choose TTS, you need to set the language and enter the prompt content of authentication success.

Audio File

If you choose audio file, you need to select an available audio file from the drop-down list or click **Audio File Management** to add a new file.

Note

The audio file's format should be wav, and the size should be within 200 KB.

4) **Optional:** Repeat substep 1 to 3.

5) **Optional:** Click to delete the configured time duration.

6. Set the time duration when authentication failed.

1) Click **Add**.

2) Set the time duration.

Note

If authentication is failed in the configured time duration, the device will broadcast the configured content.

3) Set the audio content.

TTS

If you choose TTS, you need to set the language and enter the prompt content of authentication failure.

Audio File

If you choose audio file, you need to select an available audio file from the drop-down list or click **Audio File Management** to add a new file.

Note

The audio file's format should be wav, and the size should be within 200 KB.

4) **Optional:** Repeat substep 1 to 3.

5) **Optional:** Click to delete the configured time duration.

7. Click **Save** to save the settings.

6.5.15 Upgrade and Maintenance

Reboot device, restore device parameters, and upgrade device version.

Reboot Device

Click **Maintenance and Security → Maintenance → Restart** .
Click **Restart** to reboot the device.

Upgrade

Click **Maintenance and Security → Maintenance → Upgrade** .
Select an upgrade type from the drop-down list. Click and select the upgrade file from your local PC. Click **Upgrade** to start upgrading.

Note
Do not power off during the upgrading.

Restore Parameters

Click **Maintenance and Security → Maintenance → Backup and Reset** .

Restore All

All parameters will be restored to the factory settings. You should activate the device before usage.

Restore

The device will restore to the default settings, except for the network parameters and the user information.

Import and Export Parameters

Click **Maintenance and Security → Maintenance → Backup and Reset** .

Export

Click **Export** to export the device parameters.

Note
You can import the exported device parameters to another device.

Import

Click and select the file to import. Click **Import** to start import configuration file.

6.5.16 Device Debugging

You can set device debugging parameters.

Steps

1. Click **Maintenance and Security → Maintenance → Device Debugging** .
2. You can set the following parameters.

Enable SSH

To raise network security, disable SSH service. The configuration is only used to debug the device for the professionals.

Print Log

You can click **Export** to export log.

6.5.17 Component Status

You can view the main lane and sub lane status.

Main Lane Status

Device Component

You can view the status of the access control board, lane control board, user extended interface board, and passing mode indicator board.

Peripheral

You can view the status of the RS-485 card reader and tamper input.

Temperature

You can view the pedestal temperature.

Movement

You can view the working status of motor encoder.

Sub Lane Status

Device Component

You can view the status of the lane control board, passing mode indicator board and upper IR adaptor.

Peripheral

You can view the status of the RS-485 card reader, RS-232 card receiver and tamper input.

Movement

You can view the working status of motor encoder.

Others

Passing Mode

You can view the entrance and exit mode.

IR Detector Status

You can view the status of each pair of the IR beam sensors.

Input and Output Status

You can view the status of the event input/output, alarm input/output and fire alarm.

Other Status

You can view the status of the barrier and the keyfob receiving module.

6.5.18 Log Query

You can search and view the device logs.

Go to **Maintenance and Security → Maintenance → Log** .

Set the major and minor type of the log type. Set the start time and end time for searching, and click **Search**.

The results will be displayed below, which including the No., time, the major type the minor type, the channel No., the local/remote user information, the remote host IP, etc.

6.5.19 Certificate Management

It helps to manage the server/client certificates and CA certificate.

Note

The function is only supported by certain device models.

Create and Install Self-signed Certificate

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. In the **Certificate Files** area, select a **Certificate Type** from the drop-down list.
3. Click **Create**.
4. Input certificate information.
5. Click **OK** to save and install the certificate.

   The created certificate is displayed in the **Certificate Details** area.

   The certificate will be saved automatically.
6. Download the certificate and save it to an asking file in the local computer.
7. Send the asking file to a certification authority for signature.
8. Import the signed certificate.
   1) Select a certificate type in the **Import Passwords** area, and select a certificate from the local, and click **Install**.
   2) Select a certificate type in the **Import Communication Certificate** area, and select a certificate from the local, and click **Install**.

Install Other Authorized Certificate

If you already has an authorized certificate (not created by the device), you can import it to the device directly.

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. In the **Import Passwords** and **Import Communication Certificate** areas, select certificate type and upload certificate.
3. Click **Install**.

Install CA Certificate

Before You Start

Prepare a CA certificate in advance.

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. Create an ID in the **Import CA Certificate** area.

   Note

   The input certificate ID cannot be the same as the existing ones.
3. Upload a certificate file from the local.
4. Click **Install**.

Chapter 7 Configure the Device via the Mobile Browser

7.1 Login

You can log in via mobile browser.

Note

Make sure the device is activated.

You can log in via the following methods:

- If device hotspot is disabled, make sure your mobile phone and the device are connected to the same network. Place your phone to the NFC area and the login page will pop up. If device hotspot is enabled, place your phone to the NFC area and the name and pass
- When the device hotspot is enabled, you can connect to the device hotspot and the loginpage will pop up.
  Enter the device user name and the password. Click **Login**.
- When the device hotspot is enabled, place your phone to the NFC area and the name and passwordof the device hotspot will be obtained automatically.

Note

Android system supporting NFC function is recommended. IOS system is not supported.

7.2 Overview

You can view the device status, conduct remote control, etc.

You can view the device status. If there is exception, you can tap to view the component details.

You can remotely control barrier by tap the icons.

Figure 7-1 Shortcut Entry and Network Status

You can tap to fast enter the basic settings page, user page, keyfob page, light page and network page.

7.3 Configuration

7.3.1 Turnstile Basic Parameters

You can set the basic parameters of the turnstile.

Tap **Basic Settings** of the shortcut entry on the overview page.

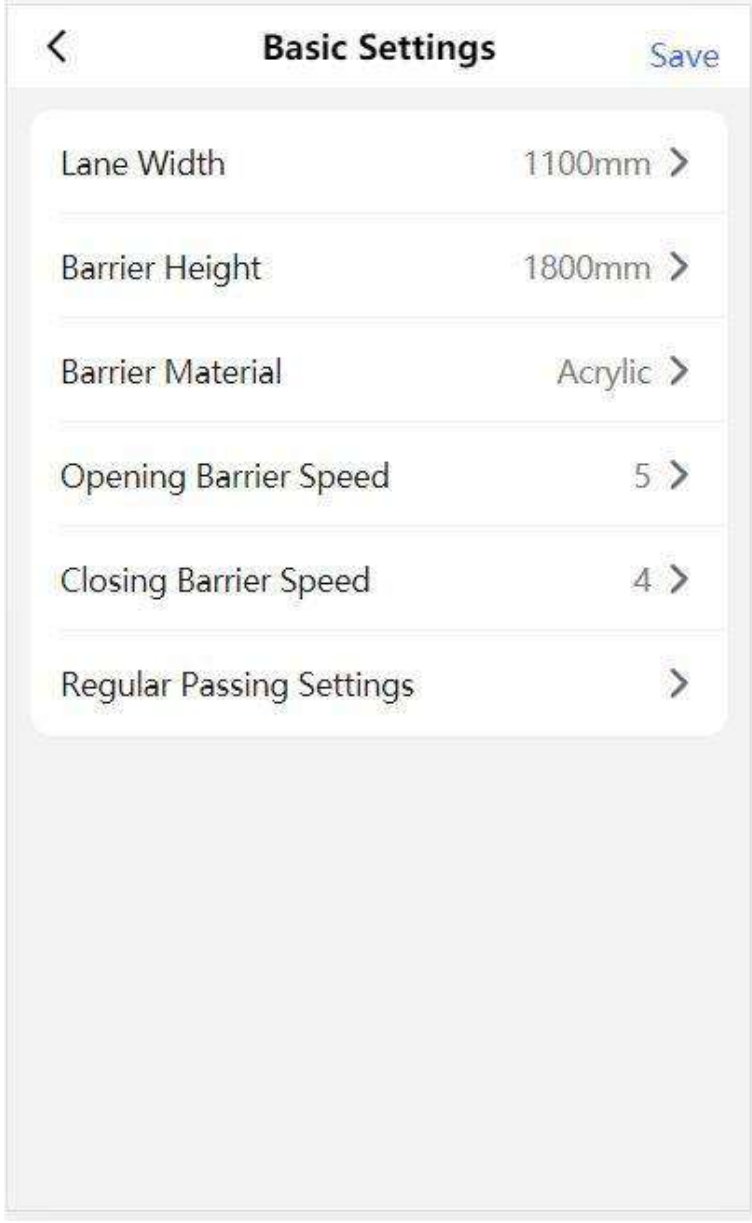


Figure 7-2 Turnstile Basic Parameters

Set **Lane Width**, **Barrier Height**, **Barrier Height**, **Barrier Opening Speed** and **Barrier Closing Speed**.
Set the regular passing mode for the entrance and exit.
Tap **Save**.

7.3.2 User Management

You can add, edit, delete, and search users via mobile Web browser.

Steps

1. Tap **User** to enter the settings page.

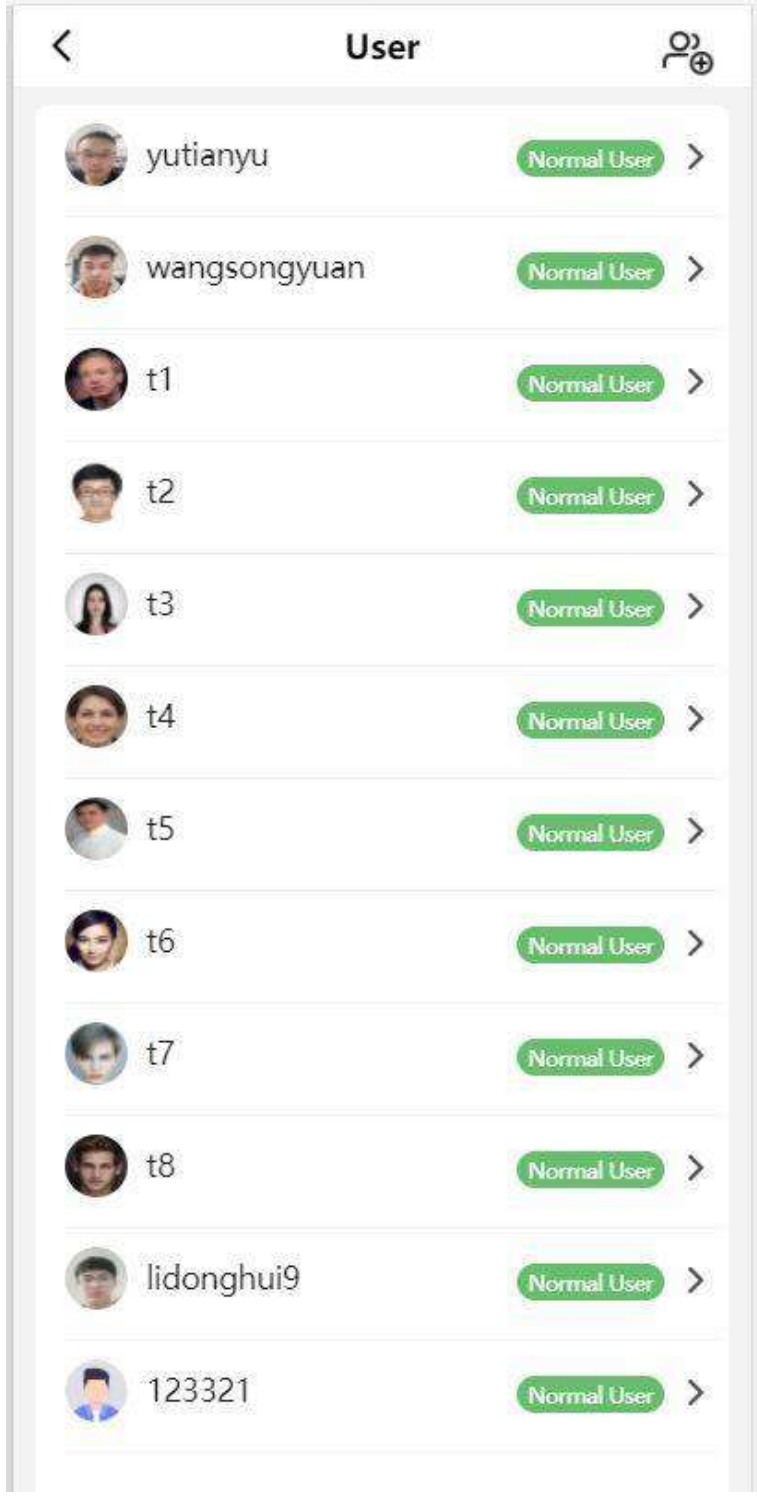


Figure 7-3 Add User

2. Add user.

1) Tap .

2) Set the following parameters.

Employee ID

Enter the employee ID. The Employee ID cannot be 0 or exceed 32 characters. It can be a combination of uppercase, lowercase letters and numbers.

Name

Enter your name. The name supports numbers, uppercase and lowercase English, and characters. The name is recommended to be within 32 characters.

User Role

Select your user role.

Card

Add card. Tap **Card → Add Card** , enter the card No. and select the card type.

3) Tap **Save**.

3. Tap the user that needs to be edited in the user list to edit the information.

7.3.3 Keyfob Settings

Tap **Keyfob** of the shortcut entry on the overview page.

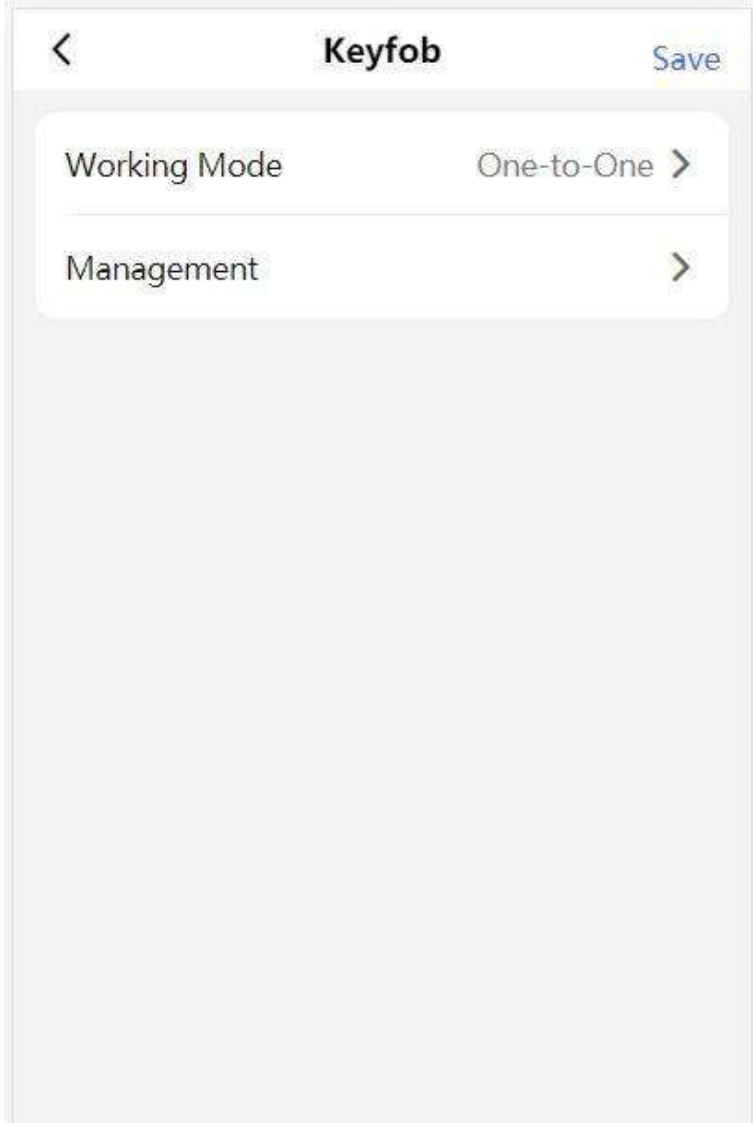


Figure 7-4 Keyfob Settings

Set **Working Mode** as **One-to-One** or **One-to-Many**.

Tap **Management** to enter the page. Tap **+** to add keyfob. Set keyfob name, serial No. and remain open permission.

7.3.4 Light Settings

Tap **Light** of the shortcut entry on the overview page.

Lane Status Indicator

Figure 7-5 Lane Status Indicator Settings

Light Brightness is set **Manual** by default. Enter the value to adjust the light brightness manually. Set light color for inductive/remain open, remain closed and controlled/barrier-free mode respectively.

Barrier Light

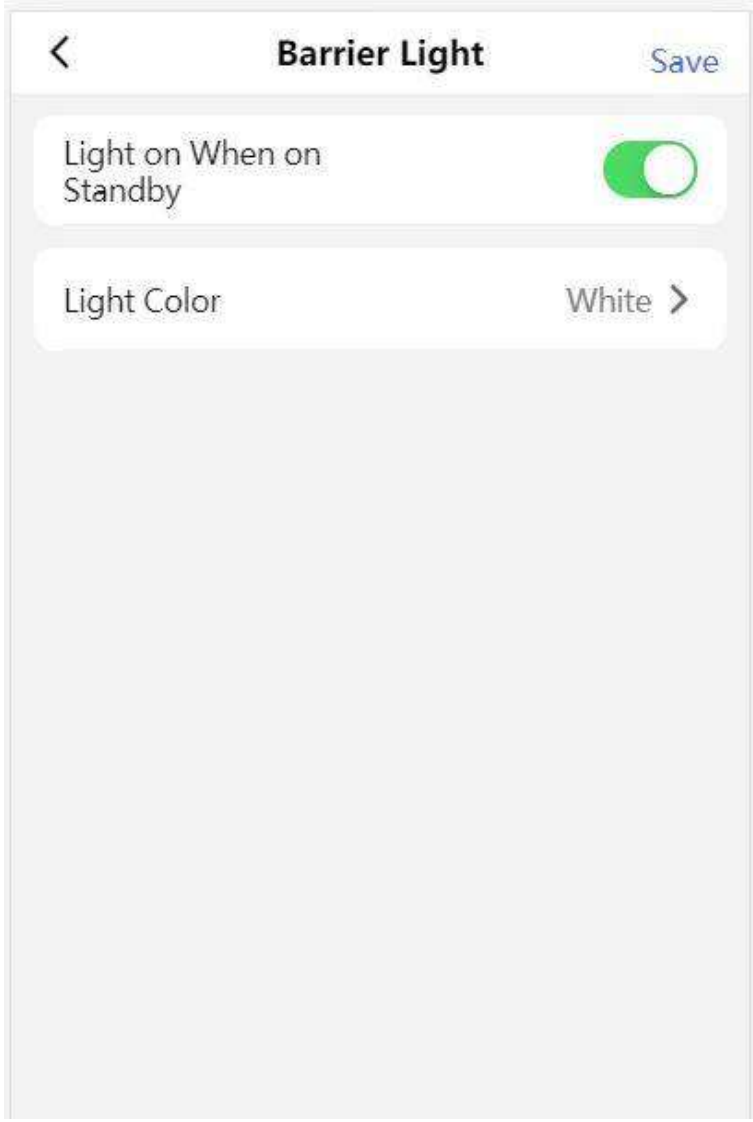


Figure 7-6 Barrier Light Settings

Tap to enable **Light on When on Standby** at your actual needs and set the barrier light color.

7.3.5 Network Settings

You can set the wired network, device hotspot and port.

Wired Network

Set wired network.

Tap **Configuration → Communication Settings → Wired Network** to enter the configuration page.

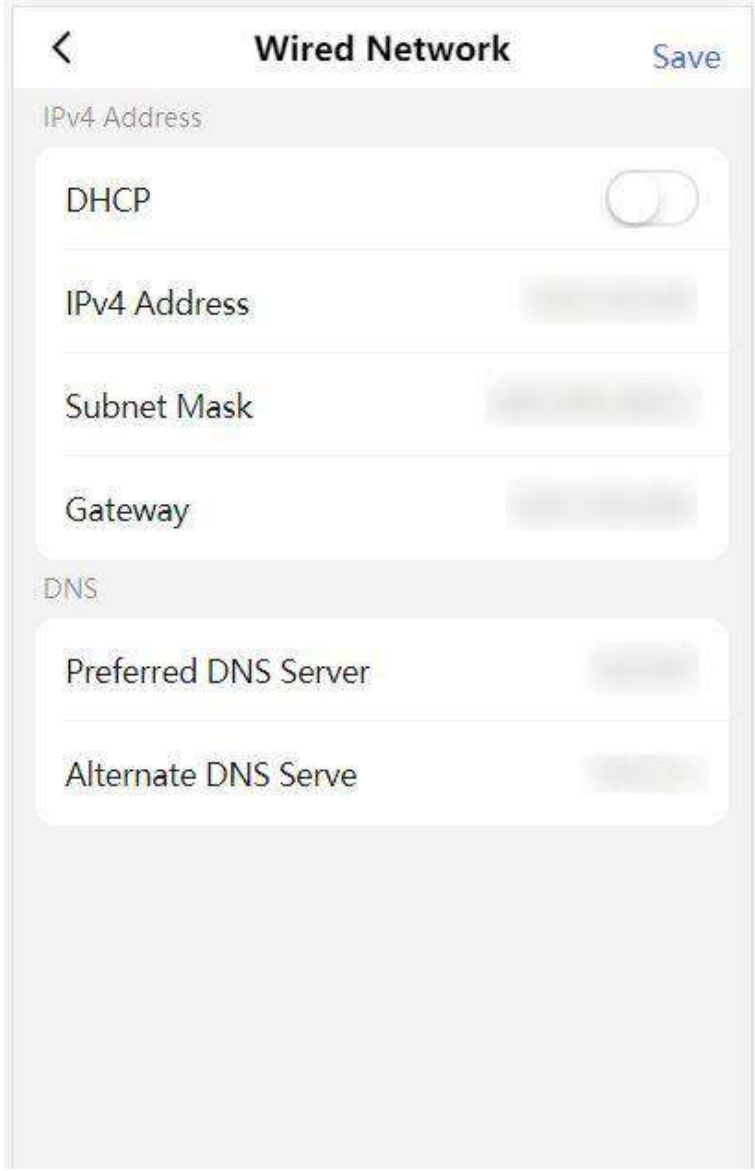


Figure 7-7 Wired Network

DHCP

If you disable the function, you should set the IPv4 address, IPv4 subnet mask, and IPv4 default gateway.

If you enable the function, the system will allocate the IPv4 address, IPv4 subnet mask, and IPv4 default gateway automatically.

DNS Server

Set the preferred DNS server and the Alternate DNS server according to your actual need.

Device Hotspot

Set device hotspot.

Tap **Configuration → Communication Settings → Device Hotspot** to enter the configuration page.

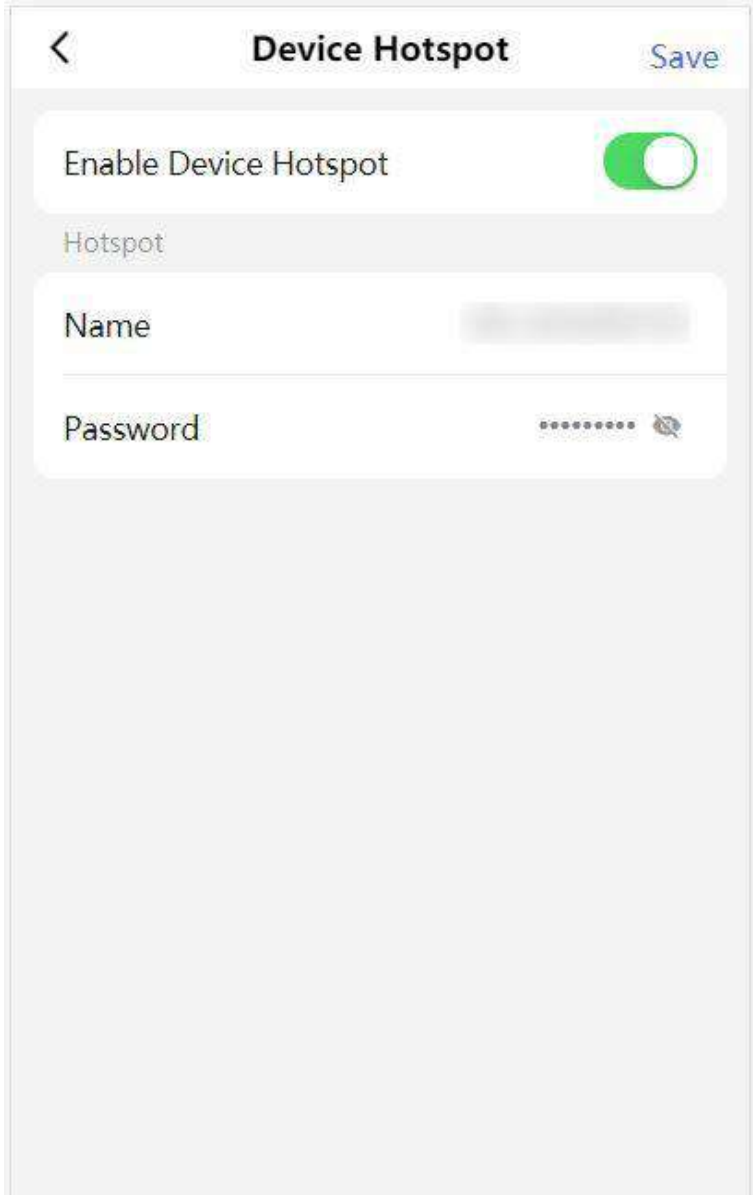


Figure 7-8 Device Hotspot

Tap to **Enable Device Hotspot**. Set hotspot **Name** and **Password**.

Click **Save**.

Serial Port Configuration

Set serial port.

Tap **Configuration → Communication Settings → Serial Port Configuration** to enter the configuration page.

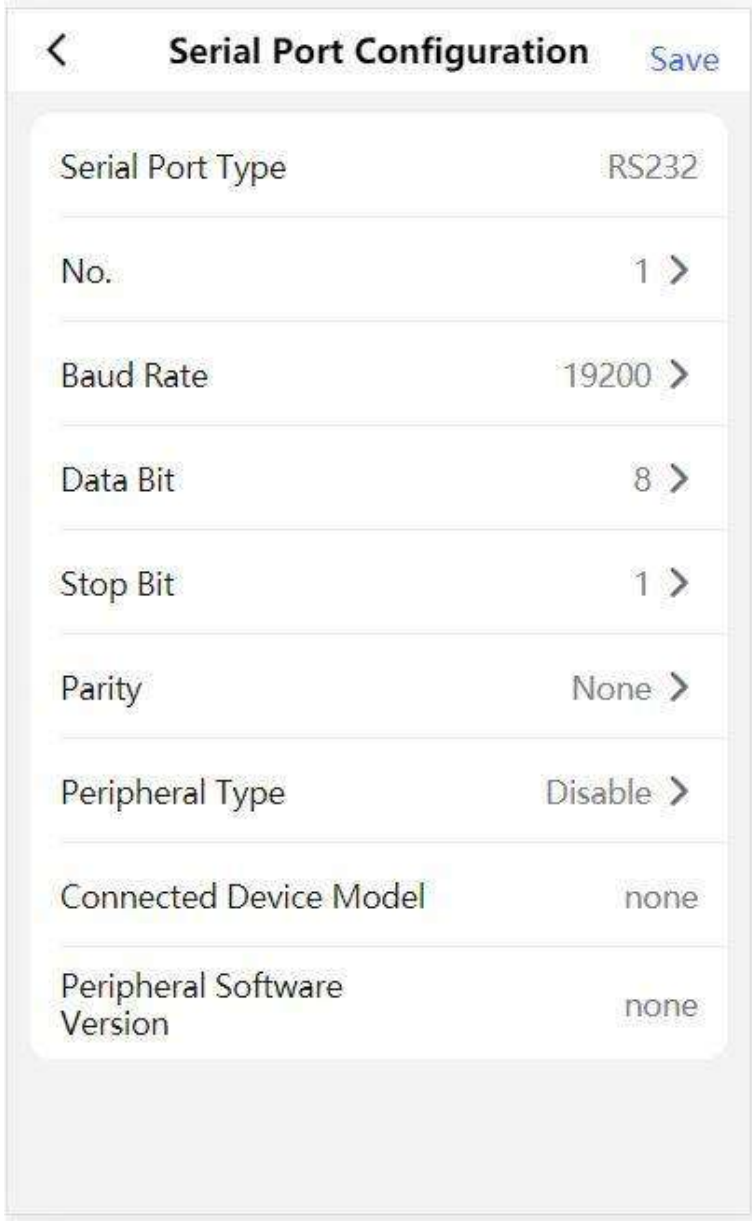


Figure 7-9 Serial Port Configuration

Select the port **No.**, and set **Baud Rate**, **Data Bit**, **Stop Bit** and **Parity**.

Set the **Peripheral Type** as **Card Reader**, **Card Receiver**, **QR Code Scanner** or **Disable**.

Tap **Save**.

7.3.6 Device Basic Settings

Set audio, time, sleep time and privacy.

Tap **Configuration → Basic Settings** to enter the configuration page.

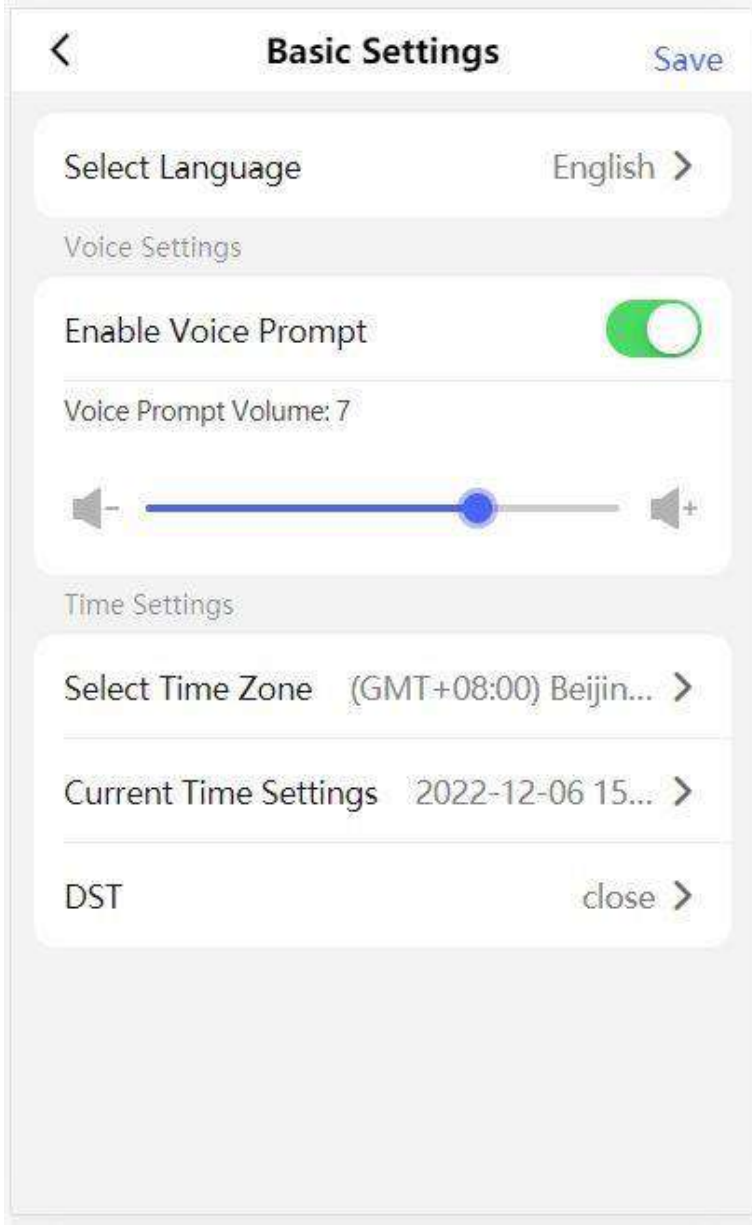


Figure 7-10 Basic Configuration

Language

The language is set English by default.

Voice Settings

Tap to **Enable Voice Prompt**, select entrance or exit to set voice prompt and drag to set the volume.

Time Settings

Tap to select the time zone and the device time.

Tap **DST** to enter the DST setting page. Enable DST and set the DST start time, end time and bias time

7.3.7 Access Control Settings

Set Door Parameters

Tap **Configuration → Access Control → Door Parameters** .

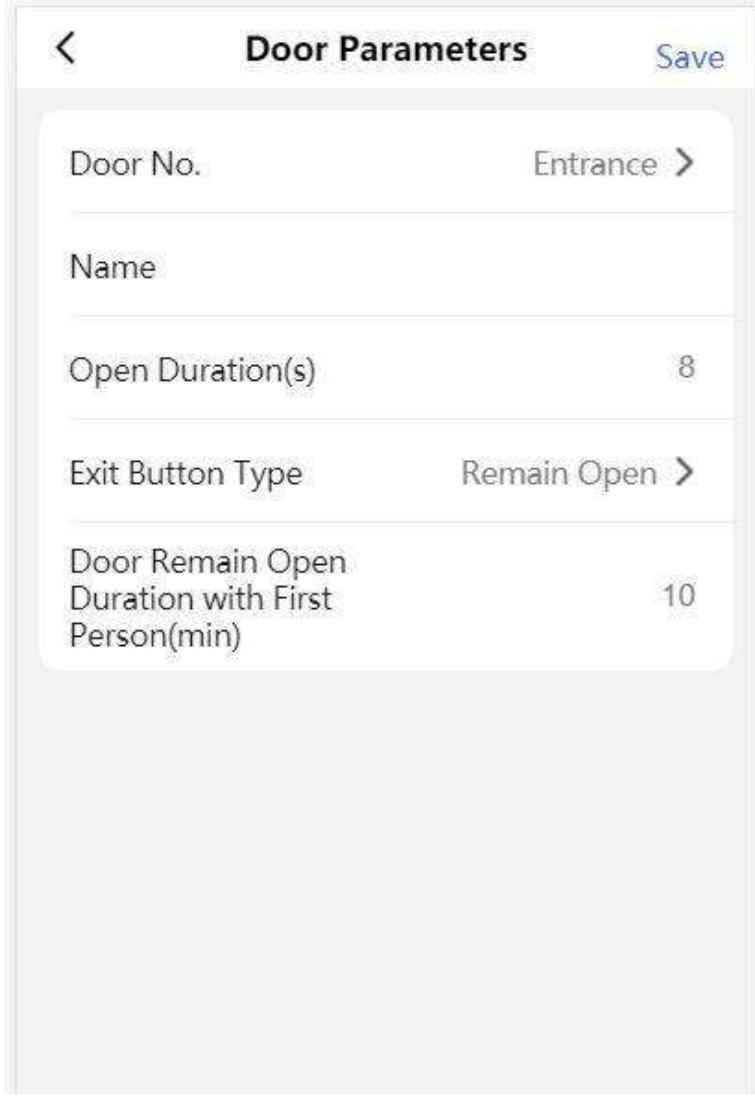


Figure 7-11 Door Parameters Settings Page

Click **Save** to save the settings after the configuration.

Door No.

Select the device corresponded door No.

Name

You can create a name for the door.

Open Duration

Set the door unlocking duration. If the door is not opened for the set time, the door will be locked.

Exit Button Type

You can set the exit button as **Remain Open** or **Remain Closed** according to your actual needs. By default, it is **Remain Open**.

Door Remain Open Duration with First Person

Set the door open duration when first person is in. After the first person is authorized, it allows multiple persons access the door or other authentication actions.

Set Authentication Parameters

Set Authentication Parameters.

Steps

1. Tap **Configuration → Access Control → Authentication Settings** .

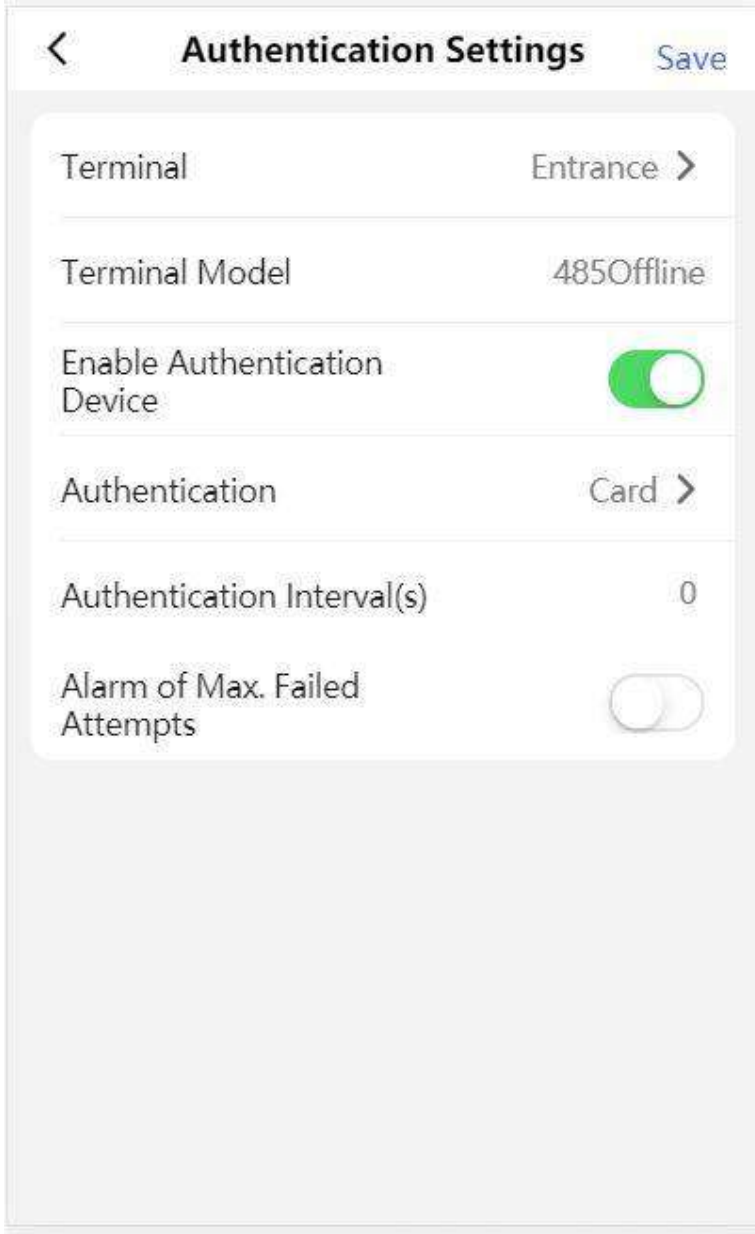


Figure 7-12 Authentication Settings

2. Tap **Save**.

Terminal

Choose **Entrance** or **Exit** for settings.

Terminal Model

Terminal model is read-only.

Enable Authentication Device

Enable the authentication function.

Authentication

Authentication via card by default.

Authentication Interval

You can set the authentication interval of the same person when authenticating. The same person can only authenticate once in the configured interval. A second authentication will be failed.

Alarm of Max. Failed Attempts

Enable to report alarm when the card reading attempts reach the set value.

Set Card Security

Tap **Configuration → Access Control → Card Security** to enter the settings page.

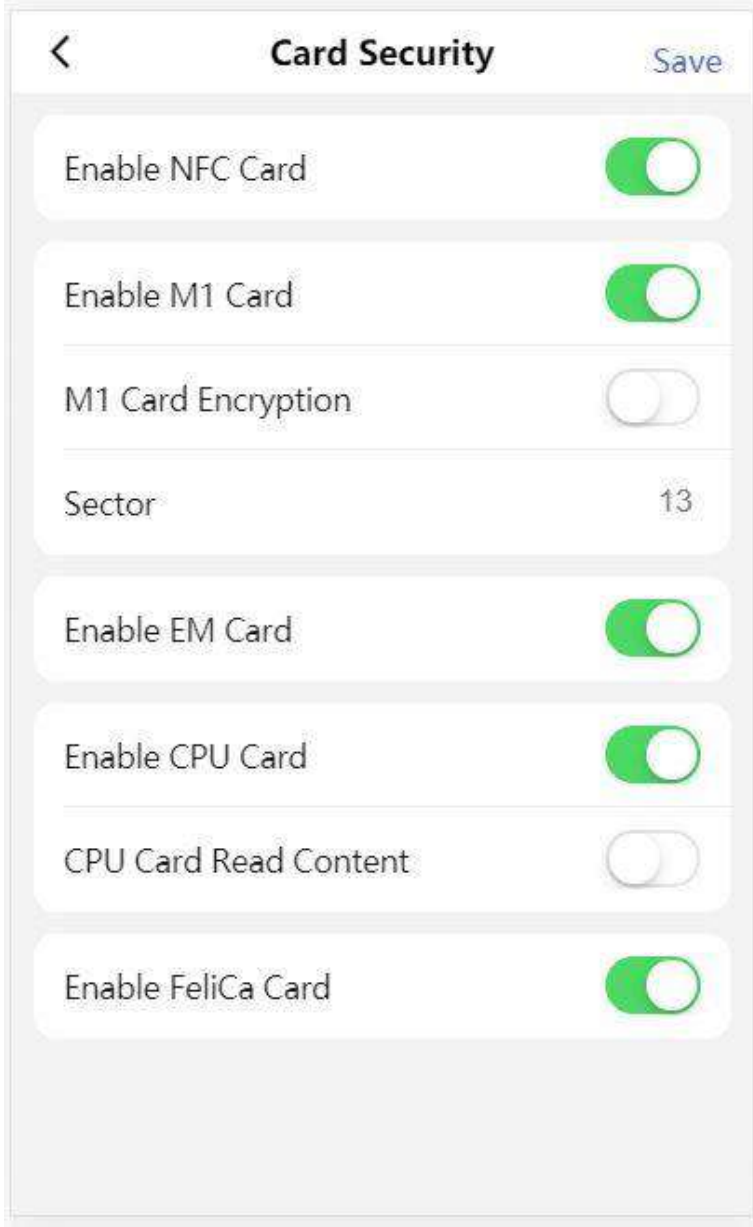


Figure 7-13 Card Security

Set the parameters and click **Save**.

Enable NFC Card

In order to prevent the mobile phone from getting the data of the access control, you can disable NFC card to increase the security level of the data.

Enable M1 Card

Enable M1 card and authenticating by presenting M1 card is available.

M1 Card Encryption

M1 card encryption can improve the security level of authentication.

Sector

Enable the function and set the encryption sector. By default, Sector 13 is encrypted. It is recommended to encrypt sector 13.

Enable EM Card

Enable EM card and authenticating by presenting EM card is available.

Note

If the peripheral card reader supports presenting EM card, the function is also supported to enable/disable the EM card function.

Enable CPU Card

The device can read the data from CPU card when enabling the CPU card function.

CPU Card Read Content

After enable the CPU card content reading function, the device can read the CPU card content.

Enable FeliCa Card

The device can read the data from FeliCa card when enabling the FeliCa card function.

Terminal Settings

Set the working mode.

Tap **Configuration → Access Control → Terminal Parameters** to enter the settings page.

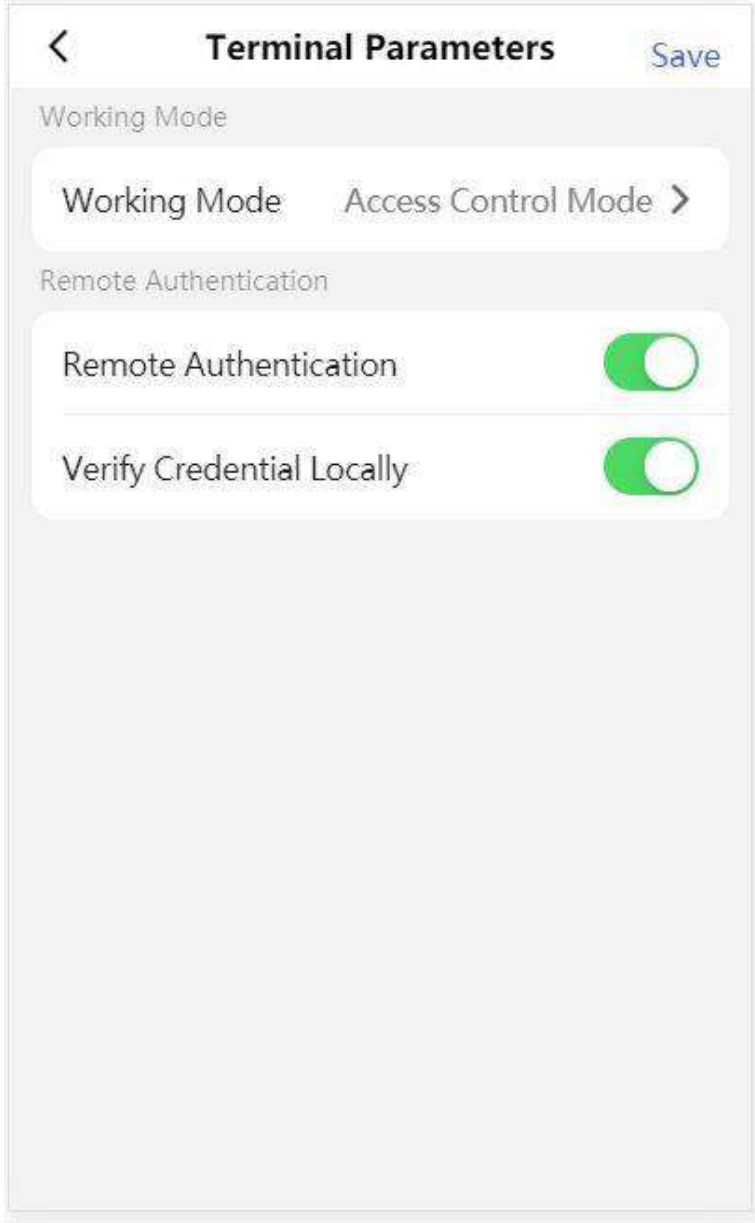


Figure 7-14 Terminal Parameters

Permission Free Mode

The device will not verify the person's permission, but only the person's validity period. If the person is in the validity period, the barrier will open.

You can enable **Verify Credential Locally**. After enabling the function, the device will only verify the person's permission without the schedule template, etc.

Access Control Mode

The device works normally and will verify the person's permission to open the barrier.

Remote Authentication

The device will upload the person's authentication information to the platform. The platform will judge to open the barrier or not.

Verify Credential Locally

The device will only verify the person's permission without the schedule template, etc.

7.3.8 View Device Information

View the device name, language, model, serial No., version, etc.

Tap **Configuration → System Information** to enter the configuration page.

You can view the language, model, serial No., version, IO input and output number, local RS-485 number, MAC address and open source license.

You can change the device name. Tap **Save**.

7.3.9 Device Capacity

Tap **Configuration → Device Capacity** to enter the page.

You can view the quantity of user, card and event.

7.3.10 Log Export

Tap **Configuration → Log Export** to enter the page.

Select a log type and tap **Export**.

7.3.11 Restore and Reboot

Reboot device and restore device parameters.

Restore

Tap **Configuration → Restore** .
All parameters will be restored to the factory settings.

Restart Devices

Tap **Configuration → Restart Devices** .
Tap **Reboot** to reboot the device.

Chapter 8 Client Software Configuration

You can call the hotline to get the iVMS-4200 client software installation package.

8.1 Configuration Flow of Client Software

Follow the flow diagram below to configure on the client software.

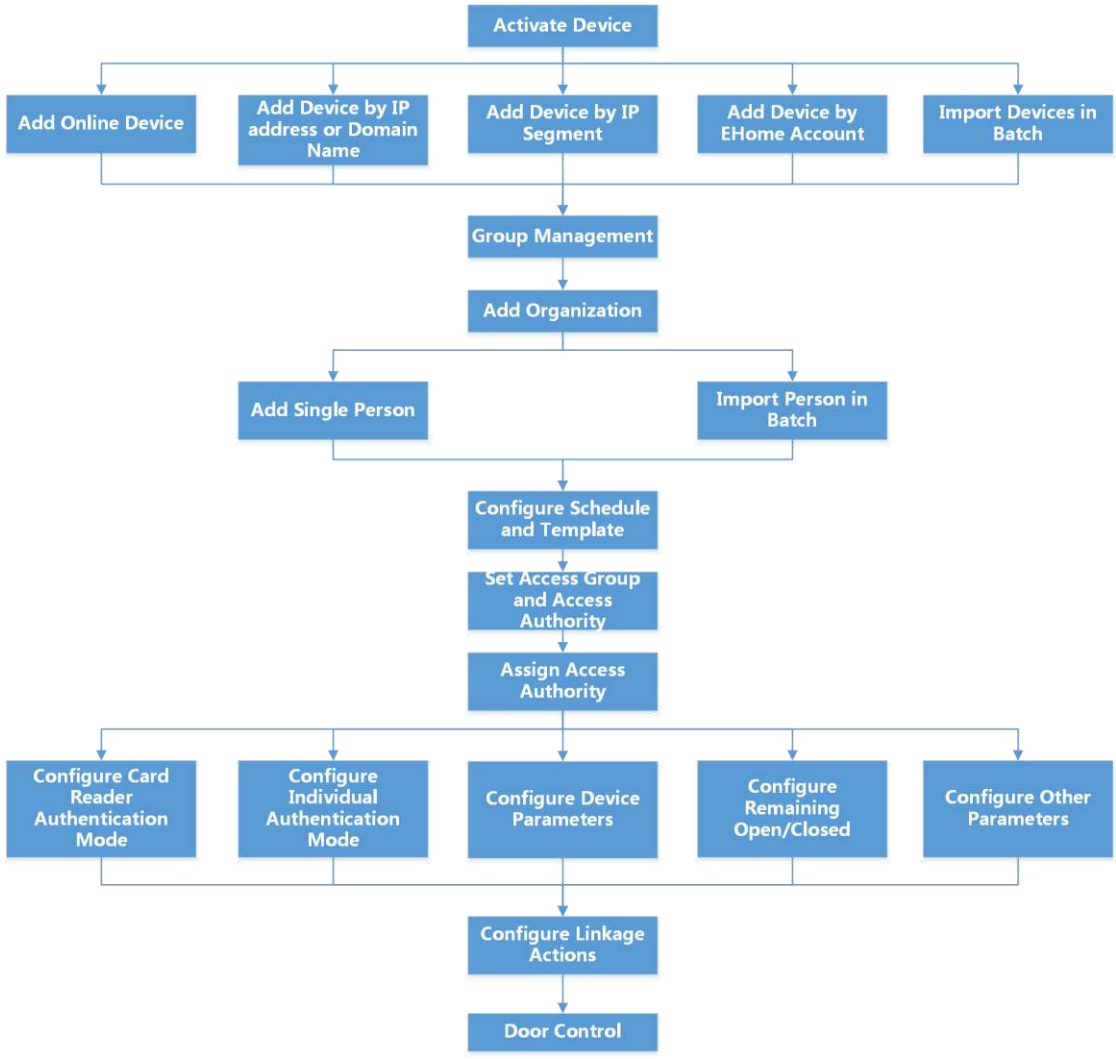


Figure 8-1 Flow Diagram of Configuration on Client Software

8.2 Device Management

The client supports managing access control devices and video intercom devices.

Example
You can control entrance & exit and manage attendance after adding access control devices to the client; you can perform video intercom with the indoor stations and door stations.

8.2.1 Add Device

The client provides three device adding modes including by IP/domain, IP segment, and ISUP protocol. The client also supports importing multiple devices in a batch when there are large amount of devices to be added.

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.
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:** 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 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 access control device, its access points, alarm inputs/outputs, and encoding channels (if exist) will be imported to this group.
8. 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.

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.
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.

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.

6. Click ··· and select the template file.

7. Click **Add** to import the devices.

8.2.2 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 **Online Device** to show the online device area.

All the online devices sharing the same subnet will be displayed in the list.

3. Select the device from the list and click on the Operation column.
4. Reset the device password.
   - 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.

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.

8.2.3 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 8-1 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	Click to set remote configuration of the corresponding device. For details, refer to the user manual of device.
View Device Status	Click to view device status, including door No., door status, etc. **Note** For different devices, you will view different information about device status.

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.

8.3 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 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 control door status, and do some other operations of the devices after managing the resources by groups.

8.3.1 Add Group

You can add group to organize the added device for convenient management.

Steps
1. Enter the Device Management module.
2. Click **Device Management → Group** to enter the group management page.
3. Create a group.
   - Click **Add Group** and enter a group name as you want.
   - Click **Create Group by Device Name** and select an added device to create a new group by the name of the selected device.

Note
The resources (such as alarm inputs/outputs, access points, etc.) of this device will be imported to the group by default.

8.3.2 Import Resources to Group

You can import the device resources (such as alarm inputs/outputs, access points, etc.) to the added group in a batch.

Before You Start
Add a group for managing devices. Refer to ***Add Group*** .

Steps
1. Enter the Device Management module.

2. Click **Device Management → Group** to enter the group management page.
3. Select a group from the group list and select the resource type as **Access Point**, **Alarm Input**, **Alarm Output**, etc.
4. Click **Import**.
5. Select the thumbnails/names of the resources in the thumbnail/list view.

Note

You can click or to switch the resource display mode to thumbnail view or to list view.

6. Click **Import** to import the selected resources to the group.

8.4 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.

8.4.1 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 surbodinate 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.

8.4.2 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.

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.

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.

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 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.

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 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).

8.4.3 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.

8.4.4 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 .
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).

8.4.5 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.

8.4.6 Set Card Issuing Parameters

The client provides two modes for reading a card's number: via card enrollment station or via the card reader of the access control device. If a card enrollment station is available, connect it to the PC running the client by USB interface or COM, and place the card on the card enrollment to read the card number. If not, you can also swipe the card on the card reader of the added access control device to get the card number. As a result, before issuing a card to one person, you need to set the card issuing parameters including the issuing mode and related parameters.

When adding a card to one person, click **Settings** to open the Card Issuing Settings window.

Local Mode: Issue Card by Card Enrollment Station

Connect a card enrollment station to the PC running the client. You can place the card on the card enrollment station to get the card number.

Card Enrollment Station

Select the model of the connected card enrollment station

Note

Currently, the supported card enrollment station models include DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E, and DS-K1F180-D8E.

Card Type

This field is only available when the model is DS-K1F100-D8E or DS-K1F180-D8E.

Select the card type as EM card or IC card according to the actual card type.

Serial Port

It is only available when the model is DS-K1F100-M.

Select the COM the card enrollment station connects to.

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

This field is only available when the model is DS-K1F100-D8, DS-K1F100-D8E, or DS-K1F180-D8E.

If the card is M1 card, and if you need to enable the M1 Card Encryption function, you should enable this function and select the sector of the card to encrypt.

Remote Mode: Issue Card by Card Reader

Select an access control device added in the client and swipe the card on its card reader to read the card number.

8.5 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*** .

8.5.1 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**.

8.5.2 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.

8.6 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.

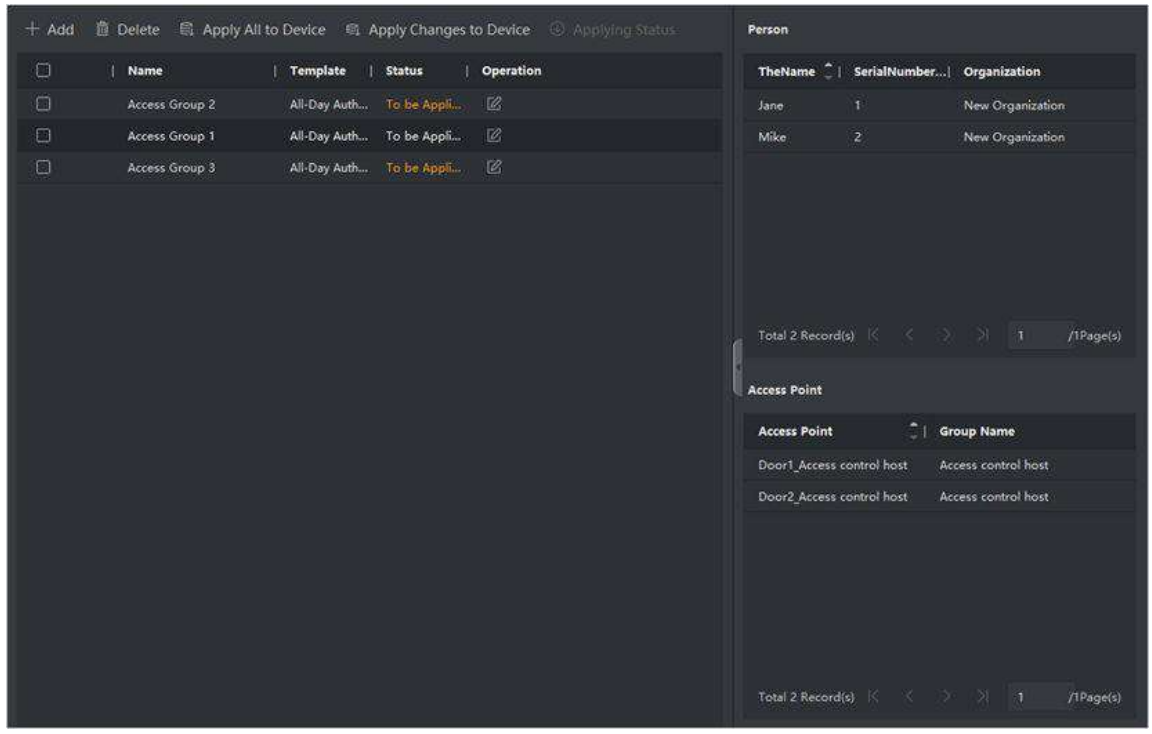


Figure 8-2 Display the Selected Person(s) and Access Point(s)

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**.

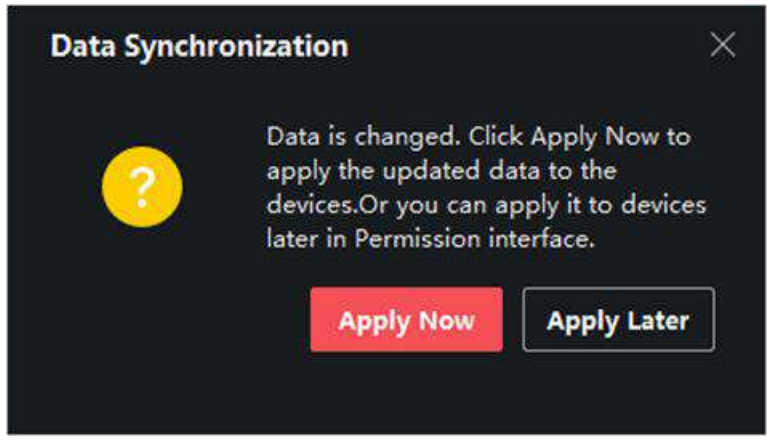


Figure 8-3 Data Synchronization

8.7 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.

8.7.1 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 accesss 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 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**.

8.7.2 Configure Other Parameters

After adding the access control device, you can set its parameters such as network parameters, capture parameters, RS-485 parameters, Wiegand parameters, etc.

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**.

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.

Note

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.

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.

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.

8.8 Door/Elevator Control

In Monitoring module, you can view the real-time status of the doors or elevators managed by the added access control device. You can also control the doors and elevators such as open/close the door, or remain the door open/closed via the client remotely. The real-time access event are displayed in this module. You can view the access details and person details.

Note

For the user with door/elevator control permission, the user can enter the Monitoring module and control the door/elevator. Or the icons used for control will not show. For setting the user permission, refer to .

8.8.1 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 .

Steps

1. Click **Monitoring** to enter the status monitoring page.
2. Select an access point group on the upper-right corner.

   Note

   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.

   Note

   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 .

Result

The icon of the doors will change in real-time according to the operation if the operation is succeeded.

8.8.2 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 8-4 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.

Appendix A. DIP Switch

A.1 DIP Switch Description

The DIP switch is on the access control board. No.1 and No 2 is from the low bit to the high bit.

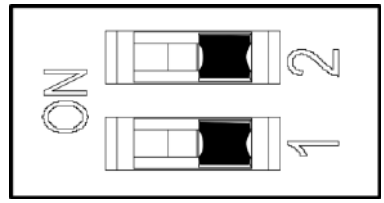


Figure A-1 DIP Switch

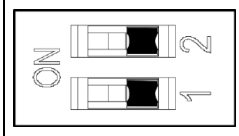
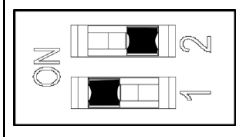
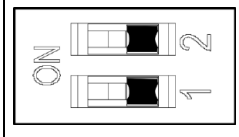
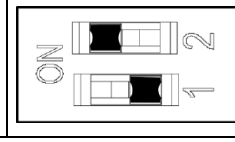
When the switch is towards ON, it means the switch is enabled, otherwise, the switch is off.

A.2 DIP Switch Corresponded Functions

Note

After setting the DIP switch, you should reboot the device, or the function cannot take effect.

The 2-bit DIP switch corresponded functions on the access control board are as follows:

Bit	Device Mode	Function	Decimal Value	DIP Switch Address Diagram
1	Work Mode	Normal Mode	0	
		Study Mode	1	
2	Keyfob Paring Mode	Disable Keyfob Paring Mode	0	
		Enable Keyfob Paring Mode	1	

Appendix B. Button Configuration Description

Refer to the table below for device configuration via button on the main lane control board.

Level-1 Configuration No.	Description	Level-1 Configuration No. and Functions	Notes
1	Study Mode	1-Exit Study Mode/ Normal Mode 2-Study Mode **Note** By default, 1 will be displayed on the display screen.	If the device is equipped with access control board, you can only set via DIP switch.
2	keyfob Pairing Mode	1-Normal Mode 2-Pairing Mode **Note** By default, 1 will be displayed on the display screen.	If the device is equipped with access control board, you can only set via DIP switch.
3	Passing Mode	1-Both sides under control **Note** By default, 1 will be displayed on the display screen. 2-Entrance under control; exit prohibited 3-Entrance under control; exit on inductive mode 4-Both sides on inductive mode	

Level-1 Configuration No.	Description	Level-1 Configuration No. and Functions	Notes
		5-Entrance on inductive mode; exit under control 6-Entrance on inductive mode; exit prohibited 7-Both sides prohibited 8-Entrance prohibited; exit under control 9-Entrance prohibited; exit on inductive mode 10-Entrance under control; exit remaining open 11-Entrance under control; exit on free mode 12-Entrance on inductive mode; exit remaining open 13-Entrance on inductive mode; exit on free mode 14-Entrance prohibited; exit remaining open 15-Entrance prohibited; exit on free mode 16-Entrance remaining open; exit under control 17-Entrance remaining open; exit on inductive mode	

Level-1 Configuration No.	Description	Level-1 Configuration No. and Functions	Notes
		18- Entrance remaining open; exit remaining open 19- Entrance remaining open; exit on free mode 20- Entrance remaining open; exit prohibited 21- Entrance on free mode; exit under control 22- Entrance on free mode; exit on inductive mode 23- Entrance on free mode; exit remaining open 24- Entrance on free mode; exit on free mode 25- Entrance on free mode; exit prohibited	
4	Memory Mode	1-Disable 2-Enable **Note** By default, 2 will be displayed on the display screen.	
5	keyfob Remote Control	1-one to one 2-one to multiple **Note** By default, 1 will be displayed on the display screen.	

Level-1 Configuration No.	Description	Level-1 Configuration No. and Functions	Notes
6	Barrier Opening Speed	1-1, 2-2, …10-10 **Note** By default, 5 will be displayed on the display screen.	
7	Barrier Closing Speed	1-1, 2-2, …10-10 **Note** By default, 5 will be displayed on the display screen.	
8	Card Reading on the Alarm Area	1-Do not open 2-Open **Note** By default, 2 will be displayed on the display screen.	
9	Enter Duration	5-5s, 6-6s, 7-7s, …, 60-60s **Note** By default, 5 will be displayed on the display screen.	
10	Exit Duration	5-5s, 6-6s, 7-7s, …, 60-60s **Note** By default, 5 will be displayed on the display screen.	
11	IR Sensing Duration	0-0s, 1-1s, 2-2s,..., 25-25s	

Level-1 Configuration No.	Description	Level-1 Configuration No. and Functions	Notes
		Note By default, 0 will be displayed on the display screen.	
12	Intrusion Duration	0-0s, 1-1s, 2-2s,..., 20-20s **Note** By default, 0 will be displayed on the display screen.	
13	Overstay Duration	0-0s, 1-1s, 2-2s,..., 20-20s **Note** By default, 0 will be displayed on the display screen.	
14	Delay Time for Barrier Closing	0-0s, 1-1s, 2-2s, 3-3s, 4-4s, 5-5s **Note** By default, 0 will be displayed on the display screen.	
15	Control Mode	1-Button Configuration 2-DIP Switch on Access Control Board **Note** By default, 1 will be displayed on the display screen.	
18	Lane Number	1-Dual Lanes	Unable to change

Level-1 Configuration No.	Description	Level-1 Configuration No. and Functions	Notes
		2-Single Lane **Note** By default, 1 will be displayed on the display screen.	
19	Motor Rotation	1-Clockwise 2-Anticlockwise **Note** By default, 1 will be displayed on the display screen.	Unable to change
21	Volume	1-0, 2-1, 3-2, 4-3, 5-4 **Note** By default, 2 will be displayed on the display screen.	The device will be muted when set to "1".
22	Authenticated Passing	1-Disable 2-Enable **Note** By default, 1 will be displayed on the display screen.	Unable to change via button
23	Invalid Card No.	1-Disable 2-Enable **Note** By default, 1 will be displayed on the display screen.	Unable to change via button

Level-1 Configuration No.	Description	Level-1 Configuration No. and Functions	Notes
24	Fingerprint Unmatched	1-Disable 2-Enable **Note** By default, 1 will be displayed on the display screen.	Unable to change via button
25	Climbing over Barrier	1-Disable 2-Enable **Note** By default, 1 will be displayed on the display screen.	
26	Reverse Passing	1-Disable 2-Enable **Note** By default, 1 will be displayed on the display screen.	
27	Exceeding Passing Duration	1-Disable 2-Enable **Note** By default, 1 will be displayed on the display screen.	
28	Intrusion Alarm	1-Disable 2-Enable **Note** By default, 1 will be displayed on the display screen.	

Level-1 Configuration No.	Description	Level-1 Configuration No. and Functions	Notes
29	Forced Passing	1-Disable 2-Enable **Note** By default, 1 will be displayed on the display screen.	Unable to change via button
30	Tailgating Alarm	1-Disable 2-Enable **Note** By default, 1 will be displayed on the display screen.	
31	Unauthorized Passing	1-Disable 2-Enable **Note** By default, 1 will be displayed on the display screen.	Unable to change via button
32	Exceeding Authentication Duration	1-Disable 2-Enable **Note** By default, 1 will be displayed on the display screen.	Unable to change via button
33	Failed Authentication	1-Disable 2-Enable **Note** By default, 1 will be displayed on the display screen.	Unable to change via button

Level-1 Configuration No.	Description	Level-1 Configuration No. and Functions	Notes
34	Expired Credential	1-Disable 2-Enable **Note** By default, 1 will be displayed on the display screen.	Unable to change via button
35	Overstaying Alarm	1-Disable 2-Enable **Note** By default, 1 will be displayed on the display screen.	
36	Barrier Material	1-Acrylic 2-Stainless Steel 3-Glass	
37	Barrier Length	1-550 2-600 3-650 4-700 5-750 6-800 7-850 8-900 9-950 10-1000 11-1100 12-1200 13-1300 14-1400	

Level-1 Configuration No.	Description	Level-1 Configuration No. and Functions	Notes
		Note By default, 8 will be displayed on the display screen.	
38	Motor Inspection	1-Disable 2-Enable on Main Lane 3-Enable on Sub Lane **Note** By default, 1 will be displayed on the display screen.	
39	Brightness of Light	0-0, 1-1, 2-2, … , 10-10 **Note** By default, 3 will be displayed on the display screen.	The higher the value is, the brighter the light will be.
40	Self-check Voice Prompt	1-Disable 2-Enable **Note** By default, 2 will be displayed on the display screen.	
41	Study Mode Voice Prompt	1-Disable 2-Enable **Note** By default, 2 will be displayed on the display screen.	

Level-1 Configuration No.	Description	Level-1 Configuration No. and Functions	Notes
42	c	4-4, 6-6, 8-8, **Note** By default, 4 will be displayed on the display screen.	Unable to change via button
43	Application Mode	1-Wind-proof 2-Indoor By default, 1 will be displayed on the display screen.	
44	Barrier Recover Duration	1-Normal Speed 2-Fast Recover By default, 1 will be displayed on the display screen.	
45	Brake	1-Disable 2-Barrier Position Exception 3-Intrusion By default, 2 will be displayed on the display screen.	
46	Brake Angle	1-5° 2-10° 3-15° By default, 1 will be displayed on the display screen.	
47	IR Sensing	1-Single Triggered 2-Triggered Simultaneously	

Level-1 Configuration No.	Description	Level-1 Configuration No. and Functions	Notes
		By default, 1 will be displayed on the display screen.	
48	Fan	1-Disabled 2-Enabled By default, 2 will be displayed on the display screen.	
49	Barrier Height	1-700 2-1200 3-1400 4-1600 5-1800 By default, 5 will be displayed on the display screen.	
99	Restore to Default	1- Default 2- Start **Note** By default, 1 will be displayed on the display screen.	

Appendix C. Event and Alarm Type

Event	Alarm Type
Tailgating	Visual and Audible
Reverse Passing	Visual and Audible
Force Accessing	None
Climb over Barrier	Visual and Audible
Overstay	Visual and Audible
Passing Timeout	None
Intrusion	Visual and Audible
Free Passing Authentication Failed	Visual and Audible
Barrier Obstructed	None

Appendix D. Table of Audio Index Related Content

Note

- If the device is not equipped with access control board, the loudspeaker shall be connected to the main extended interface board.
- If the device is equipped with access control board, the loudspeaker shall be connected to the access control board. You can set custom broadcasting context via web.

Content
Climbing over the barrier.
Reverse passing.
Passing timeout.
Intrusion.
Tailgating.
Overstay.

Appendix E. Error Code Description

The swing barrier will display the error code on the seven-segment display if error occurred. Refer to the table below to find the description of each number.

Error Reason	Code	Error Reason	Code
The First IR Beam Triggered	01	The Thirteenth IR Beam Triggered	13
The Second IR Beam Triggered	02	The Fourteenth IR Beam Triggered	14
The Third IR Beam Triggered	03	Authentication Indicator Board (Entrance) Offline	49
The Fourth IR Beam Triggered	04	Authentication Indicator Board (Exit) Offline	50
The Fifth IR Beam Triggered	05	IR Adapter Board Offline	51
The Sixth IR Beam Triggered	06	Interconnecting Exception	53
The Seventh IR Beam Triggered	07	Not Studying	54
The Eighth IR Beam Triggered	08	Obstruction	55
The Ninth IR Beam Triggered	09	Exceeding Studying Range	56
The Tenth IR Beam Triggered	10	Encoder Exception	57
The Eleventh IR Beam Triggered	11	Motor Exception	58
The Twelfth IR Beam Triggered	12	Extended Interface Board Offline (If the board is not installed, the error code of "49" will appear but the device functions normally)	59

Appendix F. Communication Matrix and Device Command

Communication Matrix

Scan the following QR code to get the device communication matrix.
Note that the matrix contains all communication ports of Hikvision access control and video intercom devices.

Figure F-1 QR Code of Communication Matrix

Device Command

Scan the following QR code to get the device common serial port commands.
Note that the command list contains all commonly used serial ports commands for all Hikvision access control and video intercom devices.

Figure F-2 Device Command


See Far, Go Further

HikCentral Profissional V2.6.1

HikCentral Professional é uma plataforma de software fornecida pela Hikvision para integrar e gerenciar sistemas de segurança. Essa plataforma foi projetada para atender a diversos desafios de segurança em uma única plataforma. Com o HikCentral Professional, você pode gerenciar múltiplos sistemas individuais com facilidade, como segurança de vídeo, controle de acesso, alarmes de segurança e muito mais, além de explorar funcionalidades entre sistemas.
As operações diárias tornam-se mais eficientes enquanto a proteção de pessoas e propriedades melhora em geral. Usuários de todos os tipos estão tomando decisões mais inteligentes.

Característica principal

Leve e Eficiente

- Leve características arquitetônicas reduzem o consumo de recursos do sistema
- Capaz de gerenciar vários sistemas de diferentes tamanhos com eficiência consistente

Unificado e Flexível

- Suporta a combinação de vários plug-ins de aplicativos em um único ambiente, arquitetura sob demanda para colaboração entre segmentos de negócios
- Novos plug-ins podem ser desenvolvidos continuamente para atender às novas necessidades de negócios

Integrado e Aberto

- Compatível com praticamente todos os produtos de Hikvision e sua abundância de aplicações, incluindo aquelas baseadas em aprendizagem profunda análises e estatísticas
- Abrir a arquitetura permite fácil integração com sistemas e hardware de terceiros

• Características dos Módulos Principais

Módulo	Características
Vídeo	● Segurança de vídeo eficiente e abrangente ● Pesquisa rápida de incidentes e localização , pesquisa conveniente de eventos e rápida execução de vídeo ● Exportação de vídeo como evidência ● Adaptabilidade de rede de baixa largura de banda ● Armazenamento confiável e flexível
Controle de Acesso	● Métodos de gerenciamento de acesso abrangentes e flexíveis ● Estratégias avançadas de acesso para áreas sensíveis ● Design e impressão convenientes de crachás para funcionários ● Orientação clara passo a passo ● Registro de pessoal remoto ● Bloquear ou destrancar portas automaticamente ● Mantenha as portas em um estado destrancado durante uma emergência ● Conte e verifique facilmente a segurança de todos ● Abrindo a porta via Bluetooth e NFC
Visitante	● Gestão digitalizada de visitantes ● Registro de visitantes com antecedência ● Permissões de acesso predefinidas e registros rastreáveis ● Uma função de lista de observação juntamente com design personalizado e impressão de crachás
Veículo	● Gestão de entradas e saídas flexível e eficiente ● Melhor experiência de estacionamento para motoristas ● Consulta de estacionamento self-service ● Faturamento flexível ● Relatórios de análise de transações e análise de operações de estacionamento intuitivos e eficientes
Monitoramento a Bordo	● Monitoramento eficiente de veículos para resposta rápida ● Gestão de arquivo confiável ● Relatórios personalizados para maior eficiência operacional
Detecção de Alarme	● Gerencie centralmente várias fontes de alarme ● Exibição em tempo real de todos os tipos de alarmes ● Ligação flexível ● Alarmes de áudio automáticos
Análise Inteligente	● O painel de análise inteligente baseado em vídeo permite aplicações digitais flexíveis e extensíveis ● Análises comerciais inteligentes
Exibição Comercial	● Gerencie e configure conteúdo para sinalização digital de forma intuitiva ● Modelos de programas pré-instalados ● Todos os programas são criados visualmente
Tempo e Presença	● Definição de regras de frequência flexíveis ● Relatórios de presença diversos e modelos personalizáveis ● Fácil integração com sistemas de folha de pagamento de terceiros ● Oferece suporte aos funcionários na busca de resultados de frequência e no envio de solicitações de correção
Aplicação Portátil	● Recuperação rápida de gravações importantes, backups de longo prazo e gerenciamento de permissões em nível de arquivo ● Detecção e adição automática de dispositivos portáteis por meio de estações de acoplamento e registros estatísticos detalhados para uso de pessoal e equipamento
Parede Inteligente	● Exibir vídeos na parede ● Troca automática de vídeo e reprodução programada ● Pop-up de alarme na parede inteligente. O vídeo do alarme será reproduzido

	automaticamente em uma janela pop-up na parede de vídeo para notificar o operador
Gestão de Estacionamento	● Gestão eficiente de entradas e saídas com regras de acesso para veículos, integração com câmeras ANPR e autenticação de veículos sem toque e sem paradas para ajudar a reduzir o congestionamento no horário de pico ● Experiência de estacionamento aprimorada com telas de orientação e displays para encontrar vagas ● Opções de cobrança flexíveis, incluindo cobrança manual e pré-pagamento
Gestão de Evidências	● Coleta conveniente de informações com vários clientes (cliente móvel, cliente da Web, cliente de controle) para upload de arquivos ● Gerenciamento unificado de arquivos de evidências entre serviços, incluindo vídeos, fotos, áudios e upload de documentos na operação diária ● Backup de longo prazo, recuperação eficiente: classificação de evidências, arquivamento, recuperação, exportação, gerenciamento centralizado
Realidade Aumentada	● Acesse facilmente as câmeras principais sem perder a visão global ● Localização rápida de recursos por meio de ações simples de "Clique" e "Filtrar" ● Processo eficiente para tratamento rápido de eventos, desde a notificação até o reconhecimento
Gestão de Patrulha	● Crie cronogramas e rotas de patrulha sem esforço usando uma interface de e-map intuitiva ● A equipe de segurança faz o check-in usando dispositivos de controle de acesso com todos os dados carregados automaticamente no software ● Reportar anomalias durante a patrulha ao centro através do Cliente Móvel ● Dispara alarmes instantaneamente se indivíduos não autorizados tentarem realizar patrulhas ● Relatórios de patrulha abrangentes permitem que os gerentes avaliem o desempenho de forma eficaz
Inspeção de Segurança	● Identificar uma ampla gama de itens proibidos de forma oportuna e precisa, reduzindo custos de mão de obra e ameaças à segurança ● Simplifique o gerenciamento centralizado com resultados de detecção em tempo real, informações de alarme e visualização ao vivo
Reunião de Emergência	● Resposta instantânea a emergências com um clique para acionar a emergência automaticamente ou manualmente ● Experiência de evacuação aprimorada com transmissão cíclica de mensagens de evacuação por meio de alto-falantes IP e portas restantes abertas ao longo da rota de fuga para rápida reunião em pontos de encontro ● Confirmação eficiente do status de segurança do pessoal nos pontos de reunião, incluindo contagem e verificação da presença de todos e verificação dos locais mais recentes de indivíduos desaparecidos
Gestão Remota de Sites	● Gerencie sistemas de vários sites em um só lugar, fornecendo uma visão unificada de diferentes recursos e todos os eventos e alarmes relacionados entre os sites. ● Soluções multisite em termos de número de dispositivos, sites remotos e eventos simultâneos a serem manipulados pelo sistema
Manutenção	● Topologia de rede e dispositivo visualizada e notificações de alarme ● Os logs estão disponíveis para rastreamento de eventos e evidências ● Verifique todos os estados de saúde com um clique ou de acordo com uma programação predefinida ● Veja claramente os riscos e exceções
Rastreamento de Pacotes	● Identificação e Rastreamento Fáceis de Pacotes ao vincular os dados dos sistemas de código de barras e dos sistemas de vídeo ● Rastrear através de sistemas de correias transportadoras com leitor de código inteligente e câmeras convencionais ● Gerenciamento de evidências de vídeo: suporte à exportação de registros de vídeo

	(MP4/AVI), suporte à exportação de registros de digitalização por ponto de verificação/ID de pacote/carimbo de data/hora)
Gestão de Docas	● Análise em tempo real da taxa de carga e descarga, localização e reprodução rápida dos processos ● Processo de despacho de veículos: reserva de doca, ANPR, tela de LED exibindo informações de fila, alto-falante para transmissão de áudio ● Exibição em tempo real e visualizada do status da doca no Mapa da Doca ● Estatísticas de tempo de operação do veículo, tempo de espera, etc. pelo painel
Consumo de Cantina	● Pagamento sem contato, melhore a eficiência e aprimore a experiência ● Modo de consumo diversificado aplicável a diferentes cenários ● Gestão unificada permite alta eficiência na gestão de grandes cantinas de plantas
Inspeção Inteligente	● Inspeção de vídeo programada ou aleatória sobre operação e produção para encontrar e corrigir problemas a tempo , garantindo a segurança da produção ● Vários métodos de inspeção disponíveis sob demanda: inspeção no local, inspeção programada e revisão de eventos ● Modelos de inspeção unificados para formular e gerenciar SOP, melhorando a eficiência da inspeção

Especificação de Software

A tabela seguinte mostra o desempenho máximo do Servidor de Gestão de Sistema (SYS, System Management Server). Para outros dados detalhados e desempenho, consulte *Requisitos e Desempenho de Software*.

<table>
<tr><th colspan="2">Características</th><th>Desempenho Máximo</th></tr>
<tr><td colspan="3">Em geral</td></tr>
<tr><td rowspan="30">Recurso Gerenciável</td><td>Dispositivos de Codificação</td><td rowspan="30">5.000
Nota:
Para alguns tipos de dispositivos, não mais do que 5.000 são suportados . Até 2.048 dispositivos de codificação adicionados pelo protocolo ONVIF, 30 radares de segurança, 32 terminais de visitantes, 2.048 dispositivos de alarme (painéis de controle de segurança e dispositivos de alarme de pânico), 1.000 estações de encaixe, 128 dispositivos de transmissão de rede, 40 entradas e saídas , 2.048 terminais de orientação, 4 UVSSs, 2.048 dispositivos de exibição comercial (incluindo sinalizações digitais, painéis planos interativos e controladores de LED), 128 alto-falantes IP , 2.048 dispositivos de proteção contra incêndio, 1.000 dispositivos de digitalização, 256 scanners de código portáteis e 100 terminais de pagamento são permitidos.</td></tr>
<tr><td>Dispositivos de Codificação que Suportam o Protocolo ONVIF</td></tr>
<tr><td>Dispositivos de Controle de Acesso</td></tr>
<tr><td>Dispositivos de Controle de Elevador</td></tr>
<tr><td>Dispositivos de Intercomunicação de Vídeo</td></tr>
<tr><td>Terminais de Visitantes</td></tr>
<tr><td>Painéis de Controle de Segurança e Dispositivos de Alarme de Pânico</td></tr>
<tr><td>Alto-falantes IP</td></tr>
<tr><td>Terminais de Consulta</td></tr>
<tr><td>Terminais de Orientação</td></tr>
<tr><td>Telas de Estacionamento</td></tr>
<tr><td>Estações de Entrada/Saída</td></tr>
<tr><td>Dispositivos de Bordo</td></tr>
<tr><td>Dispositivos de Inspeção de Segurança</td></tr>
<tr><td>UVSSs</td></tr>
<tr><td>Câmeras Corporais</td></tr>
<tr><td>Estações de Atracação</td></tr>
<tr><td>Dispositivos de Transmissão de Rede</td></tr>
<tr><td>Terminais de Sinalização Digital</td></tr>
<tr><td>Painéis Planos Interativos</td></tr>
<tr><td>Dispositivos de Proteção Contra Incêndio</td></tr>
<tr><td>Dispositivos de Decodificação</td></tr>
<tr><td>Dispositivos BACnet</td></tr>
<tr><td>Dispositivos Modbus</td></tr>
<tr><td>Terminais de Pagamento</td></tr>
<tr><td>Scanners de Código Portáteis</td></tr>
<tr><td>Dispositivos de Digitalização (incluindo leitores de código inteligente Hikvision , leitores de código de barras Hikvision e dispositivos de digitalização de terceiros)</td></tr>
<tr><td>Servidor de Análise Inteligentes</td><td>64</td></tr>
<tr><td>Servidores de Gravação</td><td>64</td></tr>
<tr><td>Servidores de Streaming</td><td>64</td></tr>
<tr><td>Câmeras</td><td>Sistema Central: 10.000
Com RSM: 1 0 0 ,000</td></tr>
<tr><td>Entradas de Alarme (excluindo painéis de controle de segurança e dispositivos de alarme de pânico)</td><td>5.000</td></tr>
<tr><td>Entradas de alarme de dispositivos de controle de segurança</td><td>10.000</td></tr>
<tr><td>Partições de Controle de Segurança (áreas)</td><td>2.048</td></tr>
<tr><td>Saídas de Alarme</td><td>3.000</td></tr>
<tr><td>Câmeras PTZ de Radar</td><td>3 0</td></tr>
<tr><td>Terminais de Reconhecimento Facial da Série DS-5600 Quando Aplicados com Catracas Hikvision</td><td>32</td></tr>
<tr><td>Câmeras ANPR</td><td>3.000</td></tr>
<tr><td>Câmeras de Contagem de Pessoas</td><td>Recomendado: 3.000</td></tr>
<tr><td>Câmeras de Mapa de Calor</td><td>Recomendado: 1.024</td></tr>
</table>

	Câmeras de Gerenciamento de Filas	Recomendado: 3.000
	Câmeras Térmicas	Recomendado: 20 ①
	Câmeras por Área	256
	Entradas de Alarme por Área	256
	Saídas de Alarme por Área	256
Evento	Eventos	10.000
	Recepção de Eventos Sem Fotos	● Valor Médio: 100/s ● Valor de Pico: 1.000/s (Este valor não dura mais que 10 minutos.)
	Recepção de Eventos com Imagems	● Quando as imagens são transmitidas diretamente de dispositivos para servidores de gravação ou NVRs: ◆ Valor médio: 100/s ◆ Valor de pico: 1.000/s (Este valor não dura mais que 10 minutos.) ● Quando os dispositivos enviam imagens para o SYS e o SYS as transmite para os Servidores de Gravação: ◆ Valor de pico: 100/s (Este valor não dura mais que 10 minutos.) ● Quando os dispositivos enviam imagens para o SYS para armazenamento: ◆ Valor de pico: 20/s (Este valor não dura mais que 10 minutos.)
	Eventos Enviados aos Clientes	100 clientes * 100 eventos/s
	Alarme Combinado	10/s
	Eventos Definidos pelo Usuário	10.000
Usuário e Função	Total de Usuários e Pessoas On-line **As pessoas referem-se aos funcionários que têm permissão para efetuar login no Self-Service, pesquisar resultados de frequência, fazer check- in e check-out pelo Mobile Client e abrir portas via bluetooth .*	5.000
	Usuários	10.000
	Funções	3.000
Pessoa	Pessoas (As pessoas incluem pessoas para Controle de Acesso e Controle de Ponto .)	100.000
	Cartãos	500.000
	Impressão Digital	400.000
	Íris	200.000
	Fotos de Perfil	100.000
	Departamentos	3.000
	Hierarquias de Departamentos	10
	Tamanho de Uma Foto de Perfil	300 KB
	Tamanho Total das Fotos do Perfil	300 GB
	Pessoas Resignadas	100.000
	Tipos de Demissão	100
Armazenamento de dados	Período de Retenção de Dados	Armazenado por 3 anos ***Observação :*** *O valor pode variar por módulos diferentes. Veja*

		Requisitos do Sistema e Desempenho para detalhes.
	Volume de Armazenamento	Ilimitado③
	Contagem de Pessoas	5 milhões por ano
	Mapa de Calor	0,25 milhões por ano
	Registros ANPR	60 milhões por ano
	Eventos	
	Alarmes	
	Registros de Acesso	1,4 bilhão por ano
	Registros de Presença	55 milhões por ano
	Registros de Visitantes	10 milhões por ano
	Registros de Operação	5 milhões por ano
	Logs de Informações de Serviço	
	Logs de Erros de Serviço	
	Marcadores de Gravação	60 milhões por ano
Relatório	Relatórios Agendados Totais	100
	Dados Totais em Um Relatório Agendado	32.000
	Relatórios personalizados no módulo de controle de ponto	128
	GPS	250/s
Vídeo e Análise Inteligente		
Segurança de vídeo	Cronograma de Gravação	30.000
	Modelo de Cronograma de Gravação	200
	Usuários para Autenticações Duplas	50
	Captura acionada por evento (armazenada diretamente em servidores de gravação)	● Valor médio: 100/s ● Valor de pico: 1.000/s (Este valor não dura mais que 10 minutos.)
	Captura acionada por evento (armazenada no SYS ou transmitida para servidores de gravação do SYS)	● Valor médio: 20/s ● Valor de pico: 100/s (Este valor não dura mais que 10 minutos.)
Reconhecimento Inteligente	Imagens de rosto para reconhecimento inteligente	1000.000
	Biblioteca de imagens de rostos	64
	Grupos de Análise Inteligente	1.000
Análise Inteligente	Total de lojas	1.000
	Grupo de Análise Total	1.000
Monitoramento de RA	Cenas de RA	100
	Plano	512
	Tags para cada cena	200
	Grupos de tags para cada cena	100
Gestão de Evidências	Casos	100.000
	Arquivos	100.000
Parede Inteligente	Paredes inteligentes	32
	Teclado de rede	32
	Visualizações	1.000
	Ver grupos	100
	Visualizações em um grupo de visualização	10
	Câmeras em uma visão	256
	Câmeras em uma janela de troca automática	20
	Janelas de uma troca automática	16
	Ver grupo de uma troca automática	1
Servidor de Streaming ②	Entrada de vídeo Largura de banda por servidor de streaming	300 × 2 Mbps
	Largura de banda de saída de vídeo por servidor de transmissão	300 × 2 Mbps

Controle de Acesso e Controle de Ponto e Visitante		
Controle de acesso	Pontos de acesso (portas + pisos)	Central : 5.000 RSM: 10.000
	Nível de acesso	1.024
	Grupo de acesso	1.024
	Horários de acesso	32
	Modelos para impressão de cartões	32
Tempo e Presença	Horário	128
	Horário de intervalo	128
	Código de pagamento (incluindo tipos de horas extras e tipos de licença)	128
	Funções de aprovação	100
	Fluxo de aprovação	1.000
Gestão de Visitantes	Visitantes	100.000
	visitantes ou registros de reservas	100.000
	Modelo de e-mail para visitantes	20
	Entidades na lista de observação	10.000
	Modelo de cartão	20
	Modelo do WhatsApp	20
Veículos e Estacionamento		
Veículos por Lista		5.000
Veículos		500.000
Tipos de veículos personalizados		10
Fotos de chassis de veículos		3.000
Estacionamentos		10
Pistas		Total: 40 Em um estacionamento: 32
Vagas de estacionamento		Total: 5.000 Em um andar: 1.500
Pisos em todos os estacionamentos		128
Cartões vinculados a veículos		250.000
Cartões temporários em um estacionamento		10.000
Monitoramento de bordo		
Informações de GPS Relatório		Relate uma informação de GPS para a plataforma a cada 5s, um total de 200 informações de GPS podem ser enviadas para a plataforma por segundo.
Regras de cerca para um veículo		4
desvio para um veículo		4
Os veículos podem ser localizados em um cliente		64
Máximo de Motoristas		10.000
máximo de rotas de condução		1.000
Execução Portátil		
Grupos de Intercomunicação		128
Pessoas em um grupo de intercomunicação		10 0
Exibição Comercial		
Materiais		10.000
Programas		2.000
Horários		1.000
Conteúdos lançados rapidamente		64
Inspeção de Segurança		
Analisador		8
Detectores de metais walk-through		64
Transmissão		
Unidade de alto-falante		128

Grupo de Roadcast	128
Bibliotecas de Mídia	100
Patrulha	
Máximo de turnos de uma única rota	8
Gestão de Docas	
Docas	500
Rastreamento de Encomendas	
Pontos de verificação	1.000
Consumo de Cantina	
Número de comerciantes	100
Grupos de pagamento	512
Regras de pagamento	128
Tipos de refeições	8
Inspeção Inteligente	
Modelos de Inspeção	100
Tipos de Resposta	20
Itens de inspeção de uma categoria	50
Cronogramas de Inspeção	100
Atributos de um ativo	10
Tipos de ativos	50
Dispositivos vinculados de um tipo de ativo	50
Partes vinculadas de um tipo de ativo	10
Câmeras vinculadas de uma parte do ativo	4

① : Este valor recomendado se refere ao número de câmeras térmicas conectadas diretamente ao sistema. Depende do desempenho máximo (processamento e armazenamento de dados) na situação em que as câmeras térmicas gerenciadas carregam dados de temperatura para o sistema. Para câmeras térmicas conectadas ao sistema via NVR, não há tal limite.

② ： No módulo Portable Enforcement, há 400 pessoas realizando intercomunicação em grupo por meio do servidor de streaming do Hik Central Professional simultaneamente.

③ : O sistema possui capacidade de gerenciar ilimitada quantidade de dispositivos de armazenamento, sendo storages ou NVRs, independente da capacidade de cada de armazenamento de cada dispositivo.

Requisitos do Sistema

** Para alta estabilidade e bom desempenho, os seguintes requisitos de sistema devem ser atendidos .*

OS para HikCentral Professional Server	Microsoft® Windows 11 de 64 bits Microsoft® Windows 10 64 bits Microsoft® Windows Server 2019 64 bits Microsoft® Windows Server 2016 de 64 bits Microsoft® Windows Server 2012 R2 64 bits Microsoft® Windows Server 2012 de 64 bits Microsoft® Windows Server 2022 **Para o Windows Server 2012 R2, certifique-se de que ele esteja instalado com o pacote cumulativo (KB2919355) atualizado em abril de 2014.*
OS para Control Client	Microsoft® Windows 11 de 64 bits Microsoft® Windows 10 64 bits Microsoft® Windows Server 2019 64 bits Microsoft® Windows Server 2016 de 64 bits Microsoft® Windows Server 2012 R2 64 bits Microsoft® Windows Server 2012 de 64 bits Microsoft® Windows Server 2022 **Para o Windows Server 2012 R2, certifique-se de que ele esteja instalado com o pacote cumulativo (KB2919355) atualizado em abril de 2014.*
Versão do Navegador	Google Chrome ® 114 e posterior Firefox ® 114 e posterior Safari ® 16.6 e posterior Microsoft ® Edge 114 e posterior Internet Explorer ® 11 e posterior
Banco de Dados	PostgreSQL V16.1
OS para Cliente Móvel	iOS 12.0 e posterior Android 6.0 e posterior
Máquina Virtual	VMware® ESXi ™ 6.x, ESXi ™ 7.x Microsoft® Hyper-V com Windows Server 2012/2012 R2/2016 (64 bits) **O Control Client não pode ser executado na máquina virtual.* **Consulte o Guia de implantação do HikCentral Professional em máquinas virtuais VMware para saber como o servidor de streaming está em execução na máquina virtual.* **A migração de servidor virtual não é suportada .*

Especificação de Hardware Recomendada

Processador	E-2324G (4 núcleos/8 MB/4 T/ 3,1-4,6 GHz/65 W)	
Memória	1 × 16 GB até 2666 MT/s DDR4 UDIMM	
Controladores de Armazenamento	Controladores Internos: SAS_H355	
Baías de Unidade	1T 7.2K SATA×2	
Fontes de Alimentação	Fonte de alimentação única de 450 W (Bronze)	
Dimensões	Fator de forma: Rack (1U) Largura do chassi: 434,00 mm (17,08 pol.) Profundidade do chassi: 595,63 mm (23,45 pol.) (3,5”HHD) ***Observação:*** essas dimensões não incluem: moldura, PSU redundante	
Dimensões com Embalagem (L × P × A)	750 mm × 614 mm × 259 mm (29,53" × 24,17" × 10,2")	
Peso líquido	12,2 kg	
Peso com Embalagem	18,5 kg	
NIC Incorporado	2 portas de controlador de interface de rede (NIC) LOM de 1 GbE	
Acesso ao Dispositivo	Portas frontais: 1x USB 2.0, 1 x porta de gerenciamento IDRAC micro USB 2.0 Portas traseiras: 2 x USB 3.0, VGA, conector serial	
Gestão Embarcada	iDRAC9 com controlador de ciclo de vida iDRAC Direto API RESTful DRAC com Redfish	
Integrações e Conexões	Integrações: Centro de Sistema Microsoft® VMware® vCenter ™ BMC Truesight (disponível na BMC) Chapéu Vermelho Ansible	Conexões: Nagios Core e Nagios XI Gerente de Operações da Micro Focus i (OMi) IBM Tivoli Netcool / OMNIbus
Sistemas Operacionais	Certificar XenServer Citrix® XenServer® Microsoft Windows Server® com Hyper-V Red Hat® Enterprise Linux Servidor Ubuntu Este modelo é instalado com o sistema operacional multilíngue Microsoft Windows Server® 2019.	Servidor SUSE® Linux Enterprise VMware® ESXi

HIKVISION

See Far, Go Further

Headquarters
No.555 Qianmo Road, Binjiang District,
Hangzhou 310051, China
T +86-571-8807-5998
www.hikvision.com

Follow us on social media to get the latest product and solution information.

Hikvision | HikvisionHQ | HikvisionHQ | Hikvision_Global | Hikvision Corporate Channel | hikvisionhq

DS-KAB6-ZU1
Bracket

- Available for face recognition terminal which supports gang box installation on the speed gates and turnstiles
- The speed gate and turnstiles' model name with "Pg" support this bracket

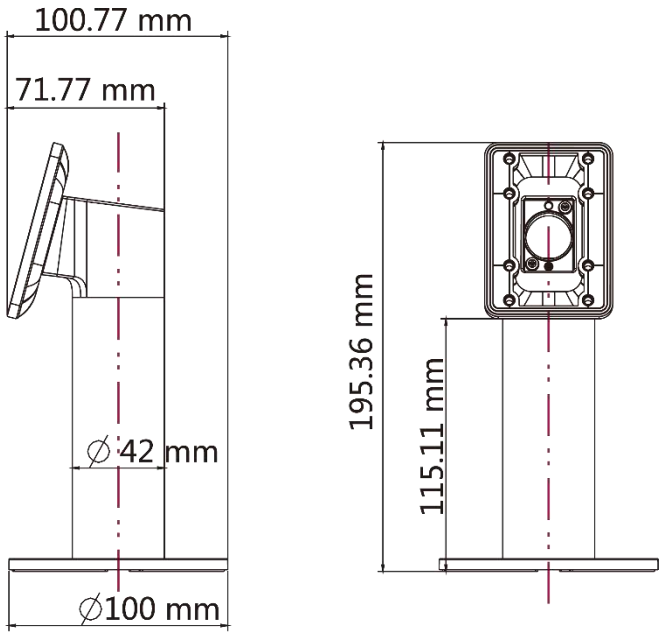
▪ Specification

General	
Dimensions	100 mm × 100 mm × 196 mm (3.94" × 3.94" × 7.72")
Weight	1.1 kg (2.4 lb)
Application environment	Indoor and outdoor
Material	AL-6061 aluminum alloy

▪ Available Model

DS-KAB6-ZU1

▪ Dimension



Distributed by

Headquarters
No.555 Qianmo Road, Binjiang District,
Hangzhou 310051, China
T +86-571-8807-5998
overseasbusiness@hikvision.com

Hikvision USA
T +1-909-895-0400
sales.usa@hikvision.com

Hikvision Europe
T +31-23-5542770
sales.eu@hikvision.com

Hikvision UK & Ireland
T +01628-902140
sales.uk@hikvision.com

Hikvision UAE
T +971-4-4432090
salesme@hikvision.com

Hikvision Russia
T +7-495-669-67-99
saleru@hikvision.com

Hikvision Australia
T +61-2-8599-4233
salesau@hikvision.com

Hikvision Italy
T +39-0438-6902
info.it@hikvision.com

Hikvision South Africa
Tel: +27 (10) 0351172
sale.africa@hikvision.com

Hikvision Singapore
T +65-6684-4718
sg@hikvision.com

Hikvision Korea
T +82-(0)31-731-8817
sales.korea@hikvision.com

Hikvision India
T +91-22-28469900
sales@pramahikvision.com

Hikvision Brazil
T +55 11 3318-0050
Latam.support@hikvision.com

Hikvision France
T +33(0)1-85-330-450
info.fr@hikvision.com

Hikvision Spain
T +34-91-737-16-55
info.es@hikvision.com

Hikvision Poland
T +48-22-460-01-50
info.pl@hikvision.com

Hikvision Canada
T +1-866-200-6690
sales.canada@hikvision.com

Hikvision Turkey
T +90 (216)521 7070- 7074
sales.tr@hikvision.com

Hikvision Kazakhstan
T +7-727-9730667
nikia.panfilov@hikvision.ru

Hikvision Tashkent
T +99-87-1238-9438
uzb@hikvision.ru

Hikvision Indonesia
T +62-21-2933759
Sales.Indonesia@hikvision.com

Hikvision Thailand
T +662-275-9949
sales.thailand@hikvision.com

Hikvision Malaysia
T +601-7652-2413
sales.my@hikvision.com

Hikvision Vietnam
T +84-974270888
sales.vt@hikvision.com

Hikvision Hong Kong
T +852-2151-1761
info.hk@hikvision.com

Hikvision Colombia
sales.colombia@hikvision.com

DS-TMG520/B-M
Barrier gates with straight boom pole

DS-TMG52X series barrier gate is applicable to entrance and exit management. It is widely used in road toll station, parking lot, community, enterprise entrance and exit, etc. to manage the entering and exiting of vehicles and record vehicle passing times. It can be controlled automatically via parking lot management system, or via handle, remote controller, buttons, etc.

- DC frequency conversion. The rising and falling speeds can be adjusted independently. The boom pole can rise in high speed to let the vehicle pass quickly.
- The boom pole can fall in low speed to avoid hitting vehicle and pedestrian and when the barrier arm collides with an object, the movement stops to mitigate object damage.
- High protection level. The chassis is produced with 2 mm cold rolled steel sheets in numerically-controlled precision. The surface is coated with plastic powder which is anti-UV, antistatic, non-peeling, and non-fading. The dustproof and waterproof level conforms to IP54.
- Multiple control modes. Rising priority. The boom pole can be controlled via relay, remote controller, and software command.
- Multiple anti-hitting modes via induction, IR, pressure wave, etc.
- The boom pole direction is adjustable from left to right, or from right to left.
- Anti-condensation. The electric motor is in low consumption even when the barrier gate is not in working status, which will keep the motor in normal temperature. So even in cold weather, the lube will not be frozen to guarantee the normal running of barrier gate.
- Auto lock. Even when the power is cut off, you can use tool to keep the barrier gate working.
- Intergated with arrow indicator to show barrier gate status.

▪ Specification

Barrier Housing	
Barrier Housing Material	SGCC
Barrier Housing Thickness	2.0 mm
Barrier Housing Door Thickness	1.5 mm
Barrier Housing Color	Orange red
Boom Pole Installation Height	880 mm
Body Indicators	Arrow Indictor
Barrier Gate General	
Matched Boom Pole Type	Cylinder boom pole: 1 to 4 m anti-collision Octagonal straight boom pole: 1 to 6 m Octagonal telescopic boom pole: 4 to 6 m Boom pole ≥ 5 m: with spindle rod
Boom Pole Direction	right by default, direction switchable
Boom Pole Falling and Rise Delay	10 s by default (configurable), min. 4 s
Boom Pole LED visual indication	Yes
Motor Type	DC brushless motor
Number of Cycles	5000000
Working Voltage	220 VAC
Remote Controller Frequency	433 MHz
Current	Max. 1.5 A
Consumption	300 W
Temperature and Humidity	Temperature: -30 °C to 70 °C (-22 °F to 158 °F)
Rising Boom Pole for Poweroff	Optional, not supported by default
Package	
Barrier Housing Dimensions (L × W × H)	1248 × 486 × 480 mm (49.1 × 19.1 × 18.9 inch)
Body Weight	59.3 ± 5 kg (130.7 ± 11.0 lb.)
Body Dimensions (with Package, Without Boom Pole) (L × W × H)	1266 × 504 × 626 mm (49.84 × 19.84 × 24.65 inch)
Barrier Gate	
Duty Cycle	100%
Interface	
Rising to Limit	1 group
Falling to Limit	1 group
Open	1 group
Close	1 group
Stop	1 group
IR/Inductive Loop/Radar	1 group
RS-485	1 group
Traffic Signal Light	1 group, external power supply required, max. 220 VAC supported
LED Indicators	1 group
Network	1 group (reserved)

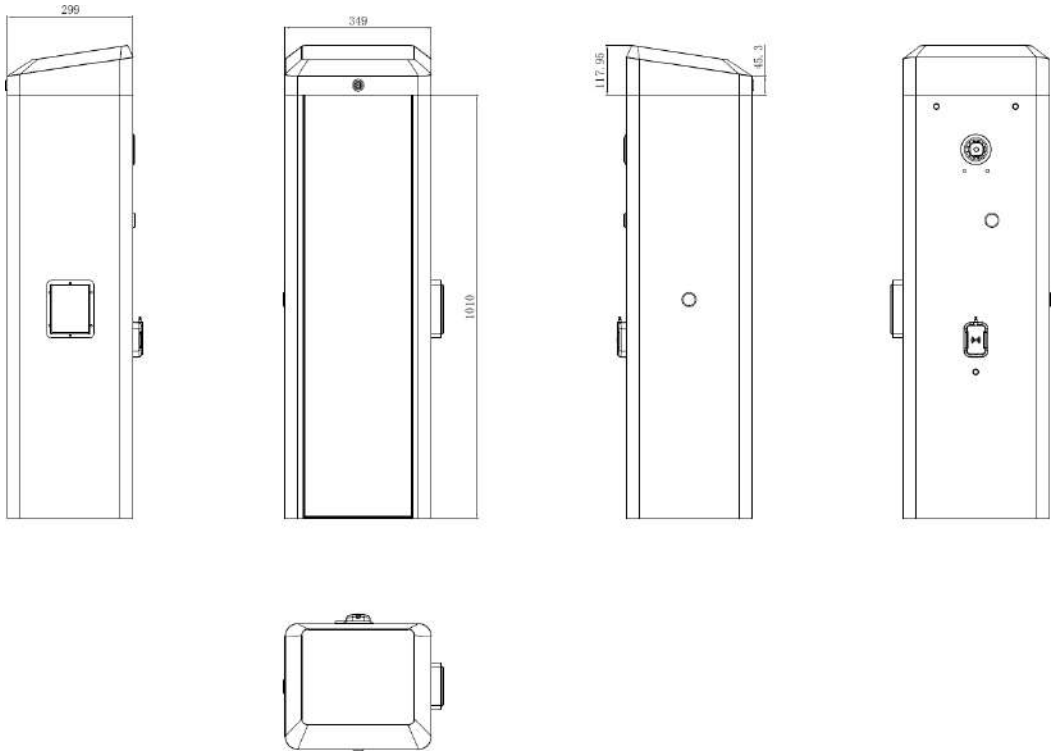
Approval	
RF	CE-RED EN 300220-1 V3.1.1 EN 300220-2 V3.1.1 EN 301489-1 V2.2.3 EN 301489-3 V2.1.1 EN IEC 62311: 2020
EMC	CE-EMC： EN 55032: 2015 + A11: 2020 + A1: 2020, EN IEC 61000-3-2: 2019 + A1: 2021, EN 61000-3-3: 2013 + A1: 2019 + A2: 2021, EN 50130-4: 2011 + A1: 2014
Security	CE-LVD: EN 62368-1: 2014 + A11: 2017 CB: IEC 62368-1: 2014 IEC 62368-1: 2018
Environment	ROHS
Protection	IP54
Boom Pole	
Boom Pole Type	Octagonal Straight Pole
Boom Pole Material	AL6061
Boom Pole Color	White background with red bar
Boom Pole Dimensions	2 m octagonal straight boom pole: 98 × 45 × 2000 mm (3.86 × 1.77 × 78.74 inch) 3 m octagonal straight boom pole: 98 × 45 × 3000 mm (3.86 × 1.77 × 118.11 inch) 4 m octagonal straight boom pole: 98 × 45 × 4000 mm (3.86 × 1.77 × 157.48 inch) 5 m octagonal straight boom pole: 119 × 55 × 5000 mm (4.69 × 2.17 × 196.85 inch) 6 m octagonal straight boom pole: 119 × 55 × 6000 mm (4.69 × 2.17 × 236.22 inch) 3 m boom pole with LED strip light: 95 × 49 × 3013 mm (3.74 × 1.93 × 118.62 inch) 4 m boom pole with LED strip light: 95 × 49 × 4013 mm (3.74 × 1.93 × 157.99 inch) 4 m octagonal telescopic boom pole: 110 × 44 × 2970 mm (4.33 × 1.73 × 116.93 inch) 5 m octagonal telescopic boom pole: 110 × 44 × 3470 mm (4.33 × 1.73 × 136.61 inch) 6 m octagonal telescopic boom pole: 110 × 44 × 6000 mm (4.33 × 1.73 × 236.22 inch) 2 m anti-collision cylinder boom pole: 80 × 80 × 2000 mm (3.15 × 3.15 × 78.74 inch) 3 m anti-collision cylinder boom pole: 80 × 80 × 3000 mm (3.15 × 3.15 × 118.11 inch) 4 m anti-collision cylinder boom pole: 80 × 80 × 4000 mm (3.15 × 3.15 × 157.48 inch)

Boom Pole Weight	2 m octagonal straight boom pole: 2.5 ± 0.3 kg (5.51 ± 0.66 lb.) 3 m octagonal straight boom pole: 2.8 ± 0.3 kg (6.17 ± 0.66 lb.) 4 m octagonal straight boom pole: 3.45 ± 0.3 kg (7.60 ± 0.66 lb.) 5 m octagonal straight boom pole: 5.9 ± 0.3 kg (13.00 ± 0.66 lb.) 6 m octagonal straight boom pole: 6.8 ± 0.3 kg (15.21 ± 0.66 lb.) 3 m boom pole with LED strip light: 3.4 ± 0.3 kg (7.50 ± 0.66 lb.) 4 m boom pole with LED strip light: 4.4 ± 0.3 kg (9.70 ± 0.66 lb.) 4 m octagonal telescopic boom pole: 4.42 ± 0.3 kg (9.74 ± 0.66 lb.) 5 m octagonal telescopic boom pole: 4.85 ± 0.3 kg (10.69 ± 0.66 lb.) 6 m octagonal telescopic boom pole: 5.65 ± 0.3 kg (12.46 ± 0.66 lb.) 2 m anti-collision round boom pole: 2.5 ± 0.3 kg (5.51 ± 0.66 lb.) 3 m anti-collision round boom pole: 3.5 ± 0.3 kg (7.71 ± 0.66 lb.) 4 m anti-collision round boom pole: 4.5 ± 0.3 kg (9.92 ± 0.66 lb.)
Boom Pole Dimensions (with Package)	2 m octagonal straight boom pole: 115 × 60 × 2020 mm (4.53 × 2.36 × 79.53 inch) 3 m octagonal straight boom pole: 115 × 60 × 3020 mm (4.53 × 2.36 × 118.90 inch) 4 m octagonal straight boom pole: 115 × 60 × 4020 mm (4.53 × 2.36 × 158.27 inch) 5 m octagonal straight boom pole: 140 × 65 × 5030 mm (5.51 × 2.56 × 198.03 inch) 6 m octagonal straight boom pole: 140 × 65 × 6030 mm (5.51 × 2.56 × 237.40 inch) 3 m boom pole with LED strip light: 100 × 60 × 3035 mm (3.94 × 2.36 × 120.07 inch) 4 m boom pole with LED strip light: 100 × 60 × 4035 mm (3.94 × 2.36 × 159.45 inch) 4 m octagonal telescopic boom pole: 120 × 51 × 3100 mm (4.72 × 2.01 × 122.05 inch) 5 m octagonal telescopic boom pole: 120 × 51 × 3500 mm (4.72 × 2.01 × 137.80 inch) 6 m octagonal telescopic boom pole: 120 × 51 × 4005 mm (4.72 × 2.01 × 157.68 inch) 2 m anti-collision round boom pole: 90 × 90 × 2030 mm (3.54 × 3.54 × 79.92 inch) 3 m anti-collision round boom pole: 90 × 90 × 3030 mm (3.54 × 3.54 × 119.29 inch) 4 m anti-collision round boom pole: 90 × 90 × 4030 mm (3.54 × 3.54 × 158.66 inch)
Boom Pole Weight (with Package)	2 m octagonal straight boom pole: 2.37 ± 0.3 kg (5.22 ± 0.66 lb.) 3 m octagonal straight boom pole: 3.11 ± 0.3 kg (6.86 ± 0.66 lb.) 4 m octagonal straight boom pole: 3.965 ± 0.3 kg (8.74 ± 0.66 lb.) 5 m octagonal straight boom pole: 7.01 ± 0.3 kg (15.45 ± 0.66 lb.) 6 m octagonal straight boom pole: 8.245 ± 0.3 kg (18.18 ± 0.66 lb.) 3 m boom pole with LED strip light: 4.0 ± 0.3 kg (8.82 ± 0.66 lb.) 4 m boom pole with LED strip lioght: 5.2 ± 0.3 kg (11.46 ± 0.66 lb.) 4 m octagonal telescopic boom pole: 5.11 ± 0.3 kg (11.27 ± 0.66 lb.) 5 m octagonal telescopic boom pole: 6.23 ± 0.3 kg (13.73 ± 0.66 lb.) 6 m octagonal telescopic boom pole: 7.25 ± 0.3 kg (15.98 ± 0.66 lb.) 2 m anti-collision round boom pole: 2.7 ± 0.3 kg (5.95 ± 0.66 lb.) 3 m anti-collision round boom pole: 4.3 ± 0.3 kg (9.48 ± 0.66 lb.) 4 m anti-collision round boom pole: 5.8 ± 0.3 kg (12.79 ± 0.66 lb.)

▪ Available Model

DS-TMG520-H/B(3m octagonal)
DS-TMG520-M/B(4m octagonal)
DS-TMG520-L/B(6m octagonal)
DS-TMG520-L/B-M(6m octagonal)

▪ Dimension



▪ Accessory

▪ Included

DS-TMG001-5 Octagonal Straight Boom Pole	DS-TMG012-5 Remote Controller	DS-TMG050 Pull Rod Antenna Assembly
		

▪ Optional

EEBracket-L800-1000(barrier) Barrier Pole	TMG080-3 TMG080-3	DS-TMG060-52 Barrier Gate Supercapacitor Board
		
DS-TMG022 Coil Vehicle Detector	DS-TMG023 Coil	DS-TVL221-1-6D Entrance & Exit Signal Light
		

Headquarters
No.555 Qianmo Road, Binjiang District,
Hangzhou 310051, China
T +86-571-8807-5998
www.hikvision.com

Follow us on social media to get the latest product and solution information.

Hikvision HikvisionHQ HikvisionHQ Hikvision_Global Hikvision Corporate Channel hikvisionhq

2.3 Security

- Mutual three pass authentication (ISO/IEC DIS 9798-2)
- Data encryption on RF-channel with replay attack protection
- Individual set of two keys per sector (per application) to support multi-application with key hierarchy
- Unique serial number for each device
- Transport key protects access to EEPROM on chip delivery

3. Ordering information

See Delivery Type Addendum of Device

4. Block diagram

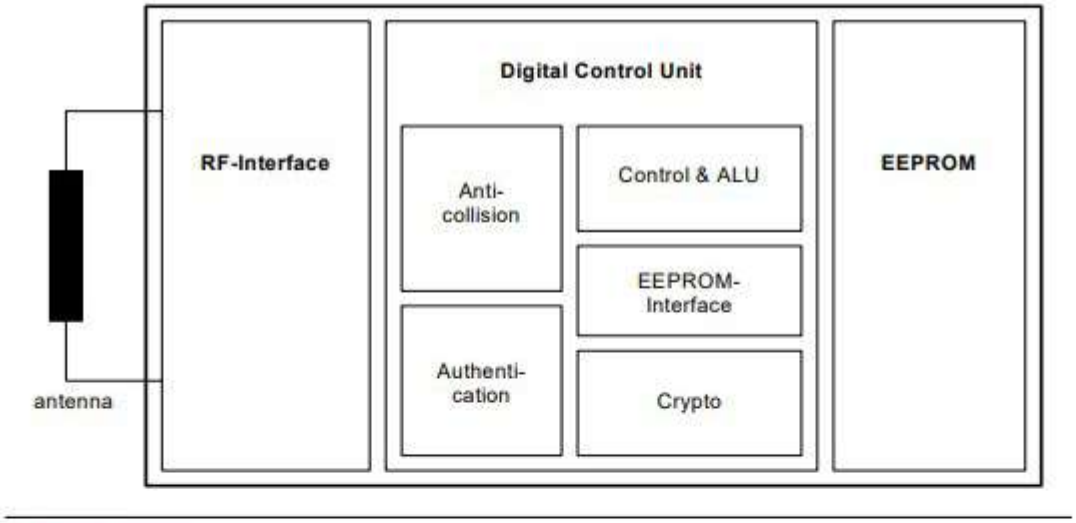


Fig 2. Block diagram

5. Pinning information

5.1 Pinning

See Delivery Type Addendum of Device

DS-KAB673-P-M
Peripheral Module

- Supports palm print and palm vein function
- Alive Detection
- Plug-and-play USB with no-driver technology, USB 2.0
- Supports linux system

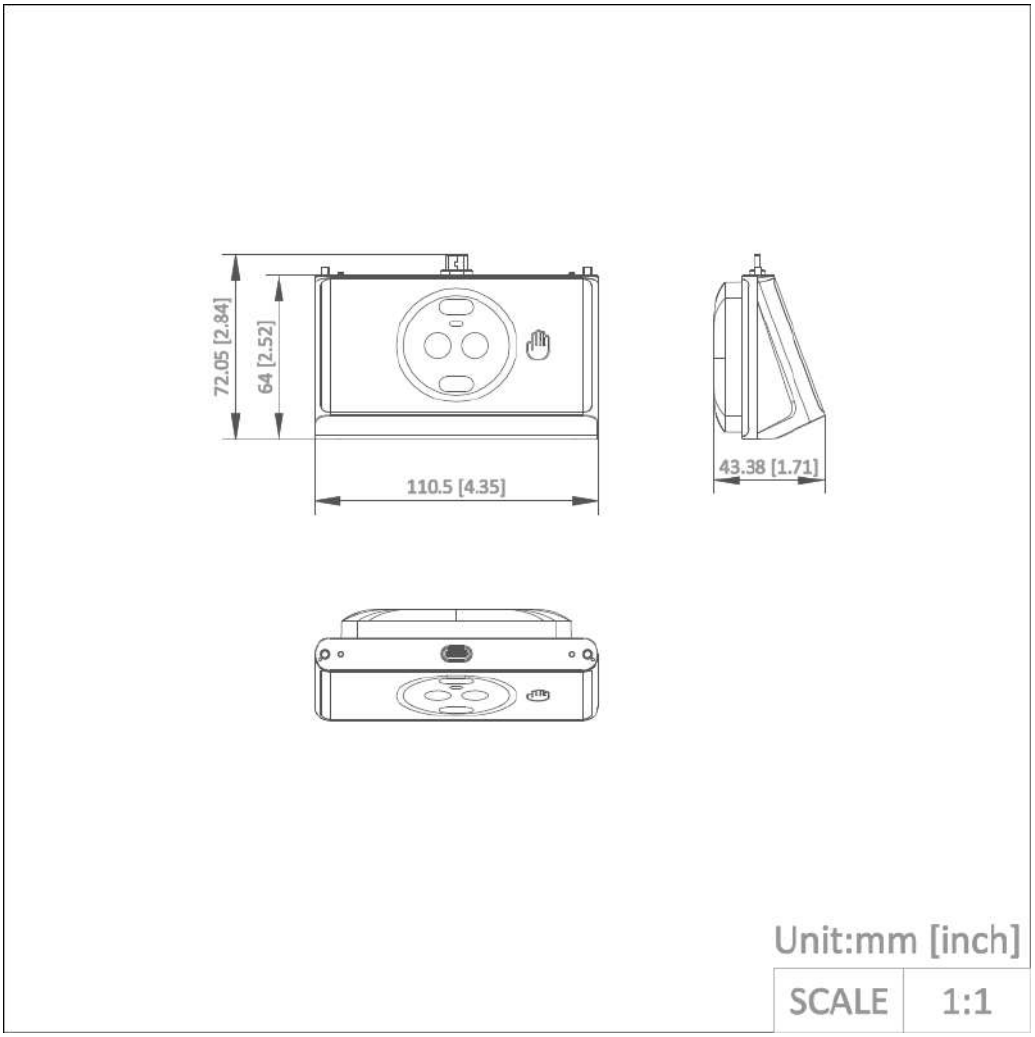
▪ Specification

System	
Operating system	Linux
Image	
Sensor	130W / 500 DPI
Capacity	
Palm print and palm vein capacity	10000
Authentication	
Palm print and palm vein recognition distance	5 cm ~12 cm
Accuracy	99,9%
Alive Detection	Yes
General	
Indicator	Support
Encryption	512 bits
Power supply	5V VDC, 1 A
Power consumption	5 W
Working temperature	-25 °C to 60 °C (-13 °F to 140 °F)
Working humidity	0 % to 90 % (no condensing)
Dimensions	110.5 mm × 72.05 mm × 43.38 mm (4.35" × 2.84" × 1.71")
Application environment	Indoor

▪ Available Model

DS-KAB673-P

▪ Dimension



- **Accessory**


DS-K1T673TDGX


DS-K1T673TDWX


DS-K1T673TDX


DS-K1T673TDX-M


DS-K1T673DX

Headquarters
No.555 Qianmo Road, Binjiang District,
Hangzhou 310051, China
T +86-571-8807-5998
www.hikvision.com

Follow us on social media to get the latest product and solution information.

Hikvision HikvisionHQ HikvisionHQ Hikvision_Global Hikvision Corporate Channel hikvisionhq

ITEM	DESCRIÇÃO	MARCA	MODELO
01	Software de controle de acesso	Hikvision	HIKCENTRAL PROFISSIONAL + Acessórios
02	Catracas Eletromecânicas do tipo Pedestal	Hikvision	DS-K3G200LXM-R/PG-DM55(O-STD) + ACESSÓRIOS
03	Leitor biométrico com pelo menos dois tipos de biometria	Hikvision	DS-K1T673TDX-M(O-STD)/BRAZIL, DS-KAB673-P-M(O-STD), DS-KAB6-ZU1 + ACESSÓRIOS
04	Cartões de proximidade	Loja RFID	CRACHÁ CLAMSHELL RFID 13,56 MHz SMART CARD MIFARE 1K - CHIP NXP MF1 IC S50
05	Catracas Eletromecânicas do tipo swing	Hikvision	DS-K3B530XM + Derivações + ACESSÓRIOS
06	Catracas Eletromecânicas do tipo Pedestal para pessoas com deficiência (PcD)	Hikvision	DS-K3BC411X-RS-M1/PG-DM90(O-STD)/SENSOR + ACESSÓRIOS
07	Kit fechadura eletromagnética para porta	Hikvision	DS-K4H255S, DS-K4H255-LZ + ACESSÓRIOS
08	Kit controle de acesso veicular tipo Barreira Eletrônica	Hikvision	DS-TMG520-L/B-M (6M OCTAGONAL) + ACESSÓRIOS
09	Catracas Eletromecânicas do tipo Swing para pessoas com deficiência (PcD)	Hikvision	DS-K3B530XM + Derivativos + ACESSÓRIOS

Belo Horizonte, 30 de outubro de 2024.

IGOR FACELLA SANTOS:05975641675

Assinado de forma digital por IGOR FACELLA SANTOS:05975641675
Dados: 2024.10.30 09:05:14 -03'00'

Emive Patrulha 24 Horas Ltda
Igor Facella Santos
Procurador
CPF: 059.756.416-75 / RG: 8.794.927