

The logo consists of a red horizontal bar with a white diagonal stripe on the left side. The word "HIKVISION" is written in white, italicized, uppercase letters on the red background.

HIKVISION

**Terminal de Reconhecimento Facial Série
DS-K1T673**

Manual do Usuário

Informação Legal

©2021 Hangzhou Hikvision Digital Technology Co., Ltd. Todos os direitos reservados.

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, INTERRUPTÃO 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

DS-K1T673 Série Rosto Reconhecimento Terminal

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, você é 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



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

DS-K1T673 Série Rosto Reconhecimento Terminal

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

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 é dividida 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:

- Toda a operação eletrônica deve estar estritamente em conformidade com os regulamentos de segurança elétrica, regulamentos de prevenção de incêndios e outros regulamentos relacionados em sua região local.
- Use o adaptador de energia, que é fornecido pela empresa normal. Este equipamento destina-se a ser fornecido a partir da fonte de alimentação protegida contra surtos de classe 2 classificada DC 12V, 3A.
- Não conecte vários dispositivos a um adaptador de energia, pois a sobrecarga do adaptador pode causar superaquecimento ou risco de incêndio.
- Certifique-se de que a alimentação foi desligada antes de ligar, instalar ou desmontar o dispositivo.
- Quando o produto estiver instalado na parede ou no tecto, o dispositivo deve ser firmemente fixado.
- 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.
- Não ingira bateria, Chemical Burn Hazard.
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.
Mantenha as pilhas novas e usadas longe das crianças. Se o compartimento da bateria não for fixado de forma segura, pare de utilizar o produto e mantenha-o afastado das crianças. Se você acha que as baterias podem ter sido engolidas ou colocadas dentro de qualquer parte do corpo, procure atendimento médico imediato.
- Se o produto não funcionar corretamente, entre em contato com seu revendedor ou com o centro de serviços mais próximo. Nunca tente desmontar o dispositivo você mesmo. (Não assumiremos qualquer responsabilidade por problemas causados por reparo ou manutenção não autorizados.)

DS-K1T673 Série Rosto Reconhecimento Terminal

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.
- 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).
- Não aponte o dispositivo para o sol ou lugares mais brilhantes. Uma floração ou esfregaço pode ocorrer de outra forma (o que não é um mau funcionamento, no entanto), e afetando a resistência do sensor ao mesmo tempo.
- Por favor, use a luva fornecida ao abrir a tampa do dispositivo, evite o contato direto com a tampa do dispositivo, porque o suor ácido dos dedos pode corroer o revestimento superficial da tampa do dispositivo.
- Por favor, use um pano macio e seco quando limpar dentro e fora das superfícies da tampa do dispositivo, não use detergentes alcalinos.
- Por favor, mantenha todos os invólucros depois de desembalá-los para uso futuro. Em caso de ocorrência de qualquer falha, você precisa devolver o dispositivo à fábrica com o invólucro original. O transporte sem o invólucro original pode resultar em danos no dispositivo e levar a custos adicionais.
- O uso inadequado ou a substituição da bateria podem resultar em risco de explosão. Substitua apenas pelo mesmo tipo ou equivalente. Descarte as baterias usadas de acordo com as instruções fornecidas pelo fabricante da bateria.
- Os produtos de reconhecimento biométrico não são completamente aplicáveis a ambientes anti-falsificação. Se você precisar de um nível de segurança mais alto, use vários modos de autenticação.
- Temperatura de trabalho: -30 °C a +60 °C
- Uso interno e externo. Se instalar o dispositivo dentro de casa, o dispositivo deve estar a pelo menos 2 metros de distância da luz e a pelo menos 3 metros de distância da janela ou da porta. Se instalar o dispositivo ao ar livre, você deve aplicar o selante Sililcone entre a área de fiação do cabo para evitar que a gota de chuva entre.
- Nível de proteção: IP65

Modelos Disponíveis

Nome do Produto	Modelo	Sem fio
Terminal de Reconhecimento Facial	DS-K1T673DX	Placa de 13,56 MHz Apresentando Frequência
	DS-K1T673DWX	Placa de 13,56 MHz Apresentando Frequência, Wi-Fi
	DS-K1T673TDX	Placa de 13,56 MHz Apresentando Frequência
	DS-K1T673TDWX	Placa de 13,56 MHz Apresentando Frequência, Wi-Fi
	DS-K1T673TDGX	Placa de 13,56 MHz Apresentando Frequência, 4G

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

Modelo	Fabricante	Padrão
C2000IC12.0-24P-DE	MOSO Fonte de Alimentação Technology Co., Ltd.	CEE (CEE)
C2000IC12.0-24P-GB	MOSO Fonte de Alimentação Technology Co., Ltd.	BS
KPL-040F-VI	Canal Bem Tecnologia Co Ltd.	CEE (CEE)

Conteúdo

Sumário

Capítulo 1 Visão geral	1
1.1 Visão geral	1
1.2 Características	1
1.2.1 Características (Série Normal)	1
1.2.2 Características (Série T)	3
Capítulo 2 Aparência	5
Capítulo 3 Instalação	7
3.1 Ambiente de Instalação	7
3.2 Montagem embutida com caixa de gangue	7
3.3 Montagem em superfície	11
3.4 Montagem com suporte	15
3.4.1 Preparação antes da montagem com suporte	15
3.4.2 Suporte de montagem	17
Capítulo 4 Fiação	20
4.1 Descrição Terminal	20
4.2 Dispositivo Normal de Fio	23
4.3 Unidade de Controle de Porta Segura de Arame	24
4.4 Módulo de incêndio de fio	25
4.4.1 Diagrama de fiação da porta aberta ao desligar	25
4.4.2 Diagrama de fiação da porta trancada ao desligar	27
Capítulo 5 Ativação	30
5.1 Ativar via Dispositivo	30
5.2 Ativar via navegador da Web	32
5.3 Ativar via SADP	33
5.4 Ativar dispositivo via software cliente iVMS-4200	34

DS-K1T673 Série Rosto Reconhecimento Terminal

Capítulo 6 Operação Rápida	36
6.1 Selecione o idioma	36
6.2 Definir o Modo de Aplicativo.....	38
6.3 Configurações de privacidade	39
6.4 Definir administrador	40
Capítulo 7 Operação de base	43
7.1 Login 43	
7.1.1 Login por Administrador	43
7.1.2 Login por Senha de Ativação	45
7.2 Configurações de comunicação	47
7.2.1 Definir parâmetros de rede com fio.....	47
7.2.2 Definir parâmetros de Wi-Fi.....	49
7.2.3 Definir parâmetros RS-485	51
7.2.4 Definir parâmetros Wiegand.....	52
7.2.5 Configurar parâmetros ISUP	52
7.2.6 Acesso à plataforma	54
7.3 Gerenciamento de usuários	54
7.3.1 Adicionar administrador	55
7.3.2 Adicionar imagem de rosto.....	56
7.3.3 Adicionar impressão digital.....	58
7.3.4 Adicionar cartão	59
7.3.5 Ver código PIN	60
7.3.6 Definir modo de autenticação.....	61
7.3.7 Pesquisar e editar usuário.....	61
7.4 Gerenciamento de dados.....	62
7.4.1 Excluir dados	62
7.4.2 Importar dados.....	62
7.4.3 Exportar dados	63

DS-K1T673 Série Rosto Reconhecimento Terminal

7.5 Autenticação de identidade	63
7.5.1 Autenticar via credencial única	63
7.5.2 Autenticar por meio de várias credenciais	65
7.6 Configurações básicas	66
7.7 Definir parâmetros biométricos	69
7.8 Definir parâmetros de controle de acesso	71
7.9 Configurações de status de horário e presença	72
7.9.1 Desativar o Modo de Presença através do Dispositivo	72
7.9.2 Definir Atendimento Manual via Dispositivo	73
7.9.3 Definir Atendimento Automático via Dispositivo	74
7.9.4 Definir Atendimento Manual e Automático via Dispositivo	76
7.10 Manutenção do Sistema	77
7.11 Vídeo Intercomunicador	79
7.11.1 Chamar software cliente do dispositivo	79
7.11.2 Call Center a partir do dispositivo	81
7.11.3 Dispositivo de chamada a partir do software cliente	81
7.11.4 Sala de chamadas a partir do dispositivo	82
7.11.5 Chamar cliente móvel do dispositivo	82
Capítulo 8 Operação via navegador da Web	83
8.1 Login	83
8.2 Visualização ao vivo	83
8.3 Gestão de Pessoas	85
8.4 Evento de Pesquisa	85
8.5 Configuração	86
8.5.1 Definir parâmetros locais	86
8.5.2 Exibir informações do dispositivo	87
8.5.3 Definir Hora	87
8.5.4 Definir horário de verão	88

DS-K1T673 Série Rosto Reconhecimento Terminal

8.5.5 Exibir licença de software de código aberto.....	88
8.5.6 Atualização e manutenção.....	88
8.5.7 Consulta de log.....	90
8.5.8 Configurações do Modo de Segurança	90
8.5.9 Gerenciamento de Certificados.....	91
8.5.10 Alterar a senha do administrador.....	92
8.5.11 Exibir informações de armar/desarmar o dispositivo	92
8.5.12 Configurações de rede	92
8.5.13 Definir parâmetros de vídeo e áudio	96
8.5.14 Personalizar conteúdo de áudio.....	97
8.5.15 Definir parâmetros de imagem	99
8.5.16 Definir Suplemento de Brilho da Luz	100
8.5.17 Definir parâmetros de beleza	100
8.5.18 Configurações de Horário e Presença.....	100
8.5.19 Configurações gerais.....	103
8.5.21 Configurações de controle de acesso	110
8.5.22 Definir parâmetros biométricos.....	114
8.5.23 Definir publicação do aviso	117
Capítulo 9 Configuração do Software Cliente	119
9.1 Fluxo de configuração do software cliente.....	119
9.2 Gerenciamento de dispositivos.....	119
9.2.1 Adicionar dispositivo.....	120
9.2.2 Redefinir senha do dispositivo	123
9.2.3 Gerenciar dispositivos adicionados.....	124
9.3 Gerenciamento de Grupo.....	125
9.3.1 Adicionar grupo.....	125
9.3.2 Importar recursos para o grupo.....	125
9.4 Gestão de Pessoas.....	126

DS-K1T673 Série Rosto Reconhecimento Terminal

9.4.1 Adicionar organização.....	126
9.4.2 Informações de identificação de pessoa de importação e exportação.....	127
9.4.3 Obter informações pessoais do dispositivo de controle de acesso.....	130
9.4.4 Emitir cartões para pessoas em lote.....	130
9.4.5 Perda de Cartão de Relatório.....	132
9.4.6 Definir parâmetros de emissão de cartão.....	132
9.5 Configurar cronograma e modelo.....	134
9.5.1 Adicionar Feriado	135
9.5.2 Adicionar modelo.....	135
9.6 Definir o Grupo de Acesso para Atribuir Autorização de Acesso a Pessoas.....	138
9.7 Configurar funções avançadas.....	140
9.7.1 Configurar parâmetros do dispositivo	140
9.7.2 Configurar parâmetros do dispositivo	150
9.8 Controle de Porta/Elevador	153
9.8.1 Status da porta de controle	153
9.8.2 Verificar registros de acesso em tempo real	154
Apêndice A. Dicas para digitalizar impressão digital	157
Apêndice B. Dicas ao coletar/comparar a imagem do rosto.....	159
Apêndice C. Dicas para o ambiente de instalação.....	161
Apêndice D. Dimensão	162
Apêndice E. Matriz de Comunicação e Comando de Dispositivo	163
Matriz de Comunicação	163

Capítulo 1 Visão geral

1.1 Visão geral

O terminal de reconhecimento facial é um tipo de dispositivo de acesso controlado 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

1.2.1 Características (Série Normal)

- Tela de toque LCD de 7 polegadas
- Lente dupla grande angular de 2 MP
- Distância de reconhecimento facial: 0,3 m a 3 m
- Face anti-spoofing
- Suporte remoto de vídeo live view
- Suporte ao reconhecimento de código QR

 **Nota**

O módulo periférico precisa ser conectado.

- Incorporado com sensor de imagem de luz estelar. O efeito de reconhecimento facial não será afetado em ambiente de luz fraca ou sem luz de suplemento branco
- Algoritmo de aprendizagem profunda
- Altura sugerida para reconhecimento facial: entre 1,4 m e 1,9 m
- Capacidade de 50.000 faces, capacidade de 50.000 cartões, capacidade de 5.000 impressões digitais

 **Nota**

Apenas o dispositivo com módulo de impressão digital periférico suporta a função de impressão digital.

 **Nota**

- Vários modos de autenticação
- Duração do reconhecimento facial $\leq 0,2$ s/Usuário; taxa de precisão de reconhecimento facial $\geq 99\%$
- O módulo leitor de cartão embutido adota o design de passar o cartão sob a tela para apoiar a identificação do cartão Mifare (cartão IC) em locais com altos níveis de segurança, como segurança pública ou local judicial.
- Vários tipos de cartão de autenticação

DS-K1T673 Série Rosto Reconhecimento Terminal

- Suporte ao reconhecimento de várias pessoas (até 5 pessoas)
-

DS-K1T673 Série Rosto Reconhecimento Terminal

- Suporte a detecção de uso de máscara
- Suporte a alarme de violação, alarme de abertura de porta por força externa, cartão de coação e alarme de senha de coação
- Suporte a vários modos de exibição, incluindo modo normal, modo de anúncio e modo simples
- Prompt de áudio
- Exibição do resultado da autenticação de suporte
- Conecta-se à unidade de controle de porta segura via protocolo RS-485 para evitar a abertura da porta quando o terminal é destruído
- Conecta-se ao controlador de acesso externo ou leitor de cartão Wiegand via protocolo Wiegand
- Visualização remota ao vivo via protocolo RTSP; modo de codificação: H.264
- Design do cão de guarda e função de adulteração
- NTP, sincronização de tempo manual e sincronização automática
- Gerenciamento de parâmetros, pesquisa e configurações do dispositivo
- Capturar links e salvar imagens capturadas
- Importa dados para o dispositivo a partir do software cliente
- Gerencie, pesquise e defina dados do dispositivo depois de fazer login no dispositivo localmente
- Áudio bidirecional com software cliente, estação de porta, estação interna e estação principal

1.2.2 Características (Série T)

- Tela de toque LCD de 7 polegadas
- Lente dupla grande angular de 2 MP
- Distância de reconhecimento facial: 0,3 m a 3 m
- Face anti-spoofing
- Suporte remoto de vídeo live view
- Suporte ao reconhecimento de código QR

Nota

O módulo periférico precisa ser conectado.

- Incorporado com sensor de imagem de luz estelar. O efeito de reconhecimento facial não será afetado em ambiente de luz fraca ou sem luz sem luz de suplemento branco
- Algoritmo de aprendizagem profunda
- Altura sugerida para reconhecimento facial: entre 1,4 m e 1,9 m
- Capacidade de 100.000 rostos, capacidade de 500.000 cartões, 10.000 impressões digitais e capacidade para 150.000 eventos

Nota

Apenas o dispositivo com módulo de impressão digital periférico suporta a função de impressão digital.

- Vários modos de autenticação
- Duração do reconhecimento facial $\leq 0,2$ s/Usuário; taxa de precisão de reconhecimento facial $\geq 99\%$
- O módulo leitor de cartão embutido adota o design de passar o cartão sob a tela para apoiar a identificação do cartão Mifare (cartão IC) em locais com altos níveis de segurança, como segurança pública ou local judicial.

DS-K1T673 Série Rosto Reconhecimento Terminal

- Vários tipos de cartão de autenticação
- Suporte ao reconhecimento de várias pessoas (até 5 pessoas)
- Suporte a detecção de uso de máscara
- Suporta alarme de violação, alarme de abertura de porta por força externa, cartão de coação e alarme de senha de coação
- Suporta vários modos de exibição, incluindo o modo normal, o modo de anúncio e o modo simples.
- Prompt de áudio
- Exibição do resultado da autenticação de suporte
- Conecta-se à unidade de controle de porta segura via protocolo RS-485 para evitar a abertura da porta quando o terminal é destruído
- Conecta-se ao controlador de acesso externo ou leitor de cartão Wiegand via protocolo Wiegand
- Visualização remota ao vivo via protocolo RTSP; modo de codificação: H.264
- Design do cão de guarda e função de adulteração
- NTP, sincronização de tempo manual e sincronização automática
- Gerenciamento de parâmetros, pesquisa e configurações do dispositivo
- Capturar links e salvar imagens capturadas
- Importa dados para o dispositivo a partir do software cliente
- Gerencie, pesquise e defina dados do dispositivo depois de fazer login no dispositivo localmente
- Áudio bidirecional com software client, estação de porta, estação interior e estação principal

Capítulo 2 Aparência

Consulte o seguinte conteúdo para obter informações detalhadas sobre o terminal de reconhecimento facial:

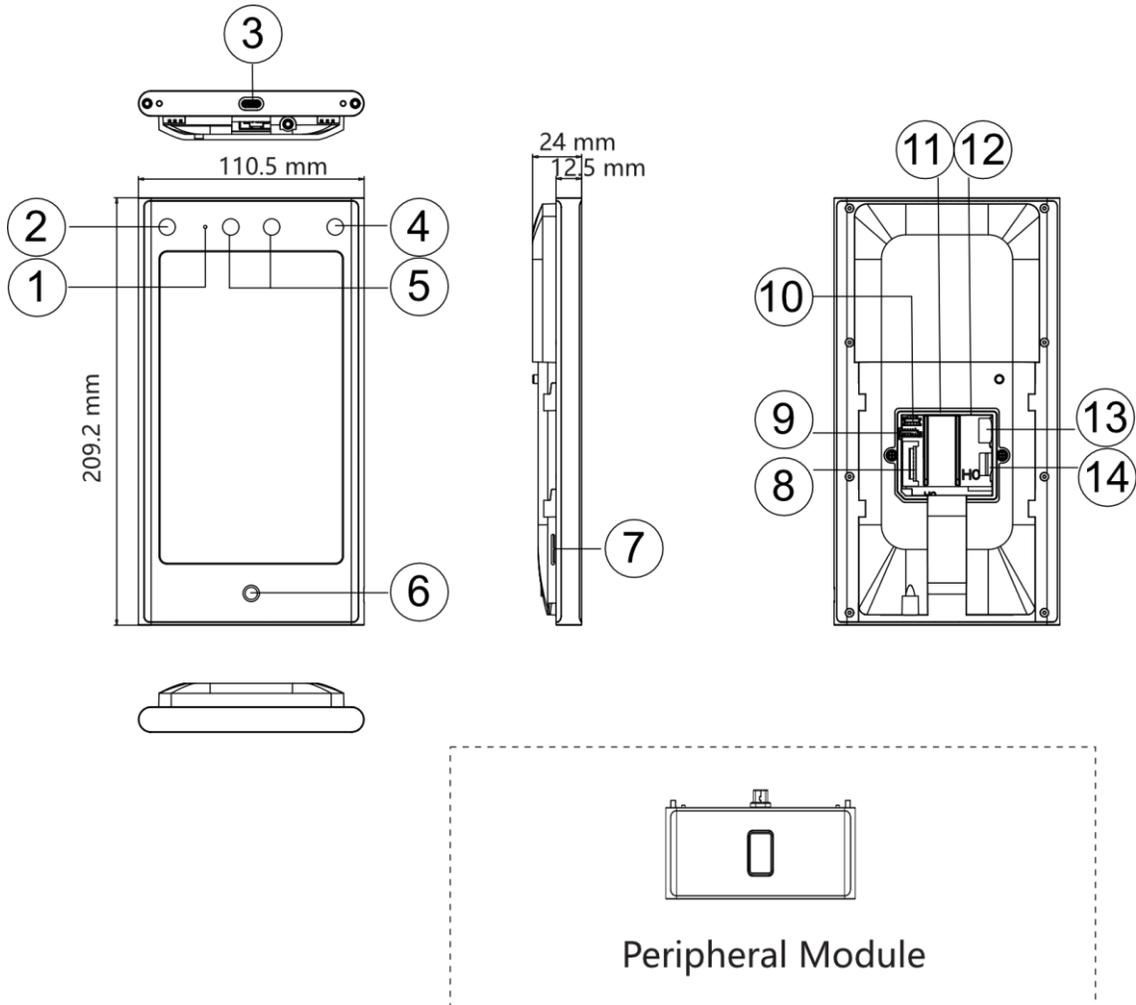


Figura 2-1 Diagrama do Terminal de Reconhecimento Facial
Tabela 2-1 Descrição do Terminal de Reconhecimento Facial

Não.	Nome
1	MICROFONE
2	Luz IR
3	Interface USB Tipo-C

DS-K1T673 Série Rosto Reconhecimento Terminal

Não.	Nome
	 Nota Para conexão com o módulo periférico.
4	Luz IR
5	Câmera
6	Luz de Respiração
7	Altifalante
8	Terminal de fiação
9	Interface do módulo de temperatura
10	Porta de depuração (somente para depuração)
11	Interface de rede
12	Saída de áudio  Nota Se o diâmetro do plugue de áudio for maior que 8 mm, um adaptador externo será necessário.
13	Adulterar
14	Slot para cartão SIM  Nota O slot para cartão SIM varia de acordo com os diferentes modelos.
15	Slot para cartão TF (reservado)

Nota

- Os valores são apenas para referência.
- O dispositivo suporta módulo de código QR externo, módulo Bluetooth, impressão digital + módulo Bluetooth, impressão digital + módulo Bluetooth + código QR, módulo Bluetooth + código QR, que pode ser acessado de acordo com suas necessidades reais.

Capítulo 3 Instalação

3.1 Ambiente de Instalação

- 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.
- Se você tiver que instalar o dispositivo ao ar livre, você deve instalar um escudo de proteção (opcional) para o dispositivo.



Nota

Para obter detalhes sobre o ambiente de instalação, consulte *Dicas para o ambiente de instalação*.

3.2 Montagem embutida com caixa de gangue

Antes de começar

Remova a folha traseira do dispositivo.

Passos

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



Nota

A caixa da gangue não é fornecida.

DS-K1T673 Série Rosto Reconhecimento Terminal

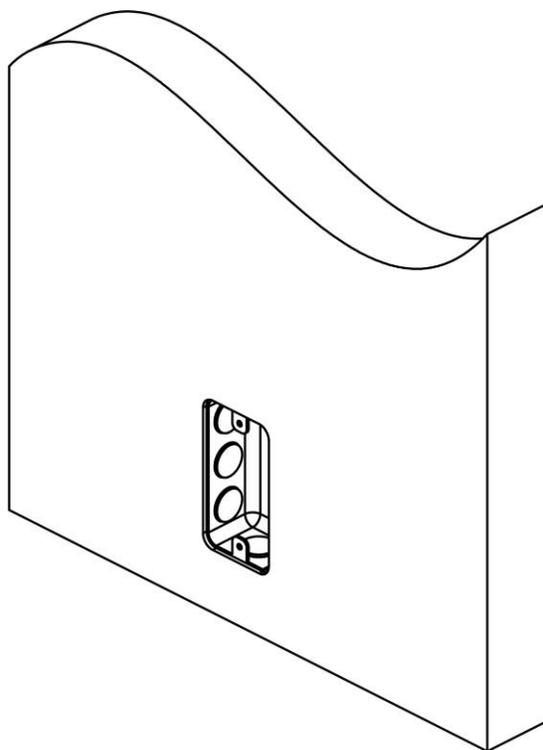


Figura 3-1 Caixa de instalação do gangue

2. Prenda a placa de montagem na caixa da gangue com 2 parafusos fornecidos (SC-K1A4X24_5).

DS-K1T673 Série Rosto Reconhecimento Terminal

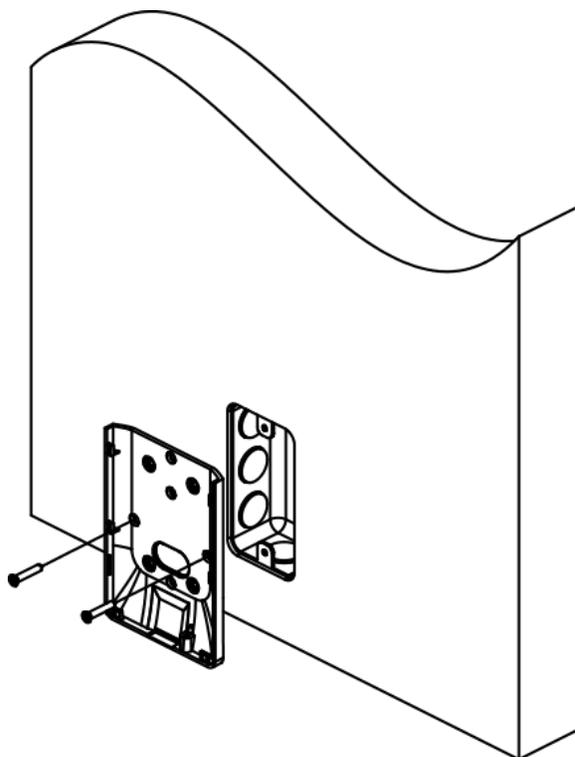


Figura 3-2 Instalar placa de montagem

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

DS-K1T673 Série Rosto Reconhecimento Terminal

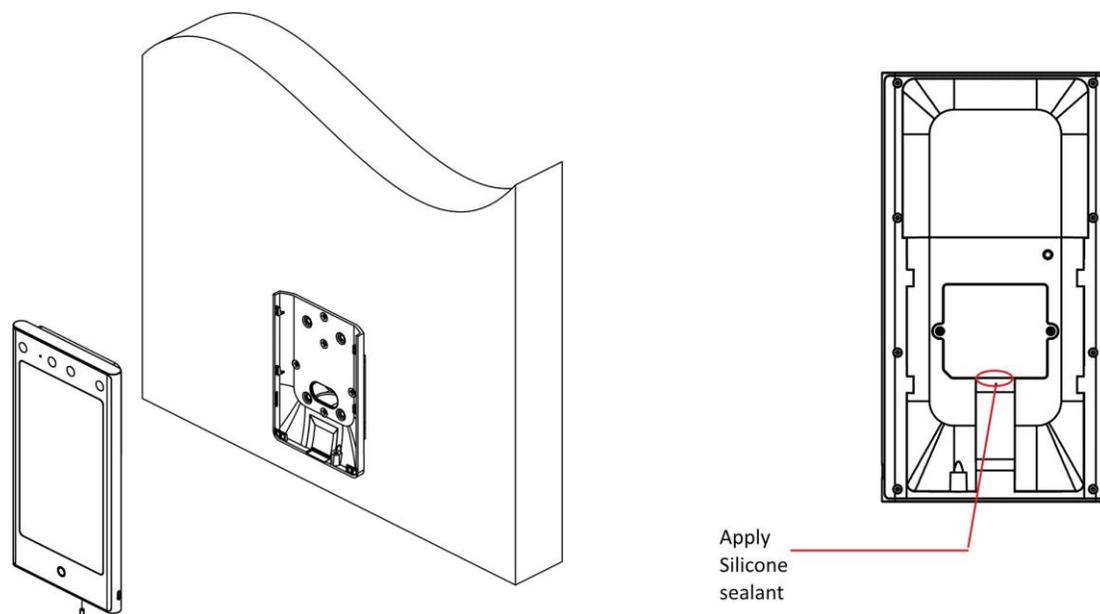


Figura 3-3 Dispositivo seguro

i Nota

Aplique selante de silicone entre a área de fiação do cabo para evitar que a gota de chuva entre.

4. Alinhe o dispositivo com a placa de montagem e prenda o dispositivo na placa de montagem com 1 parafuso fornecido (SC-KM3X6-H2-SUS).

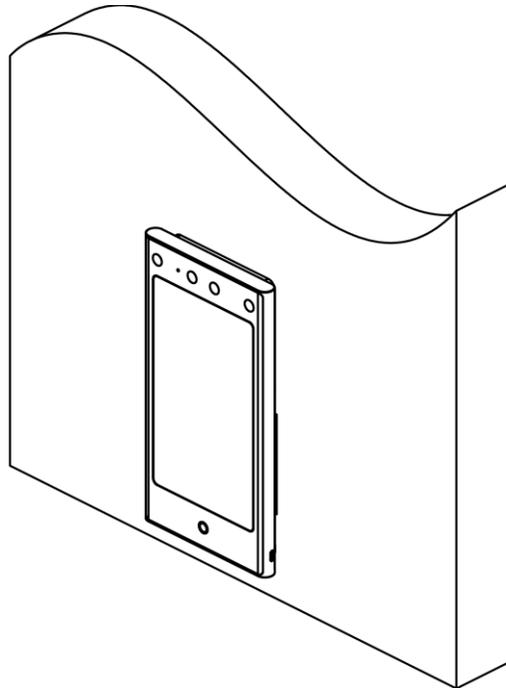


Figura 3-4 Dispositivo seguro

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

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. De acordo com a linha de dados no modelo de montagem, cole o modelo de montagem na parede ou em outras superfícies, 1,4 metros mais alto que o solo.

DS-K1T673 Série Rosto Reconhecimento Terminal

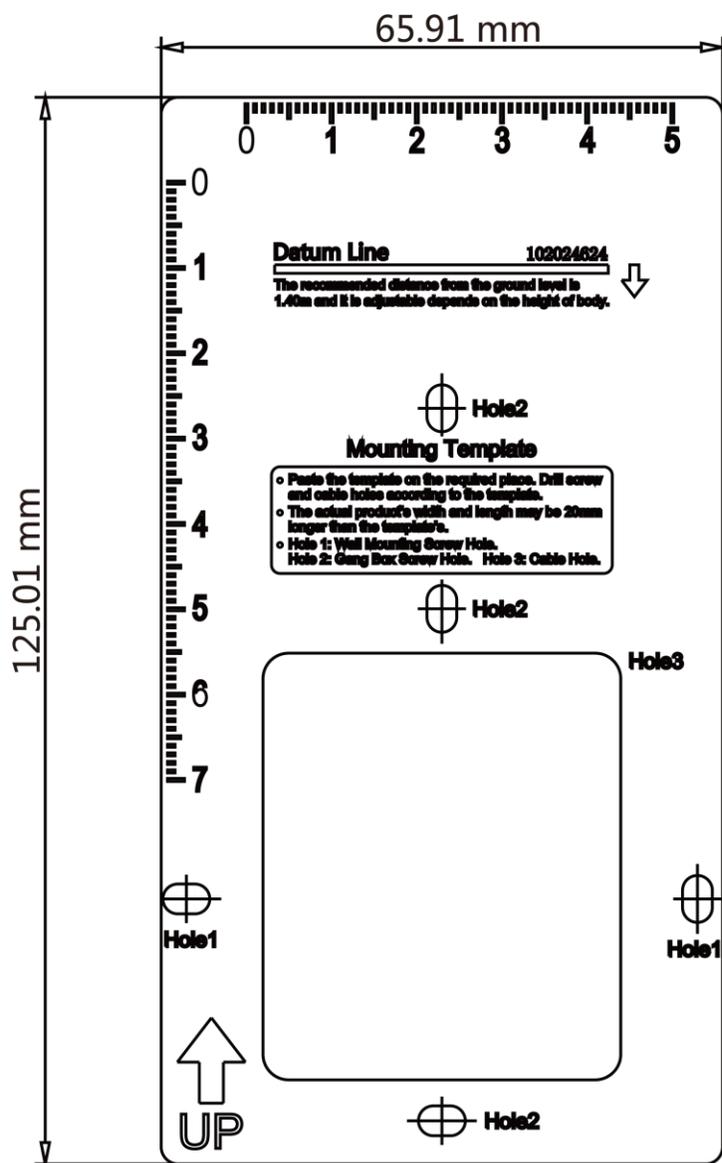


Figura 3-5 Modelo de montagem

2. Faça furos na parede ou em outra superfície de acordo com o furo 1 no modelo de montagem.
3. Remova o orifício do cabo na placa de montagem com ferramentas.
4. Alinhe os orifícios à placa de montagem e prenda a placa de montagem na parede com os 2 parafusos fornecidos (K1A×24).

DS-K1T673 Série Rosto Reconhecimento Terminal

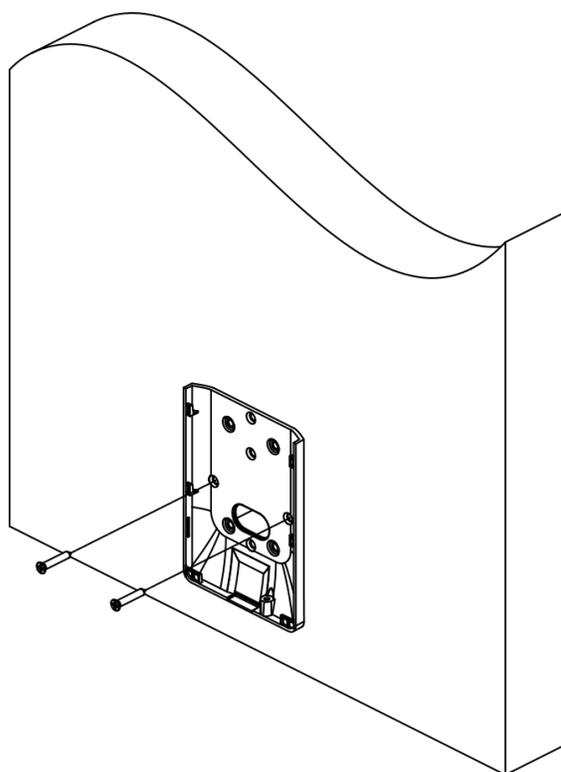


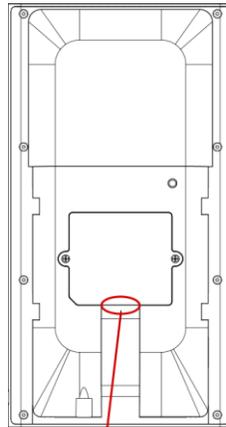
Figura 3-6 Placa de montagem de instalação

5. 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.

DS-K1T673 Série Rosto Reconhecimento Terminal



Apply Silicone
Sealant

Figura 3-7 Aplicar selante de silicone

6. Alinhe o dispositivo com a placa de montagem e pendure-o na placa de montagem.

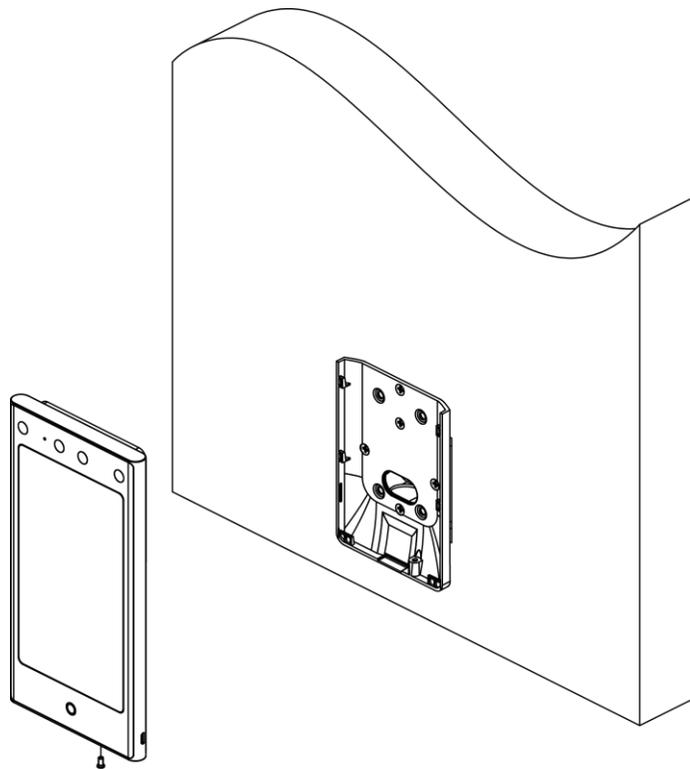


Figura 3-8 Dispositivo de travamento

7. Use 1 parafuso fornecido (KM3×6) para fixar o dispositivo e a placa de montagem.

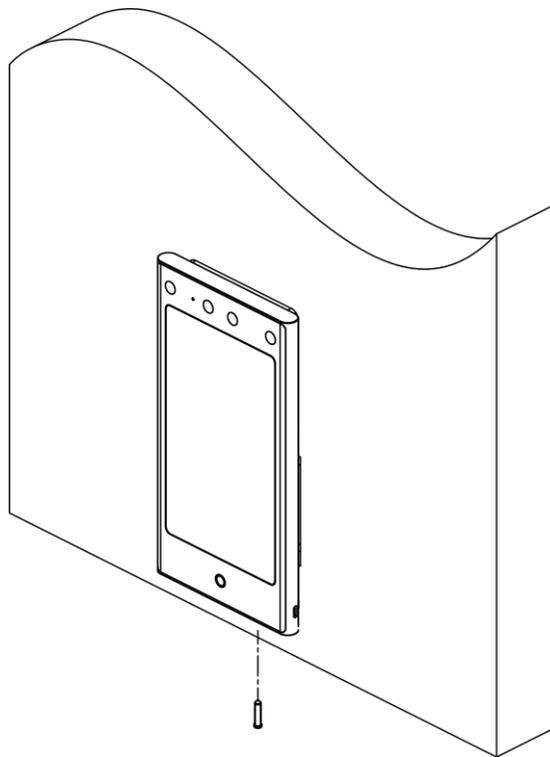


Figura 3-9 Dispositivo seguro

8. **Opcional:** Conecte o módulo periférico de acordo com suas necessidades reais.
9. 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 com suporte

3.4.1 Preparação antes da montagem com suporte

Passos

1. Faça furos na superfície da catraca de acordo com a figura exibida abaixo. E instale porcas à prova d'água.

Nota

Solda depois de pressionar rebites para evitar a entrada de água.

DS-K1T673 Série Rosto Reconhecimento Terminal

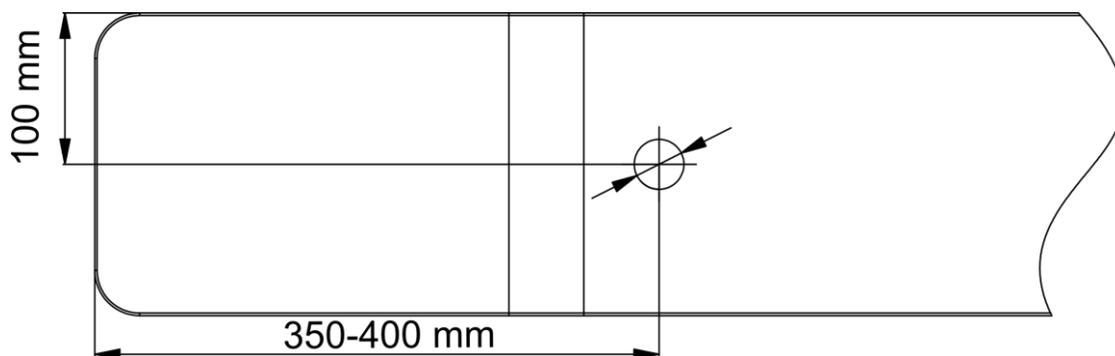


Figura 3-10 Furos de perfuração na catraca

2. Se o ângulo de instalação precisar ser de 180° perpendicular ao corpo da catraca, as seguintes operações são necessárias.

1) Tire os 3 parafusos mostrados na figura a seguir.

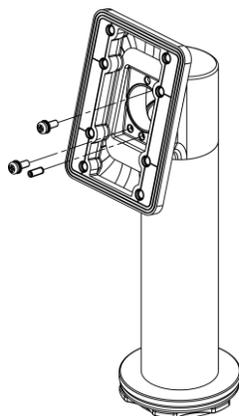


Figura 3-11 Parafusos de decolagem

2) Gire a peça fixa em 180° e instale os 3 parafusos para trás.

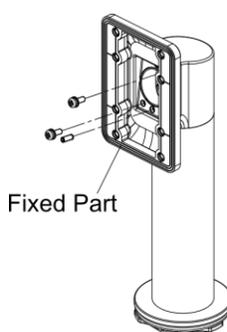


Figura 3-12 Girar peça fixa

3.4.2 Suporte de montagem

Passos

1. Passe o fundo do suporte através da catraca e fixe-o na catraca com porca autossuficiente. Ajuste o suporte para o ângulo adequado e fixe a porca firmemente junto à chave inglesa.

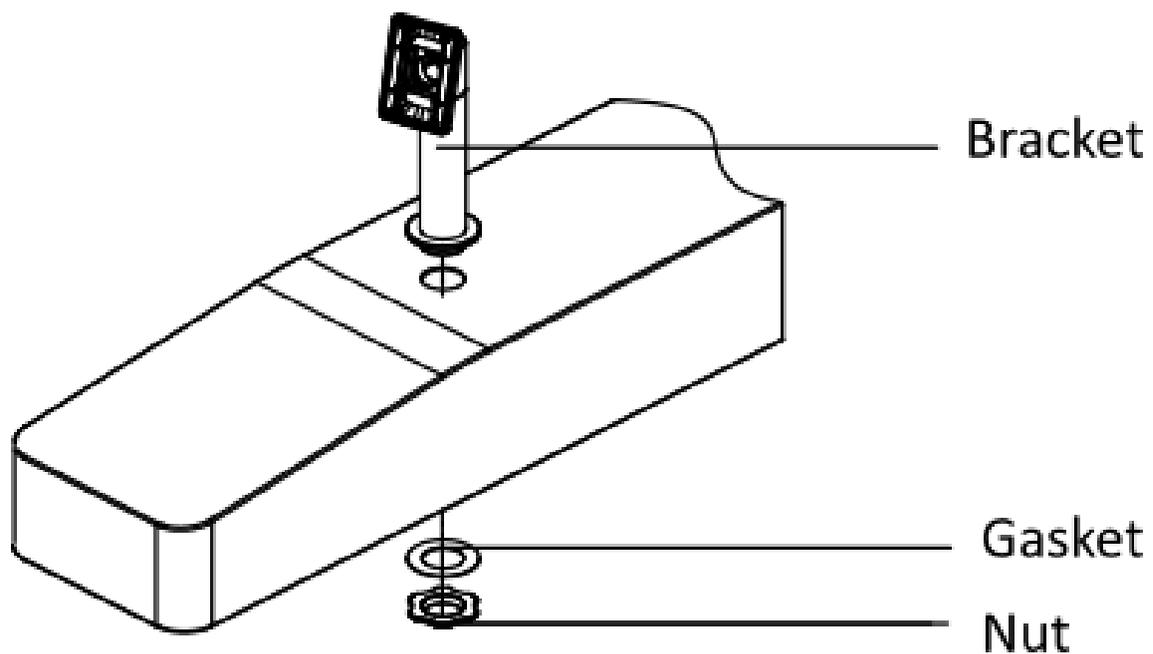


Figura 3-13 Suporte de correção

2. Fixe a placa de montagem no suporte por 4 parafusos K1M4×8-SUS.

DS-K1T673 Série Rosto Reconhecimento Terminal

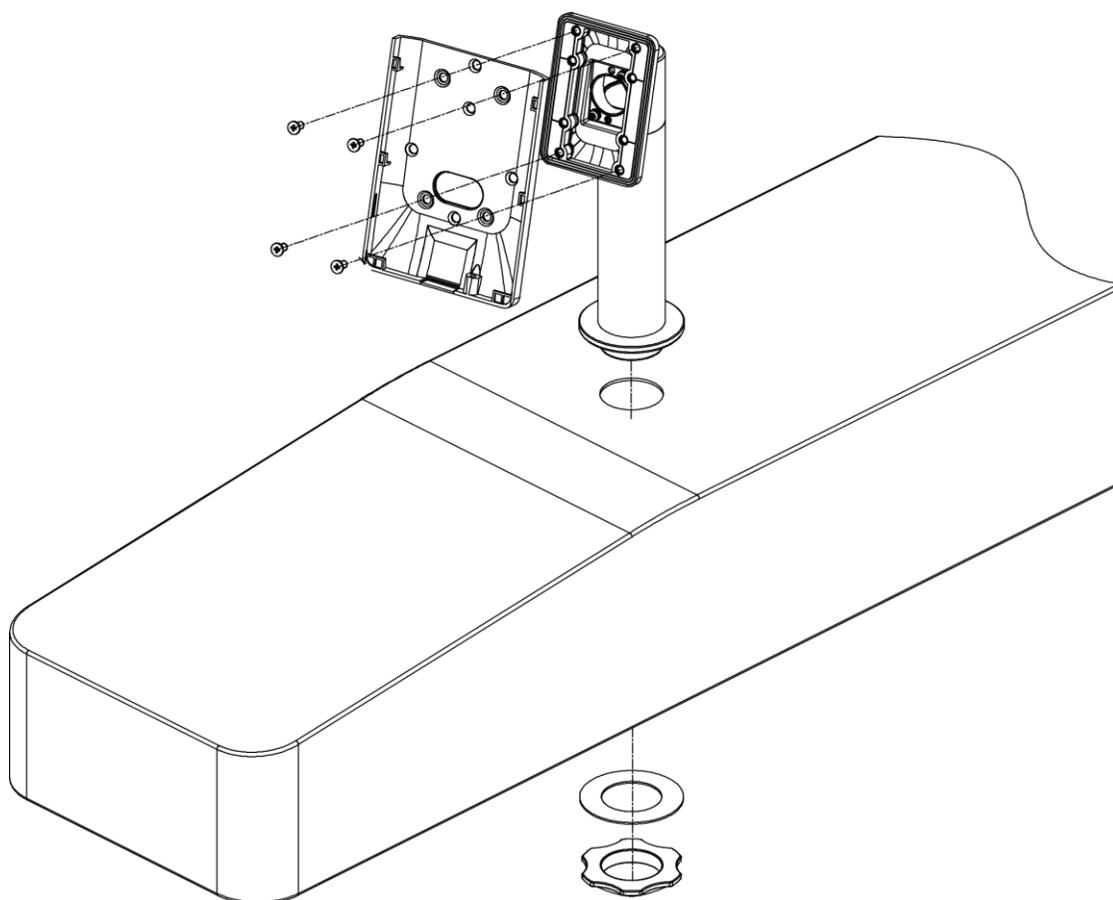


Figura 3-14 Placa de montagem fixa

3. Passe os cabos terminais de reconhecimento facial através do orifício do cabo e insira-os na catraca interna. Fixe o terminal de reconhecimento facial na placa de montagem com parafusos KM3×6-H2-SUS.

DS-K1T673 Série Rosto Reconhecimento Terminal

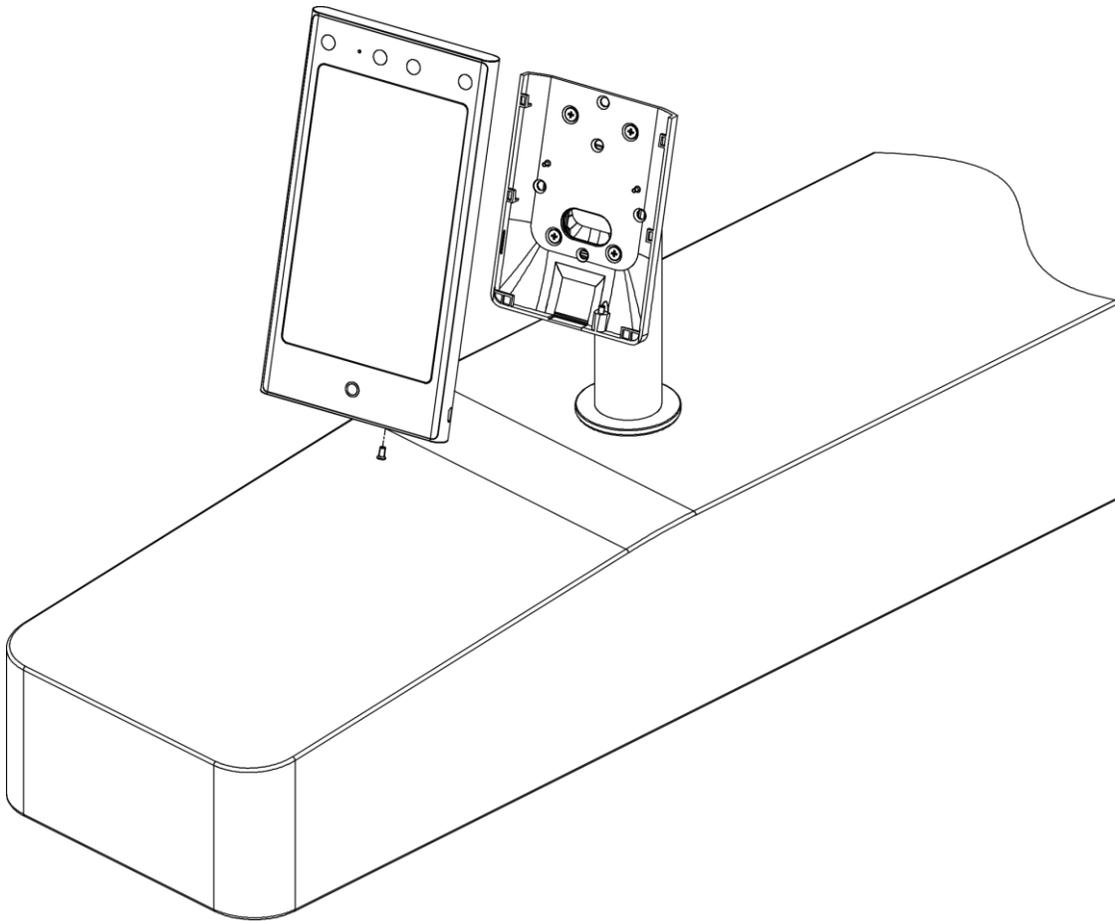


Figura 3-15 Corrigir reconhecimento facial no terminal

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

Capítulo 4 Fiação

O dispositivo suporta a conexão com o terminal RS-485, a trava da porta, o botão de saída, os dispositivos de saída / entrada de alarme, o leitor de cartão Wiegand, o controlador de acesso e a fonte de alimentação. Você pode conectar os periféricos de acordo com as descrições abaixo.

Se conectar o leitor de cartão Wiegand com o controlador de acesso, o terminal de reconhecimento facial pode transmitir as informações de autenticação para o controlador de acesso e o controlador de acesso pode julgar se deve abrir a porta ou não.



Nota

- Se o tamanho do cabo for de 18 AWG, você deve usar uma fonte de alimentação de 12 V comutada em modo. 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 deverá usar uma fonte de alimentação de modo comutado 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 cabo for de 12 AWG, você deverá usar uma fonte de alimentação de modo comutado de 12 V. E a distância entre a fonte de alimentação e o dispositivo não deve ser superior a 40 m.
-

4.1 Descrição Terminal

Os terminais contêm entrada de energia, entrada de alarme, saída de alarme, RS-485, saída Wiegand e fechadura da porta.

O diagrama do terminal é o seguinte:

DS-K1T673 Série Rosto Reconhecimento Terminal

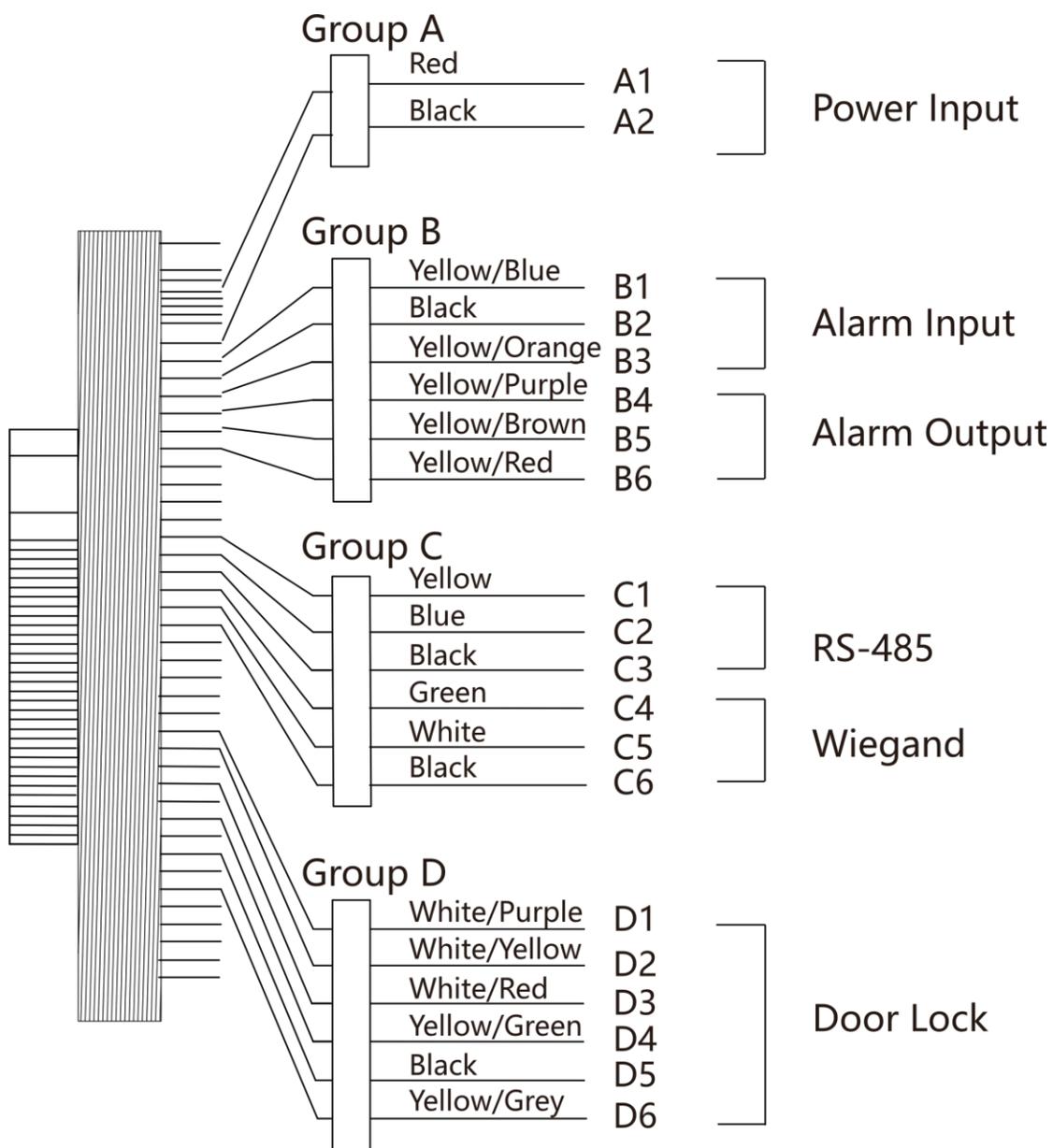


Figura 4-1 Diagrama de terminal

As descrições dos terminais são as seguintes:

DS-K1T673 Série Rosto Reconhecimento Terminal

Tabela 4-1 Descrições dos terminais

Grupo	Nã o.	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	Entrada de alarme	Amarelo/Azul	IN1	Entrada de alarme 1
	B2		Preto	GND	Chão
	B3		Amarelo/Laranja	IN2	Entrada de alarme 2
	B4	Saída de alarme	Amarelo/Roxo	NC	Fiação de saída de alarme
	B5		Amarelo/Castanho	.COM	
	B6		Amarelo/Vermelho	NÃO	
Grupo C	C1	RS-485	Amarelo	485+	Fiação RS-485
	C2		Azul	485-	
	C3		Preto	GND	Chão
	C4	Wiegand	Verde	W0	Fiação Wiegand 0
	C5		Branco	W1	Fiação Wiegand 1
	C6		Preto	GND	Chão
Grupo D	D1	Fechadura da porta	Branco/roxo	NC	Fiação de bloqueio (NC)
	D2		Branco/Amarelo	.COM	Comum
	D3		Branco/Vermelho	NÃO	Fiação de bloqueio (NÃO)
	D4		Amarelo/Verde	SENSOR	Contato da Porta
	D5		Preto	GND	Chão

DS-K1T673 Série Rosto Reconhecimento Terminal

	D6		Amarelo/Cinze nto	BTN	Saia da fiação da porta
--	----	--	----------------------	-----	-------------------------------

4.2 Dispositivo Normal de Fio

Você pode conectar o terminal com periféricos normais.

DS-K1T673 Série Rosto Reconhecimento Terminal

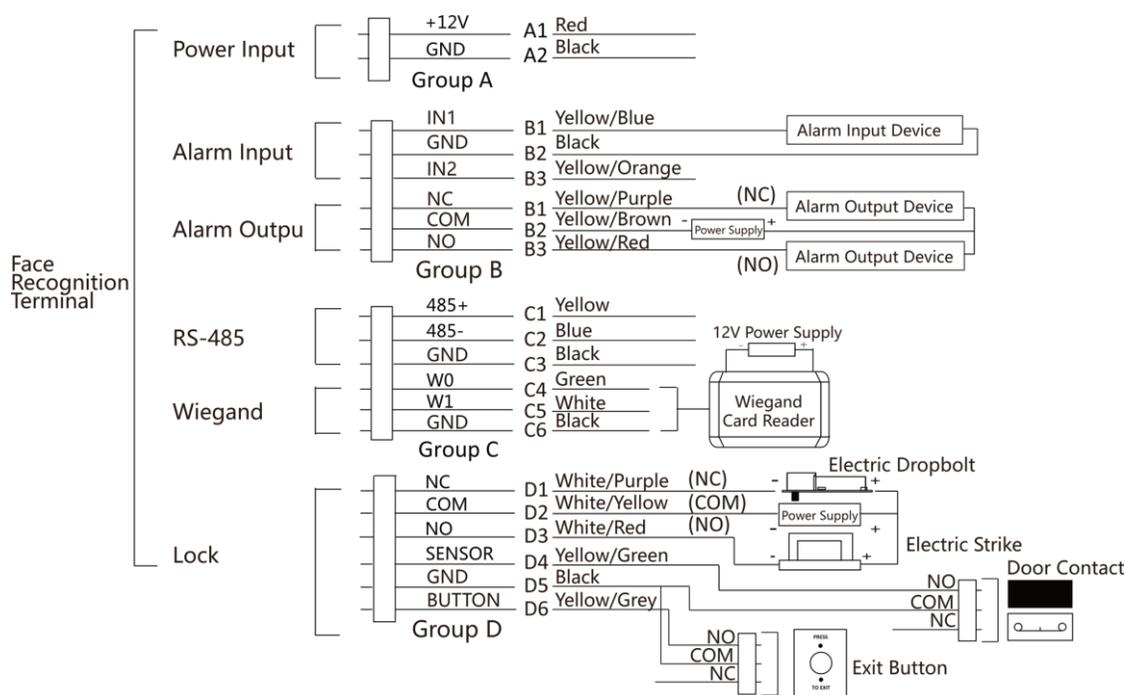


Figura 4-2 Fiação do dispositivo

Nota

- Você deve definir a direção Wiegand do terminal de reconhecimento facial como **Entrada** para se conectar a um leitor de cartão Wiegand . Se se conectar a um controlador de acesso, você deve definir a direção Wiegand como **Saída** para transmitir informações de autenticação para o controlador de acesso.
- Para obter detalhes sobre as configurações de direção de Wiegand, consulte **Definir parâmetros de Wiegand** .
- Não ligue o dispositivo directamente à alimentação eléctrica.

4.3 Unidade de Controle de Porta Segura de Arame

Você pode conectar o terminal com a unidade de controle de porta segura . O diagrama de fiação é o seguinte.

DS-K1T673 Série Rosto Reconhecimento Terminal

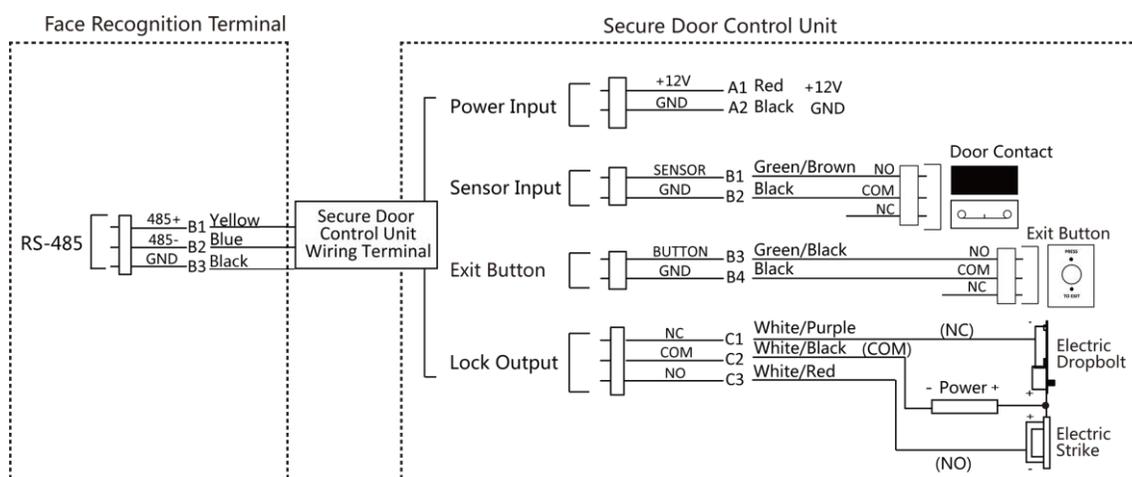


Figura 4-3 Fiação da unidade de controle de porta segura

Nota

A unidade de controle de porta segura deve se conectar a uma fonte de alimentação externa separadamente. A fonte de alimentação externa sugerida é de 12V, 0,5A.

4.4 Módulo de incêndio de fio

4.4.1 Diagrama de fiação da porta aberta ao desligar

Tipo de fechadura: Bloqueio do ânode, bloqueio magnético e parafuso elétrico (NO) Tipo de segurança: Porta aberta ao desligar

Cenário: Instalado no Acesso ao Fire Engine

Tipo 1

Nota

O sistema de incêndio controla a fonte de alimentação do sistema de controle de acesso.

DS-K1T673 Série Rosto Reconhecimento Terminal

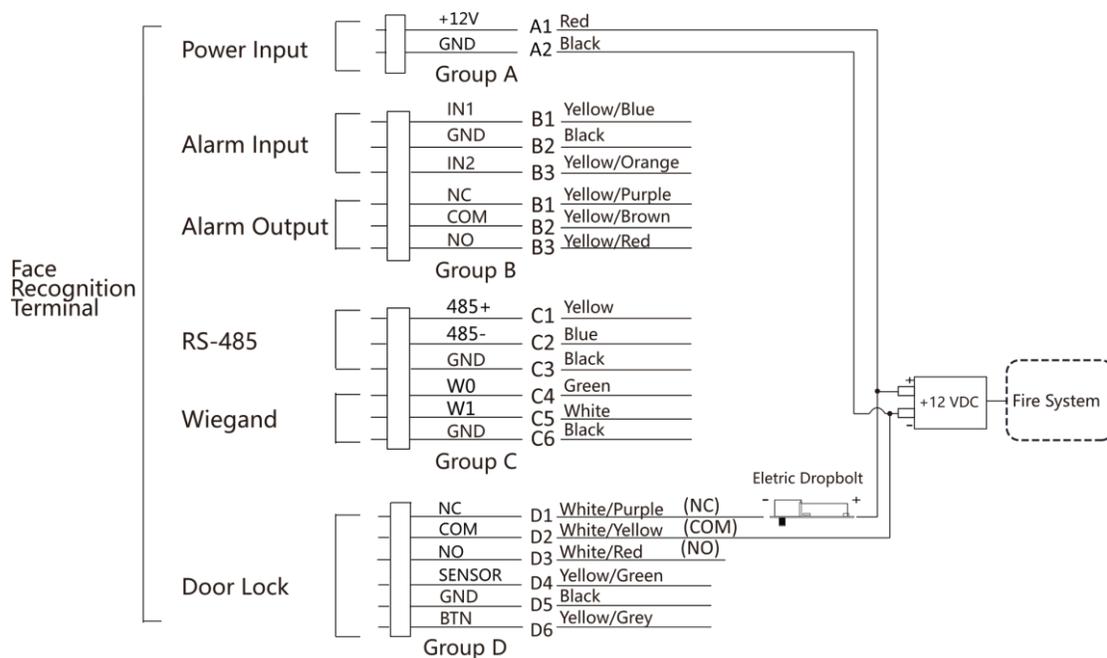


Figura 4-4 Dispositivo de fio

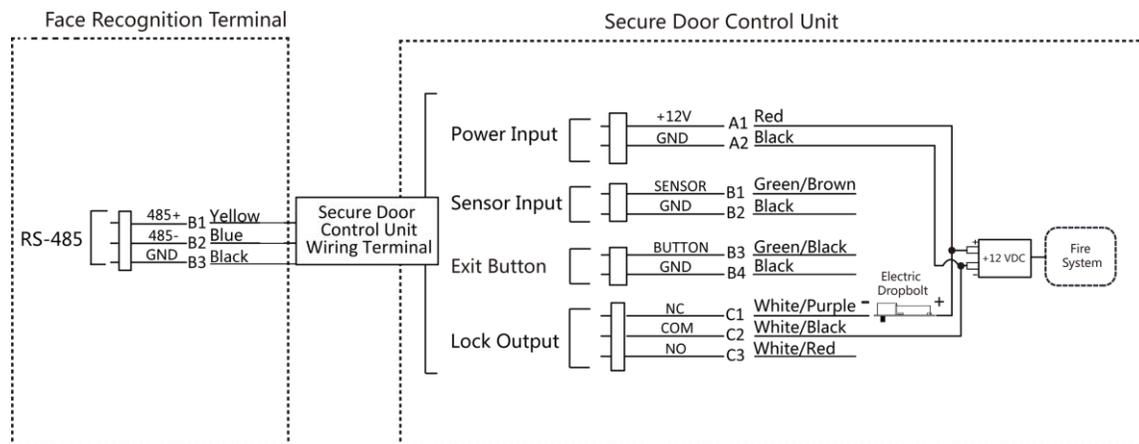


Figura 4-5 Unidade de controle de porta segura de fio

Tipo 2

Nota

O sistema de incêndio (NO e COM, normalmente aberto ao desligar) é conectado com a trava e a fonte de alimentação em série. Quando um alarme de incêndio é acionado, a porta permanece aberta. Em tempos normais, NO e COM são fechados.

DS-K1T673 Série Rosto Reconhecimento Terminal

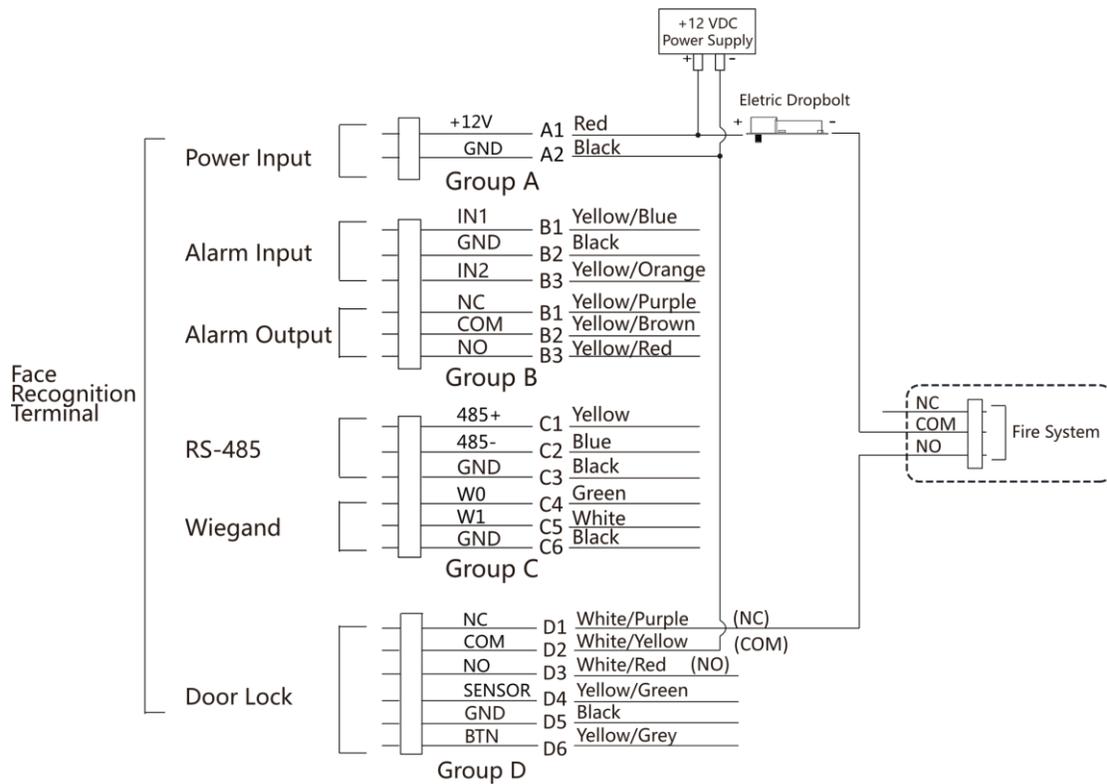


Figura 4-6 Dispositivo de fiação

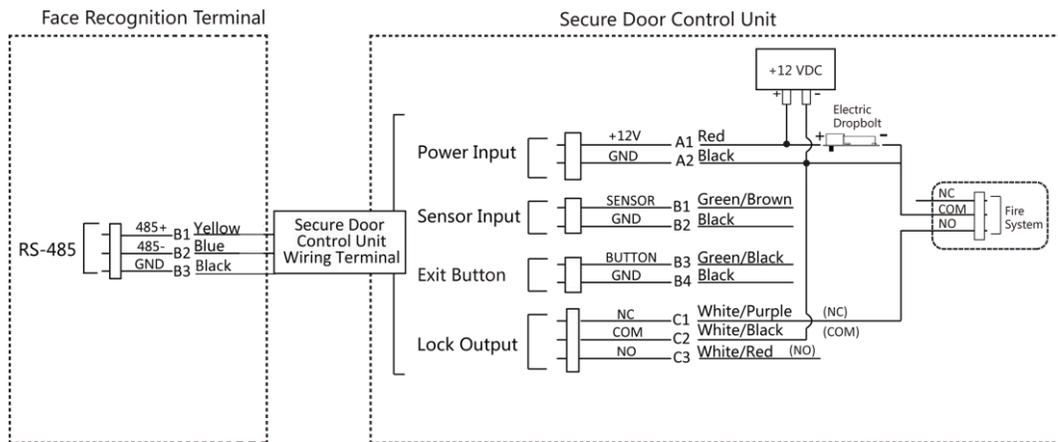


Figura 4-7 Unidade de controle de porta segura de fiação

4.4.2 Diagrama de fiação da porta trancada ao desligar

Tipo de fechadura: Fechadura catódica , fechadura elétrica e parafuso elétrico (NC) Tipo de segurança: Porta trancada ao desligar

DS-K1T673 Série Rosto Reconhecimento Terminal

Cenário: Instalado na Entrada/Saída com Ligação de Incêndio

Nota

- A Fonte de Alimentação Ininterpretável (UPS) é necessária.
- O sistema de incêndio (NC e COM, normalmente fechado ao desligar) está conectado com a fechadura e a fonte de alimentação em série. Quando um alarme de incêndio é acionado, a porta permanece aberta. Em tempos normais, NC e COM estão abertos.

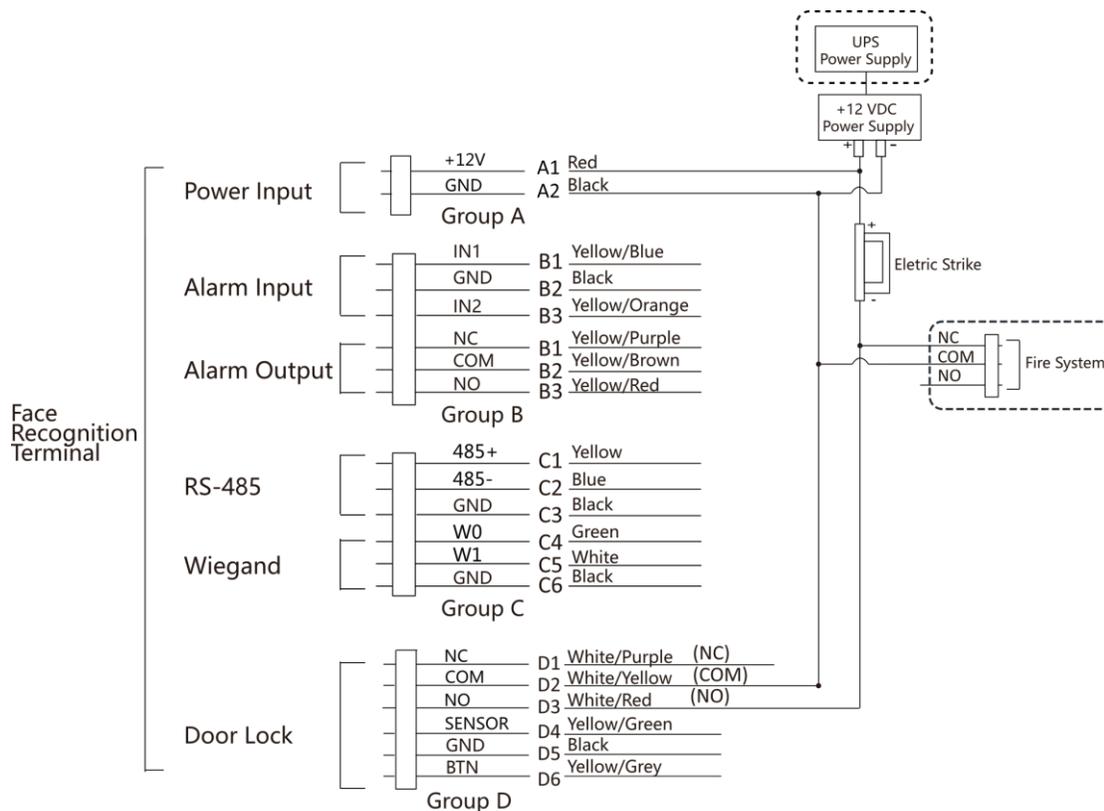


Figura 4-8 Fiação do dispositivo

DS-K1T673 Série Rosto Reconhecimento Terminal

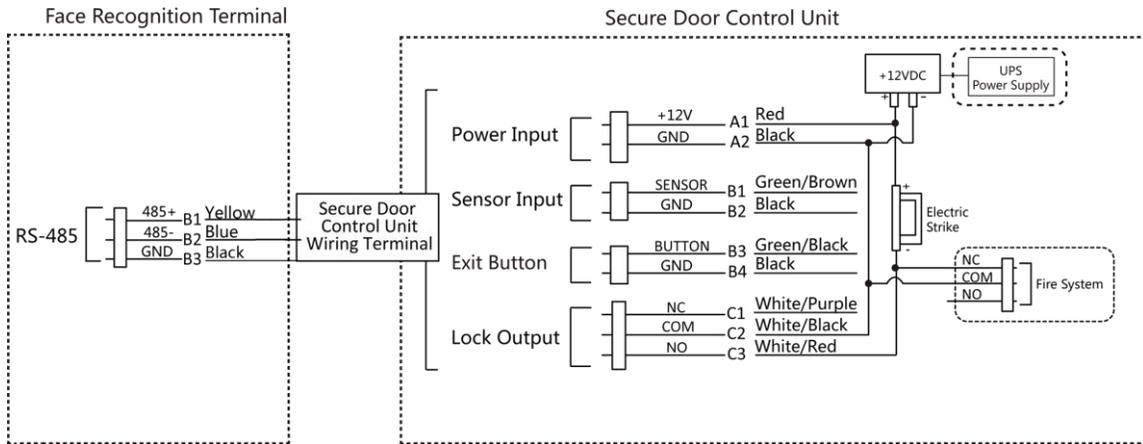


Figura 4-9 Diagrama de fiação

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.

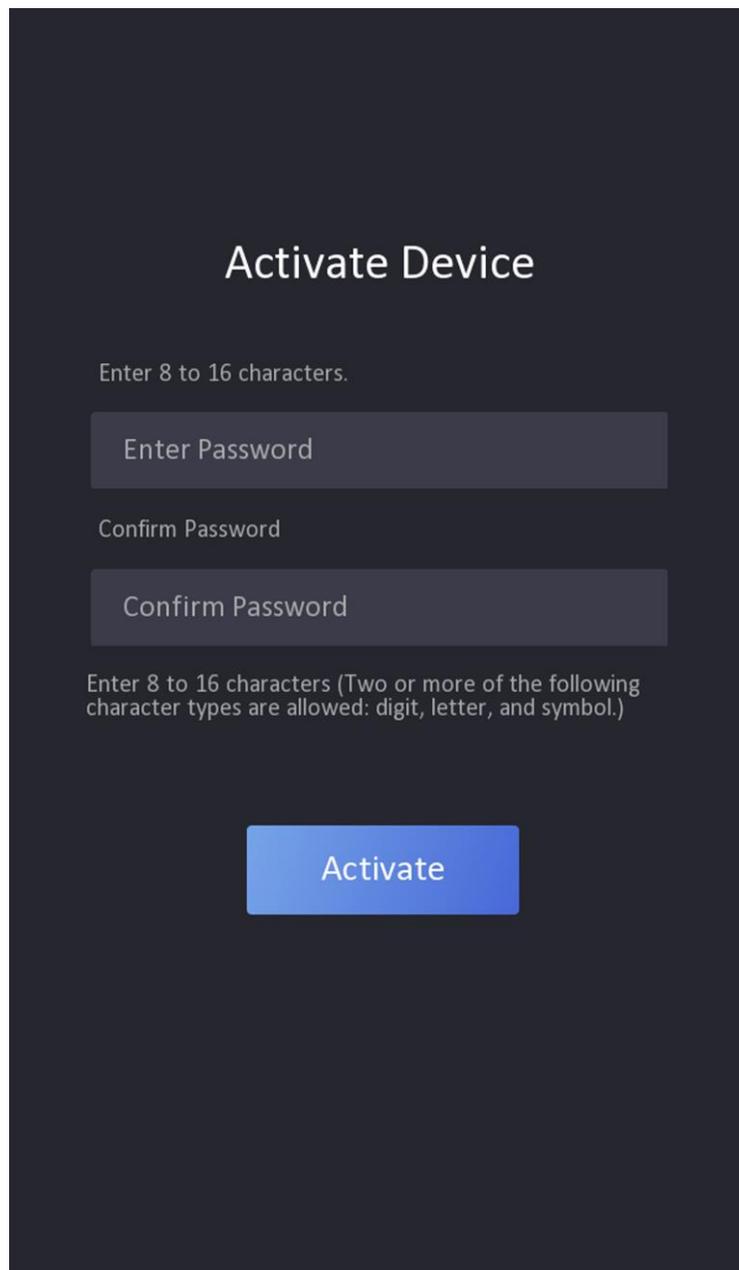
A ativação através do dispositivo, da ferramenta SADP e do software cliente é suportada. Os valores padrão do dispositivo são os seguintes:

- 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.



Activate Device

Enter 8 to 16 characters.

Enter Password

Confirm Password

Confirm Password

Enter 8 to 16 characters (Two or more of the following character types are allowed: digit, letter, and symbol.)

Activate

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, letras minúsculas, números, e especiais

DS-K1T673 Série Rosto Reconhecimento Terminal

caracteres), a fim de 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.

- Após a ativação, você deve selecionar um idioma de acordo com suas necessidades de aclura.
- Após a ativação, você deve selecionar um modo de aplicativo. Para obter detalhes, consulte **Definir modo de aplicativo**.
- 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 Ativar via navegador da Web

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, especializado no sistema de alta segurança, redefinir a senha mensal ou semanalmente pode proteger melhor o 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.

DS-K1T673 Série Rosto Reconhecimento Terminal

The screenshot shows the SADP interface with a table of devices. The table has columns for ID, Device Type, Security, IPv4 Address, Port, Software Version, IPv4 Gateway, HTTP Port, and Device Serial No. Device 007 is highlighted in red and marked as 'Inactive' with the IP address 192.0.0.64. A red box around the table is labeled 'Select inactive device.' Below the table, there is a red box labeled 'Input and confirm password.' To the right, the 'Activate the Device' dialog is shown, featuring a lock icon, the text 'The device is not activated.', a blue button 'You can modify the network parameters after the device activation.', and a form with 'New Password' and 'Confirm Password' fields, a 'Strong' indicator, and an 'Enable Hi-Connect' checkbox. A red box around the password fields is labeled 'Input and confirm password.' Below the dialog is a red 'Activate' button.

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, você é obrigado a criar a senha para ativá-los antes e eles podem 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 em, alterando 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.

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.

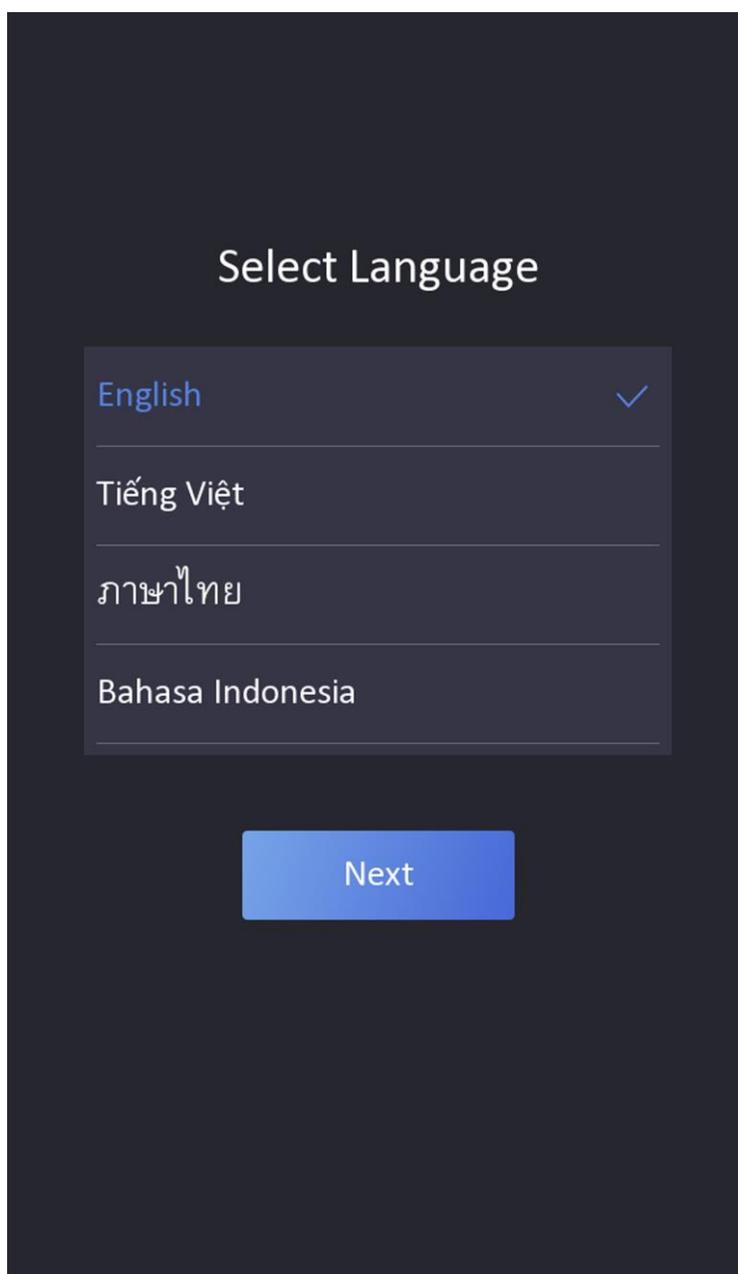


Figura 6-1 Selecione o idioma do sistema

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 o Modo de Aplicativo

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

Passos

1. Na página Bem-vindo, selecione **Interior** ou **Outros** na lista suspensa.

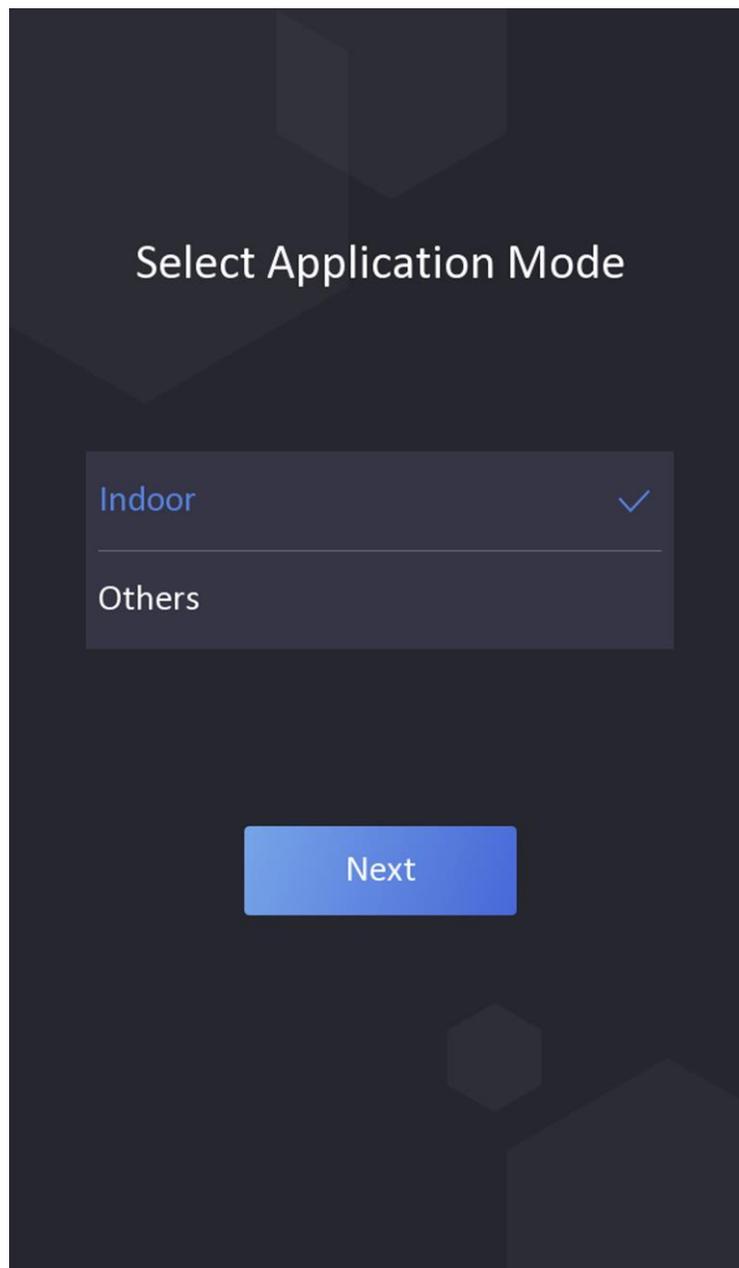


Figura 6-2 Página de boas-vindas

2. Toque em **OK** para salvar.

Nota

- Você também pode alterar as configurações em *Configurações do Sistema*.
 - 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.
-

6.3 Configurações de privacidade

Após a ativação, selecionando o modo de aplicativo e 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.

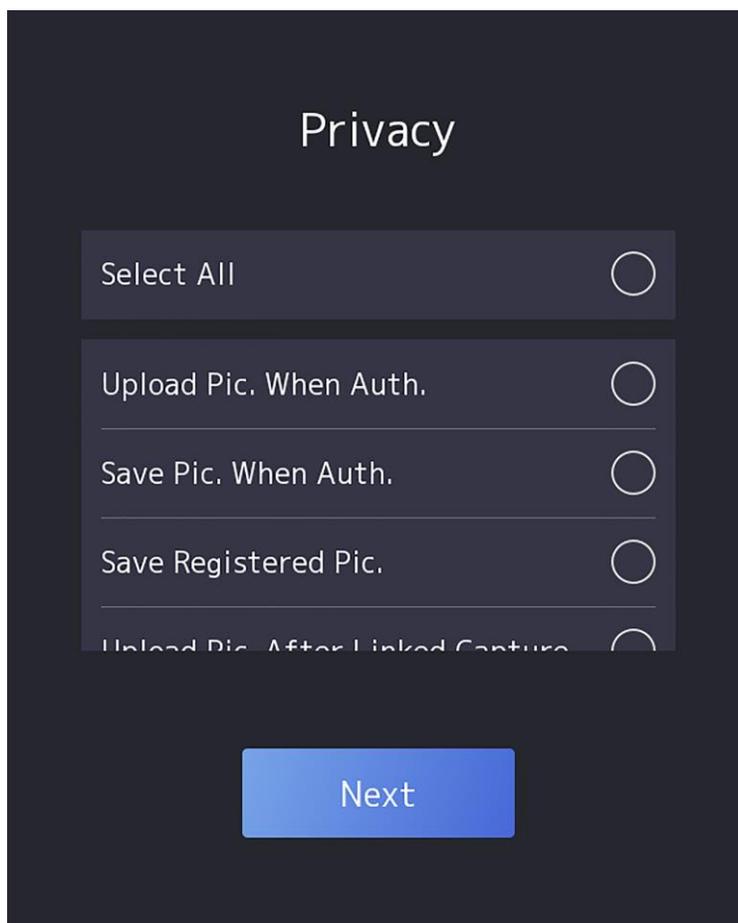


Figura 6-3 Privacidade

DS-K1T673 Série Rosto Reconhecimento Terminal

Carregar foto capturada. Quando Auth. (Carregar imagem capturada ao autenticar)

Carregue as imagens capturadas ao autenticar na plataforma automaticamente.

Salve a foto capturada. Quando Auth. (Salvar imagem capturada 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.

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

6.4 Definir administrador

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

Antes de começar

Ative o dispositivo e selecione um modo de aplicativo.

Passos

- 1. Opcional:** toque em **Ignorar** para ignorar a adição de administrador, se necessário.
- 2.** Insira o nome do administrador (opcional) e toque em **Avançar**.

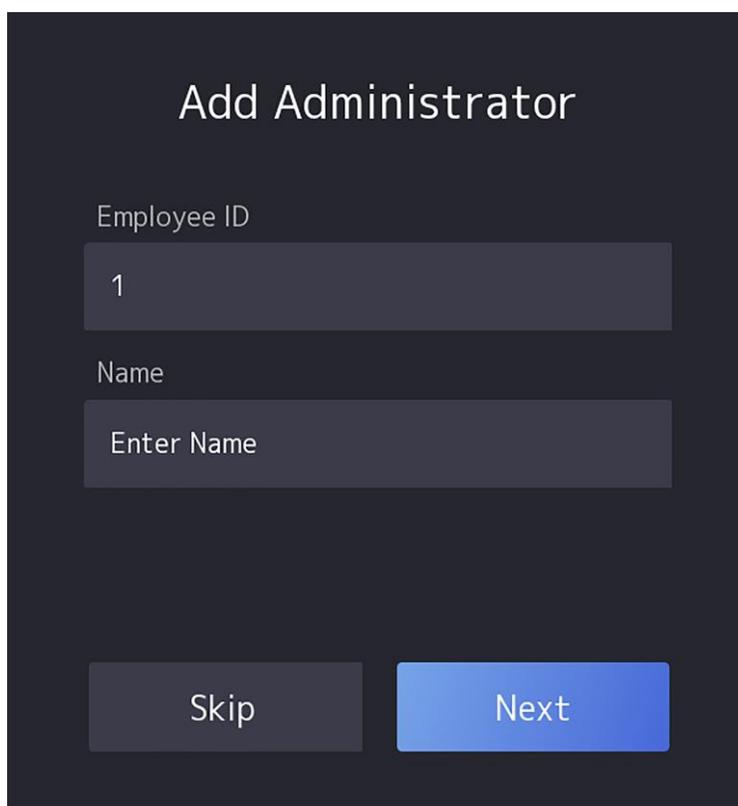


Figura 6-4 Adicionar página do administrador

3. 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. Clique  para capturar e clique  para confirmar.
-  : Pressione o dedo de acordo com as instruções na tela do dispositivo. Clique  para confirmar.
-  : Digite o cartão No. ou apresentar cartão na área de apresentação do cartão. Clique em **OK**.

 **Nota**

Apenas os dispositivos ligados ao módulo de impressão digital externo suportam a função de impressão digital .

4. Clique em **OK**.

Você entrará na página de autenticação.

Descrição do ícone de

status  / 

O dispositivo está armado / não armado.

 / 

DS-K1T673 Série Rosto Reconhecimento Terminal

O Hik-Connect está ativado/desativado.



A rede com fio do dispositivo está conectada/não conectada/falha na conexão.



O Wi-Fi do dispositivo está ativado e conectado/não conectado /habilitado, mas não conectado.

Descrição das teclas de atalho



Nota

Você pode configurar as teclas de atalho exibidas na tela. Para obter detalhes, consulte [SeFngs básicos](#).



- Digite a sala do dispositivo No. e toque em **OK** para ligar.
- Toque para ligar para a central.



Nota

O dispositivo deve ser adicionado ao centro ou a operação de chamada falhará



Digite a senha para autenticar.

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. Toque longamente na página inicial por 3 s e deslize para a esquerda / direita seguindo o gesto para entrar na página de login do administrador.

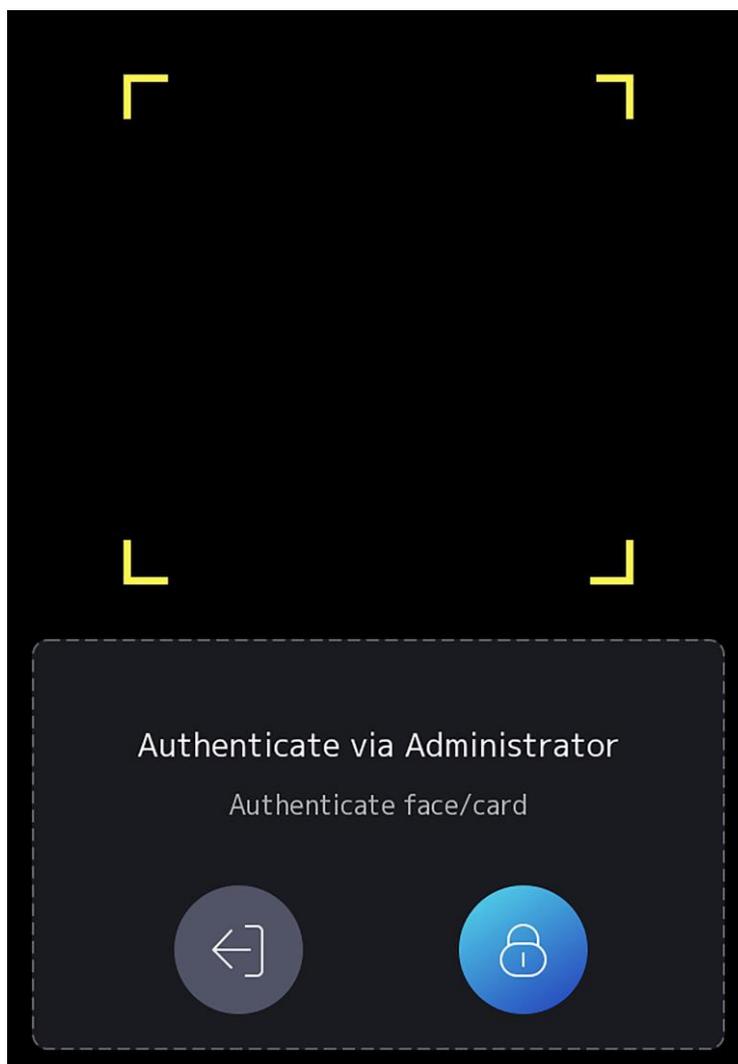


Figura 7-1 Login do administrador

2. Autentique o rosto, a impressão digital ou o cartão do administrador para entrar na página inicial.

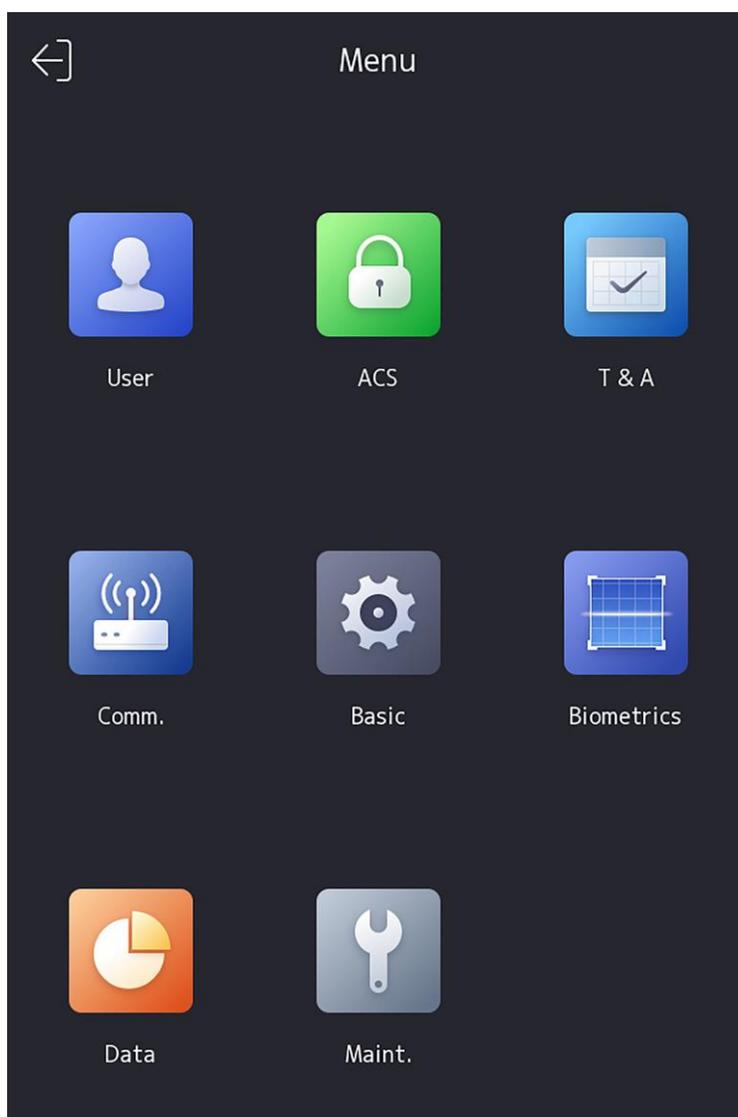


Figura 7-2 Página inicial

 **Nota**

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

3. Opcional: toque  e você pode inserir a senha de ativação do dispositivo para login.

4. Opcional: toque  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.

DS-K1T673 Série Rosto Reconhecimento Terminal

Passos

1. Toque longamente na página inicial por 3 s e deslize para a esquerda / direita seguindo o gesto para digitar a senha de entrada da página.
2. Digite a senha.
 - Se você adicionou um administrador para o dispositivo, toque  e digite a senha.
 - Se você não adicionou um administrador para o dispositivo, digite a senha.
3. Torneira OKEY Para entrar o Casa página.

Nota

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

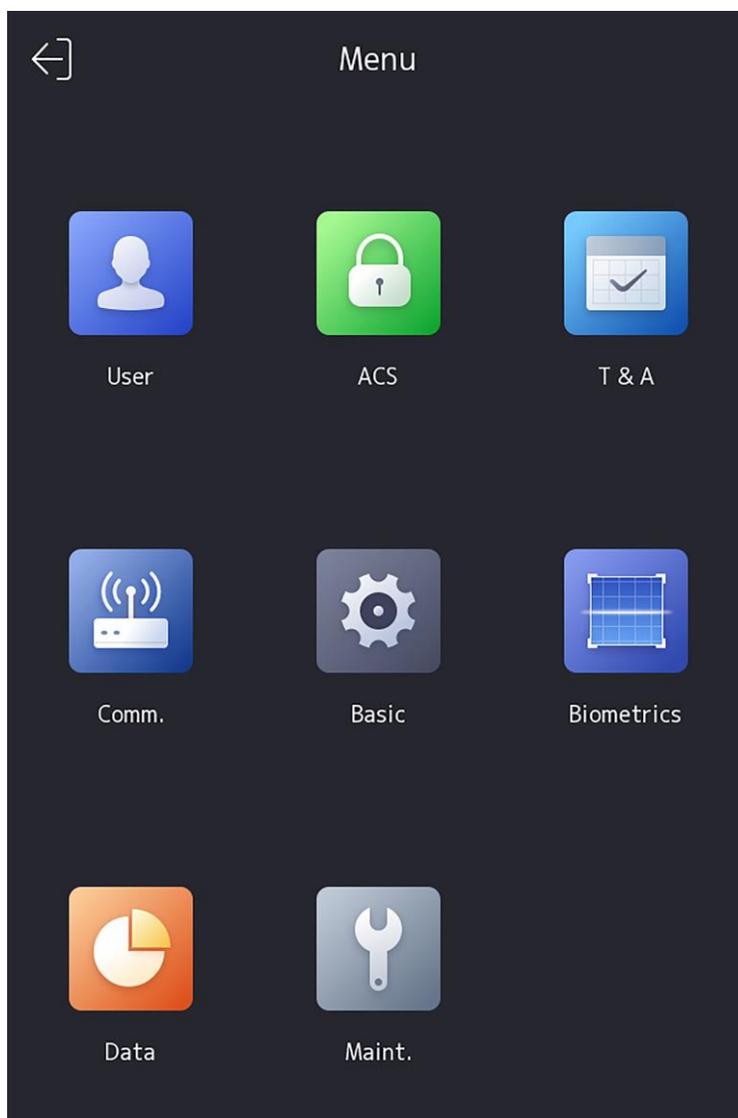


Figura 7-3 Página inicial

7.2 Configurações de comunicação

Você pode definir a rede com fio, o parâmetro Wi-Fi, os parâmetros RS-485, os parâmetros Wiegand, 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 IPv4/IPv6, a máscara de sub-rede, o gateway e os parâmetros DNS.

Passos

1. Toque em **Comm.** (Configurações de Comunicação) na página inicial para entrar na página Configurações de Comunicação.
2. Na página Configurações de Comunicação, toque em **Rede com Fio**.

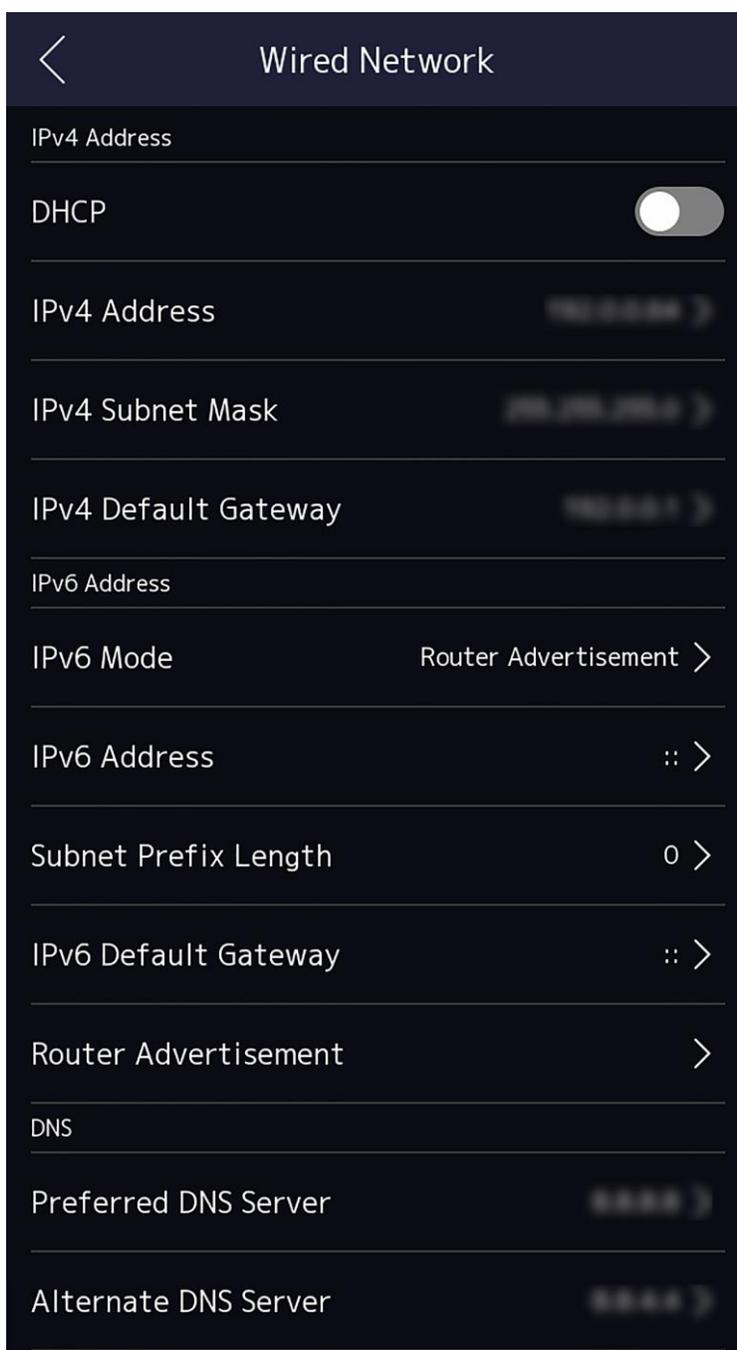


Figura 7-4 Configurações de rede com fio

- 3.** Defina Endereço IP IPv4/IPv6 , 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. Toque em **Comm.** (Configurações de Comunicação) na página inicial para entrar na página Configurações de Comunicação.
2. Na página Configurações de Comunicação, toque.

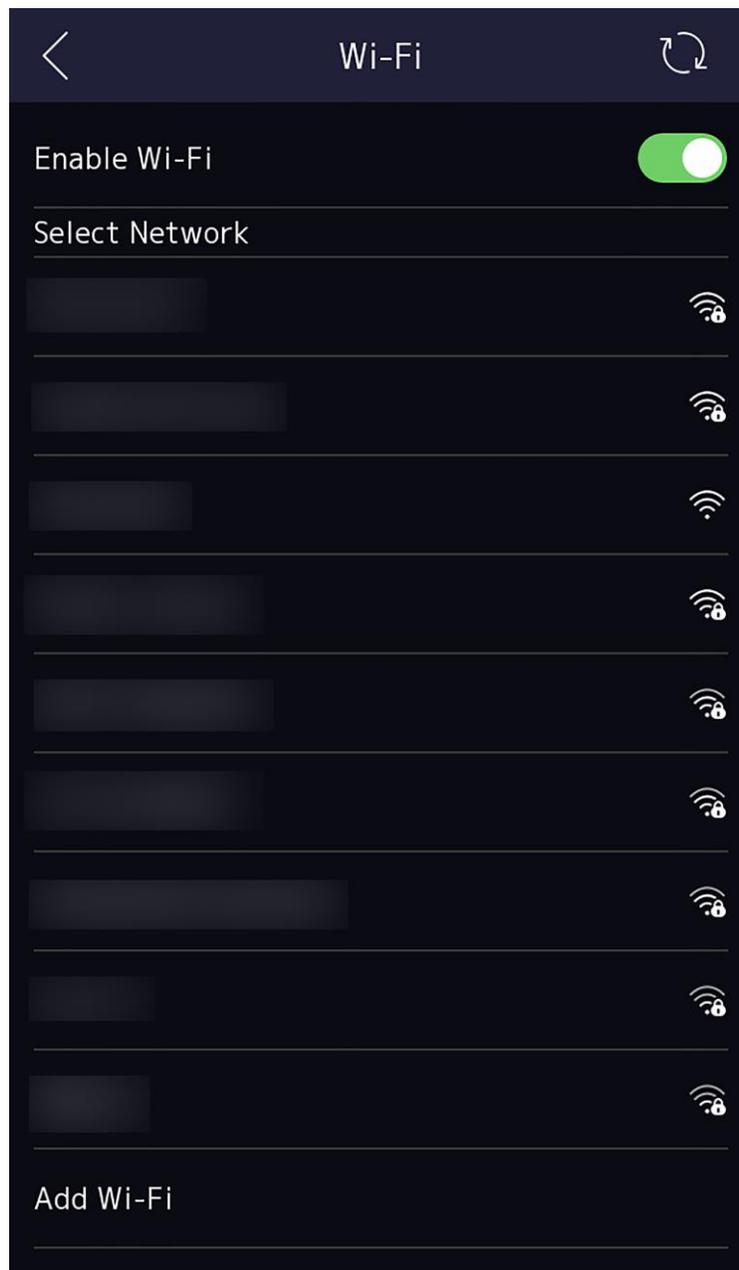


Figura 7-5 Configurações de Wi-Fi

3. Ative a função Wi-Fi.
4. Configure os parâmetros de Wi-Fi.
 - Selecione um Wi-Fi na lista e insira a senha do Wi-Fi. Toque em **OK**.
 - Se o Wi-Fi de destino não estiver na lista, toque em **Adicionar Wi-Fi**. Digite o nome e a senha do Wi-Fi. E toque em **OK**.



Nota

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

- 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.
- Toque em **OK** para salvar as configurações e volte para a guia Wi-Fi.
- Toque para salvar os parâmetros de rede.

7.2.3 Definir parâmetros RS-485

O terminal de reconhecimento facial pode conectar o controlador de acesso externo, a unidade de controle de porta segura ou o leitor de cartão através do terminal RS-485.

Passos

- Toque em **Comm.** (Configurações de Comunicação) na página inicial para entrar na página Configurações de Comunicação.
- Na página Configurações de Comunicação, toque em RS-485 para entrar na guia RS-485.

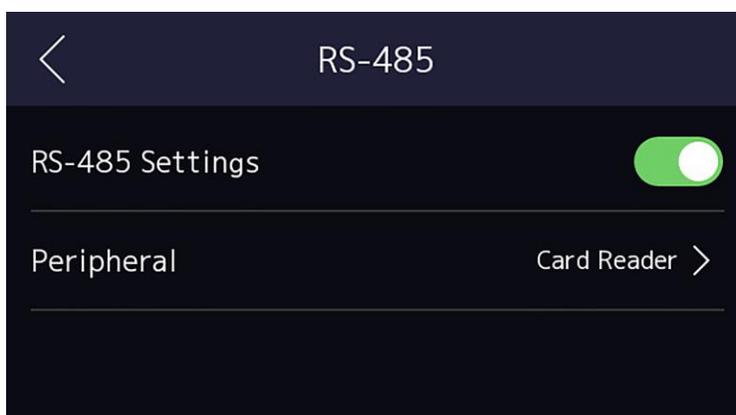


Figura 7-6 Definir parâmetros RS-485

- Selecionar ano periférico tipo Segundo Para teu real necessidades.



Nota

Se você selecionar **Controlador de acesso**: Se conectar o dispositivo a um terminal através da interface RS-485, defina o endereço RS-485 como 2. Se você conectar o dispositivo a um controlador, defina o endereço RS-485 de acordo com o número da porta.

- Toque no ícone de voltar no canto superior esquerdo e você deve reiniciar o dispositivo se você alterar os parâmetros.

7.2.4 Definir parâmetros Wiegand

Você pode definir a direção de transmissão Wiegand.

Passos

1. Toque em **Comm.** (Configurações de Comunicação) na página inicial para entrar na página Configurações de Comunicação.
2. Na página Configurações de Comunicação, toque em Wiegand para entrar na guia Wiegand.

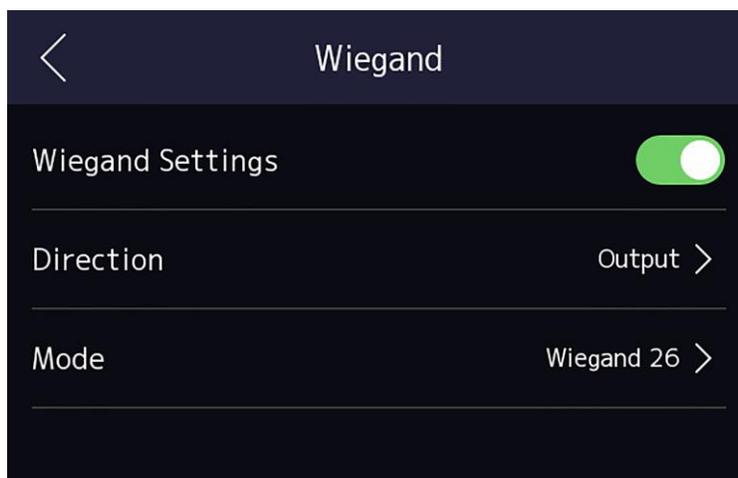


Figura 7-7 Configurações de Wiegand

3. Ative a função Wiegand.
4. Selecione uma direção de transmissão.
 - Saída: Um terminal de reconhecimento facial pode conectar um controlador de acesso externo. E os dois dispositivos transmitirão o cartão nº. via Wiegand 26 ou Wiegand 34.
 - Entrada: Um terminal de reconhecimento facial pode conectar um leitor de cartão Wiegand .
5. Torneira Para salvar o rede Parâmetros.



Nota

Se você alterar o dispositivo externo e depois de salvar os parâmetros do dispositivo , o dispositivo será reiniciado automaticamente.

7.2.5 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. Toque em **Comm. ISUP** → .

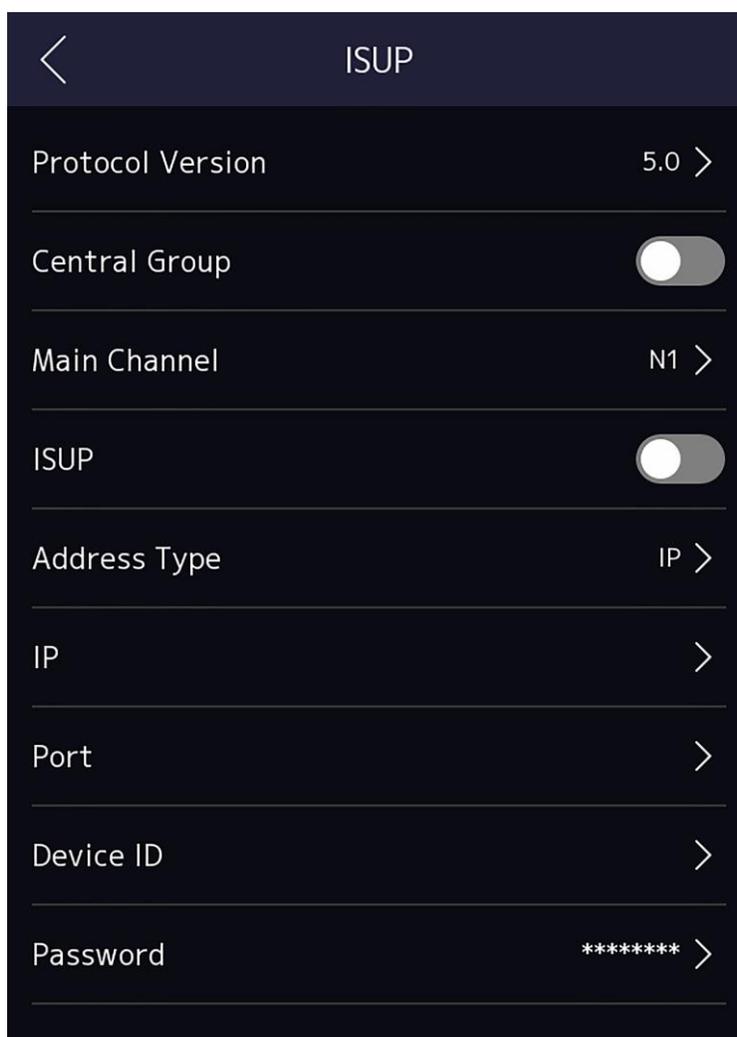


Figura 7-8 Configurações de ISUP

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

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

Tipo de Endereço

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

DS-K1T673 Série Rosto Reconhecimento Terminal

Endereço IP

Defina o endereço IP do servidor ISUP.

Nº da porta

Defina a porta nº do servidor ISUP.



Nota

Nº da porta Intervalo: 0 a 65535.

ID do dispositivo

Defina o número de série do dispositivo.

Senha

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 32 caracteres.
-

7.2.6 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. Toque em **Comm.** (Configurações de Comunicação) na página inicial para entrar na página Configurações de Comunicação.
2. Na página Configurações de Comunicação, toque em **Acesso ao Hik-Connect.**
3. Ativar o **acesso ao 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. Toque em **Usuário** → + para entrar na página Adicionar Usuário.

Add User	
Employee ID	2 >
Name	Not Configured >
Face	Not Configured >
Card	0/5 >
PIN	Not Configured
Auth. Settings	Device Mode >
User Role	Normal User >

3. Edite o ID do funcionário.

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. Toque no campo Nome e insira o nome de usuário no teclado virtual.

Nota

- Números, letras maiúsculas, letras minúsculas e caracteres especiais são permitidos no nome de usuário.
- Até 32 caracteres são permitidos no nome de usuário.

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

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 administrador.

Nota

Para obter detalhes sobre como definir o tipo de autenticação, consulte [Definir modo de autenticação](#) .

7. Habilite a função Permissão de administrador.

Habilitar Permissão de 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.

8. Toque 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

1. Toque longamente na página inicial por 3 s e deslize para a esquerda/direita seguindo o gesto e registrando o back-end.
2. Toque em **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. Toque no campo Nome e insira o nome de usuário no teclado virtual.

DS-K1T673 Série Rosto Reconhecimento Terminal

Nota

- Números, letras maiúsculas, letras minúsculas e caracteres especiais são permitidos no nome de usuário.
- O nome de usuário sugerido deve estar dentro de 32 caracteres.

5. Toque no campo Imagem de rosto para entrar na página de adição de imagem de rosto.

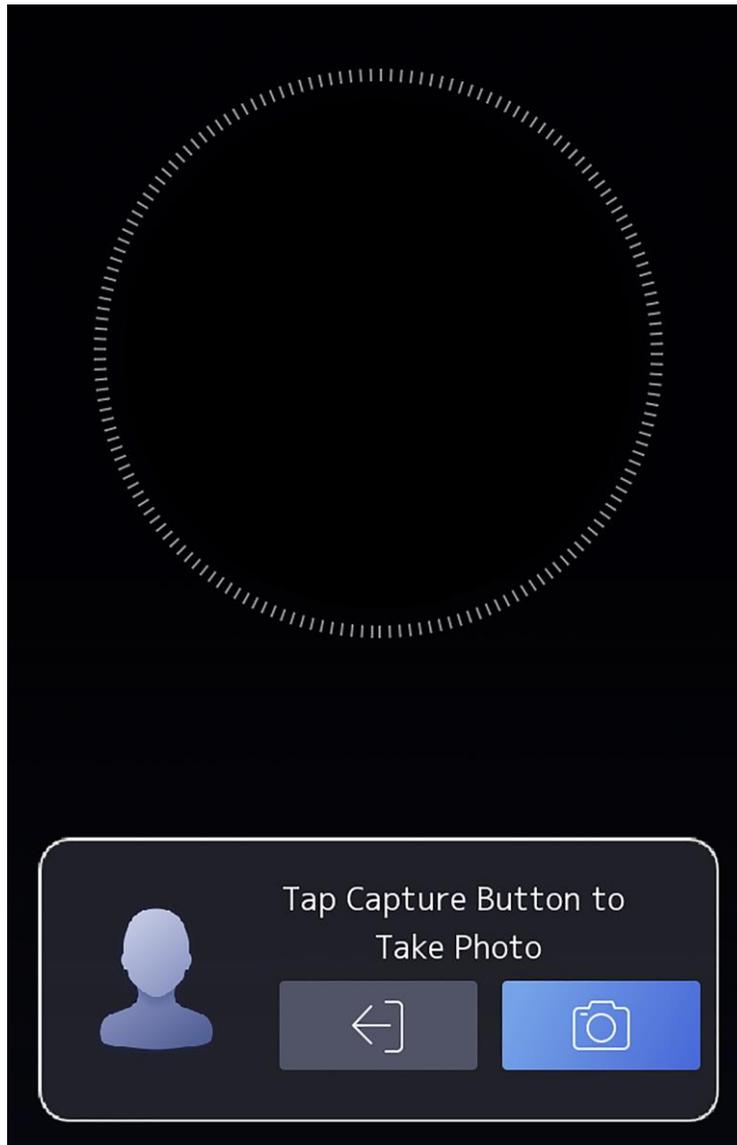


Figura 7-9 Adicionar imagem de rosto

6. Olhe para a 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 de rosto capturada será exibida no canto superior direito da página.

7. Toque em **Salvar** para salvar a imagem do rosto.

8. **Opcional:** toque em **Tentar** novamente e ajuste 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. Toque  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

- Dispositivos com módulo de impressão digital suportam a função de impressão digital.
 - Até 10.000 impressões digitais podem ser adicionadas.
-

1. Toque longamente na página inicial por 3 s e deslize para a esquerda / direita seguindo o gesto e insira o back-end do dispositivo.

2. Toque em **Usuário** → **+** para entrar na página Adicionar Usuário.

3. Torneira 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. Toque no campo Nome e insira o nome de usuário no teclado virtual.

Nota

- Números, letras maiúsculas, letras minúsculas e caracteres especiais são permitidos no nome de usuário.
 - O nome de usuário sugerido deve estar dentro de 32 caracteres.
-

5. Toque no campo Impressão digital para entrar na página Adicionar 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. Toque  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

1. Toque longamente na página inicial por 3 s e deslize para a esquerda/direita seguindo o gesto e registrando o back-end.
 2. Toque em **Usuário** → + para entrar na página Adicionar Usuário.
 3. Conecte um leitor de cartão externo de acordo com o diagrama de fiação.
 4. Torneira 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.
-

5. Toque no campo Nome e insira o nome de usuário no teclado virtual.

Nota

- Números, letras maiúsculas, letras minúsculas e caracteres especiais são permitidos no nome de usuário.
 - O nome de usuário sugerido deve estar dentro de 32 caracteres.
-

6. Toque no campo Cartão e toque em +.

7. Configure o cartão No.

- Digite o cartão No. manualmente.
 - Apresente o cartão sobre a área de apresentação do cartão para obter o número do cartão.
-

Nota

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

8. Configure o tipo de cartão.

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. Toque  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. Toque longamente na página inicial por 3 s e deslize para a esquerda/direita seguindo o gesto e registrando o back-end.
 2. Toque em **Usuário** → + para entrar na página Adicionar Usuário.
 3. Torneira 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. Toque no campo Nome e insira o nome de usuário no teclado virtual.



Nota

- Números, letras maiúsculas, letras minúsculas e caracteres especiais são permitidos no nome de usuário.
 - O nome de usuário sugerido deve estar dentro de 32 caracteres.
-

5. Toque no código PIN para ver 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. Toque  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. Toque longamente na página inicial por 3 s e deslize para a esquerda/direita seguindo o gesto e registrando o back-end.
2. Toque em **Usuário → Adicionar Usuário/Editar Usuário → Modo de Autenticação**.
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. Toque  para salvar as configurações.

7.3.7 Pesquisar e editar usuário

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

Usuário de pesquisa

Na página Gerenciamento de Usuários, toque na área de pesquisa para entrar na página Pesquisar Usuário. Toque em **Cartão** à esquerda da página e selecione um tipo de pesquisa na lista suspensa. Insira o ID do funcionário, o número do cartão ou o nome de usuário para pesquisa. Toque  para pesquisar.

Editar usuário

Na página Gerenciamento de Usuários, selecione um usuário na lista de usuários para entrar na página Editar Usuário. Siga as etapas em **Gerenciamento de usuários** para editar os parâmetros do usuário. Toque  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, toque em 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. Entrar o Criado senha quando você Exportados o dados. Se você fazer não criar a senha ao exportar os dados, deixe um espaço em branco na caixa de entrada e toque em **OKEY**



Nota

imediatamente.

- 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.

DS-K1T673 Série Rosto Reconhecimento Terminal

- As imagens importadas devem ser salvas na pasta (chamada enroll_pic) do diretório raiz e o nome da imagem deve ser seguido a regra serbaixa:
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 deve começar 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. A resolução deve ser de 640 × 480 pixels ou mais de 640 × 480 pixels. O tamanho da imagem deve estar entre 60 KB e 200 KB.
-

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 o rosto, a impressão digital, o cartão ou o código QR.

DS-K1T673 Série Rosto Reconhecimento Terminal

Rosto

DS-K1T673 Série Rosto Reconhecimento Terminal

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 impressão digital.

Cartão

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



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

Código QR

Coloque o código QR na frente da câmera do dispositivo para autenticar via código QR.



A autenticação via código QR deve ser suportada pelo dispositivo.

Senha

Digite a senha para autenticar via senha.

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.



- O cartão pode ser um cartão IC normal ou um cartão criptografado.
- Se a função de digitalização de código QR estiver ativada, você pode colocar o código QR na frente da câmera do dispositivo para autenticar via código QR.

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



- 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 tecla de atalho, o tema, as configurações de voz, as configurações de tempo, o(s) de sono (s), o número da comunidade, o número do edifício, o número da unidade e a beleza.

Toque longamente na página inicial por 3 s e deslize para a esquerda / direita seguindo o gesto e faça login na página inicial do dispositivo. Toque em **Básico**.

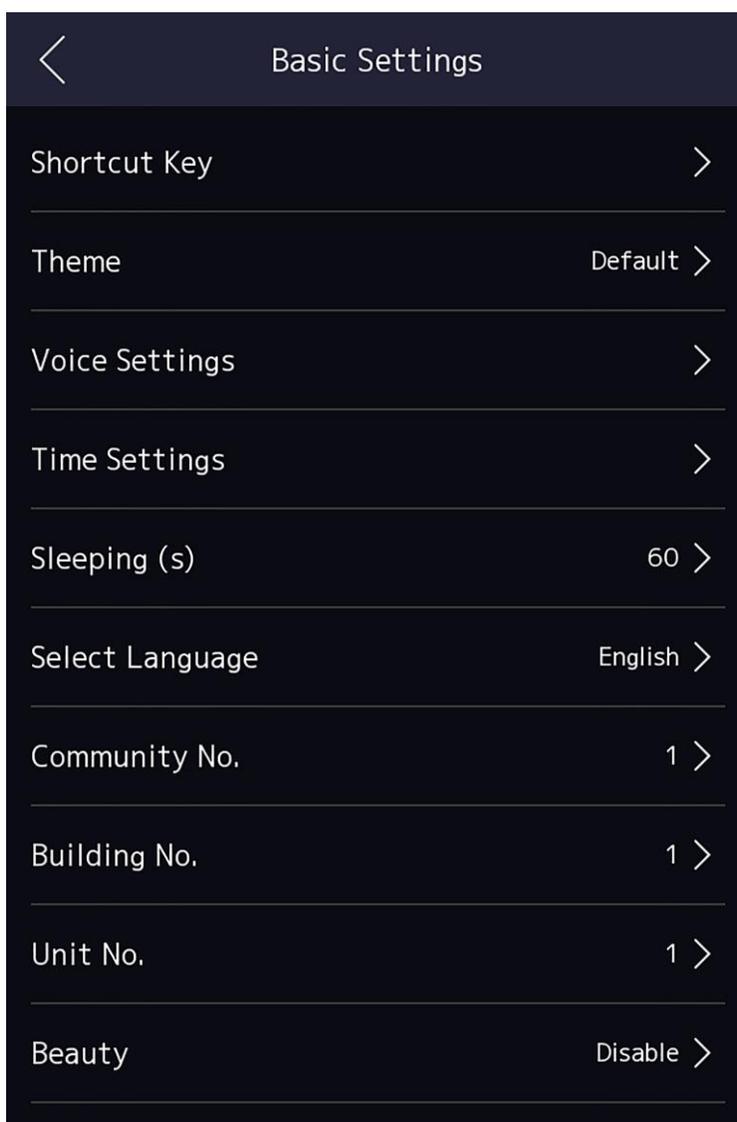


Figura 7-10 Página de configurações básicas

Tecla de atalho

Escolha a tecla de atalho exibida na página de autenticação, incluindo a função de código QR, a função de chamada, o tipo de chamada e a função de digitação de senha.

Nota

- Somente os dispositivos conectados ao módulo de código QR suportam a função de código QR.
- Você pode selecionar o tipo de chamada em Sala de Chamada, **Call Center**, Nº da Sala Especificada de **Chamada** e **Chamar APP. Sala de Chamada**.
Ao tocar no botão de chamada na página de autenticação, você deve discar um número de sala para ligar.

Central de atendimento

Ao tocar no botão de chamada na página de autenticação, você pode ligar diretamente para o centro.

Chamada Especificado Nº da Sala.

Você deve definir um quarto Não. Ao tocar no botão de chamada na página de autenticação, você pode chamar a sala configurada diretamente sem discar.

Ligue para o APP

Ao tocar no botão de chamada na página de autenticação, você ligará para o cliente móvel onde o dispositivo é adicionado.

Tema

Você pode definir o tema da janela de prompt na página de autenticação. Você pode selecionar **Tema** como **Padrão/Simples**. Se selecionar **Simples**, a visualização ao vivo da página de autenticação será desativada e, enquanto isso, o nome da pessoa, a ID do funcionário e as fotos do rosto ficarão ocultos.

Configurações de voz

Você pode ativar / desativar a função de prompt de voz e ajustar o volume de voz.

Nota

Você pode definir o volume de voz entre 0 e 10.

Configurações de Hora

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

Dormindo (s)

Defina o tempo de espera de suspensão do dispositivo (minuto). Quando você estiver na página inicial e se você definir o tempo de sono para 30 minutos, o dispositivo irá dormir após 30 minutos sem qualquer operação.

Nota

Se você definir o tempo de suspensão como 0, o dispositivo não entrará no modo de suspensão.

Selecione o idioma

Selecione o idioma de acordo com as necessidades reais.

Nº da Comunidade

DS-K1T673 Série Rosto Reconhecimento Terminal

Defina a comunidade instalada do dispositivo No.
Edifício nº.

DS-K1T673 Série Rosto Reconhecimento Terminal

Defina o dispositivo instalado edifício No.

Unidade nº.

Defina o dispositivo instalado unit No.

Beleza

Você pode ativar a função de beleza e definir o parâmetro liso e branqueador. Toque em + ou - para controlar a força do efeito.



Nota

Por padrão, a função está desabilitada.

7.7 Definir parâmetros biométricos

Você pode personalizar os parâmetros faciais para melhorar o desempenho do reconhecimento facial. Os parâmetros configuráveis incluem modo de aplicação, nível de vivacidade facial, distância de reconhecimento facial, intervalo de reconhecimento facial, ampla dinâmica, nível de segurança face 1:N, nível de segurança face 1 :1, configurações ECO, detecção facial com máscara e autenticação de múltiplas faces.

Toque longamente na página inicial por 3 s e faça o login na página inicial. Toque em **Biometria**.

Tabela 7-1 Parâmetros da imagem facial

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.
Ampla dinâmica	Sugere-se ativar a função WDR se instalar o dispositivo ao ar livre. Quando há áreas muito claras e muito escuras simultaneamente na exibição, você pode ativar a função WDR para equilibrar o brilho de toda a imagem e fornecer imagens claras com detalhes.

DS-K1T673 Série Rosto Reconhecimento Terminal

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 maior a taxa de falsa rejeição.
Configurações ECO	<p>Depois de ativar o modo ECO, o dispositivo usará a câmera IR para autenticar rostos no ambiente com pouca luz ou escuridão. E você pode definir o limite do modo ECO, o modo ECO (1:N) e o modo ECO mode (1:1).</p> <p>Limiar ECO</p> <p>Ao ativar o modo ECO, você pode definir o limite do modo ECO. Quanto maior o valor, mais fácil o dispositivo entra no modo ECO.</p> <p>Modo ECO (1:1)</p> <p>Defina o limite de correspondência ao autenticar através do modo de correspondência do modo ECO 1:1. Quanto maior o valor, menor a taxa de aceitação falsa e maior a taxa de falsa rejeição.</p> <p>Modo ECO (1:N)</p> <p>Defina o limite de correspondência ao autenticar através do modo de correspondência ECO 1:N. Quanto maior o valor, menor a taxa de aceitação falsa e maior a taxa de rejeição falsa</p>
Detecção de Rosto com Máscara	<p>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: N nível e a estratégia.</p> <p>Lembrete de Uso</p> <p>Se a pessoa não usar uma máscara facial ao autenticar, o device solicitará uma notificação e a porta será aberta.</p> <p>Deve usar</p> <p>Se a pessoa não usar uma máscara facial ao autenticar, o dispositivo solicitará uma notificação e a porta será fechada.</p>
Autenticação de várias faces	Depois que a autenticação de várias faces estiver habilitada, a autenticação de várias faces será suportada.

7.8 Definir parâmetros de controle de acesso

Você pode definir as permissões de controle de acesso, incluindo as funções do modo de autenticação, ativar o cartão NFC, ativar o cartão M1, o contato da porta, a duração (s) aberta (s) e o intervalo (s) de autenticação (s).

Na página inicial, toque em **ACS** (Configurações de Controle de Acesso) para entrar na página Configurações de Controle de Acesso . Edite os parâmetros de controle de acesso nesta página.

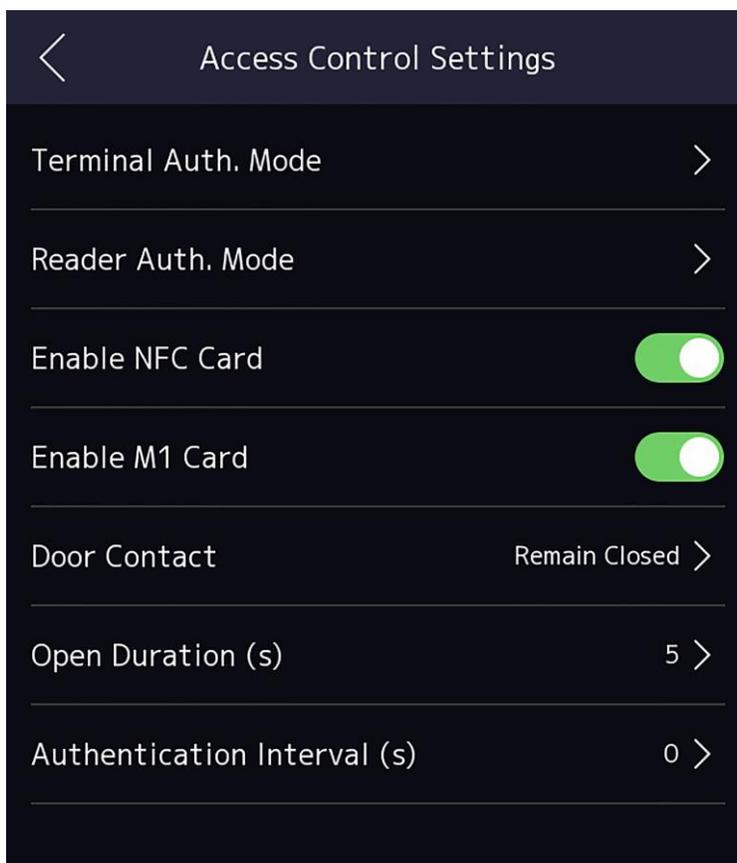


Figura 7-12 Parâmetros de controle de acesso

As descrições dos parâmetros disponíveis são as seguintes:

Tabela 7-2 Descrições de parâmetros de controle de acesso

Parâmetro	Descrição
Autenticação terminal. Modo (Modo de Autenticação de Terminal)	Selecione o modo de autenticação do terminal de reconhecimento facial. Você também pode personalizar o modo de autenticação.

DS-K1T673 Série Rosto Reconhecimento Terminal

Parâmetro	Descrição
	 Nota <ul style="list-style-type: none">• 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 anti-falsificação. 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.
Modo de Autenticação do Leitor (Modo de Autenticação do Leitor de Cartão)	Selecione o modo de autenticação do leitor de cartão.
Ativar cartão NFC	Ative a função e você pode apresentar o cartão NFC para autenticar.
Ativar cartão M1	Habilite a função e você pode apresentar o cartão M1 para autenticar.
Contato da Porta	Você pode selecionar "Permanecer Aberto" ou "Remian Fechado" de acordo com suas necessidades reais. Por padrão, é Remian Closed.
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.

DS-K1T673 Série Rosto Reconhecimento Terminal

Toque em Status **de T&A** para entrar na página **Status** de T& A.

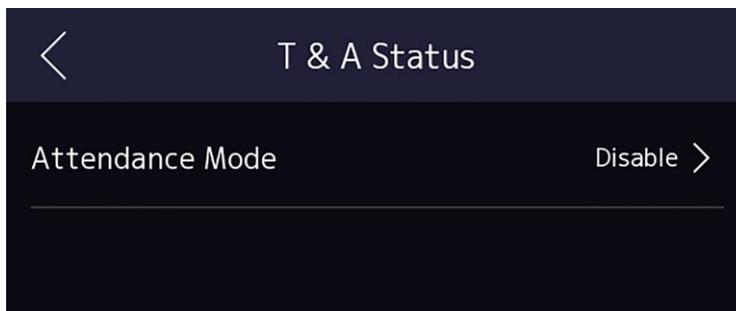


Figura 7-13 Desabilitar o modo de presença

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

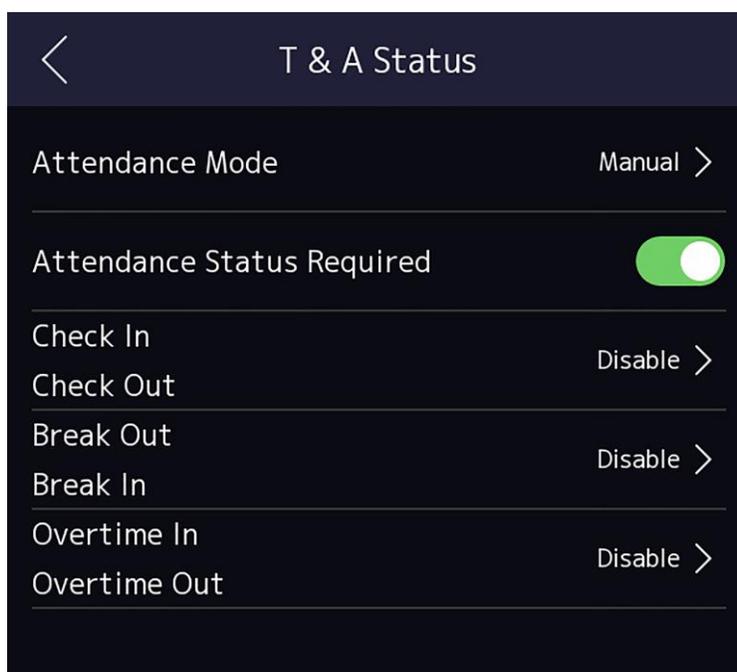


Figura 7-14 Modo de atendimento manual

3. Habilite o **status de presença necessário**.

4. Habilite o 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*.

DS-K1T673 Série Rosto Reconhecimento Terminal

Passos

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

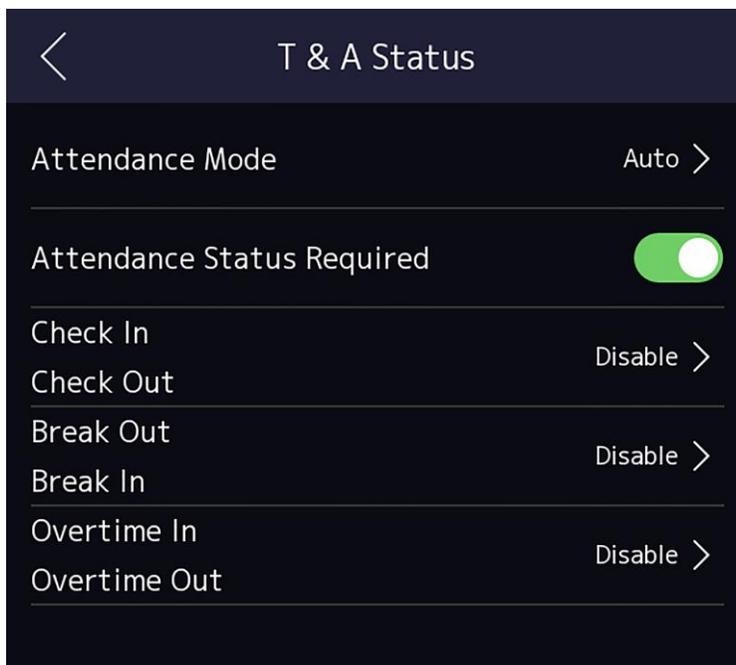


Figura 7-15 Modo de atendimento automático

3. Habilite a função **Status de Presença**.
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) Toque em **Agenda 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) Toque em **Confirmar**.
 - 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 a agenda configurada.

DS-K1T673 Série Rosto Reconhecimento Terminal

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

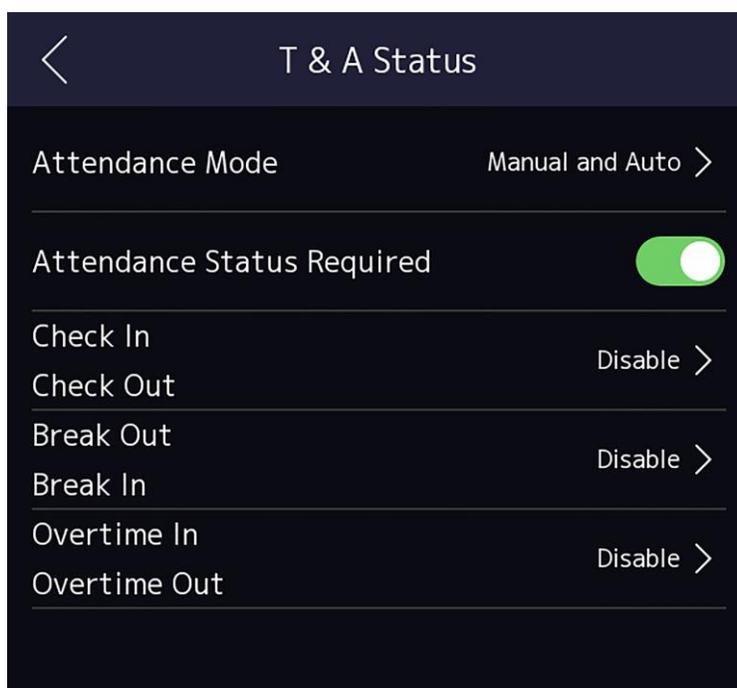


Figura 7-16 Modo manual e automático

3. Habilite a função **Status de Presença**.
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.

DS-K1T673 Série Rosto Reconhecimento Terminal

6. Defina a agenda do status.

- 1) Toque em **Agenda 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) Toque em **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 edit 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.

7.10 Manutenção do Sistema

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

Toque longamente na página inicial por 3 s e deslize para a esquerda / direita seguindo o gesto e faça login na página inicial. Toque em **Maint.**

Segure o ? no canto superior direito da página e digite a senha para visualizar a versão do dispositivo.

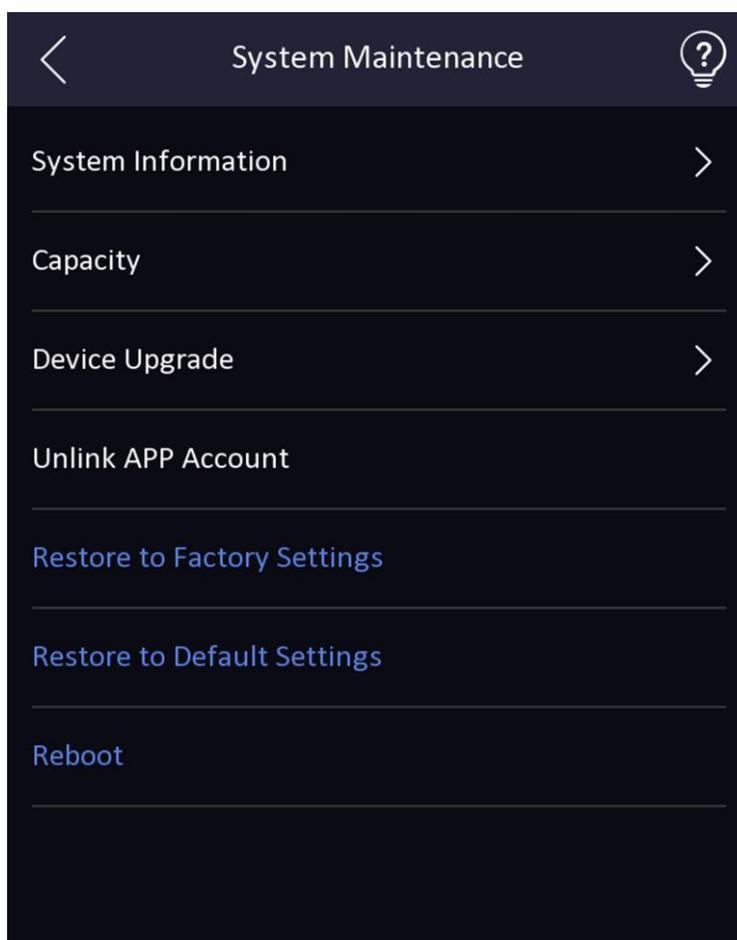


Figura 7-17 Página de manutenção

Informações do Sistema

Você pode visualizar o modelo do dispositivo, o número de série, as versões, o endereço, os dados de produção, o código QR e a licença do 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, usuário, imagem do rosto, cartão, evento e impressão digital.

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

DS-K1T673 Série Rosto Reconhecimento Terminal

Conecte a unidade flash USB na interface USB do dispositivo. Toque em **Atualizar** e o dispositivo lerá o *digicap.dav* na unidade flash USB para iniciar a atualização.

Desvincular conta APP

Depois de desvincular a conta APP, você não pode operar via APP.

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.

Restaurar para as configurações de fábrica

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

Reinicializar

Reinicie o dispositivo.

7.11 Vídeo Intercomunicador

Depois de adicionar o dispositivo ao software cliente, você pode chamar o dispositivo do software cliente, chamar a estação principal do dispositivo, chamar o software cliente do dispositivo, chamar a estação interna do dispositivo ou chamar a sala específica do device.

7.11.1 Chamar software cliente do dispositivo

Passos

1. Obtenha o software cliente do disco fornecido ou do site oficial e instale o software de acordo com os prompts.
2. Execute o software cliente e o painel de controle do software aparece.
3. Clique em Gerenciamento de Dispositivos para entrar na interface Gerenciamento de Dispositivos.
4. Adicionar o dispositivo Para o cliente software.

Nota

Para obter detalhes sobre como adicionar dispositivo, consulte *Adicionar dispositivo*.

5. Chame o software cliente.
 - 1) Toque  na página inicial do dispositivo.
 - 2) Digite **0** na janela pop-up.
 - 3) Toque  para chamar o software cliente.
6. Toque em **Responder** na página pop-up do software cliente e você poderá iniciar o áudio bidirecional entre o dispositivo e o software cliente.

Nota

Se o dispositivo for adicionado a vários softwares cliente e quando o dispositivo estiver chamando o software cliente, somente o primeiro software cliente adicionado ao dispositivo

DS-K1T673 Série Rosto Reconhecimento Terminal

exibirá a janela de recebimento de chamadas.

7.11.2 Call Center a partir do dispositivo

Passos

1. Obtenha o software cliente do disco fornecido ou do site oficial e instale o software de acordo com os prompts.
2. Execute o software cliente e o painel de controle do software aparece.
3. Clique em Gerenciamento **de** Dispositivos para entrar na interface Gerenciamento de Dispositivos.
4. Adicionar o principal estação e o dispositivo Para o cliente software.



Nota

Para obter detalhes sobre como adicionar dispositivo , consulte *Adicionar dispositivo*.

5. Pôr o principal estação IP endereço e GOLE endereço em o remoto configuração página.



Nota

Para obter detalhes sobre a operação, consulte o manual do usuário da estação principal.

6. Ligue para o centro.
 - Se você configurou para call center no ***SeFngs Básico***, você pode tocar para ligar  para o centro.
 - Se você não configurou para call center no ***SeFngs Básico***, toque  **em** → para  ligar para o centro
7. Respostas o chamar via o principal estação e Começa bidirecional áudio.



Nota

O dispositivo chamará a estação principal em prioridade.

7.11.3 Dispositivo de chamada a partir do software cliente

Passos

1. Obtenha o software cliente do disco fornecido ou do site oficial e instale o software de acordo com os prompts.
2. Execute o software cliente e o painel de controle do software aparece.
3. Clique em Gerenciamento **de** Dispositivos para entrar na página Gerenciamento de **Dispositivos**.
4. Adicionar o dispositivo Para o cliente software.



Nota

Para obter detalhes sobre como adicionar dispositivo , consulte *Adicionar dispositivo*.

5. Entrar o **Viver Vista** página e clique duas vezes o Adicionado dispositivo Para começar viver vista.



Nota

Para obter detalhes sobre as operações na página **Live View** , consulte *Live View* no manual do usuário do software cliente.

6. Clique com o botão direito do mouse na imagem de visualização dinâmica para abrir o menu do botão direito do mouse .

DS-K1T673 Série Rosto Reconhecimento Terminal

7. Clique em **Iniciar áudio bidirecional** para iniciar o áudio bidirecional entre o dispositivo e o software cliente.

7.11.4 Sala de chamadas a partir do dispositivo

Passos

1. Obtenha o software cliente do disco fornecido ou do site oficial e instale o software de acordo com os prompts.
2. Execute o software cliente e o painel de controle do software aparece.
3. Clique em Gerenciamento **de** Dispositivos para entrar na interface Gerenciamento de Dispositivos.
4. Adicionar o Interior estação e o dispositivo Para o cliente software.



Nota

Para obter detalhes sobre como adicionar dispositivo , consulte *Adicionar dispositivo*.

5. Vincule um usuário a uma estação interna e defina um número de sala. para a estação interior.
6. Ligue para a sala.
 - Se você configurou uma sala especificada No. no **SeFngs Básico** , você pode tocar  para chamar a sala.
 - Se você não tiver configurado uma sala especificada Não. no **SeFngs Básico** , você deve  tocar  na página de autenticação do dispositivo. Digite o quarto No. na página de discagem e toque para ligar  para a sala.
7. Depois que a estação interna atender a chamada, você pode iniciar o áudio bidirecional com a estação interna.

7.11.5 Chamar cliente móvel do dispositivo

Passos

1. Obtenha o cliente móvel do disco fornecido ou do site oficial e instale o software de acordo com os prompts.
2. Correr o telemóvel cliente e adicionar o dispositivo Para o telemóvel cliente.



Nota

Para obter detalhes, consulte o manual do usuário do cliente móvel.

3. **Insira Configurações Básicas → Tecla de Atalho** e habilite **Chamar APP**.
4. Volte para a página inicial e ligue para o cliente móvel.
 - 1) Toque  na página inicial do dispositivo.
 - 2) Toque  para ligar  para o cliente móvel.

Capítulo 8 Operação via navegador da Web

8.1 Login

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



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.



Certifique-se de que o endereço IP comece com "Https:".

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.

8.2 Visualização ao vivo

Você pode ver o vídeo ao vivo do dispositivo.

Depois de fazer login, você entrará na página de visualização ao vivo. Você pode executar a visualização ao vivo, captura, gravação de vídeo e outras operações.

DS-K1T673 Série Rosto Reconhecimento Terminal

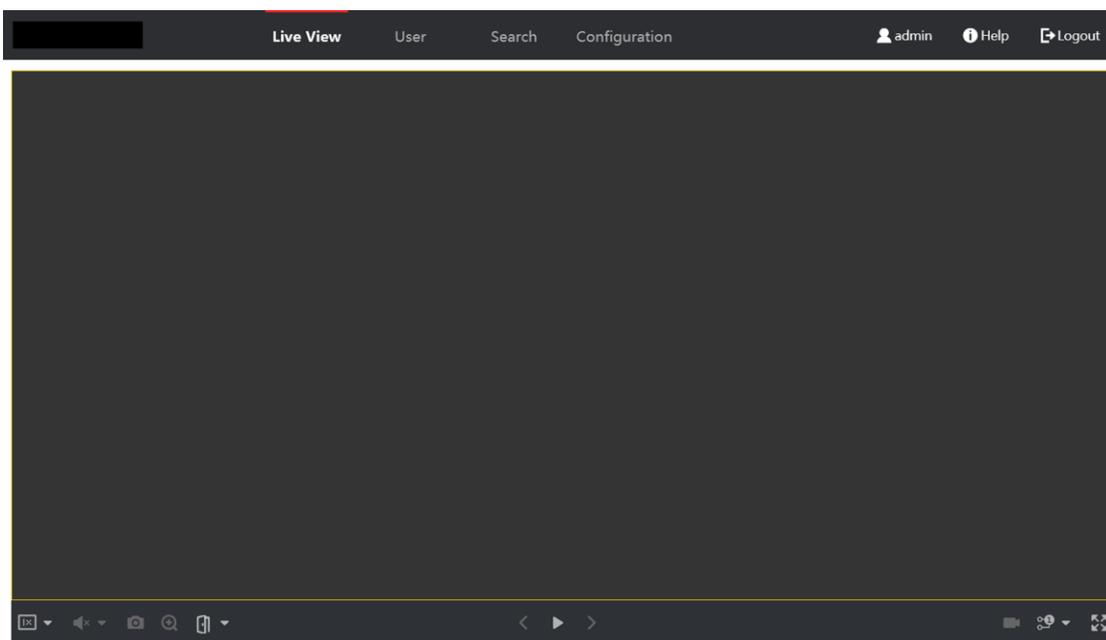


Figura 8-1 Página de visualização dinâmica

Descrições da função:



Selecione o tamanho da imagem ao iniciar a visualização ao vivo.



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. Função reservada. Você pode ampliar a



imagem da visualização ao vivo. Destrave a porta

ligada.



Iniciar ou parar a visualização dinâmica.



Inicie ou pare a gravação de vídeo.



DS-K1T673 Série Rosto Reconhecimento Terminal

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



Selecione o tipo de divisão de janela ao iniciar a



visualização dinâmica. Visualização em tela cheia.

8.3 Gestão de Pessoas

Clique e adicione as informações da pessoa, incluindo as informações básicas, o cartão, o modo de autenticação e o

Clique em **OK** para salvar a pessoa.

Adicionar informações básicas

Clique em **Usuário** → Adicionar para entrar na página Adicionar Pessoa.

Adicione as informações básicas da pessoa, incluindo a ID do funcionário, o nome da pessoa e a função de usuário.

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

Adicionar cartão

Clique em **Usuário** → Adicionar para entrar na página Adicionar Pessoa.

Clique em **Adicionar cartão**, insira o **número do cartão**, e selecione a **Propriedade** e clique em **OK** para adicionar o cartão. Clique em **Salvar** para salvar as configurações.

Adicionar imagem de rosto

Clique em **Usuário** → 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 JPEG e o tamanho deve ser inferior a 200K.

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

Adicionar modo de autenticação

Clique em **Usuário** → Adicionar para entrar na página Adicionar Pessoa. Defina o modo de autenticação.

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

8.4 Evento de Pesquisa

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

DS-K1T673 Série Rosto Reconhecimento Terminal

Event Types

Access Control Event

Employee ID

Name

Card No.

Start Time

2021-06-07 00:00:00

End Time

2021-06-07 23:59:59

Figura 8-2 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.

8.5 Configuração

8.5.1 Definir parâmetros locais

Defina os parâmetros de exibição dinâmica, registre o caminho de salvamento de arquivos e o caminho de salvamento de imagens capturadas.

Definir parâmetros de visualização dinâmica

Clique em **Configuração** → Local para entrar na página **Local**. Configure o tipo de fluxo, o desempenho de reprodução, a visualização ao vivo de início automático e o formato da imagem e clique em **Salvar**.

Definir caminho de salvamento de arquivo de registro

Clique em **Configuração** → Local para entrar na página **Local**. Selecione um tamanho de arquivo de registro e selecione um caminho de salvamento do computador local e clique em **Salvar**.

Você também pode clicar em **Abrir** para abrir a pasta de arquivos para exibir detalhes.

Definir o caminho de salvamento de imagens capturadas

Clique em **Configuração** → Local para entrar na página **Local**. Selecione um caminho de salvamento do computador local e clique em **Salvar**.

DS-K1T673 Série Rosto Reconhecimento Terminal

Você também pode clicar em **Abrir** para abrir a pasta de arquivos para exibir detalhes.

8.5.2 Exibir informações do dispositivo

Veja o nome do dispositivo, idioma, modelo, número de série, código QR, versão, número de canais, entrada de alarme, saída de alarme, bloqueio e RS-485, capacidade do dispositivo , etc.

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

Você pode ver o nome do dispositivo, idioma, modelo, número de série, código QR, versão, número de canais, entrada de alarme, saída de alarme, bloqueio e RS-485, capacidade do dispositivo , etc.

8.5.3 Definir Hora

Defina o fuso horário do dispositivo , o modo de sincronização e a hora do dispositivo. Clique em Configuração → Sistema → Configurações **do Sistema** → **Configurações de Tempo** .

Time Zone (GMT+08:00) Beijing, Urumqi, Singapore, Perth

Time Sync. NTP Manual

Server Address 2.com

NTP Port 7

Interval 7 minute(s)

Save

Figura 8-3 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

DS-K1T673 Série Rosto Reconhecimento Terminal

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.

8.5.4 Definir horário de verão

Passos

1. Clique em **Configuração** → **Sistema** → **Configurações do Sistema** → **horário de verão** .

Enable DST

Start Time Apr First Sun 02

End Time Oct Last Sun 02

DST Bias 30minute(s)

Save

Figura 8-4 Página do horário de verão

2. Marque **Ativar DST**.

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.

8.5.5 Exibir licença de software de código aberto

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

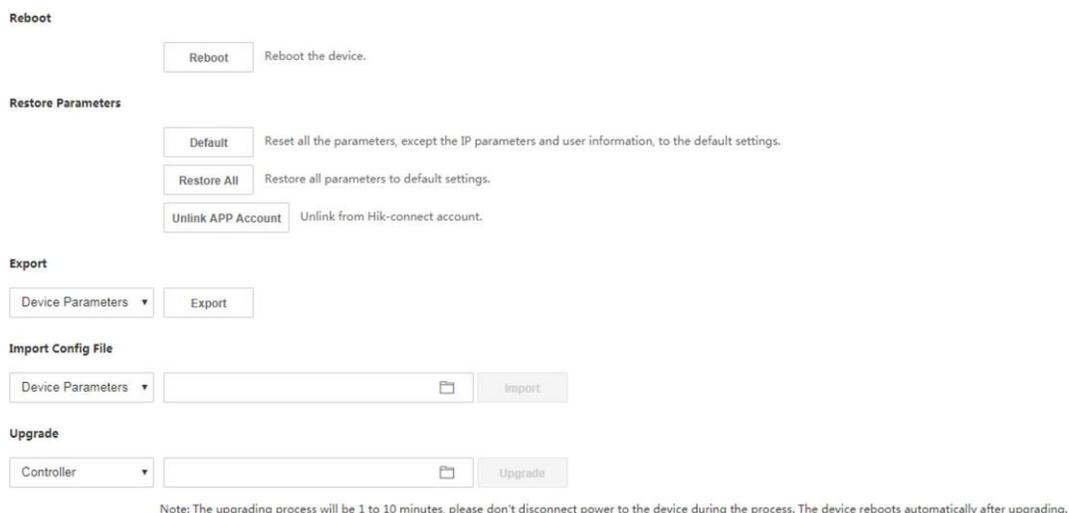
8.5.6 Atualização e manutenção

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

Dispositivo de reinicialização

Clique em **Configuração** → **Sistema** → **Manutenção** → **Atualização e Manutenção** .

DS-K1T673 Série Rosto Reconhecimento Terminal



Reboot

Reboot the device.

Restore Parameters

Reset all the parameters, except the IP parameters and user information, to the default settings.

Restore all parameters to default settings.

Unlink from Hik-connect account.

Export

Import Config File

Upgrade

Note: The upgrading process will be 1 to 10 minutes, please don't disconnect power to the device during the process. The device reboots automatically after upgrading.

Figura 8-5 Página de atualização e manutenção

Clique em **Reinicializar** para iniciar a reinicialização do dispositivo.

Restaurar parâmetros

Clique em **Configuração → Sistema → Manutenção → Atualização e Manutenção**.

Restaurar tudo

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

Inadimplência

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

Desvincular conta APP

Desvincule a conta Hik-Connect da plataforma.

Parâmetros de importação e exportação

Clique em **Configuração → Sistema → Manutenção → Atualização e Manutenção**.

Exportação

Clique em **Exportar** para exportar os logs ou 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.

Melhoramento

Clique em **Configuração** → **Sistema** → **Manutenção** → **Atualização e Manutenção** .
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.

Nota

Não desligue durante a atualização.

8.5.7 Consulta de log

Você pode pesquisar e visualizar os logs do dispositivo.

Vá para **Configuração** → **Consulta de Log de** → **de Manutenção** → **do Sistema** .

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.

8.5.8 Configurações do Modo de Segurança

Defina o modo de segurança para registrar no software cliente.

Na página Dispositivo para Gerenciamento, clique em **Configuração** → **Sistema** → **Segurança** → **Serviço de Segurança** .

Selecione um modo de segurança na lista suspensa 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.

Habilitar SSH

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

Habilitar HTTP

Para aumentar o nível de segurança de rede ao visitar sites, você pode habilitar o HTTP para adquirir um ambiente de comunicação de rede mais seguro e criptografado. A unificação de comunicação deve ser autenticada por identidade e senha de criptografia depois de habilitar o HTTP, que é salvar.

8.5.9 Gerenciamento de Certificados

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



A função só é suportada por determinados modelos de dispositivos.

Criar e instalar certificado autoassinado

Passos

1. Vá para **Configuração** → **Sistema** → **Segurança** → **Gerenciamento de Certificados**.
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 **Configuração** → **Sistema** → **Segurança** → **Gerenciamento de Certificados**.
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.

DS-K1T673 Série Rosto Reconhecimento Terminal

Passos

1. Vá para **Configuração → Sistema → Segurança → Gerenciamento de Certificados** .
 2. Criar ano ID em o **Inport 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**.

8.5.10 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 mês ou semanalmente pode proteger melhor o seu produto. A configuração adequada de todas as senhas e outras configurações de segurança é de responsabilidade do instalador e/ou usuário final.

8.5.11 Exibir informações de armar/desarmar o dispositivo

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

Vá para **Configuração → Gerenciamento de Usuários → Armand/Desarmand Informações** .

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

8.5.12 Configurações de rede

Defina TCP/IP, porta, parâmetros Wi-Fi, estratégia de relatório, acesso à plataforma e escuta HTTP.



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

Definir parâmetros básicos de rede

Clique em **Configuração** → **Configurações Básicas de Rede**

→ **TCP/IP**. Defina os parâmetros e clique em **Salvar** para salvar as configurações.

Processador DHCP

Se desmarcar a função, você deverá definir o endereço IPv4, a máscara de sub-rede IPv4, o gateway padrão IPv4, o modo IPv6, o endereço IPv6, o comprimento do prefixo da sub-rede IPv6, o gateway padrão IPv6, 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, o modo IPv6, o endereço IPv6, o comprimento do prefixo da sub-rede IPv6 e o padrão IPv6 gateway automaticamente.

Tipo de NIC

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

Servidor DNS

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

Definir parâmetros de porta

Defina os parâmetros de porta HTTP, RTSP, HTTPS e

Server. Clique em **Configuração** → **Portas de Rede**

→ **Básicas**.

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.

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.

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 Básicas** → **Wi-Fi**.

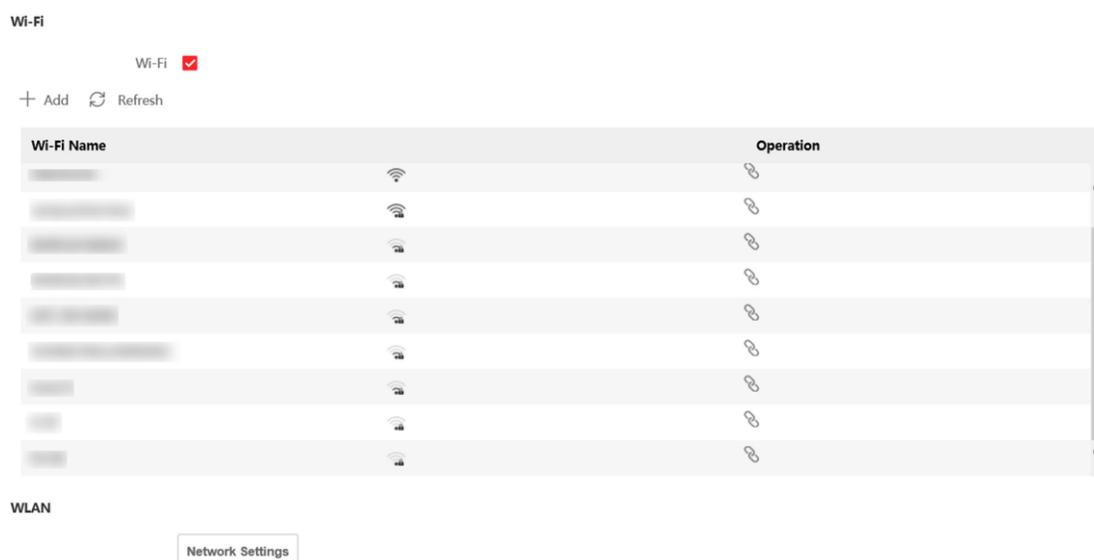


Figura 8-6 Página de configurações de Wi-Fi

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 SSID, o modo de trabalho e o tipo de criptografia. Clique em **Conectar**. Quando o Wi-Fi estiver conectado, clique em **OK**.

4. **Opcional:** Defina os parâmetros WLAN.

1) Clique em **Configurações de Rede**.

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

5. Clique em **OK**.

Configurações de estratégia de relatório

Você pode definir o grupo central para carregar o log por meio do protocolo ISUP. Vá para **Configuração** → **Rede** → **Configurações Básicas** → **Estratégia de Relatório**.

DS-K1T673 Série Rosto Reconhecimento Terminal

Você pode definir o grupo central e o sistema transferirá logs via protocolo ISUP. Clique em **Salvar** para salvar as configurações.

Grupo Centro

Selecione um grupo central na lista suspensa.

Canal Principal

O dispositivo se comunicará com o centro através do canal principal.



Nota

N1 refere-se à rede com fio.

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** → **Rede** → **Configurações Avançadas** → **Plataforma**.
 2. Selecione **ISUP** na lista suspensa do modo de acesso à plataforma.
 3. **Marque Ativar.**
 4. 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 ISUP também.

5. Clique em **Salvar**.

Configurar a escuta HTTP

O dispositivo pode enviar informações de alarme para o IP ou host de destino via protocolo HTTP/protocolo HTTPS.

Antes de começar

O IP de destino ou o nome do host deve oferecer suporte ao protocolo HTTP/protocolo HTTPS para receber as informações de alarme.



Nota

A função deve ser suportada pelo dispositivo.

Passos

1. Clique em **Configuração** → **Rede** → **Escuta Avançada** → **HTTP**.
 2. Edite o IP de destino ou o nome do host, a URL e a porta.
-

DS-K1T673 Série Rosto Reconhecimento Terminal

- 3. Opcional:** Clique em **Testar** para testar se o endereço IP ou o nome do host inseridos são válidos.
- 4. Opcional:** Clique em **Padrão** para redefinir o IP de destino ou o nome do host.
- 5.** Clique em **Salvar**.

8.5.13 Definir parâmetros de vídeo e áudio

Defina a qualidade da imagem, a resolução e o volume do dispositivo.

Definir parâmetros de vídeo

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

Video Channel	Camera1	▼
Stream Type	Main Stream	▼
Video Type	Video&Audio	▼
Resolution	1280*720	▼
Bitrate Type	Constant	▼
Video Quality	Low	▼
Frame Rate	25	▼ fps
Max. Bitrate	2048	Kbps
Video Encoding	H.264	▼
I Frame Interval	25	

Figura 8-7 Página de configurações de vídeo

Defina o canal de vídeo, o tipo de fluxo, o tipo de vídeo, a resolução, o tipo de taxa de bits, a qualidade do vídeo, a taxa de quadros, a taxa de bits máxima, a codificação de vídeo e o intervalo de quadros I.

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

Definir parâmetros de áudio

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

DS-K1T673 Série Rosto Reconhecimento Terminal

The image shows a configuration interface with the following elements:

- Stream Type:** A dropdown menu set to "Main Stream".
- Audio Encoding:** A dropdown menu set to "G.711ulaw".
- Input Volume:** A slider control with a red knob and a numeric input box showing the value "7".
- Output Volume:** A slider control with a red knob and a numeric input box showing the value "6".
- Voice Prompt:** A toggle switch that is currently turned on (green).
- Save:** A prominent red button at the bottom center.

Figura 8-8 Definir parâmetros de áudio

Arraste o bloco para ajustar o volume de entrada e saída do dispositivo. Clique em **Salvar** para salvar as configurações após a configuração.

Você também pode ativar o **Prompt de Voz**.



Nota

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

8.5.14 Personalizar conteúdo de áudio

Personalize o conteúdo de áudio de saída quando a autenticação for bem-sucedida e falhar.

Passos

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

DS-K1T673 Série Rosto Reconhecimento Terminal

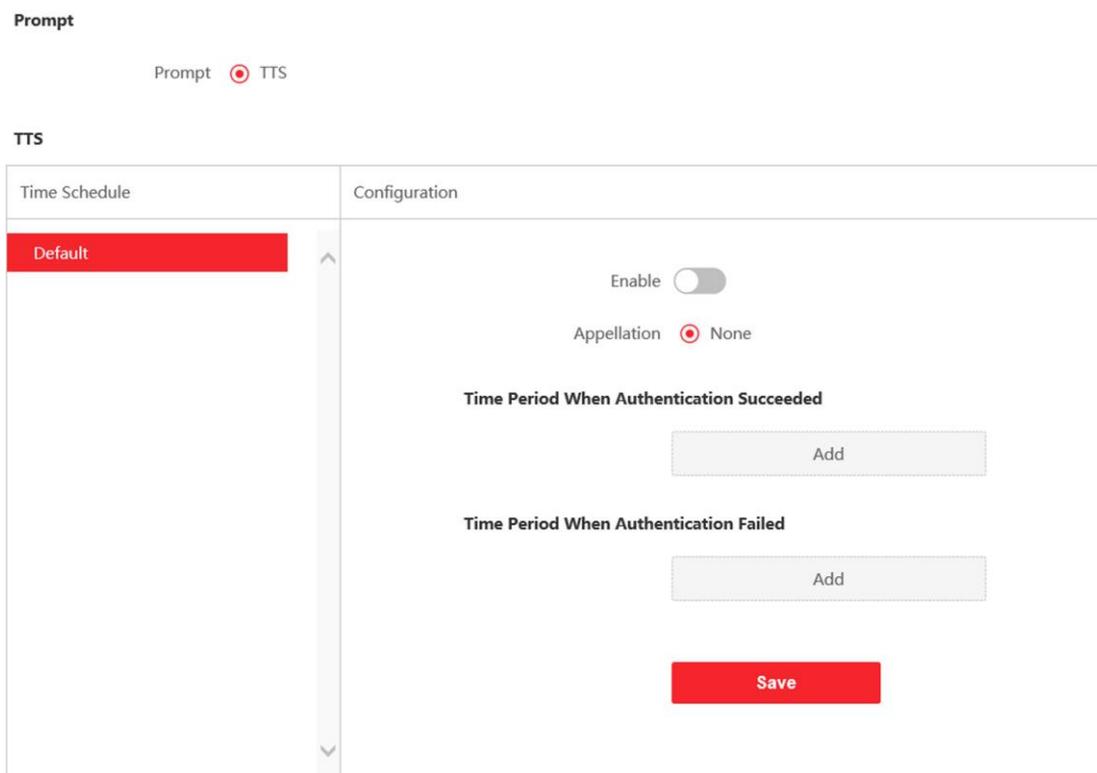


Figura 8-9 Personalizar o conteúdo de áudio

2. Defina a denominação.
3. Habilite a função.
4. Defina a duração do tempo em que a autenticação foi bem-sucedida.
 - 1) Clique em **Adicionar**.
 - 2) Defina a duração do tempo e o idioma.

Nota

Se a autenticação for bem-sucedida na duração de tempo configurada, o dispositivo transmitirá o conteúdo configurado.

- 3) Insira o conteúdo de áudio.
 - 4) **Opcional:** Repita as subetapas 1 a 3.
 - 5) **Opcional:** Clique  para excluir a duração de tempo configurada.
5. Defina a duração do tempo em que a autenticação falhou.
 - 1) Clique em **Adicionar**.
 - 2) Defina a duração do tempo e o idioma.

Nota

Se a autenticação falhar na duração de tempo configurada, o dispositivo transmitirá o conteúdo configurado.

DS-K1T673 Série Rosto Reconhecimento Terminal

- 3) Insira o conteúdo de áudio.
 - 4) **Opcional:** Repita as subetapas 1 a 3.
 - 5) **Opcional:** Clique  para excluir a duração de tempo configurada.
- 6. Opcional:** Importar prompt personalizado.
- 1) Selecione **Tipo Personalizado**.
 - 2) Selecione o caminho de importação e clique em **Importar**.
- 7.** Clique em **Salvar** para salvar as configurações.

8.5.15 Definir parâmetros de imagem

Defina o padrão de vídeo, WDR, brilho, contraste e saturação.

Passos

1. Clique em **Configuração** → **Ajuste de Imagem**.
2. Configure os parâmetros para ajustar a imagem.

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.

WDR

Habilite ou desative a função WDR.

Quando há áreas muito claras e muito escuras simultaneamente na exibição, o WDR equilibra o nível de brilho de toda a imagem e fornece imagens claras com detalhes.

Brilho/contraste/saturação/nitidez

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



Início/fim da gravação de



vídeo. Capture a imagem.

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

8.5.16 Definir Suplemento de Brilho da Luz

Defina o dispositivo de suportede brilho da luz.

Passos

1. Clique em **Configuração → Imagem → Complementar Parâmetros de Luz** .
2. Selecione um tipo e modo de luz de suplemento na lista suspensa. Se você selecionar o modo como **ON**, deverá definir o brilho.

8.5.17 Definir parâmetros de beleza

Você pode ativar a câmera de beleza e definir os parâmetros.

Passos

1. Clique em **Configuração → Imagem → Parâmetros de Beleza** .
2. **Marque Ativar Fotos de Beleza** e ajuste o Nível de **Clareamento** e o **Nível de Alisamento da Pele** de acordo com suas necessidades reais.

8.5.18 Configurações de Horário e Presença

Se você quiser rastrear e monitorar quando as pessoas iniciam/param o trabalho e monitorar suas horas de trabalho e chegadas tardias, partidas antecipadas, tempo de pausas e absenteísmo, você pode adicionar a pessoa ao grupo de turno e atribuir um horário de turno (uma regra para a participação que define como o horário se repete, o tipo de turno, configurações de quebra e a regra de passar o dedo do cartão.) ao grupo de turnos para definir os parâmetros de assiduidade para as pessoas do grupo deplantação.

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 → Atendimento** para entrar na página de configurações.
2. Defina o **Modo de Atendimento**

como **Desabilitar**. **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 **Configurações de → de Tempo** para entrar na página de configurações.
2. Selecione **Tipo de status**.
3. **Opcional:** Edite o **nome da agenda** de acordo com as necessidades reais.
4. Arrastar rato Para pôr o horário.



Nota

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

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 → Atendimento** 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. 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.

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.

DS-K1T673 Série Rosto Reconhecimento Terminal

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 → Atendimento** para entrar na página de configurações.
 2. Defina o **Modo de Atendimento** como **Automático**.
 3. Habilite a função **Status de Presença**.
 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 → Atendimento** para entrar na página de configurações.
 2. Defina o **Modo de Atendimento** como **Manual e Automático**.
 3. Habilite a função **Status de Presença**.
 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.

8.5.19 Configurações gerais

Definir parâmetros de autenticação

Clique em **Configuração** → **Configurações Gerais de Autenticação** → .



Nota

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

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

Leitor de Cartão

Selecione **Leitor de Cartão** Principal ou **Subleitor de Cartão** na lista suspensa.

Leitor de Cartão Principal

Você pode configurar os parâmetros do leitor de cartão de dispositivo.

Sub Leitor de Cartão

Você pode configurar os parâmetros do leitor de cartão periférico conectado.

Se selecionar **Leitor de Cartão Principal**:

Tipo de Leitor de Cartão/Descrição do Leitor de Cartão

Obtenha o tipo e a descrição do leitor de cartão. Eles são 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.

Autenticação de várias pessoas

Várias pessoas podem ser autenticadas ao mesmo tempo.

Intervalo de reconhecimento

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

DS-K1T673 Série Rosto Reconhecimento Terminal

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.

Se seleccionar **Sub Leitor de Cartão**:

Tipo de Leitor de Cartão/Descrição do Leitor de Cartão

Obtenha o tipo e a descrição do leitor de cartão. Eles são 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.

Autenticação de várias pessoas

Várias pessoas podem ser autenticadas ao mesmo tempo.

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.

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.

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.

Comunicação 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.

Intervalo máximo ao inserir a senha

Quando você digita a senha no leitor de cartão, se o intervalo entre pressionar dois dígitos for maior do que o valor definido, o dígitos pressionado antes será limpo automaticamente.

OK LED Polaridade / Erro LED Polaridade

Defina OK LED Polaridade / Erro LED Polaridade do dispositivo de controle de acesso de acordo com os parâmetros do leitor de cartão. Geralmente, adota as configurações padrão.

Habilitar detecção de violação

DS-K1T673 Série Rosto Reconhecimento Terminal

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

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** → **Privacidade Geral** → .

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 com a duração de tempo configurada.

Excluir eventos antigos por hora especificada

Defina uma hora e todos os eventos serão excluídos no time configurado.

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 verificar **Face Picture**, **Name**, **Employee ID** e **Temperature**, 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

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

DS-K1T673 Série Rosto Reconhecimento Terminal

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

Limpar todas as imagens no dispositivo



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.

Definir parâmetros de reconhecimento facial

Você pode definir parâmetros de reconhecimento facial para acessar.

Clique em **Configuração** → **Parâmetros Gerais de Reconhecimento Facial** → .

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.

Definir segurança do cartão

Clique em **Configuração** → **Segurança Geral do Cartão** de → 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 cartão EM

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



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.

Ativar o cartão DESFire

O dispositivo pode ler os dados do cartão DESFire ao ativar a função do cartão DESFire.

Conteúdo de leitura do cartão DESFire

Depois de ativar a função de leitura de conteúdo do cartão DESFire, o dispositivo pode ler o conteúdo do cartão DESFire.

Definir parâmetros de autenticação de cartão

Defina o conteúdo de leitura do cartão quando autenticar via cartão no dispositivo. Vá para **Configuração → Configurações Gerais de**

Autenticação do Cartão de → .

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).

8.5.20 Configurações de

intercomunicador de vídeo

Definir parâmetros de

intercomunicador de vídeo

O dispositivo pode ser usado como uma estação de porta, estação de porta externa ou dispositivo de controle de acesso. Você deve definir o dispositivo No. antes do uso.

Clique em **Configuração → Intercomunicador → Dispositivo No. .**

Se definir o tipo de dispositivo como **Door Station** ou **Access Control Device**, você poderá definir o piso No., door station No. e clicar em **Advanced Settings** para definir o **Phase No. , Nº do Edifício. e Unidade nº.**

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

DS-K1T673 Série Rosto Reconhecimento Terminal

Tipo de dispositivo

O dispositivo pode ser usado como uma estação de porta ou estação de porta externa .
Selecione um tipo de dispositivo na lista suspensa.

DS-K1T673 Série Rosto Reconhecimento Terminal



Nota

Se você alterar o tipo de dispositivo, reinicie o dispositivo.

Piso nº.

Defina o dispositivo instalado no piso nº.

Porta Estação No.

Defina o dispositivo instalado no piso nº.



Nota

Se você alterar o Não., você deve reiniciar o dispositivo.

Fase nº.

Defina a fase do dispositivo No.

Edifício nº.

Defina o dispositivo de construção No.

Unidade nº.

Defina a unidade de dispositivo No.



Nota

Se você alterar o Não., você deve reiniciar o dispositivo.

Se definir o tipo de dispositivo como **Outer Door Station**, você poderá definir o período No., a estação da porta externa No. e a comunidade No.

Estação da Porta Exterior No.

Se você selecionar a estação da porta externa como o tipo de dispositivo, deverá inserir um número entre 1 e

99.



Nota

Se você alterar o Não., você deve reiniciar o dispositivo.

Fase nº.

Defina a fase do dispositivo No.

Configurar parâmetros SIP

Defina o endereço IP do dispositivo e o endereço IP do servidor SIP. Depois de definir os parâmetros, você pode se comunicar entre o dispositivo de controle de acesso, a estação da porta, a estação interna, a estação principal e a plataforma.

Nota

Apenas o dispositivo de controle de acesso e outros dispositivos ou sistemas (como estação de porta, estação interna, estação principal, plataforma) estão no mesmo segmento IP, o áudio bidirecional pode ser realizado.

Vá para **Configuração** → **Videoproteiro** → **Configurações de Rede Vinculadas** . Defina o endereço IP da estação principal e o endereço IP do servidor SIP.
Clique em **Salvar**.

Pressione o botão para chamar

Passos

1. Clique em **Intercomunicador** → **pressione Button to Call** para entrar na página de configurações.
 2. Defina os parâmetros.
 - Editar chamada No. para cada botão.
 - Marque **Call Management Center** para definir o botão call center.
-

Nota

Se você marcar **Call Management Center** e definir a chamada No. além disso, o call management center tem privilégios mais altos do que o número de chamada.

8.5.21 Configurações de controle de acesso

Definir parâmetros da porta

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

DS-K1T673 Série Rosto Reconhecimento Terminal

Door No.

Name

Open Duration s

Door Open Timeout Alarm s

Door Contact Remain Closed Remain Open

Exit Button Type Remain Closed Remain Open

Door Lock Powering Off Status Remain Closed Remain Open

Extended Open Duration s

Door Remain Open Duration with First Person m

Duress Code
Enter 0 to 8 digits.

Super Password
Enter 0 to 8 digits.

Figura 8-10 Página de configurações de parâmetros da 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

DS-K1T673 Série Rosto Reconhecimento Terminal

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 Password

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



O código de coação e o supercódigo devem ser diferentes.

Definir parâmetros RS-485

Você pode definir os parâmetros RS-485, incluindo o periférico, endereço, taxa de transmissão, etc. Clique em **Configuração → Controle de Acesso → Configurações RS-485**.

Marque Ativar RS-485 e defina os parâmetros.

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

Não.

Defina o RS-485 No.

Tipo de periférico

Selecione um periférico na lista suspensa de acordo com a situação real. Você pode selecionar entre

Leitor de Cartão, Módulo de Extensão, Controlador de Acesso ou Desativar.



Depois que o periférico for alterado e salvo, o dispositivo será reinicializado automaticamente.

Endereço RS-485

Defina o endereço RS-485 de acordo com suas necessidades reais.

Nota

Se você selecionar **Controlador de acesso**: Se conectar o dispositivo a um terminal através da interface RS-485, defina o endereço RS-485 como 2. Se você conectar o dispositivo a um controlador, defina o endereço RS-485 de acordo com o número da porta.

Taxa de transmissão

A taxa de transmissão quando os dispositivos estão se comunicando através do protocolo RS-485.

Definir parâmetros Wiegand

Você pode definir a direção de transmissão Wiegand.

Passos

Nota

Alguns modelos de dispositivos não suportam esta função. Consulte os produtos reais ao configurar.

1. Clique em **Configuração** → **Controle de Acesso** → **Configurações do Wiegand**.



Wiegand

Wiegand Direction Input Output

Save

Figura 8-11 Página Wiegand

2. Verifique Wiegand para ativar a função Wiegand.
3. Defina uma direção de transmissão.

Entrada

O dispositivo pode conectar um leitor de cartão Wiegand.

Saída

O pode conectar um controlador de acesso externo. E os dois dispositivos transmitirão o cartão nº. via Wiegand 26 ou 34.

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



Se você alterar o periférico e depois de salvar os parâmetros do dispositivo , o dispositivo será reinicializado automaticamente.

8.5.22 Definir parâmetros biométricos

Definir parâmetros básicos

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

DS-K1T673 Série Rosto Reconhecimento Terminal

Host Parameter

Face Anti-spoofing

Live Face Detection Security Level Normal High Profile Highest

Recognition Distance Automatic 0.5m 1m 1.5m 2m

Application Mode Indoor Other

Face Recognition Mode

Continuous Face Recognition Interval 3 s

Pitch Angle 45 °

Yaw Angle 45 °

Face Grading 50

1:1 Matching Threshold 80

1:N Matching Threshold 88

Face Recognition Timeout Value 3 s

ECO Mode

ECO Mode Threshold 4

ECO Mode (1:1) 80

ECO Mode (1:N) 89

Face with Mask Detection

Face without Mask Strategy

Face with Mask 1:N Matching Threshold 75

Face with Mask 1:N Matching Threshold (ECO Mode) 70

Figura 8-12 Definir parâmetros de face

Nota

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

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

Face Anti-spoofing

DS-K1T673 Série Rosto Reconhecimento Terminal

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 ativar a função anti-falsificação facial, você pode definir o nível de segurança do matching 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 Modo Normal

Reconheça o rosto através da câmera normalmente.

Modo Profundo

No modo profundo, você pode adicionar as imagens de rosto apenas através da função de adição do usuário do dispositivo ou da estação de registro. Não é suportado para adicionar imagens de rosto através da importação de imagens.



Nota

Os dois modos não podem ser compatíveis entre si. Não altere o modo depois que ele for selecionado. Se você alterar o modo, todas as imagens de rosto do modo anterior serão desmarcadas.

Intervalo de Reconhecimento Facial Contínuo

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

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.

Classificação de Face

Defina a classificação do rosto de acordo com suas necessidades.

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

DS-K1T673 Série Rosto Reconhecimento Terminal

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.

Modo ECO

Depois de ativar o modo ECO, o dispositivo usará a câmera IR para autenticar rostos no ambiente com pouca luz ou escuridão. E você pode definir o limite do modo ECO, o modo ECO (1:N) e o modo ECO (1:1).

Modo ECO (1:1)

Defina o limite de correspondência ao autenticar via modo ECO 1 :1 correspondente mode. Quanto maior o valor, menor a taxa de aceitação falsa e maior a taxa de falsa rejeição.

Modo ECO (1:N)

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

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, é o modo ECO e a estratégia.

Nenhum

O dispositivo detectará o rosto com máscara sem avisar.

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.

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.

8.5.23 Definir publicação do aviso

Você pode definir a proteção de tela e o tempo de suspensão do dispositivo.

DS-K1T673 Série Rosto Reconhecimento Terminal

Clique em **Configuração** → **Tema** .

Modo de Exibição

Você pode selecionar o tema de exibição para autenticação de dispositivo. Você pode selecionar **Modo de exibição** como **Simples**, **Modo de anúncio** ou **Normal**. Quando você seleciona **Simples**, as informações de nome, ID, imagem do rosto não serão exibidas. Quando você seleciona **Modo de Anúncio**, o anúncio será exibido na tela.

Dormir

Ative a suspensão e o dispositivo irá ativar o modo de suspensão quando nenhuma operação dentro do tempo de suspensão configurado.

Gerenciamento de Temas

Você pode clicar em + no quadro e carregar as imagens de proteção de tela do PC local.

Você pode configurar as mensagens de boas-vindas. Selecione o **Modelo** e insira o título principal e o subtítulo, e selecione o **Tamanho da Fonte** e a **Cor da Fonte**. Você também pode clicar em **Personalizar** para selecionar a imagem de plano de fundo personalizada.



Nota

Até agora, há apenas um tema pode ser adicionado.

Horário de Reprodução

Depois de criar um tema, você pode selecioná-lo e desenhar um cronograma na linha do tempo. Selecione a programação sorteada e você pode editar a hora exata de início e término. Selecione a agenda desenhada e você pode clicar em Excluir ou **Excluir tudo** para excluir a agenda.

Intervalo de apresentação de slides

Arraste o bloco ou insira o número para definir o intervalo da apresentação de slides. A imagem será alterada de acordo com o intervalo.

Capítulo 9 Configuração do Software Cliente

9.1 Fluxo de configuração do software cliente

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

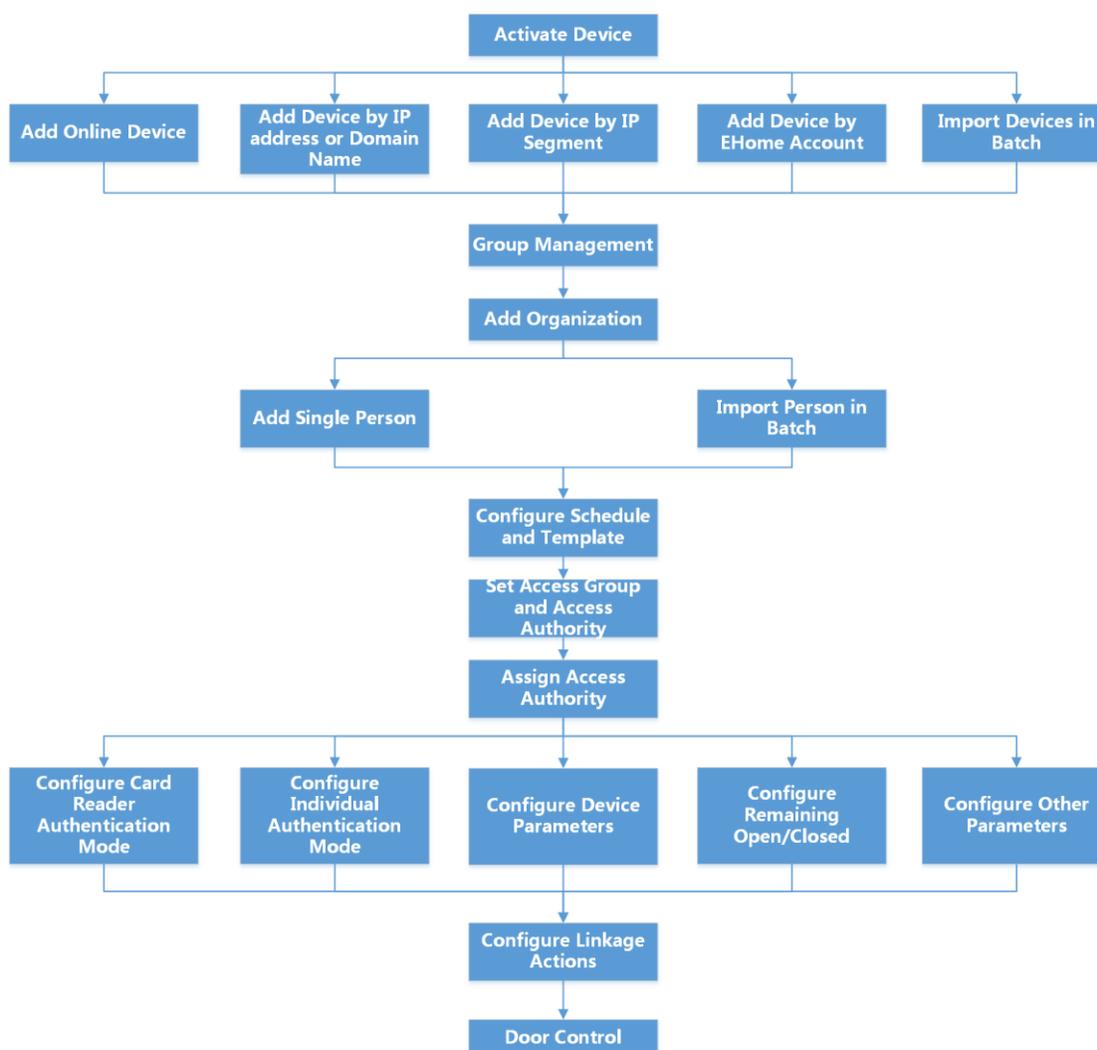


Figura 9-1 Diagrama de fluxo de configuração no software cliente

9.2 Gerenciamento de dispositivos

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

DS-K1T673 Série Rosto Reconhecimento Terminal

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.

9.2.1 Adicionar dispositivo

O cliente fornece três modos de adição de dispositivos, incluindo por IP /domínio, segmento IP e protocolo ISUP. 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 port. 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

DS-K1T673 Série Rosto Reconhecimento Terminal

você altera 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.

-
- 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

DS-K1T673 Série Rosto Reconhecimento Terminal

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

DS-K1T673 Série Rosto Reconhecimento Terminal

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 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.

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.

9.2.2 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 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.

9.2.3 Gerenciar dispositivos adicionados

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

Tabela 9-1 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.

9.3 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.

9.3.1 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.

9.3.2 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 You Start

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.

9.4 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.

9.4.1 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.

9.4.2 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 Pessoa Information

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).
-

9.4.3 Obter informações pessoais do dispositivo de controle de acesso

Se o dispositivo de controle de acesso adicionado tiver sido configurado com informações de pessoa (incluindo detalhes de pessoa e informações de cartão emitidas), você poderá obter as informações de 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, e os cartões vinculados (se configurados), serão importados para a organização selecionada.

9.4.4 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**.
-

DS-K1T673 Série Rosto Reconhecimento Terminal

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

DS-K1T673 Série Rosto Reconhecimento Terminal

- 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*.
- Clique em **Inicializar** para inicializar a estação de registro de cartão ou o leitor de cartão para prepará-lo para a emissão de cartões.
- 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).

9.4.5 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

- Insira o **módulo Pessoa** .
- Selecione a pessoa para a qual você deseja denunciar a perda do cartão e clique em Editar para abrir a janela Editar pessoa.
- 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.
- 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.
- 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.

9.4.6 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**

DS-K1T673 Série Rosto Reconhecimento Terminal

de emissão do cartão.

DS-K1T673 Série Rosto Reconhecimento Terminal

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 reais.

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.

9.5 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](#).

9.5.1 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. Adicione o período do feriado e configure a 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 transformar em .
 - 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**.

9.5.2 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.

DS-K1T673 Série Rosto Reconhecimento Terminal

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 cursor se voltar para .
 - 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

DS-K1T673 Série Rosto Reconhecimento Terminal

Para obter detalhes sobre como adicionar um feriado, consulte [**Adicionar feriado**](#).

DS-K1T673 Série Rosto Reconhecimento Terminal

- 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.

9.6 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, aplicar o grupo de acesso ao dispositivo de controle de acesso para entrar em vigor.

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 no 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, imagem do rosto, ligação entre o número do cartão e a ligação entre o número do cartão e o cartão), senha, período de vigência 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.

DS-K1T673 Série Rosto Reconhecimento Terminal

The screenshot shows a web interface with a table of access groups on the left and a detailed view on the right. The table has columns for Name, Template, Status, and Operation. The detailed view shows a 'Person' section with columns for TheName, SerialNumber..., and Organization, and an 'Access Point' section with columns for Access Point and Group Name.

Name	Template	Status	Operation
Access Group 2	All-Day Auth...	To be Appli...	
Access Group 1	All-Day Auth...	To be Appli...	
Access Group 3	All-Day Auth...	To be Appli...	

TheName	SerialNumber...	Organization
Jane	1	New Organization
Mike	2	New Organization

Access Point	Group Name
Door1_Access control host	Access control host
Door2_Access control host	Access control host

Figura 9-2 Exibe a(s) pessoa(s) selecionada(s) e o(s) ponto(s) de acesso

- Depois de adicionar os grupos de acesso, você precisa aplicá-los ao dispositivo de controle de acesso para entrar em vigor.
 - Selecione o(s) grupo(s) de acesso a ser aplicado ao dispositivo de controle de acesso.
 - 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.
 - 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).
 - 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) vinculado(s).

- 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**.

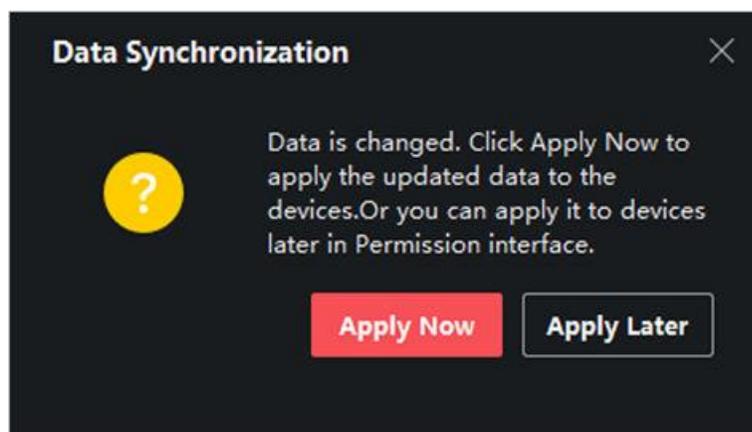


Figura 9-4 Sincronização de dados

9.7 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.
-

9.7.1 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 Access

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.

Antes de começar

Adicione o dispositivo de controle de acesso ao cliente.

Passos

1. Clique **Acesso Controle** → **Avançado Função** → **Dispositivo Parâmetro** .



Nota

Se você não conseguir encontrar o parâmetro de dispositivo na lista de 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.

RS-485 Com. Redundância

Você deve ativar essa função se você conectar o leitor de cartão RS-485 ao dispositivo de controle de acesso de forma redundante.

Exibir rosto detectado

Exiba a imagem do rosto ao autenticar.

Número do cartão de exibição

Exiba as informações do cartão ao autenticar.

Exibir informações da pessoa

Exiba as informações da pessoa ao autenticar.

Sobrepôr informações da pessoa. na imagem

Exiba as informações da pessoa na imagem capturada.

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.

DS-K1T673 Série Rosto Reconhecimento Terminal

Pressione a tecla para inserir o número do cartão

Se você ativar essa função, poderá inserir o cartão No. pressionando a tecla.

Sonda Wi-Fi

Se você ativar essa função, o dispositivo poderá sondar o endereço MAC dos dispositivos de comunicação ao redor e carregar o endereço MAC no sistema. Se o endereço MAC corresponder ao endereço MAC especificado, o sistema poderá acionar algumas ações de ligação.

3G/4G

Se você ativar essa função, o dispositivo poderá se comunicar em rede 3G/4G.

Anticlonagem NFC

Se você habilitar essa função, não poderá usar o cartão clonado para autenticação e aumentar ainda mais a segurança.

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) selecionado(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

DS-K1T673 Série Rosto Reconhecimento Terminal

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 campanha 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

DS-K1T673 Série Rosto Reconhecimento Terminal

Adicione o dispositivo de controle de acesso ao cliente.

DS-K1T673 Série Rosto Reconhecimento Terminal

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. Editar o cartão leitor básico Parâmetros em o Básico Informação página.



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 campanha

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 leitura do cartão atingirem o valor definido.

Tempos máximos de falha do cartão

Defina o máximo tentativas de falha do cartão de leitura.

Deteção de adulteração

Habilite a deteção 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 buzzing 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

DS-K1T673 Série Rosto Reconhecimento Terminal

Selecione o nível de reconhecimento de impressão digital na lista suspensa.

Modo de autenticação padrão do leitor de cartão

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.

Deteção de rosto ao vivo

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

Nível de segurança de deteção 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 deteção de rosto ao vivo. O sistema bloqueará o rosto do usuário por 5 minutos se a deteção 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 cum autenticar 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 deteção de rosto ao vivo falhar por mais do que as tentativas confi gured. O

DS-K1T673 Série Rosto Reconhecimento Terminal

mesmo

DS-K1T673 Série Rosto Reconhecimento Terminal

o 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 o interior ou outros modos de aplicação de acordo com o 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.

Configurar parâmetros para o controlador de faixa

Depois de adicionar o controlador de faixa ao cliente, você pode configurar seus parâmetros para passar pela pista.

Antes de começar

Adicione o dispositivo de controle de acesso ao cliente.

Passos

1. Clique em **Controle de Acesso** → **Função Avançada** → **Parâmetro de Dispositivo** para entrar na página Configurações de Parâmetro.

2. Na lista de dispositivos à esquerda, selecione um controlador de faixa e você pode editar os parâmetros do controlador de faixa à direita.

DS-K1T673 Série Rosto Reconhecimento Terminal

3. Edite os parâmetros.

DS-K1T673 Série Rosto Reconhecimento Terminal

Modo de passagem

Selecione o controlador que controlará o status de barreira do dispositivo.

- Se você selecionar **De acordo com as Configurações DIP do Lane Controller**, o dispositivo seguirá as configurações DIP do controlador de faixa para controlar a barreira. As configurações no software serão inválidas.
- Se você selecionar **De acordo com** as configurações do controlador **principal**, o dispositivo seguirá as configurações do software para controlar a barreira. As configurações de DIP do controlador de faixa serão inválidas.

Autenticação de Passagem Gratuita

Se você ativar essa função, quando o modo de barreira de entrada e saída for Permanecer Aberto, os pedestres deverão se autenticar cada vez que passarem pela pista. Ou um alarme será acionado.

Velocidade de Barreira de Abertura/ Fechamento

Defina a velocidade de abertura e fechamento da barreira. Você pode selecionar de 1 a 10. Quanto maior o valor, mais rápida a velocidade.



Nota

O valor recomendado é 6.

Duração do prompt audível

Defina quanto tempo o áudio vai durar, que é reproduzido quando um alarme é acionado.



Nota

O refere-se ao áudio do alarme que será reproduzido até que o alarme seja encerrado.

Unidade de Temperatura

Selecione a unidade de temperatura exibida no status do dispositivo.

4. Clique em **OK**.

9.7.2 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.

DS-K1T673 Série Rosto Reconhecimento Terminal

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. Pôr o 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 bloqueio), 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.

Antes de começar

Adicione o dispositivo de controle de acesso ao cliente e verifique se o dispositivo oferece suporte à interface RS-485.

Passos

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.
-

DS-K1T673 Série Rosto Reconhecimento Terminal

- Defina a taxa de transmissão, o bit de dados, o bit de parada, o tipo de paridade, o modo de comunicação, o modo de trabalho e o modo de conexão na lista suspensa.



Nota

Quando o modo de conexão é **Conectar Dispositivo de Controle de Acesso**, você pode selecionar **Número do cartão.** ou **ID da pessoa** como o tipo de saída.

- 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. Depois de definir os parâmetros Wiegand, o dispositivo pode se conectar ao leitor de cartões Wiegand via comunicação Wiegand.

Antes de começar

Adicione o dispositivo de controle de acesso ao cliente e verifique se o dispositivo é compatível com Wiegand.

Passos

- Entre no módulo Controle de Acesso.
- Na barra de navegação à esquerda, insira **Função Avançada → Mais Parâmetros**.
- Selecione um dispositivo de controle de acesso na lista de dispositivos e clique em **Wiegand** para entrar na página Configurações do Wiegand.
- Defina o interruptor como ativado para ativar a função Wiegand para o dispositivo.
- Selecione 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**.

- 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.

DS-K1T673 Série Rosto Reconhecimento Terminal

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 Criptografia de Cartão M1 para entrar na página Criptografia de Cartão M1.
4. Defina a opção como ativada para ativar a função de criptografia do cartão M1.
5. Defina a ID do setor.
O ID do setor varia de 1 a 100.
6. Clique em **Salvar** para salvar as configurações.

9.8 Controle de Porta/Elevador

No módulo Monitoramento, você pode visualizar o status em tempo real das portas ou elevadores gerenciados pelo dispositivo de controle de acesso adicionado. Você também pode controlar as portas e elevadores, 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/elevador, o usuário pode entrar no módulo de Monitoramento e controlar a porta/elevador. Ou os ícones usados para controle não serão exibidos. Para definir a permissão do usuário, consulte .

9.8.1 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

Resultado

O ícone das portas mudará em tempo real de acordo com a operação, se a operação for bem-sucedida.

9.8.2 Verificar registros de acesso em tempo real

Os registros de acesso em tempo real podem ser exibidos no cliente, incluindo registros de passagem de cartão, registros de reconhecimento facial, informações de temperatura da superfície da pele, etc. Além disso, você pode visualizar as informações da pessoa e visualizar a imagem capturada durante o acesso.

DS-K1T673 Série Rosto Reconhecimento Terminal

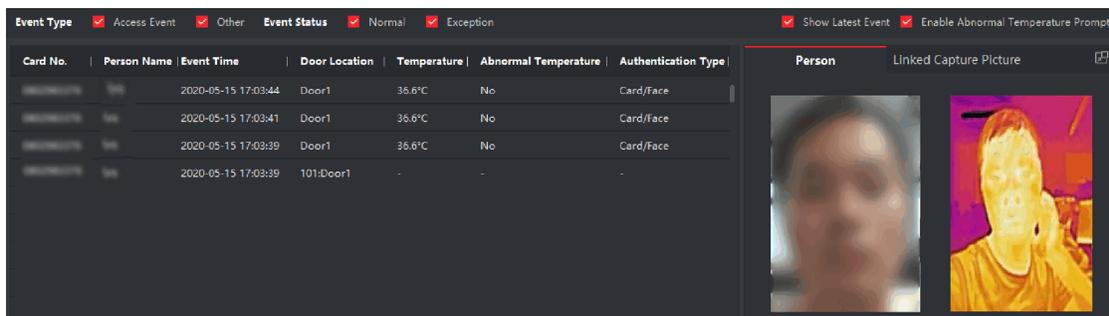
Antes de começar

Você adicionou pessoa(s) e dispositivo (s) de controle de acesso ao client. Para obter detalhes, consulte [Gerenciamento de pessoas](#) e [Adicionar dispositivo](#).

Passos

1. Clique em **Monitoramento** para entrar no módulo de monitoramento.

Os registros de acesso em tempo real são exibidos na parte inferior da página. Você pode visualizar os detalhes do registro, incluindo o número do cartão, o nome da pessoa, a hora do evento, a localização da porta, a temperatura, o tipo de autenticação, etc.



Event Type	Access Event	Other	Event Status	Normal	Exception	Show Latest Event	Enable Abnormal Temperature Prompt	
Card No.	Person Name	Event Time	Door Location	Temperature	Abnormal Temperature	Authentication Type	Person	Linked Capture Picture
		2020-05-15 17:03:44	Door1	36.6°C	No	Card/Face		
		2020-05-15 17:03:41	Door1	36.6°C	No	Card/Face		
		2020-05-15 17:03:39	Door1	36.6°C	No	Card/Face		
		2020-05-15 17:03:39	101:Door1	-	-	-		

Figura 9-5 Registros de acesso em tempo real

Nota

Você pode clicar 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.

2. **Opcional:** selecione um grupo de pontos de acesso na lista suspensa no canto superior direito para mostrar os registros de acesso em tempo real do grupo selecionado.
3. **Opcional:** Verifique o tipo de evento e o status do evento.
Os eventos detectados do tipo e status verificados serão exibidos na lista abaixo.
4. **Opcional:** Marque **Mostrar evento mais recente** para exibir o registro de acesso mais recente. A lista de registros será listada cronologicamente de forma inversa.
5. **Opcional:** Marque **Ativar Prompt de Temperatura Anormal** para ativar a superfície anormal da pele prompt de temperatura.

Nota

Quando ativado, se houver informações de temperatura anormais, uma janela Temperatura Anormal aparecerá quando você entrar no módulo Monitoramento, exibindo a imagem da pessoa, a temperatura da superfície da pele, o número do cartão, o nome da pessoa, etc.

6. **Opcional:** Clique no acontecimento Para vista pessoa Fotos (incluindo Capturado imagem e

Nota

perfil).

No campo **Imagem de Captura Vinculada**, você pode clicar duas vezes na imagem capturada para exibir uma imagem ampliada.

DS-K1T673 Série Rosto Reconhecimento Terminal

7. **Opcional:** Clique  para ver os detalhes (incluindo as informações detalhadas da pessoa e a imagem capturada).
-



Na janela pop-up, você pode clicar  para ver detalhes em tela |

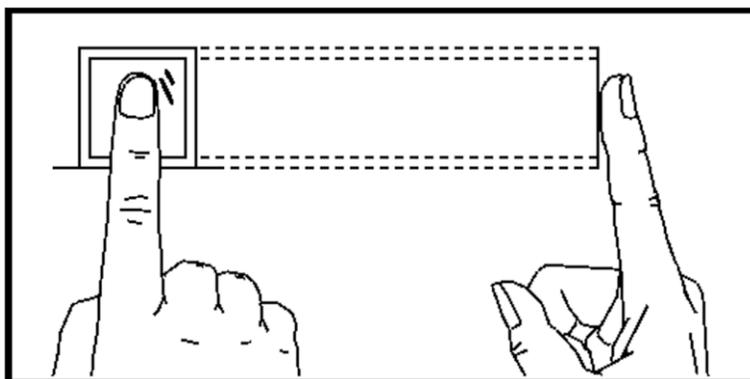
Apêndice A. Dicas para digitalizar impressão digital

Dedo recomendado

Dedo indicador, dedo médio ou terceiro dedo.

Varredura correta

A figura exibida abaixo é a maneira correta de digitalizar seu dedo:

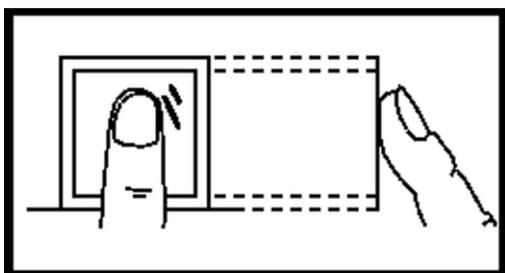


Você deve pressionar o dedo no scanner horizontalmente. O centro do dedo digitalizado deve estar alinhado com o centro do scanner.

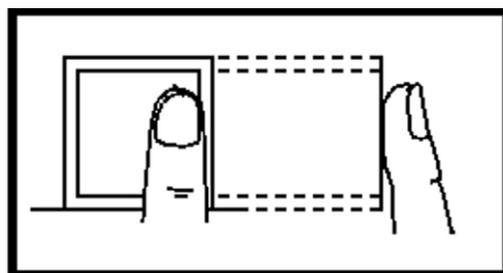
Varredura incorreta

As figuras de digitalização de impressões digitais exibidas abaixo estão incorretas:

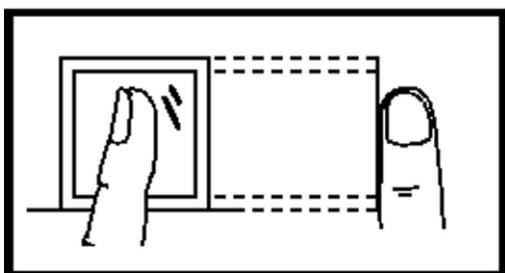
DS-K1T673 Série Rosto Reconhecimento Terminal



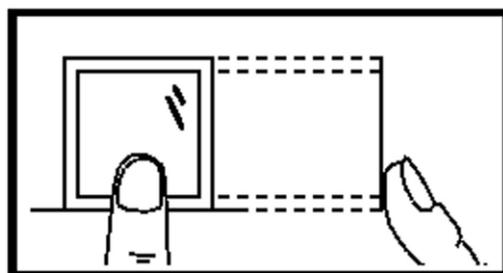
Vertical



Edge I



Side



Edge II

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

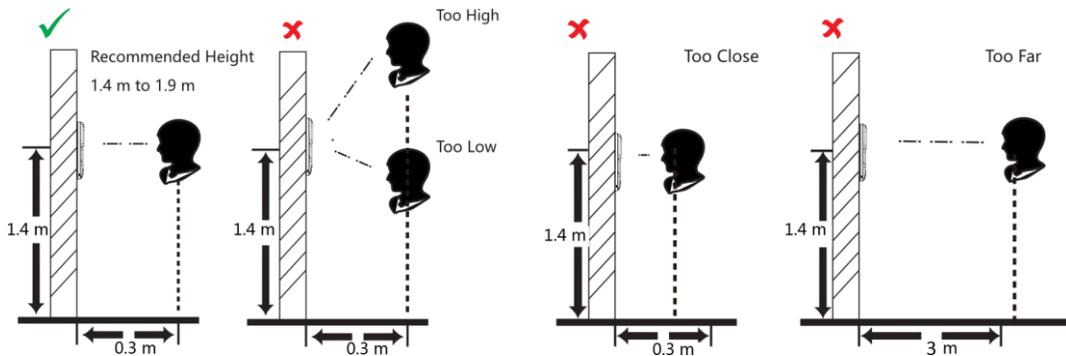
Se a sua impressão digital for superficial ou se for difícil digitalizá-la, recomendamos que utilize outros métodos de autenticação.

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 : 0,3 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

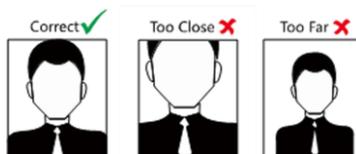
Para obter uma imagem de rosto de boa qualidade e precisa, posicione seu rosto olhando para a câmera ao coletar ou comparar fotos de rosto.



DS-K1T673 Série Rosto Reconhecimento Terminal

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



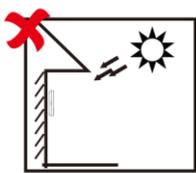
Lâmpada: 100~850Lux



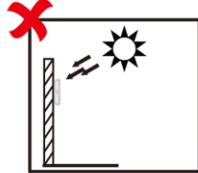
Luz solar: Mais de 1200Lux



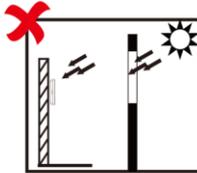
2. Evite luz de fundo, luz solar direta e indireta



Backlight



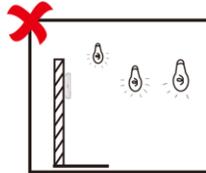
Direct Sunlight



Direct Sunlight
through Window

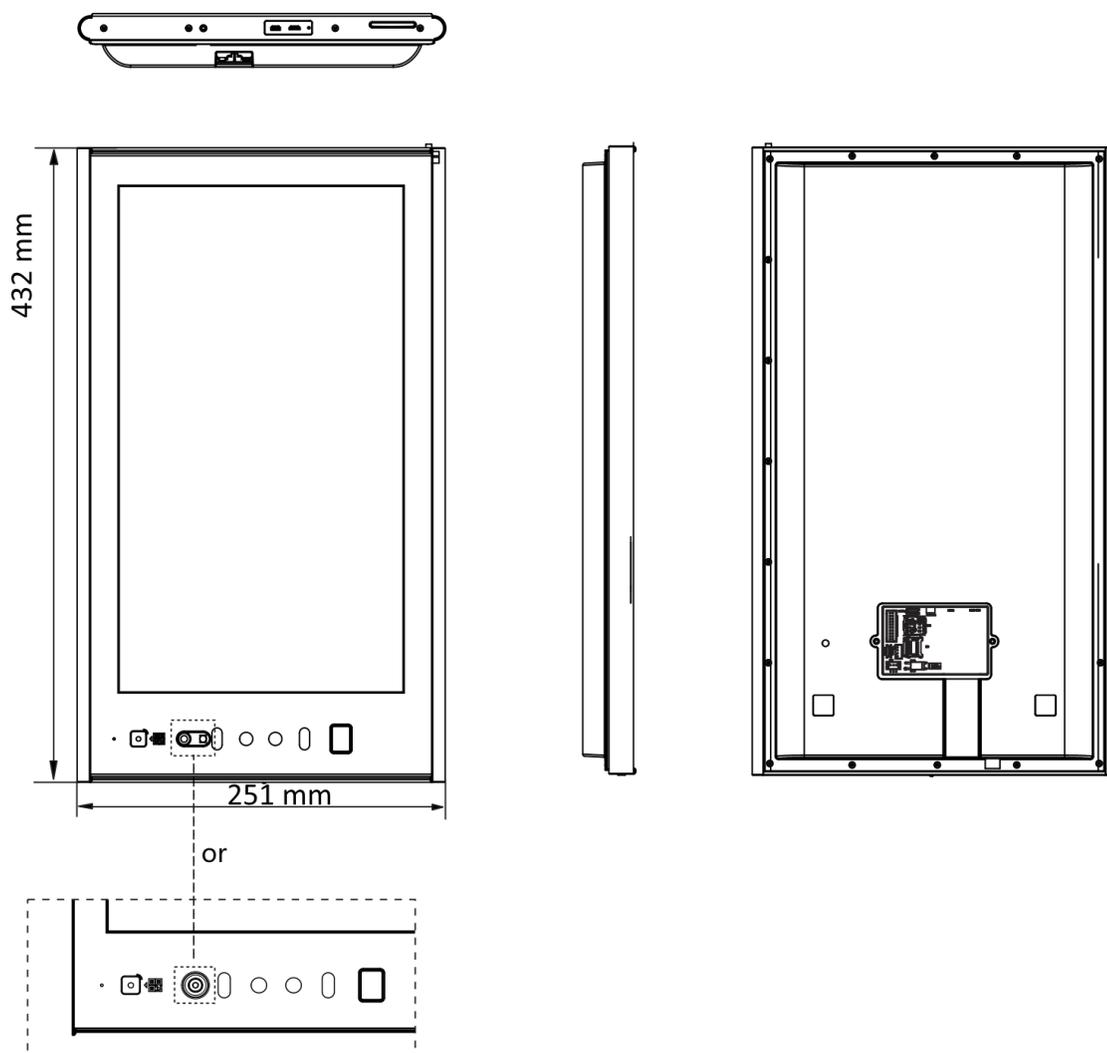


Indirect Light
through Window



Close to Light

Apêndice D. 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