DS-K1T320 Series Terminal de Reconhecimento Facial

Manual do Usuário

DS-K1T320 Série Rosto Recoginção Terminal Utilizador

Informação Legal

Sobre este Manual

O Manual inclui instruções para usar e gerenciar o Produto. Imagens, gráficos, imagens e todas as outras informações a seguir são apenas para descrição e explicação. As informações contidas no Manual estão sujeitas a alterações, sem aviso prévio, devido a atualizações de firmware ou outros motivos. Por favor, encontre a versão mais recente deste Manual no site da Hikvision (***https:// www.hikvision.com/***).
Por favor, use este Manual com a orientação e assistência de profissionais treinados no suporte ao Produto.

Marcas comerciais

HIKVISION e outras marcas comerciais e logotipos da Hikvision são propriedades da Hikvision em várias jurisdições.
Outras marcas comerciais e logotipos mencionados são de propriedade de seus respectivos proprietários.

Disclaimer

NA EXTENSÃO MÁXIMA PERMITIDA PELA LEI APLICÁVEL, ESTE MANUAL E O PRODUTO DESCRITO, COM SEU HARDWARE, SOFTWARE E FIRMWARE, SÃO FORNECIDOS "NO ESTADO EM QUE SE ENCONTRAM" E "COM TODAS AS FALHAS E ERROS". A HIKVISION NÃO OFERECE GARANTIAS, EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÃO, COMERCIALIZAÇÃO, QUALIDADE SATISFATÓRIA OU ADEQUAÇÃO A UMA FINALIDADE ESPECÍFICA. O USO DO PRODUTO POR VOCÊ É POR SUA CONTA E RISCO. EM NENHUMA CIRCUNSTÂNCIA A HIKVISION SERÁ RESPONSÁVEL PERANTE VOCÊ 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), PRODUTO RESPONSABILIDADE, 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 FORNECE RISCOS DE SEGURANÇA INERENTES, E A HIKVISION NÃO ASSUMIRÁ NENHUMA RESPONSABILIDADE POR OPERAÇÃO ANORMAL, VAZAMENTO DE PRIVACIDADE OU OUTROS DANOS RESULTANTES DE ATAQUE CIBERNÉTICO, ATAQUE DE HACKERS, INFECÇÃO POR VÍRUS OU OUTROS RISCOS DE SEGURANÇA NA 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 INFRINJA OS DIREITOS DE TERCEIROS, INCLUINDO, SEM LIMITAÇÃO, DIREITOS DE PUBLICIDADE, DIREITOS DE PROPRIEDADE INTELECTUAL OU PROTEÇÃO DE DADOS E OUTROS DIREITOS DE PRIVACIDADE. VOCÊ NÃO DEVE USAR ESTE PRODUTO PARA QUAISQUER USOS FINAIS PROIBIDOS, INCLUINDO O

DESENVOLVIMENTO OU PRODUÇÃO DE ARMAS DE DESTRUIÇÃO MACIÇA, DESENVOLVIMENTO OU PRODUÇÃO DE ARMAS QUÍMICAS OU BIOLÓGICAS, QUAISQUER ACTIVIDADES NO CONTEXTO RELACIONADAS COM QUALQUER EXPLOSIVO NUCLEAR OU CICLO DE COMBUSTÍVEL NUCLEAR INSEGURO, OU EM APOIO A VIOLAÇÕES DOS DIREITOS HUMANOS.

NO CASO DE QUAISQUER CONFLITOS ENTRE ESTE MANUAL E A LEI APLICÁVEL, ESTA ÚLTIMA PREVALECE.

Proteção de Dados

Durante o uso do dispositivo, os dados pessoais serão coletados, armazenados e processados. Para proteger os dados, o desenvolvimento de dispositivos Hikvision incorpora a privacidade por princípios de design. Por exemplo, para dispositivos com recursos de reconhecimento facial, os dados biométricos são armazenados em seu dispositivo com método de criptografia; para o dispositivo de impressão digital, apenas o modelo de impressão digital será salvo, o que é impossível reconstruir uma imagem de impressão digital.

Como controlador de dados, vocêé aconselhado a coletar, armazenar, processar e transferir dados de acordo com as leis e regulamentos de proteção de dados aplicáveis, incluindo, sem limitação, a realização de controles de segurança para proteger os dados pessoais, como, por exemplo, a implementação de uma administração razoável e controles de segurança física, realizar revisões periódicas e avaliações da eficácia de seus controles de segurança.

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, resultará ou 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.
Nota	Fornece informações adicionais para enfatizar ou complementar pontos importantes do texto principal.

Informações Regulatórias

Informações da FCC

Por favor, tome atenção que alterações ou modificações não expressamente aprovadas pela parte responsável pela conformidade podem anular a autoridade do usuário para operar o equipamento.

Conformidade com a FCC: Este equipamento foi testado e considerado em conformidade com os limites para um dispositivo digital de Classe B, de acordo com a parte 15 das Regras da FCC. Esses limites são projetados para fornecer proteção razoável contra interferências prejudiciais em uma instalação residencial. Este equipamento gera, utiliza e pode irradiar energia de radiofrequência e, se não for instalado e utilizado de acordo com as instruções, pode causar interferências prejudiciais às comunicações de rádio. No entanto, não há garantia de que a interferência não ocorrerá em uma instalação específica. Se este equipamento causar interferência prejudicial à recepção de rádio ou televisão, que pode ser determinada desligando e ligando o equipamento , o usuário é encorajado a tentar corrigir a interferência por uma ou mais das seguintes medidas:

—Reorientar ou realocar a antena receptora.

—Aumentar a separação entre o eo receptor.

—Ligue o equipamento a uma tomada num circuito diferente daquele a que o receptor está ligado.

—Consulte o revendedor ou um técnico de rádio/TV experiente para obter ajuda

Este equipamento deve ser instalado e operado com uma distância mínima de 20cm entre o radiador e o seu corpo.

Condições da FCC

Este dispositivo está em conformidade com a parte 15 das Regras da FCC. A operação está sujeita às duas condições seguintes:

1. Este dispositivo pode não causar interferência prejudicial.
2. Este dispositivo deve aceitar qualquer interferência recebida, incluindo interferência que possa causar operação indesejada.

Declaração de conformidade UE

CE

Este produto e - se aplicável - os acessórios fornecidos também estão marcados com "CE" e, portanto, cumprem as normas europeias harmonizadas aplicáveis listadas

nos termos da Diretiva EMC 2014/30/UE, da Diretiva RE 2014/53/UE, da Diretiva RoHS 2011/65/UE

2012/19/UE (Diretiva REEE): Os produtos marcados com este símbolo não podem ser eliminados como resíduos urbanos não triados na União Europeia. Para uma reciclagem adequada, devolva este produto ao seu fornecedor local após a compra de um novo equipamento equivalente ou elimine-o em pontos de recolha designados. Para mais informações see: www.recyclethis.info

2006/66/EC (diretiva relativa às baterias): Este produto contém uma bateria que não pode ser eliminada como resíduos urbanos não triados na União Europeia. Consulte a documentação do produto para obter informações específicas sobre a bateria. A bateria é marcada com este símbolo, que pode incluir letras para indicar cádmio (Cd), chumbo (Pb) ou mercúrio (Hg). Para uma reciclagem adequada, devolva a bateria ao seu fornecedor ou a um ponto de recolha designado. Para obter mais informações, consulte:www.recyclethis.info

Este dispositivo está em conformidade com o(s) padrão(s) RSS isento(s) de licença da Industry Canada. A operação está sujeita às duas condições seguintes:
(1) este dispositivo não pode causar interferências, e
(2) este dispositivo deve aceitar qualquer interferência, incluindo interferências que possam causar o funcionamento indesejado do dispositivo.
Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radioexempts de licence. L'exploitation est autorisée aux deux conditions suivantes :
(1) l'appareil ne doit pas produire de brouillage, et
(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Instruções de Segurança

Estas instruções destinam-se a garantir que o usuário possa usar o produto corretamente para evitar perigo ou perda de propriedade.

A medida de precaução divide-se em Perigos e Precauções:

Perigos: Negligenciar qualquer um dos avisos pode causar ferimentos graves ou morte.

Precauções: Negligenciar qualquer um dos cuidados pode causar ferimentos ou danos ao equipamento.

⚠	⚠
Perigos: Siga estas salvaguardas para evitar ferimentos graves ou morte.	**Precauções:** Siga estas precauções para evitar possíveis lesões ou danos materiais.

⚠ Perigo:

- No uso do produto, você deve estar em estrita conformidade com os regulamentos de segurança elétrica da nação e da região.
- Não conecte vários dispositivos a um adaptador de energia, pois a sobrecarga do adaptador pode causar superaquecimento ou risco de incêndio.
- Se a fumaça, os odores ou o ruído subirem do dispositivo, desligue a alimentação imediatamente e desligue o cabo de alimentação e, em seguida, contacte o centro de assistência.
- A tomada deve estar instalada perto do equipamento e ser facilmente acessível.
- 1. Não ingerir bateria. Risco de queimadura química!
  2. Este produto contém uma bateria de célula de moeda/botão. Se a bateria da moeda/célula de botão for engolida, pode causar queimaduras internas graves em apenas 2 horas e pode levar à morte.
  3. Mantenha as pilhas novas e usadas longe das crianças.
  4. Se o compartimento da bateria não fechar com segurança, pare de usar o produto e mantenha-o longedas crianças.
  5. Se você acha que as baterias podem ter sido engolidas ou colocadas dentro de qualquer parte do corpo, procure atendimento médico imediato.
  6. CUIDADO: Risco de explosão se a bateria for substituída por um tipo incorreto.
  7. A substituição inadequada da bateria por um tipo incorreto pode prejudicar uma salvaguarda (por exemplo, no caso de alguns tipos de baterias de lítio).
  8. Não descarte a bateria no fogo ou em um forno quente, ou esmague ou corte mecanicamente a bateria, o que pode resultar em uma explosão.
  9. Não deixe a bateria em um ambiente circundante de temperatura extremamente alta, o que pode resultar em uma explosão ou vazamento de líquido ou gás inflamável.
  10. Não submeta a bateria a um pressure de ar extremamente baixo, o que pode resultar em uma explosão ou vazamento de líquido ou gás inflamável.
  11. Descarte as pilhas usadas de acordo com as instruções.

⚠ Cuidados:

- Não solte o dispositivo ou submeta-o a choque físico e não o exponha a alta radiação de eletromagnetismo. Evite a instalação do equipamento na superfície de vibrações ou locais sujeitos a choque (a ignorância pode causar danos ao equipamento).
- Não coloque o dispositivo em locais extremamente quentes (consulte a especificação do dispositivo para a temperatura de funcionamento detalhada), frio, empoeirado ou húmido, e não o exponha a radiações eletromagnéticas elevadas.
- Expor o equipamento à luz solar direta, baixa ventilação ou fonte de calor, como aquecedor ou radiador, é proibido (a ignorância pode causar perigo de incêndio).
- A tampa do dispositivo para uso interior deve ser mantida longe da chuva e da humidade.
- Expor o equipamento à luz solar direta, baixa ventilação ou fonte de calor, como aquecedor ou radiador, é proibido (a ignorância pode causar perigo de incêndio).
- Por favor, use um pano macio e seco quando limpar dentro e fora das superfícies da tampa do dispositivo, não use detergentes alcalinos.
- Os produtos de reconhecimento biométrico não são completamente aplicáveis a ambientes anti-spoofing. Se você precisar de um nível de segurança mais alto, use vários modos de autenticação.
- A porta serial do equipamento é usada apenas para depuração.
- Instale o equipamento de acordo com as instruções deste manual. Para evitar lesões, este equipamento deve ser firmemente fixado ao chão/parede de acordo com as instruções de instalação.
- O uso inadequado ou a substituição da bateria podem resultar em neblinade explosão. Substitua apenas pelo mesmo tipo ou equivalente. Descarte as baterias usadas de acordo com as instruções fornecidas pelo fabricante da bateria.
- Este suporte destina-se a ser utilizado apenas com dispositivos equipados. O uso com outros equipamentos pode resultar em instabilidade causando ferimentos.
- Este equipamento é para uso apenas com suporte equipado. O uso com outros (carrinhos, suportes ou transportadores) pode resultar em instabilidade causando ferimentos.

Modelos Disponíveis

Nome do Produto	**Modelo**	**Sem fio**
Terminal de Reconhecimento Facial	DS-K1T320MFWX	Placa de 13,56 MHz Apresentando Frequência, Wi-Fi, 2.4G
	DS-K1T320MFX	Placa de 13,56 MHz Apresentando Frequência
	DS-K1T320MWX	Placa de 13,56 MHz Apresentando Frequência, Wi-Fi, 2.4G
	DS-K1T320MX	Placa de 13,56 MHz Apresentando Frequência
	DS-K1T320EFWX	Placa de 125 KHz Apresentando Frequência, Wi-Fi, 2.4G
	DS-K1T320EFX	Placa de 125 KHz Apresentando Frequência
	DS-K1T320EWX	Placa de 125 KHz Apresentando Frequência, Wi-Fi, 2.4G
	DS-K1T320EX	Placa de 125 KHz Apresentando Frequência

Use apenas as fontes de alimentação listadas nas instruções do usuário:

Modelo	**Fabricante**	**Padrão**
TS-A012-120100E2 05K000C00	Shenzhen Transin Technologies Co., Ltd - Português	CE (em inglês)

Conteúdo

Sumário

Capítulo 1 Visão geral

1.1 Visão geral

O terminal de reconhecimento facial é um tipo de dispositivo de controle de acesso para reconhecimento facial, que é aplicado principalmente em sistemas de controle de acesso de segurança, como centros logísticos, aeroportos, campi universitários, centrais de alarme, residências, etc.

1.2 Características

- Tela LCD de 2,4 polegadas, lente de 2 MP
- Vários métodos de autenticação, incluindo rosto, impressão digital, cartão e PIN, etc.
- Suporta cartão Mifare ou cartão EM de acordo com diferentes modelos
- Máximo de 500 rostos, 1.000 cartões, 1.000 impressões digitais e 100.000 eventos
- Duração do reconhecimento facial < 0,2 s/Usuário
- Oferece suporte aos protocolos ISAPI e ISUP 5.0
- Configuração através do navegador da Web do PC e do navegador da Web móvel

Capítulo 2 Aparência

A aparência do dispositivo com impressão digital é a seguinte :

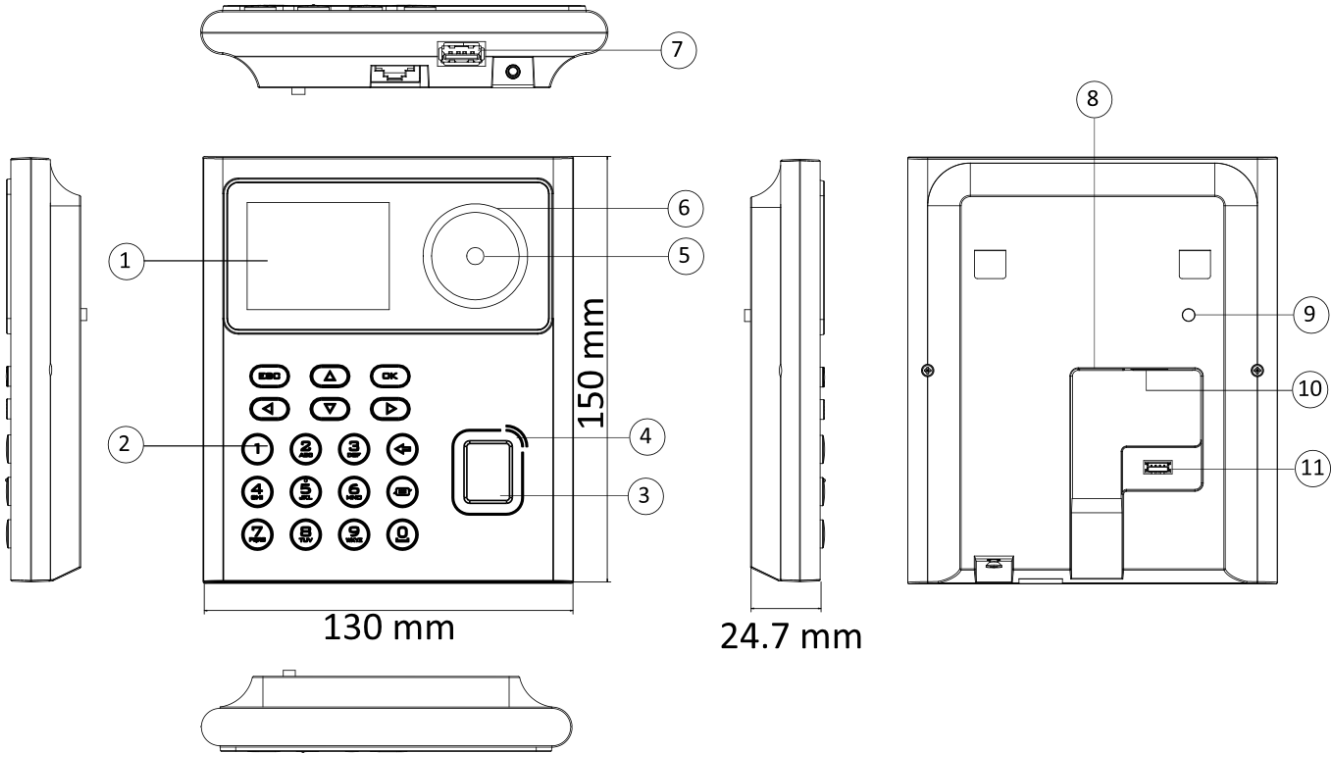


Figura 2-1 Aparência (com impressão digital)

A aparência do dispositivo sem impressão digital é a seguinte :

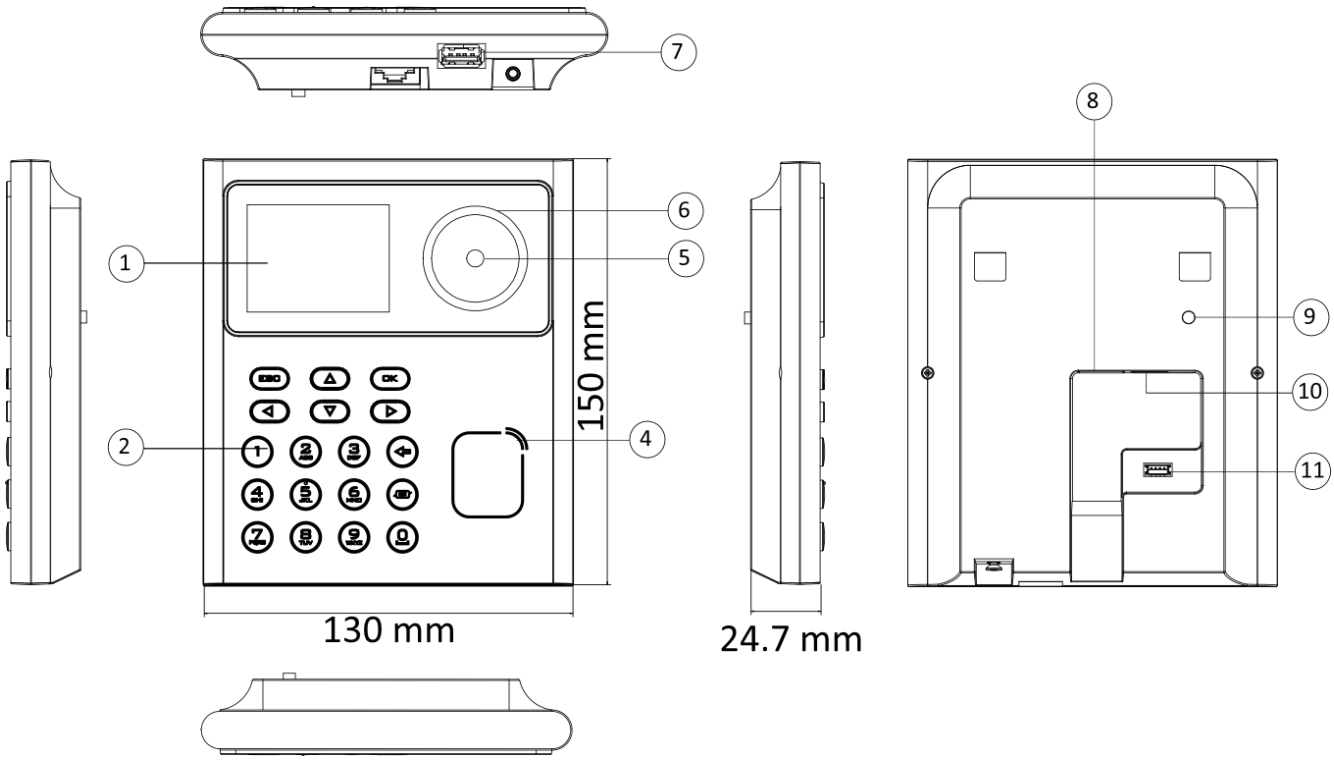


Figura 2-2 Aparência （Sem Impressão digital)

Tabela 2-1 Descrição da aparência

Não.	Nomo
1	Tela
2	Teclado numérico
3	Módulo de impressão | digital **Nota** Somente os dispositivos | que suportam um função de impressão digital | contêm um módulo de impressão digital.
4	Área de Deslizamento do Cartão
5	Câmera |
6	Suplemento Luz
7	Interface USB
8	Interface de rede |
9	Adulterar

Não.	Nome
10	Terminal de fiação (incluindo interface de fonte de alimentação)
11	Porta de depuração (somente para depuração)

Capítulo 3 Instalação

3.1 Ambiente de Instalação

- Apenas para uso interno.
- Evite luz de fundo, luz solar direta e luz solar indireta.
- Para melhor reconhecimento, deve haver fonte de luz dentro ou perto do ambiente de instalação.
- O peso mínimo de suporte da parede ou de outros locais deve ser 3 vezes mais pesado do que o peso do dispositivo.

3.2 Instalar com Gang Box

Passos

1. Fazer certo o gangue caixa É Instalado em o parede.

Nota

Você deve comprar a caixa da gangue separadamente.

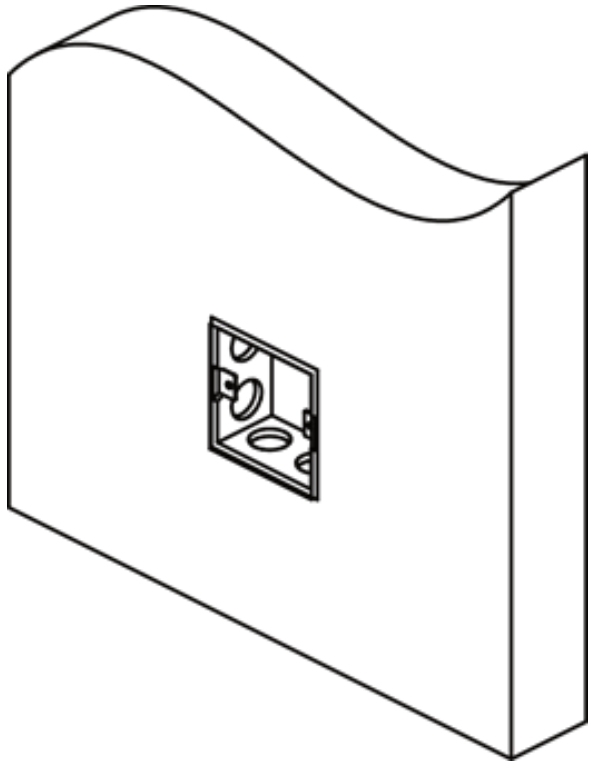


Figura 3-1 Caixa de instalação do gangue

2. Prenda a placa de montagem na caixa da gangue com dois parafusos fornecidos (SC-KA4X22).

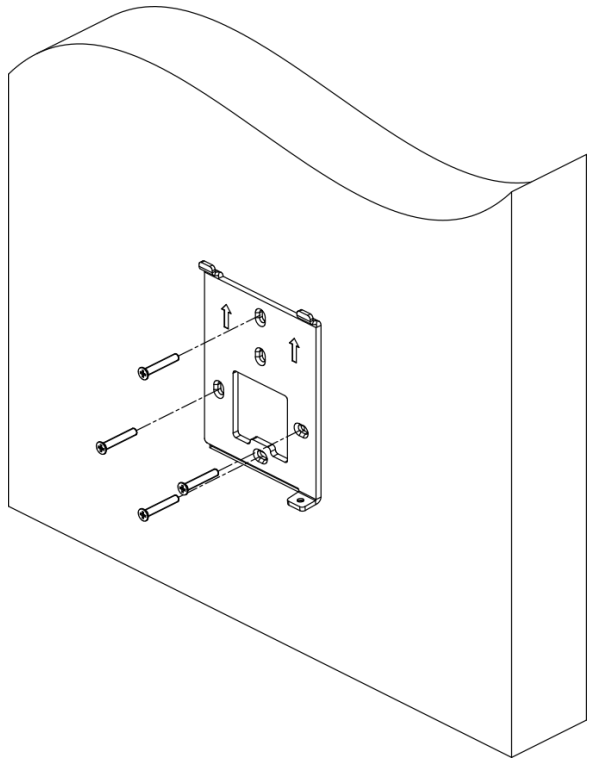


Figura 3-2 Instalar placa de montagem

3. Encaminhe o cabo através do orifício do cabo, conecte os cabos e insira os cabos na caixa da gangue.

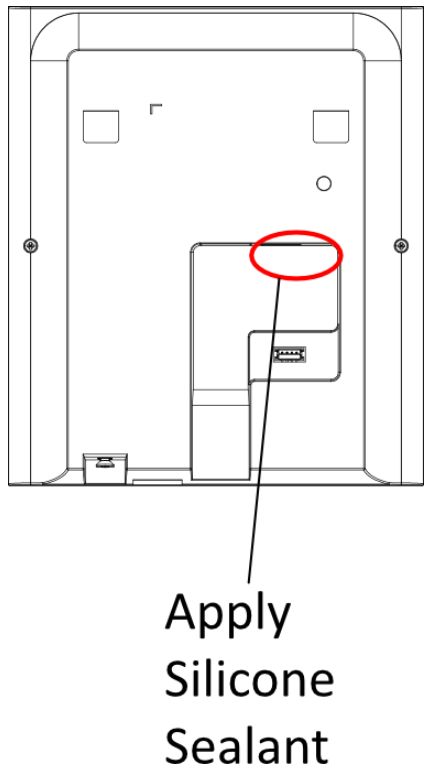


Figura 3-3 Aplicar selante de silicone

4. Alinhe o dispositivo com a placa de montagem e prenda o dispositivo na placa de montagem com 1 parafuso fornecido (SC-CM4X14-5T10-SUSS).

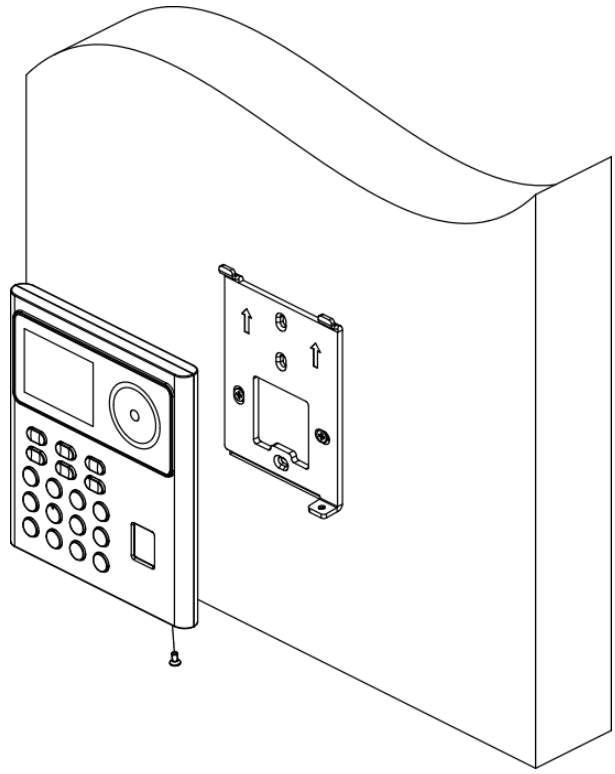


Figura 3-4 Dispositivo seguro

3.3 Montagem em superfície

Passos

Nota

A força adicional deve ser igual a três vezes o peso do equipamento. O equipamento e os meios de montagem associados devem permanecer seguros durante a instalação. Após a instalação, o equipamento, incluindo qualquer placa de montagem associada, não deve ser danificado.

1. Prenda a placa de montagem na parede com os 4 parafusos fornecidos (SC-KA4X22).

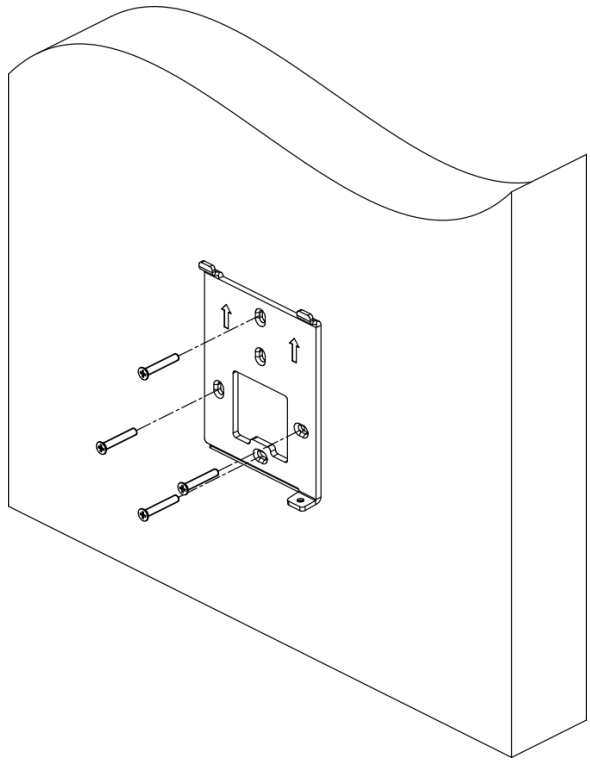


Figura 3-5 Placa de montagem de instalação

2. Encaminhe o cabo através do orifício do cabo da placa de montagem e conecte-se aos cabos periféricos correspondentes.

Nota

Se o dispositivo estiver instalado ao ar livre, você deve aplicar selante de silicone na saída da fiação para evitar a entrada de água.

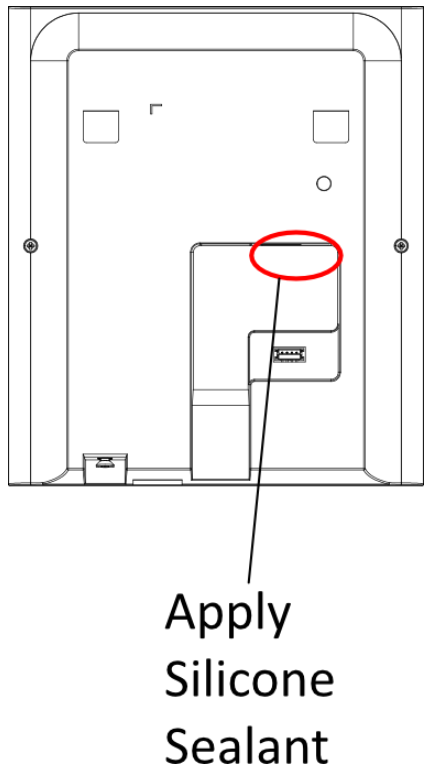


Figura 3-6 Aplicar selante de silicone

3. Alinhe o dispositivo com a placa de montagem e pendure-o na placa de montagem. Use 1 parafuso fornecido (SC-CM4X14_5T10-SUSS) para fixar o dispositivo e a placa de montagem.

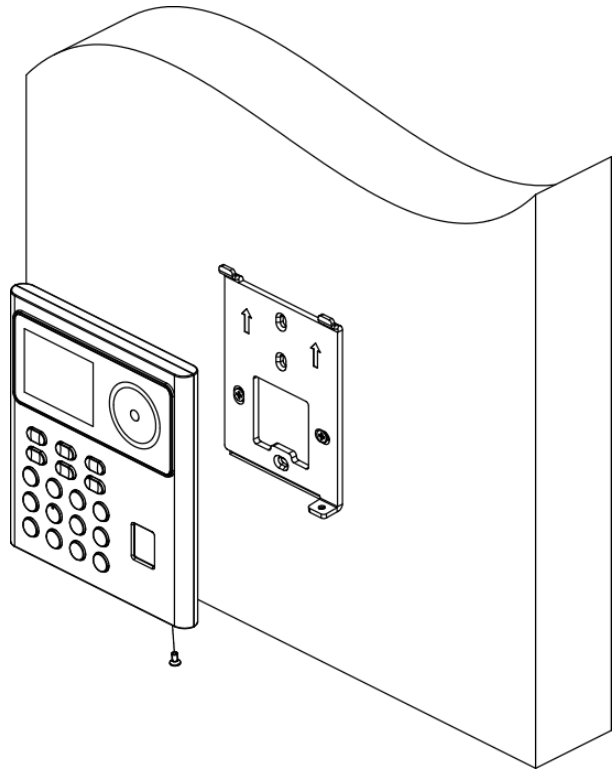


Figura 3-7 Dispositivo de travamento

4. Após a instalação, para o uso adequado do dispositivo (uso externo), cole a película de proteção (partes dos modelos fornecidos) na tela.

3.4 Montagem de Base

Passos

1. Encaminhe os cabos através do orifício do cabo do suporte e conecte os terminais com cabos periféricos. Coloque o suporte perto da parte de trás do dispositivo.

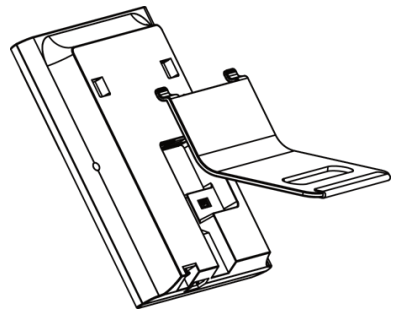


Figura 3-8 Coloque o suporte perto do lado de trás do dispositivo

2. Pressione o suporte com as duas mãos e certifique-se de que a fivela do suporte se encaixa com a parte de trás do dispositivo. Prenda o colchete na direção da seta.

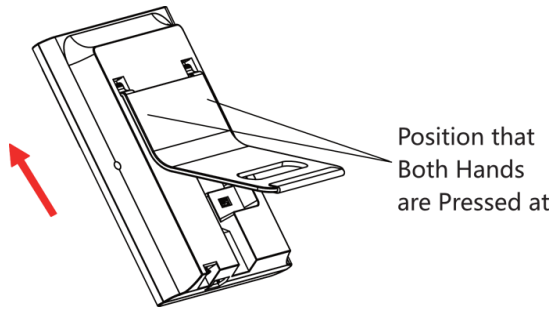


Figura 3-9 Suporte de fixação

3. Aperte o cinto no suporte até o final para concluir a instalação.

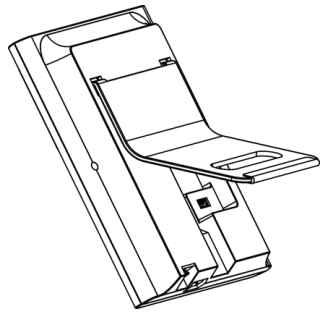


Figura 3-10 Instalação concluída

Capítulo 4 Fiação

Pode ligar o terminal NC/NO e COM com a fechadura da porta, ligar o terminal SEN e GND ao contacto da porta e o terminal BTN/GND com o botão de saída.

Nota

- Se o tamanho do cabo for de 18 AWG, você deve usar uma fonte de alimentação de 12 V. E a distância entre a fonte de alimentação e o dispositivo não deve ser superior a 20 m.
- Se o tamanho do cabo for de 15 AWG, você deve usar uma fonte de alimentação de 12 V. E a distância entre a fonte de alimentação e o dispositivo não deve ser superior a 30 m.
- Se o tamanho do cable for de 12 AWG, você deve usar uma fonte de alimentação de 12 V. E a distância entre a fonte de alimentação e o dispositivo não deve ser superior a 40 m.
- O leitor de cartão externo, a trava da porta, o botão de saída e o magnético da porta precisam de fonte de alimentação individual.

4.1 Descrição do terminal

Os terminais contêm entrada de energia e

fechadura da porta. As descrições dos terminais

são as seguintes:

Tabela 4-1 Descrições dos terminais

Grupo	Não.	Função	Cor	Nome	Descrição
Grupo A	A1	Entrada de energia	Vermelho	+12 V	Fonte de alimentação de 12 VDC
	A2		Preto	GND	Chão
Grupo B	B1	Fechadura da porta	Branco/roxo	NC	Fiação de bloqueio (NC)
	B2		Branco/Amarelo	.COM	Comum
	B3		Branco/Vermelho	NÃO	Fiação de bloqueio (NÃO)
	B4		Amarelo/Verde	SENSOR	Contato da Porta
	B5		Preto	GND	Chão

	B6		Amarelo/Cinzento	BOTÃO	Saia da fiação da porta

4.2 Dispositivo Normal de Fio

Você pode conectar o terminal com periféricos normais.

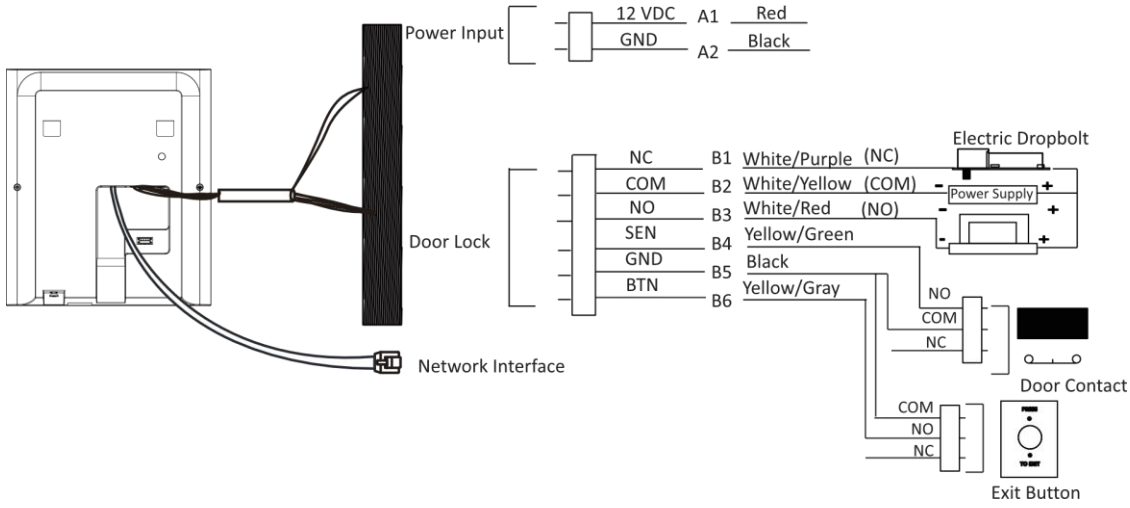


Figura 4-1 Fiação do dispositivo

Nota

- Não ligue o dispositivo diretamente à fonte de alimentação elétrica.
- Ao conectar o contato da porta e o botão de saída, o dispositivo deve usar a mesma conexão comum.
- A fonte de alimentação externa sugerida para a fechadura da porta é de 12 V, 1 A

Capítulo 5 Ativação

Você deve ativar o dispositivo antes do primeiro login. Depois de ligar o dispositivo, o sistema mudará para a página Ativação do dispositivo.

A ativação através do dispositivo, da ferramenta SADP e do software

cliente é suportada. Os valores padrão do dispositivo são os seguintes:

- O endereço IP padrão: 192.0.0.64
- A porta padrão No.: 8000
- O nome de usuário padrão: admin

5.1 Ativar via Dispositivo

Se o dispositivo não estiver ativado, você poderá ativá-lo depois que ele for ligado.

Na página Ativar Dispositivo, crie uma senha e confirme a senha. Toque em **Ativar** e o dispositivo será ativado.

Figura 5-1 Página de ativação

Cuidado

A força da senha do dispositivo pode ser verificada automaticamente. É altamente recomendável que você altere a senha de sua própria escolha (usando um mínimo de 8 caracteres, incluindo pelo menos três tipos de categorias a seguir:letras maiúsculas por caso, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. E recomendamos que você mude o seu

senha regularmente, especialmente no sistema de alta segurança, alterar a senha mensal ou semanalmente pode proteger melhor o seu produto.
Apropriado configuração de todo Senhas e outro segurança Configurações É o responsabilidade de o instalador e/ou o utilizador final.

Nota

Não há suporte para que os caracteres que contenham admin e nimda sejam definidos como senha de ativação.

- Após a ativação, você deve selecionar um idioma de acordo com suas necessidades reais.
- Após a ativação, você deve definir a rede. Para obter detalhes, consulte ***Definir parâmetros de rede*** .
- Após a ativação, você pode adicionar o dispositivo à plataforma. Para obter detalhes, consulte ***Acesso à plataforma*** .
- Após a ativação, se você precisar definir a privacidade, verifique o item. Para obter detalhes, consulte ***Privacidade SeFngs*** .
- Após a ativação, se você precisar adicionar administrador para gerenciar os parâmetros do dispositivo, defina administrador. Para obter detalhes, consulte ***Adicionar administrador*** .

5.2 Umctivate via Web Browser

Você pode ativar o dispositivo através do navegador da web.

Passos

1. Insira o endereço IP padrão do dispositivo (192.0.0.64) na barra de endereços do navegador da Web e pressione **Entre**.

   Nota

   Verifique se o endereço IP do dispositivo e o do computador devem estar no mesmo segmento IP.

2. Criar a Novo senha (administrador senha) e confirmar o senha.

   Cuidado

   SENHA FORTE RECOMENDADA - Recomendamos que você crie uma senha forte de sua própria escolha (usando um mínimo de 8 caracteres, incluindo 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 mensal ou semanalmente pode proteger melhor seu produto.

   Nota

   Não há suporte para que os caracteres que contenham admin e nimda sejam definidos como senha de ativação.

3. Clique em **Ativar**.
4. Edite o endereço IP do dispositivo. Você pode editar o endereço IP por meio da

ferramenta SADP, do dispositivo e do software cliente.

5.3 Ativar via SADP

SADP é uma ferramenta para detectar, ativar e modificar o endereço IP do dispositivo através da LAN.

Antes de começar

- Obtenha o software SADP do disco fornecido ou do site oficial ***http:// www.hikvision.com/en/*** e instale o SADP de acordo com os prompts.
- O dispositivo e o PC que executa a ferramenta SADP devem estar dentro da mesma sub-rede.

As etapas a seguir mostram como ativar um dispositivo e modificar seu endereço IP. Para ativação em lote e modificação de endereços IP, consulte o *Manual do Usuário do SADP* para obter detalhes.

Passos

1. Execute o software SADP e pesquise os dispositivos online.

2. Localize e selecione seu dispositivo na lista de dispositivos online.

3. Entrada Novo senha (administrador senha) e confirmar o senha.

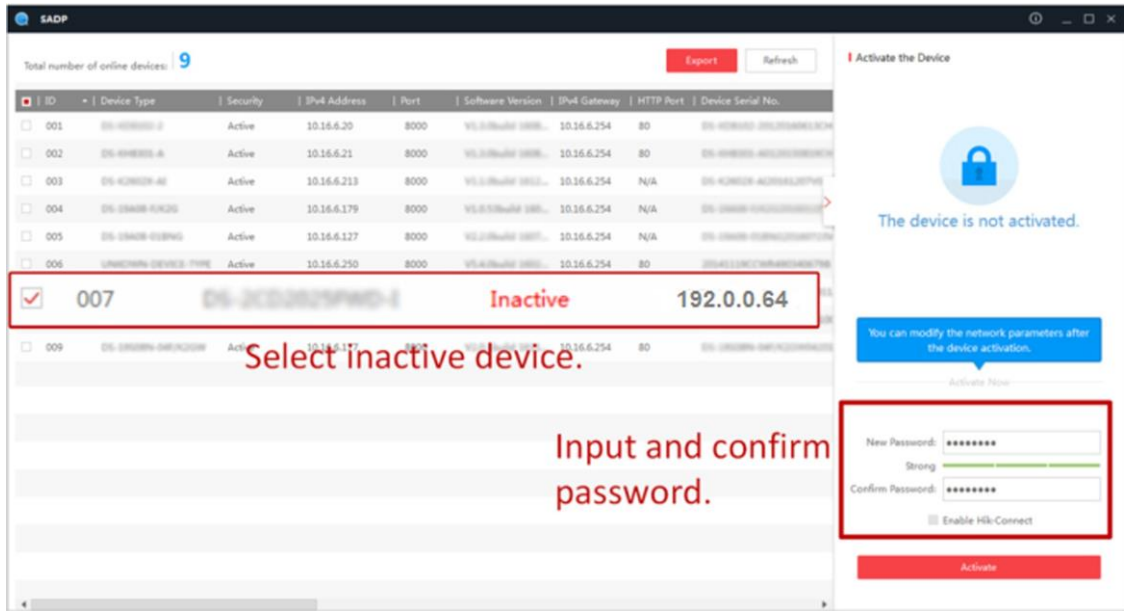
Cuidado

SENHA FORTE RECOMENDADA - Recomendamos que você crie uma senha forte de sua própria escolha (usando um mínimo de 8 caracteres, incluindo 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 dealta segurança, redefinir a senha mensal ou semanalmente pode proteger melhor seu produto.

Nota

Não há suporte para que os caracteres que contenham admin e nimda sejam definidos como senha de ativação.

4. Clique em **Ativar** para iniciar a ativação.



O status do dispositivo torna-se **ativo** após a ativação bem-sucedida.

5. Modifique o endereço IP do dispositivo.

1) Selecione o dispositivo.

2) Altere o endereço IP do dispositivo para a mesma sub-rede do computador modificando o endereço IP manualmente ou marcando **Habilitar DHCP**.

3) Insira a senha de administrador e clique em **Modificar** para ativar a modificação do endereço IP.

5.4 Ativar dispositivo via software cliente iVMS-4200

Para alguns dispositivos, é necessário criar a senha para ativá-los antes que eles possam ser adicionados ao software iVMS-4200 e funcionar corretamente.

Passos

Nota

Esta função deve ser suportada pelo dispositivo.

1. Entre na página Gerenciamento de dispositivos.

2. Clique à direita de **Gerenciamento** de **dispositivos** e selecione **Dispositivo**.

3. Clique em **Dispositivo Online** para mostrar a área do dispositivo online. Os dispositivos online pesquisados são exibidos na lista.

4. Verifique o status do dispositivo (mostrado na coluna **Nível de Segurança**) e selecione um dispositivo inativo.

5. Clique em **Ativar** para abrir a caixa de diálogo Ativação.

6. Crie uma senha no campo de senha e confirme a senha.

Cuidado

A força da senha do dispositivo pode ser verificada automaticamente. É altamente recomendável que você altere a senha de sua própria escolha (usando um mínimo de 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: 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, alterando a senha mensal ou semanalmente pode proteger melhor seu produto. Apropriado configuração de todo Senhas e outro segurança Configurações É o responsabilidade de o instalador e/ou o utilizador final.

Nota

Não há suporte para que os caracteres que contenham admin e nimda sejam definidos como senha de ativação.

7. Clique em **OK** para ativar o dispositivo.

Capítulo 6 Operação Rápida

6.1 Selecione o idioma

Você pode selecionar um idioma para o sistema do dispositivo.

Após a ativação do dispositivo, você pode selecionar um idioma para o sistema do dispositivo.

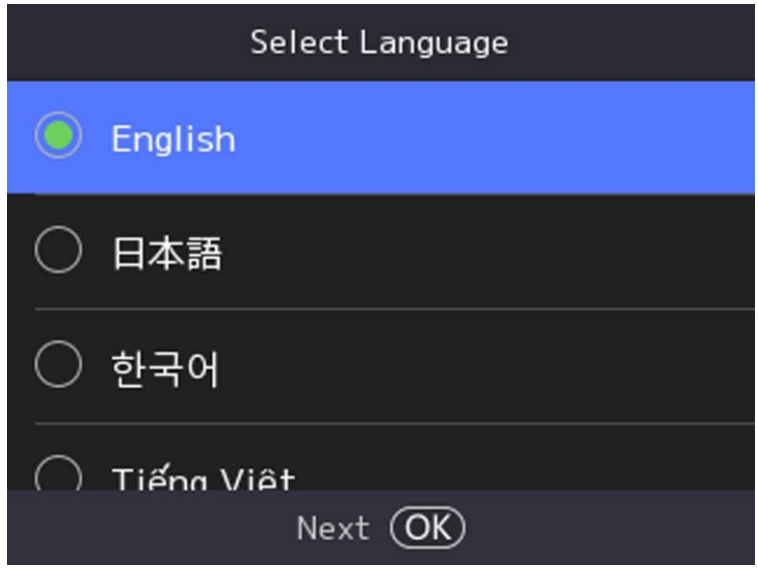


Figura 6-1 Selecione o idioma do sistema

Por padrão, o idioma do sistema é o inglês.

Nota

Depois de alterar o idioma do sistema, o dispositivo será reinicializado automaticamente.

6.2 Definir parâmetros de rede

Após a ativação e selecione o modo de aplicativo, você pode definir a rede para o dispositivo

Passos

1. Ao entrar na página Selecionar Rede, selecione **Rede com Fio** ou **Wi-Fi** para suas necessidades reais.

Figura 6-2 Selecionar rede

Nota

Desconecte a rede com fio antes de conectar um Wi-Fi.

2. Selecionar **Próximo**.

Nota

Wired Rede

Verifique se o dispositivo se conectou a uma rede.

Se ativar **o DHCP,** o sistema atribuirá o endereço IP e outros parâmetros automaticamente. Se desabilitar **DHCP,** você deverá definir o endereço IP, a máscara de sub-rede e o gateway.

Wi-Fi gratuito

Selecione um Wi-Fi e digite a senha do Wi-Fi para se conectar.

Ou selecione **Adicionar** Wi-Fi e digite o nome do Wi-Fi e a senha para se conectar.

3. Opcional: Selecione **Voltar** para ignorar as configurações de rede.

6.3 Acesso à Plataforma

Ative a função e o dispositivo pode se comunicar via Hik-Connect. Você pode adicionar o dispositivo ao cliente de modificação Hik-Connect e assim por diante.

Passos

1. Habilite o Acesso **ao Hik-Connect** e defina o IP do Servidor e **o** Código de Verificação.

2. Toque em **Next**.

6.4 Configurações de privacidade

Após a ativação, selecionando a rede, você deve definir os parâmetros de privacidade, incluindo o upload e o armazenamento de imagens.

Selecione parâmetros de acordo com suas necessidades reais.

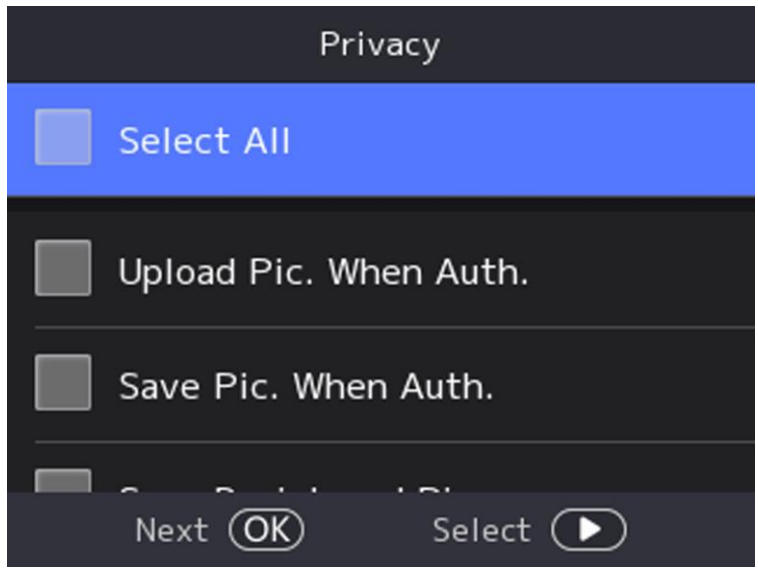


Figura 6-3 Foto de

carregamento de privacidade. Quando Auth. (Carregar imagem

ao autenticar)

Carregue as imagens capturadas ao autenticar na plataforma automaticamente.

Salvar foto. Quando Auth. (Salvar imagem ao autenticar)

Se você ativar essa função, poderá salvar a imagem ao autenticar no dispositivo.

Salve a foto registrada. (Salvar foto registrada)

A imagem do rosto registrado será salva no sistema se você ativar a função.

Carregar Foto. Após a captura vinculada (carregar imagem após a captura vinculada)

Carregue as imagens capturadas pela câmera vinculada para a plataforma automaticamente.

Salvar foto. Após a captura vinculada (salvar imagens após a captura vinculada)

Se você ativar essa função, poderá salvar a imagem capturada pela câmera vinculada no dispositivo.

Selecione **Avançar** para concluir as configurações.

6.5 Definir administrador

Após a ativação do dispositivo, você pode adicionar um administrador para gerenciar os parâmetros do dispositivo.

Antes de começar
Ative o dispositivo.

Passos
1. Insira o nome do administrador (opcional) e selecione **Avançar**.

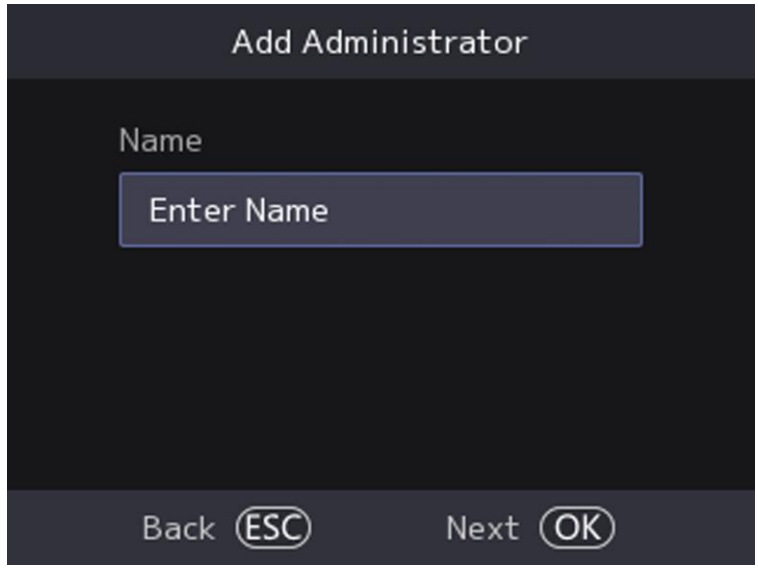


Figura 6-4 Adicionar página do administrador

2. Selecionar a credencial Para adicionar.

Nota

Até uma credencial deve ser adicionada.

- : Volte para a frente para a câmera. Certifique-se de que o rosto está na área de reconhecimento facial. Pressione OK para capturar e pressione OK para confirmar.
- : Pressione o dedo de acordo com as instruções na tela do dispositivo. Pressione OK para confirmar.
- : Digite o cartão No. ou apresentar cartão na área de apresentação do cartão. Pressione OK para confirmar.

3. Pressione OK.

Capítulo 7 Operação de base

7.1 Login

Faça login no dispositivo para definir os parâmetros básicos do dispositivo.

7.1.1 Login por Administrador

Se você tiver adicionado um administrador para o dispositivo , somente o administrador poderá fazer login no dispositivo para operação do dispositivo.

Passos

1. Pressione por muito tempo OK para entrar na página de login do administrador.

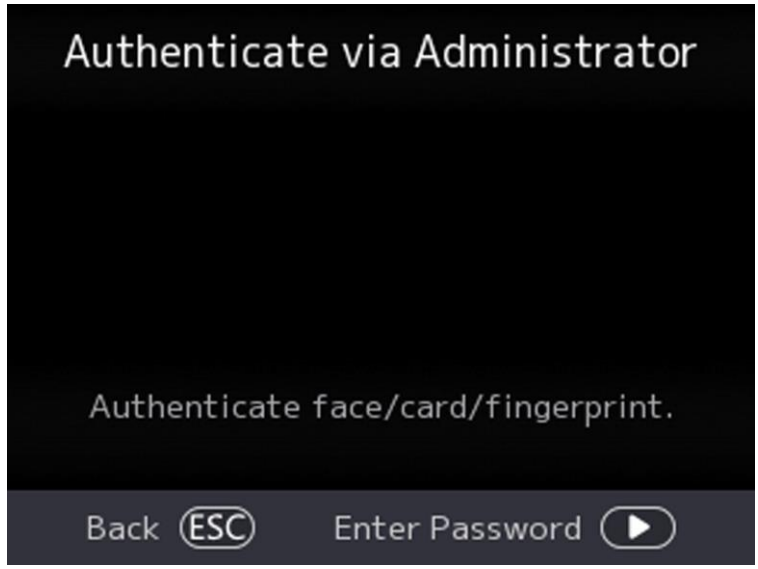


Figura 7-1 Login do administrador

2. Autenticar o do administrador rosto impressão digital ou cartão Para entrar o Casa página.

Nota

O dispositivo será bloqueado por 30 minutos após 5 tentativas de impressão digital ou cartão com falha.

3. **Opcional:** Pressione OK e você pode inserir a senha de ativação do dispositivo para login.
4. **Opcional:** Pressione ESC e você pode sair da página de login do administrador.

7.1.2 Login por Senha de Ativação

Você deve fazer login no sistema antes de outras operações do dispositivo. Se você não configurar um administrador, siga as instruções abaixo para fazer login.

Passos

1. Pressione por OK para entrar em Autenticar via página Administrador.
2. Pressione para digitar a senha.
   - Se você adicionou um administrador para o dispositivo, pressione OK e digite a senha.
   - Se você não adicionou um administrador para o dispositivo, digite a senha.
3. Imprensa OKEY Para entrar o Casa página.

Nota

O dispositivo será bloqueado por 30 minutos após 5 tentativas de senha com falha.

7.1.3 Esqueceu a senha

Se você esquecer a senha durante a autenticação, poderá alterá-la .

Passos

1. Pressione por OK para entrar na página Autenticar via Administrador.
2. Pressione para inserir a página de digitação de senha e pressione ESC.
3. Selecione **Esqueceu a senha**.
4. Responda às perguntas de segurança configuradas durante a ativação.
5. Crie uma nova senha e confirme-a.
6. Pressione **OK.**

7.2 Configurações de comunicação

Você pode definir a rede com fio, o parâmetro Wi-Fi, os parâmetros RS-485, os parâmetros Wiegan, ISUP e acesso ao Hik-Connect na página de configurações de comunicação.

7.2.1 Definir parâmetros de rede com fio

Você pode definir os parâmetros de rede com fio do dispositivo, incluindo o endereço IP, a máscara de sub-rede, o gateway e os parâmetros DNS.

Passos

1. Selecione **Comunicação de → Básica.** (Comunicação) para entrar na página Configurações de comunicação.
2. Na página Comunicação, selecione **Rede com fio**.

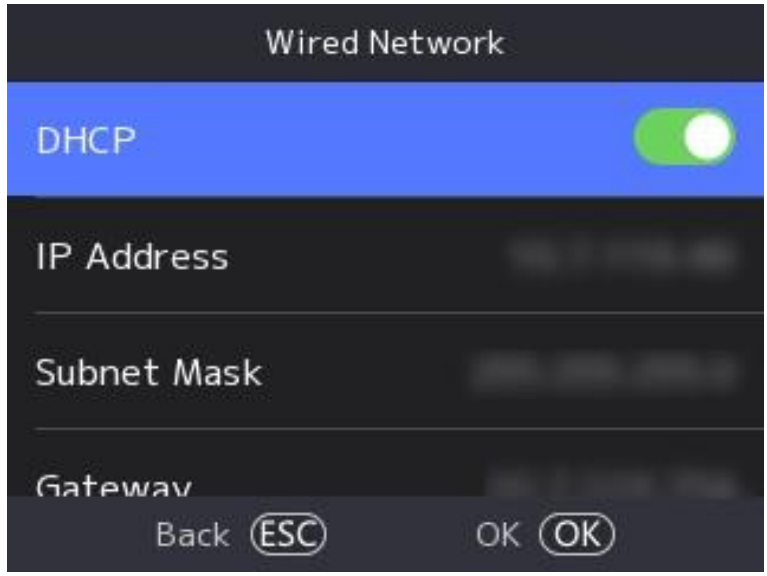


Figura 7-2 Configurações de rede com fio

3. Defina Endereço IP, Máscara de Sub-rede e Gateway.

- Habilite o **DHCP** e o sistema atribuirá endereço IP, máscara de sub-rede e gateway automaticamente.
- Desative **o DHCP** e você deve definir o endereço IP, a máscara de sub-rede e o gateway manualmente.

Nota

O endereço IP do dispositivo e o endereço IP do computador devem estar no mesmo segmento IP.

4. Defina os parâmetros DNS. Você pode habilitar **a** obtenção **automática de** DNS, definir o servidor DNS preferencial e o servidor DNS alternativo.

7.2.2 Definir parâmetros de Wi-Fi

Você pode ativar a função Wi-Fi e definir os parâmetros relacionados ao Wi-Fi.

Passos

Nota

A função deve ser suportada pelo dispositivo.

1. Selecione **Comunicação de → Básica.** (Comunicação) para entrar na página Configurações de comunicação.

2. Na página Configurações de comunicação, selecione **Wi-Fi**.

Figura 7-3 Configurações de Wi-Fi

3. Ative a função Wi-Fi.

4. Selecionar a Wi-Fi De o lista e entrar o Wi-Fi senha. Torneira **OKEY**.

Nota

Somente dígitos, letras e caracteres especiais são permitidos na senha.

5. Defina os parâmetros do Wi-Fi.

- Por padrão, o DHCP é habilitado. O sistema alocará o endereço IP, a máscara de sub-rede e o gateway automaticamente.
- Se desabilitar o DHCP, você deverá inserir o endereço IP, a máscara de sub-rede e o gateway manualmente.

6. Pressione OK para salvar as configurações e voltar para a guia Wi-Fi.

7. Pressione ESC para salvar os parâmetros de rede.

7.2.3 Configurar parâmetros ISUP

Configure os parâmetros ISUP e o dispositivo pode carregar dados através do protocolo ISUP.

Antes de começar

Verifique se o dispositivo está conectado a uma rede.

Passos

1. Selecione **Comm. ISUP →** .

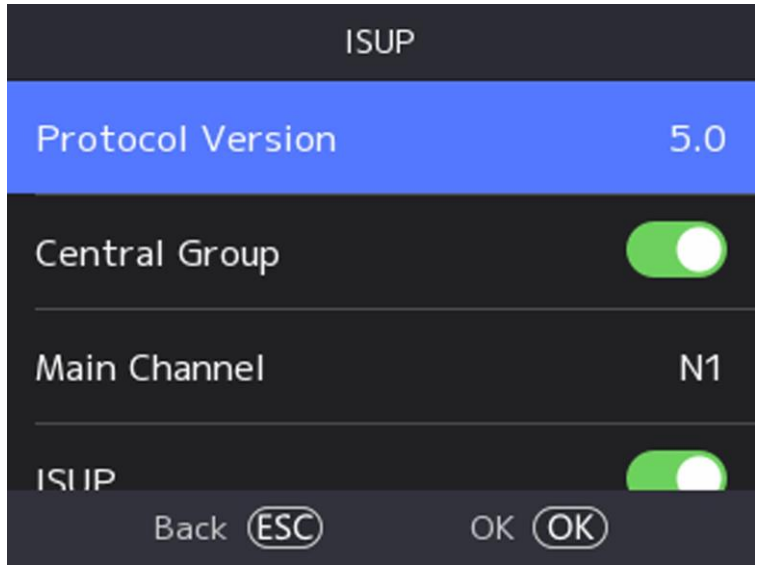


Figura 7-4 Configurações de ISUP

2. Habilite a função ISUP e defina os parâmetros do servidor ISUP.

Versão ISUP

Defina a versão ISUP de acordo com suas necessidades reais.

Grupo Central

Habilite o grupo central e os dados serão carregados no grupo central.

Canal Principal

Suporte N1 ou Nenhum.

ISUP

Habilite a função ISUP e os dados serão carregados através do protocolo ISUP.

Tipo de Endereço

Selecione um tipo de endereço de acordo com suas necessidades reais.

IP

Defina o endereço IP do servidor ISUP.

Porta

Defina a porta nº do servidor ISUP.

Nota

Nº da porta Intervalo: 1 a 65535.

ID do dispositivo

Defina o número de série do dispositivo.

Chave ISUP

Se você escolher V5.0, você deve criar uma conta e chave ISUP. Se você escolher outra versão, deverá criar apenas uma conta ISUP.

Nota

- Lembre-se da conta ISUP e da chave ISUP. Você deve inserir o nome da conta ou a chave quando o dispositivo deve se comunicar com outras plataformas via protocolo ISUP.
- Intervalo de teclas ISUP : 8 a 16 caracteres.

7.2.4 Acesso à plataforma

Você pode alterar o código de verificação do dispositivo e definir o endereço do servidor antes de adicionar o dispositivo ao cliente móvel Hik-Connect.

Antes de começar

Verifique se o dispositivo se conectou a uma rede.

Passos

1. Selecione **Comm.** (Comunicação) na página inicial para entrar na página Configurações de comunicação.
2. Na página Configurações de comunicação, selecione **Hik-Connect**.
3. Ativar **o Hik-Connect**
4. Insira **o IP do servidor**.
5. Crie o Código de **Verificação** e você precisa inserir o código de verificação ao gerenciar os dispositivos via **Hik-Connect**.

7.3 Gerenciamento de usuários

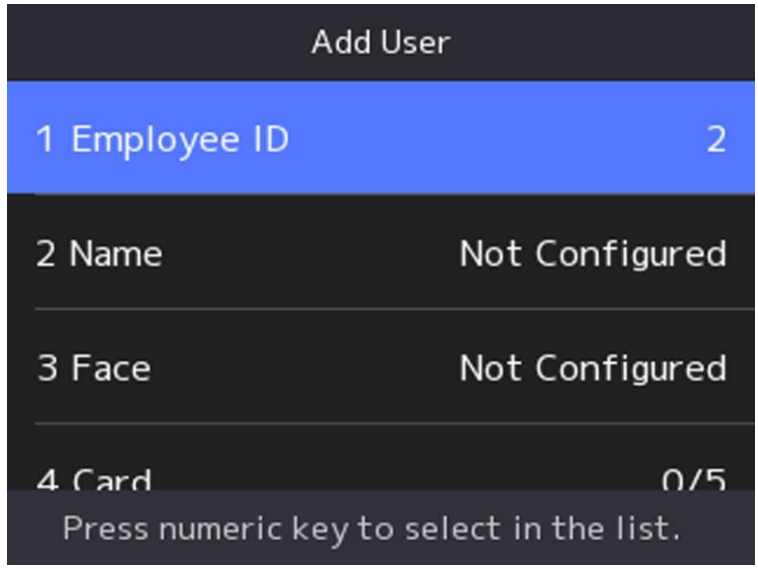
Na interface de gerenciamento de usuários, você pode adicionar, editar, excluir e pesquisar o usuário.

7.3.1 Adicionar administrador

O administrador pode efetuar login no back-end do dispositivo e configurar os parâmetros do dispositivo.

Passos

1. Toque longamente na página inicial e faça login no back-end.
2. Selecione Usuário → Adicionar Usuário para entrar na página **Adicionar Usuário**.



3. Editar o empregado ID.

Nota

- A ID do funcionário deve ter menos de 32 caracteres. E pode ser uma combinação de letras inferiores, letras superiores e números.
- O ID do funcionário não deve ser duplicado.

4. Selecione o campo Nome e insira o nome de usuário no teclado.

Nota

- Números, letras maiúsculas, letras minúsculas e caracteres especiais são permitidos no nome de usuário.
- Até 128 caracteres são permitidos no nome de usuário.

5. Opcional: adicione uma imagem de rosto, impressões digitais, cartões ou Pin para o usuário.

Nota

- Durante Detalhes sobre Adicionando a rosto imagem ver ***Adicionar Rosto Imagem*** .
- **Nota**

  Para obter detalhes sobre como adicionar uma impressão digital, consulte ***Adicionar impressão digital*** .
- Para obter detalhes sobre como adicionar um cartão , consulte ***Adicionar cartão*** .
- Para obter detalhes sobre como adicionar uma senha, consulte ***Exibir código PIN*** .

6. Opcional: defina o tipo de autenticação do usuário.

Nota

Para obter detalhes sobre como definir o tipo de autenticação, consulte ***Definir modo de autenticação*** .

7. Defina a função de usuário.

Administrador

O usuário é o administradortrator. Exceto para a função de presença normal, o usuário também pode entrar na página inicial para operar depois de autenticar a permissão.

Usuário Normal

O Usuário é o usuário normal. O usuário só pode autenticar ou participar da página inicial.

8. Pressione ESC e, em seguida, pressione OK para salvar as configurações.

7.3.2 Adicionar imagem de rosto

Adicione a imagem do rosto do usuário ao dispositivo. E o usuário pode usar a imagem do rosto para autenticar.

Passos

Nota

Até 500 fotos de rosto podem ser adicionadas.

1. Pressione longamente OK e faça login no dispositivo.

2. Selecione Usuário → Adicionar Usuário para entrar na página **Adicionar Usuário**.

3. Editar o empregado ID.

Nota

- A ID do funcionário deve ter menos de 32 caracteres. E pode ser uma combinação de letras inferiores, letras superiores e números.
- O ID do funcionário não deve ser duplicado.

4. Selecione o campo Nome e insira o nome de usuário no teclado.

Nota

- Números, letras maiúsculas, letras minúsculas e caracteres especiais são permitidos no nome de usuário.
- O nome de usuário sugerido deve estar dentro de 128 caracteres.

5. Selecione o campo Face para inserir a página de adição de imagem de rosto.

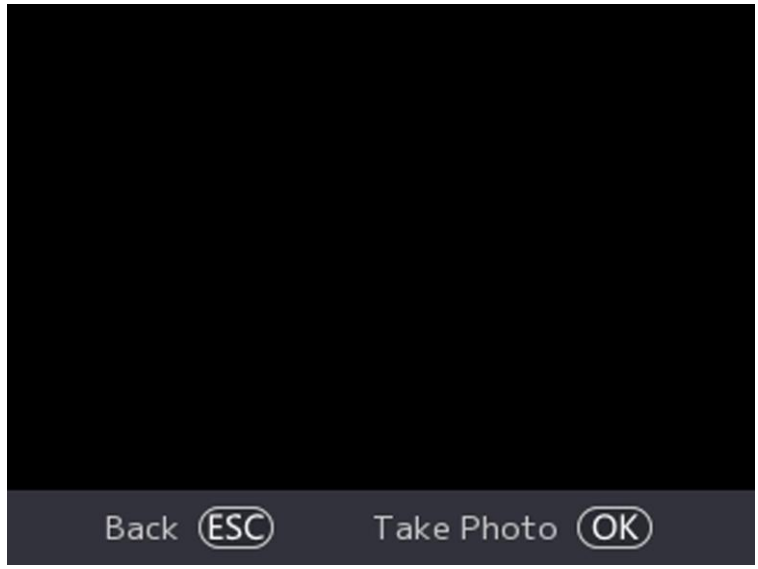


Figura 7-5 Adicionar imagem facial

6. Olhar em o câmera.

Nota

- Certifique-se de que a imagem do rosto está no contorno da imagem do rosto ao adicionar a imagem do rosto.
- Certifique-se de que a imagem do rosto capturada esteja em boa qualidade e seja precisa.
- Para obter detalhes sobre as instruções de adicionar imagens de rosto, consulte ***Dicas ao coletar/comparar imagens faciais*** .

Depois de adicionar completamente a imagem do rosto, uma imagem do rosto capturada será exibida no centro da página.

7. Pressione OK para salvar a imagem do rosto .

8. Opcional: pressione ESC para selecionar **Retomar** e ajustar a posição do rosto para adicionar a imagem do rosto novamente.

9. Defina a função de usuário.

Administrador

O usuário é o administrador. Exceto para a função de presença normal, o usuário também pode entrar na página inicial para operar depois de autenticar a permissão.

Usuário Normal

O Usuário é o usuário normal. O usuário só pode autenticar ou participar da página inicial.

10. Pressione ESC e, em seguida, pressione OK para salvar as configurações.

7.3.3 Adicionar impressão digital

Adicione uma impressão digital para o usuário e o usuário pode autenticar através da impressão digital adicionada.

Passos

Nota

- A função deve ser suportada pelo dispositivo.
- Até 1000 impressões digitais podem ser adicionadas.

1. Pressione longamente OK e faça login no dispositivo.
2. Pressione Usuário → Adicionar Usuário para entrar na página **Adicionar Usuário**.
3. Selecionar o Empregado ID campo e editar o empregado ID.

   Nota

   - A ID do funcionário deve ter menos de 32 caracteres. E pode ser uma combinação de letras inferiores, letras superiores e números.
   - O ID do funcionário não deve começar com 0 e não deve ser duplicado.
4. Selecione o campo Nome e insira o nome de usuário no teclado.

   Nota

   - Números, letras maiúsculas, letras minúsculas e caracteres especiais são permitidos no nome de usuário.
   - O nome de usuário sugerido deve estar dentro de 128 caracteres.
5. Selecione o campo Impressão digital para entrar na página Impressão digital.
6. Seguir o Instruções Para adicionar a impressão digital.

   Nota

   - A mesma impressão digital não pode ser adicionada repetidamente .
   - Até 10 impressões digitais podem ser adicionadas para um usuário.
   - Você também pode usar o software cliente ou o gravador de impressões digitais para gravar impressões digitais.

     Para obter detalhes sobre as instruções de digitalização de impressões digitais, consulte ***Dicas para digitalizar impressão digital*** .
7. Defina a função de usuário.

   Administrador

   O usuário é o administrador. Exceto para a função de presença normal, o usuário também pode entrar na página inicial para operar depois de autenticar a permissão.

   Usuário Normal

   O Usuário é o usuário normal. O usuário só pode autenticar ou participar da página inicial.
8. Pressione ESC e, em seguida, pressione OK para salvar as configurações.

7.3.4 Adicionar cartão

Adicione um cartão para o usuário e o usuário pode autenticar através do cartão adicionado.

Passos

Nota

O dispositivo suporta cartão EM ou cartão Mifare. O tipo de cartão suportado varia entre modelos diferentes.

1. Pressione longamente OK e faça login no dispositivo.
2. Selecione Usuário → Adicionar Usuário para entrar na página **Adicionar Usuário**.
3. Selecionar o Empregado ID campo e editar o empregado ID.

Nota

- A ID do funcionário deve ter menos de 32 caracteres. E pode ser uma combinação de letras inferiores, letras superiores e números.
- O ID do funcionário não deve ser duplicado.

4. Selecione o campo Nome e insira o nome de usuário no teclado.

Nota

- Números, letras maiúsculas, letras minúsculas e caracteres especiais são permitidos no nome de usuário.
- O nome de usuário sugerido deve estar dentro de 128 caracteres.

5. Selecione o campo Cartão e pressione OK para entrar na página Adicionar cartão.
6. Configure o cartão No.
   - Digite o cartão No. manualmente.
   - Apresente o cartão sobre a área de deslizamento do cartão para obter o cartão Não.

Nota

- O cartão nº. não pode estar vazio.
- Até 20 caracteres são permitidos no cartão No.
- O cartão nº. não pode ser duplicado.

7. Configure o tipo de cartão.
8. Defina a função de usuário.

   Administrador

   O usuário é o administrador. Exceto para a função de presença normal, o usuário também pode entrar na página inicial para operar depois de autenticar a permissão.

   Usuário Normal

   O Usuário é o usuário normal. O usuário só pode autenticar ou participar da página inicial.
9. Pressione ESC e, em seguida, pressione OK para salvar as configurações.

7.3.5 Ver código PIN

Adicione um código PIN para o usuário e o usuário pode autenticar através do código PIN.

Passos

1. Pressione longamente OK e faça login no dispositivo.
2. Selecione Usuário → Adicionar Usuário para entrar na página **Adicionar Usuário**.
3. Editar o empregado ID.

Nota

- A ID do funcionário deve ter menos de 32 caracteres. E pode ser uma combinação de letras inferiores, letras superiores e números.
- O ID do funcionário não deve ser duplicado.

4. Selecione o campo Nome e insira o nome de usuário no teclado.

Nota

- Números, letras maiúsculas, letras minúsculas e caracteres especiais são permitidos no nome de usuário.
- O nome de usuário sugerido deve estar dentro de 128 caracteres.

5. Selecione o campo PIN para exibir o código PIN.

Nota

O código PIN não pode ser editado. Ele só pode ser aplicado pela plataforma.

6. Defina a função de usuário.

Administrador

O usuário é o administrador. Exceto para a função de presença normal, o usuário também pode entrar na página inicial para operar depois de autenticar a permissão.

Usuário Normal

O Usuário é o usuário normal. O usuário só pode autenticar ou participar da página inicial.

7. Pressione ESC e, em seguida, pressione OK para salvar as configurações.

7.3.6 Definir modo de autenticação

Depois de adicionar a imagem do rosto, a senha ou outras credenciais do usuário, você deve definir o modo de autenticação e o usuário pode autenticar sua identidade por meio do modo de autenticação configurado.

Passos

1. Pressione longamente OK e faça login no dispositivo.
2. Selecione **Usuário → Adicionar Autenticação de → de Usuário. Configurações** .

3. Selecione Dispositivo ou Personalizado como o modo de autenticação.

Dispositivo

Se você quiser selecionar o modo de dispositivo, você deve definir o modo de autenticação de terminal na página Configurações de Controle de Acesso primeiro. Para obter detalhes, consulte *Definindo parâmetros de controle de acesso*.

Costume

Você pode combinar diferentes modos de autenticação de acordo com suas necessidades reais.

4. Pressione ESC para salvar as configurações.

7.3.7 Editar usuário

Depois de adicionar o usuário, você pode editá-lo.

Editar usuário

Na página Gerenciamento de Usuários, selecione um usuário na Lista de Usuários para entrar na página Informações do Usuário. Siga as etapas em ***Gerenciamento de usuários*** para editar os parâmetros do usuário. Pressione ESC para salvar as configurações.

Nota

A ID do funcionário não pode ser editada.

7.4 Gerenciamento de dados

Você pode excluir dados , importar dados e exportar dados.

7.4.1 Excluir dados

Excluir dados do usuário.

Na página inicial, selecione Dados → **Excluir** Dados → **Dados do Usuário** . Todos os dados do usuário adicionados no dispositivo serão excluídos.

7.4.2 Importar dados

Passos

1. Conecte uma unidade flash USB no dispositivo.

2. Na página inicial, toque em **Dados → Importar dados** .

3. Torneira **Utilizador Dados**, **Rosto Dados** ou **Acesso Controle Parâmetros** .

Nota

Os parâmetros de controle de acesso importados são arquivos de configuração do dispositivo.

4. Insira a senha criada ao exportar os dados. Se você não criar uma senha ao exportar os dados, deixe um espaço em branco na caixa de entrada e toque em **OK** imediatamente.

Nota

- Se você quiser transferir todas as informações do usuário de um dispositivo (Dispositivo A) para outro (Dispositivo B), exporte as informações do Dispositivo A para a unidade flash USB e, em seguida, importe da unidade flash USB para o Dispositivo B. Nesse caso, você deve importar os dados do usuário antes de importar a foto do perfil.
- O formato de unidade flash USB suportado é FAT32.
- As imagens importadas devem ser salvas na pasta (chamada enroll_pic) do diretório raiz e o nome da imagem deve ser seguir a regra abaixo:
  No._Name_Department_Employee de ID_Gender.jpg de cartão
- Se a pasta enroll_pic não puder salvar todas as imagens importadas, poderá criar outras pastas, chamadas enroll_pic1, enroll_pic2, enroll_pic3 enroll_pic4, no diretório raiz.
- A ID do funcionário deve ter menos de 32 caracteres. Pode ser uma combinação de letras inferiores, letras superiores e números. Ele não deve ser duplicado e não devecomeçar com 0.
- Os requisitos da foto facial devem seguir as regras abaixo: Ela deve ser tirada em visão de rosto inteiro, diretamente voltada para a câmera. Não use um chapéu ou cobertura de cabeça ao tirar a foto do rosto. O formato deve ser JPEG ou JPG.

7.4.3 Exportar dados

Passos

1. Conecte uma unidade flash USB no dispositivo.

2. Na página inicial, toque em **Dados → Exportar dados** .

3. Torneira **Rosto Dados**, **Acontecimento Dados**, **Utilizador Dados**, ou **Acesso Controle Parâmetros**.

Nota

Os parâmetros de controle de acesso exportados são arquivos de configuração do dispositivo.

4. Opcional: Criar a senha durante Exportadores. Quando você importação aqueles dados Para outro dispositivo você deve digitar a senha.

Nota

- O formato de unidade flash USB suportado é DB.
- O sistema suporta a unidade flash USB com o armazenamento de 1G a 32G. Verifique se o espaço livre da unidade flash USB é superior a 512M.
- Os dados do usuário exportados são um arquivo de banco de dados, que não pode ser editado.

7.5 Autenticação de identidade

Após a configuração de rede, a configuração dos parâmetros do sistema e a configuração do usuário, você pode voltar para a página inicial para autenticação de identidade. O sistema autenticará a pessoa de acordo com o modo de autenticação configurado.

7.5.1 Autenticar via credencial única

Defina o tipo de autenticação do usuário antes da autenticação. Para obter detalhes, consulte ***Definir modo de autenticação*** . Autentice rosto, impressão digital, cartão ou PIN.

Rosto

Fique virado para a frente na câmara e inicie a autenticação através do face.

Impressão digital

Coloque a impressão digital inscrita no módulo de impressão digital e inicie a autenticação via fingerprint.

Cartão

Apresente o cartão na área de passagem do cartão e inicie a autenticação via cartão.

Nota

O cartão pode ser um cartão IC normal ou um cartão criptografado.

Código PIN

Introduza o código PIN para autenticar através do código PIN.

Se a autenticação for concluída, um prompt "Autenticado" será exibido.

7.5.2 Autenticar por meio de várias credenciais

Antes de começar

Defina o tipo de autenticação do usuário antes da autenticação. Para obter detalhes, consulte ***Definir modo de autenticação*** .

Passos

1. Se o modo de autenticação for Cartão e Rosto, Senha e Rosto, Cartão e Senha, Cartão e Rosto e Impressão Digital , autentique qualquer credencial de acordo com as instruções na visualização ao vivo página.

Nota

- O cartão pode ser um cartão IC normal ou um cartão criptografado.

2. Depois que a credencial anterior for autenticada, continue autenticando outras credenciais.

Nota

- Para obter informações detalhadas sobre a digitalização de impressão digital, consulte *Dicas para digitalizar impressão digital*.
- Para obter informações detalhadas sobre como autenticar rosto, consulte *Dicas ao coletar/comparar imagem facial*.

Se a autenticação for bem-sucedida, o prompt "Autenticado" será exibido.

7.6 Configurações básicas

Você pode definir a voz, o tempo, o sono (s), o idioma, a luz do suplemento, o número da comunidade, o número do edifício e a unidade nº .

Pressione longamente OK e faça login no dispositivo. Selecione **Básico** para entrar na página Configurações do Sistema. Em seguida, select **Basic** para entrar na página Configurações básicas.

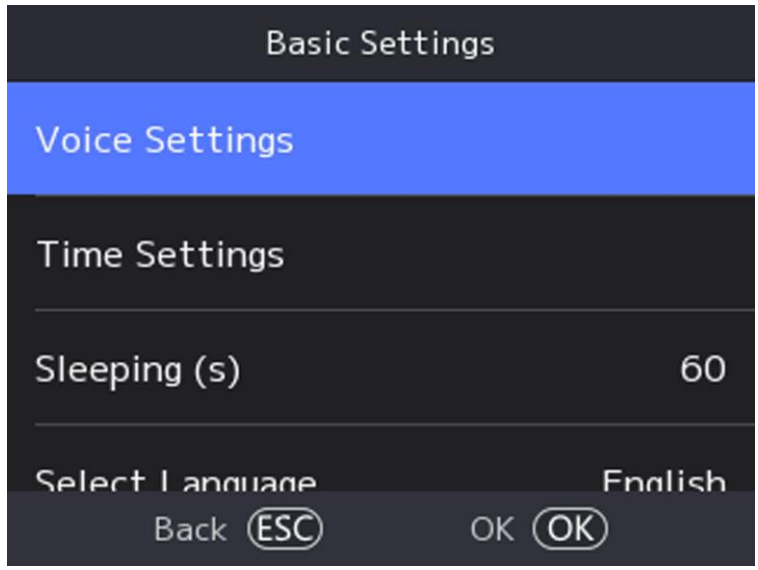


Figura 7-6 Página de configurações básicas

Configurações de voz

Você pode ativar/desativar a função de voz.

Configurações de Hora

Defina o fuso horário , a hora do dispositivo e o horário de verão.

Dormindo (s)

Defina o(s) tempo(s) de espera de suspensão do dispositivo. Por exemplo, quando você estiver na página inicial e se você definir o tempo de suspensão para 30 s, o dispositivo entrará em repouso após 30 s sem qualquer operação.

Nota

20 s a 999 s estão disponíveis para configuração.

Selecione o idioma

Selecione o idioma de acordo com as necessidades reais.

Suplemento Light

Defina o modo de luz branca, brilho, hora de início e hora de término.

Nº da Comunidade

Defina a comunidade instalada do dispositivo No.

Edifício nº.

Defina o dispositivo instalado edifício No.

Unidade nº.

Defina a unidade instalada do dispositivo No.

7.7 Definir parâmetros biométricos

Você pode personalizar os parâmetros faciais para melhorar o desempenho do reconhecimento facial. Os parâmetros configuráveis incluem o modo de aplicação, o nível de vivacidade do rosto, a distância de reconhecimento facial, o intervalo de reconhecimento facial, o nível de segurança face 1:N, o nível de segurança face 1:1 e o rosto com detecção de máscara.

Pressione longamente OK e faça login no dispositivo. Selecione **Básico** para entrar na página Configurações do Sistema. Em seguida, selecione
Biometria para entrar na página Configurações de biometria.

Tcapaz 7-1 Face Picture Parâmetros

Parâmetro	Descrição
Modo de Aplicação	Selecione outros ou internos de acordo com o ambiente real.
Nível de vivacidade do rosto	Depois de habilitar a função antifalsificação facial, você pode definir o nível de segurança correspondente ao executar a autenticação facial ao vivo.
Distância de reconhecimento facial	Defina a distância válida entre o usuário e a câmera ao autenticar.
Intervalo de Reconhecimento Facial	O intervalo de tempo entre dois reconhecimentos faciais contínuos durante a autenticação. **Nota** Você pode inserir o número de 1 a 10.

Parâmetro	Descrição
Face 1:N Nível de Segurança	Defina o limite de correspondência ao autenticar por meio do modo de correspondência 1: N. Quanto maior o valor, menor a taxa de aceitação falsa e maior a taxa de falsa rejeição.
Nível de segurança Face 1:1	Defina o limite de correspondência ao autenticar por meio do modo de correspondência 1 :1. Quanto maior o valor, menor a taxa de aceitação falsa e d, maior a taxa de falsa rejeição.
Detecção de Rosto com Máscara	Depois de ativar o rosto com detecção de máscara, o sistema reconhecerá o rosto capturado com a imagem da máscara. Você pode definir o rosto com máscara e rosto 1: 1 nível e 1: N nível e a estratégia. **Lembrete de Uso** Se a pessoa não usar uma máscara facial ao autenticar, o dispositivo solicitará uma notificação e a porta será aberta. **Deve usar** Se a pessoa não usar uma máscara facial ao autenticar, o dispositivo solicitará uma notificação e a porta será fechada. **Nenhum** Se a pessoa não usar uma máscara facial ao autenticar, o dispositivo não solicitará uma notificação.

7.8 Definir parâmetros de controle de acesso

Você pode definir as permissões de controle de acesso, incluindo as funções do modo de autenticação, habilitar cartão NFC, contato de porta, duração (s) aberta (s) e intervalo (s) de autenticação (s).

Na home page, selecione **ACS** (Configurações de Controle de Acesso) para entrar na página Configurações de Controle de Acesso . Edite os parâmetros de controle de acesso nesta página.

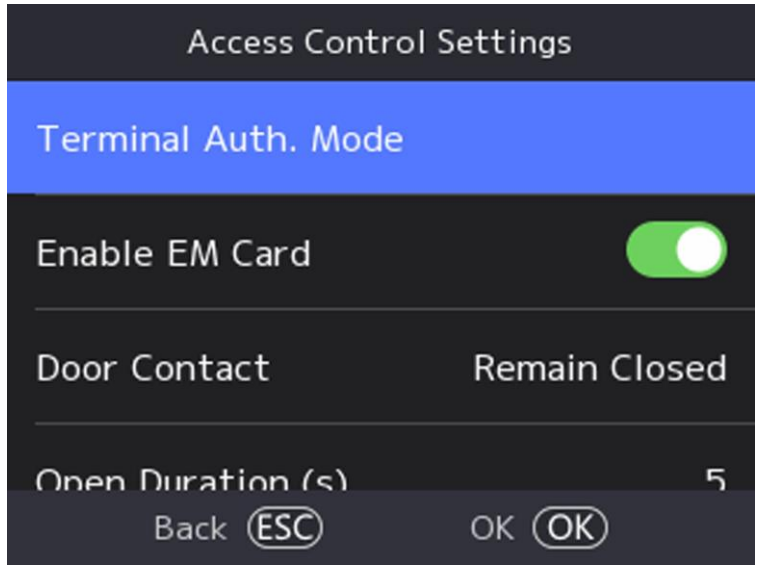


Figura 7-7 Parâmetros de controle de acesso

As descrições dos parâmetros disponíveis são as seguintes:

Tabela 7-2 Descrições de parâmetros de controle de acesso

Parâmetro	Descrição
Autenticação terminal. Modo	Selecione o modo de autenticação do terminal de reconhecimento facial. Você também pode personalizar o modo de autenticação. **Nota** • Apenas o dispositivo com o módulo de impressão digital suporta a função relacionada com a impressão digital. • Os produtos de reconhecimento biométrico não são completamente aplicáveis a ambientes antifalsificação. Se você precisar de um nível de segurança mais alto, use vários modos de autenticação. • Se você adotar vários modos de autenticação, deverá autenticar outros métodos antes de autenticar o rosto.
Ativar cartão NFC	Ative a função e você pode apresentar o cartão NFC para autenticar.
Contato da Porta	Você pode selecionar "Permanecer Aberto" ou "Permanecer Fechado" de acordo com suas necessidades reais. Por padrão, é "Permanecer Fechado".

Parâmetro	Descrição
Duração Aberta	Defina a duração do destravamento da porta. Se a porta não for aberta para o tempo definido, a porta será trancada. Intervalo de tempo disponível com travamento da porta: 1 a 255s.
Intervalo de autenticação	Defina o intervalo de autenticação do dispositivo. Intervalo de intervalo de autenticação disponível: 0 a 65535.

7.9 Configurações de status de horário e presença

Você pode definir o modo de atendimento como check-in, check-out, break-out, arrombamento , hora extra dentro e horas extras de acordo com sua situação real.

Nota

A função deve ser usada cooperativamente com função de tempo e presença no software cliente.

7.9.1 Desativar o Modo de Presença através do Dispositivo

Desative o modo de presença e o sistema não exibirá o status de presença na página inicial.

Selecione T&A para entrar na página Status de T& A.

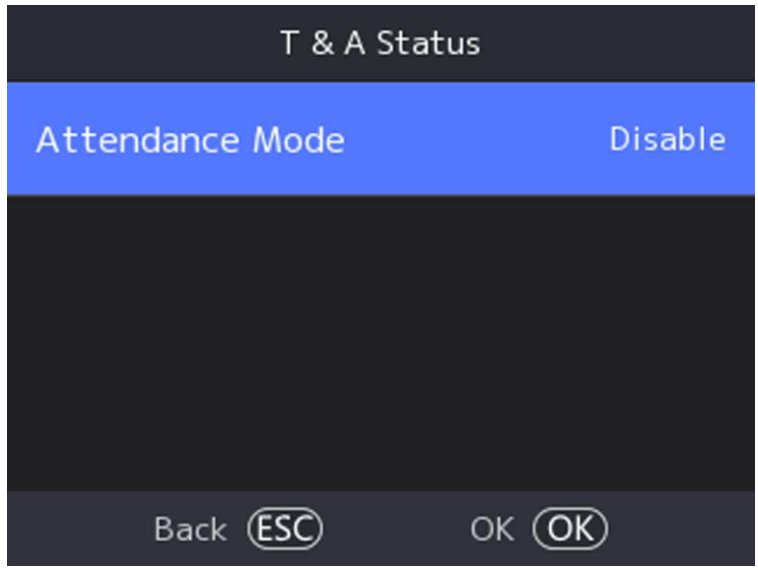


Figura 7-8 Desabilitar o modo de presença

Defina o **Modo de Atendimento** como **Desabilitar**.

Você não exibirá ou configurará o status de presença na página inicial. E o sistema seguirá a regra de assiduidade que configurou na plataforma.

7.9.2 Definir Atendimento Manual via Dispositivo

Defina o modo de presença como manual e você deve selecionar um status manualmente ao receber presença.

Antes de começar

Adicione pelo menos um usuário e defina o modo de autenticação do usuário. Para obter detalhes, consulte *Gerenciamento de usuários*.

Passos

1. Selecione T&A para entrar na página Status de T& A.
2. Defina o **Modo de Atendimento** como **Manual**.

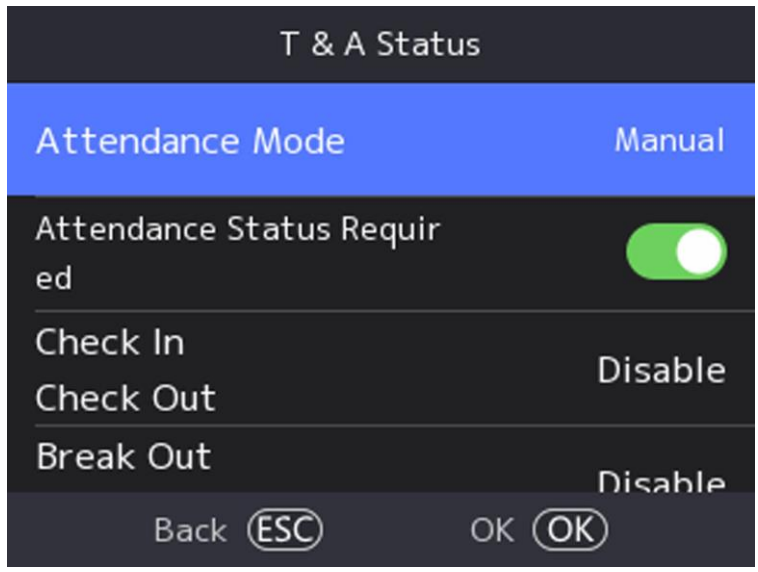


Figura 7-9 Modo de atendimento manual

3. Habilite o **status de presença necessário**.
4. Habilitar a grupo de assiduidade estado.

Nota

A Propriedade de Assiduidade não será alterada.

5. **Opcional:** selecione um status e altere seu nome, se necessário.
   O nome será exibido na página Status de T&A e na página de resultados da autenticação.

Resultado

Você deve selecionar um status de presença manualmente após a autenticação.

Nota

Se você não selecionar um status, a autenticação falhará e não será marcada como uma presença válida.

7.9.3 Definir Atendimento Automático via Dispositivo

Defina o modo de presença como automático e você pode definir o status de presença e sua agenda disponível. O sistema alterará automaticamente o status de presença de acordo com a programação configurada.

Antes de começar

Adicione pelo menos um usuário e defina o modo de autenticação do usuário. Para obter detalhes, consulte *Gerenciamento de usuários*.

Passos

1. Toque em Status **de T**&A para entrar na página **Status** de T& A.
2. Defina o **Modo de Atendimento** como **Automático**.

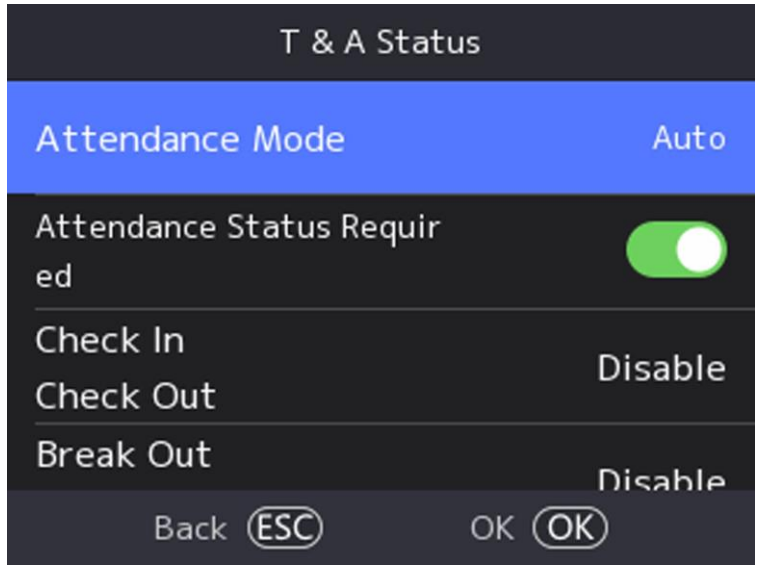


Figura 7-10 Modo de atendimento automático

3. Habilite a função **Status de Presença Necessária**.
4. Habilitar a grupo de assiduidade estado.

Nota

A Propriedade de Assiduidade não será alterada.

5. **Opcional:** selecione um status e altere seu nome, se necessário.
   O nome será exibido na página Status de T&A e na página de resultados da autenticação.
6. Defina a agenda do status.
   1) Selecione **Agendamento de presença**.
   2) Selecione Segunda-feira, terça-feira, **quarta-feira**, **quinta-feira**, **sexta-feira**, sábado ou domingo.

3) Defina a hora de início do dia do status de presença selecionado.
4) Pressione OK.
5) Repita os passos 1 a 4 de acordo com as suas necessidades reais.

Nota

O status de presença será válido dentro da programação configurada.

Resultado

Quando você autentica na página inicial, a autenticação será marcada como o status de presença configurado de acordo com o sche dule configurado.

Exemplo

Se definir o Break **Out** como segunda-feira 11:00 e **Break In** como segunda-feira 12:00, a autenticação do usuário válido de segunda-feira 11:00 a 12:00 será marcada como quebra.

7.9.4 Definir Atendimento Manual e Automático via Dispositivo

Defina o modo de atendimento como **Manual** e **Automático**, e o sistema alterará automaticamente o status de presença de acordo com a programação configurada. Ao mesmo tempo, você pode alterar manualmente o status de presença após a autenticação.

Antes de começar

Adicione pelo menos um usuário e defina o modo de autenticação do usuário. Para obter detalhes, consulte *Gerenciamento de usuários*.

Passos

1. Selecione T&A para entrar na página Status de T& A.
2. Defina o **Modo de Atendimento** como **Manual e Automático**.

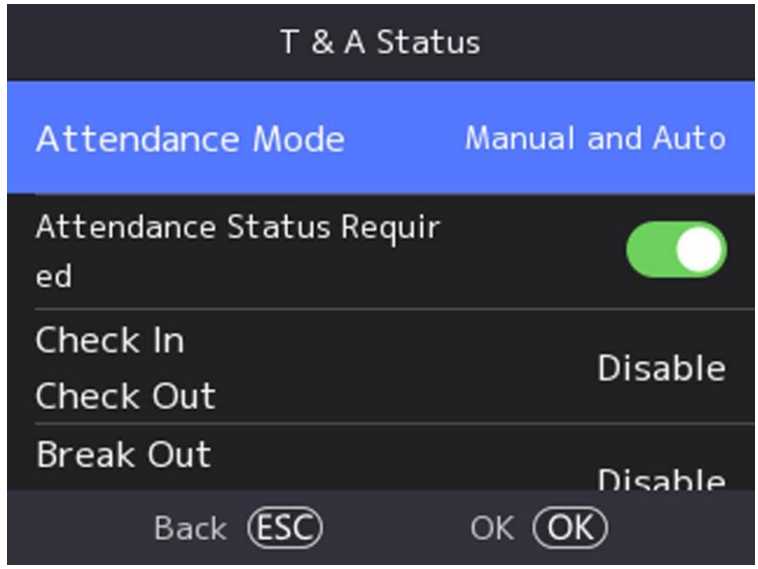


Figura 7-11 Modo manual e automático

3. Habilite a função **Status de Presença Necessária**.
4. Habilitar a grupo de assiduidade estado.

Nota

A Propriedade de Assiduidade não será alterada.

5. **Opcional:** selecione um status e altere seu nome, se necessário.
   O nome será exibido na página Status de T&A e na página de resultados da autenticação.
6. Defina a agenda do status.
   1) Selecione **Agendamento de presença**.
   2) Selecione Segunda-feira, terça-feira, **quarta-feira**, **quinta-feira**, **sexta-feira**, sábado ou domingo.
   3) Defina a hora de início do dia do status de presença selecionado.
   4) Pressione OK.
   5) Repita os passos 1 a 4 de acordo com as suas necessidades reais.

Nota

O status de presença será válido dentro da programação configurada.

Resultado

Na página inicial e autenticar. A autenticação será marcada como o status de presença configurado de acordo com a programação. Se você tocar no ícone de edição na guia de resultados, poderá selecionar um status a ser obtido manualmente, a autenticação será marcada como o status de presença editado.

Exemplo

Se definir o Break **Out** como segunda-feira 11:00 e **Break In** como segunda-feira 12:00, a autenticação do usuário válido de segunda-feira 11:00 a 12:00 será marcada como quebra.

7.10 Manutenção do Sistema

Você pode visualizar as informações e a capacidade do sistema do dispositivo. Você também pode atualizar o dispositivo, restaurar o sistema para as configurações de fábrica, configurações padrão e reiniciar o sistema.

Pressione longamente OK e faça login no dispositivo. Selecione **Maint.** para entrar na página Manutenção do Sistema.

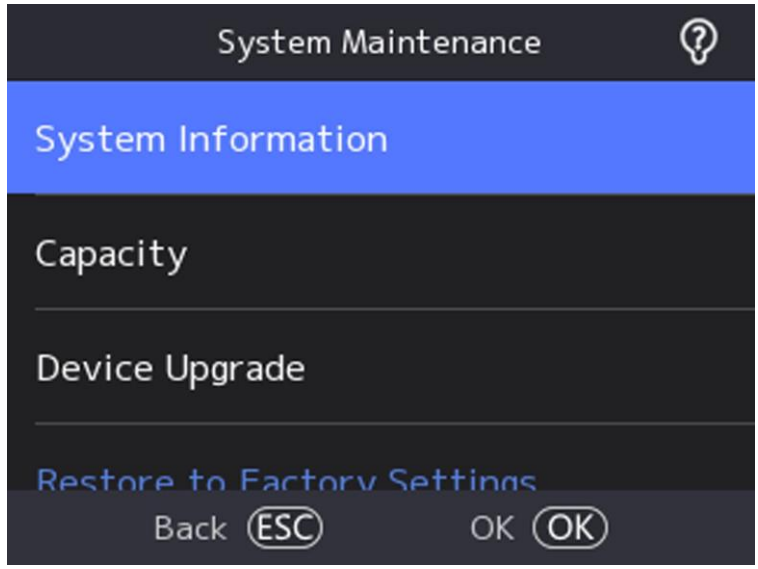


Figura 7-12 Página de manutenção

Informações do Sistema

Você pode visualizar as informações do dispositivo, incluindo modelo do dispositivo, número de série, versão do firmware, endereço MAC, dados de produção e licença de código-fonte aberto.

Nota

A página pode variar de acordo com diferentes modelos de dispositivos. Refere-se à página real para obter detalhes.

Capacidade

Você pode visualizar o número de usuários, a imagem do rosto, o cartão e o evento.

Nota

Partes dos modelos de dispositivos suportam a exibição do número da impressão digital. Refere-se à página real para obter detalhes.

Atualização do dispositivo

Conecte a unidade flash USB na interface USB do dispositivo. Selecione **Atualizar → OK** e o dispositivo lerá o arquivo *digicap.dav* na unidade flash USB para iniciar a atualização.

Restaurar para as configurações do ator F

Todos os parâmetros serão restaurados para as configurações de fábrica. O sistema será reinicializado para entrar em vigor.

Restaurar para as configurações padrão

Todos os parâmetros, exceto as configurações de comunicação, informações de usuário importadas remotamente, serão restaurados para as configurações padrão. O sistema será reinicializado para entrar em vigor.

Reinicializar

O dispositivo será reinicializado após a confirmação.

Selecione , pressione longamente OK e digite a senha de administrador para exibir as informações de versão do dispositivo.

Capítulo 8 Configurar o dispositivo através do navegador móvel

8.1 Login

Você pode fazer login via navegador móvel.

Nota

- Partes do modelo suportam configurações de Wi-Fi.
- Verifique se o dispositivo está ativado.

Obtenha o endereço IP do dispositivo depois que o Wi-Fi estiver habilitado. Verifique se o segmento IP do dispositivo e do computador são os mesmos. Para obter detalhes, consulte ***Definir parâmetros de Wi-Fi*** .

Digite o endereço IP do dispositivo na barra de endereços do navegador móvel e pressione **Enter** para entrar na página de login.

Insira o nome de usuário do dispositivo e a senha. Toque em **Login**.

8.2 Evento de Pesquisa

Toque em **Pesquisar** para entrar na página Pesquisar.

Insira as condições de pesquisa, incluindo o ID do funcionário, o nome, o número do cartão, a hora de início e a hora de término e toque em **Pesquisar**.

Nota

Suporte a pesquisa de nomes dentro de 32 dígitos.

8.3 Gerenciamento de usuários

Você pode adicionar, editar, excluir e pesquisar usuários por meio do navegador da Web móvel.

Passos

1. Toque em **Usuário** para entrar na página de configurações.

2. Adicionar usuário.

1) Toque**+**.

2) Defina os seguintes parâmetros.

ID do funcionário

Insira o ID do funcionário. A ID do funcionário não pode ser 0 ou exceder 32 caracteres. Pode ser uma combinação de letras maiúsculas, minúsculas e números.

Nome

Digite o nome. O nome suporta números, letras maiúsculas e minúsculas e caracteres. Recomenda-se que o nome esteja dentro de 32 caracteres.

Função de usuário

Selecione o seu usuário role.

Andar No. /Room No.

Entre no piso No./room No.

Rosto

Adicionar imagem de rosto. Toque em **Rosto**, toque em **Importar** e selecione o modo para importar o rosto.

Nº do cartão

Digite o cartão No.

Impressão digital

Adicione impressão digital. Toque em Impressão digital, toque em **+** e adicione impressão digital através do módulo de impressão digital.

Data de início/data de término

Defina Data de **Início** e **Data** de **Término** da permissão do usuário.

Administrador

Se o usuário precisar ser definido como administrador, você poderá habilitar **Administrador**.

Tipo de autenticação

Defina o tipo de autenticação.

3) Toque em **Salvar**.

3. Toque no usuário que precisa ser editado na lista de usuários para editar as informações.

4. Toque no usuário que precisa ser excluído na lista de usuários e toque para excluir o usuário.

5. Você pode pesquisar o usuário inserindo o ID ou o nome do funcionário na barra de pesquisa.

8.4 Configuração

8.4.1 Exibir informações do dispositivo

Você pode visualizar o nome do dispositivo, número do dispositivo, idioma, modelo, número de série, versão, capacidade do dispositivo , etc.

Toque em **Configuração** → Sistema → **Configurações do Sistema → Informações Básicas** , para entrar na página de configurações.

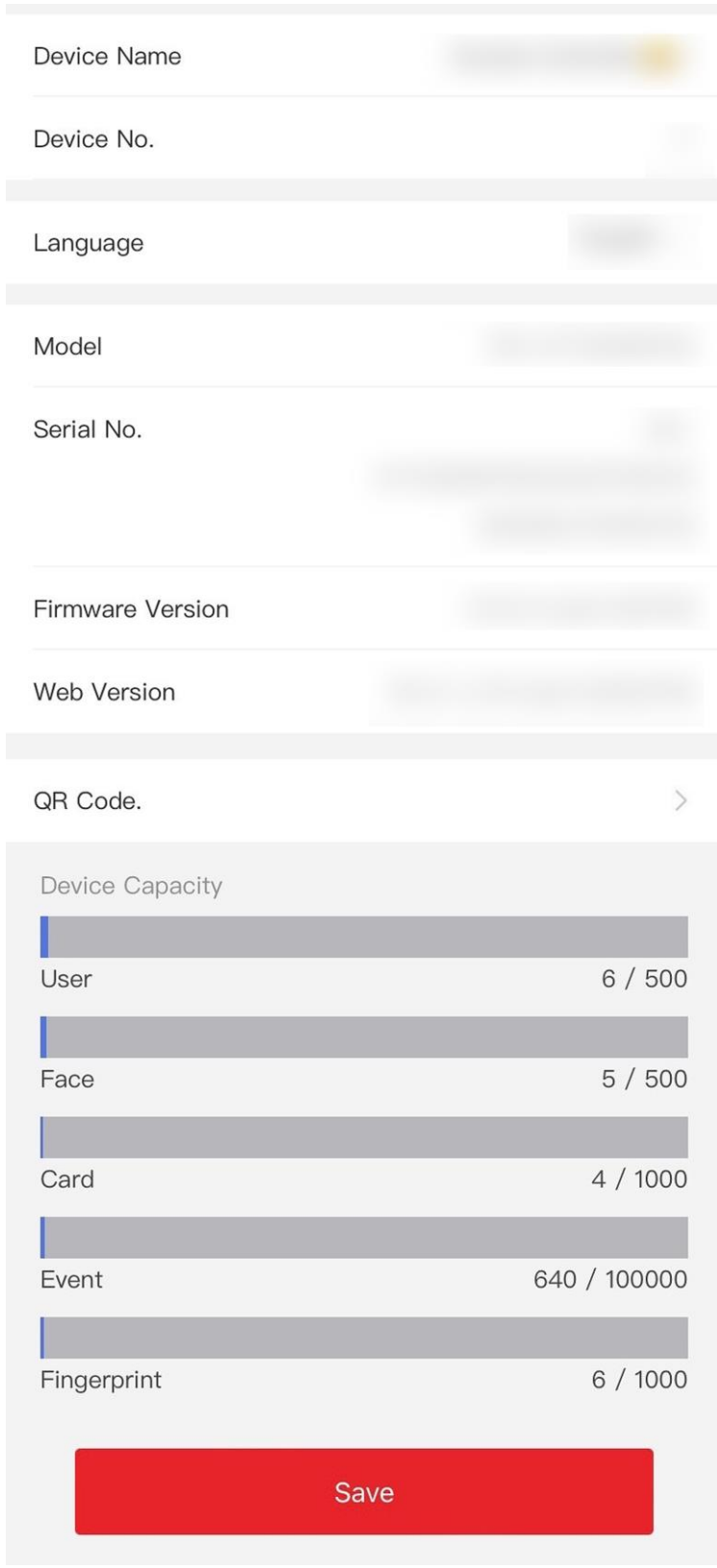


Figura 8-1 Informações do dispositivo

Você pode visualizar o nome do dispositivo, número do dispositivo, idioma, modelo, número de série, versão, capacidade do dispositivo , etc.

8.4.2 Configurações de Hora

Defina o fuso horário, a sincronização de horário. e tempo exibido.

Toque em **Configuração** → Sistema → Configurações **do Sistema** → **Configurações de Tempo** para entrar na página de configurações.

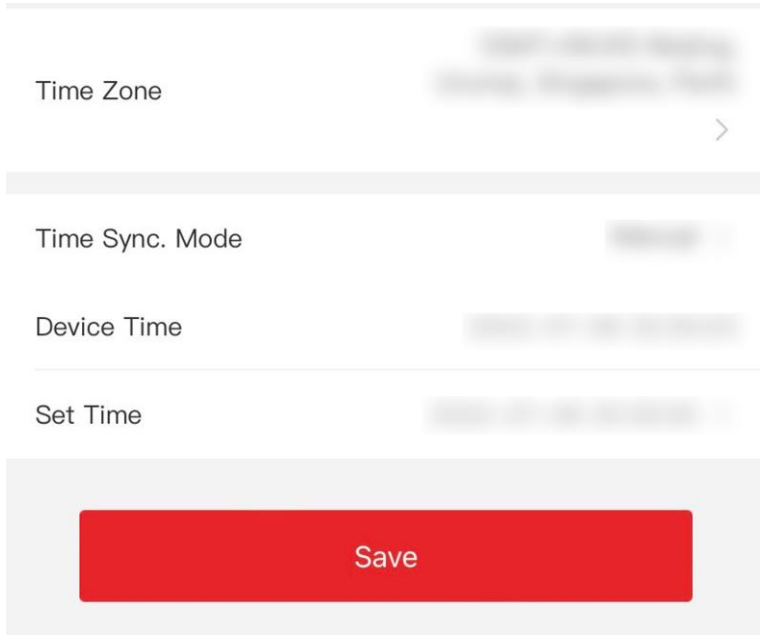


Figura 8-2 Configurações de tempo

Toque em **Salvar** para salvar as configurações.

Fuso Horário

Selecione o fuso horário onde o dispositivo está localizado na lista suspensa.

Sincronização de

Tempo. Manual do

modo

Por padrão, a hora do dispositivo deve ser sincronizada manualmente. Você pode definir a hora do dispositivo manualmente.

NTP

Defina o endereço IP, a porta nº e o intervalo do servidor NTP.

8.4.3 Definir horário de verão

Passos

1. Toque em **Configuração** → Sistema → **Configurações do Sistema** → **horário de verão** , para entrar

na página de configurações.

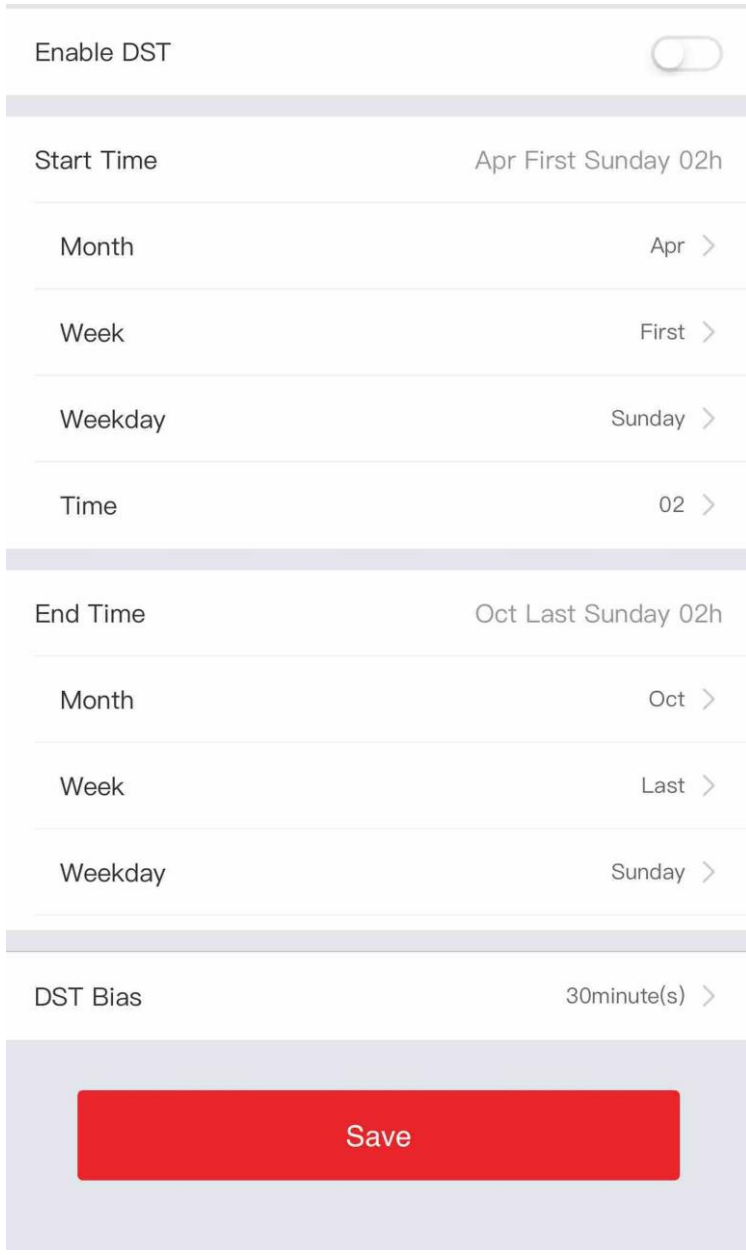


Figura 8-3 DST

2. Toque em **Ativar horário de verão**.
3. Defina a hora de início, a hora de término e o viés do horário de verão.
4. Toque em **Salvar**.

8.4.4 Exibir licença de software de código aberto

Toque em **Configuração** → Sistema → **Configurações** do **Sistema → Sobre** e toque em **Exibir Licenças** para exibir a licença do dispositivo.

8.4.5 Gerenciamento de usuários

Passos

1. Toque em **Configuração** → **Sistema** → **Gerenciamento de Usuários** → **administrador** → **Modificar Senha** para entrar na página de configurações.
2. Digite a senha antiga e crie uma nova senha.
3. Confirme a nova senha.
4. Torneira **OKEY**.

Nota

A força da senha do dispositivo pode ser verificada automaticamente. É altamente recomendável que você altere a senha de sua própria escolha (usando de 8 a 16 caracteres, incluindo pelo menos dois tipos de categorias a seguir: 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, alterando a senha mensal ou semanalmente pode proteger melhor seu produto.

8.4.6 Atualização e manutenção

Reinicialize o dispositivo, restaure os parâmetros do dispositivo, atualize a versão do dispositivo e desvincule o aplicativo.

Dispositivo de reinicialização

Toque em **Configuração** → **Manutenção do Sistema →** . Toque em **Reinicializar** para reiniciar o dispositivo.

Melhoramento

Toque em **Configuração → Manutenção do Sistema →** .
Se o dispositivo tiver sido conectado ao Hik-Connect e à rede, quando houver um novo pacote de instalação no Hik-Connect, você poderá tocar em **Atualizar** após a Atualização Online para atualizar o sistema do dispositivo.

Nota

Não desligue durante a atualização.

Restaurar parâmetros

Toque em **Configuração → Manutenção do Sistema →** .

Inadimplência

O dispositivo será restaurado para as configurações padrão, exceto para o endereço IP do dispositivo e as informações do usuário.

Restaurar tudo

Todos os parâmetros serão restaurados para as configurações de fábrica. Você deve ativar o dispositivo antes do uso.

Desvincular

Toque em **Configuração** → **Manutenção do Sistema** → . Toque em **Desvincular** para desvincular o aplicativo.
Depois de desvincular a conta APP, você não pode operar via APP.

8.4.7 Configurações de segurança

Você pode definir o SSH e o HTTP de acordo com as necessidades reais.

Toque em **Configuração** → **Segurança do Sistema** → , para entrar na página de configurações. Marque **Ativar** para habilitar o SSH.

Marque Habilitar para habilitar o HTTP.

8.4.8 Configurações de rede

Você pode definir a porta e os parâmetros Wi-Fi.

Definir parâmetros de Wi-Fi

Defina os parâmetros Wi-Fi para a conexão sem fio do dispositivo.

Passos

Nota

A função deve ser suportada pelo dispositivo.

1. Toque em **Configuração** → **Rede** → **Configurações Básicas** → **Wi-Fi** para entrar na página de configurações.
2. **Marque Ativar Wi-Fi**.

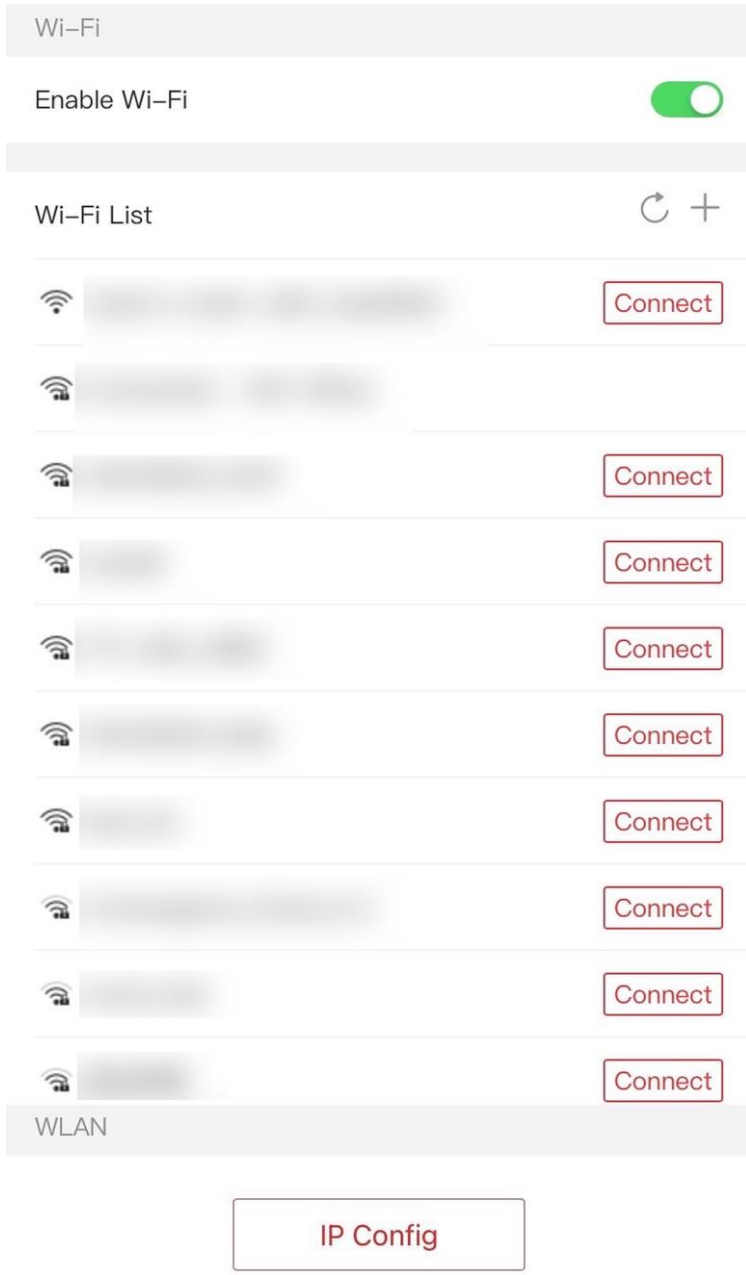


Figura 8-4 Wi-Fi

3. Adicione Wi-Fi.
1) Toque em **+**.

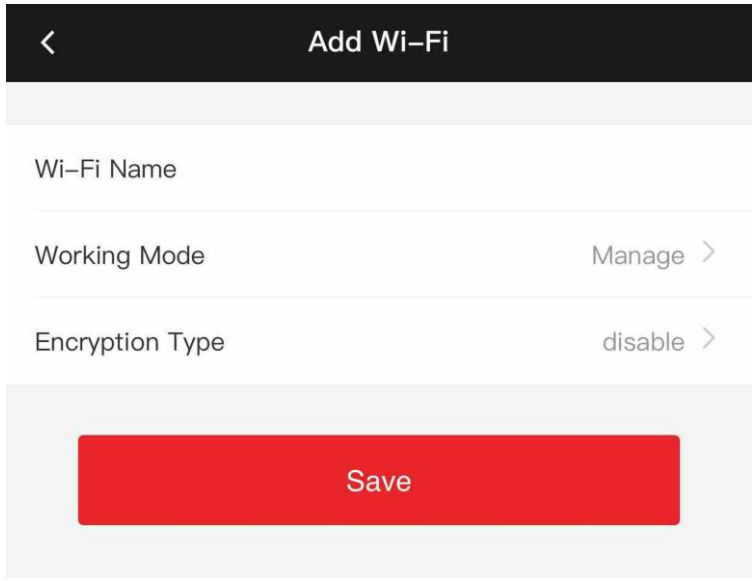


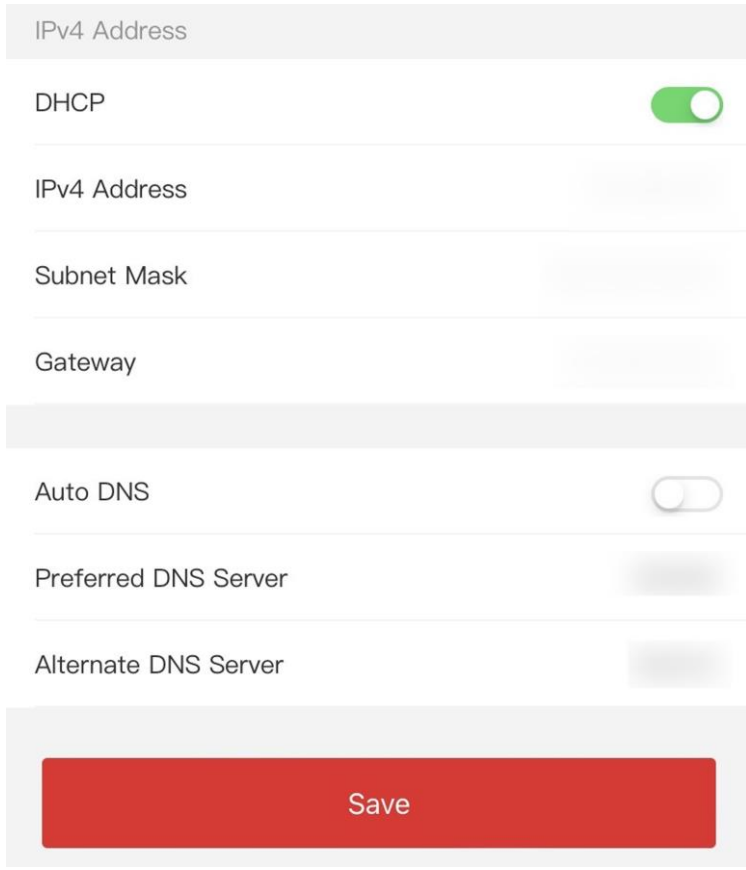
Figura 8-5 Adicionar Wi-Fi

2) Insira **Nome** do Wi-Fi e **Senha do Wi-Fi** e selecione **Modo de Trabalho** e Tipo **de Criptografia**.
3) Toque em **Salvar**.

4. Selecione o nome do Wi-Fi e toque em **Conectar**.

5. Digite a senha e toque em **Salvar**.

6. Defina parâmetros WLAN.



1) Defina o endereço IP, a máscara de sub-rede e o gateway. Ou habilite o DHCP e o sistema alocará o endereço IP, a máscara de sub-rede e o gateway automaticamente.
2) Defina os parâmetros DNS. Você pode habilitar a obtenção automática de DNS , definir o servidor DNS preferencial e o servidor DNS alternativo.
3) Toque em **Salvar**.

Definir parâmetros de porta

Você pode definir o HTTP, RTSP, HTTPS, e Server de acordo com as necessidades reais ao acessar o dispositivo via rede.

Toque em **Configuração** → **Rede** → **Configurações Básicas** → **Porta** , para entrar na página de configurações.

Correio HTTP

Refere-se à porta através da qual o navegador acessa o dispositivo.

RTSP

Refere-se à porta do protocolo de streaming em tempo real.

HTTPS (em inglês)

Defina o HTTPS para acessar o navegador. O certificado é necessário ao acessar.

Servidor

Refere-se à porta através da qual o cliente adiciona o dispositivo.

Acesso à plataforma

O acesso à plataforma oferece uma opção para gerenciar os dispositivos via plataforma.

Passos

1. Torneira **Configuração → Rede → Avançado → Caminhada-Conexão** Para entrar o Configurações página.

Nota

Hik-Connect é um aplicativo para dispositivos móveis. Com o aplicativo, você pode visualizar a imagem ao vivo do dispositivo, receber notificação de alarme e assim por diante.

2. **Marque Ativar** para ativar a função.
3. Entrar o servidor endereço e riacho encriptação.

Nota

6 a 12 letras (a a z, A a Z) ou números (0 a 9), diferenciando maiúsculas de minúsculas. Recomenda-se que você use uma combinação de pelo menos 8 letras ou números.

4. Você pode visualizar o **Status do Registro** e **o Código QR do Dispositivo**.
5. Toque em **Salvar** para ativar as configurações.

Configurar parâmetros ISUP

Defina os parâmetros ISUP para acessar o dispositivo via protocolo ISUP.

Passos

Nota

A função deve ser suportada pelo dispositivo.

1. Toque em **Configuração → ISUP Avançado de → de Rede →** .
2. **Marque Ativar**.
3. Pôr o ISUP Versão IP Endereço Porta e Conta.

Nota

Se você selecionar 5.0 como a versão, você deve definir a chave de criptografia também.

4. Defina o Grupo Central.

Grupo Centro

Selecione um grupo central na lista suspensa.

Canal Principal/Canal de Backup

O dispositivo se comunicará com o centro através do canal principal. Quando a exceção ocorre no canal principal, o dispositivo e o centro se comunicarão entre si por meio do canal de backup.

5. Toque em **Salvar** para salvar as configurações.

Escuta HTTP

Você pode definir os parâmetros de escuta HTTP.

Passos

1. Toque em **Configuração → Rede → Escuta Avançada → HTTP** .

2. Edite o IP de destino ou o nome de domínio, a URL e a porta.

3. Opcional: toque em **Padrão** para redefinir o IP ou o nome de domínio de destino.

4. Toque em **Salvar**.

8.4.9 Configurações gerais

Definir parâmetros de autenticação

Defina parâmetros de autenticação.

Passos

1. Toque em **Configuração → Configurações Gerais → Configurações de Autenticação** .

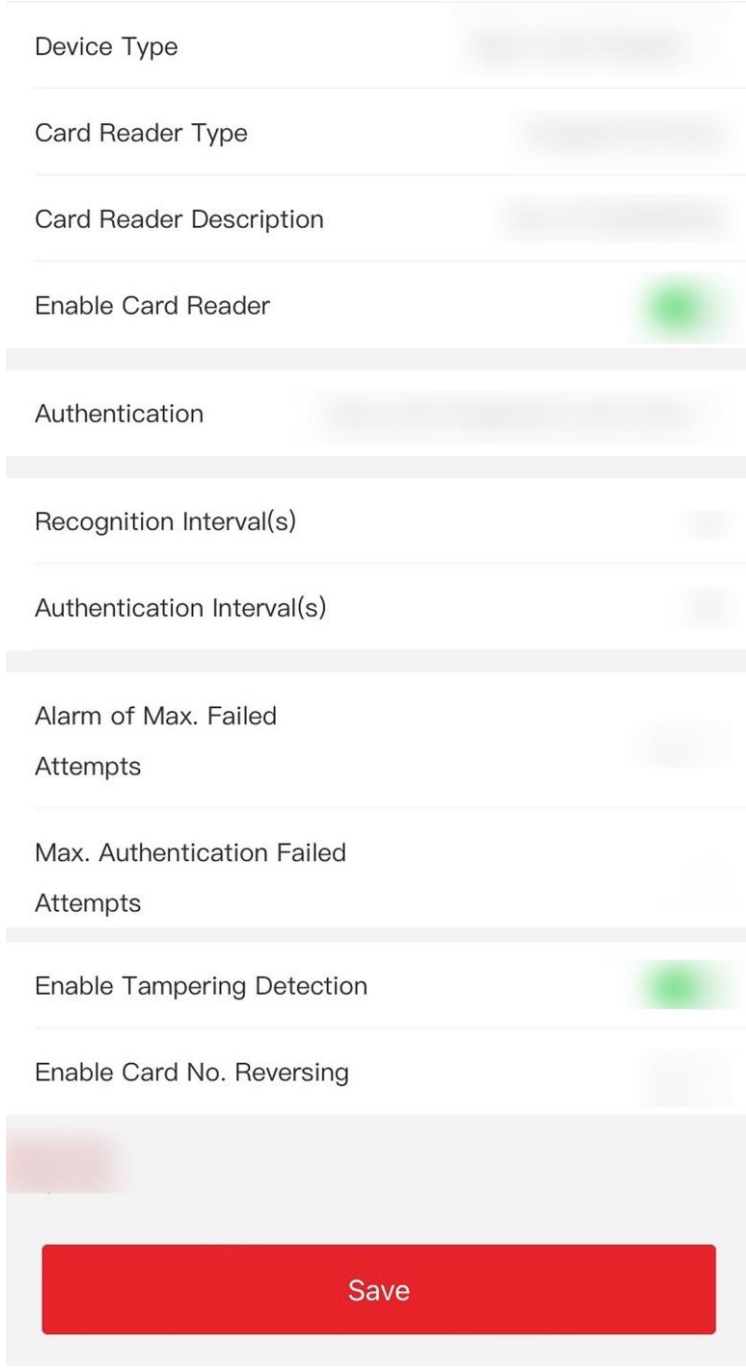


Figura 8-6 Configurações de autenticação

2. Toque em **Salvar**.

Tipo de dispositivo

Leitor de Cartão Principal

Você pode configurar os parâmetros do leitor de cartão de dispositivo. Se você selecionar o leitor de cartão principal, precisará configurar os seguintes parâmetros: **Tipo** de Leitor **de Cartão**, Descrição **do Leitor** de Cartão, **Habilitar Leitor** de **Cartão**, **Autenticação** , Intervalo (s**) de Reconhecimento (s), Intervalo(s) mínimo(s) de passagem do cartão**, **Máx. Falha na autenticação Tentativas de** alarme **/alarme de máx. Tentativas com falha**, habilite **a detecção de violação** e **habilite o número do cartão. Revertendo**.

Tipo de leitor de cartão

Obtenha o tipo de leitor de cartão.

Descrição do leitor de cartão

Obtenha a descrição do leitor de cartão. É somente leitura.

Ativar leitor de cartão

Ative a função do leitor de cartões.

Autenticação

Selecione um modo de autenticação de acordo com suas necessidades reais na lista suspensa.

Intervalo de reconhecimento

Se o intervalo entre a apresentação do cartão do mesmo cartão for menor que o valor configurado, a apresentação do cartão será inválida. O intervalo de tempo do intervalo é de 0 a 255 segundos (quando definido como 0, significa que o intervalo de reconhecimento não está habilitado e a mesma autenticação pode ser usada por tempo ilimitado).

Intervalo de autenticação

Você pode definir o intervalo de autenticação da mesma pessoa ao autenticar. A mesma pessoa só pode autenticar uma vez no intervalo configurado. Uma segunda autenticação será falhada.

Máximo de Tentativas de Falha de Autenticação Alarme/Alarme de Máximo. Tentativas fracassadas

Habilite para relatar alarme quando as tentativas de leitura do cartão atingirem o valor definido.

Habilitar detecção de violação

Habilite a detecção anti-adulteração para o leitor de cartão.

Ativar número do cartão. Inversão

O cartão de leitura nº. estará em sequência inversa depois de ativar a função.

Definir parâmetros de privacidade

Defina o tipo de armazenamento de eventos, os parâmetros de carregamento e armazenamento de imagens e os parâmetros de limpeza de imagens.

Toque em **Configuração → Configurações gerais → Privacidade** .

Configurações de armazenamento de eventos

Selecione um método para excluir o evento. Você pode selecionar **entre** Excluir eventos antigos

periodicamente, **Excluir eventos antigos por hora especificada** ou **Substituir**.

Excluir eventos antigos periodicamente

Insira o número para definir o período de exclusão do evento. Todos os eventos serão excluídos de acordo com a duração de tempo configurada.

Excluir eventos antigos por hora especificada

Defina uma hora e todos os eventos serão excluídos na hora configurada.

Substituindo

Os primeiros 5% de eventos serão excluídos quando o sistema detectar que os eventos armazenados foram mais de 95% do espaço completo.

Configurações de autenticação

Exibir resultado de autenticação

Verifique a Foto do Rosto, o Nome ou o ID do Funcionário. Quando a autenticação for concluída, o sistema exibirá o conteúdo selecionado no resultado.

Desidentificação de nomes

As informações do nome são dessensibilizadas com um asterisco.

Desidentificação de ID

As informações de ID são dessensibilizadas com um asterisco.

Carregamento e armazenamento de imagens

Você pode carregar e armazenar fotos.

Carregar imagem capturada ao autenticar

Carregue as imagens capturadas ao autenticar na plataforma automaticamente.

Salvar imagem capturada ao autenticar

Se você ativar essa função, poderá salvar a imagem ao autenticar no dispositivo.

Salvar imagem registrada

A imagem do rosto registrado será salva no sistema se você ativar a função.

Carregar imagem após a captura vinculada

Carregue as imagens capturadas pela câmera vinculada para a plataforma automaticamente.

Salvar imagens após a captura vinculada

Se você ativar essa função, poderá salvar a imagem capturada pela câmera vinculada no dispositivo.

Limpar todas as imagens no dispositivo

Você pode limpar fotos de rosto registradas e fotos capturadas no dispositivo.

Limpar fotos de rosto registradas

Selecione **Imagem de rosto e** toque em **Limpar**. Todas as imagens registradas no dispositivo serão excluídas.

Limpar autenticação/ imagem capturada

Selecione **Autenticação/Imagem Capturada** e toque em **Limpar**. Todas as imagens de autenticação/capturadas no dispositivo serão excluídas.

Definir segurança do cartão

Toque em **Configuração** → **Configurações Gerais → Segurança do Cartão** para entrar na página de configurações.

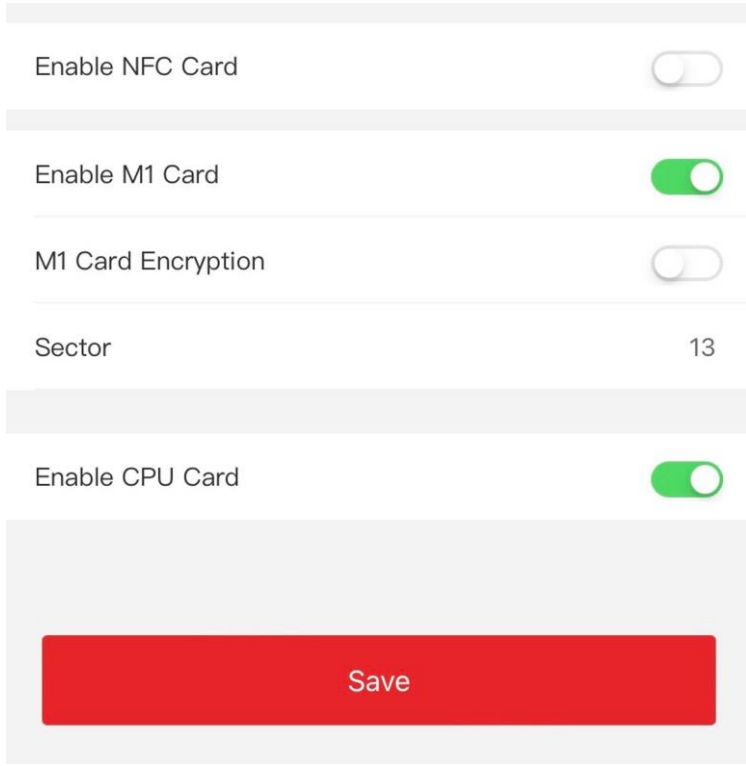


Figura 8-7 Segurança da placa

Defina os parâmetros e toque em

Salvar. **Ativar cartão NFC**

Para evitar que o celular obtenha os dados do controle de acesso, você pode ativar o cartão NFC para aumentar o nível de segurança dos dados.

Ativar cartão M1

Habilite o cartão M1 e a autenticação apresentando o cartão M1 está disponível.

Criptografia de cartão M1

A criptografia de cartão M1 pode melhorar o nível de segurança da autenticação.

Setor

Habilite a função e defina o setor de criptografia. Por padrão, o Setor 13 é criptografado. Recomenda-se criptografar o setor 13.

Ativar placa de CPU

O dispositivo pode ler os dados da placa de CPU quando enabling a função de placa de CPU.

Definir parâmetros de autenticação de cartão

Defina o conteúdo de leitura do cartão quando autenticar via cartão no dispositivo. Toque em **Configuração** → Configurações **Gerais** → **Configurações** de **Autenticação de Cartão** .

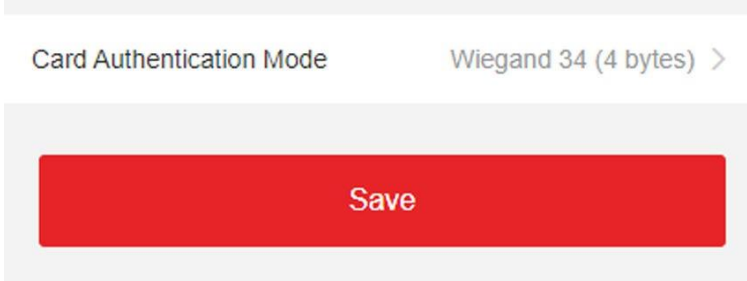


Figura 8-8 Página de autenticação de cartão

Selecione um modo de autenticação de cartão e toque em **Salvar**. **Nº do Cartão Completo.**

Todos os cartões nº. será lido.

Wiegand 26 (3 bytes)

O dispositivo irá ler o cartão via protocolo Wiegand 26 (leia 3 bytes).

Wiegand 34 (4 bytes)

O dispositivo irá ler o cartão através do protocolo Wiegand 34 (leia 4 bytes).

8.4.10 Configurações de parâmetros faciais

Defina parâmetros de face .

Configurações de parâmetros faciais

Toque em **Configuração → Parâmetro Inteligente → Inteligente** .

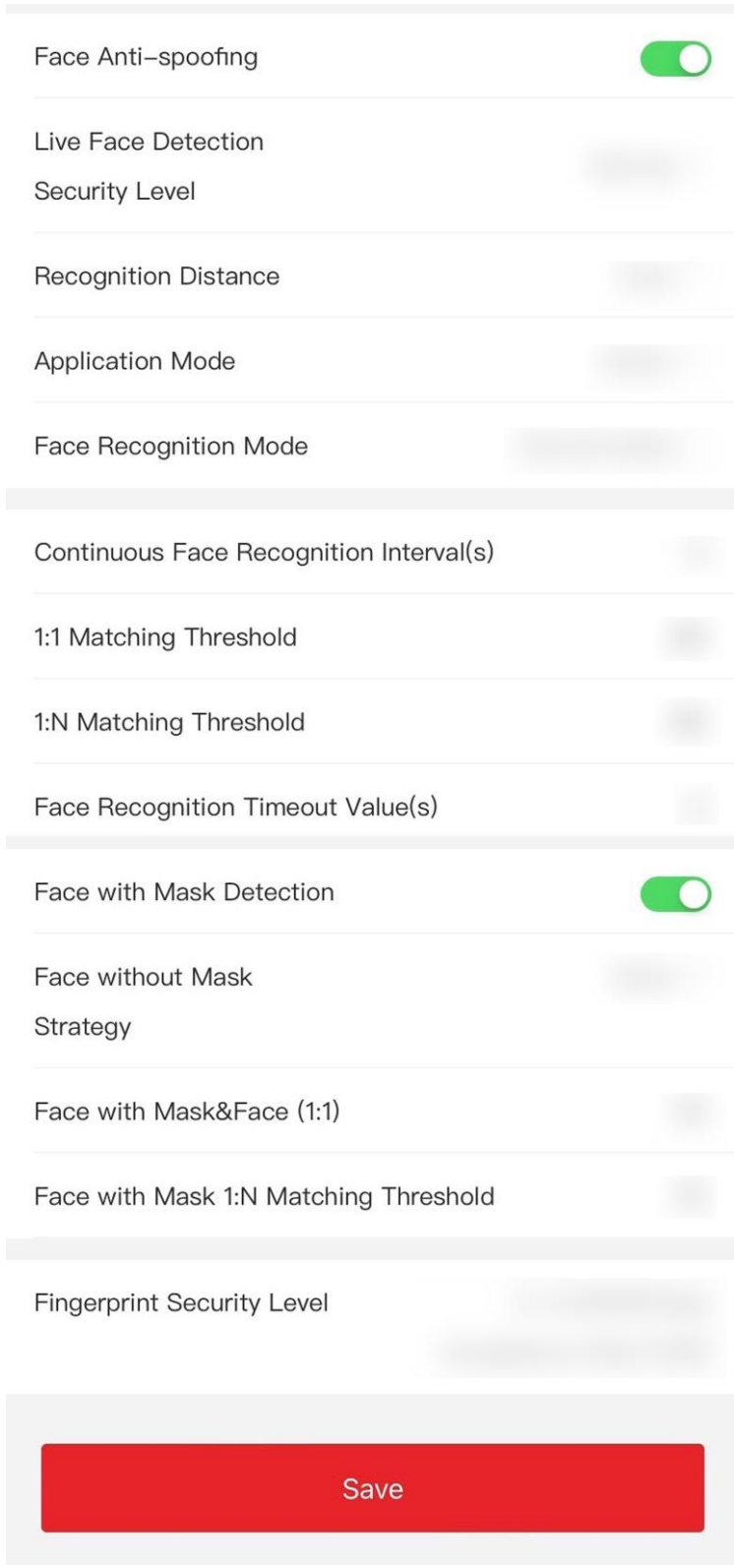


Figura 8-9 Parâmetros faciais

Nota

As funções variam de acordo com diferentes modelos. Refere-se ao dispositivo real para obter detalhes.

Defina parâmetros de face.

Face Anti-spoofing

Ative ou desative a função de detecção de rosto ao vivo. Ao ativar a função, o dispositivo pode reconhecer se a pessoa é viva ou não.

Nível de segurança de detecção de rosto ao vivo

Depois de habilitar a função antifalsificação facial, você pode definir o nível de segurança correspondente ao executar a autenticação facial ao vivo.

Distância de Reconhecimento

Selecione a distância entre o usuário autenticador e a câmera do dispositivo.

Modo de Aplicação

Selecione **Indoor** ou **Outros de** acordo com o ambiente real. Na cena externa, na cena interna perto da janela ou no ambiente ruim, você pode escolher **Outros**.

Nota

Se o dispositivo não for ativado por outras ferramentas, o dispositivo usará o modo interno como ambiente por padrão.

Modo de

Reconhecimento

Facial Modo Normal

O dispositivo usa uma câmera para realizar o reconhecimento facial.

O dispositivo usa uma câmera para realizar o reconhecimento facial.

Intervalo(s) de Reconhecimento Facial Contínuo (s)

Defina o intervalo de tempo entre dois reconhecimentos faciais contínuos ao autenticar.

Nota

Intervalo de valores: 1 a 10.

Limite de correspondência 1:1

Defina o limite de correspondência ao autenticar por meio do modo de correspondência 1 :1. Quanto maior o valor, menor a taxa de aceitação falsa e maior a taxa de falsa rejeição.

1:N Limiar de Correspondência

Defina o limite de correspondência ao autenticar por meio do modo de correspondência 1: N. Quanto maior o valor, menor a taxa de aceitação falsa e maior a taxa de falsa rejeição. O valor máximo é 100.

Valor(es) de Tempo Limite de Reconhecimento Facial

Configure o período de tempo limite para reconhecimento facial. Se o tempo de reconhecimento facial exceder o valor configurado, o dispositivo solicitará o tempo limite de reconhecimento facial.

Detecção de Rosto com Máscara

Depois de ativar o rosto com detecção de máscara, o sistema reconhecerá o rosto capturado com a imagem da máscara. Você pode definir o rosto com o limite de correspondência mask1:N, seu modo ECO e a estratégia.

Nenhum

Se a pessoa não usar uma máscara facial ao autenticar, o dispositivo não solicitará uma notificação.

Lembrete de Uso

Se a pessoa não usar uma máscara facial ao autenticar, o dispositivo solicitará uma notificação e a porta será aberta.

Deve usar

Se a pessoa não usar uma máscara facial ao autenticar, o dispositivo solicitará uma notificação e a porta será fechada.

Rosto com máscara e rosto (1:1)

Defina o valor correspondente ao autenticar com máscara facial por meio do modo de correspondência 1 :1. Quanto maior o valor, menor a taxa de aceitação falsa e maior a taxa de falsa rejeição.

Face with Máscara 1:N Limiar de Correspondência

Defina o limite de correspondência ao autenticar com máscara facial por meio do modo de correspondência 1: N. Quanto maior o valor, menor a taxa de aceitação falsa e maior a taxa de falsa rejeição.

Nível de segurança de impressão digital

Você pode definir o nível de segurança da impressão digital. Quanto maior o nível de segurança definido, menor será a Taxa de Falsa Aceitação (FAR). Quanto maior o nível de segurança definido, menor será a FRR (Taxa de Rejeição Falsa).

Definir área de reconhecimento

Toque em Configuração → **Configuração** da **Área de → Inteligente** para entrar na página.
Arraste o quadro azul no vídeo ao vivo para ajustar a área de reconhecimento. Somente a face dentro da área pode ser reconhecida pelo sistema.
Arraste o controle deslizante para configurar a área efetiva do reconhecimento facial. Toque em Salvar para salvar as configurações.

8.4.11 Configurações de

controle de acesso **definem**

parâmetros de porta

Toque em **Configuração → Controle de Acesso → Parâmetros da Porta** .

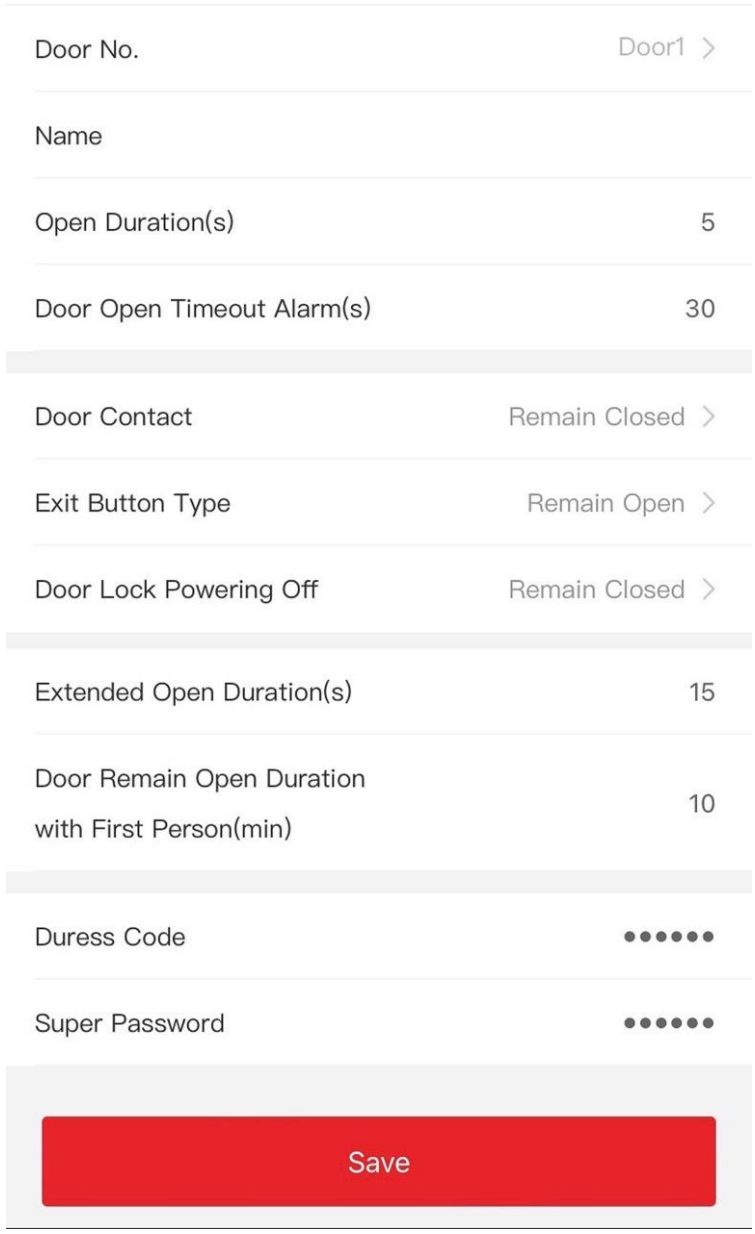


Figura 8-10 Página de configurações de parâmetros da porta

Toque em **Salvar** para salvar as configurações após a configuração.

Porta nº.

Selecione o dispositivo correspondente porta No.

Nome

Você pode criar um nome para a porta.

Duração Aberta

Defina a duração do destravamento da porta. Se a porta não for aberta para o tempo definido, a porta será trancada.

Alarme de Tempo Limite de Abertura da Porta

Um alarme será acionado se a porta não tiver sido fechada dentro do período de tempo configurado.

Contato da Porta

Você pode definir o contato da porta como Permanecer **Aberto** ou **Permanecer Fechado** de acordo com suas necessidades reais. Por padrão, ele é **Permanecer Fechado**.

Tipo de botão Sair

Você pode definir o botão de saída como Permanecer **Aberto** ou **Permanecer Fechado** de acordo com suas necessidades reais. Por padrão, é **Permanecer Aberto**.

Status de desligamento da trava da porta

Você pode definir o status da fechadura da porta quando a fechadura da porta estiver desligada. Por padrão, ele é **Permanecer Fechado**.

Duração de abertura estendida

O contato da porta pode ser ativado com o devido atraso depois que a pessoa com necessidades de acesso estendido passar o cartão.

Porta permanece aberta duração com a primeira pessoa

Defina a duração da porta aberta quando a primeira pessoa entrar. Depois que a primeira pessoa é autorizada, permite que várias pessoas acessem a porta ou outrasações autênticas.

Código Duress

A porta pode se abrir inserindo o código de coação quando há coação. Ao mesmo tempo, o cliente pode relatar o evento de coação.

Super Senha

A pessoa específica pode abrir a porta inserindo a super senha.

Nota

O código de coação e o supercódigo devem ser diferentes. E o dígito varia de 4 a 8.

8.5 Operação da Porta

Você pode operar a porta remotamente via web

móvel . Toque em **Operação da porta** para entrar

na página de operação.

Toque para abrir a porta.

Toque para fechar a porta.

Toque para definir a porta para

permanecer aberta. Toque para

definir a porta para permanecer

fechada.

Capítulo 9 Operação rápida via navegador da Web

9.1 Selecione o idioma

Você pode selecionar um idioma para o sistema do dispositivo.

Clique no canto superior direito da página da Web para entrar na página **Configurações de idioma do** dispositivo . Você pode selecionar um idioma para o sistema de dispositivos na lista suspensa.

Por padrão, o idioma do sistema é o inglês.

Nota

Depois de alterar o idioma do sistema, o dispositivo será reinicializado automaticamente.

Clique em **Avançar** para concluir as configurações.

9.2 Configurações de Hora

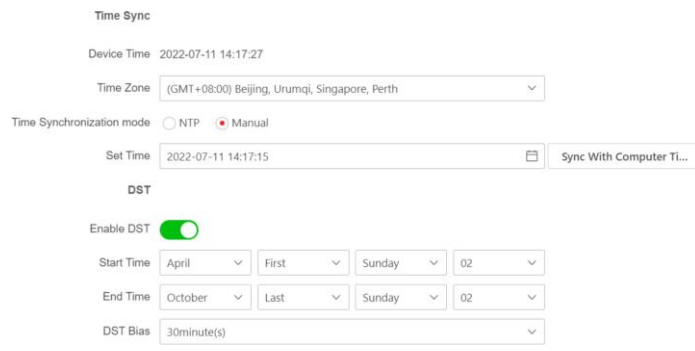


Figura 9-1 Definir hora e horário de verão

Clique no canto superior direito da página da Web para entrar na página do assistente. Depois de definir o idioma do dispositivo, você pode clicar em **Avançar** para entrar na página **Configurações de Hora**.

Fuso Horário

Selecione o fuso horário localizado no dispositivo na lista suspensa.

Sincronização de Tempo.

NTP

Você deve definir o endereço IP, a porta nº e o intervalo do servidor NTP.

Manual

Por padrão, a hora do dispositivo deve ser sincronizada manualmente. Você pode definir a hora do dispositivo manualmente ou marcar **Sincronizar**. com Hora do Computador para sincronizar a hora do dispositivo com a hora do computador.

Endereço do Servidor/Porta/Intervalo NTP

Você pode definir o endereço do servidor, a porta NTP e o intervalo.

DST

Você pode visualizar a hora de início do horário de verão, a hora de término e a hora do viés.

Clique em **Avançar** para salvar as configurações e vá para o próximo parâmetro. Ou clique em **Ignorar** para ignorar as configurações de tempo.

9.3 Configurações do ambiente

Depois de ativar o dispositivo , você deve selecionar um modo de aplicativo para melhor aplicativo do dispositivo.

Passos

1. Clique no canto superior direito da página da Web para entrar na página do assistente. Depois de definir o idioma e a hora do dispositivo, você pode clicar em **Avançar** para entrar na página **Configurações do Ambiente**.
2. Selecionar **Interior** ou **Outro**.

Nota

- Se você instalar o dispositivo em ambientes fechados, perto da janela, ou se a função de reconhecimento facial não estiver funcionando bem, selecione **Outros**.
- Se você não configurar o modo de aplicativo e tocar em **Avançar**, o sistema selecionará **Indoor** por padrão.
- Se você ativar o dispositivo por meio de outras ferramentas remotamente, o sistema selecionará **Indoor** como o modo de aplicativo por padrão.

Clique em **Avançar** para salvar as configurações e ir para o próximo parágrafo. Ou clique em **Ignorar** para ignorar as configurações do ambiente.

9.4 Configurações de privacidade

Defina os parâmetros de upload e armazenamento de imagens.

Clique no canto superior direito da página da Web para entrar na página do assistente. Depois de definir o idioma, a hora e o ambiente do dispositivo, você pode clicar em **Avançar** para entrar na página **Configurações de privacidade**.

Carregamento e armazenamento de imagens

Salvar imagem ao autenticar

Salve a imagem ao autenticar automaticamente.

Carregar imagem ao autenticar

Carregue as imagens ao autenticar na plataforma automaticamente.

Salvar imagem registrada

A imagem do rosto registrado será salva no sistema se você ativar a função.

Carregar imagem após a captura vinculada

Carregue as imagens capturadas pela câmera vinculada para a plataforma automaticamente.

Salvar imagens após a captura vinculada

Se você ativar esta função, você pode salvar aimagem capturada pela câmera vinculada para o dispositivo. Clique em **Avançar** para salvar as configurações e ir para o próximo parágrafo. Ou clique em **Ignorar** para ignorar as configurações de privacidade.

9.5 Configurações do administrador

Passos

1. Clique no canto superior direito da página da Web para entrar na página do assistente. Depois de definir o idioma, a hora, o ambiente e a privacidade do dispositivo, você pode clicar em **Avançar** para entrar na página **Configurações** do administrador.
2. Insira a ID do funcionário e o nome do administrador.
3. Selecionar a credencial Para adicionar.

Nota

Você deve selecionar pelo menos uma credencial.

1) Clique em **Adicionar Rosto** para carregar uma imagem facial do armazenamento local.

Nota

A imagem carregada deve estar dentro de 200 K, no formato JPG、JPEG、PNG.

2) Clique **Adicionar Cartão** Para entrar o Cartão Não. e selecionar o propriedade de o cartão.

Nota

Até 5 cartões podem ser suportados.

3) Clique **Adicionar Impressão digital** Para adicionar Impressões digitais.

Nota

Até 10 impressões digitais são permitidas.

Clique em **Concluir** para concluir as configurações.

Capítulo 10 Operação via navegador da Web

10.1 Login

Você pode fazer login através do navegador da Web ou da configuração remota do software cliente.

Nota

Verifique se o dispositivo está ativado. Para obter informações detalhadas sobre ativação, consulte ***Ativação*** .

Login via Web Browser

Digite o endereço IP do dispositivo na barra de endereços do navegador da Web e pressione **Enter** para entrar na página de login.
Insira o nome de usuário do dispositivo e a senha. Clique em **Login**.

Login via Configuração Remota do Software Cliente

Baixe e abra o software cliente. Depois de adicionar o dispositivo, clique para entrar na página Configuração.

10.2 Esquecer senha

Se você esquecer a senha ao fazer login, poderá alterá-la por endereço de e-mail ou perguntas de segurança.

Na página de login, clique em **Esquecer**

Senha. Selecione **Modo de verificação**.

Verificação de Perguntas de Segurança

Responda às perguntas de segurança.

Verificação de e-mail

1. Exporte o código QR e envie-o para ***pw_recovery@hikvision.com*** como anexo.
2. Você receberá um código de verificação dentro de 5 minutos em seu e-mail reserved.
3. Insira o código de verificação no campo do código de verificação para verificar sua identificação. Clique em **Avançar**, crie uma nova senha e confirme-a.

10.3 Visualização ao vivo

Você pode visualizar o vídeo ao vivo do dispositivo, o evento em tempo real, as informações da pessoa, o status da rede, as informações básicas e a capacidade do dispositivo.

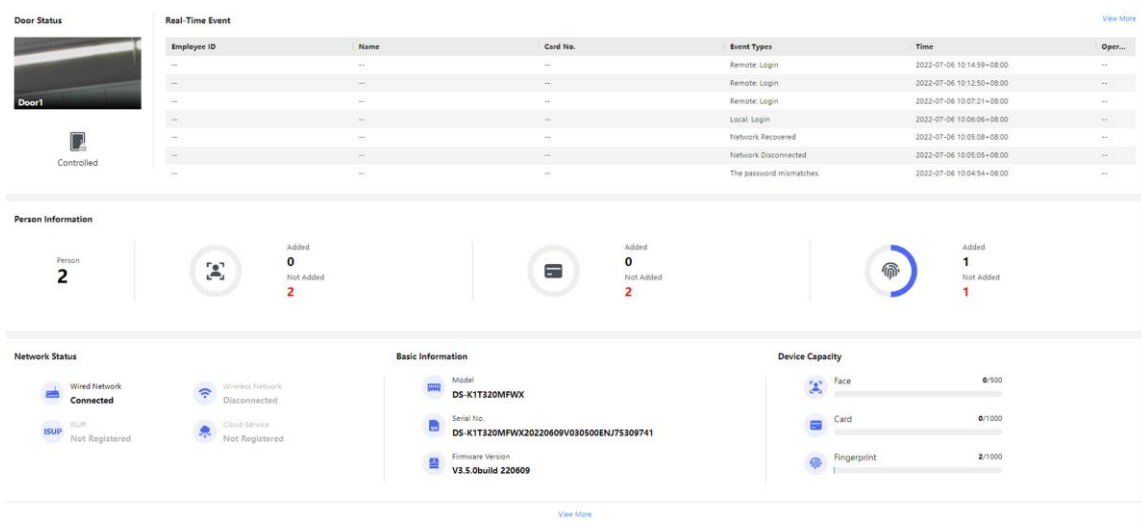


Figura 10-1 Página de visualização dinâmica

Descrições da função:

Status da porta

Clique para ver a visualização dinâmica do dispositivo.

Defina o volume ao iniciar a visualização ao vivo.

Nota

Se você ajustar o volume ao iniciar o áudio bidirecional, poderá ouvir sons repetidos.

Você pode capturar a imagem ao iniciar a visualização ao vivo.

Selecione o tipo de streaming ao iniciar a visualização ao vivo. Você pode selecionar entre o fluxo principal e o subfluxo.

Visualização em tela cheia.

/ / /

O status da porta é aberto/fechado/permanecendo aberto/permanecendo fechado .

Status controlado

Você pode selecionar o status aberto/fechado/permanecendo aberto/permanecendo fechado de acordo com suas necessidades reais.

Evento em Tempo Real

Você pode exibir a ID do Funcionário, o Nome, o Número do Cartão, o Tipo de Evento, a Hora e a Operação do evento. Você também pode clicar em **Exibir Mais** para inserir as condições de pesquisa, incluindo o tipo de evento, a ID do funcionário, o nome, o número do cartão, a hora de início e a hora de término, e clique em **Pesquisar**. Os resultados serão exibidos no painel direitol.

Informações da Pessoa

Você pode exibir as informações adicionadas e não adicionadas do rosto, cartão e impressão digital da pessoa.

Status da rede

Você pode visualizar o status conectado e registrado da rede com fio, rede sem fio, ISUP e serviço de nuvem.

Informação Básica

Você pode ver o modelo, número de série. e versão do firmware.

Capacidade do dispositivo

Você pode visualizar a capacidade de rosto, cartão e impressão digital .

Ver mais

Você pode clicar em **Ver mais** para ver o nome do dispositivo, número do dispositivo, idioma, modelo, número de série, versão, número de canais, entrada de E /S, saída de E/S, bloqueio, entrada de alarme, saída de alarme e capacidade do dispositivo, etc.

10.4 Gestão de Pessoas

Clique em **Adicionar** para adicionar as informações da pessoa, incluindo as informações básicas, o certificado, a autenticação e as configurações.

Adicionar informações básicas

Clique em **Gerenciamento de Pessoas →** Adicionar para entrar na página **Adicionar** Pessoa. Adicione as informações básicas da pessoa, incluindo a ID do funcionário, o nome da pessoa e o tipo de pessoa.
Se você selecionar **Visitante** como o tipo de pessoa, poderá definir os horários de visita. Clique em **Salvar** para salvar as configurações.

Definir Hora de Permissão

Clique em **Gerenciamento de Pessoas →** Adicionar para entrar na página **Adicionar** Pessoa. Habilite **o Usuário Efetivo de Longo Prazo** ou defina a Hora de Início e a **Hora de Término** e a pessoa só poderá ter a permissão dentro do período de tempo configurado de acordo com suas necessidades reais.
Clique em **Salvar** para salvar as configurações.

Definir Quarto No.

Clique em **Gerenciamento de Pessoas →** Adicionar para entrar na página **Adicionar** Pessoa. Clique em **Adicionar** para adicionar o número do **andar.** e **Quarto nº.** .

Clique para excluí-lo.

Clique em **Salvar** para salvar as configurações.

Configurações de autenticação

Clique em **Gerenciamento de Pessoas →** Adicionar para entrar na página **Adicionar** Pessoa. Defina o tipo de autenticação.
Clique em **Salvar** para salvar as configurações.

Adicionar cartão

Clique em **Gerenciamento de Pessoas →** Adicionar para entrar na página **Adicionar** Pessoa.
Clique em **Adicionar cartão**, insira o **número do cartão.** e selecione a **Propriedade** e clique em **Salvar** para adicionar o cartão. Clique em **Salvar** para salvar as configurações.

Adicionar impressão digital

Nota

Somente os dispositivos que suportam a função de impressão digital podem adicionar a impressão digital.

Clique em **Gerenciamento de Pessoas →** Adicionar para entrar na página **Adicionar** Pessoa.
Clique em **Adicionar** impressão digital e pressione o dedo no módulo de impressão digital do dispositivo para adicionar sua impressão digital.
Clique em **Salvar** para salvar as configurações.

Adicionar imagem de rosto

Clique em **Gerenciamento de Pessoas →** Adicionar para entrar na página **Adicionar** Pessoa. Clique em **+** à direita para carregar uma imagem facial do PC local.

Nota

O formato de imagem deve ser JPG ou JPEG ou PNG, e o tamanho deve ser inferior a 200 K.

Clique em **Salvar** para salvar as configurações.

10.5 Evento de Pesquisa

Clique em **Pesquisa de Eventos** para entrar na página Pesquisar.

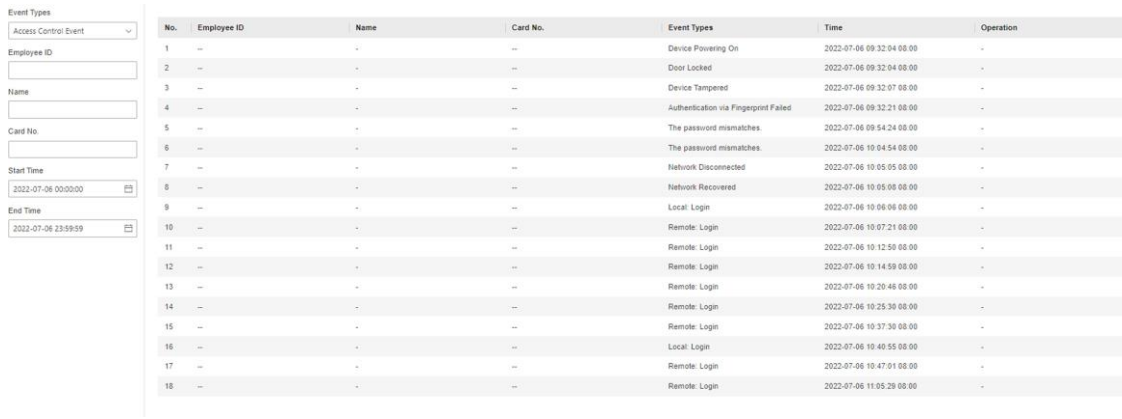


Figura 10-2 Evento de pesquisa

Insira as condições de pesquisa, incluindo o tipo de evento, a ID do funcionário, o nome, o número do cartão, a hora de início e a hora de término e clique em **Pesquisar**.

Os resultados serão exibidos no painel direito.

10.6 Configuração

10.6.1 Definir parâmetros locais

Defina os parâmetros de visualização ao vivo, as configurações de imagem e clipe.

Definir parâmetros de visualização dinâmica

Clique em **Configuração →** Local para entrar na página **Local** . Configure o tipo de fluxo, o desempenho de reprodução e clique em **Salvar**.

Configurações de imagem **e clipe**

Clique em **Configuração →** Local para entrar na página **Local** . Selecione o formato da imagem, salvando o caminho e clique em
Salve.
Você também pode clicar em **Abrir** para abrir a pasta de arquivos para exibir detalhes.

10.6.2 Exibir informações do dispositivo

Veja o nome do dispositivo, número do dispositivo, idioma, modelo, número de série, versão, número de canais, entrada de E/S , saída de E/S, bloqueio, entrada de alarme, saída de alarme e capacidade do dispositivo , etc.

Clique em **Configuração** → Sistema → **Configurações do Sistema → Informações Básicas** para entrar na página de configuração.

Você pode visualizar o nome do dispositivo, número do dispositivo, idioma, modelo, número de série, versão, número de canais, entrada de E/S, saída de E/S, bloqueio, entrada de alarme, saída de alarme e capacidade do dispositivo , etc.

10.6.3 Definir Hora

Defina o fuso horário, o modo de sincronização, o endereço do servidor, a porta NTP e o intervalo do dispositivo . Clique em Configuração → Configurações do Sistema → **Configurações do Sistema → Tempo** .

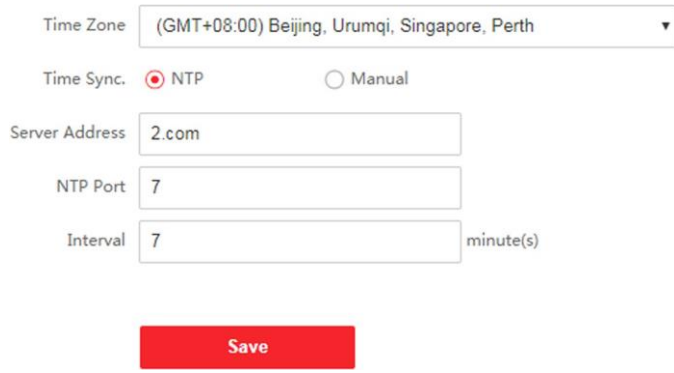


Figura 10-3 Configurações de tempo

Clique em **Salvar** para salvar as configurações após a configuração.

Fuso Horário

Selecione o fuso horário localizado no dispositivo na lista suspensa.

Sincronização de Tempo.

NTP

Você deve definir o endereço IP, a porta nº e o intervalo do servidor NTP.

Manual

Por padrão, a hora do dispositivo deve ser sincronizada manualmente. Você pode definir a hora do dispositivo manualmente ou marcar **Sincronizar**. com Hora do Computador para sincronizar a hora do dispositivo com a hora do computador.

Tipo de Complementode Servidor/Endereço do Servidor/Porta/Intervalo NTP

Você pode definir o tipo de endereço do servidor, o endereço do servidor, a porta NTP e o intervalo.

10.6.4 Definir horário de verão

Passos

1. Clique em **Configuração → Sistema → Configurações do Sistema → Configurações de Tempo** .

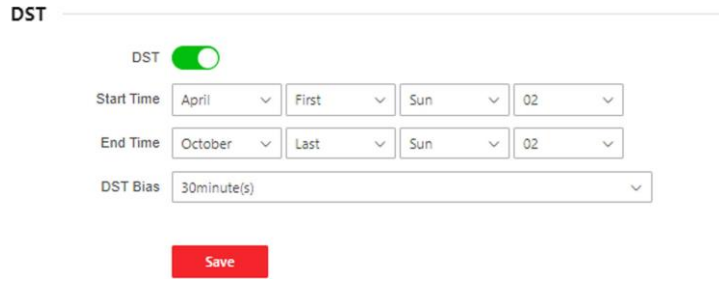


Figura 10-4 Página do horário de verão

2. Habilite o **horário de verão**.
3. Defina a hora de início do horário de verão, a hora de término e a hora do viés.
4. Clique em **Salvar** para salvar as configurações.

10.6.5 Alterar a senha do administrador

Passos

1. Clique em **Configuração → Gerenciamento de Usuários** .
2. Clique em .
3. Digite a senha antiga e crie uma nova senha.
4. Confirme a nova senha.
5. Clique **OKEY**.

Cuidado

A força da senha do dispositivo pode ser verificada automaticamente. É altamente recomendável que você altere a senha de sua própria escolha (usando um mínimo de 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: 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, alterando a senha mensal 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.

10.6.6 Exibir informações de armar/desarmar o dispositivo

Visualize o tipo de armamento do dispositivo e o endereço IP de armamento.

Vá para **Configuração → Informações de Armação/Desarmamento** .

Você pode visualizar as informações de armamento/desarmamento do dispositivo. Clique em **Atualizar** para atualizar a página.

10.6.7 Configurações de rede

Defina TCP/IP, porta, parâmetros Wi-Fi, ISUP e acesso à plataforma.

Nota

Alguns modelos de dispositivos não suportam definições de Wi-Fi ou de dados móveis. Consulte os produtos reais ao configurar.

Definir parâmetros básicos de rede

Clique em **Configuração → Rede → Configurações de Rede → TCP/IP** .

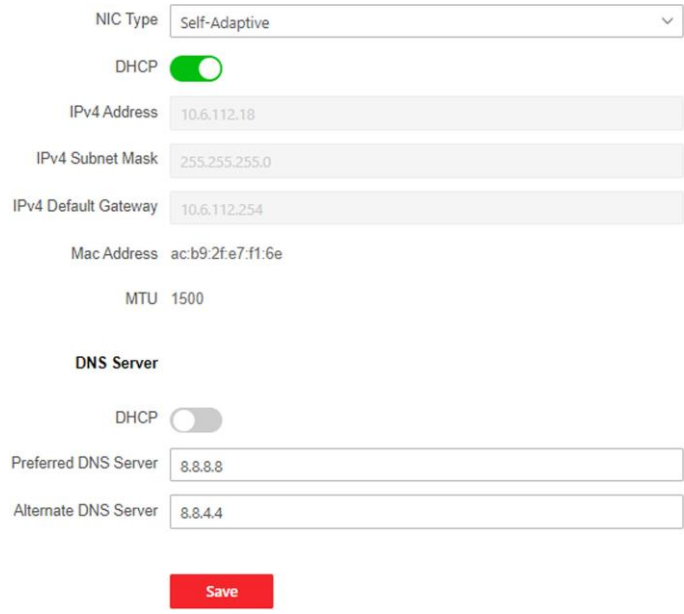


Figura 10-5 Página de configurações de TCP/IP

Defina os parâmetros e clique em **Salvar** para salvar as configurações.

Tipo de NIC

Selecione um tipo de NIC na lista suspensa. Por padrão, é **Automático**.

Processador DHCP

Se desmarcar a função, você deverá definir o endereço IPv4, a máscara de sub-rede IPv4, o gateway padrão IPv4 , o endereço Mac e a MTU.

Se você verificar a função, o sistema alocará o endereço IPv4, a máscara de sub-rede IPv4 , o gateway padrão IPv4 automaticamente.

Servidor DNS

Defina o servidor DNS preferencial e o servidor DNS alternativo de acordo com sua necessidade real.

Definir parâmetros de Wi-Fi

Defina os parâmetros Wi-Fi para a conexão sem fio do dispositivo.

Passos

Nota

A função deve ser suportada pelo dispositivo.

1. Clique em **Configuração → Rede → Configurações de Rede → Wi-Fi** .

Figura 10-6 Página de configurações de Wi-Fi

2. Verifique o **Wi-Fi**.

3. Selecione um Wi-Fi

- Clique em um Wi-Fi na lista e insira a senha do Wi-Fi.
- Clique em **Adicionar** e insira o nome, a senha e o tipo de criptografia de um Wi-Fi. Clique em **Conectar**. Quando o Wi-Fi estiver conectado, clique em **OK.**

4. Opcional: Defina os parâmetros WLAN.

1) Defina o endereço IP, a máscara de sub-rede e o gateway padrão. Ou habilite o **DHCP** e o sistema alocará o endereço IP, a máscara de sub-rede e o gateway padrão automaticamente.

5. Clique em **Salvar**.

Definir parâmetros de porta

Defina os parâmetros HTTP , HTTPS, HTTP Listening, RTSP e Server port.

Clique em **Configuração → Serviço de Rede → Rede → HTTP(S)** .

Correio HTTP

Refere-se à porta através da qual o navegador acessa o dispositivo. Por exemplo, quando a porta HTTP é modificada para 81, você precisa inserir ***http://192.0.0.65:81*** no navegador para login.

HTTPS (em inglês)

Defina o HTTPS para acessar o navegador. O certificado é necessário ao acessar.

Escuta HTTP

O dispositivo pode enviar informações de alarme para o endereço IP de alarme de evento ou nome de domínio via protocolo HTTP/protocolo HTTPS. Edite o endereço IP ou o nome de domínio, a URL, a porta e o protocolo do alarme de evento.

Nota

O endereço IP ou nome de domínio do alarme de evento deve oferecer suporte ao protocolo HTTP/protocolo HTTPS para receber as informações de alarme.

Clique em **Configuração → Serviço de Rede → de Rede → RTSP** .

RTSP

Refere-se à porta do protocolo de streaming em tempo real.

Clique em **Configuração → Acesso à Rede → Dispositivo → Servidor SDK** .

Servidor SDK

Refere-se à porta através da qual o cliente adiciona o dispositivo.

Acesso à plataforma

O acesso à plataforma oferece uma opção para gerenciar os dispositivos via plataforma.

Passos

1. Clique **Configuração → Rede → Dispositivo Acesso → Caminhada-Conexão** Para entrar o

Nota

Configurações página.

Hik-Connect é um aplicativo para dispositivos móveis. Com o aplicativo, você pode visualizar a imagem ao vivo do dispositivo, receber notificação de alarme e assim por diante.

2. **Marque Ativar** para ativar a função.
3. **Opcional:** Marque a caixa de seleção **Personalizado** e você pode definir o endereço do servidor por conta própria.
4. Entrar o servidor IP endereço e verificação código.

Nota

6 a 12 letras (a a z, A a Z) ou números (0 a 9), diferenciando maiúsculas de minúsculas. Recomenda-se que você use uma combinação de pelo menos 8 letras ou números.

5. Clique em **Salvar** para ativar as configurações.

Configurar parâmetros ISUP

Defina os parâmetros ISUP para acessar o dispositivo via protocolo ISUP.

Passos

Nota

A função deve ser suportada pelo dispositivo.

1. Clique em **Configuração → Acesso à Rede → Dispositivo → ISUP** .
2. **Marque Ativar**.
3. Pôr o ISUP Versão servidor endereço dispositivo ID e o ISUP estado.

Nota

Se você selecionar 5.0 como a versão, você deve definir a chave de criptografia também.

4. Defina os parâmetros de escuta ISUP, incluindo o endereço IP/nome de domínio da central de alarme ISUP , o URL da central de alarme ISUP e a porta da central de alarme ISUP.
5. Clique em **Salvar**.

10.6.8 Definir parâmetros de vídeo e áudio

Defina a qualidade e a resolução da imagem.

Definir parâmetros de vídeo

Clique em **Configuração → Vídeo /Áudio → Vídeo** .

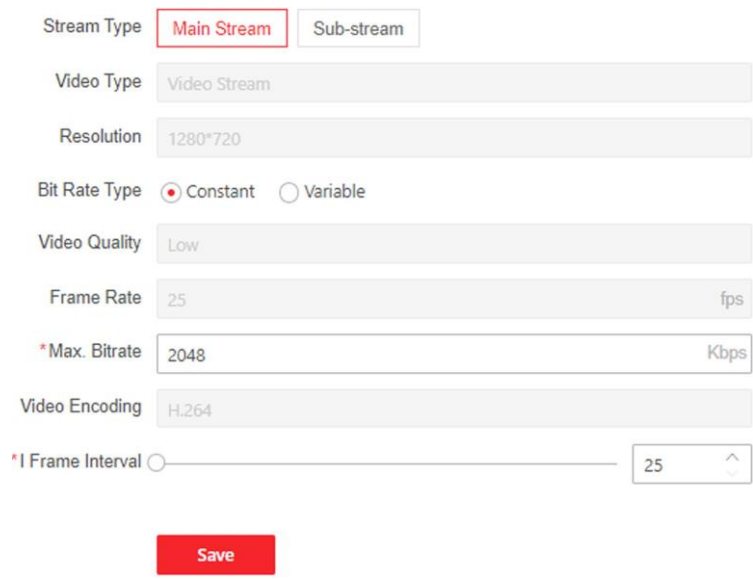


Figura 10-7 Página de configurações de vídeo

Defina o tipo de fluxo, o tipo de vídeo, o tipo de taxa de bits, a taxa de quadros , o Max. bitrate, a codificação de vídeo e I Frame Interval.
Clique em **Salvar** para salvar as configurações após a configuração.

Nota

As funções variam de acordo com diferentes modelos. Refere-se ao dispositivo real para obter detalhes.

10.6.9 Definir parâmetros de imagem

Você pode ajustar os parâmetros de imagem, parâmetros de vídeo, parâmetros de suplemento e intervalo de captura.

Passos

1. Clique em **Configuração → Imagem** .

2. Configure os parâmetros para ajustar a imagem.

Ajuste de vídeo (padrão de vídeo)

Defina a taxa de quadros do vídeo ao executar a visualização ao vivo remotamente. Depois de alterar o padrão, você deve reiniciar o dispositivo para entrar em vigor.

AMIGO

25 quadros por segundo. Adequado para a China continental, Hong Kong (China), os países do Oriente Médio, países da Europa, etc.

NTSC

30 quadros por segundo. Adequado para os EUA, Canadá, Japão, Taiwan (China), Coreia, Filipinas, etc.

Ajuste de imagem

Arraste o bloco ou insira o valor para ajustar o brilho, o contraste, a saturação e a nitidez do vídeo ao vivo.

Parâmetros de luz do suplemento

Defina o tipo de luz do suplemento, modo, hora de início e hora de término. Você também pode definir o brilho.

Intervalo de captura

Você pode selecionar o intervalo de captura de acordo com suas necessidades reais.

3. Clique em **Padrão** para restaurar os parâmetros para as configurações padrão.

10.6.10 Configurações de

controle de acesso Definir

parâmetros de autenticação

Clique em **Configuração → Controle de Acesso → Configurações de Autenticação** .

Nota

As funções variam de acordo com diferentes modelos. Refere-se ao dispositivo real para obter detalhes.

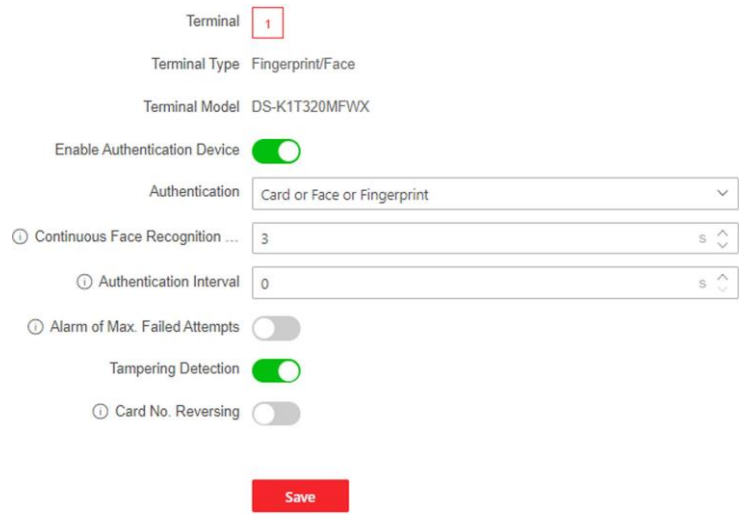


Figura 10-8 Definir parâmetros de autenticação

Clique em **Salvar** para salvar as configurações após a configuração.

Terminal/Tipo de Terminal/Modelo de Terminal

Obtenha a descrição do terminal. Eles são somente leitura.

Habilitar dispositivo de autenticação

Habilite a função de autenticação.

Autenticação

Selecione um modo de autenticação de acordo com suas necessidades reais na lista drop-down.

Intervalo de Reconhecimento Facial Contínuo

Você pode definir o intervalo entre 2 reconhecimento contínuo de uma mesma pessoa durante a autenticação. No intervalo configurado, a Pessoa A só pode ser reconhecida uma vez. Se outra pessoa (Pessoa B) reconheceu durante o intervalo, a Pessoa A pode reconhecer novamente.

Intervalo de autenticação

Você pode definir o intervalo de autenticação da mesma pessoa ao autenticar. A mesma pessoa só pode autenticar uma vez no interval. Uma segunda autenticação será falhada.

Alarme de Max. Tentativas fracassadas

Habilite para relatar alarme quando as tentativas de leitura do cartão atingirem o valor definido.

Tentativas de falha de autenticação

Habilite para relatar alarme quando as tentativas de leitura do cartão atingirem o valor definido.

Detecção de adulteração

Habilite a detecção anti-adulteração para o leitor de cartão.

Nº do cartão Inversão

O cartão de leitura nº. estará em sequência inversa depois de ativar a função.

Definir parâmetros da porta

Clique em **Configuração → Controle de Acesso → Parâmetros da Porta** .

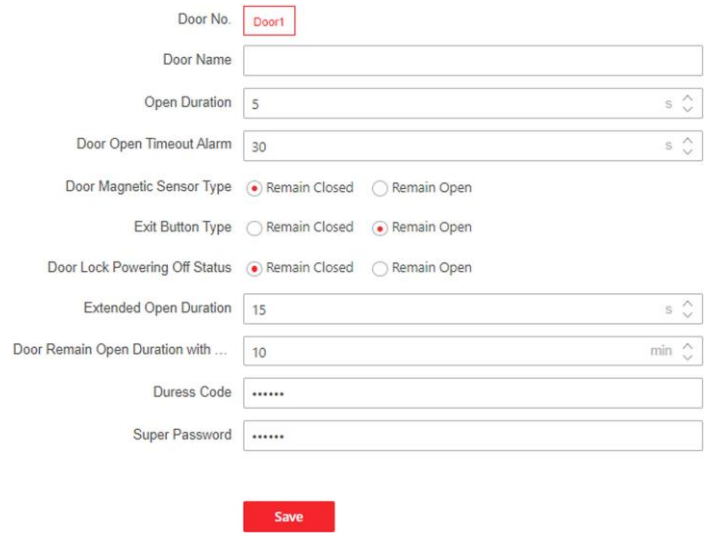


Figura 10-9 Página de configurações de parâmetros de porta

Clique em **Salvar** para salvar as configurações após a configuração.

Porta nº.

Selecione o dispositivo correspondente porta No.

Nome

Você pode criar um nome para a porta.

Duração Aberta

Defina a duração do destravamento da porta. Se a porta não for aberta para o tempo definido, a porta será trancada.

Alarme de Tempo Limite de Abertura da Porta

Um alarme será acionado se a porta não tiver sido fechada dentro do período de tempo configurado.

Contato da Porta

Você pode definir o contato da porta como Permanecer **Aberto** ou **Permanecer Fechado** de acordo com suas necessidades reais. Por padrão, ele é **Permanecer Fechado**.

Tipo de botão Sair

Você pode definir o botão de saída como Permanecer **Aberto** ou **Permanecer Fechado** de acordo com suas necessidades reais. Por padrão, é **Permanecer Aberto**.

Status de desligamento da trava da porta

Você pode definir o status da fechadura da porta quando a fechadura da porta estiver desligada. Por padrão, ele é **Permanecer Fechado**.

Duração de abertura estendida

O contato da porta pode ser ativado com o devido atraso depois que a pessoa com necessidades de acesso estendido passar o cartão.

Porta permanece aberta duração com a primeira pessoa

Defina a duração da porta aberta quando a primeira pessoa entrar. Depois que a primeira pessoa é autorizada, ele permite que várias pessoas acessem a porta ou outras ações de autenticação.

Código Duress

A porta pode se abrir inserindo o código de coação quando há coação. Ao mesmo tempo, o cliente pode relatar o evento de coação.

Super Senha

A pessoa específica pode abrir a porta inserindo a super senha.

Nota

O código de coação e o supercódigo devem ser diferentes.

Definir parâmetros do terminal

Você pode definir parâmetros de terminal para acesso.

Clique em **Configuração → Controle de Acesso → Parâmetros do Terminal** .

Você pode definir **o** Modo de Trabalho como **Modo** de **Controle de Acesso**. O modo de controle de acesso é o modo normal do dispositivo. Você deve autenticar sua credencial para acesso.

Clique em **Salvar** para salvar as configurações após a configuração.

10.6.11

Configurações do

cartão **Definir**

segurança do cartão

Clique em **Configuração** → **Configurações** do Cartão **→ Tipo** de **Cartão** para

entrar na página **de** configurações. Defina os parâmetros e clique em **Salvar**.

Ativar cartão NFC

Para evitar que o celular obtenha os dados do controle de acesso, você pode ativar o cartão NFC para aumentar o nível de segurança dos dados.

Ativar cartão M1

Habilite o cartão M1 e a autenticação apresentando o cartão M1 está disponível.

Setor de criptografia de cartão M1

A criptografia de cartão M1 pode melhorar o nível de segurança da autenticação.

Habilite a função e defina o setor de criptografia. Por padrão, o Setor 13 é criptografado. Recomenda-se criptografar o setor 13.

Ativar placa de CPU

Habilite a placa de CPU e a autenticação apresentando a placa de CPU está disponível.

Definir o número do cartão. Parâmetros de autenticação

Defina o conteúdo de leitura do cartão quando autenticar via cartão no dispositivo.

Vá para **Configuração** → **Configurações** do **Cartão → Nº do Cartão.**

Configurações de autenticação . Selecione um modo de autenticação de cartão e clique em **Salvar**.

Nº do Cartão Completo .

Todos os cartões nº. será lido.

Wiegand 26 (3 bytes)

O dispositivo irá ler o cartão via protocolo Wiegand 26 (leia 3 bytes).

Wiegand 34 (4 bytes)

O dispositivo irá ler o cartão através do protocolo Wiegand 34 (leia 4 bytes).

10.6.12 Definir parâmetros de privacidade

Defina o tipo de armazenamento de eventos, os parâmetros de carregamento e armazenamento de imagens e os parâmetros de limpeza de imagens.

Vá para **Configuração → Configurações de Segurança → Privacidade**

Configurações de armazenamento de eventos

Selecione um método para excluir o evento. Você pode selecionar **entre** Excluir eventos antigos **periodicamente**, **Excluir eventos antigos por hora especificada** ou **Substituir**.

Excluir eventos antigos periodicamente

Arraste o número de bloco ou insira para definir o período de exclusão do evento. Todos os eventos serão excluídos de acordo coma duração de tempo configurada.

Excluir eventos antigos por hora especificada

Defina uma hora e todos os eventos serão excluídos na hora configurada.

Substituindo

Os primeiros 5% de eventos serão excluídos quando o sistema detectar que os eventos armazenados foram mais de 95% do espaço completo.

Configurações de autenticação

Exibir resultado de autenticação

Você pode marcar **Imagem facial**, **Nome** e **ID do funcionário** para exibir o resultado da autenticação.

Desidentificação do nome

Você pode marcar **Desidentificação de** nome e o nome inteiro não será exibido.

Carregamento e armazenamento de imagens

Salvar imagem ao autenticar

Salve a imagem ao autenticar automaticamente.

Carregar imagem ao autenticar

Carregue as imagens ao autenticar na plataforma automaticamente.

Salvar imagem registrada

A imagem do rosto registrado será salva no sistema se você ativar a função.

Carregar imagem após a captura vinculada

Carregue as imagens capturadas pela câmera vinculada para a plataforma automaticamente.

Salvar imagens após a captura vinculada

Se você ativar essa função, poderá salvar a imagem capturada pela câmera vinculada no dispositivo.

Limpar todas as imagens no dispositivo

Nota

Todas as imagens não podem ser restauradas depois de serem excluídas.

Limpar fotos de rosto registradas

Todas as imagens registradas no dispositivo serão excluídas.

Limpar imagens capturadas

Todas as imagens capturadas no dispositivo serão excluídas.

10.6.13 Configurações de Horário e Presença

Se você quiser rastrear e monitorar quando as pessoas começam / param de trabalhar e monitorar suas horas de trabalho e chegadas tardias, partidas antecipadas, tempo tomado em pausas e absenteísmo, você pode adicionar a pessoa ao grupo de turnos e atribuir umchedule de turno (uma regra para o comparecimento definindo como o

repetências de agendamento, o tipo de turno, as configurações de quebra e a regra de passar o dedo do cartão.) ao grupo de turno para definir os parâmetros de atendimento para as pessoas do grupo de plantão.

Desativar o Modo de Atendimento via Web

Desative o modo de presença e o sistema não exibirá o status de presença na página inicial.

Passos

1. Clique em **Configuração → Status de T&A** para entrar na página de configurações.
2. Desative o **Horário e Presença**.

Resultado

Você não exibirá ou configurará o status de presença na página inicial. E o sistema seguirá a regra de assiduidade que configurou na plataforma.

Configurações de Hora

Passos

1. Clique em **Configuração → Status de T&A** para entrar na página de configurações.
2. Selecione **Modelo de agendamento**.
3. Arrastar rato Para pôr o horário.

Nota

Defina o horário de segunda a domingo de acordo com as necessidades reais.

4. Você pode ativar o **trabalho on/off**, **quebrar horas extras de** acordo com suas necessidades reais e definir o nome personalizado.
5. **Opcional:** selecione uma linha do tempo e clique em **Excluir**. Ou clique em **Excluir tudo** para limpar as configurações.
6. Clique em **Salvar**.

Definir Atendimento Manual via Web

Defina o modo de presença como manual e você deve selecionar um status manualmente ao receber presença.

Antes de começar

Adicione pelo menos um usuário e defina o modo de autenticação do usuário. Para obter detalhes, consulte *Gerenciamento de usuários*.

Passos

1. Clique em **Configuração → Status de T&A** para entrar na página de configurações.
2. Defina o **Modo de Atendimento** como **Manual**.
3. Habilite o **Status** de **Presença Obrigatório** e defina o status **de** presença por duração.
4. Habilite um grupo de status de presença.

Nota

A Propriedade de Assiduidade não será alterada.

5. **Opcional:** selecione um status e altere seu nome, se necessário.

Resultado

Você deve selecionar um status de presença manualmente após a autenticação.

Nota

Se você não selecionar um status, a autenticação falhará e não será marcada como uma presença válida.

Definir Atendimento Automático via Web

Defina o modo de presença como automático e você pode definir o status de presença e sua agenda disponível. O sistema alterará automaticamente o status de presença de acordo com a programação configurada.

Antes de começar

Adicione pelo menos um usuário e defina o modo de autenticação do usuário. Para obter detalhes, consulte *Gerenciamento de usuários*.

Passos

1. Clique em **Configuração → Status de T&A** para entrar na página de configurações.
2. Defina o **Modo de Atendimento** como **Automático**.
3. Habilite a função **Status de Presença Necessária**.
4. Habilitar a grupo de assiduidade estado.

Nota

A Propriedade de Assiduidade não será alterada.

5. **Opcional:** selecione um status e altere seu nome, se necessário.
6. Defina a agenda do status. Refere-se a ***Time SeFngs*** para obter detalhes.

Definir Atendimento Manual e Automático via Web

Defina o modo de atendimento como **Manual** e **Automático**, e o sistema alterará automaticamente o status de presença de acordo com a programação configurada. Ao mesmo tempo, você pode alterar manualmente o status de presença após a autenticação.

Antes de começar

Adicione pelo menos um usuário e defina o modo de autenticação do usuário. Para obter detalhes, consulte *Gerenciamento de usuários*.

Passos

1. Clique em **Configuração → Status de T&A** para entrar na página de configurações.
2. Defina o **Modo de Atendimento** como **Manual e Automático**.
3. Habilite a função **Status de Presença Necessária**.

4. Habilitar a grupo de assiduidade estado.

Nota

A Propriedade de Assiduidade não será alterada.

5. Opcional: selecione um status e altere seu nome, se necessário.

6. Defina a agenda do status. Refere-se a ***Time SeFngs*** para obter detalhes.

Resultado

Na página inicial e autenticar. A autenticação será marcada como o status de presença configurado de acordo com a programação. Se você tocar no ícone de edição na guia de resultados, poderá selecionar um status para receber a participação manualmente, a autenticação será marcada como o status de presença editada.

Exemplo

Se definir o Break **Out** como segunda-feira 11:00 e **Break In** como segunda-feira 12:00, a autenticação do usuário válido de segunda-feira 11:00 a 12:00 será marcada como quebra.

10.6.14 Definir parâmetros

biométricos Definir parâmetros

básicos

Clique em **Configuração → Smart → Smart** .

Nota

As funções variam de acordo com diferentes modelos. Refere-se ao dispositivo real para obter detalhes.

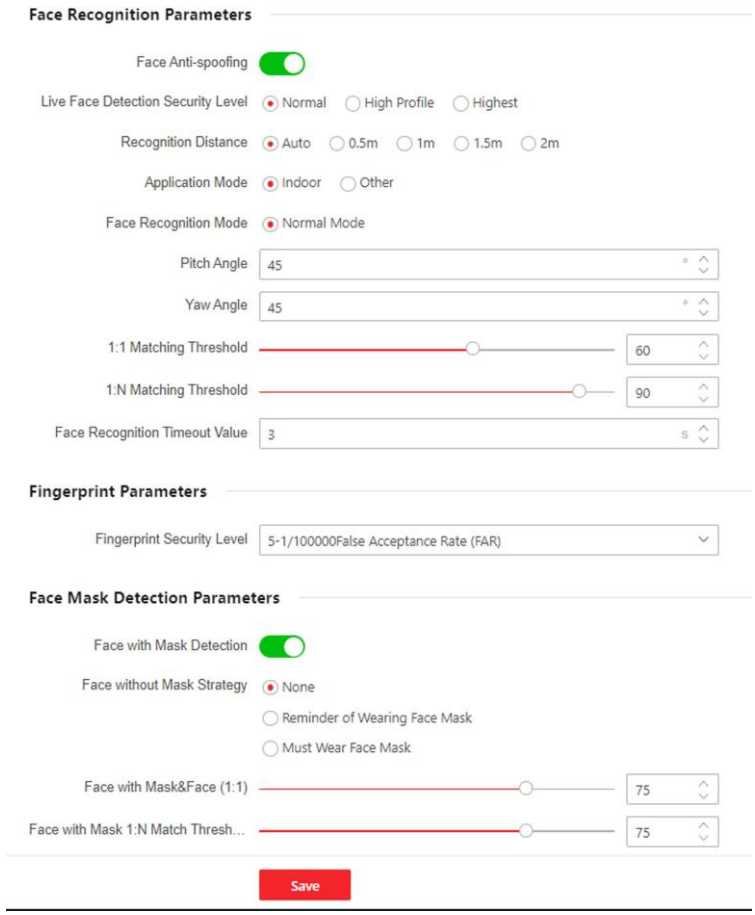


Figura 10-10 Página de configurações inteligentes

Clique em **Salvar** para salvar as configurações após a configuração.

Face Anti-spoofing

Ative ou desative a função de detecção de rosto ao vivo. Ao ativar a função, o dispositivo pode reconhecer se a pessoa é viva ou não.

Nota

Os produtos de reconhecimento biométrico não são completamente aplicáveis a ambientes antifalsificação. Se você precisar de um nível de segurança mais alto, use vários modos de autenticação.

Nível de segurança de detecção de rosto ao vivo

Depois de habilitar a função antifalsificação facial, você pode definir o nível de segurança correspondente ao executar a autenticação facial ao vivo.

Distância de Reconhecimento

Selecione a distância entre o usuário autenticador e a câmera do dispositivo.

Modo de Aplicação

Selecione outros ou internos de acordo com o ambiente real.

Modo de

Reconhecimento

Facial de Modo

Normal

Reconheça o rosto através da câmera normalmente.

Ângulo de inclinação

O ângulo de inclinação máximo ao iniciar a autenticação de face.

Ângulo de guinada

O ângulo de guinada máximo ao iniciar a autenticação de face.

Limite de correspondência 1:1

Defina o limite de correspondência ao autenticar por meio do modo de correspondência 1 :1. Quanto maior o valor, menor a taxa de aceitação falsa e maior a taxa de falsa rejeição.

1:N Limiar de Correspondência

Defina o limite de correspondência ao autenticar por meio do modo de correspondência 1: N. Quanto maior o valor, menor a taxa de aceitação falsa e maior a taxa de falsa rejeição.

Valor de Tempo Limite de Reconhecimento Facial

Defina o valor de tempo limite ao reconhecer o rosto. Se o tempo de reconhecimento facial for maior do que o valor configurado, o sistema exibirá um prompt.

Detecção de Rosto sem Máscara

Depois de ativar o rosto sem detecção de máscara, o sistema reconhecerá o rosto capturado com imagem de máscara ou não. Você pode definir o rosto com o limite de correspondência mask1:N, é o modo ECO e a estratégia.

Nenhum

A função está desativada. O dispositivo não detectará se uma pessoa está usando uma máscara facial ou não.

Lembrete do uso de máscara facial

Se a pessoa não usar a máscara facial ao se autenticar, o dispositivo exibirá um prompt e a porta será aberta.

Deve usar máscara facial

Se a pessoa não usar a máscara facial ao autenticar, o dispositivo exibirá um prompt e a porta permanecerá fechada.

Rosto com máscara e rosto (1:1)

Defina o valor correspondente ao autenticar com máscara facial por meio do modo de correspondência 1 :1. Quanto maior o valor, menor a taxa de aceitação falsa e maior a taxa de falsa rejeição.

Rosto com Máscara 1:N Limiar de Correspondência

Defina o limite de correspondência ao autenticar com máscara facial por meio do modo de correspondência 1: N. Quanto maior o valor, menor a taxa de aceitação falsa e maior a taxa de

falsa rejeição.

Definir área de reconhecimento

Clique em **Configuração → Configuração da Área de → Inteligente** .
Arraste o quadro amarelo no vídeo ao vivo para ajustar a área de reconhecimento. Somente a face dentro da área pode ser reconhecida pelo sistema.
Clique em **Salvar** para salvar as configurações.
Clique ou para gravar vídeos ou capturar imagens.

10.6.15 Definir preferência

Você pode definir o tema de exibição e o tempo de suspensão do dispositivo.

Definir tema

Clique em **Configuração → Preferência** .

Dormir

Habilite a suspensão e o dispositivo entrará no modo de suspensão quando nenhuma operação dentro do tempo de suspensão configurado.

Modo de Exibição

Você pode selecionar o tema de exibição para autenticação de dispositivo. Você pode selecionar **Modo de exibição** como **Padrão** ou **Simples**. Quando você seleciona **Simples**, as informações de nome, ID, imagem do rosto não serão exibidas.

10.6.16 Atualização e manutenção

Reinicialize o dispositivo, restaure os parâmetros do dispositivo e atualize a versão do dispositivo.

Dispositivo de reinicialização

Clique em Manutenção **e Segurança → Manutenção →**
Reiniciar . Clique em **Reiniciar** para reiniciar o dispositivo.

Melhoramento

Clique em Manutenção **e Segurança → Manutenção → Atualização** .
Selecione um tipo de atualização na lista suspensa. Clique e selecione o arquivo de atualização do seu PC local. Clique em **Atualizar** para iniciar a atualização.
Se o dispositivo tiver sido conectado ao Hik-Connect e à rede, quando houver um novo pacote de instalação no Hik-Connect, você poderá clicar em **Atualizar** após a Atualização Online para atualizar o sistema do dispositivo.

Nota

Não desligue durante a atualização.

Restaurar parâmetros

Clique em Manutenção e **Segurança → Manutenção → Backup e Redefinição** .

Restaurar tudo

Todos os parâmetros serão restaurados para as configurações de fábrica. Você deve ativar o dispositivo antes do uso.

Restaurar

O dispositivo será restaurado para as configurações padrão, exceto para o endereço IP do dispositivo e as informações do usuário.

Parâmetros de importação e exportação

Clique em Manutenção e **Segurança → Manutenção → Backup e Redefinição** .

Exportação

Clique em **Exportar** para exportar os parâmetros do dispositivo.

Nota

Você pode importar os parâmetros do dispositivo exportado para outro dispositivo.

Importação

Clique e selecione o arquivo a ser importado. Clique em **Importar** para iniciar a importação do arquivo de configuração.

10.6.17 Depuração de dispositivos

Você pode definir parâmetros de depuração de dispositivo.

Passos

1. Clique em Manutenção **e Segurança → Manutenção → Depuração de Dispositivos** .
2. Você pode definir os seguintes parâmetros.

Habilitar SSH

Para aumentar a segurança da rede, desative o serviço SSH. A configuração é usada apenas para depurar o dispositivo para os profissionais.

Imprimir Log

Você pode clicar em **Exportar** para exportar o log.

Capturar pacote de rede

Você pode definir a **Duração** do Pacote de **Captura**, **o Tamanho do Pacote de Captura** e clicar em **Iniciar** para capturar.

10.6.18 Consulta de log

Você pode pesquisar e visualizar os logs do dispositivo.

Vá para **Manutenção e Segurança → Manutenção → Log** .

Defina o tipo principal e secundário do tipo de log. Defina a hora de início e a hora de término da pesquisa e clique em **Pesquisar**.

Os resultados serão exibidos abaixo, que incluem o No., a hora, o tipo principal o tipo secundário, o canal No., as informações do usuário local / remoto, o IP do host remoto, etc.

10.6.19 Configurações do Modo de Segurança

Defina o modo de segurança para registrar no software cliente.

Na página Dispositivo para Gerenciamento, clique em **Manutenção e** Segurança → **Serviço de** Segurança → **Segurança** .

Selecione um modo de segurança e

clique em **Salvar**. **Modo de segurança**

Alto nível de segurança para verificação de informações do usuário ao efetuar login no software cliente.

Modo compatível

A verificação das informações do usuário é compatível com a versão antiga do software cliente ao efetuar login.

10.6.20 Gerenciamento de Certificados

Ele ajuda a gerenciar os certificados de servidor/cliente e o certificado de autoridade de certificação.

Nota

A função só é suportada por determinados modelos de dispositivos.

Criar e instalar certificado autoassinado

Passos

1. Vá para **Manutenção e Segurança → Gerenciamento de Certificados de → de Segurança** .
2. Na área **Arquivos** de Certificado , selecione um **Tipo** de **Certificado** na lista suspensa.
3. Clique em **Criar**.
4. Insira informações de certificado .
5. Clique em **OK** para salvar e instalar o certificado.

O certificado criado é exibido na área **Detalhes** do **Certificado**. O certificado será salvo automaticamente.

6. Baixe o certificado e salve-o em um arquivo de solicitação no computador local.
7. Envie o arquivo de solicitação para uma autoridade de certificação para assinatura.
8. Importe o certificado assinado.

1) Selecione um tipo de certificado na área **Importar Senhas**, selecione um certificado no local e clique em **Instalar**.

2) Selecione um tipo de certificado na área **Importar Certificado** de **Comunicação**, selecione um certificado no local e clique em **Instalar**.

Instalar outro certificado autorizado

Se você já tiver um certificado autorizado (não criado pelo dispositivo), poderá importá-lo diretamente para o dispositivo.

Passos

1. Vá para **Manutenção e Segurança → Gerenciamento de Certificados de → de Segurança** .
2. Nas áreas Importar **Senhas** e **Importar Certificado de Comunicação**, selecione o tipo de certificado e carregue o certificado.
3. Clique em **Instalar**.

Instalar o certificado de autoridade de certificação

Antes de começar

Prepare um certificado de autoridade de certificação com antecedência.

Passos

1. Vá para **Manutenção e Segurança → Gerenciamento de Certificados de → de Segurança** .
2. Criar ano ID em o **Importação CA Certificado** área.

Nota

A ID do certificado de entrada não pode ser a mesma que as existentes.

3. Carregue um arquivo de certificado do local.
4. Clique em **Instalar**.

Capítulo 11 Configuração do Software Cliente

11.1 Fluxo de configuração do software cliente

Siga o diagrama de fluxo abaixo para configurar no software cliente.

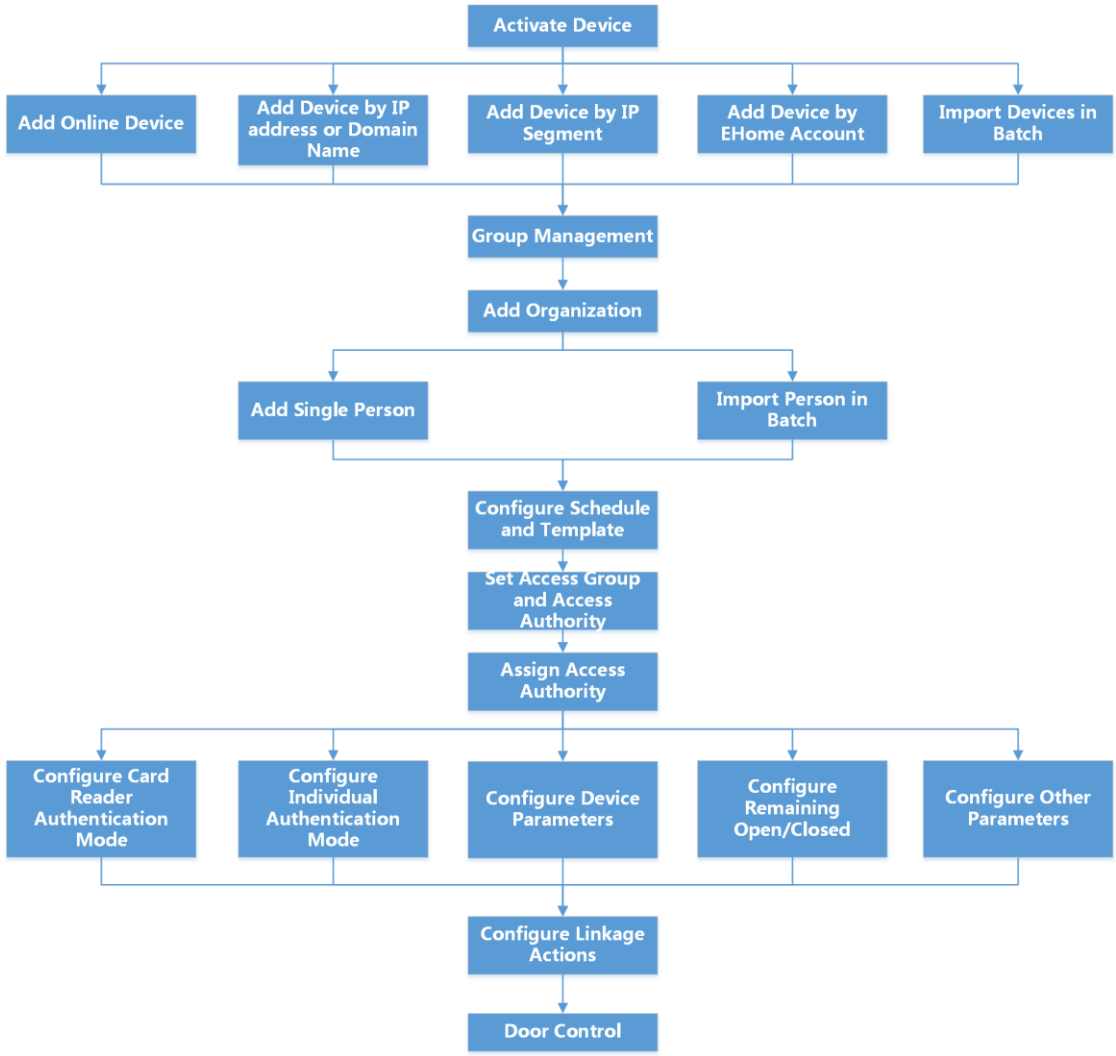


Figura 11-1 Diagrama de fluxo da configuração no software cliente

11.2 Gerenciamento de dispositivos

O cliente oferece suporte ao gerenciamento de dispositivos de controle de acesso e dispositivos de vídeo porteiro.

Exemplo
Você pode controlar a entrada e saída e gerenciar o atendimento depois de adicionar dispositivos de controle de acesso ao cliente; você pode executar o interfone de vídeo com as estações internas e as estações de porta.

11.2.1 Adicionar dispositivo

O cliente fornece três modos de adição de dispositivos, incluindo por IP /domínio, segmento IP e protocolo EHome. O cliente também oferece suporte à importação de vários dispositivos em lote quando há uma grande quantidade de dispositivos a serem adicionados.

Adicionar dispositivo por endereço IP ou nome de domínio

Se você souber o endereço IP ou o nome de domínio do dispositivo a ser adicionado, poderá adicionar dispositivos ao cliente especificando o endereço IP (ou nome de domínio), nome de usuário, senha, etc.

Passos
1. Entre no módulo Gerenciamento de dispositivos .
2. Clique na guia **Dispositivo** na parte superior do painel direito.
   Os dispositivos adicionados são exibidos no painel direito.
3. Clique em Adicionar para abrir a janela Adicionar e selecione **IP/Domínio** como o modo de adição.
4. Insira as informações necessárias.

   Nome

   Crie um nome descritivo para o dispositivo. Por exemplo, você pode usar um apelido que pode mostrar a localização ou o recurso do dispositivo.

   Endereço

   O endereço IP ou nome de domínio do dispositivo.

   Porta

   Os dispositivos a serem adicionados compartilham o mesmo número de porta. O valor padrão é ***8000***.

   Nome de usuário

   Insira o nome de usuário do dispositivo. Por padrão, o nome de usuário é ***admin***.

   Senha

   Digite a senha do dispositivo.

   Cuidado

   A força da senha do dispositivo pode ser verificada automaticamente. É altamente recomendável que você altere a senha de sua própria escolha (usando um mínimo de 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: letras maiúsculas, letras minúsculas , números e caracteres especiais) para aumentar a segurança do seu produto. E recomendamos

você muda sua senha regularmente, especialmente no sistema de alta segurança, alterando a senha mensal ou semanalmente pode proteger melhoro seu produto.
A configuração adequada de todas as senhas e outras configurações de segurança é de responsabilidade do instalador e/ou usuário final.

5. **Opcional: Verifique a Criptografia de Transmissão** (TLS) para habilitar a criptografia de transmissão usando o protocolo TLS (Transport Layer Security) para fins de segurança.

Nota

- Esta função deve ser suportada pelo dispositivo.
- Se você tiver habilitado a Verificação de Certificado, clique em **Abrir Diretório de Certificados** para abrir a pasta padrão e copie o arquivo de certificado exportado do dispositivo para esse diretório padrão para fortalecer a segurança. Consulte para obter detalhes sobre como habilitar a verificação de certificados.
- Você pode fazer login no dispositivo para obter o arquivo de certificado pelo navegador da Web.

6. Marque **Synchronize Time** para sincronizar a hora do dispositivo com o PC que executa o cliente depois de adicionar o dispositivo ao cliente.
7. **Opcional:** Marque **Importar para Grupo** para criar um grupo pelo nome do dispositivo e importe todos os canais do dispositivo para esse grupo.

Exemplo

Para o dispositivo de controle de acesso, seus pontos de acesso, entradas/saídas de alarme e canais de codificação (se existirem) serão importados para esse grupo.

8. Termine de adicionar o dispositivo.
   - Clique em **Adicionar** para adicionar o dispositivo e voltar à página de listagem do dispositivo.
   - Clique em **Adicionar** e **Novo** para salvar as configurações e continuar a adicionar outro dispositivo.

Importar dispositivos em lote

Você pode adicionar vários dispositivos ao cliente em um lote inserindo os parâmetros do dispositivo em um arquivo CSV predefinido.

Passos

1. Entre no módulo Gerenciamento de dispositivos.
2. Clique na guia **Dispositivo** na parte superior do painel direito.
3. Clique em Adicionar para abrir a janela Adicionar e selecione **Importação em lote** como o modo de adição.
4. Clique em **Exportar Modelo** e, em seguida, guarde o modelo predefinido (ficheiro CSV) no PC.
5. Abra o arquivo de modelo exportado e insira as informações necessárias dos dispositivos a serem adicionados na coluna correspondente.

Nota

Para obter uma descrição detalhada dos campos obrigatórios, consulte as introduções no modelo.

Adicionando modo

Digite ***0*** ou ***1*** ou ***2***.

Endereço

Edite o endereço do dispositivo.

Porta

Insira o número da porta do dispositivo. O número da porta padrão é ***8000***.

Nome de usuário

Insira o nome de usuário do dispositivo. Por padrão, o nome de usuário é ***admin***.

Senha

Digite a senha do dispositivo.

Cuidado

A força da senha do dispositivo pode ser verificada automaticamente. É altamente recomendável que você altere a senha de sua própria escolha (usando um mínimo de 8 caracteres, incluindo pelo menos osseguintes tipos de 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, alterando a senha mensal ou semanalmente pode proteger melhor seu produto. A configuração adequada de todas as palavras-passe e outras definições de segurança é da responsabilidade do nstaller e/ou do utilizador final.

Importar para o grupo

Digite ***1*** para criar um grupo pelo nome do dispositivo. Todos os canais do dispositivo serão importados para o grupo correspondente por padrão. Digite ***0*** para desativar essa função.

6. Clique e selecione o arquivo de modelo.

7. Clique em **Adicionar** para importar os dispositivos.

11.2.2 Redefinir senha do dispositivo

Se você esqueceu a senha dos dispositivos on-line detectados, poderá redefinir a senha do dispositivo por meio do cliente.

Passos

1. Entre na página Gerenciamento de dispositivos.

2. Clique em **Dispositivo Online** para mostrar a área do dispositivo online.

Todos os dispositivos online que compartilham a mesma sub-rede serão exibidos na lista.

3. Selecione o dispositivo na lista e clique na coluna Operação.

4. Redefina a senha do dispositivo.

- Clique em **Gerar** para abrir a janela QR Code e clique em **Download** para salvar o código QR no seu PC. Você também pode tirar uma foto do código QR para salvá-lo em seu telefone. Envie a foto para o nosso suporte técnico.

Nota

Durante o seguinte Operações durante Redefinir o senha contato nosso técnico apoio.

Cuidado

A força da senha do dispositivo pode ser verificada automaticamente. É altamente recomendávelque você altere a senha de sua própria escolha (usando um mínimo de 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: 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, alterando a senha mensal 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 do usuário final.

11.2.3 Gerenciar dispositivos adicionados

Depois de adicionar dispositivos à lista de dispositivos, você pode gerenciar os dispositivos adicionados, incluindo a edição de parâmetros do dispositivo, configuração remota, visualização do status do dispositivo, etc.

Tabela 11-1 Gerenciar dispositivos adicionados

Editar dispositivo	Clique para editar as informações do dispositivo, incluindo nome do dispositivo, endereço, nome de usuário, senha, etc.
Excluir dispositivo	Verifique um ou mais dispositivos e clique em **Excluir** para excluir os dispositivos selecionados.
Configuração remota	Clique para definir a configuração remota do dispositivo correspondente. Para obter detalhes, consulte o manual do usuário do dispositivo.
Exibir status do dispositivo	Clique para ver o status do dispositivo, incluindo o número da porta, o status da porta, etc. **Nota** Para dispositivos diferentes , você exibirá informações diferentes sobre o status do dispositivo.
Exibir usuário on-line	Clique para ver os detalhes do usuário on-line que acessa o dispositivo, incluindo nome de usuário, tipo de usuário, endereço IP e tempo de login.
Atualizar informações do dispositivo	Clique para atualizar e obter as informações mais recentes sobre o dispositivo.

11.3 Gerenciamento de Grupo

O cliente fornece grupos para gerenciar os recursos adicionados em diferentes grupos. Você pode agrupar os recursos em diferentes grupos de acordo com os locais dos recursos.

Exemplo
Por exemplo, no 1º andar, montaram 16 portas, 64 entradas de alarme e 16 saídas de alarme. Você pode organizar esses recursos em um grupo (chamado 1º andar) para um gerenciamento conveniente. Você pode controlar o status da porta e fazer algumas outras operações dos dispositivos depois de gerenciar os recursos por grupos.

11.3.1 Adicionar grupo

Você pode adicionar grupo para organizar o dispositivo adicionado para um gerenciamento conveniente.

Passos
1. Entre no módulo Gerenciamento de dispositivos.
2. Clique em Gerenciamento de **Dispositivos → Grupo** para entrar na página de gerenciamento de grupo.
3. Crie um grupo.
   - Clique em **Adicionar Grupo** e insira um nome de grupo como desejar.
   - Clique em **Criar** grupo **por** nome de dispositivo e selecione um dispositivo adicionado para criar um novo grupo pelo **nome** do dispositivo selecionado.

Nota

Os recursos (como entradas/saídas de alarme, pontos de acesso, etc.) deste dispositivo será importado para o grupo por padrão.

11.3.2 Importar recursos para o grupo

Você pode importar os recursos do dispositivo (como entradas/saídas de alarme, pontos de acesso, etc.) para o grupo adicionado em um lote.

Antes de começar
Adicione um grupo para gerenciar dispositivos. Consulte Adicionar ***grupo*** .

Passos
1. Entre no módulo Gerenciamento de dispositivos.
2. Clique em Gerenciamento de **Dispositivos → Grupo** para entrar na página de gerenciamento de grupo.
3. Selecione um grupo na lista de grupos e selecione o tipo de recurso como Ponto de **Acesso**, **Entrada** de Alarme, **Saída de Alarme**, etc.
4. Clique em **Importar**.
5. Selecione as miniaturas/nomes dos recursos na visualização de miniaturas/ lista.

Nota

Você pode clicar ou alternar o modo de exibição de recursos para o modo de exibição de miniatura ou para o modo de exibição de lista.

6. Clique em **Importar** para importar os recursos selecionados para o grupo.

11.4 Gestão de Pessoas

Você pode adicionar informações pessoais ao sistema para outras operações, como controle de acesso, vídeo porteiro, tempo e presença, etc. Você pode gerenciar as pessoas adicionadas, como emitir cartões para elas em um lote, importar e exportar informações pessoais em um lote, etc.

11.4.1 Adicionar organização

Você pode adicionar uma organização e importar informações pessoais para a organização para um gerenciamento eficaz das pessoas. Você também pode adicionar uma organização de sobrebodina para a adicionada.

Passos

1. Insira **o módulo Pessoa** .

2. Selecione uma organização pai na coluna esquerda e clique em **Adicionar** no canto superior esquerdo para adicionar uma organização.

3. Criar a nome durante o Adicionado organização.

Nota

Até 10 níveis de organizações podem ser adicionados.

4. Opcional: Execute a(s) seguinte(s) operação(ões).

Editar Organização	Passe o mouse sobre uma organização adicionada e clique para editar seu nome.
Excluir organização	Passe o mouse sobre uma organização adicionada e clique para excluí-la.

Nota

- O nível inferior Organizações vontade ser deletado como poço se você excluir ano organização.
- Verifique se não há nenhuma pessoa adicionada sob a organização ou se a organização não pode ser excluída.

Mostrar Pessoas na Sub-Organização	**Marque Mostrar Pessoas na Suborganização** e selecione uma organização para mostrar as pessoas em suas suborganizações.

11.4.2 Informações de identificação de pessoa de importação e exportação

Você pode importar as informações e imagens de várias pessoas para o software cliente em um lote. Enquanto isso, você também pode exportar as informações e fotos da pessoa e salvá-las em seu PC.

Importar informações de pessoa

Você pode inserir as informações de várias pessoas em um modelo predefinido (arquivo CSV/Excel) para importar as informações para o cliente em um lote.

Passos

1. Entre no módulo Pessoa.
2. Selecione uma organização adicionada na lista ou clique em **Adicionar** no canto superior esquerdo para adicionar uma organização e selecione-a.
3. Clique em **Importar** para abrir o painel Importar.
4. Selecione **Informações da pessoa** como o modo de importação.
5. Clique em **Baixar** modelo para **importar pessoa** para baixar o modelo.
6. Entrar o pessoa informação em o Baixado modelo.

Nota

- Se a pessoa tiver vários cartões, separe o cartão Não. com ponto-e-vírgula.
- Itens com asterisco são necessários.
- Por padrão, a Data de Contratação é a data atual.

7. Clique para selecionar o arquivo CSV/Excel com informações pessoais do PC local.
8. Clique **Importação** Para começar Importação.

Nota

- Se uma pessoa Não. já existe no banco de dados do cliente, exclua as informações existentes antes de importar.
- Você pode importar informações de não mais de 2.000 pessoas.

Importar imagens de pessoa

Depois de importar fotos faciais para as pessoas adicionadas ao cliente, as pessoas nas fotos podem ser identificadas por um terminal de reconhecimento facial adicionado. Você pode importar imagens de pessoas uma a uma ou importar várias imagens de cada vez, de acordo com sua necessidade.

Antes de começar

Certifique-se de ter importado informações pessoais para o cliente de antemão.

Passos

1. Entre no módulo Pessoa.
2. Selecione uma organização adicionada na lista ou clique em **Adicionar** no canto superior esquerdo para adicionar uma organização e selecione-a.
3. Clique em Importar para abrir o painel **Importar** e marque **Face**.
4. **Opcional:** habilite **Verificar por** dispositivo para verificar se o dispositivo de reconhecimento facial gerenciado no cliente pode reconhecer o rosto na foto.
5. Clique para selecionar um arquivo de imagem de rosto.

Nota

- A (pasta de) imagens de rosto deve estar no formato ZIP.
- Cada arquivo de imagem deve estar no formato JPG e não deve ser maior que 200 KB.
- Cada arquivo de imagem deve ser nomeado como "Pessoa ID_Name". O ID da pessoa deve ser o mesmo com o das informações da pessoa importada.

6. Clique em **Importar** para iniciar a importação.
O progresso e o resultado da importação serão exibidos.

Exportar informações pessoais

Você pode exportar as informações das pessoas adicionadas para o PC local como um arquivo CSV/Excel.

Antes de começar
Certifique-se de ter adicionado pessoas a uma organização.

Passos
1. Entre no módulo Pessoa.
2. Opcional: Selecionar ano organização em o lista.

Nota

As informações de todas as pessoas serão exportadas se você não selecionar nenhuma organização.

3. Clique em **Exportar** para abrir o painel Exportar.
4. Marque **Informações da Pessoa** como o conteúdo a ser exportado.
5. Verifique os itens desejados para exportar.
6. Clique em **Exportar** para salvar o arquivo exportado no arquivo CSV/Excel no seu PC.

Exportar fotos de pessoa

Você pode exportar o arquivo de imagem facial das pessoas adicionadas e salvar no seu PC.

Antes de começar
Certifique-se de ter adicionado pessoas e suas fotos de rosto a uma organização.

Passos
1. Entre no módulo Pessoa.
2. Opcional: Selecionar ano organização em o lista.

Nota

As fotos do rosto de todas as pessoas serão exportadas se você não selecionar nenhuma organização.

3. Clique em Exportar para abrir o painel Exportar e marque **Face** como o conteúdo a ser exportado.
4. Clique em **Exportar** para iniciar a exportação.

Nota

- O arquivo exportado está no formato ZIP.
- A imagem de rosto exportada é nomeada como "Pessoa ID_Name_0" ("0" é para uma face frontal completa).

11.4.3 Obter informações pessoais do dispositivo de controle de acesso

Se o dispositivo de controle de acesso adicionado tiver sido configurado com informações da pessoa (incluindo detalhes da pessoa, impressão digital e informações do cartão emitido), você poderá obter as informações da pessoa do dispositivo e importá-las para o cliente para operações adicionais.

Passos

Nota

- Se o nome da pessoa armazenada no dispositivo estiver vazio, o nome da pessoa será preenchido com o número do cartão emitido. depois de importar para o cliente.
- Se o número do cartão ou ID da pessoa (ID do funcionário) armazenado no dispositivo já existir no banco de dados do cliente , a pessoa com esse número de cartão ou ID de pessoa não será importada para o cliente.

1. Insira **o módulo Pessoa** .
2. Selecione uma organização para importar as pessoas.
3. Clique em **Obter do dispositivo**.
4. Selecionar ano Adicionado acesso Controle dispositivo ou o inscrição estação De o lista suspensa

Nota

lista.

Se você selecionar a estação de registro, deverá clicar em **Login** e definir Endereço IP, porta No., nome de usuário e senha do dispositivo.

5. Clique **Importação** Para começar Importação o pessoa informação Para o cliente.

Nota

Até 2.000 pessoas e 5.000 cartões podem ser importados.

As informações da pessoa, incluindo os detalhes da pessoa, as informações da impressão digital da pessoa (se configuradas) e os cartões vinculados (se configurados), serão importadas para a organização selecionada.

11.4.4 Emitir cartões para pessoas em lote

O cliente fornece uma maneira conveniente de emitir cartões para várias pessoas em um lote.

Passos

1. Insira **o módulo Pessoa** .
2. Clique em **Cartões** de **emissão em lote**.

Todas as pessoas adicionadas sem cartão emitido serão exibidas no painel direito.

3. **Opcional** : Insira palavras-chave (nome ou ID da pessoa) na caixa de entrada para filtrar a(s) pessoa(s) que precisa (m) de emitir cartões.
4. **Opcional:** Clique em **Configurações** para definir os parâmetros de emissão do cartão. Para obter detalhes, consulte *Emitir um cartão pelo modo local*.
5. Clique em **Inicializar** para inicializar a estação de registro de cartão ou o leitor de cartão para prepará-lo para a emissão de cartões.
6. Clique no **número do cartão.** e insira o número do cartão.
   - Coloque o cartão na estação de inscrição do cartão.
   - Passe o cartão no leitor de cartões.
   - Insira manualmente o número do cartão e pressione a tecla Enter. A(s) pessoa(s) na lista serão(ão) emitido(s) cartão(ões).

11.4.5 Perda de Cartão de Relatório

Se a pessoa perdeu seu cartão , você pode relatar a perda do cartão para que a autorização de acesso relacionada ao cartão fique inativa.

Passos

1. Insira **o módulo Pessoa** .
2. Selecione a pessoa para a qual você deseja denunciar a perda do cartão e clique em Editar para abrir a janela Editar pessoa.
3. No painel **Credencial → Cartão**, clique no cartão adicionado para definir este cartão como cartão perdido.
   Após a perda do cartão de relatório , a autorização de acesso deste cartão será inválida e inativa. Outra pessoa que recebe este cartão não pode acessar as portas passando este cartão perdido.
4. **Opcional:** Se o cartão perdido for encontrado, você pode clicar para cancelar a perda.
   Após o cancelamento da perda do cartão, a autorização de acesso da pessoa será válida e ativa.
5. Se o cartão perdido for adicionado a um grupo de acesso e o grupo de acesso já estiver aplicado ao dispositivo, após relatar a perda do cartão ou cancelar a perda do cartão, uma janela será exibida para notificá-lo para aplicar as alterações ao dispositivo. Depois de aplicar ao dispositivo , essas alterações podem ter efeito no dispositivo.

11.4.6 Definir parâmetros de emissão de cartão

O cliente fornece dois modos para ler o número de um cartão: através da estação de registro do cartão ou através do leitor de cartão do dispositivo de controle de acesso. Se uma estação de registro de cartão estiver disponível,conecte-a ao PC que executa o cliente por interface USB ou COM e coloque o cartão no registro do cartão para ler o número do cartão. Caso contrário, você também pode passar o cartão no leitor de cartão do dispositivo de controle de acesso adicionado para obter o número do cartão. Como resultado, antes de emitir um cartão para uma pessoa, você precisa definir os parâmetros de emissão do cartão, incluindo o modo de emissão e os parâmetros relacionados.

Ao adicionar um cartão a uma pessoa, clique em Configurações para abrir a janela **Configurações** de emissão do cartão.

Modo Local: Emitir Cartão por Estação de Registro de Cartão

Conecte uma estação de registro de cartão ao PC que executa o cliente. Você pode colocar o cartão na estação de inscrição do cartão para obter o número do cartão.

Estação de Inscrição de Cartão

Selecione o modelo da estação de registro de cartão conectado

Nota

Atualmente, os modelos de estação de registro de placa suportados incluem DS-K1F100-D8, DS-K1F100-M , DS-K1F100-D8E e DS-K1F180-D8E.

Tipo de cartão

Este campo só está disponível quando o modelo é DS-K1F100-D8E ou DS-K1F180-D8E. Selecione o tipo de cartão como cartão EM ou cartão IC de acordo com o tipo de cartão real.

Porta serial

Só está disponível quando o modelo é DS-K1F100-M.

Selecione o COM ao qual a estação de registro do cartão se conecta.

Zumbido

Ative ou desative o zumbido quando o número do cartão for lido com êxito.

Nº do cartão Tipo

Selecione o tipo de número do cartão de acordo com as necessidades actua l.

Criptografia de cartão M1

Este campo só está disponível quando o modelo é DS-K1F100-D8, DS-K1F100-D8E ou DS-K1F180-D8E.

Se o cartão for o cartão M1 e se você precisar ativar a função de criptografia do cartão M1, você deve ativar essa função e selecionar o setor do cartão a ser criptografado.

Modo remoto: Cartão de emissão por leitor de cartão

Selecione um dispositivo de controle de acesso adicionado ao cliente e passe o cartão em seu leitor de cartão para ler o número do cartão.

11.5 Configurar cronograma e modelo

Você pode configurar o modelo, incluindo a programação de feriados e semanas. Depois de definir o modelo, você pode adotar o modelo configurado para acessar grupos ao definir os grupos de acesso, para que o grupo de acesso tenha efeito nas durações de tempo do modelo.

Nota

Para obter as configurações do grupo de acesso, consulte ***Definir*** grupo de ***acesso para atribuir autorização de acesso a pessoas*** .

11.5.1 Adicionar Feriado

Você pode criar feriados e definir os dias nos feriados, incluindo data de início, data de término e duração do feriado em um dia.

Passos

Nota

Você pode adicionar até 64 feriados no sistema de software.

1. Clique em **Controle de Acesso → Agendar → Feriados** para entrar na página Feriados.
2. Clique em **Adicionar** no painel esquerdo.
3. Crie um nome para o feriado.
4. **Opcional:** insira as descrições ou algumas notificações deste feriado na caixa Observação .
5. Adicionar a feriado período Para o feriado lista e configurar o feriado duração.

Nota

Até 16 períodos de férias podem ser adicionados a um feriado.

1) Clique em **Adicionar** no campo Lista de Feriados.
2) Arraste o cursor para desenhar a duração do tempo, o que significa que nesse período de tempo, o grupo de acesso configurado é ativado.

Nota

Até 8 durações de tempo podem ser definidas para um período de férias.

3) **Opcional:** Execute as seguintes operações para editar as durações de tempo.
   - Mova o cursor para a duração do tempo e arraste a duração do tempo na barra da linha do tempo para a posição desejada quando o cursor se transformar em .
   - Clique na duração da hora e edite diretamente a hora de início/término na caixa de diálogo exibida.
   - Mova o cursor para o início ou o fim da duração do tempo e arraste para alongar ou encurtar a duração do tempo quando o cursor se voltar para .
4) **Opcional:** selecione a(s) duração(ões) de tempo que precisa(m) ser excluída(s) e clique na coluna Operação para excluir a(s) duração(ões) de tempo selecionada(s).
5) **Opcional:** Clique na coluna Operação para limpar todas as durações de tempo na barra de tempo.
6) **Opcional:** Clique na coluna Operação para excluir esse período de feriado adicionado da lista de feriados.
6. Clique em **Salvar**.

11.5.2 Adicionar modelo

O modelo inclui programação de semana e feriado. Você pode definir a programação da semana e atribuir a duração do tempo de autorização de acesso para diferentes pessoas ou grupos. Você também pode selecionar o(s) feriado(s) adicionado(s) para o modelo.

Passos

Nota

Você pode adicionar até 255 modelos no sistema de software.

1. Clique **Acesso Controle → Horário → Modelo** Para entrar o Modelo página.

Nota

Há dois modelos padrão: Autorizado durante todo o dia e Dia inteiro negado, e eles não podem ser editados ou excluídos.

Autorizado durante todo o dia

A autorização de acesso é válida em todos os dias da semana e não tem feriado.

Dia inteiro negado

A autorização de acesso é inválida em cada dia da semana e não tem feriado.

2. Clique em **Adicionar** no painel esquerdo para criar um novo modelo.
3. Crie um nome para o modelo.
4. Insira as descrições ou alguma notificação desse modelo na caixa Observação .
5. Edite a programação da semana para aplicá-la ao modelo.
   1) Clique na guia **Agenda da semana** no painel inferior.
   2) Selecione um dia da semana e desenhe durações(ões) de tempo na barra da linha do tempo.

Nota

Até 8 duração(ões) de tempo podem ser definidas para cada dia na programação da semana.

   3) **Opcional:** Execute as seguintes operações para editar as durações de tempo.
      - Mova o cursor para a duração do tempo e arraste a duração do tempo na barra da linha do tempo para a posição desejada quando o cursor se transformar em .
      - Clique na duração da hora e edite diretamente a hora de início/término na caixa de diálogo exibida.
      - Mova o cursor para o início ou o fim da duração do tempo e arraste para alongar ou encurtar a duração do tempo quando o curso r se transformar em .
   4) Repita as duas etapas acima para desenhar mais durações de tempo nos outros dias da semana.
6. Adicionar a feriado Para aplicar ela Para o modelo.

Nota

Até 4 feriados podem ser adicionados a um modelo.

   1) Clique na guia Feriado.
   2) Selecione um feriado na lista à esquerda e ele será adicionado à lista selecionada no painel direito.
   3) **Opcional:** clique em **Adicionar** para adicionar um novo feriado.

Nota

Para obter detalhes sobre como adicionar um feriado, consulte ***Adicionar feriado*** .

4) **Opcional:** Selecione um feriado selecionado na lista à direita e clique para remover o ⊗ selecionado ou clique em **Limpar** para limpar todos os feriados selecionados na lista correta.

7. Clique em **Salvar** para salvar as configurações e concluir a adição do modelo.

11.6 Definir o Grupo de Acesso para Atribuir Autorização de Acesso a Pessoas

Depois de adicionar a pessoa e configurar as credenciais da pessoa, você pode criar os grupos de acesso para definir qual(is) pessoa(s) pode(m) obter acesso a qual(is) porta(s) e, em seguida, colocaro grupo de acesso no dispositivo de controle de acesso para entrar em vigor.

Antes de começar

- Adicionar pessoa ao cliente.
- Adicione o dispositivo de controle de acesso aos pontos de acesso do cliente e do grupo. Para obter detalhes, consulte ***Gerenciamento de Grupo*** .
- Adicionar modelo.

Passos

Quando as configurações do grupo de acesso são alteradas, você precisa aplicar os grupos de acesso aos dispositivos novamente para entrar em vigor. As alterações do grupo de acesso incluem alterações de modelo, configurações do grupo de acesso, configurações do grupo de acesso da pessoa e detalhes da pessoa relacionada (incluindo número do cartão, impressão digital, imagem facial, ligação entre o número do cartão e a impressão digital, ligação entre o número do cartão e a impressão digital, palavra-passe do cartão, período de eficácia do cartão, etc.).

1. Clique em **Controle de** Acesso → **Autorização →** Grupo de **Acesso** para entrar na interface do **Grupo de** Acesso .

2. Clique em **Adicionar** para abrir a janela Adicionar.

3. No campo **de** texto Nome , crie um nome para o grupo de acesso como desejar.

4. Selecionar a modelo durante o acesso grupo.

Nota

Você deve configurar o modelo antes das configurações do grupo de acesso. Consulte ***Configurar Cronograma e Modelo*** para obter detalhes.

5. Na lista à esquerda do campo Selecionar Pessoa, selecione pessoa(s) para atribuir autoridade de acesso.

6. Na lista à esquerda do campo Selecionar Ponto de Acesso, selecione porta(s), estação(ões) de porta ou andar(es) para as pessoas selecionadas acessarem.

7. Clique em **Salvar**.

Você pode visualizar a(s) pessoa(s) selecionada(s) e o(s) ponto(s) de acesso selecionado (s) no lado direito da interface.

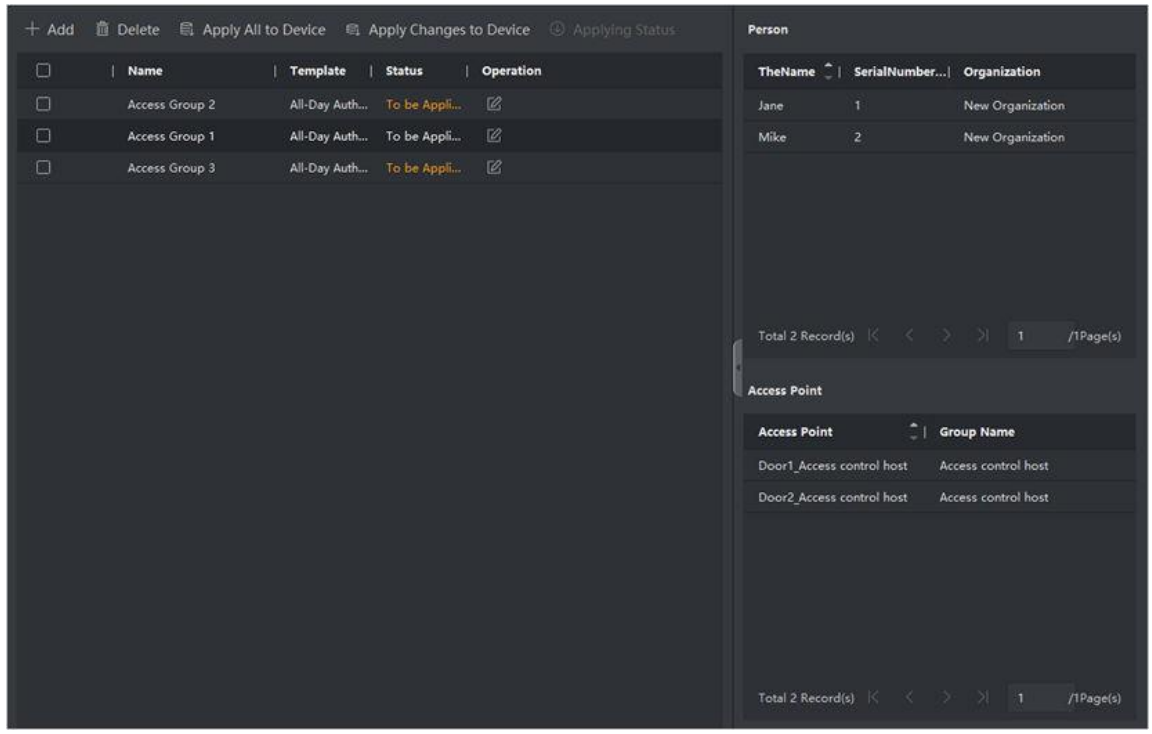


Figura 11-2 Exibir a(s) pessoa(s) selecionada(s) e o(s) ponto(s) de acesso

8. Depois de adicionar os grupos de acesso, você precisa aplicá-los ao dispositivo de controle de acesso para entrar em vigor.

1) Selecione o(s) grupo(s) de acesso a ser aplicado ao dispositivo de controle de acesso.
2) Clique em **Aplicar tudo aos dispositivos** para começar a aplicar todos os grupos de acesso selecionados ao dispositivo de controle de acesso ou à estação da porta.
3) Clique em Aplicar **tudo aos dispositivos** ou **Aplicar alterações aos dispositivos**. **Aplicar tudo aos dispositivos**

Essa operação limpará todos os grupos de acesso existentes dos dispositivos selecionados e, em seguida, aplicará o novo grupo de acesso ao dispositivo.

Aplicar alterações a dispositivos

Esta operação não limpará os grupos de acesso existentes dos dispositivos selecionados e aplicará apenas a parte alterada do(s) grupo(s) de acesso selecionado(s) ao(s) dispositivo(s).

4) Exiba o status da aplicação na coluna Status ou clique em **Aplicando Status** para exibir todos os grupos de acesso aplicados.

Nota

Você pode marcar **Exibir somente falha** para filtrar os resultados da aplicação.

As pessoas selecionadas nos grupos de acesso aplicados terão a autorização para entrar/sair das portas/estações de porta selecionadas com o(s) seu(s) cartão(ões) ligado(s) ou impressões digitais.

9. Opcional: Clique para editar o grupo de acesso, se necessário.

Nota

Se você alterar as informações de acesso das pessoas ou outras informações relacionadas, exibirá o prompt**Grupo de Acesso a Ser Aplicado** no canto direito do cliente.
Você pode clicar no prompt para aplicar os dados alterados ao dispositivo. Você pode selecionar Aplicar **agora** ou **Aplicar mais tarde**.

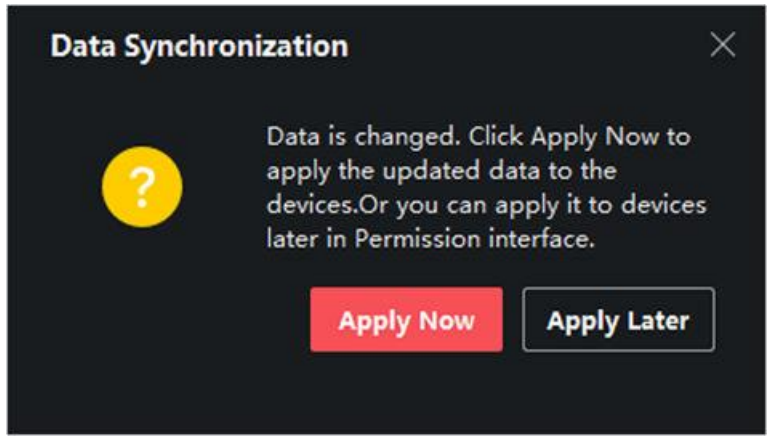


Figura 11-3 Sincronização de dados

11.7 Configurar funções avançadas

Você pode configurar as funções avançadas de controle de acesso para atender a alguns requisitos especiais em diferentes cenas.

Nota

- Para as funções relacionadas ao cartão (o tipo de cartão de controle de acesso), somente o(s) cartão(ões) com o grupo de acesso aplicado serão listados ao adicionar cartões.
- As funções avançadas devem ser suportadas pelo dispositivo.
- Passe o cursor sobre a função avançada e, em seguida, clique para personalizar a(s) função(ões) avançada(s) a serem exibidas.

11.7.1 Configurar parâmetros do dispositivo

Depois de adicionar o dispositivo de controle de acesso, você pode configurar os parâmetros do dispositivo de controle de acesso , pontos de controle de acesso.

Configurar parâmetros para o dispositivo de controle de acesso

Depois de adicionar o dispositivo de controle de acesso, você pode configurar seus parâmetros, incluindo a sobreposição de informações do usuário na imagem, o upload de imagens após a captura, o salvamento de imagens capturadas, etc.

Passos

1. Clique **Acesso Controle → Avançado Função → Dispositivo Parâmetro** .

Nota

Se você puder encontrar Parâmetro de dispositivo na lista Função avançada, passe o cursor sobre a função avançada e, em seguida, clique para selecionar o parâmetro de dispositivo a ser exibido.

2. Selecione um dispositivo de acesso para mostrar seus parâmetros na página correta.
3. Virar o interruptor Para EM Para habilitar o correspondente Funções.

Nota

- Os parâmetros exibidos podem variar para diferentes dispositivos de controle de acesso.
- Alguns dos parâmetros a seguir não estão listados na página Informações Básicas, clique em **Mais** para editar os parâmetros.

Prompt de voz

Se você ativar essa função, o prompt de voz será ativado no dispositivo. Você pode ouvir o prompt de voz ao operar no dispositivo.

Carregar Foto. Após a captura vinculada

Carregue as imagens capturadas pela câmera vinculada ao sistema automaticamente.

Salvar foto. Após a captura vinculada

Se você ativar essa função, poderá salvar a imagem capturada pela câmera vinculada no dispositivo.

Modo de

Reconhecimento

Facial Modo Normal

Reconheça o rosto através da câmera normalmente.

Modo Profundo

O dispositivo pode reconhecer um alcance de pessoas muito maior do que o modo normal. Esse modo é aplicável a um ambiente mais complicado.

Ativar cartão NFC

Se ativar a função, o dispositivo pode reconhecer o cartão NFC. Você pode apresentar o cartão NFC no dispositivo.

Ativar cartão M1

Se ativar a função, o dispositivo pode reconhecer o cartão M1. Você pode apresentar o cartão M1 no dispositivo.

Ativar cartão EM

Se ativar a função, o dispositivo pode reconhecer o cartão EM. Você pode apresentar o cartão EM no dispositivo.

Nota

Se o leitor de cartão periférico suportar a apresentação do cartão EM, a função também é suportada para ativar/desativar a função do cartão EM.

4. Clique em **OK.**
5. **Opcional:** Clique em **Copiar** para e selecione o(s) dispositivo(s) de controle de acesso para copiar os parâmetros na página para o(s) dispositivo(s) especificado(s).

Configurar parâmetros para porta/elevador

Depois de adicionar o dispositivo de controle de acesso, você pode configurar seus parâmetros de ponto de acesso (porta ou piso).

Antes de começar

Adicione o dispositivo de controle de acesso ao cliente.

Passos

1. Clique em **Controle de Acesso → Função Avançada → Parâmetro de Dispositivo** .
2. Selecione um dispositivo de controle de acesso no painel esquerdo e clique para mostrar as portas ou pisos do dispositivo selecionado.
3. Selecione uma porta ou piso para mostrar seus parâmetros na página direita.
4. Editar o porta ou chão Parâmetros.

Nota

- Os parâmetros exibidos podem variar para diferentes dispositivos de controle de acesso.
- Alguns dos parâmetros a seguir não estão listados na página Informações Básicas, clique em **Mais** para editar os parâmetros.

Nome

Edite o nome do leitor de cartão conforme desejado.

Contato da Porta

Você pode definir o sensor da porta como permanecendo fechado ou permanecendo aberto. Normalmente, ele permanece fechado.

Tipo de botão Sair

Você pode definir o botão de saída como permanecendo fechado ou permanecendo aberto. Normalmente, ele está permanecendo aberto.

Tempo de Travamento da Porta

Depois de passar o cartão normal e a ação do relé, o temporizador para travar a porta começa a funcionar.

Duração de abertura estendida

O contato da porta pode ser ativado com a devida demora depois que a pessoa com acessos estendidos precisar passar o cartão.

Porta Deixada Aberta Alarme de Tempo Limite

O alarme pode ser acionado se a porta não tiver sido fechada em um período de tempo configurado. Se ele estiver definido como 0, nenhum alarme será acionado.

Porta de bloqueio quando a porta fechada

A porta pode ser trancada uma vez que está fechada, mesmo que o **tempo de bloqueio** da **porta** não seja atingido.

Código Duress

A porta pode se abrir inserindo o código de coação quando há coação. Ao mesmo tempo, o cliente pode relatar o evento de coação.

Super Senha

A pessoa específica pode abrir a porta inserindo a super senha.

Dispensar código

Crie um código de descarte que possa ser usado para parar a campainha do leitor de cartão (inserindo o código de descarte no teclado).

Nota

- O código de coação, o supercódigo e o código de descartação devem ser diferentes.
- O código de coação, a super senha e o código de descartação devem ser diferentes da senha de autenticação.
- O comprimento do código de coação, super senha e o código de descartar é de acordo com o dispositivo, geralmente ele deve conter de 4 a 8 dígitos.

5. Clique em **OK.**
6. **Opcional:** Clique em **Copiar** para , e selecione a(s) porta(s) de andar(es) para copiar os parâmetros na página **para** a(s) porta(s /andar(es) selecionado(s).

Nota

As configurações de duração de status da porta ou do piso também serão copiadas para a(s) porta(s) selecionada(s).

Configurar parâmetros para o leitor de cartão

Depois de adicionar o dispositivo de controle de acesso, você pode configurar seus parâmetros de leitor de cartão.

Antes de começar

Adicione o dispositivo de controle de acesso ao cliente.

Passos

1. Clique em **Controle de Acesso → Função Avançada → Parâmetro de Dispositivo** .
2. Na lista de dispositivos à esquerda, clique para expandir a porta, selecione um leitor de cartão e você pode editar os parâmetros do leitor de cartão à direita.
3. Edite os parâmetros básicos do leitor de cartão na página Informações básicas.

Nota

- Os parâmetros exibidos podem variar para diferentes dispositivos de controle de acesso. Há parte dos parâmetros listados a seguir. Consulte o manual do usuário do dispositivo para obter mais detalhes.
- Alguns dos parâmetros a seguir não estão listados na página Informações Básicas, clique em **Mais** para editar os parâmetros.

Nome

Edite o nome do leitor de cartão conforme desejado.

OK LED Polaridade / Erro LED Polaridade / Polaridade da campainha

Defina OK LED Polaridade / Erro LED Polaridade / Buzzer LED Polaridade da placa principal de acordo com os parâmetros do leitor de cartão. Geralmente, adota as configurações padrão.

Intervalo mínimo de deslizamento do cartão

Se o intervalo entre o passar do cartão do mesmo cartão for menor que o valor definido, o passar o dedo do cartão será inválido. Você pode defini-lo como 0 para 255.

Intervalo máximo ao inserir PWD

Quando você insere a senha no leitor de cartão, se o intervalo entre pressionar dois dígitos for maior do que o valor definido, os dígitos pressionados antes serão limpos automaticamente.

Alarme de Max. Tentativas fracassadas

Habilite para relatar alarme quando as tentativas de reading do cartão atingirem o valor definido.

Tempos máximos de falha do cartão

Defina o máximo. tentativas de falha do cartão de leitura.

Detecção de adulteração

Habilite a detecção anti-adulteração para o leitor de cartão.

Comunique-se com o controlador a cada

Quando o dispositivo de controle de acesso não pode se conectar com o leitor de cartão por mais tempo do que o tempo definido, o leitor de cartão irá ligar a linha automaticamente.

Tempo de zumbido

Defina o tempo de zumbido do leitor de cartão. O tempo disponível varia de 0 a 5.999s. 0 representa zumbido contínuo.

Tipo de Leitor de Cartão/Descrição do Leitor de Cartão

Obtenha o tipo e a descrição do leitor de cartão. Eles são somente leitura.

Nível de reconhecimento de impressão digital

Selecione o nível de reconhecimento de impressão digital na lista suspensa.

Leitor de cartão padrão Authenticatino modo

Exiba o modo de autenticação padrão do leitor de cartão.

Capacidade de impressão digital

Veja o número máximo de impressões digitais disponíveis.

Número de impressão digital existente

Exiba o número de impressões digitais existentes no dispositivo.

Pontuação

O dispositivo marcará a imagem capturada de acordo com o ângulo de guinada, ângulo de inclinação e distância pupilar. Se a pontuação for menor que o valor configurado, o reconhecimento facial falhará.

Valor de Tempo Limite de Reconhecimento Facial

Se o tempo de reconhecimento for maior do que o tempo configurado, o dispositivo o lembrará .

Intervalo de Reconhecimento Facial

O intervalo de tempo entre dois reconhecimentos faciais contínuos durante a autenticação. Por padrão, é 2s.

Limite de correspondência de face 1:1

Defina o limite de correspondência ao autenticar por meio do modo de correspondência 1 :1. Quanto maior o valor, menor a taxa de aceitação falsa e maior a taxa de rejeição falsa durante a autenticação.

1:N Nível de segurança

Defina o nível de segurança correspondente ao autenticar por meio do modo de correspondência 1:N. Quanto maior o valor, menor a taxa de aceitação falsa e maior a taxa de rejeição falsa durante a autenticação.

Detecção de rosto ao vivo

Ative ou desative a função de detecção de rosto ao vivo. Se ativar a função, o dispositivo pode reconhecer se a pessoa é uma pessoa vivaou não.

Nível de segurança de detecção de rosto ao vivo

Depois de ativar a função Live Face Detection, você pode definir o nível de segurança correspondente ao executar a autenticação de rosto ao vivo.

Tentativas fracassadas de autenticação facial.

Defina o máximo de tentativas com falha de detecção de rosto ao vivo. O sistema bloqueará o rosto do usuário por 5 minutos se a detecção de rosto ao vivo falhar por mais do que as tentativas configuradas. O mesmo usuário não pode autenticar através do rosto falso dentro de 5 minutos. Dentro dos 5 minutos, o usuário pode authenticate através do rosto real duas vezes continuamente para desbloquear.

Falha na Autenticação de Bloqueio de Face

Depois de ativar a função Live Face Detection, o sistema bloqueará o rosto do usuário por 5 minutos se a detecção de rosto ao vivo falhar por mais do que as tentativas configuradas. O mesmo usuário não pode autenticar através do rosto falso dentro de 5 minutos. Dentro dos 5 minutos, o usuário pode autenticar através do rosto real duas vezes continuamente para desbloquear.

Modo de Aplicação

Você pode selecionar modos de aplicação internos ou outros que se conectam ao ambiente

real.

4. Clique em **OK.**

5. **Opcional:** Clique em **Copiar** para e selecione o(s) leitor(es) de cartão para copiar os parâmetros na página para o(s) leitor(es) de cartão selecionado(s).

Configurar parâmetros para saída de alarme

Depois de adicionar o dispositivo de controle de acesso, se o dispositivo se vincular a saídas de alarme, você poderá configurar os parâmetros.

Antes de começar
Adicione o dispositivo de controle de acesso ao cliente e verifique se o dispositivo suporta saída de alarme.

Passos
1. Clique em Controle de **Acesso** → **Função Avançada → Parâmetro de Dispositivo** para entrar na página de configuração do parâmetro de controle de acesso.
2. Na lista de dispositivos à esquerda, clique para expandir a porta, selecione uma entrada de alarme e você pode editar os parâmetros da entrada de alarme à direita.
3. Defina os parâmetros de saída do alarme.

   Nome

   Edite o nome do leitor de cartão conforme desejado.

   Tempo ativo de saída de alarme

   Quanto tempo a saída do alarme durará após o disparo.
4. Clique em **OK.**
5. **Opcional:** Defina o interruptor no canto superior direito como **ON** para acionar a saída do alarme.

11.7.2 Configurar parâmetros do dispositivo

Depois de adicionar o dispositivo de controle de acesso, você pode definir seus parâmetros, como parâmetros de rede.

Definir parâmetros para o Terminal de Reconhecimento Facial

Para o terminal de reconhecimento facial, você pode definir seus parâmetros, incluindo banco de dados de imagens faciais, autenticação de código QR, etc.

Passos

Nota

Esta função deve ser suportada pelo dispositivo.

1. Entre no módulo Controle de Acesso.
2. Na barra de navegação à esquerda, insira **Função Avançada → Mais Parâmetros** .
3. Selecione um dispositivo de controle de acesso na lista de dispositivos e clique em Terminal **de Reconhecimento Facial**.
4. Defina os parâmetros.

Nota

Esses parâmetros exibidos variam de acordo com os diferentes modelos de dispositivos.

.COM

Selecione uma porta COM para configuração. COM1 refere-se à interface RS-485 e COM2 refere-se à interface RS-232.

Banco de dados de imagens faciais

selecione Deep Learning como o banco de dados de imagens faciais.

Autenticar por QR Code

Se ativada, a câmera do dispositivo pode digitalizar o código QR para autenticação. Por padrão, a função está desabilitada.

Autenticação de lista de bloqueios

Se ativado, o dispositivo comparará a pessoa que deseja acessar com as pessoas na lista de bloqueio.

Se correspondido (a pessoa está na lista de bloqueios), o acesso será negado e o dispositivo enviará um alarme para o cliente.

Se incompatível (a pessoa não está na lista de bloqueio), o acesso será concedido.

Salvar imagem de rosto de autenticação

Se habilitada, a imagem de rosto capturada ao autenticar será salva no dispositivo.

Versão do MCU

Veja a versão do MCU do dispositivo.

5. Clique em **Salvar**.

Definir parâmetros RS-485

Você pode definir os parâmetros RS-485 do dispositivo de controle de acesso, incluindo a taxa de transmissão, o bit de dados, o bit de parada, o tipo de paridade, o tipo de controle de fluxo, o modo de comunicação, o modo de trabalho e o modo de conexão.

Passos

Nota

As configurações RS-485 devem ser suportadas pelo dispositivo.

1. Entre no módulo Controle de Acesso.

2. Na barra de navegação à esquerda, insira **Função Avançada → Mais Parâmetros** .

3. Selecione um dispositivo de controle de acesso na lista de dispositivos e clique em RS-485 para entrar na página Configurações RS-485.

4. Selecione o número da porta de série na lista suspensa para definir os parâmetros RS-485.

5. Defina o número de série, o dispositivo externo, o centro de autenticação, a taxa de transmissão, o bit de dados, o bit de parada, o tipo de paridade, o tipo de controle de fluxo , o modo de comunicação e o modo de trabalho na lista suspensa.

6. Clique em **Salvar**.
- Os parâmetros configurados serão aplicados ao dispositivo automaticamente.
- Quando você altera o modo de trabalho ou o modo de conexão, o dispositivo será reinicializado automaticamente.

Definir parâmetros Wiegand

Você pode definir o canal Wiegand do dispositivo de controle de acesso e o modo de comunicação.

Passos

Nota

Esta função deve ser suportada pelo dispositivo.

1. Entre no módulo Controle de Acesso.
2. Na barra de navegação à esquerda, insira **Função Avançada → Mais Parâmetros** .
3. Selecione um dispositivo de controle de acesso na lista de dispositivos e clique em Wiegand para entrar na página Configurações do Wiegand.
4. Defina o interruptor como ativado para ativar a função Wiegand para o dispositivo.
5. Selecionar o Wiegand canal Não. e o comunicação modo De o lista suspensa lista.

Nota

Se você definir **a Direção** de **Comunicação** como **Envio**, será necessário definir o **Modo Wiegand** como
Wiegand 26 ou **Wiegand 34**.

6. **Marque Ativar** Wiegand para ativar a função Wiegand.
7. Clique em **Salvar**.
- Os parâmetros configurados serão aplicados ao dispositivo automaticamente.
- Depois de alterar a direção da comunicação, o dispositivo será reinicializado automaticamente.

Ativar criptografia de cartão M1

A criptografia de cartão M1 pode melhorar o nível de segurança da autenticação.

Passos

Nota

A função deve ser suportada pelo dispositivo de controle de acesso e pelo leitor de cartão.

1. Entre no módulo Controle de Acesso.
2. Na barra de navegação à esquerda, insira **Função Avançada → Mais Parâmetros** .
3. Selecione um dispositivo de controle de acesso na lista de dispositivos e clique em Verificação de Criptografia de Cartão M1 para entrar na página Verificação de Criptografia **de Cartão M1**.
4. Defina a opção como ativada para ativar a função de criptografia do cartão M1.

5. Pôr o setor ID.

Nota

- O ID do setor varia de 1 a 100.
- Por padrão, o Setor 13 é criptografado. Recomenda-se criptografar o setor 13.

6. Clique em **Salvar** para salvar as configurações.

11.8 Controle de Portas

No módulo Monitoramento, você pode visualizar o status em tempo real das portas gerenciadas pelo dispositivo de controle de acesso adicionado. Você também pode controlar as portas, como abrir / fechar a porta, ou permanecer a porta aberta / fechada através do cliente remotamente. O evento de acesso em tempo real é exibido neste módulo. Você pode visualizar os detalhes de acesso e os detalhes da pessoa.

Nota

Para o usuário com permissão de controle de porta, o usuário pode entrar no módulo de Monitoramento e controlar a porta. Ou os ícones usados para controle não serão exibidos. Para definir a permissão do usuário, consulte ***Gerenciamento de Pessoas*** .

11.8.1 Status da porta de controle

Você pode controlar o status da(s) porta(s), incluindo porta destrancada, porta trancada, restante da porta destrancada, permanecendo a porta trancada, permanecer toda destrancada, etc.

Antes de começar

- Adicione pessoa e atribua autorização de acesso à pessoa projetada, e a pessoa terá a autorização de acesso aos pontos de acesso (portas). Para obter detalhes, consulte ***Gerenciamento*** de Pessoas e ***Definir Grupo de Acesso para Atribuir Autorização de Acesso a Pessoas*** .
- Certifique-se de que o usuário da operação tenha a permissão dos pontos de acesso (portas). Para obter detalhes, consulte .

Passos

1. Clique em **Monitoramento** para entrar na página de monitoramento de status.

2. Selecionar ano acesso ponto grupo em o canto superior direito canto.

Nota

Para gerenciar o grupo de pontos de acesso, consulte ***Gerenciamento*** de ***Grupo*** .

As portas no grupo de controle de acesso selecionado serão exibidas.

3. Clique em um ícone de porta para selecionar uma porta ou pressione **Ctrl** e selecione várias portas.

Nota

Para Permanecer Tudo **Desbloqueado** e **Permanecer Tudo Bloqueado**, ignore esta etapa.

4. Clique nos botões a seguir para controlar a porta.

Destravar

Quando a porta estiver trancada, destrave-a e ela estará aberta por uma vez. Após a duração aberta, a porta será fechada e trancada novamente automaticamente.

Fechadura

Quando a porta estiver destrancada, tranque-a e ela será fechada. A pessoa que tem a autorização de acesso pode acessar a porta com credenciais.

Permanecer desbloqueado

A porta será destrancada (não importa fechada ou aberta). Todas as pessoas podem acessar a porta sem a necessidade de credenciais.

Permanecer bloqueado

A porta será fechada e trancada. Nenhuma pessoa pode acessar a porta , mesmo que tenha as credenciais autorizadas, exceto os superusuários.

Permanecer tudo desbloqueado

Todas as portas do grupo serão destrancadas (não importa fechadas ou abertas). Todas as pessoas podem acessar as portas sem a necessidade de credenciais.

Permanecer tudo bloqueado

Todas as portas do grupo serão fechadas e trancadas. Nenhuma pessoa pode acessar as portas, mesmo que tenha as credenciais autorizadas, exceto os superusuários.

Capturar

Capture uma imagem manualmente.

Nota

O botão **Capturar** está disponível quando o dispositivo suporta a função de captura. A imagem é salva no PC que executa o cliente. Para definir o caminho de salvamento , consulte *Definir* caminho de *salvamento* de *arquivo* no manual do usuário do software cliente.

Resultado

O ícone das portas mudará em tempo real de acordo com a operação , se a operação for bem-sucedida.

11.8.2 Verificar registros de acesso em tempo real

Os registros de acesso serão exibidos em tempo real, incluindo registros de passagem de cartão, registros de reconhecimento facial, registros de comparação de impressões digitais, etc. Você pode visualizar as informações da pessoa e visualizar a imagem capturada durante o acesso.

Passos

1. Clique **em Seg** e selecione um grupo na lista suspensa no canto superior direito.

   Os registros de acesso acionados nas portas do grupo selecionado serão exibidos em tempo real. Você pode visualizar os detalhes dos registros, incluindo o número do cartão, nome da pessoa, organização, hora do evento, etc.
2. **Opcional:** Verifique o tipo de evento e o status do evento para que esses eventos sejam exibidos na lista se os eventos forem detectados. Os eventos de tipo ou status não marcados não serão exibidos na lista.
3. **Opcional:** Marque **Mostrar Evento Mais Recente** e o registro de acesso mais recente será selecionado e exibido na parte superior da lista de registros.
4. **Opcional:** Clique no evento para disputaros detalhes da pessoa acessada, incluindo fotos da pessoa (foto e perfil capturados), número da pessoa, nome da pessoa, organização, telefone, endereço de contato , etc.

   Nota

   Você pode clicar duas vezes na imagem capturada para ampliá-la e exibir os detalhes.
5. **Opcional: Clique com** o botão direito do mouse no nome da coluna da tabela de eventos de acesso para mostrar ou ocultar a coluna de acordo com as necessidades reais.

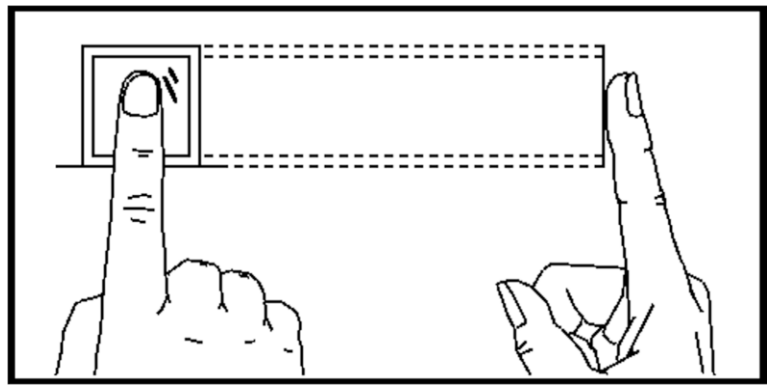
Apêndice A. Dicas para digitalizar impressão digital

Dedo recomendado

Dedo indicador, dedo médio ou terceiro dedo.

Varredura correta

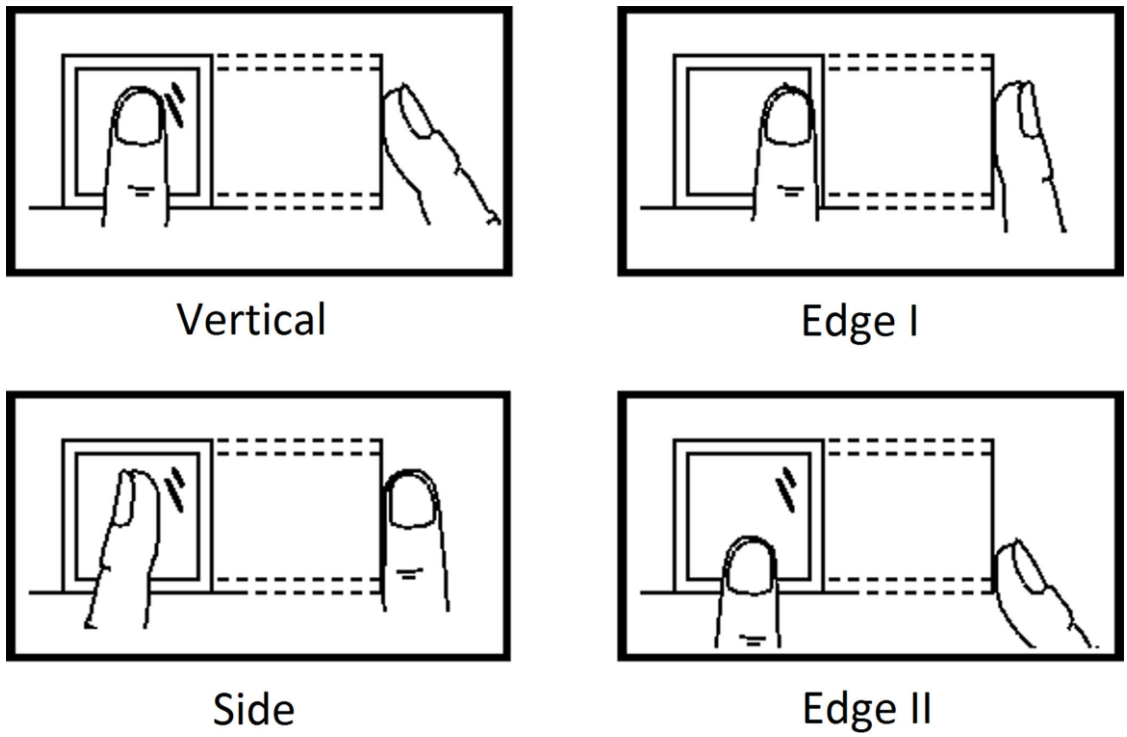
A figura exibida abaixo é a maneira correta de digitalizar seu dedo:



Você deve pressionar o dedo no scanner horizontalmente. O centro do dedo digitalizado deve estar alinhado com o centro do scanner.

Varredura incorreta

As figuras de digitalização de impressões digitais exibidas abaixo estão incorretas:



Ambiente

O scanner deve evitar luz solar direta, alta temperatura, condições úmidas e chuva. Quando está seco, o scanner pode não reconhecer sua impressão digital com êxito. Você pode soprar o dedo e digitalizar novamente.

Outros

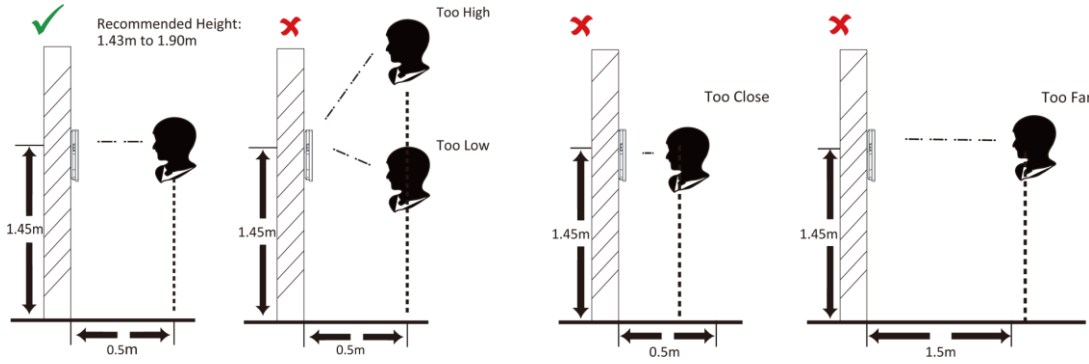
Se a sua impressão digital for superficial ou se for necessário digitalizá-la, recomendamos que utilize outros métodos de autenticação.

Se você tiver lesões no dedo digitalizado, o scanner pode não reconhecer. Você pode mudar outro dedo e tentar novamente.

Apêndice B. Dicas ao coletar/comparar a imagem do rosto

A posição ao coletar ou comparar a imagem do rosto é a seguinte:

Posições (Distância recomendada : 0,5 m)



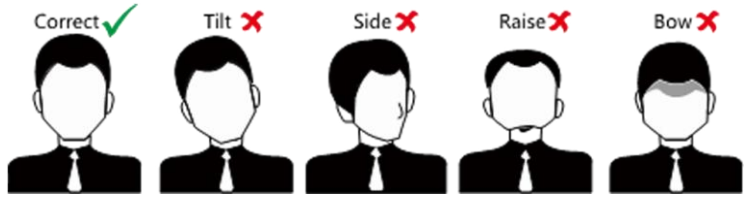
Expressão

- Mantenha sua expressão naturalmente ao coletar ou comparar fotos de rosto, assim como a expressão na imagem abaixo.

- Não use chapéu, óculos de sol ou outros acessórios que possam afetar a função de reconhecimento facial.
- Não faça o cabelo cobrir os olhos, ouvidos, etc. e maquiagem pesada não é permitida.

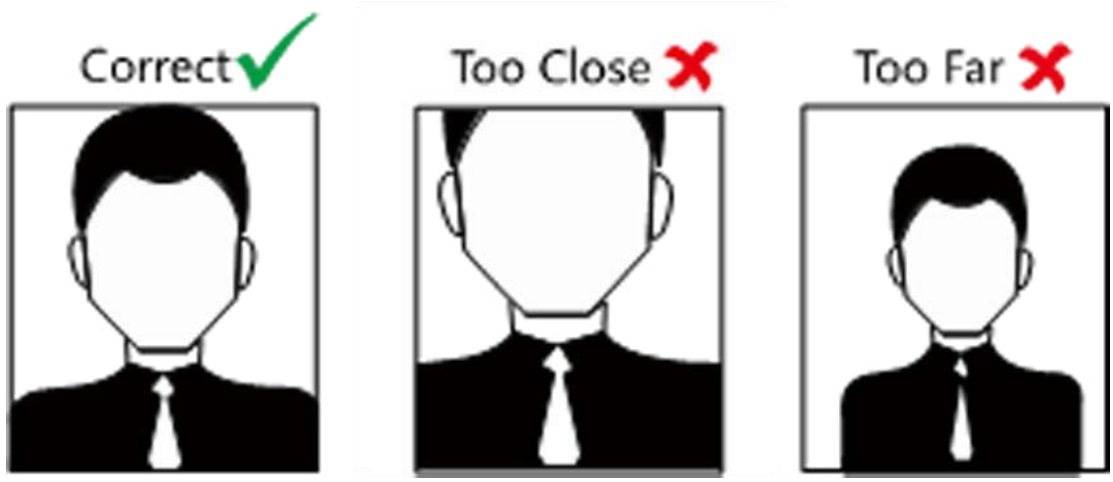
Postura

Para obter uma imagem de rosto de boa qualidade e precisa , posicione seu rosto olhando para a câmera ao coletar ou comparar fotos de rosto.



Tamanho

Certifique-se de que seu rosto esteja no meio da janela de coleta.



Apêndice C. Dicas para o ambiente de instalação

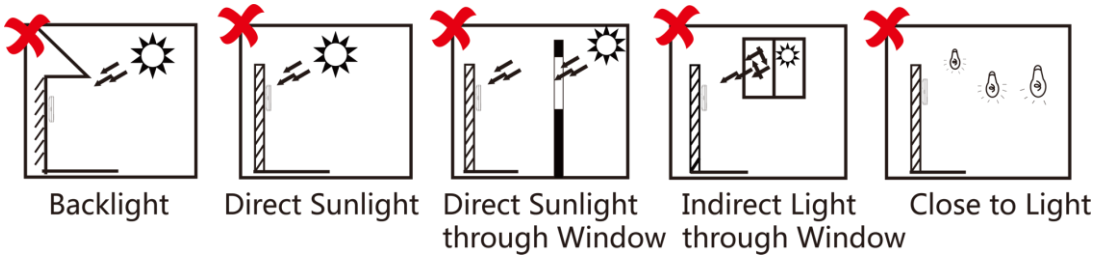
1. Valor de referência de iluminação da fonte de luz

Vela: 10Lux

Lâmpada: 100~850Lux

Luz solar: Mais de 1200Lux

2. Evite luz de fundo, luz solar direta e indireta



Apêndice D. Dimensão

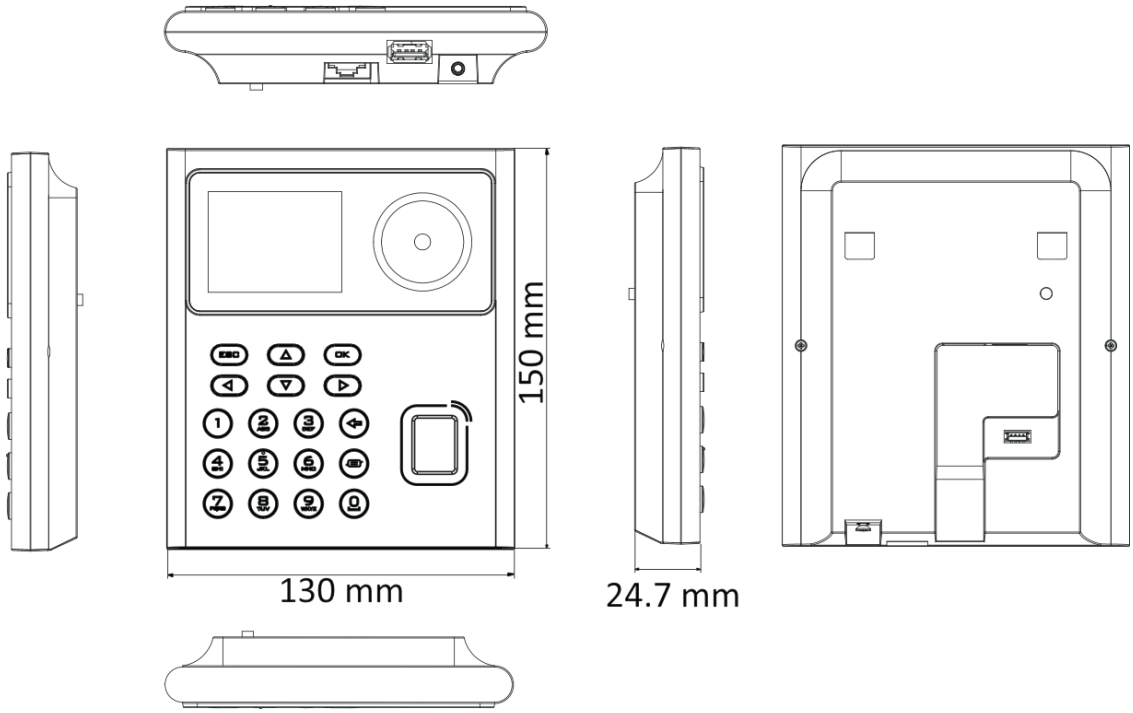


Figura D-1 Dimensão

Apêndice E. Matriz de Comunicação e Comando de Dispositivo

Matriz de Comunicação

Digitalize o seguinte código QR para obter a matriz de comunicação do dispositivo.
Observe que a matriz contém todas as portas de comunicação do controle de acesso Hikvision e dispositivos de vídeo porteiro.

Figura E-1 Código QR da Matriz de Comunicação

Comando do dispositivo

Digitalize o seguinte código QR para obter os comandos de porta serial comuns do dispositivo.
Observe que a lista de comandos contém todos os comandos de portas seriais comumente usados para todos os dispositivos de controle de acesso e vídeo porteiro Hikvision.

Figura E-2 Comando do dispositivo


See Far, Go Further