

Terminal de reconhecimento facial

Manual do usuário

Informação legal

© 2020 Hangzhou Hikvision Digital Technology Co., Ltd. Todos os direitos reservados.

Sobre este manual

O manual inclui instruções para usar e gerenciar o produto. Fotos, gráficos, imagens e todas as outras informações a seguir são apenas para descrição e explicação. As informações contidas no Manual estão sujeitas a alterações, sem prévio aviso, devido a atualizações de firmware ou outros motivos. Encontre a versão mais recente deste manual no site da Hikvision (<https://www.hikvision.com/>).

Use este Manual com a orientação e assistência de profissionais treinados no suporte ao Produto.

Marcas Registradas

e outras marcas registradas e logotipos da HIKVISION são propriedades da Hikvision em várias jurisdições.

Outras marcas comerciais e logotipos mencionados são propriedades de seus respectivos proprietários.

aviso Legal

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, COMERCIALIZABILIDADE, QUALIDADE SATISFATÓRIA OU ADEQUAÇÃO A UM DETERMINADO FIM. O USO DO PRODUTO POR VOCÊ É POR SUA PRÓPRIA CONTA E RISCO. EM NENHUMA HIKVISION SERÁ RESPONSÁVEL POR VOCÊ POR QUAISQUER DANOS ESPECIAIS, CONSEQÜENCIAIS, INCIDENTAIS OU INDIRETOS, INCLUINDO, ENTRE OUTROS, DANOS POR PERDA DE LUCROS DE NEGÓCIOS, INTERRUPÇÃO DE NEGÓCIOS, OU PERDA DE DADOS, CORRUPÇÃO DE SISTEMAS, OU PERDA DE DOCUMENTOS SEJA COM BASE NA VIOLAÇÃO DE CONTRATO, DELITO (INCLUINDO NEGLIGÊNCIA), RESPONSABILIDADE DO PRODUTO, OU DE OUTRA FORMA, EM RELAÇÃO AO USO DO PRODUTO, MESMO SE A HIKVISION TIVER SIDO AVISADA DA POSSIBILIDADE DE TAIS DANOS OU PERDAS.

VOCÊ RECONHECE QUE A NATUREZA DA INTERNET FORNECE PARA RISCOS DE SEGURANÇA INERENTES, E A HIKVISION NÃO DEVE ASSUMIR QUALQUER RESPONSABILIDADE POR OPERAÇÃO ANORMAL, FUGA DE PRIVACIDADE OU OUTROS DANOS RESULTANTES DE ATAQUE CIBERNÉTICO, ATAQUE DE HACKER, OU OUTROS RISCOS DE INTERNET VIRUS; NO ENTANTO, A HIKVISION FORNECERÁ SUPORTE TÉCNICO OPORTUNO SE NECESSÁRIO.

VOCÊ CONCORDA EM USAR ESTE PRODUTO EM CONFORMIDADE COM TODAS AS LEIS APLICÁVEIS E É O ÚNICO RESPONSÁVEL POR GARANTIR QUE SEU USO ESTÁ CONFORME AS LEIS APLICÁVEIS. ESPECIALMENTE, VOCÊ É RESPONSÁVEL, POR USAR ESTE PRODUTO DE FORMA QUE NÃO VIOLE 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 FINIS PROIBIDOS,

INCLUINDO O DESENVOLVIMENTO OU PRODUÇÃO DE ARMAS DE DESTRUIÇÃO DE MASSA, O DESENVOLVIMENTO OU PRODUÇÃO DE ARMAS QUÍMICAS OU BIOLÓGICAS, QUAISQUER ATIVIDADES NO CONTEXTO RELACIONADO A QUALQUER CICLO NUCLEAR EXPLOSIVO OU INSEGURO , OU EM APOIO A ABUSOS DE DIREITOS HUMANOS. EM CASO DE QUAISQUER CONFLITOS ENTRE ESTE MANUAL E A LEI APLICÁVEL, O POSTERIOR ANTES.




Proteção de dados

Durante o uso do dispositivo, dados pessoais serão coletados, armazenados e processados. Para proteger os dados, o desenvolvimento de dispositivos Hikvision incorpora 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 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 implementação de controles de segurança física e administrativa razoáveis, conduza análises e avaliações periódicas da eficácia de seus controles de segurança.

Convenções de símbolo

Os símbolos que podem ser encontrados neste documento são definidos a seguir.

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.

Informação Regulatória

Informação FCC

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

- Reorientar ou reposicionar a antena receptora.
- Aumente a separação entre o equipamento e o receptor.
- Conecte o equipamento a uma tomada em um circuito diferente daquele ao qual o receptor está conectado.
- Consulte o revendedor ou um técnico experiente de rádio / TV para obter ajuda

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

Condições FCC

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

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

Declaração de conformidade da UE



Este produto e - se aplicável - os acessórios fornecidos também são marcados com "CE" e, portanto, está em conformidade com os padrões europeus harmonizados aplicáveis listados na Diretiva EMC 2014/30 / EU, Diretiva RE 2014/53 / EU, a Diretiva RoHS 2011 / 65 / EU



2012/19 / EU (diretiva WEEE): Os produtos marcados com este símbolo não podem ser descartados como lixo municipal não classificado na União Europeia. Para a reciclagem adequada, devolva este produto ao seu fornecedor local ao adquirir um novo equipamento equivalente ou descarte-o em pontos de coleta



designados. Para mais informações, consulte:
www.recyclethis.info

2006/66 / EC (diretiva de bateria): Este produto contém uma bateria que não pode ser descartada como lixo municipal não classificado 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 a reciclagem adequada, devolva a bateria ao seu fornecedor ou a um ponto de coleta designado. Para mais informações, consulte:
www.recyclethis.info

Este dispositivo está em conformidade com os padrões RSS isentos de licença da Industry Canada. A operação está sujeita às seguintes duas condições:

- (1) este dispositivo não pode causar interferência, e
- (2) este dispositivo deve aceitar qualquer interferência, incluindo interferência que pode causar operação indesejada do dispositivo.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

- (1) l'appareil ne doit pas produire de brouillage, et
- (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.



Instruções de segurança

Estas instruções têm como objetivo 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 Cuidados:

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

Cuidados: 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 ferimentos ou danos materiais.

Perigo:

- Toda a operação eletrônica deve estar estritamente de acordo com os regulamentos de segurança elétrica, regulamentos de prevenção de incêndio e outros regulamentos relacionados em sua região local.
- Use o adaptador de energia, que é fornecido por uma empresa normal. Este equipamento deve ser fornecido com fonte de alimentação protegida contra sobretensão Classe 2, com classificação de 12 VCC, 2 A.
- 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 energia foi desconectada antes de conectar, instalar ou desmontar o dispositivo.
- Quando o produto é instalado na parede ou no teto, o dispositivo deve ser firmemente fixado.
- Se fumaça, odores ou ruído aumentar do dispositivo, desligue a energia imediatamente, desconecte o cabo de alimentação e entre em contato com a central de atendimento.
- Não ingerir bateria, perigo de queimadura química.
Este produto contém uma bateria tipo moeda / botão. Se a bateria tipo moeda / botão for engolida, isso pode causar queimaduras internas graves em apenas 2 horas e pode levar à morte.
Mantenha as baterias novas e usadas fora do alcance das crianças. Se o compartimento da bateria não fechar com segurança, pare de usar o produto e mantenha-o fora do alcance das crianças. Se você acha que as pilhas podem ter sido engolidas ou colocadas dentro de qualquer parte do corpo, consulte imediatamente um médico.
- Se o produto não funcionar corretamente, entre em contato com seu revendedor ou centro de serviço mais próximo. Nunca tente desmontar o dispositivo sozinho. (Não assumiremos qualquer responsabilidade por problemas causados por reparos ou manutenção não autorizados.)

Cuidados:

- Não deixe cair o dispositivo nem o sujeite a choques físicos, e não o exponha a altas radiações de eletromagnetismo. Evite a instalação do equipamento em superfícies com vibrações ou locais sujeitos a choques (o desconhecimento pode causar danos ao equipamento).
- Não coloque o dispositivo em locais extremamente quentes (consulte as especificações do dispositivo para obter a temperatura de operação detalhada), frios, empoeirados ou úmidos e não o exponha a alta radiação eletromagnética.
- A tampa do dispositivo para uso interno deve ser protegida de chuva e umidade.
- É proibida a exposição do equipamento à luz solar direta, baixa ventilação ou fonte de calor como aquecedor ou radiador (ignorância pode causar perigo de incêndio).
- Não aponte o dispositivo para o sol ou locais com muita luz. Caso contrário, pode ocorrer uma floração ou manchas (o que não é um mau funcionamento), afetando a durabilidade do sensor ao mesmo tempo.
- 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 da superfície da tampa do dispositivo.
- Use um pano macio e seco para limpar as superfícies interna e externa da tampa do dispositivo, não use detergentes alcalinos.
- Guarde todos os invólucros depois de desempacotá-los para uso futuro. Caso ocorra alguma falha, é necessário devolver o dispositivo à fábrica com a embalagem original. O transporte sem a embalagem original pode resultar em danos ao dispositivo e gerar custos adicionais.
- O uso ou substituição inadequada da bateria pode resultar em risco de explosão. Substitua pelo mesmo tipo ou equivalente apenas. Descarte as baterias usadas de acordo com as instruções fornecidas pelo fabricante da bateria.
- Produtos de reconhecimento biométrico não são 100% aplicáveis a ambientes anti-spoofing. Se você precisar de um nível de segurança mais alto, use vários modos de autenticação.
- Temperatura de trabalho: 0 ° C a 50 ° C; Umidade de trabalho: 10% a 90% (sem condensação)
- Uso interno. O dispositivo deve estar a pelo menos 2 metros da luz e a pelo menos 3 metros da janela.
- Versão: 1.0, Data de Emissão: 20200519

Modelos Disponíveis

Nome do Produto	Modelo
Terminal de reconhecimento facial	DS-K1TA70 DS-K1T671TM-3XF

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

Modelo	Fabricante	Padrão
C2000IC12.0-24P-DE	MOSO Power Supply Technology Co., Ltd.	CEE
C2000IC12.0-24P-GB	MOSO Power Supply Technology Co., Ltd.	BS
KPL-040F-VI	Channel Well Technology Co Ltd.	CEE

Conteúdo

Capítulo 1 Visão Geral.....	14
1.1 Visão geral.....	14
1.2 Características	14
Capítulo 2 Aparência.....	16
Capítulo 3 Instalação	20
3.1 Ambiente de instalação	20
3.2 Montagem.....	20
3.3 Montagem de superfície.....	23
Capítulo 4 Fiação	25
4.1 Descrição do terminal.....	26
4.2 Fiação do Dispositivo.....	30
4.3 Unidade de controle da porta de proteção com fio.....	31
4.4 Módulo de incêndio com fio	31
4.4.1 Diagrama de fiação da porta aberta ao desligar	31
4.4.2 Diagrama de fiação da porta bloqueada ao desligar	33
Capítulo 5 Ativação.....	35
5.1 Ativar via dispositivo	35
5.2 Ativar via SADP.....	36
5.3 Ativar dispositivo via software cliente	37
Capítulo 5 Operações Básicas.....	39
6.1 Definir o modo de aplicação	39
6.2 Login	40
6.2.1 Login pela primeira vez	40
6.2.2 Login pelo Administrador	41
6.3 Configurações de comunicação	43
6.3.1 Definir parâmetros de rede	44
6.3.2 Definir parâmetros RS-485	44
6.3.3 Set Parâmetros de Wiegand	45
6.4 Gerenciamento de Usuários	46

6.4.1 Adicionar administrador	46
6.4.2 Adicionar imagem facial	47
6.4.3 Adicionar cartão.....	49
6.4.4 Adicionar senha	50
6.4.5 Modo de autenticação	51
6.4.6 Pesquisar e editar usuário	52
6.5 Medição da temperatura	52
6.5.1 Configurações de medição de temperatura	52
6.5.2 Black Body Configurações	54
6.6 Importação e exportação de dados	56
6.6.1 Exportação de dados	56
6.6.2 Importação de dados	56
6.7 Autenticação de identidade	57
6.7.1 Autenticar via Credencial Múltipla	57
6.7.2 Autenticar via Credencial Única.....	58
6.8 Configurações do sistema	58
6.8.1 Configurar parâmetros básicos.....	58
6.8.2 Set Parâmetros de imagem facial	59
6.8.3 Configurar tempo.....	62
6.9 Configurar parâmetros do Controle de Acesso	63
6.10 Manutenção	64
6.10.1 Atualização de Firmware	64
6.10.2 Gerenciamento de Data	65
6.10.3 Log	65
6.11 Status e configuração de Tempo e Atendimento	66
6.11.1 Desativação de Modo Atendimento via Terminal	66
6.11.2 Automático Modo Atendimento via Terminal	67
6.11.3 Manual Modo Atendimento via Terminal.....	68
6.11.4 Configurar Manual e Automático Modo Atendimento via Terminal	68
6.12 Visualizar configurações do sistema.....	70
6.13 Video Intercom	71

6.13.1 Chamar software cliente do Terminal	71
6.13.2 Chamar Master Station do Terminal	72
6.13.3 Chamar Terminal do Software Cliente	72
6.13.4 Chamar Telas internas do Terminal	73
Capítulo 7 Configuração do software cliente	74
7.1 Configurações de fluxo no Software Cliente.....	74
7.2 Gerenciamento de dispositivos.....	74
7.2.1 Adicionar dispositivo	75
7.2.2 Resetar senha do Dispositivo	83
7.3 Gestão de Grupo	84
7.3.1 Adicionar Grupo	84
7.3.2 Importar recursos de Grupo	85
7.3.3 Editar parâmetros dos recursos.....	85
7.3.4 Remover recursos do Grupo	86
7.4 Gerenciamento de Pessoas.....	86
7.4.1 Adicionar Organização	86
7.4.2 Configuração Basica de Informações	87
7.4.3 Problemas com Cartão no modo Local	88
7.4.4 Carregar fotos via PC Local	89
7.4.5 Tirar foto via software Cliente.....	90
7.4.6 Coletar face via Terminal de controle de acesso	91
7.4.7 Configurar informações de controle de acesso	92
7.4.8 Customizar informações de pessoas	94
7.4.9 Configurar informações de residentes	95
7.4.10 Configurar informações adicionais	96
7.4.11 Importar e exportar informações de pessoas	96
7.4.12 Importar informações de pessoas	96
7.4.13 Importar Fotos de pessoas	97
7.4.14 Exportar informações de pessoas	98
7.4.15 Exportar fotos de pessoas	98
7.4.16 Coletar informações de pessoas pelo terminal de controle de acesso	99

7.4.17 Mover pessoas para uma outra Organização	100
7.4.18 Problemas em cartões de pessoas em lote	100
7.4.19 Reportar cartão perdido.....	101
7.4.20 Configurar cartão com problema	101
7.5 Configurar padrão de Agenda	102
7.5.1 Adicionar Feriado	103
7.5.2 Adicionar Padrão de Agenda	104
7.6 Set Grupo de acesso autorizado a Pessoas	105
7.7 Configurações Avançadas	108
7.7.1 Configurar parâmetros do Terminal	108
7.7.2 Configurar permanecer Aberto/Fechado	114
7.7.3 Configurar autenticação Multipla	116
7.7.4 Configurar autenticação de Cartão no modo Agenda	118
7.7.5 Configurar primeira pessoa de acesso	120
7.7.6 Configurar Anti-Passback	121
7.7.7 Configurar Parâmetros do Terminal	122
7.8 Configurar ligação de ações para o Terminal	129
7.8.1 Configurar ações no Cliente para acesso aos eventos	129
7.8.2 Configurar ações do Terminal para acesso aos eventos	130
7.8.3 Configurar ações do terminal para Cartão Roubado	131
7.8.4 Configurar ações do Terminal por ID de pessoa	132
7.9 Controle de porta	133
7.9.1 Controle de status de porta.....	134
7.9.2 Verificar em tempo real as gravações de acesso	135
7.10 Central de eventos.....	135
7.10.1 Ativar recebimento de eventos do Terminal	136
7.10.2 Visualizar eventos em Tempo Real	136
7.10.3 Procurar Historico de eventos	138
7.11 Tempo e Atendimento	141
7.11.1 Configurar Parâmetros de atendimento	141
7.11.2 Adicionar calendário geral	147

7.11.3 Adicionar Troca	150
7.11.4 Gerenciar troca de Agenda	152
7.11.5 Corrigir Manualmente gravação de Entrada/Saida	156
7.11.6 Adicionar ausente e viagem a trabalho	157
7.11.7 Calcular dados de atendimento	159
7.11.8 Estatísticas de atendimento	160
7.12 Configurações Remota (Web)	163
7.12.1 Visualizar Informações do Terminal	163
7.12.2 Modificar Senha	164
7.12.3 Manutenção de data	165
7.12.4 Manutenção do Sistema.....	166
7.12.5 Configurar RS-485	167
7.12.6 Modo de segurança.....	168
7.12.7 Configurações de REDE.....	168
7.12.8 Configurações de envio de informações	169
7.12.9 Central de parâmetros de rede.....	169
7.12.10 Configurar SIP	169
7.12.11 Parâmetros de Relé.....	170
7.12.12 Configurar parâmetros de controle de acs	170
7.12.13 Configurar parâmetros do reconhecimento facial	171
7.12.14 Configurar parâmetros da Foto da face	172
7.12.15 Configurarar suplemento de Luz	173
7.12.16 Configurar numero do dispositivo	174
7.12.17 Configurar parâmetros de vide e audio.....	174
7.12.18 Configurar volume de entrada e saída	174
7.12.19 Operação do Relé	174
7.12.20 Visualizar status do Relé.....	175
A. Dicas ao coletar/comparar imagem facial	175
B. Dicas para ambiente de instalação	176
C. Dimensão	177

Capítulo 1 Visão geral

1.1 Visão Geral

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

1.2 Recursos

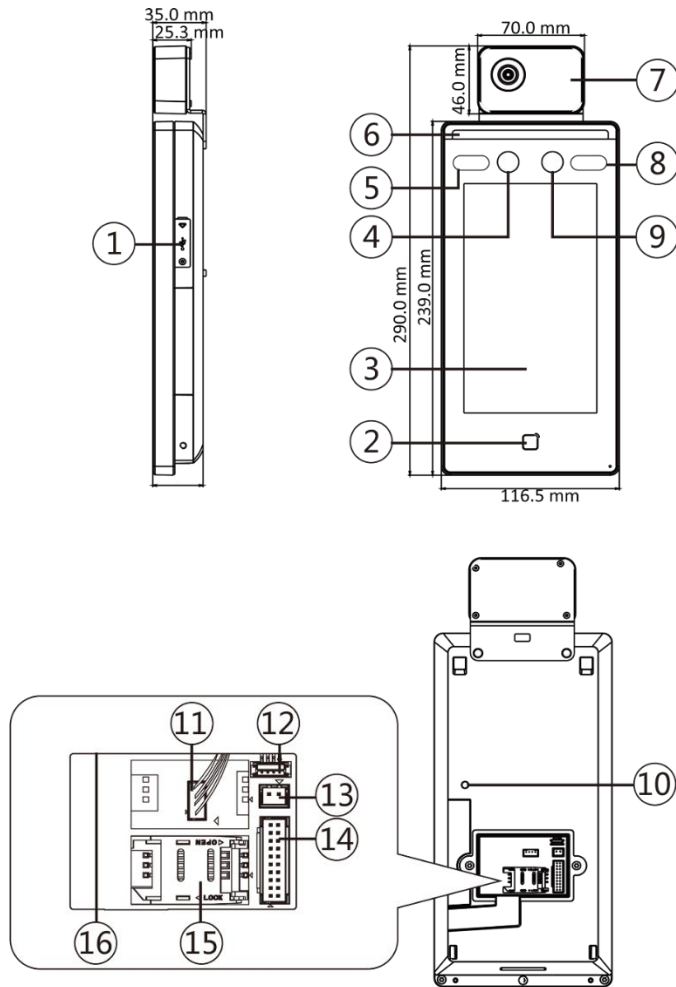
- Suporta sensor não resfriado de óxido de vanádio para medir a temperatura do alvo
- Faixa de medição de temperatura: 30 ° C a 45 ° C (86 ° F a 113 ° F), precisão: 0,1 ° C, desvio: ± 0,5 ° C
- Distância de reconhecimento: 0,3 a 1,8 m
- Modo rápido de medição de temperatura: Detecta o rosto e mede a temperatura da superfície da pele sem autenticação de identidade.
- Vários modos de autenticação estão disponíveis: cartão e temperatura, rosto e temperatura, cartão e rosto e temperatura, etc.
- Alerta de uso de máscara facial
Se o rosto que está reconhecendo não usar máscara, o dispositivo solicitará um lembrete de voz. Ao mesmo tempo, a autenticação ou presença é válida.
- Alerta forçado de uso de máscara
Se o rosto que está reconhecendo não usar máscara, o dispositivo solicitará um lembrete de voz. Ao mesmo tempo, a autenticação ou atendimento falhará.
- Exibe os resultados da medição de temperatura na página de autenticação
- Aciona prompt de voz ao detectar temperatura anormal
- Status de porta configurável (aberto / fechado) ao detectar temperatura anormal
- Transmite informações de temperatura online e offline para o software cliente via comunicação TCP / IP e salva os dados no software cliente
- Duração do reconhecimento facial < 0,2 s / Usuário; taxa de precisão de reconhecimento de rosto ≥ 99%
- Capacidade de 6.000 faces, capacidade de 6.000 cartões e capacidade de 100.000 eventos
- Altura sugerida para reconhecimento facial: entre 1,4 m e 1,9 m
- Suporta 6 status de presença, incluindo check in, check out, break in, break out, hora extra dentro, hora extra
- Design de vigilância e função de violação

Face Recognition Terminal User Manual

- Prompt de áudio para resultado de autenticação
- NTP, sincronização de tempo manual e sincronização automática
- Conecta-se a um controlador de acesso externo ou leitor de cartão Wiegand via protocolo Wiegand
- Conecta-se a uma unidade de controle de porta segura via protocolo RS-485 para evitar a abertura da porta quando o terminal é destruído
- Importa e exporta dados para o dispositivo do software cliente

Capítulo 2 Aparência

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

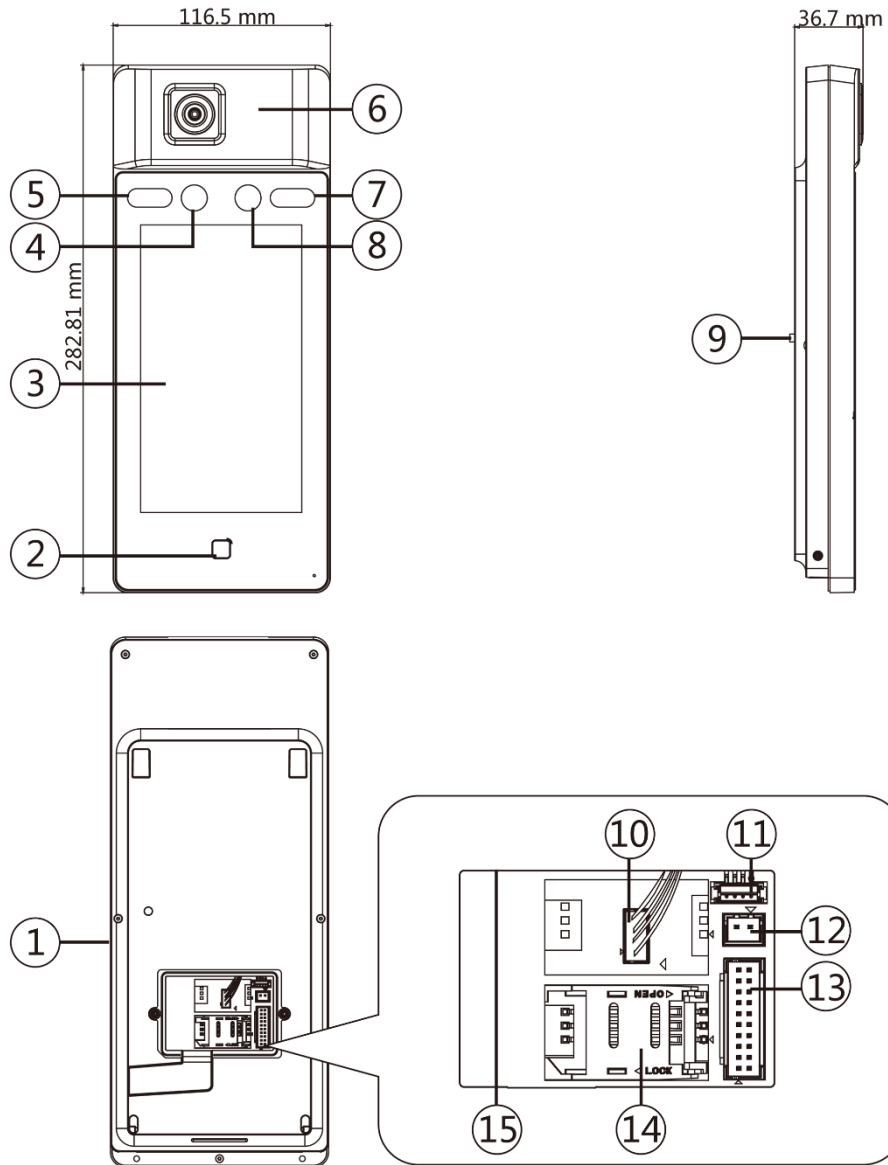


Não.	Nome
1	Interface USB
2	Área de passagem do cartão
3	Tela sensível ao toque
4	Câmera
5	IR Light
6	Luz branca

Face Recognition Terminal User Manual

N.º.	Nome
7	Módulo Termográfico
8	IR Light
9	Câmara
10	TAMPER
11	Interface do módulo termográfico
12	Porta de depuração
13	Interface de energia
14	Terminais de fiação
15	Slot para cartão PSAM (reservado)
16	Interface de rede

Face Recognition Terminal User Manual



No.	Name
1	Interface USB
2	Área de passagem do cartão
3	Tela sensível ao toque
4	Câmera
5	IR Light
6	Módulo Termográfico

Face Recognition Terminal User Manual

No.	Name
7	IR Light
8	Câmera
9	TAMPER
10	Interface do módulo termográfico
11	Porta de depuração
12	Interface de energia
13	Terminais de fiação
14	Slot para cartão PSAM (reservado)
15	Interface de rede

Figura 2-1 Diagrama do terminal de reconhecimento facial

Tabela 2-1 Descrição do terminal de reconhecimento facial

Capítulo 3 Instalação

3.1 Ambiente de Instalação

- Evite luz de fundo, luz solar direta e luz solar indireta.
- Para melhor reconhecimento, deve haver uma fonte de luz dentro ou perto do ambiente de instalação.
- A luz solar, o vento, o ar quente / frio do ar condicionado e outros fatores externos, que podem afetar a temperatura da superfície, criarão o desvio na medição da temperatura. Para obter um resultado preciso, certifique-se de que o dispositivo seja aplicado em ambientes internos e sem pensar (onde está relativamente isolado do ambiente externo). A temperatura de trabalho deve se manter entre 0 ° C e 50 ° C. Se não houver ambientes adequados para medição de temperatura (a área está voltada para o interior e conecta o exterior, a área na porta do ambiente interno, etc.), sugere-se construir um ambiente temporário de medição de temperatura.
- Fatores de influência da medição de temperatura:
 - Vento: O vento levará o calor embora, o que pode afetar o resultado da medição.
 - Suor: O suor tira o calor, o que pode afetar o resultado da medição.
 - Ar condicionado (ar frio): Se a temperatura interna for baixa, a temperatura da superfície também pode ser inferior à temperatura real, o que pode afetar o resultado da medição.
 - Ar condicionado (calor) ou aquecimento: Se a temperatura interna for alta, a temperatura da superfície também pode ser superior à temperatura real, o que pode afetar o resultado da medição.
- Para que o dispositivo funcione corretamente, você deve aguardar 30 minutos após ligá-lo.
- Para obter detalhes sobre o ambiente de instalação, consulte **Dicas para o ambiente de instalação**.

3.2 Montagem embutida

Passos

1. Instale uma caixa de distribuição.
2. Conecte o módulo termográfico e o corpo principal.

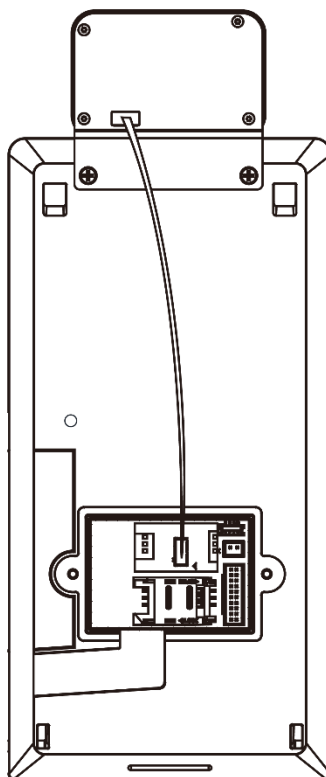


Figura 3-1 Conecte o módulo termográfico

3. Use os 5 parafusos fornecidos (4_KA4 × 22-SUS) para prender a placa de montagem na caixa de distribuição.
4. Passe o cabo pelo orifício do cabo da placa de montagem e conecte aos cabos dos dispositivos externos correspondentes.
5. Alinhe o dispositivo com a placa de montagem e pendure o dispositivo na placa de montagem. Certifique-se de que as duas folhas de cada lado da placa de montagem estejam nos slots na parte traseira do dispositivo

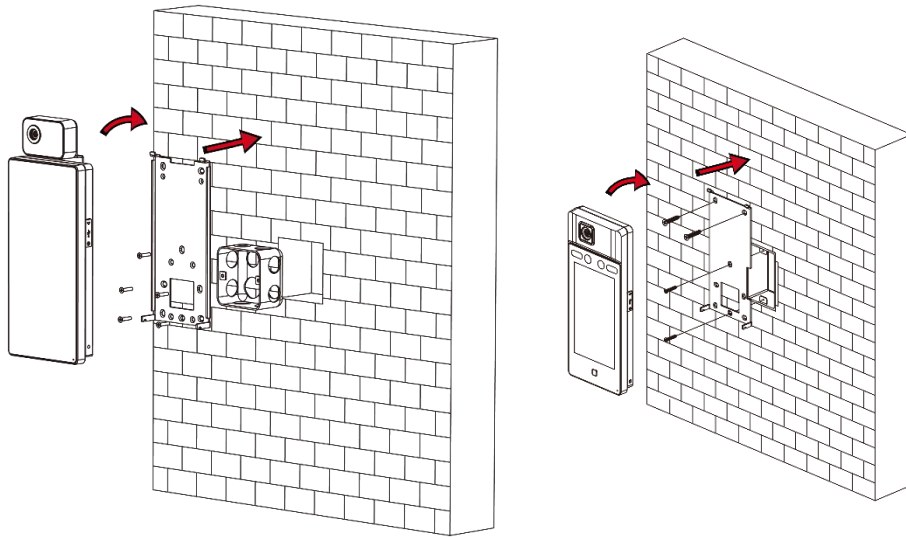


Figura 3-2 Instalar dispositivo

6. Use os 2 parafusos fornecidos (SC-M4 × 14,5TP10-SUS) para prender o dispositivo e a placa de montagem.
-

Nota

Quando a cabeça do parafuso está abaixo da superfície do dispositivo, o dispositivo está seguro.

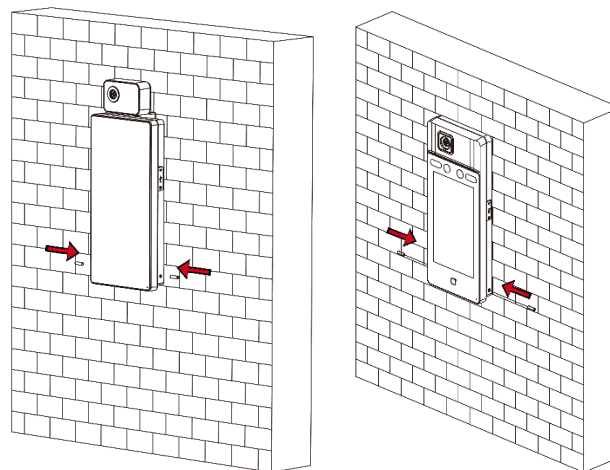


Figura 3-3 Dispositivo Seguro

Nota

- A altura de instalação aqui é a altura recomendada. Você pode alterá-lo de acordo com suas necessidades reais.
-

- Para uma instalação fácil, faça orifícios na superfície de montagem de acordo com o modelo de montagem fornecido.

3.3 Montagem em Superfície

Passos

1. De acordo com a linha de referência no gabarito de montagem, cole o gabarito de montagem na parede ou outra superfície, 1,4 metros acima do solo.

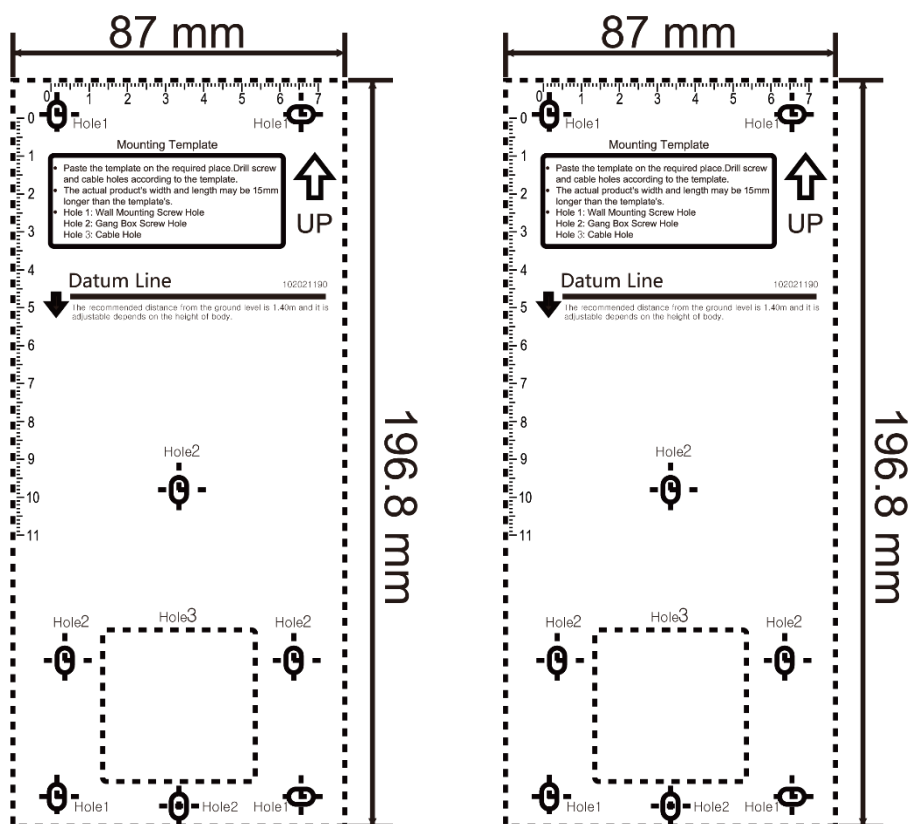


Figura 3-4 Modelo de montagem

2. Faça 5 furos na parede ou outra superfície de acordo com o modelo de montagem.
3. Insira os soquetes dos parafusos de ajuste nos orifícios perfurados.

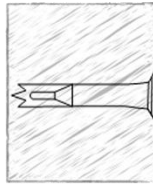


Figura 3-5 Insira o soquete do parafuso

4. Alinhe os 6 orifícios à placa de montagem com os orifícios perfurados.
5. Passe o cabo pelo orifício do cabo da placa de montagem e conecte aos cabos dos dispositivos externos correspondentes.
6. Alinhe o dispositivo com a placa de montagem e pendure o dispositivo na placa de montagem.

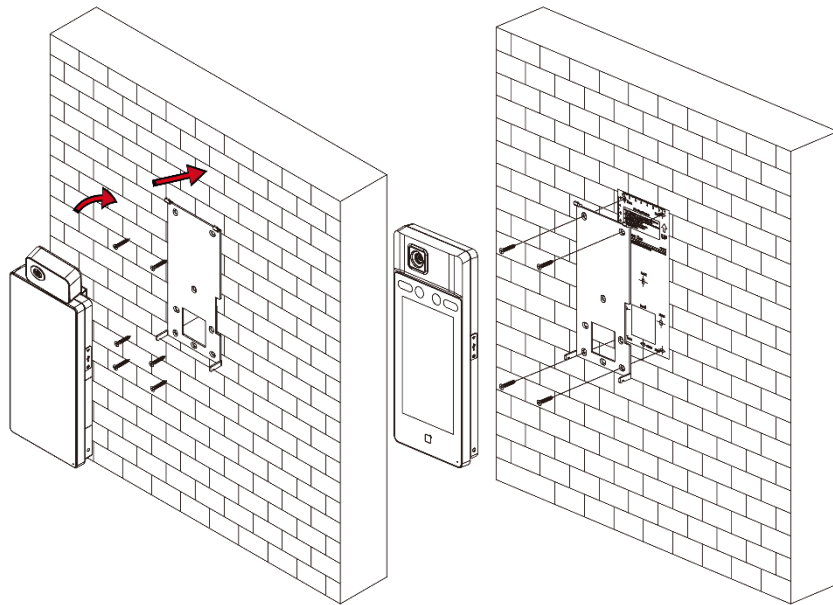


Figura 3-6 Instalar dispositivo

7. Use os 2 parafusos fornecidos (SC-M4 × 14,5TP10-SUS) para prender o dispositivo e a placa de montagem.

Nota

Quando a cabeça do parafuso está abaixo da superfície do dispositivo, o dispositivo está seguro.

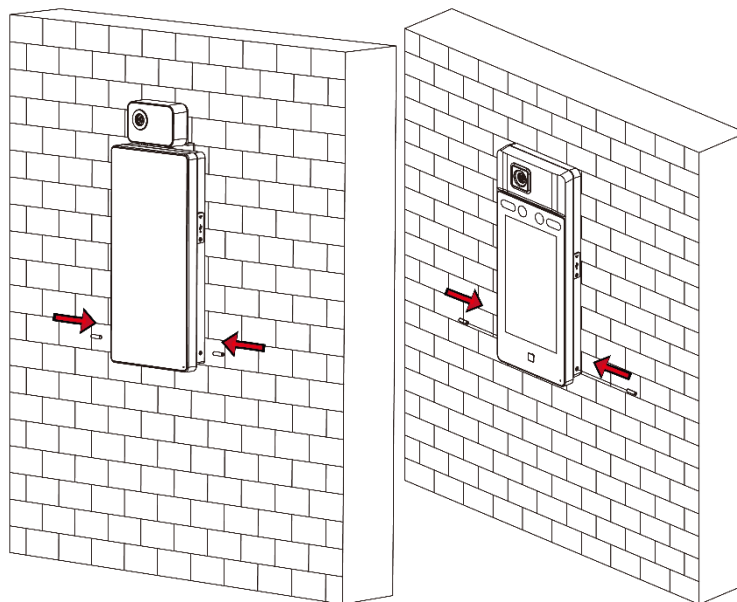


Figura 3-7 Dispositivo Seguro

Nota

- A altura de instalação aqui é a altura recomendada. Você pode alterá-lo de acordo com suas necessidades reais.
 - Para uma instalação fácil, faça orifícios na superfície de montagem de acordo com o modelo de montagem fornecido.
-

Capítulo 4 Fiação

Você pode conectar o terminal RS-485 com o leitor de cartão RS-485, conectar o terminal NC e COM com a fechadura da porta, conectar o terminal SENSOR com o contato da porta, o terminal BTN / GND com o botão de saída, conectar a saída de alarme e terminal de entrada com os dispositivos de saída / entrada de alarme e conectar o terminal Wiegand com o leitor de cartão Wiegand ou o controlador de acesso.

Se conectar o terminal 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 18 AWG, você deve usar uma fonte de alimentação de 12 V. E a distância entre a fonte de alimentação e o dispositivo não deve ser superior a 20 m.
 - Se o tamanho do cabo for 15 AWG, você deve usar uma fonte de alimentação de 12 V. E a distância entre a fonte de alimentação e o dispositivo não deve ser superior a 30 m.
 - Se o tamanho do cabo for 12 AWG, você deve usar uma fonte de alimentação de 12 V. E a distância entre a fonte de alimentação e o dispositivo não deve ser superior a 40 m.
-

4.1 Descrição do Terminal

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

O diagrama do terminal é o seguinte:

Face Recognition Terminal User Manual

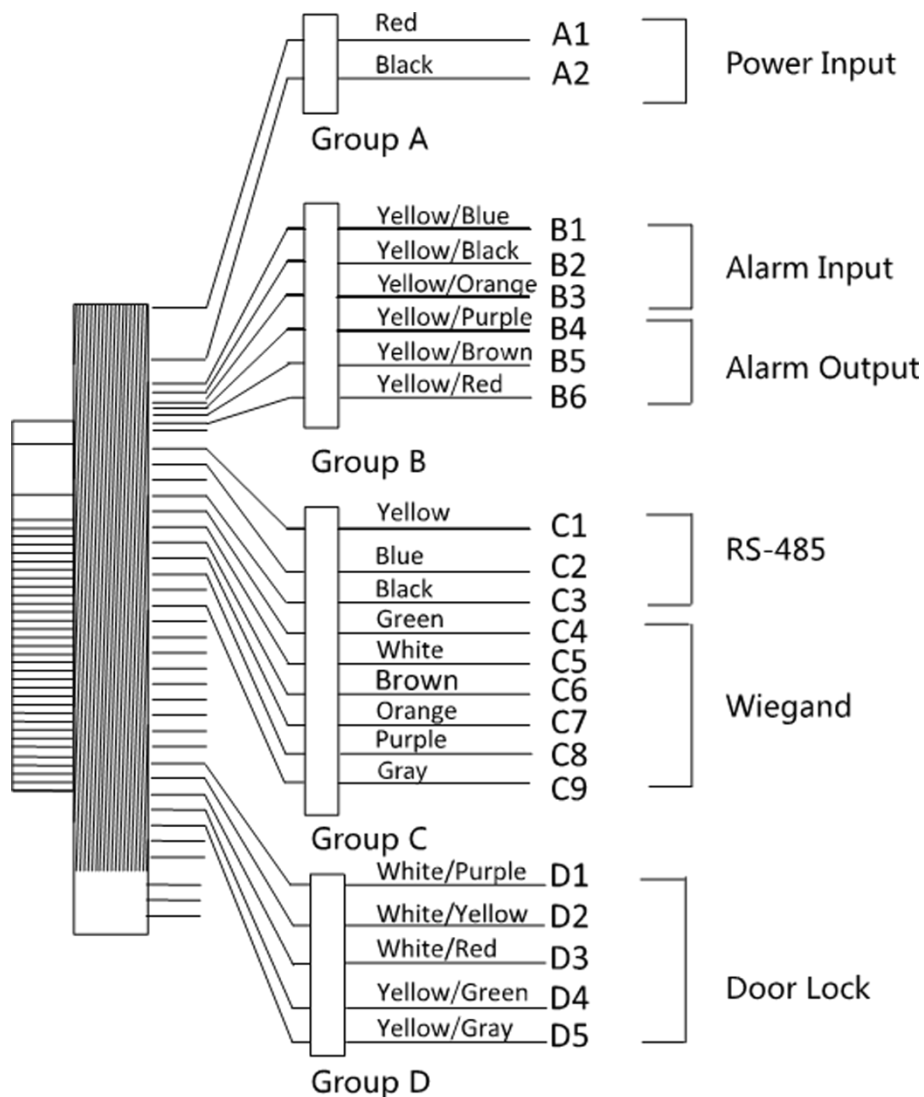


Figura 4-1 Diagrama do Terminal 671TM-3XF / A70

As descrições dos terminais são as seguintes:

Tabela 4-1 Descrições do terminal

Grupo	Não.	Função	Cor	Nome	Descrição
grupo A	A1	Entrada de energia	Vermelho	+12 V	Fonte de alimentação 12 VDC
	A2		Preto	GND	Terra
Grupo B	B1	Entrada de Alarme	Amarelo azul	EM 1	Entrada de Alarme 1

Face Recognition Terminal User Manual

Grupo	Não.	Função	Cor	Nome	Descrição
	B2		Amarelo / Preto	GND	Terra
	B3		Amarelo alaranjado	EM 2	Entrada de Alarme 2
	B4	Saída de Alarme	Amarelo / Roxo	NC	Fiação de saída de alarme
	B5		Amarelo marrom	COM	
	B6		Amarelo vermelho	NÃO	
Grupo C	C1	RS-485	Amarelo	485+	Fiação RS-485
	C2		Azul	485-	
	C3		Preto	GND	Terra
	C4	Wiegand	Verde	W0	Fiação Wiegand 0
	C5		Branco	W1	Fiação Wiegand 1
	C6		Castanho	WG_OK	Wiegand autenticado
	C7		laranja	WG_ERR	Falha na autenticação Wiegand
	C8		Roxa	BUZZER	Fiação da campainha
	C9		cinzento	TAMPER	Fiação de alarme de violação
Grupo D	D1	Fechadura da porta	Branco / Roxo	NC	Fiação de bloqueio (NC)
	D2		Branco amarelo	COM	Comum

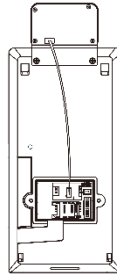
Face Recognition Terminal User Manual

Grupo	Não.	Função	Cor	Nome	Descrição
	D3		Branco / Vermelho	NÃO	Fiação de bloqueio (NO)
	D4		Amarelo verde	SENSOR	Contato da porta
	D5		Amarelo / cinza	BTN	Fiação da porta de saída

4.2 Dispositivo de fio normal

Você pode conectar o terminal com periféricos normais.

Siga o diagrama abaixo para conectar o módulo termográfico e o corpo principal do dispositivo:



O diagrama de fiação sem unidade de controle de porta segura é o seguinte.

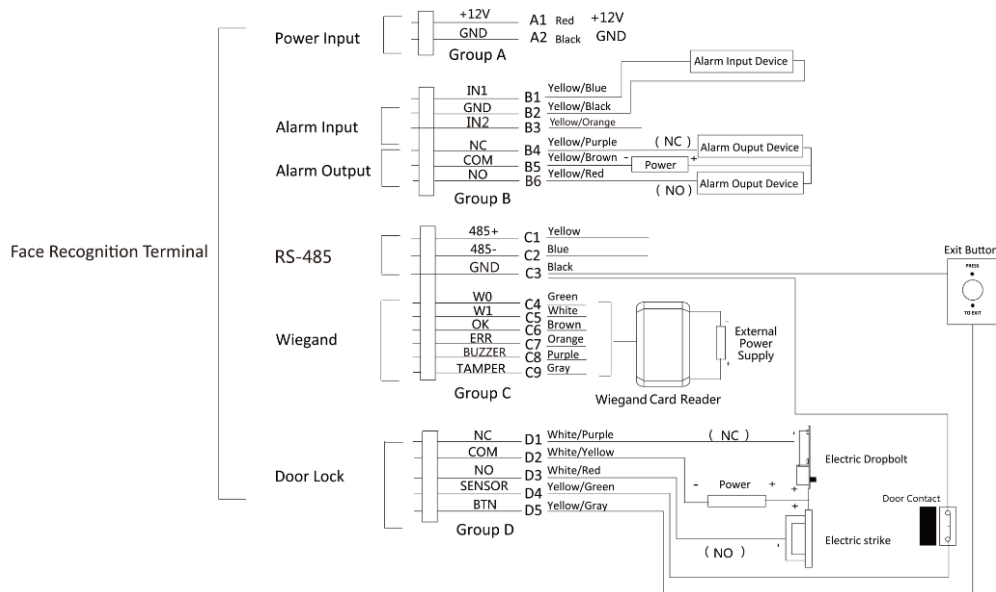


Figura 4-2 Fiação do dispositivo

Nota

- Você deve definir a direção Wiegand do terminal de reconhecimento de rosto como "Entrada" para se conectar a um leitor de cartão Wiegand. Se conectar a um controlador de acesso, você deve definir a direção do Wiegand como "Saída" para transmitir informações de autenticação para o controlador de acesso.
- Para obter detalhes sobre as configurações de direção do Wiegand, consulte *Definição dos parâmetros Wiegand nas configurações de comunicação*.
- A fonte de alimentação para o dispositivo deve ser 12 VDC / 2 A. A fonte de alimentação externa sugerida para a fechadura da porta é 12 V, 1 A. A fonte de alimentação externa sugerida para o leitor de cartão Wiegand é 12 V, 1A.

Face Recognition Terminal User Manual

- O diâmetro do cabo de alimentação sugerido: 22 AWG. O diâmetro do outro cabo sugerido: 26 AWG.
- Não conecte o dispositivo diretamente à fonte de alimentação.

Aviso

O terminal de reconhecimento facial deve adaptar uma fonte de alimentação externa de Classe 2 listada com função protegida contra sobretensão.

4.3 Unidade de Controle de Porta Segura de Fio

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

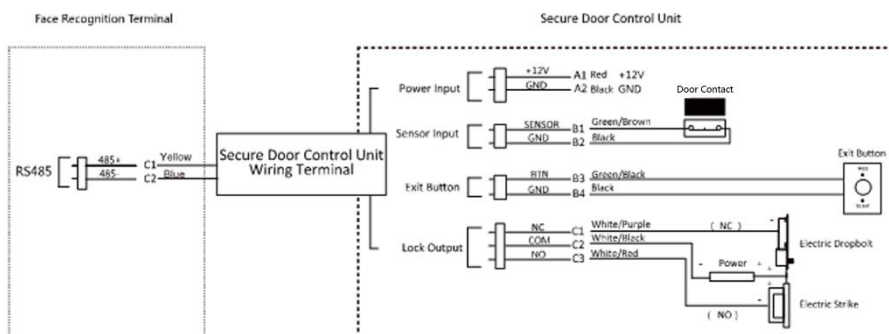


Figura 4-3 Fiação da Unidade de Controle de Porta Segura

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 12 V, 0,5 A.

4.4 Módulo de incêndio de fio

4.4.1 Diagrama de fiação da porta aberta ao desligar

Tipo de bloqueio: âncora, bloqueio magnético e parafuso elétrico (NO)

Tipo de segurança: porta aberta ao desligar

Cenário: Instalado em Acesso via Fire Engine

Tipo 1

Face Recognition Terminal User Manual

Nota

O sistema de incêndio controla o fornecimento de energia do sistema de controle de acesso.

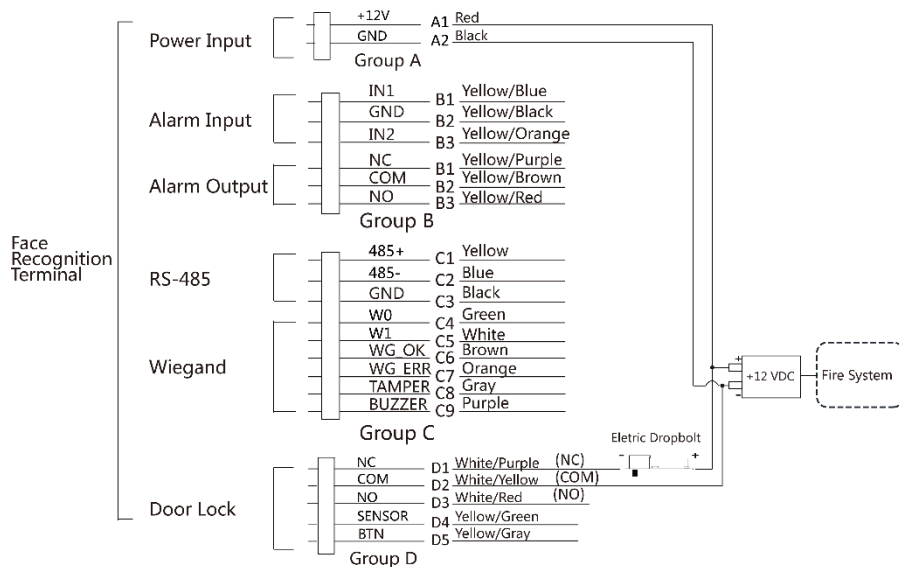


Figura 4-4 Dispositivo de fio

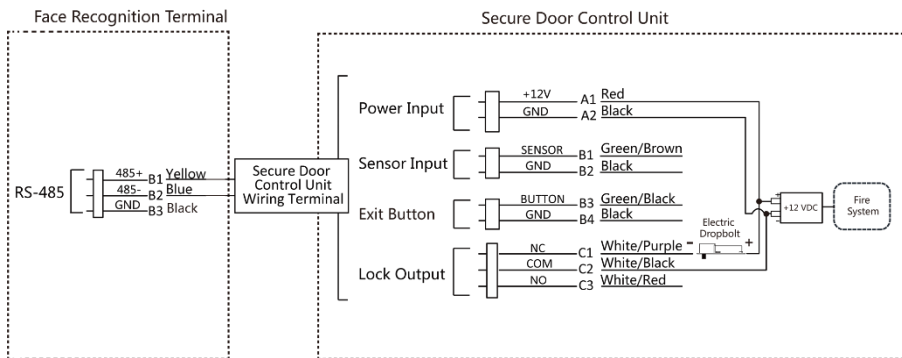


Figura 4-5 Unidade de controle de porta segura com fio

Tipo 2

Nota

O sistema de incêndio (NO e COM, normalmente aberto 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, NO e COM estão fechados.

Face Recognition Terminal User Manual

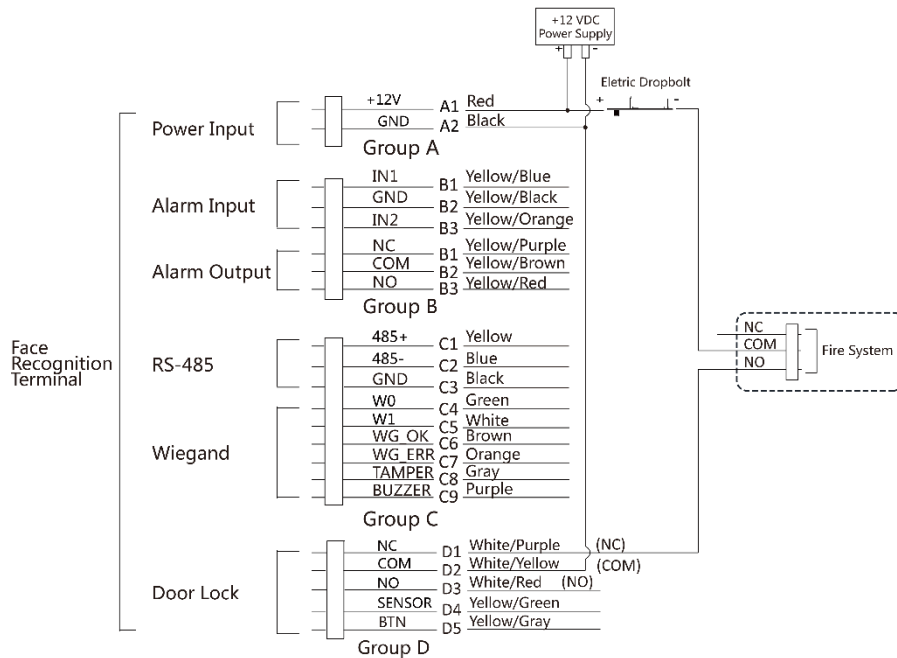


Figura 4-6 Dispositivo de fiação

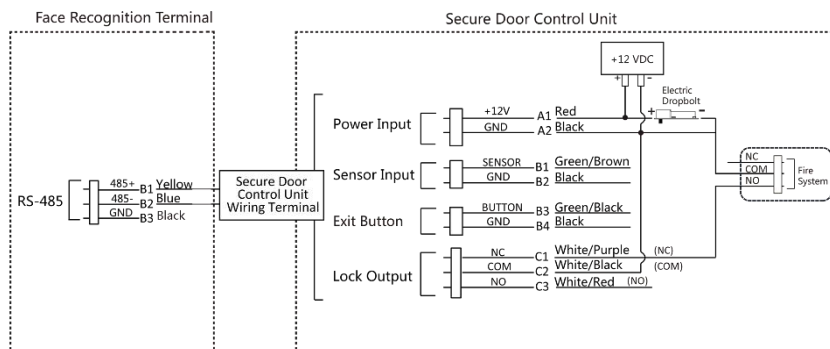


Figura 4-7 Fiação da Unidade de Controle de Porta Segura

4.4.2 Diagrama de fiação da porta trancada ao desligar

Tipo de bloqueio: bloqueio catódico, bloqueio elétrico e parafuso elétrico (NC)

Tipo de segurança: porta trancada ao desligar

Cenário: Instalado na Entrada / Saída com Rede de Incêndio

Nota

- O Uninterpretable Power Supply (UPS) é necessário.
- O sistema de incêndio (NC e COM, normalmente fechado ao desligar) está conectada 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.

Face Recognition Terminal User Manual

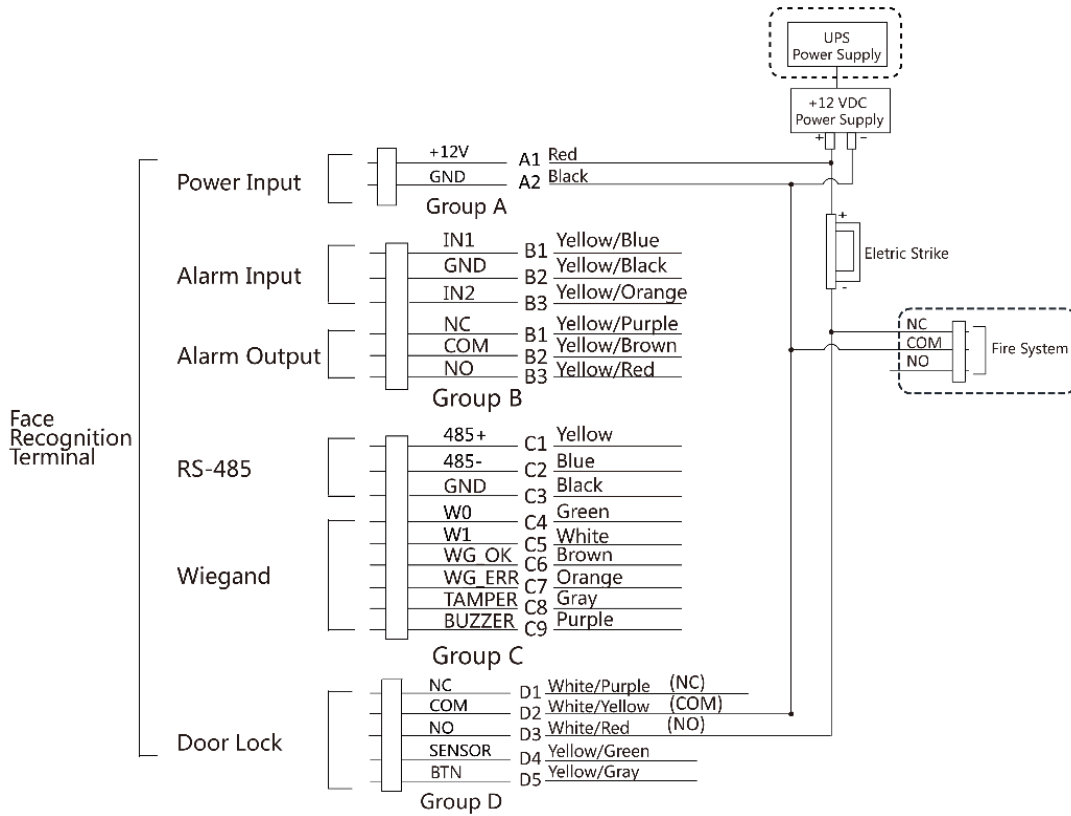


Figura 4-8 Fiação do dispositivo

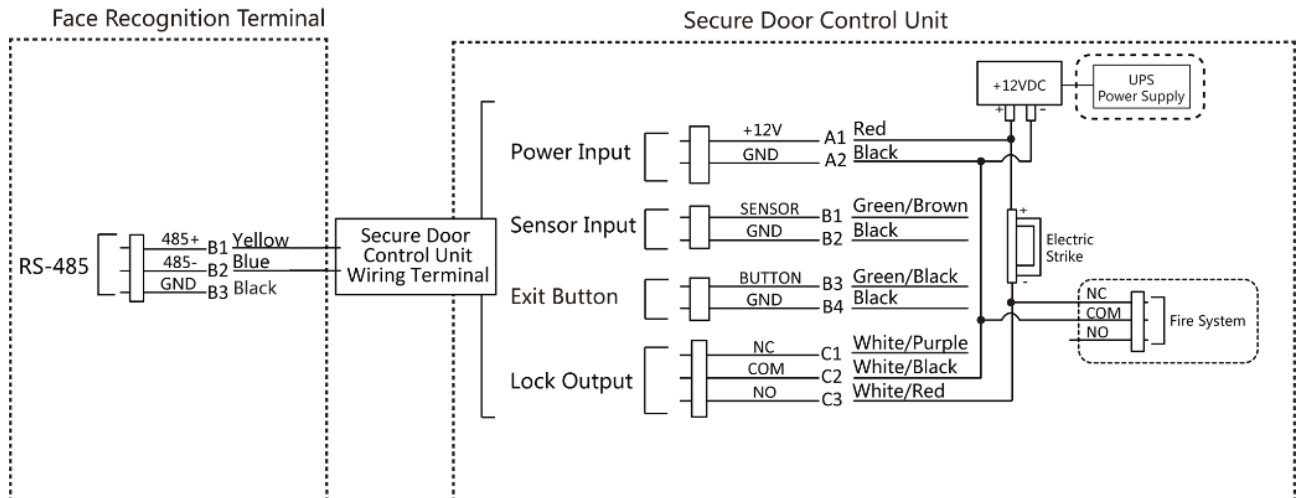


Figura 4-9 Diagrama de fiação

Capítulo 5 Ativação

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

A ativação através do dispositivo, ferramenta SADP e o software cliente são suportados.

Os valores padrão do dispositivo são os seguintes:

- O endereço IP padrão: 192.0.0.64
- O número da porta padrão: 8000
- O nome de usuário padrão: admin

5.1 Ativar via dispositivo

Se o dispositivo não estiver ativado, você poderá ativá-lo após ligá-lo.

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

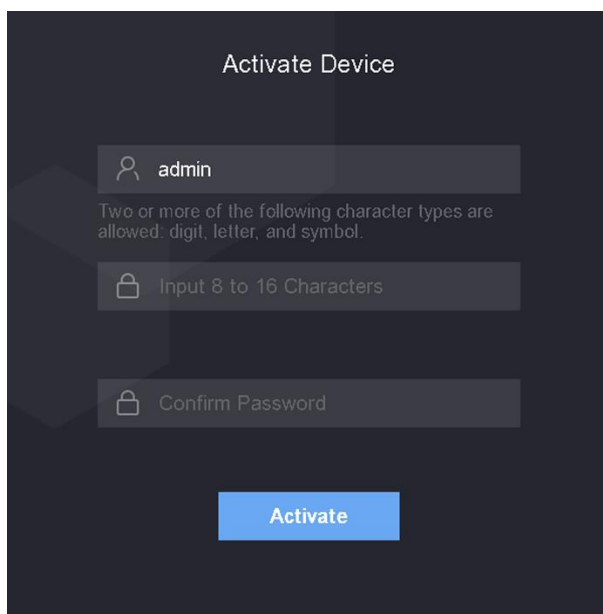


Figura 5-1 Página de ativação

Cuidado

A força da senha do dispositivo pode ser verificada automaticamente. É altamente recomendável que você altere a senha de sua escolha (usando no mínimo 8 caracteres, incluindo pelo menos três tipos das seguintes categorias: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança de sua produtos. E recomendamos

Face Recognition Terminal User Manual

que você altere sua senha regularmente, principalmente no sistema de alta segurança, alterando a senha mensal 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.

- Após a ativação, você deve selecionar um modo de aplicativo. Para obter detalhes, consulte ***Definir modo de aplicativo***
- Após a ativação, se precisar adicionar o dispositivo ao software cliente ou outras plataformas, você deve editar o endereço IP do dispositivo. Para obter detalhes, consulte *Configurações de comunicação* .

5.2 Ativar via SADP

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

Antes que você comece

- Obtenha o software SADP no disco fornecido ou no site oficial <http://www.hikvision.com/en/> e instale o SADP de acordo com as instruções.
- O dispositivo e o PC que executa a ferramenta SADP devem estar na mesma sub-rede.

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

Passos

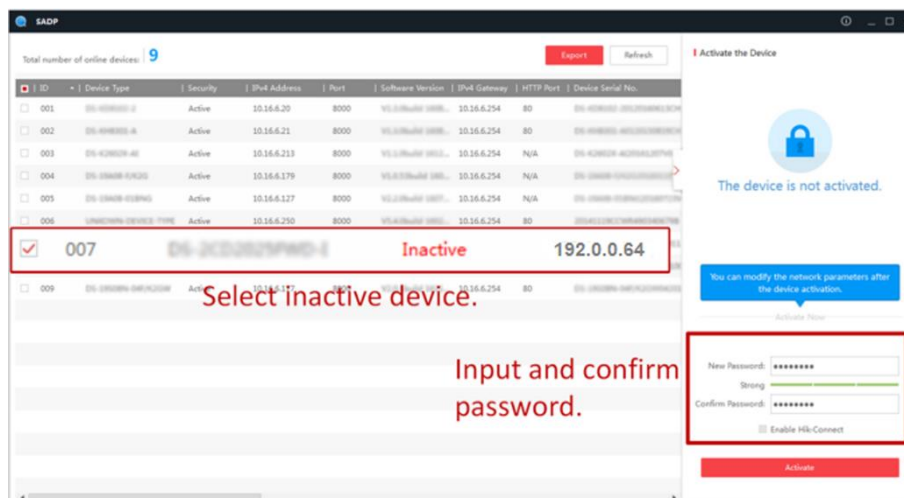
1. Execute o software SADP e pesquise os dispositivos online.
 2. Encontre e selecione seu dispositivo na lista de dispositivos online.
 3. Insira a nova senha (senha de administrador) e confirme a senha.
-

Cuidado

SENHA FORTE RECOMENDADA - Recomendamos enfaticamente que você crie uma senha forte de sua escolha (usando no mínimo 8 caracteres, incluindo letras maiúsculas, 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.

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

Face Recognition Terminal User Manual



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

5. Modifique o endereço IP do dispositivo.

- 1) Selecione o dispositivo.
- 2) Mude o endereço IP do dispositivo para a mesma sub-rede do seu computador, modificando o endereço IP manualmente ou marcando **Habilitar DHCP**.
- 3) Insira a senha do administrador e clique em **Modificar** para ativar a modificação do endereço IP.

5.3 Ativar Dispositivo por Software Cliente

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

Passos

Nota

Esta função deve ser suportada pelo dispositivo.

1. Acesse a 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

Face Recognition Terminal User Manual

A força da senha do dispositivo pode ser verificada automaticamente. É altamente recomendável que você altere a senha de sua escolha (usando no mínimo 8 caracteres, incluindo pelo menos três tipos das seguintes categorias: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança de sua produtos. E recomendamos que você altere sua senha regularmente, principalmente no sistema de alta segurança, alterando a senha mensal 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.

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

Capítulo 6 Operação Básica

6.1 Definir modo de aplicação

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

Passos

1. Na página de Boas-vindas, selecione **Interno** ou **Outros** na lista suspensa.

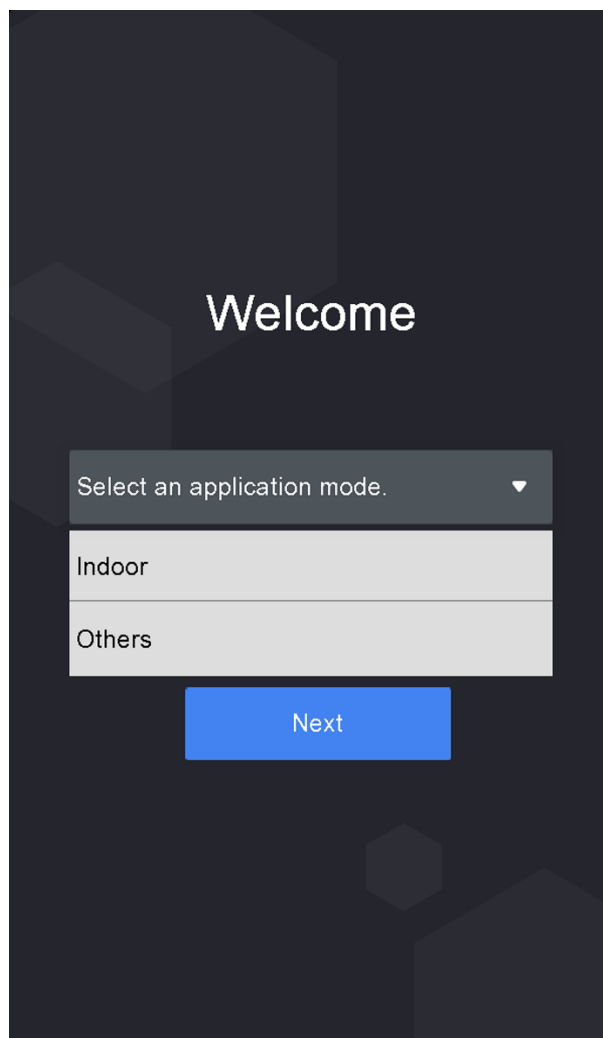


Figura 6-1 Página de boas-vindas

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

Nota

- Você também pode alterar as configurações em *Configurações do sistema* .
 - Se você instalar o dispositivo em um ambiente interno próximo à janela ou a função de reconhecimento de rosto não estiver funcionando bem, selecione **Outros** .
 - Se você não configurar o modo do aplicativo e tocar em **Avançar** , o sistema selecionará **Interno** por padrão.
 - Se você ativar o dispositivo por meio de outras ferramentas remotamente, o sistema selecionará **Interno** como o modo de aplicativo por padrão.
-

6.2 Login

Faça login no dispositivo para definir os parâmetros básicos do dispositivo. Você deve inserir a senha de ativação do dispositivo para o primeiro login. Ou, se você adicionou a credencial de administrador, pode fazer o login por meio da credencial configurada.

6.2.1 Login pela primeira vez

Você deve fazer o login no sistema antes de outras operações do dispositivo.

Passos

1. Dê um toque longo na página inicial por 3 s para entrar na página de entrada de senha.
2. Toque no campo Senha e insira a senha de ativação do dispositivo.
3. Toque em **OK** para entrar na página inicial.

Nota

- O dispositivo será bloqueado por 30 minutos após 5 tentativas de senha malsucedidas.
 - Para obter detalhes sobre como configurar o modo de autenticação do administrador, consulte *Adicionar usuário* .
-

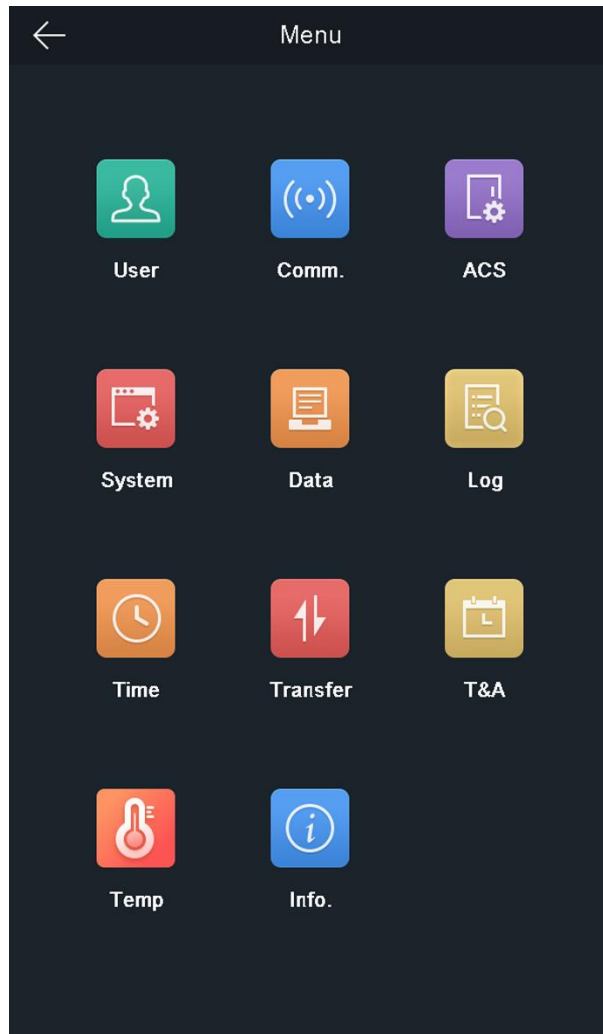


Figura 6-2 Página inicial

6.2.2 Login do Administrador

Depois de adicionar o administrador para o dispositivo, apenas o administrador pode fazer login no dispositivo para operação do dispositivo.

Passos

1. Toque longamente na página inicial por 3 s para entrar na página de login do administrador.

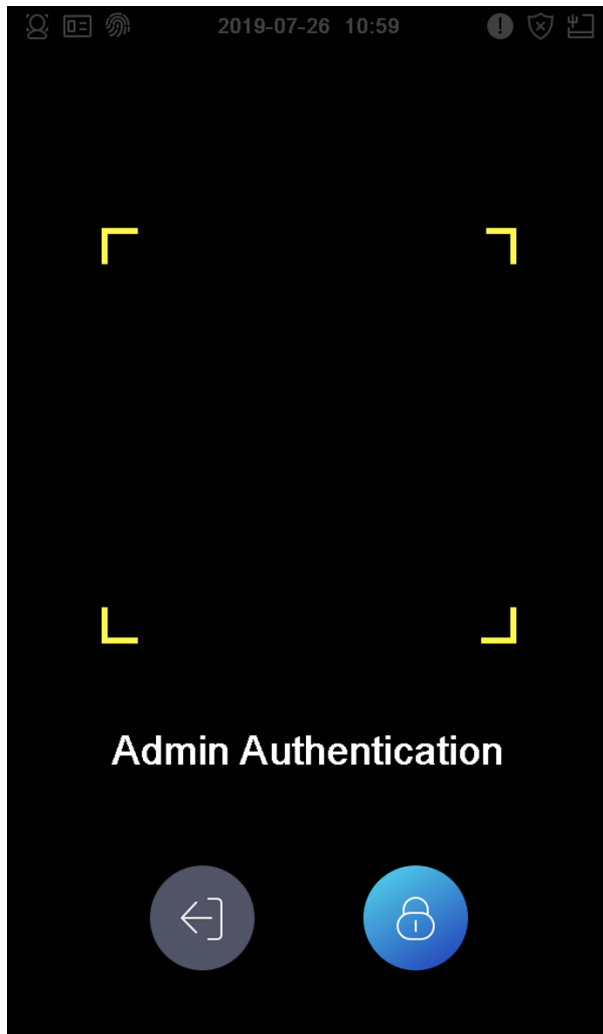


Figura 6-3 Login de administrador

2. Autentique o rosto ou cartão do administrador para entrar na página inicial.

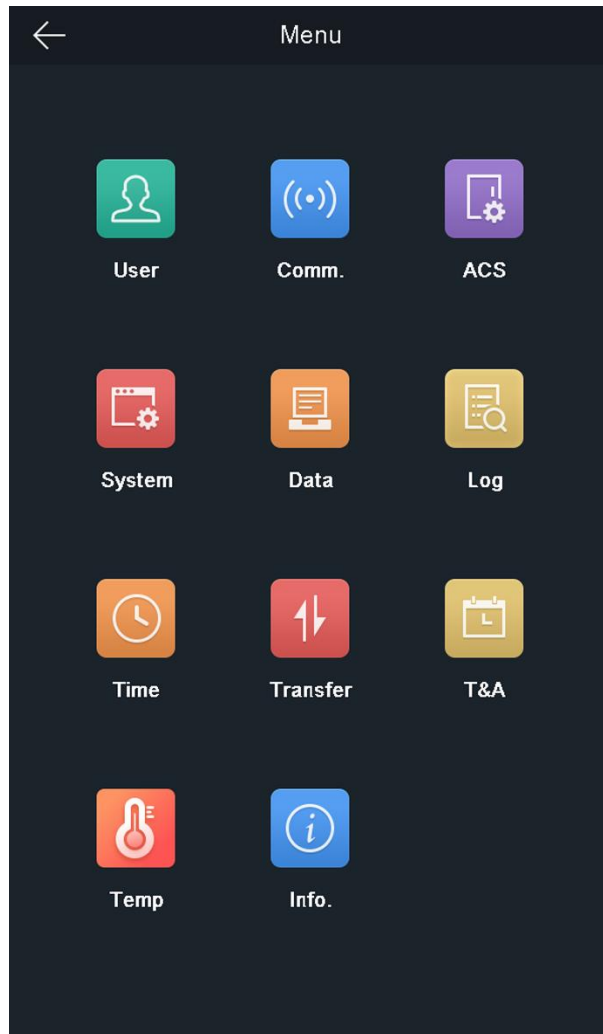




Figura 6-4 Página inicial

Nota

O dispositivo será bloqueado por 30 minutos após 5 tentativas falhas de rosto ou cartão.

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.

6.3 Configurações de comunicação

Você pode definir os parâmetros de rede, os parâmetros RS-485 e os parâmetros Wiegand na página de configurações de comunicação.

6.3.1 Definir parâmetros de rede

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

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** para entrar na guia Rede.

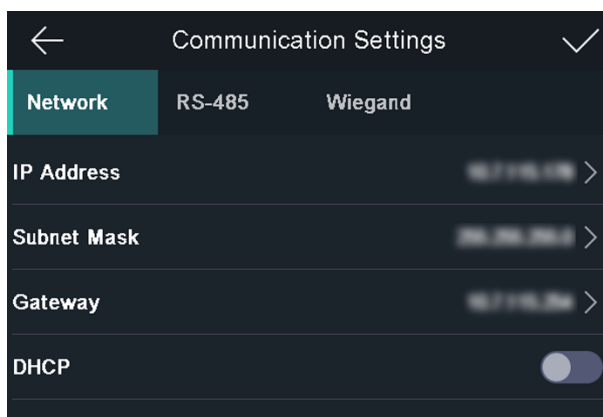


Figura 6-5 Configurações de rede

3. Toque em Endereço IP, Máscara de sub-rede ou Gateway e insira os parâmetros.
4. Toque em **OK** para salvar as configurações.

Nota

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

5. Toque **OK** para salvar os parâmetros de rede.

6.3.2 Definir os Parâmetros RS-485

O terminal de reconhecimento de face pode conectar controlador de acesso externo, unidade de controle de porta segura ou leitor de cartão por meio do terminal RS-485.

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 **RS-485** para entrar na guia RS-485.

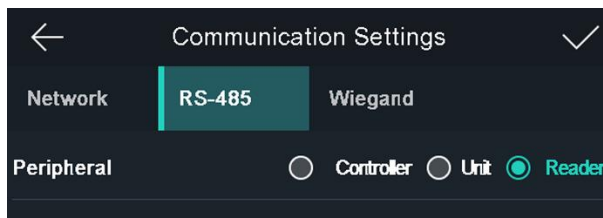



Figura 6-6 Definir parâmetros RS-485

3. Selecione um tipo de periférico de acordo com suas necessidades reais.

Nota

- O controlador representa o controlador de acesso, a unidade representa a unidade de controle da porta segura e o leitor representa o leitor de cartão.
- Se você selecionar **Controlador** : Se conectar o dispositivo a um terminal por meio 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 nº da porta

4. Toque  para salvar os parâmetros de rede.

Nota

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

6.3.3 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.

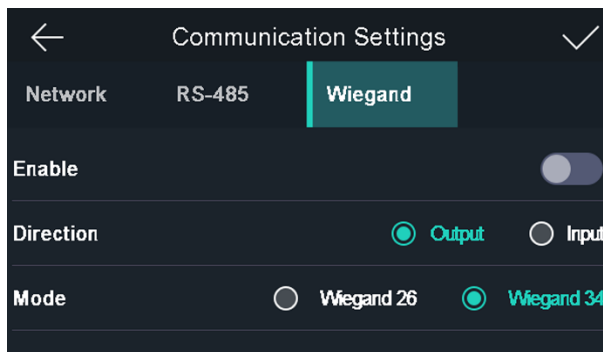



Figura 6-7 Configurações de Wiegand

3. Ative a função Wiegand.
 4. Selecione uma direção de transmissão.
 - Saída: um terminal de reconhecimento de rosto pode conectar um controlador de acesso externo. E os dois dispositivos vão transmitir o nº do cartão via Wiegand 26 ou Wiegand 34.
 - Entrada: Um terminal de reconhecimento de rosto pode conectar um leitor de cartão Wiegand.
 5. Toque  para salvar os parâmetros de rede.
-

Nota

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

6.4 Gerenciamento de usuários

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

6.4.1 Adicionar Administrador

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

Passos

1. Dê um toque longo na página inicial e faça login no backend.
 2. Toque em **Usuário** → + para entrar na página Adicionar usuário.
 3. Edite a ID do funcionário.
-

Nota

- A ID do funcionário deve ter menos de 32 caracteres. E pode ser uma combinação de letras minúsculas, maiúsculas e números.
 - A ID do funcionário não deve ser duplicada.
-

4. Toque no campo Nome e insira o nome do usuário no teclado virtual.
-

Nota

- Números, letras maiúsculas, letras minúsculas e caracteres especiais são permitidos no nome do usuário.
-

Face Recognition Terminal User Manual

- São permitidos até 32 caracteres no nome do usuário.
-

5. Opcional: adicione uma imagem de rosto, cartões ou senha para o administrador.

Nota

- Para obter detalhes sobre como adicionar uma foto de rosto, consulte [**Adicionar foto de rosto**](#) .
 - Para obter detalhes sobre como adicionar um cartão, consulte [**Adicionar cartão**](#) .
 - Para obter detalhes sobre como adicionar uma senha, consulte [**Adicionar senha**](#) .
-

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. Ative a função de permissão do administrador.

Habilitar permissão de administrador

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

8. Toque para salvar as configurações.

6.4.2 Adicionar imagem de rosto

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

Passos

1. Dê um toque longo na página inicial e faça login no backend.
 2. Toque em **Usuário** → + para entrar na página Adicionar usuário.
 3. Edite a ID do funcionário.
-

Nota

- A ID do funcionário deve ter menos de 32 caracteres. E pode ser uma combinação de letras minúsculas, maiúsculas e números.
 - A ID do funcionário não deve ser duplicada.
-

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

Nota

Face Recognition Terminal User Manual

- Números, letras maiúsculas, letras minúsculas e caracteres especiais são permitidos no nome do usuário.
 - São permitidos até 32 caracteres no nome do usuário.
-

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

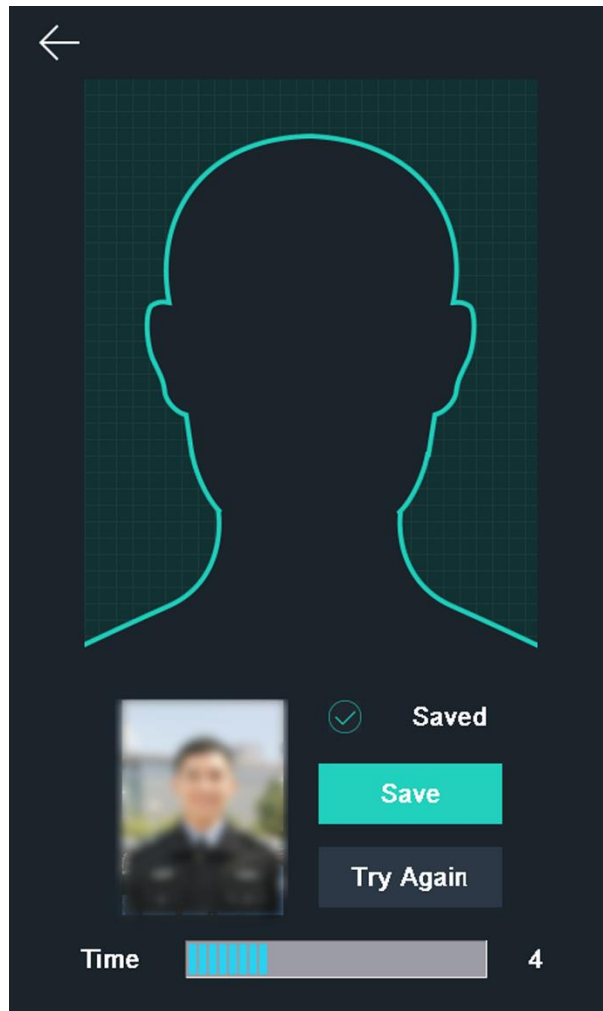


Figura 6-8 Adicionar imagem de rosto

6. Posicione seu rosto olhando para a câmera.

Nota

- Certifique-se de que a imagem do seu rosto está no contorno da imagem do rosto ao adicioná-la.
- Certifique-se de que a foto do rosto capturada é de boa qualidade e precisa.
- Para obter detalhes sobre as instruções sobre como adicionar fotos de rostos, consulte *Dicas ao coletar / comparar fotos de rostos*.

Face Recognition Terminal User Manual

Depois de adicionar completamente a imagem do rosto, uma imagem capturada do rosto 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.
-

Nota

A duração máxima para adicionar uma foto de rosto é 15s. Você pode verificar o tempo restante para adicionar uma foto de rosto à esquerda da página.

9. Ative ou desative a função de permissão do administrador.

Habilitar permissão de administrador

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

Desativar permissão de administrador

O usuário é o usuário normal. O usuário só pode se autenticar ou atender na página inicial.

10. Toque para salvar as configurações.

6.4.3 Adicionar Cartão

Adicione um cartão para o usuário e o usuário pode se autenticar por meio do cartão adicionado.

Passos

1. Dê um toque longo na página inicial e faça login no backend.
 2. Toque em **Usuário** → + para entrar na página Adicionar usuário.
 3. Toque em ID do funcionário. campo e edite o ID do funcionário.
-

Nota

- A ID do funcionário deve ter menos de 32 caracteres. E pode ser uma combinação de letras minúsculas, maiúsculas e números.
 - A ID do funcionário não deve ser duplicada.
-

4. Toque no campo Nome e insira o nome do usuário no teclado virtual.
-

Nota

- Números, letras maiúsculas, letras minúsculas e caracteres especiais são permitidos no nome do usuário.
 - São permitidos até 32 caracteres no nome do usuário.
-

Face Recognition Terminal User Manual

5. Toque no campo Cartão e insira o nº do cartão

6. Configure o número do cartão

Insira o nº do cartão manualmente. Passe o cartão sobre a área de deslizamento do cartão para obter o número do cartão

Nota

- O nº do cartão não pode estar vazio.
 - São permitidos até 20 caracteres no número do cartão
 - O nº do cartão não pode ser duplicado.
-

7. Opcional: ative a função Cartão de coação. O cartão adicionado

Quando o usuário se autentica passando este cartão de coação, o dispositivo carrega um evento de cartão de coação para o software cliente.

8. Ative ou desative a função de permissão do administrador.

Habilitar permissão de administrador

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

Desativar permissão de administrador

O usuário é o usuário normal. O usuário só pode se autenticar ou atender na página inicial.

9. Toque para salvar as configurações.

6.4.4 Adicionar senha

Adicione uma senha para o usuário e o usuário poderá se autenticar por meio da senha.

Passos

1. Dê um toque longo na página inicial e faça login no backend.
 2. Toque em **Usuário** → + para entrar na página Adicionar usuário.
 3. Toque em ID do funcionário. campo e edite o ID do funcionário.
-

Nota

- A ID do funcionário deve ter menos de 32 caracteres. E pode ser uma combinação de letras minúsculas, maiúsculas e números.
 - A ID do funcionário não deve ser duplicada.
-

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

Nota

- Números, letras maiúsculas, letras minúsculas e caracteres especiais são permitidos no nome do usuário.
 - São permitidos até 32 caracteres no nome do usuário.
-

5. Toque no campo Senha, crie uma senha e confirme a senha.
-

Nota

- Somente números são permitidos na senha.
 - São permitidos até 8 caracteres na senha.
-

6. Ative ou desative a função de permissão do administrador.

Habilitar permissão de administrador

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

Desativar permissão de administrador

O usuário é o usuário normal. O usuário só pode se autenticar ou atender na página inicial.

7. Toque para salvar as configurações.

6.4.5 Definir modo de autenticação

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

Passos

1. Dê um toque longo na página inicial e faça login no backend.
2. Toque em **Usuário** → **Adicionar usuário / Editar usuário** → **Modo de autenticação** .
3. Selecione Dispositivo ou Personalizado como o modo de autenticação.

Dispositivo

Se você deseja selecionar o modo do dispositivo, deve primeiro definir o modo de autenticação do terminal na página Configurações de controle de acesso. Para obter detalhes, consulte *Definição de parâmetros de controle de acesso* .

personalizadas


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

4. Toque para salvar as configurações.
-


6.4.6 Pesquisar e Editar Usuário

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

Pesquisar usuário

Na página Gerenciamento de usuário, 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 a ID do funcionário, o número do cartão ou o nome de usuário para pesquisa. Toque  procurar.

Editar usuário

Na página Gerenciamento de usuários, selecione um usuário da 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

O ID do funcionário não pode ser editado.

6.5 Medição de Temperatura

6.5.1 Configurações de medição de temperatura

Você pode definir os parâmetros de medição de temperatura, incluindo detecção de temperatura, limite de alarme de superaquecimento, compensação de temperatura, porta não aberta quando a temperatura é anormal, modo de medição de temperatura, unidade de temperatura, calibração de área de medição, área de medição, corpo preto, etc.

Na página inicial, toque em **Temp** (temperatura) para entrar na página Configurações de temperatura. Edite os parâmetros de medição de temperatura nesta página e toque em  para salvar as configurações.

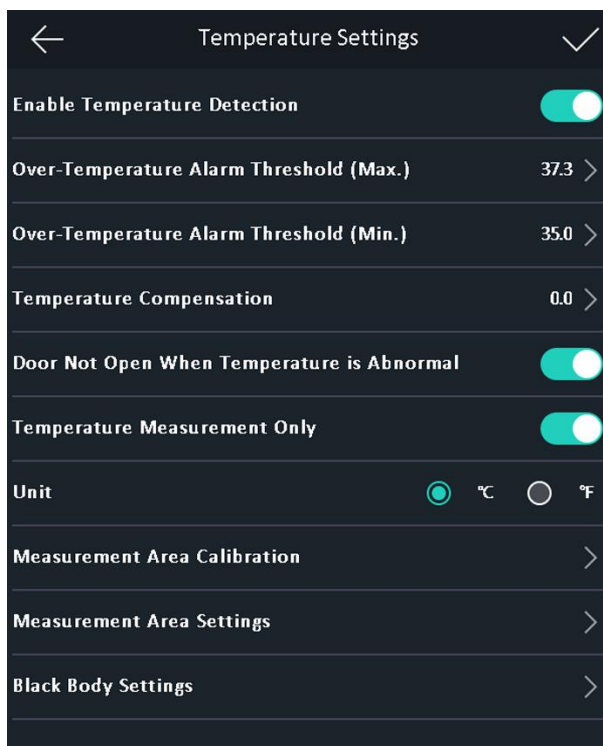


Figura 6-9 Parâmetros de medição de temperatura

As descrições dos parâmetros disponíveis são as seguintes:

Tabela 6-1 Descrições dos parâmetros de medição de temperatura

Parâmetro	Descrição
Habilitar detecção de temperatura	Ao habilitar a função, o aparelho irá autenticar as permissões e ao mesmo tempo medir a temperatura. Ao desativar o dispositivo, o dispositivo autenticará apenas as permissões.
Limite de alarme de superaquecimento (máx. / Min.)	Edite o limite de acordo com a situação real. Se a temperatura detectada for superior ou inferior aos parâmetros configurados, um alarme será acionado. Por padrão, o valor é 37,3 °.
Compensação de Temperatura	Se a temperatura medida for maior / menor que a temperatura real do objeto, você pode definir a temperatura de compensação aqui. Faixa disponível: -99 ° C a 99 ° C
Porta não aberta quando a temperatura está anormal	Ao habilitar a função, a porta não abrirá quando a temperatura detectada for superior ou inferior ao limite de temperatura configurado. Por padrão, a função está habilitada.

Face Recognition Terminal User Manual

Parâmetro	Descrição
Medição de temperatura apenas	Ao habilitar a função, o aparelho não irá autenticar as permissões, apenas medirá a temperatura. Ao desabilitar a função, o aparelho irá autenticar as permissões e ao mesmo tempo medir a temperatura.
Unidade	Selecione uma unidade de temperatura de acordo com sua preferência.
Calibração da área de medição / Configurações da área de medição	Configure a área de medição de temperatura e os parâmetros de correção.
Configurações de corpo negro	<p>Ao habilitar a função, você pode configurar os parâmetros do corpo negro, incluindo distância, temperatura e emissividade.</p> <hr/> <p>Nota</p> <p>Ao medir o corpo preto, certifique-se de que a câmera do dispositivo esteja voltada para o corpo preto e que não haja outros objetos entre o corpo preto e a câmera. Uma vez que o corpo preto da amostra é calibrado, certifique-se de que a área de medição do corpo preto de medição deve ser a mesma que o calibrado, ou a medição da temperatura pode falhar.</p> <hr/>

6.5.2 Configurações de corpo negro

O corpo negro pode corrigir a temperatura de medição. Você deve definir os parâmetros do corpo negro se a cena de medição da temperatura do corpo negro for necessária. Se nenhum corpo preto ruim for necessário, não defina os parâmetros do corpo preto, ou a temperatura pode não corrigir.

Passos

Nota

Ao medir o corpo preto, certifique-se de que a câmera do dispositivo esteja voltada para o corpo preto e que não haja outros objetos entre o corpo preto e a câmera. Uma vez que o corpo preto da amostra é calibrado, certifique-se de que a área de medição do corpo preto de medição deve ser a mesma que o calibrado, ou a medição da temperatura pode falhar.

1. Na página inicial, toque em **Temp (temperatura)** → **Configurações do corpo negro** para entrar na página Configurações do corpo negro.

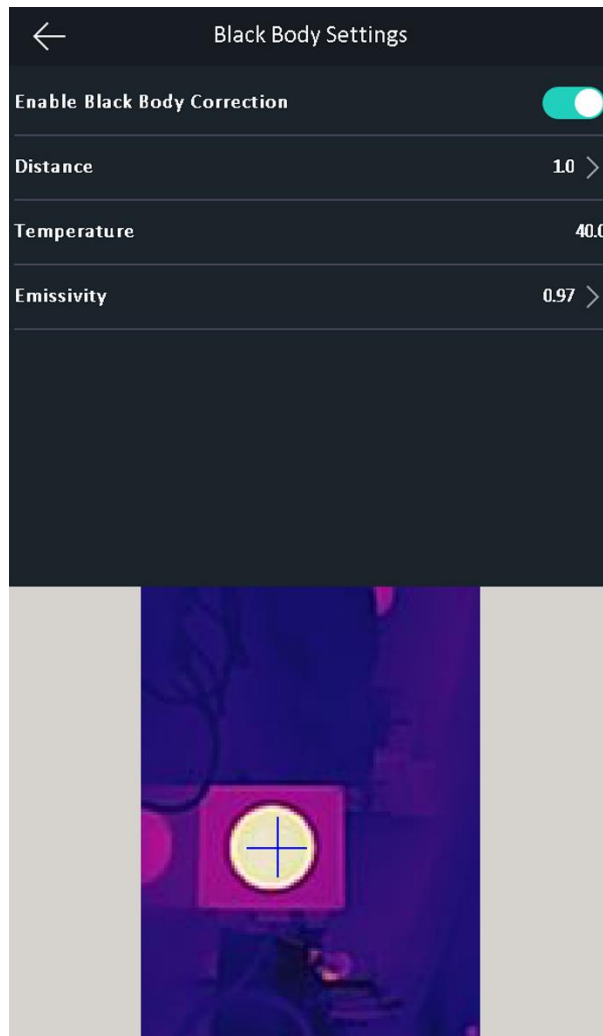


Figura 6-10 Página de configurações de corpo negro

2. Habilite a função de correção de corpo negro.
3. Coloque um corpo preto na frente da câmera. Certifique-se de que não haja outros objetos entre a câmera e o corpo negro.
4. Defina a distância entre o corpo preto e a câmera (linha reta) e a emissividade do corpo preto.

Nota

A temperatura do corpo negro é fixa.

5. Toque na posição do corpo negro na parte inferior da página. Quando + é exibido no corpo preto na tela, o corpo preto é calibrado.

6.6 Importar e exportar dados

Na página de transferência, você pode exportar o evento, os dados do usuário, a imagem do usuário e a imagem capturada para a unidade flash USB. Você também pode importar os dados e a imagem do usuário da unidade flash USB.

6.6.1 Exportar Dados

Passos

1. Toque em **Transferir** na página inicial para entrar na página Transferir.
2. Na página Transferir, toque em Exportar Evento, Exportar Dados do Usuário, Exportar Foto do Perfil e exportar a imagem capturada.
3. Toque em **Sim** na página pop-up e os dados serão exportados do dispositivo para a unidade flash USB.

Nota

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

6.6.2 Importar Dados

Passos

1. Conecte uma unidade flash USB no dispositivo.
2. Na página de transferência, toque em Importar dados do usuário e em Importar foto do perfil.
3. Toque em **Sim** na janela pop-up e os dados serão importados da unidade flash USB para o dispositivo.

Nota

- Se você deseja transferir todas as informações do usuário de um dispositivo (Dispositivo A) para outro (Dispositivo B), você deve exportar as informações do Dispositivo A para a unidade flash USB e, em seguida, importar da unidade flash USB para o Dispositivo B. Neste caso, você deve importar os dados do usuário antes de importar a foto do perfil.
 - O formato de unidade flash USB compatível é FAT32.
-

- As imagens importadas devem ser salvas no diretório raiz (register_pic) e o nome do arquivo da imagem deve seguir a regra abaixo:
Cartão No._Name_Department_Employee ID_Gender.jpg
 - A ID do funcionário deve ter menos de 32 caracteres. Pode ser uma combinação de letras minúsculas, letras maiúsculas e números. Não deve ser duplicado e não deve começar com 0.
 - Os requisitos de fotografia de rosto devem seguir as regras abaixo: Deve ser tirada em visão completa, de frente para a câmera. Não use chapéu ou cobertura para a cabeça ao tirar a foto do rosto. O formato deve ser JPEG ou JPG. A resolução deve ser de 640 × 480 pixels ou mais do que 640 × 480 pixels. O tamanho da imagem deve ser entre 60 KB e 200 KB.
-

6.7 Autenticação de Identidade

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

Você pode autenticar a identidade por meio de correspondência 1: 1 ou correspondência 1: N.

Correspondência 1: N

Compare a imagem de rosto capturada com todas as imagens de rosto armazenadas no dispositivo.

1: 1 correspondência

Compare a imagem de rosto capturada com a imagem de rosto vinculada ao usuário.

6.7.1 Autenticar por meio de múltiplas credenciais

Antes que você comece

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, autentique qualquer credencial de acordo com as instruções na página de exibição ao vivo.

Nota

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

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

Nota

Para obter informações detalhadas sobre a autenticação de rosto, consulte *Dicas ao coletar / comparar imagens de rosto* .

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

6.7.2 Autenticar por meio de credencial única

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

Autenticar rosto ou cartão.

Cara

Fique de frente para a câmera e inicie a autenticação via rosto.

Cartão

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

Nota

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

Se a autenticação for concluída, um prompt "Autenticado" aparecerá.

6.8 Configurações do sistema

Na página Configurações do sistema, você pode definir os parâmetros básicos do sistema, os parâmetros de face e atualizar o firmware.

6.8.1 Definir parâmetros básicos

Você pode definir o nº da comunidade, nº do prédio, nº da unidade, prompt de voz, volume de voz, modo de aplicação e brilho da luz branca.

Na página inicial, toque em **Sistema** (Configurações do sistema) para entrar na página Configurações do sistema.

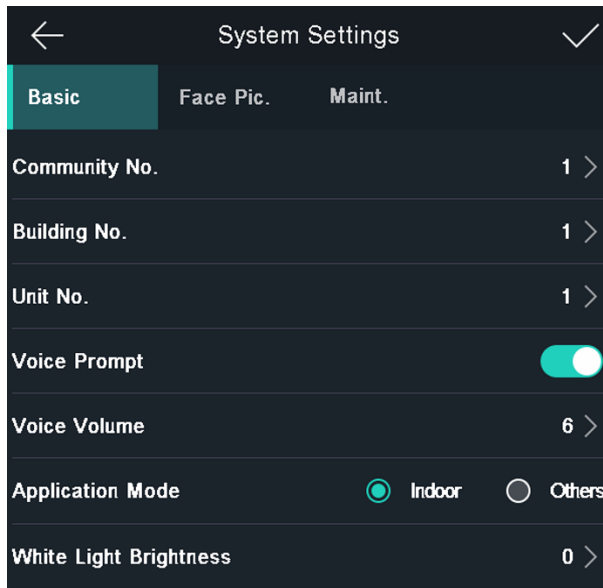




Figura 6-11 Parâmetros básicos

Tabela 6-2 Parâmetros básicos

Parâmetro	Descrição
Comunidade No.	Defina o número da comunidade instalada no dispositivo
Edifício No.	Defina o número do edifício instalado no dispositivo
Unidade No.	Defina o número da unidade instalada no dispositivo
Comando de voz	Toque  ou  para desativar ou ativar o prompt de voz.
Volume de Voz	Ajuste o volume da voz. Quanto maior for o valor, mais alto será o volume.
Modo de Aplicação	Você pode selecionar outros ou internos de acordo com o ambiente real.
Brilho da luz branca	Defina o brilho da luz branca suplementar. O brilho varia de 0 a 100. 0 refere-se a desligar a luz. 1 se refere ao mais escuro e 100 se refere ao mais claro

6.8.2 Definir os parâmetros da imagem do rosto

Você pode definir o nível de rosto 1: N (segurança), nível 1: 1 (segurança), intervalo de reconhecimento, nível de segurança de vivacidade, nível de WDR, distância pupilar, rosto com detecção de máscara e modo ECO.

Face Recognition Terminal User Manual

Na página inicial, toque em **Sistema** (Configurações do sistema) para entrar na página Configurações do sistema.

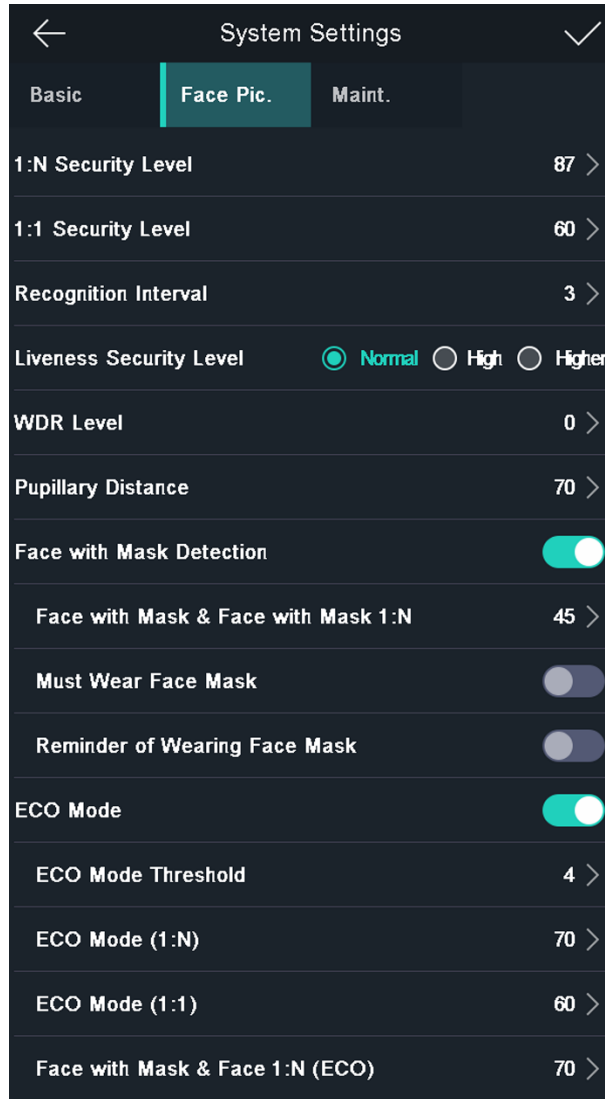


Figura 6-12 Parâmetros da imagem do rosto

Tabela 6-3 Parâmetros da imagem do rosto

Parâmetro	Descrição
1: N (Segurança) Nível	Defina o limite de correspondência ao autenticar por meio do modo de correspondência 1: N. Quanto maior o valor, menor é a taxa de falsa aceitação e maior a taxa de falsa rejeição. Por padrão, o valor é 84.

Face Recognition Terminal User Manual

Parâmetro	Descrição
Nível 1: 1 (segurança)	Defina o limite de correspondência ao autenticar por meio do modo de correspondência 1: 1. Quanto maior o valor, menor é a taxa de falsa aceitação e maior a taxa de falsa rejeição. Por padrão, o valor é 75.
Intervalo de Reconhecimento	Defina o intervalo de tempo entre dois reconhecimentos contínuos de rosto ao autenticar a permissão de uma pessoa. <hr/> Nota Você pode inserir o número de 1 a 10. <hr/>
Nível de vivacidade (nível de segurança de vivacidade)	Depois de ativar a função de detecção de rosto ao vivo, você pode definir o nível de segurança correspondente ao executar a autenticação de rosto ao vivo.
Nível WDR	O dispositivo pode habilitar automaticamente a função WDR. Quanto mais alto o nível, o dispositivo pode entrar no modo WDR mais facilmente. 0 representa que WDR está desabilitado.
Distância Pupilar	A resolução mínima entre dois alunos ao iniciar o reconhecimento de rosto. A resolução real deve ser maior que o valor configurado. Por padrão, a resolução é 40.
Detecção de rosto com máscara	Depois de habilitar esta função, quando uma pessoa autentica as permissões na página de autenticação, o dispositivo pode reconhecer o rosto, usando máscara ou não, e solicita o uso de máscara de acordo com a configuração.
Rosto com máscara e rosto com máscara (1: N)	Limiar de correspondência para rosto com máscara 1: N. Quanto maior o valor, menor a taxa de falsa aceitação e maior a taxa de falsa rejeição. The Max. o valor é 100.
Deve usar máscara facial	Após habilitar esta função, a pessoa autenticada deve usar uma máscara facial, caso contrário, a autenticação falhará.
Lembrete de usar máscara facial	Depois de habilitar esta função, se a pessoa autenticada não usar uma máscara facial, um aviso aparecerá para lembrá-lo de usar uma máscara facial.
Modo Eco	Após ativar o modo ECO, o dispositivo usará a câmera infravermelha para autenticar rostos em ambientes com pouca luz ou escuro. E

Face Recognition Terminal User Manual

Parâmetro	Descrição
	you can define the limit of the ECO mode, ECO mode (1: N) and ECO mode (1: 1).
Limiar do modo ECO	When enabling the ECO mode, you can define the limit of the ECO mode. The higher the value, the easier it will be for the device to enter the ECO mode. Available range: 0 to 8.
Modo ECO (1: N)	Define the limit of correspondence when authenticating through the ECO mode 1: mode of correspondence N. The higher the value, the lower the false acceptance rate and the higher the false rejection rate. By default, the value is 84.
Modo ECO (1: 1)	Define the limit of correspondence when authenticating through the ECO mode 1: 1 mode of correspondence. The higher the value, the lower the false acceptance rate and the higher the false rejection rate. By default, the value is 75.
Rosto com máscara e rosto (1: N) (ECO)	Threshold of correspondence for masked face 1: N in ECO mode. The higher the value, the lower the false acceptance rate and the higher the false rejection rate. The Max. value is 100.

6.8.3 Definir hora

You can define the time of the device and DST in this section.

Tap **Time** (Time Settings) on the home page to enter the Time Settings page. Edit the time parameters and tap **OK** to save the settings.

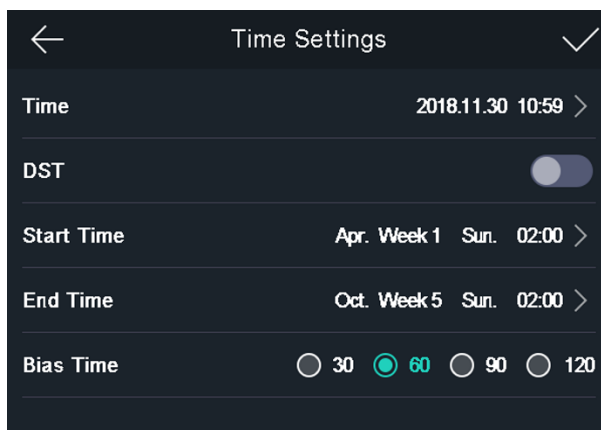


Figura 6-13 Parâmetros de tempo

6.9 Definir parâmetros de controle de acesso

Você pode definir as permissões de controle de acesso, incluindo as funções de autenticação do terminal. modo, autenticação do leitor. modo, autenticação remota, contato da porta e tempo de travamento da porta, etc.

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 e toque em para salvar as configurações.

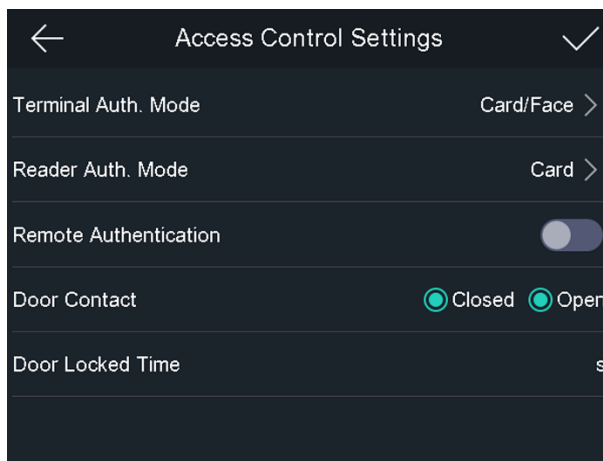


Figura 6-14 Parâmetros de controle de acesso

As descrições dos parâmetros disponíveis são as seguintes:

Tabela 6-4 Descrições dos parâmetros de controle de acesso

Parâmetro	Descrição
Terminal Auth. Modo	<p>Selecione o modo de autenticação do terminal de reconhecimento facial. Você também pode personalizar o modo de autenticação.</p> <hr/> <p>Nota</p> <ul style="list-style-type: none"> Os produtos de reconhecimento biométrico não são 100% aplicáveis a ambientes anti-spoofing. Se você precisar de um nível de segurança mais alto, use vários modos de autenticação. Se você adotar vários modos de autenticação, deve autenticar outros métodos antes de autenticar o rosto. <hr/>
Reader Auth. Modo	Selecione o modo de autenticação do leitor de cartão.

Face Recognition Terminal User Manual

Parâmetro	Descrição
Autenticação Remota	Ao autenticar a permissão, a plataforma controlará se concederá o acesso ou não remotamente.
Contato da porta	Você pode selecionar Aberto ou Fechado de acordo com suas necessidades reais. Por padrão, ele está fechado .
Tempo de porta fechada	Defina a duração do desbloqueio da porta. Se a porta não for aberta no tempo definido, ela será trancada. Intervalo de tempo disponível com porta fechada: 1 a 255 s.

6.10 Manutenção

6.10.1 Atualizar Firmware

Conecte a unidade flash USB. Toque em Manter. (Manutenção) na página Configurações do sistema e toque em **Atualizar** . O dispositivo irá ler automaticamente o arquivo de atualização na unidade flash USB e atualizar o firmware.

Nota

- Não desligue durante a atualização do dispositivo.
- O arquivo de atualização deve estar no diretório raiz.
- O nome do arquivo de atualização deve ser digicap.dav.

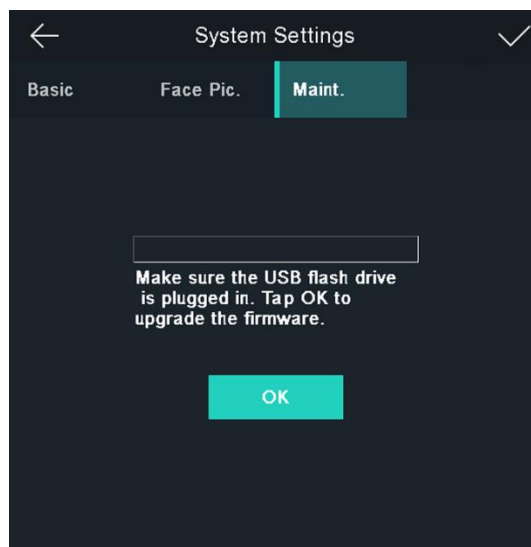


Figura 6-15 Atualização

6.10.2 Gerenciamento de Dados

Na página Gerenciamento de dados, você pode excluir dados do usuário, restaurar as configurações de fábrica ou restaurar as configurações padrão. Toque em **Dados** (Gerenciamento de dados) para entrar na página Gerenciamento de dados. Toque no botão na página para gerenciar os dados. Toque em **Sim** na janela pop-up para concluir as configurações. As descrições dos botões disponíveis são as seguintes:

Tabela 6-5 Descrições de dados

Parâmetros	Descrição
Excluir dados do usuário	Exclua todos os dados do usuário no dispositivo.
Restaurar para a fábrica	Restaure o sistema para as configurações de fábrica. O dispositivo será reiniciado após a configuração.
Restaurar para o padrão	Restaure o sistema para as configurações padrão. O sistema salvará as configurações de comunicação e as configurações do usuário remoto. Outros parâmetros serão restaurados ao padrão. O dispositivo será reiniciado após as configurações.

6.10.3 Consulta de Log

Você pode pesquisar os registros de autenticação dentro de um período de tempo, inserindo a ID do funcionário, o número do cartão ou o nome do usuário.

Passos

1. Na página inicial, toque em **Log** (Log) para entrar na página Log.

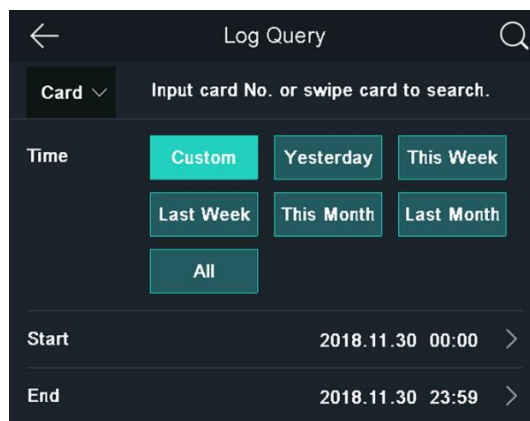



Figura 6-16 Consulta de registro

2. Toque em **Cartão** à esquerda da página e selecione um tipo de pesquisa na lista suspensa.
3. Toque na caixa de entrada e insira a ID do funcionário, o número do cartão ou o nome do usuário para pesquisa.
4. Selecione um horário.

Nota

Você pode selecionar entre Personalizado, Ontem, Esta semana, Semana passada, Este mês, Mês passado ou Todos. Se você selecionar Personalizado, poderá personalizar a hora de início e a hora de término da pesquisa.

5. Toque  para iniciar a pesquisa.
O resultado será exibido na página.

6.11 Configurações de status de tempo e presença

Defina a hora e o status de presença. Você pode definir o modo de atendimento como check in, check out, break out, break in, hora extra dentro e hora extra de acordo com a sua situação real.

Nota

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

6.11.1 Desativar modo de atendimento via dispositivo

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

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

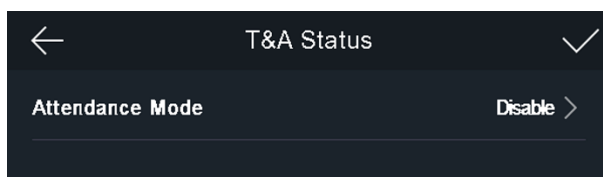


Figura 6-17 Desativar modo de atendimento

Defina o **modo de atendimento** como **Desativar** . E toque  .

Você não irá visualizar ou configurar o status de atendimento na página inicial. E o sistema seguirá a regra de atendimento que configurou na plataforma.

6.11.2 Definir atendimento automático via dispositivo

Defina o modo de atendimento como automático e você pode definir o status de atendimento e sua programação disponível. O sistema irá alterar automaticamente o status de atendimento de acordo com os parâmetros configurados.

Antes que você comece

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

Passos

1. Toque em **T&A Status** para entrar na página T&A Status.
2. Defina o **modo de atendimento** como **automático**.

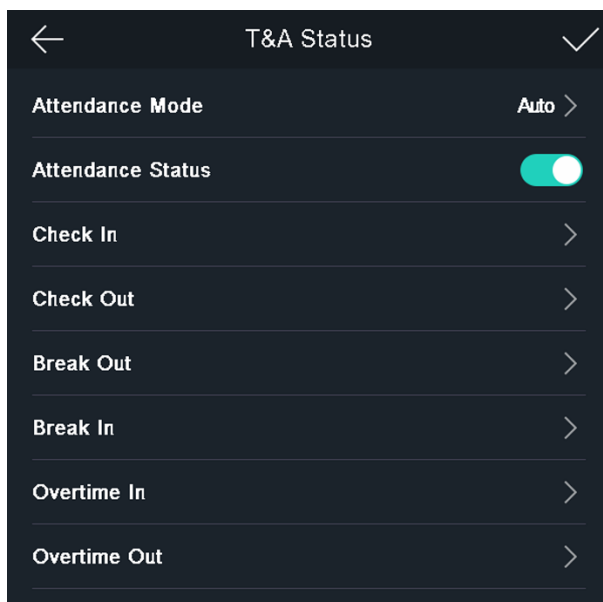


Figura 6-18 Modo de atendimento automático

3. Selecione um status de atendimento e defina sua programação.
 - 1) Selecione **Check In**, **Check Out**, **Break Out**, **Break In**, **Horas extras** ou **Horas extras** como o status de presença.
 - 2) Toque em **Agendar**.
 - 3) Selecione **segunda**, **terça**, **quarta**, **quinta**, **sexta**, **sábado** ou **domingo**.
 - 4) Toque na data selecionada e defina a hora de início do status de atendimento selecionado.
 - 5) Toque em **Confirmar**.
 - 6) Repita os passos 1 a 5 de acordo com suas necessidades reais.

Nota

O status de atendimento será válido dentro da programação configurada.

4. Toque .

Resultado

Ao autenticar na página inicial, a autenticação será marcada como o status de atendimento configurado de acordo com a programação configurada.

Exemplo

Se for definido o **Break Out Schedule** como segunda-feira 11:00 e o **Break In Schedule** como segunda-feira 12:00, a autenticação válida do usuário de segunda-feira 11:00 a 12:00 será marcada como break.

6.11.3 Definir atendimento manual via dispositivo

Defina o modo de atendimento como manual e você pode selecionar um status manualmente ao assumir o atendimento.

Antes que você comece

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

Passos

1. Toque em **T&A Status** para entrar na página T&A Status.
2. Defina o **modo de atendimento** como **manual**.

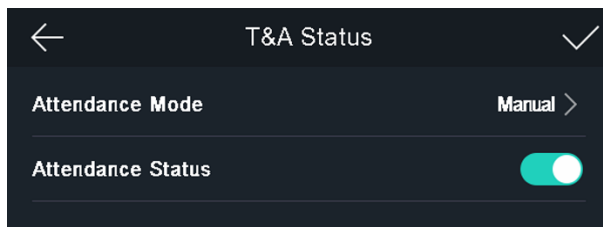


Figura 6-19 Modo de atendimento manual

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

Resultado

Você deve selecionar o status de atendimento manualmente após a autenticação.

Nota

Se você não selecionar um status, a autenticação falhará e não será marcada como um atendimento válido.

6.11.4 Definir atendimento manual e automático via dispositivo

Face Recognition Terminal User Manual

Defina o modo de atendimento como **Manual e Automático** , e o sistema irá alterar automaticamente o status de atendimento de acordo com os parâmetros configurados. Ao mesmo tempo, você pode alterar manualmente o status de atendimento após a autenticação.

Antes que você comece

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

Passos

1. Toque em **T&A Status** para entrar na página T&A Status.
2. Defina o **modo de atendimento** como **manual e automático** .

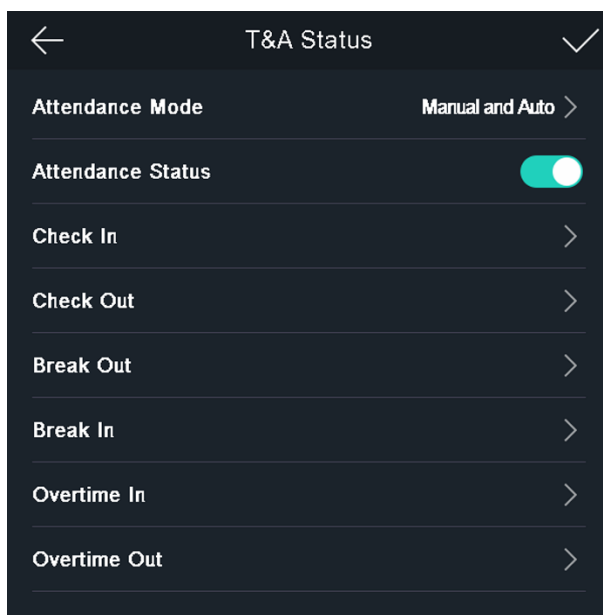


Figura 6-20 Modo manual e automático

3. Selecione um status de atendimento e defina sua programação.
 - 1) Selecione **Check In** , **Check Out** , **Break Out** , **Break In** , **Horas extras** ou **Horas extras** como o status de presença.
 - 2) Toque em **Agendar** .
 - 3) Selecione **segunda** , **terça** , **quarta** , **quinta** , **sexta** , **sábado** ou **domingo** .
 - 4) Toque na data selecionada e defina a hora de início do status de atendimento selecionado.
 - 5) Toque em **Confirmar** .
 - 6) Repita os passos 1 a 5 de acordo com suas necessidades reais.

Nota

O status de atendimento será válido dentro da programação configurada.

4. Toque .

Resultado

Na página inicial e autentique. Se você não selecionar um status, a autenticação será marcada como o status de atendimento configurado de acordo com a programação. Se você tocar em **Selecionar status** e selecionar um status para obter participação, a autenticação será marcada como o status de participação selecionado.

Exemplo

Se for definido o **Break Out Schedule** como segunda-feira 11:00 e o **Break In Schedule** como segunda-feira 12:00, a autenticação válida do usuário de segunda-feira 11:00 a 12:00 será marcada como break.

6.12 Exibir informações do sistema

Visualize a capacidade do dispositivo, as informações do dispositivo e a licença do software de código aberto.

Ver capacidade

Você pode ver o número do usuário adicionado, o número da foto do rosto, o número do rosto com máscara, o número do cartão e o número do evento.

Toque em **Informações. (Informações do sistema) → Capacidade** na página inicial para entrar na página Capacidade.

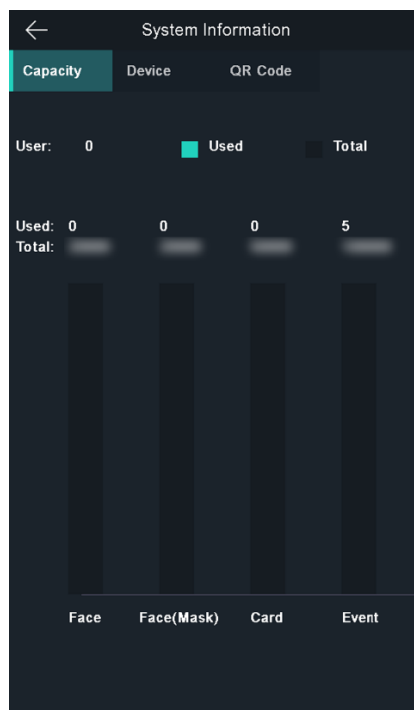


Figura 6-21 Capacidade

Ver informações do dispositivo

Você pode ver as informações do dispositivo.

Toque em **Informações. (Informações do sistema)** → **Dispositivo** para entrar na página Dispositivo.

Licença de código aberto

Visualize as informações da Licença de código aberto.

Toque em **Informações. (Informações do sistema)** → **Licença** para entrar na página Licenças de software de código aberto.

6.13 Intercomunicador de vídeo

Depois de adicionar o dispositivo ao software cliente, você pode chamar o dispositivo do software cliente, chamar a estação mestre do dispositivo, chamar o software cliente do dispositivo ou chamar a estação interna do dispositivo.

6.13.1 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 as instruções.
2. Execute o software cliente e o painel de controle do software aparecerá.
3. Clique em **Gerenciamento de dispositivos** para entrar na interface de gerenciamento de dispositivos.
4. Adicione o dispositivo ao software cliente.

Nota

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

5. Ligue para o software cliente.
 - 1) Toque em **Chamar** na página inicial do dispositivo.
 - 2) Insira **0** na janela pop-up.
 - 3) Toque em **Chamar** para chamar o software cliente.
6. Toque em **Resposta** na página pop-up do software cliente e você pode 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, apenas o primeiro software cliente adicionado ao dispositivo abrirá a janela de recebimento de chamadas.

6.13.2 Chamar estação mestre do dispositivo

Passos

1. Obtenha o software cliente do disco fornecido ou do site oficial e instale o software de acordo com as instruções.
 2. Execute o software cliente e o painel de controle do software aparecerá.
 3. Clique em **Gerenciamento de dispositivos** para entrar na interface de gerenciamento de dispositivos.
 4. Adicione a estação mestre e o dispositivo ao software cliente.
-

Nota

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

5. Defina o endereço IP e o endereço SIP da estação mestre na página de configuração remota.
-

Nota

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

6. Atende a chamada através da estação mestre e inicia o áudio bidirecional.
-

Nota

O dispositivo irá chamar a estação mestre em prioridade quando tocar .

6.13.3 Dispositivo de chamada do software cliente

Passos

1. Obtenha o software cliente do disco fornecido ou do site oficial e instale o software de acordo com as instruções.
 2. Execute o software cliente e o painel de controle do software aparecerá.
 3. Clique em **Gerenciamento de dispositivos** para entrar na página Gerenciamento de dispositivos.
 4. Adicione o dispositivo ao software cliente.
-

Nota

Face Recognition Terminal User Manual

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

5. Entre na página **Visualização** ao **vivo** e clique duas vezes no dispositivo adicionado para iniciar a visualização ao vivo.
-

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 na imagem de exibição ao vivo para abrir o menu do botão direito.
7. Clique em **Iniciar áudio bidirecional** para iniciar o áudio bidirecional entre o dispositivo e o software cliente.



6.13.4 Chamar estação interna do dispositivo

Passos

1. Obtenha o software cliente do disco fornecido ou do site oficial e instale o software de acordo com as instruções.
 2. Execute o software cliente e o painel de controle do software aparecerá.
 3. Clique em **Gerenciamento de dispositivos** para entrar na interface de gerenciamento de dispositivos.
 4. Adicione a estação interna e o dispositivo ao software cliente.
-

Nota

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

5. Conecte um usuário a uma estação interna e defina um número de sala para a estação interna.
6. Toque  na página de autenticação do dispositivo.
7. Insira o número do quarto na página de discagem e toque em  para chamar a estação interna.
8. Depois que a estação interna atender a chamada, você pode iniciar o áudio bidirecional com a estação interna.

Capítulo 7 Configuração do software cliente

7.1 Fluxo de configuração do software cliente

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

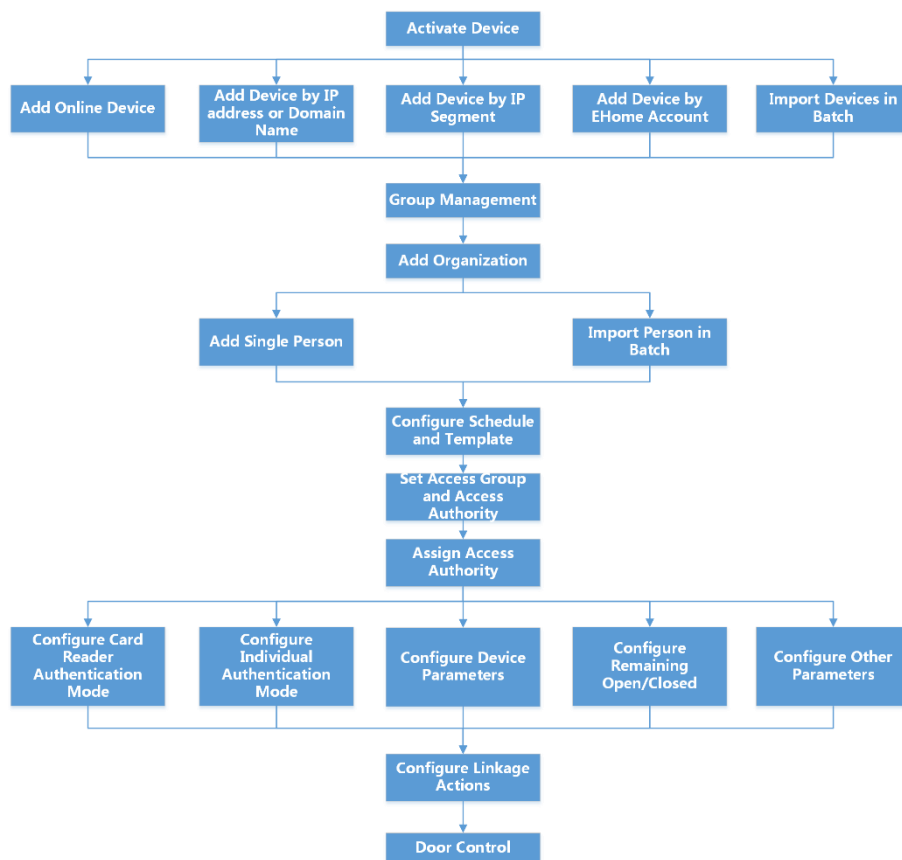


Figura 7-1 Diagrama de fluxo de configuração no software cliente

7.2 Gerenciamento de Dispositivos

O cliente suporta o gerenciamento de dispositivos de controle de acesso e dispositivos de intercomunicação de vídeo.

Exemplo

Você pode controlar a entrada e saída e gerenciar o atendimento após adicionar dispositivos de controle de acesso ao cliente; você pode executar vídeo porteiro com estações internas e estações externas.

7.2.1 Adicionar Dispositivo

O cliente fornece três modos de adição de dispositivo, incluindo por IP / domínio, segmento de IP e protocolo ISUP. O cliente também suporta a importação de vários dispositivos em um lote quando há uma grande quantidade de dispositivos a serem adicionados.

Adicionar Dispositivo Online

Os dispositivos online ativos na mesma sub-rede local com o software cliente serão exibidos na área **Dispositivo online** . Você pode clicar em **Atualizar a cada 60s** para atualizar as informações dos dispositivos online.

Adicionar um dispositivo online detectado

Você pode selecionar um dispositivo online detectado exibido na lista de dispositivos online e adicioná-lo ao cliente.

Passos

1. Entre no módulo de gerenciamento de dispositivos.
2. Clique na guia **Dispositivo** na parte superior do painel direito.
3. Clique em **Dispositivo online** para mostrar a área do dispositivo online.
Os dispositivos online pesquisados são exibidos na lista.
4. Selecione um dispositivo online na área **Dispositivo online** e clique em **Adicionar** para abrir a janela de adição de dispositivo.

Nota

Para o dispositivo inativo, você precisa criar uma senha antes de adicionar o dispositivo corretamente. Para obter etapas detalhadas, consulte.

5. Insira as informações necessárias.

Nome

Insira um nome descritivo para o dispositivo.

Endereço de IP

Digite o endereço IP do dispositivo. O endereço IP do dispositivo é obtido automaticamente neste modo de adição.

Porta

Você pode personalizar o número da porta. O número da porta do dispositivo é obtido automaticamente neste modo de adição.

Nome do usuário

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 escolha (usando no mínimo 8 caracteres, incluindo pelo menos três tipos das seguintes categorias: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança de sua produtos. E recomendamos que você altere sua senha regularmente, principalmente no sistema de alta segurança, alterando a senha mensal 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.

6. Opcional: Marque **Transmission Encryption (TLS)** para ativar 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 ativou a Verificação de certificado, deve clicar em **Abrir diretório de certificado** para abrir a pasta padrão e copiar o arquivo de certificado exportado do dispositivo para este diretório padrão para fortalecer a segurança. Consulte para obter detalhes sobre como habilitar a verificação de certificado.
 - Você pode fazer login no dispositivo para obter o arquivo do certificado pelo navegador da web.
-

7. Marque **Sincronizar hora** para sincronizar a hora do dispositivo com o PC que executa o cliente após adicionar o dispositivo ao cliente.
8. Opcional: Marque **Import to Group** para criar um grupo pelo nome do dispositivo e importar todos os canais do dispositivo para este grupo.

Exemplo

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

9. Clique em **Adicionar** .

Adicionar vários dispositivos online detectados

Para dispositivos online detectados que compartilham o mesmo nome de usuário e senha, você pode adicioná-los ao cliente em um lote.

Antes que você comece

Certifique-se de que os dispositivos a serem adicionados estejam online.

Face Recognition Terminal User Manual

Passos

1. Entre no módulo de gerenciamento de dispositivos.
2. Clique na guia **Dispositivo** na parte superior do painel direito.
3. Clique em **Dispositivo online** para mostrar a área do dispositivo online na parte inferior da página.
Os dispositivos online pesquisados são exibidos na lista.
4. Selecione vários dispositivos.

Nota

Para o dispositivo inativo, você precisa criar uma senha antes de adicionar o dispositivo corretamente. Para obter detalhes, consulte.

5. Clique em **Adicionar** para abrir a janela de adição de dispositivos.
6. Insira as informações necessárias.

Nome do usuário

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 escolha (usando no mínimo 8 caracteres, incluindo pelo menos três tipos das seguintes categorias: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança de sua produtos. E recomendamos que você altere sua senha regularmente, principalmente no sistema de alta segurança, alterando a senha mensal 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.

7. Opcional: Marque **Sincronizar hora** para sincronizar a hora do dispositivo com o PC que executa o cliente após adicionar o dispositivo ao cliente.
8. Opcional: Marque **Import to Group** para criar um grupo pelo nome do dispositivo e importar todos os canais do dispositivo para este grupo.

Exemplo

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

9. Clique em **Adicionar** para adicionar os dispositivos.

Adicionar dispositivo por endereço IP ou nome de domínio

Se você souber o endereço IP ou 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 de 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 característica do dispositivo.

Endereço

O endereço IP ou nome de domínio do dispositivo.

Porta

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

Nome do usuário

Digite 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 escolha (usando no mínimo 8 caracteres, incluindo pelo menos três tipos das seguintes categorias: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança de sua produtos. E recomendamos que você altere sua senha regularmente, principalmente no sistema de alta segurança, alterando a senha mensal 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.

5. Opcional: Marque **Transmission Encryption (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 ativou a Verificação de certificado, deve clicar em **Abrir diretório de certificado** para abrir a pasta padrão e copiar o arquivo de certificado exportado do dispositivo para este diretório padrão para fortalecer a segurança. Consulte para obter detalhes sobre como habilitar a verificação de certificado.
 - Você pode fazer login no dispositivo para obter o arquivo do certificado pelo navegador da web.
-

6. Marque **Sincronizar hora** para sincronizar a hora do dispositivo com o PC que executa o cliente após adicionar o dispositivo ao cliente.
7. Opcional: Marque **Import to Group** para criar um grupo pelo nome do dispositivo e importar todos os canais do dispositivo para este grupo.

Exemplo

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

8. Conclua a adição do dispositivo.
 - Clique em **Adicionar** para adicionar o dispositivo e voltar à página da lista de dispositivos.
 - Clique em **Adicionar e Novo** para salvar as configurações e continuar adicionando outro dispositivo.

Adicionar dispositivos por segmento de IP

Se os dispositivos compartilham o mesmo número de porta, nome de usuário e senha, e seus intervalos de endereços IP no mesmo segmento de IP, você pode adicioná-los ao cliente especificando o endereço IP inicial e o endereço IP final, número da porta, usuário nome, senha, etc. dos dispositivos.

Passos

1. Entre no módulo de 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.

4. Selecione **Segmento IP** como o modo de adição.
5. Insira as informações necessárias.

IP inicial

Insira um endereço IP inicial.

Face Recognition Terminal User Manual

IP final

Insira um endereço IP final no mesmo segmento de rede com o IP inicial.

Porta

Digite o nº da porta do dispositivo. O valor padrão é **8000**.

Nome do usuário

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 escolha (usando no mínimo 8 caracteres, incluindo pelo menos três tipos das seguintes categorias: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança de sua produtos. E recomendamos que você altere sua senha regularmente, principalmente no sistema de alta segurança, alterando a senha mensal 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.

6. Opcional: Marque **Transmission Encryption (TLS)** para ativar 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 ativou a Verificação de certificado, você deve clicar em **Abrir pasta de certificado** para abrir a pasta padrão e copiar o arquivo de certificado exportado do dispositivo para este diretório padrão para fortalecer a segurança. Consulte para obter detalhes sobre como habilitar a verificação de certificado.
 - Você pode fazer login no dispositivo para obter o arquivo do certificado pelo navegador da web.
-

7. Marque **Sincronizar hora** para sincronizar a hora do dispositivo com o PC que executa o cliente após adicionar o dispositivo ao cliente.
8. Opcional: Marque **Import to Group** para criar um grupo pelo nome do dispositivo e importar todos os canais do dispositivo para o grupo.
9. Conclua a adição do dispositivo.
- Clique em **Adicionar** para adicionar o dispositivo e voltar à página da lista de dispositivos.
-

Face Recognition Terminal User Manual

- Clique em **Adicionar e Novo** para salvar as configurações e continuar adicionando outro dispositivo.

Adicionar dispositivo por conta ISUP

Para dispositivos de controle de acesso com suporte ao protocolo ISUP 5.0, você pode adicioná-los ao cliente pelo protocolo ISUP após inserir o ID do dispositivo e a chave, se tiver configurado seus endereços de servidor, número de porta e IDs de dispositivo.

Antes que você comece

Certifique-se de que os dispositivos estejam conectados à rede corretamente.

Passos

1. Entre no módulo de gerenciamento de dispositivos.
Os dispositivos adicionados são exibidos no painel direito.
2. Clique em **Adicionar** para abrir a janela Adicionar.
3. Selecione **ISUP** como o modo de adição.
4. Insira as informações necessárias.

Conta do dispositivo

Insira o nome da conta registrada no protocolo ISUP.

Chave ISUP

Para dispositivos ISUP 5.0, insira a chave ISUP se você a definiu ao configurar o parâmetro do centro de rede para o dispositivo.

Nota

Esta função deve ser suportada pelo dispositivo.





5. Opcional: Marque **Sincronizar hora** para sincronizar a hora do dispositivo com o PC que executa o cliente após adicionar o dispositivo ao cliente.
 6. Opcional: Marque **Importar para Grupo** para criar um grupo pelo nome do dispositivo e importar todos os canais do dispositivo para o grupo.
 7. Conclua a adição do dispositivo.
 - Clique em **Adicionar** para adicionar o dispositivo e voltar para a lista de dispositivos.
 - Clique em **Adicionar e Novo** para salvar as configurações e continuar adicionando outro dispositivo.
-

Nota

Imagens de rosto não podem ser aplicadas a dispositivos adicionados pela conta ISUP, exceto as séries DS-K1T671 e DS-K1T331.

8. Opcional: execute as seguintes operações.
-

Face Recognition Terminal User Manual

Status do dispositivo	Clique  na coluna Operação para visualizar o status do dispositivo.
Editar informações do dispositivo	Clique  na coluna Operação para editar as informações do dispositivo, como nome do dispositivo, conta do dispositivo e chave ISUP.
Verificar usuário online	Clique  na coluna Operação para verificar os usuários online que acessam o dispositivo, como nome de usuário, tipo de usuário, endereço IP do usuário e hora de login.
Atualizar	Clique  na coluna Operação para obter as informações mais recentes do dispositivo.
Apagar Dispositivo	Selecione um ou vários dispositivos e clique em Excluir para excluir o (s) dispositivo (s) selecionado (s) do cliente.

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 de 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 salve o modelo predefinido (arquivo CSV) em seu PC.
5. Abra o arquivo de modelo exportado e insira as informações necessárias dos dispositivos a serem adicionados na coluna correspondente.

Nota

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

Modo de adição

Insira **0** ou **1** ou **2**.

Endereço

Edite o endereço do dispositivo.

Face Recognition Terminal User Manual

Porta

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

Nome do usuário

Digite 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 escolha (usando no mínimo 8 caracteres, incluindo pelo menos três tipos das seguintes categorias: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança de sua produtos. E recomendamos que você altere sua senha regularmente, principalmente no sistema de alta segurança, alterando a senha mensal 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.

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. Insira **0** para desativar esta função.

6. Clique  e selecione o arquivo de modelo.
7. Clique em **Adicionar** para importar os dispositivos.

7.2.2 Redefinir senha do dispositivo

Se você esqueceu a senha dos dispositivos online detectados, pode redefinir a senha do dispositivo por meio do cliente.

Passos

1. Entre na página de 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 da lista e clique em  na coluna Operação.
4. Redefina a senha do dispositivo.
 - Clique em **Gerar** para abrir a janela do código QR 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 nosso suporte técnico.

Nota

Para as seguintes operações para redefinir a senha, entre em contato com nosso suporte técnico.

Cuidado

A força da senha do dispositivo pode ser verificada automaticamente. É altamente recomendável que você altere a senha de sua escolha (usando no mínimo 8 caracteres, incluindo pelo menos três tipos das seguintes categorias: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança de sua produtos. E recomendamos que você altere sua senha regularmente, principalmente no sistema de alta segurança, alterando a senha mensal 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.

7.3 Gestão do Grupo

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

Exemplo

Por exemplo, no 1º andar, foram montadas 16 portas, 64 entradas de alarme e 16 saídas de alarme. Você pode organizar esses recursos em um grupo (denominado 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.

7.3.1 Adicionar Grupo

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

Passos

1. Entre no módulo de 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 digite um nome de grupo como você deseja.

- Clique em **Criar grupo por nome de dispositivo** e selecione um dispositivo adicionado para criar um novo grupo com o nome do dispositivo selecionado.
-

Nota

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

7.3.2 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 que você comece

Adicione um grupo para gerenciar dispositivos. Consulte [**Adicionar grupo**](#).

Passos

1. Entre no módulo de gerenciamento de dispositivos.
 2. Clique em **Gerenciamento de dispositivos** → **Grupo** para entrar na página de gerenciamento de grupo.
 3. Selecione um grupo da lista de grupos e selecione o tipo de recurso como **Access Point**, **Entrada de alarme**, **saída de alarme**, etc.
 4. Clique em **Importar**.
 5. Selecione as miniaturas / nomes dos recursos na exibição de miniaturas / lista.
-

Nota

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

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

7.3.3 Editar Parâmetros de Recursos


Depois de importar os recursos para o grupo, você pode editar os parâmetros do recurso. Para o ponto de acesso, você pode editar o nome do ponto de acesso. Para entrada de alarme, você pode editar o nome da entrada de alarme. Aqui, tomamos o ponto de acesso como exemplo.

Antes que você comece

Importe os recursos para o grupo.

Passos

1. Entre no módulo de gerenciamento de dispositivos.
-

2. Clique em **Gerenciamento de dispositivos** → **Grupo** para entrar na página de gerenciamento de grupo.
Todos os grupos adicionados são exibidos à esquerda.
3. Selecione um grupo na lista de grupos e clique em **Ponto de Acesso** .
Os pontos de acesso importados para o grupo serão exibidos.
4. Clique  na coluna Operação para abrir a janela Editar recurso.
5. Edite o nome do recurso.
6. Clique em **OK** para salvar as novas configurações.

7.3.4 Remover Recursos do Grupo

Você pode remover os recursos adicionados do grupo.

Passos

1. Entre no módulo de gerenciamento de dispositivos.
2. Clique em **Gerenciamento de dispositivos** → **Grupo** para entrar na página de gerenciamento de grupo.
Todos os grupos adicionados são exibidos à esquerda.
3. Clique em um grupo para mostrar os recursos adicionados a este grupo.
4. Selecione o (s) recurso (s) e clique em **Excluir** para remover o (s) recurso (s) do grupo.

7.4 Gestão de Pessoas

Você pode adicionar informações pessoais ao sistema para outras operações, como controle de acesso, vídeo porteiro, horário 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.

7.4.1 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 subordinada à adicionada.

Passos


1. Entre no módulo **Pessoa** .
2. Selecione uma organização pai na coluna esquerda e clique em **Adicionar** no canto superior esquerdo para adicionar uma organização.
3. Crie um nome para a organização adicionada.


Nota

Face Recognition Terminal User Manual

Podem ser adicionados até 10 níveis de organizações.

4. Opcional: execute as seguintes operações.

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-lo.

Nota

- As organizações de nível inferior também serão excluídas se você excluir uma organização.
 - Certifique-se de que não haja nenhuma pessoa adicionada à organização, ou a organização não pode ser excluída.
-

Mostrar pessoas na suborganização Marque **Mostrar** pessoas na suborganização e selecione uma organização para mostrar pessoas em suas suborganizações.

7.4.2 Configurar informações básicas

Você pode adicionar uma pessoa ao software cliente uma por uma e configurar as informações básicas da pessoa, como nome, sexo, número de telefone, etc.

Passos

1. Entre no módulo **Pessoa**.
2. Selecione uma organização na lista de organizações para adicionar a pessoa.
3. Clique em **Adicionar** para abrir a janela de adição de pessoa.
O ID da pessoa será gerado automaticamente.
4. Insira as informações básicas, incluindo nome da pessoa, sexo, telefone, endereço de e-mail, etc.
5. Opcional: Defina o período de vigência da pessoa. Uma vez expiradas, as credenciais e configurações de controle de acesso da pessoa serão inválidas e a pessoa não terá autorização para acessar as portas \ andares.

Exemplo

Por exemplo, se a pessoa for um visitante, seu período de vigência pode ser curto e temporário.

6. Confirme para adicionar a pessoa.
 - Clique em **Incluir** para incluir a pessoa e feche a janela Incluir Pessoa.

- Clique em **Adicionar e Novo** para adicionar a pessoa e continuar a adicionar outras pessoas.

7.4.3 Emitir um Cartão pelo Modo Local

Se uma estação de registro de cartão estiver disponível, você pode emitir um cartão pelo modo local. Para ler o número do cartão, você deve conectar a estação de registro do cartão ao PC que executa o cliente por interface USB ou COM e colocar o cartão na estação de registro do cartão.

Passos

1. Entre no módulo **Pessoa**.
2. Selecione uma organização na lista de organizações para adicionar a pessoa e clique em **Adicionar** para entrar no painel Adicionar pessoa.

Nota

Insira as informações básicas da pessoa primeiro. Para obter detalhes sobre como configurar as informações básicas da pessoa, consulte [**Configurar informações básicas**](#).

3. Na área **Credencial** → **Cartão**, clique em +.
4. Clique em **Configurações** para entrar na página Configurações.
5. Selecione **Local** como o modo de emissão do cartão.

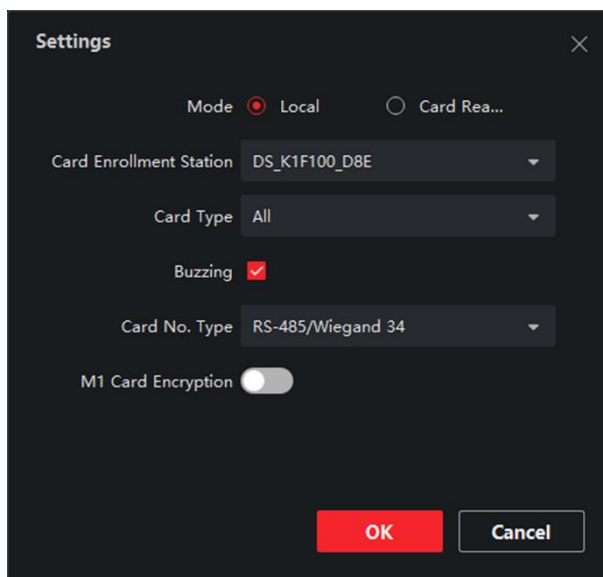


Figura 7-2 Emitir um cartão pelo modo local

6. Defina outros parâmetros relacionados.

Estação de inscrição de cartão

Face Recognition Terminal User Manual

Selecione o modelo da estação de registro de cartão conectada.

Nota

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

Tipo de carta

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

Zumbido

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

Tipo nº do cartão

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

Criptografia de cartão M1

Este campo está disponível apenas quando o modelo é DS-K1F100-D8, DS-K1F100-D8E ou DS-K1F180-D8E. Se o cartão for um cartão M1, você poderá ativar a função de criptografia do cartão M1 e selecionar o setor do cartão a ser criptografado.

7. Clique em **OK** para confirmar a operação.
8. Coloque o cartão na estação de inscrição do cartão e clique em **Ler** para obter o número do cartão.
O número do cartão será exibido no campo N° do cartão automaticamente.
9. Clique em **Adicionar** .
O cartão será emitido para a pessoa.

7.4.4 Carregar uma foto de rosto do PC local

Ao adicionar uma pessoa, você pode carregar uma foto de rosto armazenada no PC local para o cliente como o perfil da pessoa.

Passos

1. Entre no módulo **Pessoa** .
2. Selecione uma organização na lista de organizações para adicionar a pessoa e clique em **Adicionar** .

Nota

Insira as informações básicas da pessoa primeiro. Para obter detalhes sobre como configurar as informações básicas da pessoa, consulte [***Configurar informações básicas***](#) .

Face Recognition Terminal User Manual

3. Clique em **Adicionar rosto** no painel Informações básicas.
 4. Selecione **Upload**.
 5. Selecione uma imagem do PC executando o cliente.
-

Nota

A imagem deve estar no formato JPG ou JPEG e menor que 200 KB.

6. Opcional: ative **Verificar por dispositivo** para verificar se o dispositivo de reconhecimento facial gerenciado no cliente pode reconhecer o rosto na foto.
7. Confirme para adicionar a pessoa.
 - Clique em **Incluir** para incluir a pessoa e feche a janela Incluir Pessoa.
 - Clique em **Adicionar e Novo** para adicionar a pessoa e continuar a adicionar outras pessoas.

7.4.5 Tirar uma foto via cliente

Ao adicionar uma pessoa, você pode tirar uma foto dela por meio do cliente e definir essa foto como o perfil da pessoa.

Antes que você comece

Certifique-se de que o PC que está executando o cliente tenha uma câmera ou se você conectou outra câmera USB ao PC.

Passos



1. Entre no módulo **Pessoa**.
2. Selecione uma organização na lista de organizações para incluir a pessoa e clique em **Incluir** para entrar na janela Incluir Pessoa.

Nota

Insira as informações básicas da pessoa primeiro. Para obter detalhes, consulte **Configurar informações básicas**.

3. Clique em **Adicionar rosto** na área Informações básicas.
 4. Selecione **Tirar foto** para entrar na janela Tirar foto.
 5. Opcional: ative **Verificar por dispositivo** para verificar se a foto de rosto capturada pode atender aos requisitos de upload.
 6. Tire uma foto.
-

Face Recognition Terminal User Manual

- 1) Fique de frente para a câmera e certifique-se de que seu rosto esteja no meio da janela de coleta.
- 2) Clique  para capturar uma foto de rosto.
- 3) Opcional: Clique  para capturar novamente.
- 4) Clique em **OK** para salvar a foto capturada.

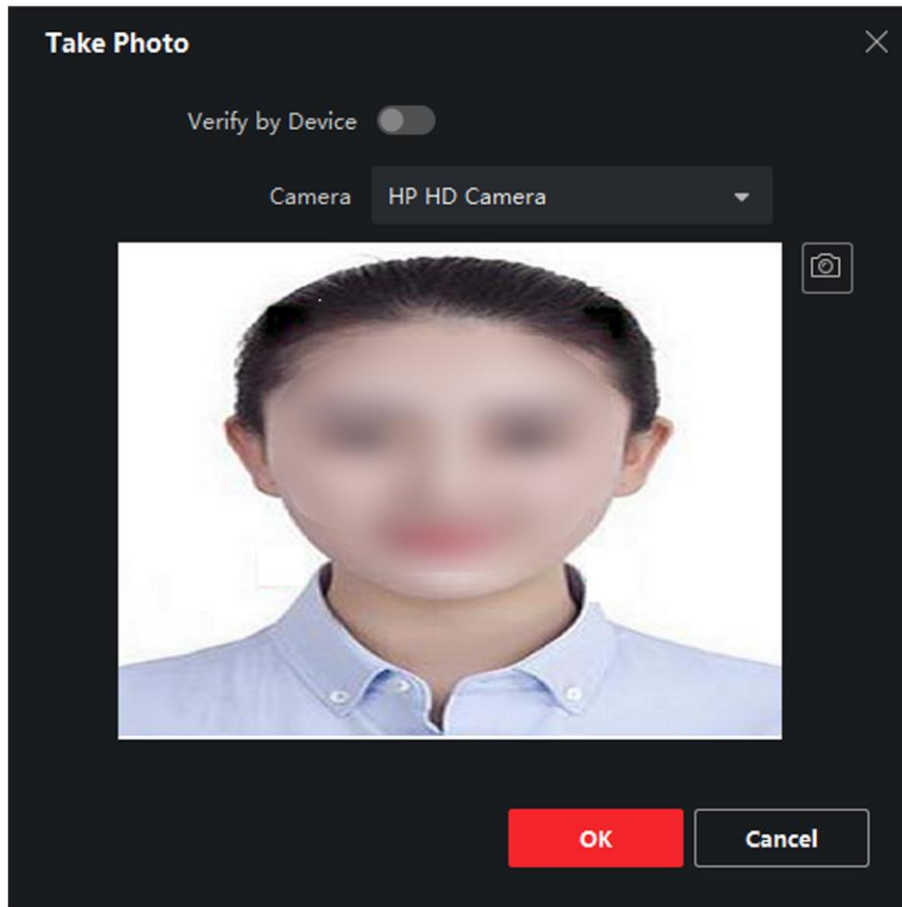


Figura 7-3 Tirar uma foto via cliente

7. Confirme para adicionar a pessoa.
 - Clique em **Incluir** para incluir a pessoa e feche a janela Incluir Pessoa.
 - Clique em **Adicionar e Novo** para adicionar a pessoa e continuar a adicionar outras pessoas.

7.4.6 Coletar Face via Dispositivo de Controle de Acesso

Ao adicionar uma pessoa, você pode coletar o rosto da pessoa por meio do dispositivo de controle de acesso adicionado ao cliente que suporta a função de reconhecimento facial.

Passos

Face Recognition Terminal User Manual

1. Entre no módulo **Pessoa** .
 2. Selecione uma organização na lista de organizações para adicionar a pessoa e clique em **Adicionar** .
-

Nota

Insira as informações básicas da pessoa primeiro. Para obter detalhes sobre como configurar as informações básicas da pessoa, consulte [**Configurar informações básicas**](#) .


3. Clique em **Adicionar rosto** no painel Informações básicas.
 4. Selecione **Coleta remota** .
 5. Selecione um dispositivo de controle de acesso adicionado ou a estação de inscrição na lista suspensa.
-

Nota

Se você selecionar a estação de inscrição, deverá clicar em **Login** para definir os parâmetros relacionados do dispositivo, incluindo endereço IP, número da porta, nome de usuário e senha. Além disso, você pode marcar o **Anti-spoofing de rosto** e selecionar o nível de vivacidade como Baixo, Médio ou Alto.

Anti-spoofing de rosto

Se você marcar esta função, o dispositivo pode detectar se o rosto a ser coletado é autêntico.

6. Colete o rosto.
 - 1) Fique de frente para a câmera do dispositivo de controle de acesso selecionado e certifique-se de que seu rosto esteja no meio da janela de coleta.
 - 2) Clique  para capturar uma foto.
 - 3) Clique em **OK** para salvar a foto capturada.
7. Confirme para adicionar a pessoa.
 - Clique em **Incluir** para incluir a pessoa e feche a janela Incluir Pessoa.
 - Clique em **Adicionar e Novo** para adicionar a pessoa e continuar a adicionar outras pessoas.

7.4.7 Configurar informações de controle de acesso

Ao adicionar uma pessoa, você pode definir suas informações de controle de acesso, como vincular um grupo de controle de acesso à pessoa, configurar o código PIN, definir a pessoa como um visitante, uma pessoa da lista negra ou um superusuário, etc.

Passos

Face Recognition Terminal User Manual

1. Entre no módulo **Pessoa** .
 2. Selecione uma organização na lista de organizações para adicionar a pessoa e clique em **Adicionar** .
 3. Na área **Controle de acesso** , clique para selecionar o (s) grupo (s) de acesso para a pessoa.
-

Nota

Para obter detalhes, consulte [Definir grupo de acesso para atribuir autorização de acesso a pessoas](#) .

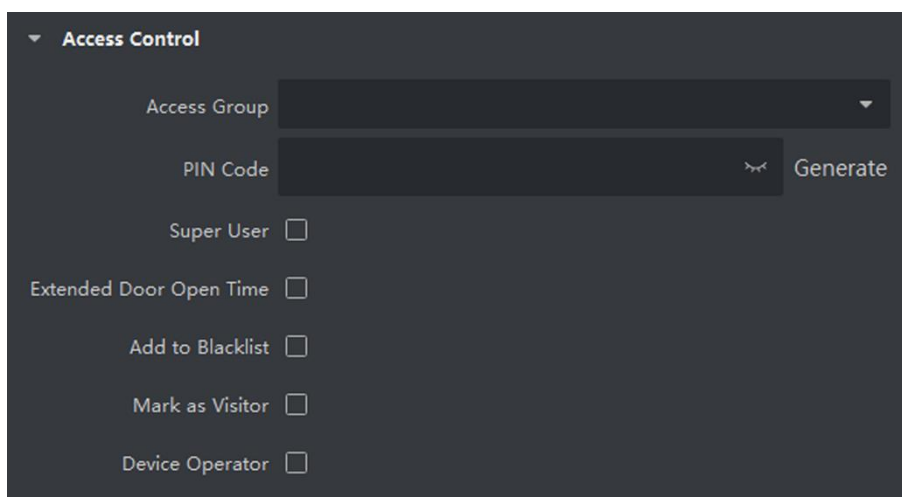


Figura 7-4 Configurar informações de controle de acesso

4. Defina um código PIN exclusivo para a pessoa que pode ser usado para autenticação de acesso.
 - Insira manualmente um código PIN com 4 a 8 dígitos.
-

Nota

Os códigos PIN das pessoas não podem ser repetidos.

- Clique em **Gerar** para gerar aleatoriamente um código PIN não repetido de 6 dígitos.
-

Nota

Se houver códigos PIN repetidos, um prompt aparecerá no cliente. O administrador pode gerar um novo código PIN para substituir o código PIN repetido e notificar as pessoas relacionadas.

5. Verifique as permissões de operação da pessoa.

Superusuário

Face Recognition Terminal User Manual

Se a pessoa for definida como um superusuário, ela terá autorização para acessar todas as portas / andares e ficará isenta das demais restrições de fechamento, de todas as regras anti-passageira de volta e da autorização de primeira pessoa.

Tempo alargado de porta aberta

Use esta função para pessoas com mobilidade reduzida. Ao acessar a porta, a pessoa terá mais tempo do que outras para passar pelas portas.

Para obter detalhes sobre como definir a duração da abertura da porta, consulte [Configurar parâmetros para porta](#).

Adicionar à lista negra

Adicione a pessoa à lista negra e quando a pessoa tentar acessar portas / andares, um evento será acionado e enviado ao cliente para notificar o pessoal de segurança.

Marcar como visitante

Se a pessoa for um visitante, você deve definir os horários válidos para a visita.

Nota

O tempo válido para visita é de 1 a 100. Você também pode marcar **No Limit**, então não há horários limitados para o visitante acessar portas / andares.

Operador de dispositivo

Para pessoa com função de operador de dispositivo, ele / ela está autorizado a operar nos dispositivos de controle de acesso.

Nota

As funções Superusuário, Tempo de porta aberta estendido, adicionar à lista negra e Marcar como visitante não podem ser ativadas simultaneamente. Por exemplo, se uma pessoa for definida como superusuário, você não pode habilitar o tempo de porta aberta para ela, adicioná-la à lista negra ou defini-la como visitante.

6. Confirme para adicionar a pessoa.

- Clique em **Incluir** para incluir a pessoa e feche a janela Incluir Pessoa.
- Clique em **Adicionar e Novo** para adicionar a pessoa e continuar a adicionar outras pessoas.

7.4.8 Personalizar as informações da pessoa

Você pode personalizar as propriedades da pessoa que não são predefinidas no cliente de acordo com as necessidades reais, por exemplo, local de nascimento. Depois de personalizar, ao adicionar uma pessoa, você pode inserir as informações personalizadas para tornar as informações da pessoa completas.

Passos

1. Entre no módulo **Pessoa** .
 2. Defina os campos de informações personalizadas.
 - 1) Clique em **Propriedade personalizada** .
 - 2) Clique em **Adicionar** para adicionar uma nova propriedade.
 - 3) Digite o nome da propriedade.
 - 4) Clique em **OK** .
 3. Defina as informações personalizadas ao adicionar uma pessoa.
 - 1) Selecione uma organização na lista de organizações para adicionar a pessoa e clique em **Adicionar** .
-

Nota

Insira as informações básicas da pessoa primeiro. Para obter detalhes sobre como configurar as informações básicas da pessoa, consulte [***Configurar informações básicas***](#) .

- 2) No painel **Informações personalizadas** , insira as informações da pessoa.
- 3) Clique em **Adicionar** para adicionar a pessoa e fechar a janela Adicionar pessoa ou clique em **Adicionar e Novo** para adicionar a pessoa e continuar adicionando outras pessoas.

7.4.9 Configurar as informações do residente

Se a pessoa for residente, para fins de videoporteiro, você precisa definir o número da sala para ela e ligar uma estação interna. Depois de vinculado, você pode ligar para essa pessoa ligando para a estação interna e realizar o videoporteiro com ela.

Passos

1. Entre no módulo **Pessoa** .
 2. Selecione uma organização na lista de organizações para adicionar a pessoa e clique em **Adicionar** .
-

Nota

Insira as informações básicas da pessoa primeiro. Para obter detalhes sobre como configurar as informações básicas da pessoa, consulte [***Configurar informações básicas***](#) .

3. No painel **Informações do residente** , selecione a estação interna para vinculá-la à pessoa.
-

Nota

Se você selecionar **Estação Interna Analógica** , o campo **Botoneira** será exibido e você deverá selecionar a estação interna para se comunicar com a estação interna analógica.

4. Digite o nº do andar e o nº do quarto da pessoa.
5. Confirme para adicionar a pessoa.
 - Clique em **Incluir** para incluir a pessoa e feche a janela Incluir Pessoa.
 - Clique em **Adicionar e Novo** para adicionar a pessoa e continuar a adicionar outras pessoas.

7.4.10 Configurar Informações Adicionais

Ao adicionar pessoa, você pode configurar as informações adicionais para a pessoa, como tipo de identidade da pessoa, número de identidade, país, etc., de acordo com as necessidades reais.

Passos

1. Entre no módulo **Pessoa**.
2. Selecione uma organização na lista de organizações para adicionar a pessoa e clique em **Adicionar**.

Nota

Insira as informações básicas da pessoa primeiro. Para obter detalhes sobre como configurar as informações básicas da pessoa, consulte [**Configurar informações básicas**](#).

3. No painel **Informações adicionais**, insira as informações adicionais da pessoa, incluindo o tipo de identificação da pessoa, número de identificação, cargo, etc., de acordo com as necessidades reais.
4. Confirme para adicionar a pessoa.
 - Clique em **Incluir** para incluir a pessoa e feche a janela Incluir Pessoa.
 - Clique em **Adicionar e Novo** para adicionar a pessoa e continuar a adicionar outras pessoas.

7.4.11 Importar e exportar informações de identificação de pessoa

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

7.4.12 Informações da Pessoa Importada

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

Face Recognition Terminal User Manual

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 pessoa importadora** para baixar o modelo.
6. Insira as informações da pessoa no modelo baixado.

Nota

- Se a pessoa tiver vários cartões, separe o número do cartão com ponto e vírgula.
- Itens com asterisco são obrigatórios.
- 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 em **Importar** para iniciar a importação.

Nota

- Se um nº de pessoa já existe no banco de dados do cliente, exclua as informações existentes antes de importar.
 - Você pode importar informações de no máximo 2.000 pessoas.
-


7.4.13 Importar Imagens de Pessoas

Depois de importar as imagens de rosto das pessoas adicionadas para o cliente, as pessoas nas imagens podem ser identificadas por um terminal de reconhecimento de rosto adicionado. Você pode importar fotos de pessoas uma por uma ou importar várias fotos de uma vez, de acordo com sua necessidade.

Antes que você comece

Certifique-se de ter importado as informações pessoais para o cliente com antecedência.

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: ative **Verificar por dispositivo** para verificar se o dispositivo de reconhecimento de rosto gerenciado no cliente pode reconhecer o rosto na foto.
5. Clique  para selecionar um arquivo de imagem de rosto.

Nota

- A (pasta de) fotos 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 "Person ID_Name". O ID da pessoa deve ser o mesmo das informações da pessoa importada.
-

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

7.4.14 Exportar informações da pessoa

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

Antes que você comece

Certifique-se de adicionar pessoas a uma organização.

Passos

1. Entre no módulo Pessoa.
 2. Opcional: Selecione uma organização na 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. Marque os itens desejados para exportar.
6. Clique em **Exportar** para salvar o arquivo exportado em arquivo CSV / Excel em seu PC.

7.4.15 Exportar fotos de pessoas

Você pode exportar o arquivo de imagem do rosto das pessoas adicionadas e salvá-lo em seu PC.

Antes que você comece

Certifique-se de adicionar pessoas e suas fotos de rosto a uma organização.

Passos

1. Entre no módulo Pessoa.
 2. Opcional: Selecione uma organização na lista.
-

Face Recognition Terminal User Manual

Nota

As fotos de 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 facial exportada é nomeada como "Person ID_Name_0" ("0" é para um rosto totalmente frontal).
-

7.4.16 Obter informações pessoais do dispositivo de controle de acesso

Se o dispositivo de controle de acesso adicionado foi configurado com informações da pessoa (incluindo detalhes da pessoa e informações do cartão emitido), você pode obter as informações da pessoa do dispositivo e importá-las para o cliente para operações futuras.

Passos

Nota

- Se o nome da pessoa armazenado no dispositivo estiver vazio, o nome da pessoa será preenchido com o nº do cartão emitido após a importação para o cliente.
 - O sexo das pessoas será **Masculino** por padrão.
 - 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 este número do cartão ou ID da pessoa não será importada para o cliente.
-

1. Entre no módulo **Pessoa** .
 2. Selecione uma organização para importar as pessoas.
 3. Clique em **Obter do dispositivo** .
 4. Selecione um dispositivo de controle de acesso adicionado ou a estação de inscrição na lista suspensa.
-

Nota

Se você selecionar a estação de inscrição, deverá clicar em **Login** e definir o endereço IP, o número da porta, o nome de usuário e a senha do dispositivo.

5. Clique em **Importar** para começar a importar as informações da pessoa para o cliente.

Nota

Podem ser importados até 2.000 pessoas e 5.000 cartões.

As informações da pessoa, incluindo detalhes da pessoa e os cartões vinculados (se configurados), serão importados para a organização selecionada.

7.4.17 Mover pessoas para outra organização

Você pode mover as pessoas adicionadas para outra organização, se necessário.

Antes que você comece

- Certifique-se de ter adicionado pelo menos duas organizações.
- Certifique-se de ter importado as informações da pessoa.

Passos

1. Entre no módulo **Pessoa** .
2. Selecione uma organização no painel esquerdo.
As pessoas sob a organização serão exibidas no painel direito.
3. Selecione a pessoa a ser movida.
4. Clique em **Alterar organização** .
5. Selecione a organização para a qual mover as pessoas.
6. Clique em **OK** .

7.4.18 Emitir cartões para pessoas em lote

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

Passos


1. Entre no módulo **Pessoa** .
2. Clique em **Cartões de emissão em lote** .
Todas as pessoas adicionadas sem nenhum cartão emitido serão exibidas no painel direito.
3. Opcional: Digite palavras-chave (nome ou ID da pessoa) na caixa de entrada para filtrar a (s) pessoa (s) que precisam emitir os cartões.
4. Opcional: Clique em **Configurações** para definir os parâmetros de emissão do cartão. Para obter detalhes, consulte.


5. Clique em **Inicializar** para inicializar a estação de registro de cartão ou leitor de cartão para torná-lo pronto para a emissão de cartões.
6. Clique na coluna **Nº** do cartão e insira o número do cartão.
 - Coloque o cartão na estação de inscrição de cartão.
 - Passe o cartão no leitor de cartão.
 - Insira manualmente o número do cartão e pressione a tecla **Enter** .A (s) pessoa (s) da lista receberão cartão (ões).

7.4.19 Relatório de perda do cartão

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

Passos

1. Entre no módulo **Pessoa** .
2. Selecione a pessoa para a qual deseja relatar a perda do cartão e clique em **Editar** para abrir a janela Editar pessoa.
3. No painel **Credencial** → **Cartão** , clique em  no cartão adicionado para definir este cartão como cartão perdido.

Após relatar a perda do cartão, a autorização de acesso deste cartão será inválida e inativa. A outra pessoa que receber este cartão não pode acessar as portas passando o cartão perdido.
4. Opcional: se o cartão perdido for encontrado, você pode clicar  para cancelar a perda.

Após cancelar a perda do cartão, a autorização de acesso da pessoa será válida e ativa.
5. Se o cartão perdido for adicionado a um grupo de acesso e o grupo de acesso já estiver aplicado ao dispositivo, após relatar a perda do cartão ou cancelar a perda do cartão, uma janela aparecerá para notificá-lo para aplicar as alterações ao dispositivo. Depois de aplicar ao dispositivo, essas alterações podem ter efeito no dispositivo.

7.4.20 Definir os parâmetros de emissão do cartão

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

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

Modo local: Emissão de 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 inscrição de cartão conectada

Nota

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

Tipo de carta

Este campo está disponível apenas 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 sucesso.

Tipo nº do cartão

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

Criptografia de cartão M1

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

Se o cartão for M1, e se você precisar habilitar a função M1 Card Encryption, você deve habilitar esta função e selecionar o setor do cartão para criptografar.

Modo remoto: emitir cartão pelo 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.

7.5 Configurar Cronograma e Modelo

Você pode configurar o modelo incluindo feriado e programação semanal. Depois de definir o modelo, você pode adotar o modelo configurado para grupos de acesso ao definir os grupos de acesso, de modo que o grupo de acesso terá efeito nas durações de tempo do modelo.

Nota

Para configurações de grupo de acesso, consulte [Definir grupo de acesso para atribuir autorização de acesso a pessoas](#).

7.5.1 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** → **Programação** → **Feriado** para entrar na página Feriado.
 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 um período de feriado à lista de feriados e configure a duração do feriado.
-




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 o tempo de duração, ou seja, nesse período de tempo, o grupo de acesso configurado é ativado.
-

Nota

Podem ser definidas até 8 durações de tempo 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 virar para .
 - Clique na duração do tempo e edite diretamente a hora de início / término na caixa de diálogo exibida.
 - Mova o cursor para o início ou o fim da duração de tempo e arraste para aumentar ou diminuir a duração de tempo quando o cursor muda para .
 - 4) Opcional: selecione as durações de tempo que precisam ser excluídas e clique em  na coluna Operação para excluir a (s) duração (ões) de tempo selecionada.
-

- 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 este período de feriado adicionado da lista de feriados.
6. Clique em **Salvar** .

7.5.2 Adicionar modelo

O modelo inclui programação da semana e feriado. Você pode definir a programação semanal e atribuir a duração do tempo de autorização de acesso para uma pessoa ou grupo diferente. Você também pode selecionar o (s) feriado (s) adicionado (s) ao modelo.

Passos

Nota

Você pode adicionar até 255 modelos no sistema de software.

1. Clique em **Controle de acesso** → **Programação** → **Modelo** para entrar na página Modelo.
-

Nota

Existem dois modelos padrão: o dia todo autorizado e o dia todo negado, e eles não podem ser editados ou excluídos.

Todo o dia autorizado

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

O dia todo 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 deste modelo na caixa Observação.
 5. Edite a programação semanal para aplicá-la ao modelo.
 - 1) Clique na guia **Programação da semana** no painel inferior.
 - 2) Selecione um dia da semana e desenhe a (s) duração (ões) de tempo na barra da linha do tempo.
-

Nota

Podem ser definidas durações de até 8 horas para cada dia da programação da semana.

- 3) Opcional: execute as seguintes operações para editar as durações de tempo.

Face Recognition Terminal User Manual

- 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 virar para .
 - Clique na duração do tempo e edite diretamente a hora de início / término na caixa de diálogo exibida.
 - Mova o cursor para o início ou o fim da duração de tempo e arraste para aumentar ou diminuir a duração de tempo quando o cursor muda para .
- 4) Repita as duas etapas acima para desenhar mais durações de tempo nos outros dias da semana.
6. Adicione um feriado para aplicá-lo ao modelo.
-


Nota

Até 4 feriados podem ser adicionados a um modelo.

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

Nota

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

- 4) Opcional: Selecione um feriado selecionado na lista da direita e clique  para remover o selecionado ou clique em **Limpar** para limpar todos os feriados selecionados na lista da direita.
7. Clique em **Salvar** para salvar as configurações e terminar de adicionar o modelo.

7.6 Definir Grupo de Acesso para Atribuir Autorização de Acesso a Pessoas

Depois de adicionar a pessoa e configurar suas credenciais, você pode criar os grupos de acesso para definir quais pessoas podem obter acesso a quais portas 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 que tenham efeito. As alterações do grupo de acesso incluem alterações de modelo, configurações de grupo de acesso, configurações de grupo de acesso da pessoa e detalhes da pessoa relacionada (incluindo número do cartão, imagem do

Face Recognition Terminal User Manual

rostro, vínculo entre o número do cartão e vínculo entre o número do cartão e a senha do cartão, 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 que você deseja.
4. Selecione um modelo para o grupo de acesso.

Nota

Você deve configurar o modelo antes de acessar as configurações do grupo. Consulte **Configurar programação e modelo** para obter detalhes.

5. Na lista à esquerda do campo Seleccionar Pessoa, selecione a (s) pessoa (s) para atribuir autoridade de acesso.
6. Na lista à esquerda do campo Seleccionar Ponto de Acesso, selecione porta (s), estação (ões) de vídeo porteiro (s) ou andar (es) para as pessoas selecionadas acessarem.
7. Clique em **Salvar**.
Você pode visualizar a (s) pessoa (s) selecionada (s) e os pontos de acesso selecionados no lado direito da interface.

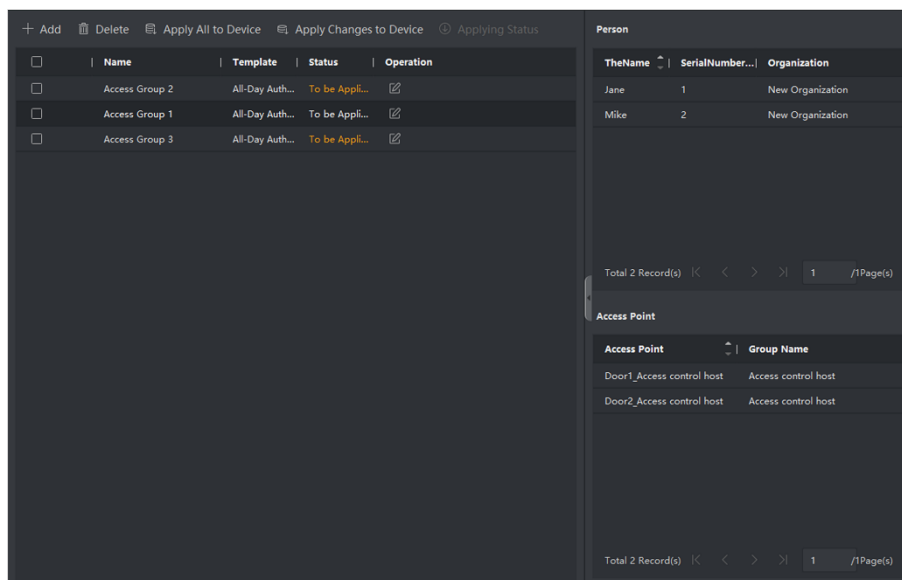


Figura 7-5 Exibir a (s) pessoa (s) e ponto (s) de acesso selecionados

Figura 7-6 Exibir a (s) pessoa (s) e ponto (s) de acesso selecionados

8. Depois de adicionar os grupos de acesso, você precisa aplicá-los ao dispositivo de controle de acesso para que tenham efeito.

Face Recognition Terminal User Manual

- 1) Selecione o (s) grupo (s) de acesso a serem aplicados ao dispositivo de controle de acesso.
- 2) Clique em **Aplicar tudo aos dispositivos para** começar a aplicar todos os grupos de acesso selecionados ao dispositivo de controle de acesso ou estação externa.
- 3) Clique em **Aplicar tudo aos dispositivos** ou **Aplicar alterações aos dispositivos** .

Aplicar tudo aos dispositivos

Esta operação irá limpar todos os grupos de acesso existentes dos dispositivos selecionados e então aplicar o novo grupo de acesso ao dispositivo.

Aplicar alterações aos dispositivos

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

- 4) Visualize o status da aplicação na coluna Status ou clique em **Applying Status** para visualizar todos os grupos de acesso aplicados.

Nota

Você pode marcar **Exibir apenas falhas** para filtrar os resultados da aplicação.

As pessoas selecionadas nos grupos de acesso aplicados terão autorização para entrar / sair das portas / estações externas selecionadas com 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, verá 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** .

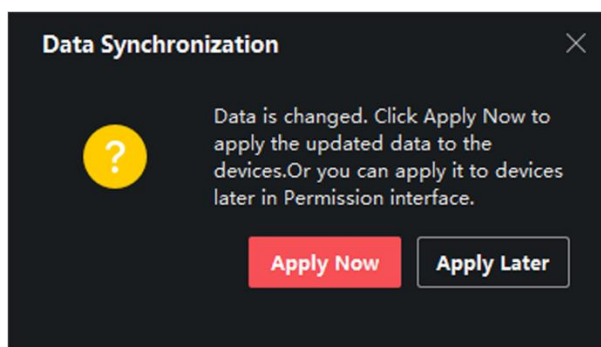



Figura 7-7 Sincronização de dados

7.7 Configurar funções avançadas

Você pode configurar as funções avançadas de controle de acesso para atender a alguns requisitos especiais em diferentes cenários.

Nota

- Para as funções relacionadas ao cartão (o tipo de cartão de controle de acesso), apenas 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 clique em  para personalizar as funções avançadas a serem exibidas.
-

7.7.1 Configurar os 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 Dispositivo de Controle de Acesso

Depois de adicionar o dispositivo de controle de acesso, você pode configurar seus parâmetros, incluindo sobreposição de informações do usuário na imagem, upload de imagens após a captura, salvamento de imagens capturadas, etc.

Passos

1. Clique em **Controle de acesso** → **Função avançada** → **Parâmetro do dispositivo** .
-

Nota

Se você encontrar o parâmetro do dispositivo na lista de funções avançadas, passe o cursor sobre a função avançada e clique em  para selecionar o parâmetro do dispositivo a ser exibido.

2. Selecione um dispositivo de acesso para mostrar seus parâmetros na página direita.
 3. Gire a chave para ON para habilitar as funções correspondentes.
-

Nota

- Os parâmetros exibidos podem variar para diferentes dispositivos de controle de acesso.
-

Face Recognition Terminal User Manual

- Alguns dos parâmetros a seguir não estão listados na página Informações básicas, clique em **Mais** para editar os parâmetros.
-

Comando de voz

Se você ativar esta função, o prompt de voz será ativado no dispositivo. Você pode ouvir o prompt de voz ao operar no dispositivo.

Faça o upload da foto. Após a captura vinculada

Carregue as fotos capturadas pela câmera vinculada ao sistema automaticamente.

Salvar foto. Após a captura vinculada

Se você habilitar esta função, você pode salvar a imagem capturada pela câmera conectada ao dispositivo.

Modo de reconhecimento facial

Modo normal

Reconhecer rosto pela câmera normalmente.

Modo Profundo

O dispositivo pode reconhecer uma faixa de pessoas muito mais ampla do que o modo normal. Este modo é aplicável a um ambiente mais complicado.

Habilitar cartão NFC

Se ativar a função, o dispositivo pode reconhecer o cartão NFC. Você pode apresentar o cartão NFC no dispositivo.

Habilitar cartão M1

Se habilitar a função, o dispositivo pode reconhecer o cartão M1. Você pode apresentar o cartão M1 no dispositivo.

Habilitar cartão EM

Se habilitar a função, o dispositivo pode reconhecer o cartão EM. Você pode apresentar o cartão EM no dispositivo.

Habilitar placa de CPU

Reservado. Se habilitar a função, o dispositivo pode reconhecer a placa da CPU. Você pode apresentar o cartão da CPU no dispositivo.

Habilitar cartão de identificação


Reservado. Se ativar a função, o dispositivo pode reconhecer o cartão de identificação. Você pode apresentar o cartão de identificação no dispositivo.

4. Clique em **OK** .
5. Opcional: Clique em **Copiar para** e selecione o (s) dispositivo (s) de controle de acesso para copiar os parâmetros da página para o (s) dispositivo (s) selecionado (s).

Configurar Parâmetros para Porta

Depois de adicionar o dispositivo de controle de acesso, você pode configurar seus parâmetros de ponto de acesso (porta).

Passos

1. Clique em **Controle de acesso** → **Função avançada** → **Parâmetro do dispositivo** .
2. Selecione um dispositivo de controle de acesso no painel esquerdo e clique em  para mostrar as portas ou pisos do dispositivo selecionado.
3. Selecione uma porta ou piso para mostrar seus parâmetros na página certa.
4. Edite os parâmetros da porta ou do piso.

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 aberto. Normalmente permanece fechado.

Tipo de botão de saída

Você pode definir o botão de saída como permanecendo fechado ou aberto. Normalmente, ele permanece aberto.

Tempo de porta fechada

Depois de passar o cartão normal e a ação de retransmissão, o cronômetro para trancar a porta começa a funcionar.

Duração Aberta Estendida

O contato da porta pode ser habilitado com o atraso apropriado após a pessoa com necessidade de acesso estendido passar seu cartão.

Alarme de tempo limite de porta esquerda aberta

Face Recognition Terminal User Manual

O alarme pode ser disparado se a porta não for fechada em um período de tempo configurado. Se for definido como 0, nenhum alarme será acionado.

Código de Coação

A porta pode ser aberta inserindo o código de coação quando houver coação. Ao mesmo tempo, o cliente pode relatar o evento de coação.

Super senha

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

Nota

- O código de coação e a super senha devem ser diferentes.
 - O código de coação e a super senha devem ser diferentes da senha de autenticação.
 - O comprimento do código de coação e da super senha está de acordo com o dispositivo, geralmente deve conter de 4 a 8 dígitos.
-

5. Clique em **OK** .
 6. Opcional: Clique em **Copiar para** e selecione a porta para copiar os parâmetros na página para as portas selecionadas.
-


Nota

As configurações de duração do status da porta ou do piso também serão copiadas para a porta selecionada.

Configurar parâmetros para leitor de cartão

Depois de adicionar o dispositivo de controle de acesso, você pode configurar seus parâmetros de leitor de cartão.

Passos

1. Clique em **Controle de acesso** → **Função avançada** → **Parâmetro do dispositivo** .
 2. Na lista de dispositivos à esquerda, clique em  para expandir a porta, selecione um leitor de cartão e você pode editar os parâmetros do leitor de cartão à direita.
 3. Edite os parâmetros básicos do leitor de cartão na página Informações básicas.
-

Nota

- Os parâmetros exibidos podem variar para diferentes dispositivos de controle de acesso. Há parte dos parâmetros listados a seguir. Consulte o manual do usuário do dispositivo para obter mais detalhes.
 - Alguns dos parâmetros a seguir não estão listados na página Informações básicas, clique em **Avançado** para editar os parâmetros.
-

Informação básica

Nome

Edite o nome do leitor de cartão conforme desejado.

Intervalo mínimo de passagem do cartão

Se o intervalo entre a passagem do cartão do mesmo cartão for menor que o valor definido, a passagem do cartão é inválida. Você pode defini-lo como 0 a 255.

Alarme de Max. Tentativas falhas

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

Tipo de leitor de cartão / Descrição do leitor de cartão

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

Avançado

Habilitar leitor de cartão

Habilite a função e o dispositivo pode ser usado como leitor de cartão.

Polaridade do LED OK / Polaridade do LED de erro / Polaridade da campainha

Definir OK Polaridade LED / Erro LED Polaridade / Buzzer LED Polaridade da placa principal de acordo com os parâmetros do leitor de cartão. Geralmente, adota as configurações padrão.

Máx. Intervalo ao entrar no PWD

Ao inserir a senha no leitor de cartão, se o intervalo entre o pressionamento de dois dígitos for maior que o valor definido, os dígitos pressionados antes serão apagados automaticamente.

Detecção de adulteração

Ative a detecção anti-violação para o leitor de cartão.

Comunique-se com o controlador a cada

Quando o dispositivo de controle de acesso não puder se conectar ao leitor de cartão por mais tempo do que o definido, o leitor de cartão ficará off-line automaticamente.

Face 1: N Limiar de correspondência

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

Intervalo de reconhecimento facial

Face Recognition Terminal User Manual

O intervalo de tempo entre dois reconhecimentos contínuos de rosto durante a autenticação. Por padrão, é 2s.

Anti-spoofing facial

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

Limite de correspondência de face 1: 1

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

Modo de Aplicação

Você pode selecionar modos de aplicação internos ou outros de acordo com o ambiente real.

Bloqueio de rosto com falha de autenticação

Após ativar a função de detecção de rosto ao vivo, o sistema irá bloquear o rosto do usuário por 5 minutos se a detecção de rosto ao vivo falhar por mais do que as tentativas configuradas. O mesmo usuário não consegue autenticar por meio do rosto falso em 5 minutos. Dentro de 5 minutos, o usuário pode autenticar via face real duas vezes continuamente para desbloquear.

Nível de segurança de detecção de vivacidade

Depois de ativar a função de detecção de rosto ao vivo, você pode definir o nível de segurança correspondente ao executar a autenticação de rosto ao vivo.

4. Clique em **OK** .
5. Opcional: Clique em **Copiar para** e selecione o (s) leitor (es) de cartão para copiar os parâmetros da 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 pode configurar os parâmetros.

Passos

1. Clique em **Controle de acesso** → **Função avançada** → **Parâmetro do dispositivo** para entrar na página de configuração do parâmetro de controle de acesso.
2. Na lista de dispositivos à esquerda, clique em 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 de alarme.

Nome

Edite o nome do leitor de cartão conforme desejado.

Tempo de ativação da saída de alarme

Quanto tempo a saída de alarme irá durar após o acionamento.

4. Clique em **OK**.
5. Opcional: Defina a chave no canto superior direito para **ON** para acionar a saída de alarme.

7.7.2 Configurar Aberto / Fechado Restante

Você pode definir o status da porta como aberta ou fechada. Por exemplo, você pode definir a permanência da porta fechada no feriado e definir a permanência da porta aberta no período especificado do dia útil.

Antes que você comece



Adicione os dispositivos de controle de acesso ao sistema.

Passos

1. Clique em **Controle de acesso** → **Função avançada** → **Permanecer aberto / fechado** para entrar na página Permanecer aberto / fechado.
2. Selecione a porta que precisa ser configurada no painel esquerdo.
3. Para definir o status da porta durante o dia de trabalho, clique em **Agenda da semana** e execute as seguintes operações.
 - 1) Clique em **Permanecer aberto** ou **Permanecer fechado**.
 - 2) Arraste o cursor para desenhar o tempo de duração, ou seja, nesse período de tempo, o grupo de acesso configurado é ativado.

Nota

Podem ser definidas até 8 durações de tempo para cada dia da 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 virar para .
 - Clique na duração do tempo e edite diretamente a hora de início / término na caixa de diálogo exibida.
 - Mova o cursor para o início ou o fim da duração de tempo e arraste para aumentar ou diminuir a duração de tempo quando o cursor muda para .
- 4) Clique em **Salvar**.

Operações Relacionadas






Face Recognition Terminal User Manual

Copiar para a semana inteira	Selecione uma duração na barra de tempo, clique em Copiar para a semana inteira para copiar todas as configurações de duração nesta barra de tempo para outros dias da semana.
Excluir selecionado	Selecione uma duração na barra de tempo, clique em Excluir selecionados para excluir esta duração.
Claro	Clique em Limpar para limpar todas as configurações de duração na programação semanal.

4. Para definir o status da porta durante o feriado, clique em **Feriado** e execute as seguintes operações.
- 1) Clique em **Permanecer aberto** ou **Permanecer fechado**.
 - 2) Clique em **Adicionar**.
 - 3) Insira a data de início e a data de término.
 - 4) Arraste o cursor para desenhar a duração do tempo, ou seja, nessa duração de tempo, o grupo de acesso configurado é ativado.

Nota

Podem ser definidas até 8 durações de tempo para um período de férias.

- 5) Execute as seguintes operações para editar as durações do 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 virar para .
 - Clique na duração do tempo e edite diretamente a hora de início / término na caixa de diálogo exibida.
 - Mova o cursor para o início ou o fim da duração de tempo e arraste para aumentar ou diminuir a duração de tempo quando o cursor muda para .
- 6) Opcional: Selecione as durações de tempo que precisam ser excluídas e clique em  na coluna Operação para excluir a (s) duração (ões) de tempo selecionada.
- 7) Opcional: Clique  na coluna Operação para limpar todas as durações de tempo na barra de tempo.
- 8) Opcional: Clique  na coluna Operação para excluir este período de feriado adicionado da lista de feriados.
- 9) Clique em **Salvar**.
5. Opcional: Clique em **Copiar para** para copiar as configurações de status da porta desta porta para outra (s) porta (s).

7.7.3 Configurar autenticação multifator

Você pode gerenciar as pessoas por grupo e definir a autenticação para várias pessoas de um ponto de controle de acesso (porta).

Antes que você comece

Defina o grupo de acesso e aplique o grupo de acesso ao dispositivo de controle de acesso. Para obter detalhes, consulte [Definir grupo de acesso para atribuir autorização de acesso a pessoas](#).

Execute esta tarefa quando quiser definir autenticações para vários cartões de um ponto de controle de acesso (porta).

Passos

1. Clique em **Controle de acesso** → **Função avançada** → **Autenticação multifator**.
2. Selecione um dispositivo de controle de acesso na lista de dispositivos no painel esquerdo.
3. Adicione uma pessoa / grupo de cartões para o dispositivo de controle de acesso.
 - 1) Clique em **Adicionar** no painel direito.
 - 2) Crie um nome para o grupo conforme desejado.
 - 3) Especifique a hora de início e a hora de término do período de vigência para a pessoa / grupo de cartões.
- 4) Selecione o (s) membro (s) e o (s) cartão (ões) na lista Disponível, e o (s) membro (s) e cartão (ões) selecionados serão adicionados à lista Selecionado.

Nota

Certifique-se de ter emitido o cartão para a pessoa.

Certifique-se de ter definido o grupo de acesso e aplicado o grupo de acesso ao dispositivo de controle de acesso com êxito.

- 5) Clique em **Salvar**.
- 6) Opcional: Selecione a pessoa / grupo (s) de cartão e clique em **Excluir** para excluí-los.
- 7) Opcional: Selecione a pessoa / grupo (s) de cartão e clique em **Aplicar** para reaplicar o grupo de acesso que não foi aplicado anteriormente ao dispositivo de controle de acesso.
4. Selecione um ponto de controle de acesso (porta) do dispositivo selecionado no painel esquerdo.
5. Insira o intervalo máximo ao inserir a senha.
6. Adicione um grupo de autenticação para o ponto de controle de acesso selecionado.
 - 1) Clique em **Adicionar** no painel Grupos de autenticação.
 - 2) Selecione um modelo configurado como o modelo de autenticação na lista suspensa.

Nota

Para definir o modelo, consulte [Configurar programação e modelo](#).

- 3) Selecione o tipo de autenticação como **Autenticação local** , **Autenticação local e Porta aberta remotamente** ou **Autenticação local e Super senha** na lista suspensa.

Autenticação Local

Autenticação pelo dispositivo de controle de acesso.

Autenticação local e porta aberta remotamente

Autenticação pelo dispositivo de controle de acesso e pelo cliente. Quando a pessoa passa o cartão no dispositivo, uma janela é exibida. Você pode destrancar a porta através do cliente.

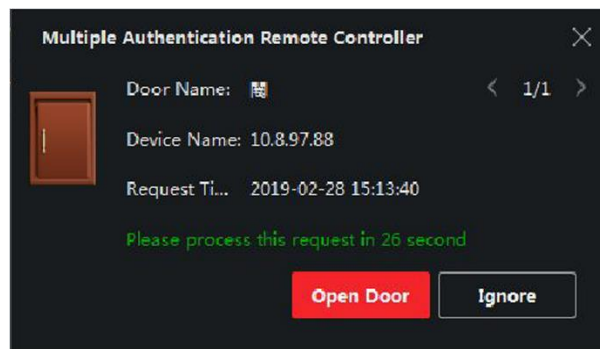


Figura 7-8 Porta aberta remotamente

Nota

Você pode marcar a **Autenticação offline** para habilitar a autenticação de super senha quando o dispositivo de controle de acesso for desconectado do cliente.

Autenticação local e super senha

Autenticação pelo dispositivo de controle de acesso e pela super senha.

- 4) Selecione a pessoa / grupo de cartão adicionado na lista à esquerda abaixo e ele será adicionado à lista Selecionado à direita como o grupo de autenticação.
- 5) Clique no grupo de autenticação adicionado na lista da direita para definir os horários de autenticação na coluna Auth Times.
-

Nota

- Os tempos de autenticação devem ser maiores que 0 e menores que a quantidade de pessoal adicionada ao grupo de pessoal.
 - O valor máximo de tempos de autenticação é 16.
-

- 6) Clique em **Salvar** .
-

Nota

- Para cada ponto de controle de acesso (porta), até quatro grupos de autenticação podem ser adicionados.
 - Para o grupo de autenticação cujo tipo de autenticação é **Autenticação local** , até 8 grupos de pessoas / cartões podem ser adicionados ao grupo de autenticação.
 - Para o grupo de autenticação cujo tipo de autenticação é **Autenticação local e Super senha** ou **Autenticação local e porta aberta remotamente** , até 7 grupos de pessoas / cartões podem ser adicionados ao grupo de autenticação.
-

7. Clique em **Salvar** .

7.7.4 Configurar modo de autenticação do leitor de cartão e programação

Você pode definir as regras de passagem para o leitor de cartão do dispositivo de controle de acesso de acordo com suas necessidades reais.

Passos

1. Clique em **Controle de acesso** → **Função avançada** → **Autenticação** para entrar na página de configuração do modo de autenticação.
2. Selecione um leitor de cartão à esquerda para configurar.
3. Defina o modo de autenticação do leitor de cartão.
 - 1) Clique em **Configuração** .

Face Recognition Terminal User Manual

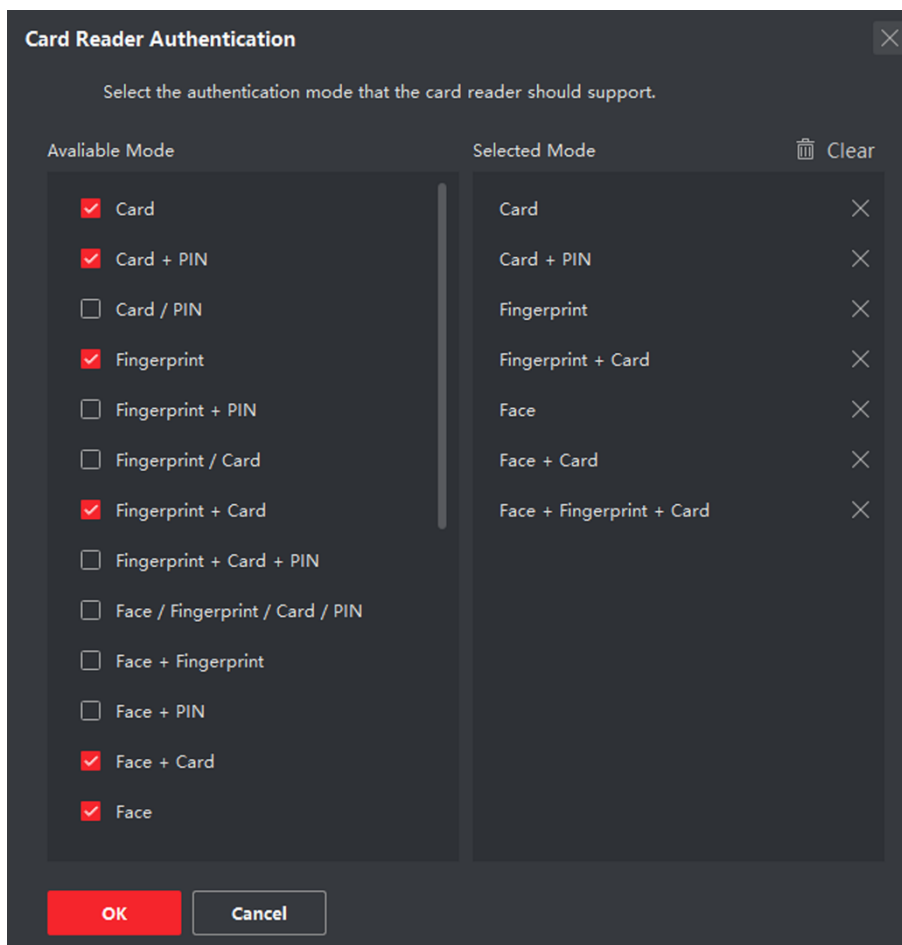


Figura 7-9 Seleccione o modo de autenticação do leitor de cartão

Nota

PIN refere-se ao código PIN definido para abrir a porta. Consulte [**Configurar informações de controle de acesso**](#) .

- 2) Verifique os modos na lista de modos disponíveis e eles serão adicionados à lista de modos selecionados.
- 3) Clique em **OK** .
Depois de selecionar os modos, os modos selecionados serão exibidos como ícones com cores diferentes.
4. Clique no ícone para selecionar um modo de autenticação do leitor de cartão e arraste o cursor para desenhar uma barra colorida na programação, o que significa que nesse período de tempo a autenticação do leitor de cartão é válida.
5. Repita a etapa acima para definir outros períodos de tempo.

Face Recognition Terminal User Manual

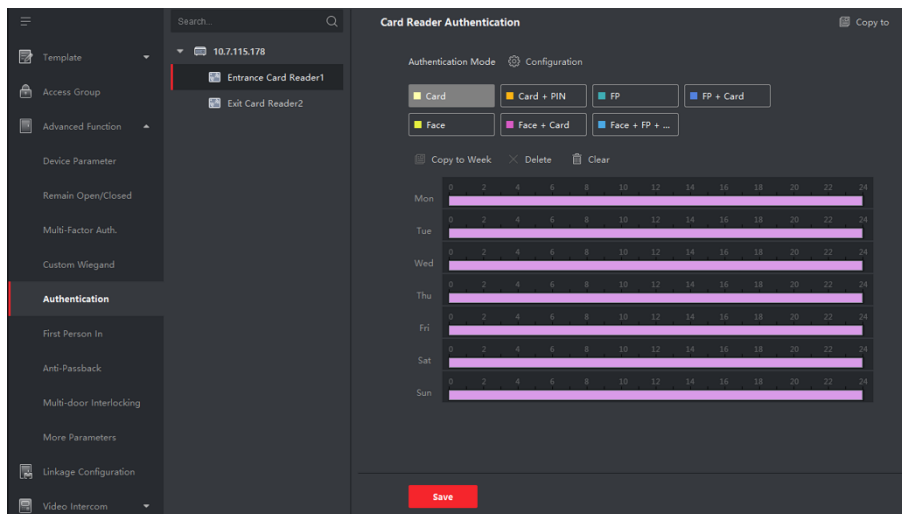


Figura 7-10 Definir modos de autenticação para leitores de cartão

6. Opcional: Selecione um dia configurado e clique em **Copiar para a semana** para copiar as mesmas configurações para a semana inteira.
7. Opcional: Clique em **Copiar para** para copiar as configurações para outros leitores de cartão.
8. Clique em **Salvar** .

7.7.5 Configurar Primeira Pessoa em

Você pode definir várias primeiras pessoas para um ponto de controle de acesso. Depois que a primeira pessoa é autorizada, ele permite que várias pessoas acessem a porta ou outras ações de autenticação.

Antes que você comece

Defina o grupo de acesso e aplique o grupo de acesso ao dispositivo de controle de acesso. Para obter detalhes, consulte **Definir grupo de acesso para atribuir autorização de acesso a pessoas** .

Execute esta tarefa quando quiser configurar a abertura da porta com a primeira pessoa.

Passos

1. Clique em **Controle de acesso** → **Função avançada** → **Primeira pessoa** a entrar para entrar na página **Primeira pessoa** a entrar.
2. Selecione um dispositivo de controle de acesso na lista do painel esquerdo.
3. Selecione o modo atual como **Ativar restante aberto após a primeira pessoa** ou **Desativar restante aberto após a primeira pessoa** na lista suspensa para cada ponto de controle de acesso do dispositivo selecionado.

Habilitar Permanente Aberto após a Primeira Pessoa

Face Recognition Terminal User Manual

A porta permanece aberta pelo período de tempo configurado após a primeira pessoa ser autorizada até que o período de permanência aberta termine. Se você selecionar este modo, deverá definir a duração de permanência em aberto.

Nota

A duração da permanência em aberto deve ser entre 0 e 1440 minutos. Por padrão, a duração de permanência aberta é de 10 minutos.

Desativar restante aberto após a primeira pessoa

Desative a função de primeira pessoa em, ou seja, autenticação normal.

Nota

Você pode autenticar pela primeira pessoa novamente para desativar o modo de primeira pessoa.

4. Clique em **Adicionar** no painel Lista da primeira pessoa.
5. Selecione a (s) pessoa (s) na lista à esquerda e a (s) pessoa (s) serão adicionadas às pessoas selecionadas como a (s) primeira (s) pessoa (s) nas portas.
A (s) primeira (s) pessoa (s) adicionada (s) será (ão) listada (s) na Lista da primeira pessoa
6. Opcional: Selecione uma primeira pessoa da lista e clique em **Excluir** para remover a pessoa da lista de primeira pessoa.
7. Clique em **Salvar** .

7.7.6 Configurar o Anti- Pass back

Você pode definir para passar apenas pelo ponto de controle de acesso de acordo com o caminho especificado e apenas uma pessoa poderia passar pelo ponto de controle de acesso após passar o cartão.

Antes que você comece

Ative a função anti-passagem de volta do dispositivo de controle de acesso.


Execute esta tarefa quando quiser configurar o anti-passagem de volta para o dispositivo de controle de acesso.

Passos

Nota

Tanto a função anti-passagem de volta quanto a função de intertravamento de múltiplas portas podem ser configuradas para um dispositivo de controle de acesso ao mesmo tempo. Para a configuração de intertravamento de múltiplas portas, consulte.

Face Recognition Terminal User Manual

1. Clique em **Controle de acesso** → **Função avançada** → **Anti-Pass back** para entrar na página de configurações do pacote Anti-Pass.
 2. Selecione um dispositivo de controle de acesso no painel esquerdo.
 3. Selecione um leitor de cartão como o início do caminho no campo **Primeiro leitor de cartão** .
 4. Clique  no primeiro leitor de cartão selecionado na coluna **Leitor de cartão depois** para abrir o diálogo de seleção do leitor de cartão.
 5. Selecione os leitores de cartão posteriores para o primeiro leitor de cartão.
-

Nota

Até quatro leitores de cartão posteriores podem ser adicionados como leitores de cartão posteriores para um leitor de cartão.

6. Clique em **OK** na caixa de diálogo para salvar as seleções.
7. Clique em **Salvar** na página Configurações do Anti-Pass Back para salvar as configurações e entrar em vigor.

Exemplo

Definir o caminho de passagem do cartão Se você selecionar Reader in_01 como o início e selecionar Reader in_02, Reader Out_04 como os leitores de cartão vinculados. Então, você só pode passar pelo ponto de controle de acesso passando o cartão na ordem como Leitor in_01, Leitor in_02 e Leitor Saída_04.

7.7.7 Configurar os parâmetros do dispositivo

Depois de adicionar o dispositivo de controle de acesso, você pode definir seus parâmetros, como parâmetros de rede.

Definir vários parâmetros de NIC

Se o dispositivo oferece suporte a várias interfaces de rede, você pode definir os parâmetros de rede dessas NICs por meio do cliente, como endereço IP, endereço MAC, número da porta, etc.

Passos

Nota

Esta função deve ser suportada pelo dispositivo.

1. Entre no módulo de 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 **NIC** para entrar na página Multiple NIC Settings.
 4. Selecione uma NIC que deseja configurar na lista suspensa.
-

5. Defina seus parâmetros de rede, como endereço IP, gateway padrão, máscara de sub-rede, etc.

Endereço MAC

Um endereço de controle de acesso à mídia (endereço MAC) é um identificador exclusivo atribuído à interface de rede para comunicações no segmento físico da rede.

MTU

A unidade de transmissão máxima (MTU) da interface de rede.

6. Clique em **Salvar** .

Definir parâmetros de rede

Depois de adicionar o dispositivo de controle de acesso, você pode definir o modo de upload de registro do dispositivo e criar uma conta ISUP via rede com fio.

Definir modo de upload de registro

Você pode definir o modo do dispositivo para fazer upload de registros por meio do protocolo ISUP.

Passos

1. Entre no módulo de 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 entre em **Rede** → **Modo de Upload** .
4. Selecione o grupo central na lista suspensa.
5. Marque **Habilitar** para habilitar para definir o modo de upload.
6. Selecione o modo de upload na lista suspensa.
 - Habilite **N1** ou **G1** para o canal principal e o canal de backup.Selecione **Fechar** para desativar o canal principal ou o canal de backup

Nota

O canal principal e o canal de backup não podem habilitar N1 ou G1 ao mesmo tempo.

7. Clique em **Salvar** .

Criar conta ISUP no modo de comunicação com fio

Você pode definir a conta para o protocolo ISUP no modo de comunicação com fio. Então você pode adicionar dispositivos via protocolo ISUP.

Passos

Nota

Esta função deve ser suportada pelo dispositivo.

1. Entre no módulo de 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 entre em **Rede** → **Centro de Rede** .
 4. Selecione o grupo central na lista suspensa.
 5. Selecione o **Tipo de endereço** como **Endereço IP** ou **Nome de domínio** .
 6. Insira o endereço IP ou nome de domínio de acordo com o tipo de endereço.
 7. Digite o número da porta para o protocolo.
-

Nota

O número da porta da rede sem fio e da rede com fio deve ser consistente com o número da porta do ISUP.

8. Selecione o **tipo de protocolo** como **ISUP** .
9. Defina um nome de conta para o centro de rede.
10. Clique em **Salvar** .

Definir parâmetros de captura do dispositivo

Você pode configurar os parâmetros de captura do dispositivo de controle de acesso, incluindo captura manual e captura acionada por evento.

Nota

- A função de captura deve ser suportada pelo dispositivo.
 - Antes de definir os parâmetros de captura, você deve definir o armazenamento de imagens primeiro para definir onde as imagens disparadas por evento são salvas. Para obter detalhes, consulte *Definir armazenamento de imagens* no manual do usuário do software cliente.
-

Definir parâmetros de captura acionada

Quando ocorre um evento, a câmera do dispositivo de controle de acesso pode ser acionada para capturar a (s) imagem (ns) para registrar o que acontece quando o evento ocorre. Você pode ver as imagens capturadas ao verificar os detalhes do evento no Event Center. Antes disso, você precisa definir os parâmetros para a captura, como número de fotos capturadas por vez.

Antes que você comece

Antes de definir os parâmetros de captura, você deve definir o armazenamento de fotos primeiro para definir onde as fotos capturadas serão salvas. Para obter detalhes, consulte *Definir armazenamento de imagens* no manual do usuário do software cliente.

Passos

Nota

Esta função deve ser suportada pelo dispositivo

1. Entre no módulo de controle de acesso.
2. Na barra de navegação à esquerda, insira **Função avançada** → **Mais parâmetros** → **Captura** .
3. Selecione um dispositivo de controle de acesso na lista de dispositivos e selecione **Captura vinculada** .
4. Defina o tamanho e a qualidade da imagem.
5. Defina os tempos de captura, uma vez acionado, o que define quantas fotos serão capturadas por vez.
6. Se o tempo de captura for maior que 1, defina o intervalo para cada captura.
7. Clique em **Salvar** .

Definir parâmetros de captura manual

No módulo Monitoramento de status, você pode capturar uma imagem manualmente pela câmera do dispositivo de controle de acesso clicando em um botão. Antes disso, você precisa definir os parâmetros de captura, como a qualidade da imagem.

Antes que você comece

Antes de definir os parâmetros de captura, você deve definir o caminho de salvamento primeiro para definir onde as imagens capturadas serão salvas. Para obter detalhes, consulte *Definir armazenamento de imagens* no manual do usuário do software cliente.

Passos

Nota

Esta função deve ser suportada pelo dispositivo

1. Entre no módulo de controle de acesso.
2. Na barra de navegação à esquerda, insira **Função avançada** → **Mais parâmetros** → **Captura** .
3. Selecione um dispositivo de controle de acesso na lista de dispositivos e selecione **Captura manual** .
4. Selecione a resolução das imagens capturadas na lista suspensa.
5. Selecione a qualidade da imagem como **Alta** , **Média** ou **Baixa** . Quanto maior for a qualidade da imagem; quanto maior será o tamanho da imagem.
6. Clique em **Salvar** .

Definir parâmetros para terminal de reconhecimento facial

Face Recognition Terminal User Manual

Para o terminal de reconhecimento de rosto, você pode definir seus parâmetros, incluindo banco de dados de fotos de rosto, etc.

Passos

Nota

Esta função deve ser suportada pelo dispositivo.

1. Entre no módulo de controle de acesso.
 2. Na barra de navegação à esquerda, insira **Função avançada** → **Mais parâmetros** .
 3. Selecione um dispositivo de controle de acesso na lista de dispositivos e clique em **Terminal de reconhecimento facial** .
 4. Defina os parâmetros.
-

Nota

Esses parâmetros exibidos variam de acordo com os diferentes modelos de dispositivos.

Algoritmo

Selecione **Deep Learning** como banco de dados de imagens faciais.

Salvar foto de rosto de autenticação

Se ativado, a imagem do rosto capturada durante a autenticação será salva no dispositivo.

Modo Eco

Depois de ativar o modo ECO, o dispositivo pode autenticar rostos em ambientes com pouca luz ou escuro. E você pode definir o limite do modo ECO, modo ECO (1: N) e modo ECO (1: 1).

Modo ECO (1: 1)

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

Modo ECO (1: N)

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

Limiar do modo ECO

Ao habilitar o modo ECO, você pode definir o limite do modo ECO. Quanto maior o valor, mais fácil será o dispositivo entrar no modo ECO. Faixa disponível: 0 a 8.

Modo de trabalho

Defina o modo de trabalho do dispositivo 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.

5. Clique em **Salvar** .

Ativar criptografia de cartão M1

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

Passos

Nota

A função deve ser suportada pelo dispositivo de controle de acesso e leitor de cartão.

1. Entre no módulo de 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 chave como ligada para ativar a função de criptografia do cartão M1.
 5. Defina o ID do setor.
-

Nota

- O ID do setor varia de 1 a 100.
 - Por padrão, o Setor 13 é criptografado. Recomenda-se criptografar o setor 13.
-

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

Definir parâmetros RS-485

Você pode definir os parâmetros RS-485 do dispositivo de controle de acesso, incluindo taxa de transmissão, bit de dados, bit de parada, tipo de paridade, tipo de controle de fluxo, modo de comunicação, modo de trabalho e modo de conexão.

Passos

Nota

As configurações RS-485 devem ser suportadas pelo dispositivo.

1. Entre no módulo de controle de acesso.
 2. Na barra de navegação à esquerda, insira **Função avançada** → **Mais parâmetros** .
-

Face Recognition Terminal User Manual

3. Selecione um dispositivo de controle de acesso na lista de dispositivos e clique em **RS-485** para entrar na página de configurações RS-485.
 4. Selecione o número da porta serial na lista suspensa para definir os parâmetros RS-485.
 5. Defina a taxa de transmissão, bit de dados, bit de parada, tipo de paridade, modo de comunicação, modo de trabalho e modo de conexão na lista suspensa.
-

Nota

Quando o modo de conexão é **Conectar dispositivo de controle de acesso**, você pode selecionar **Nº do cartão** ou **ID da pessoa** como o tipo de saída.

6. Clique em **Salvar**.
 - Os parâmetros configurados serão aplicados ao dispositivo automaticamente.
 - Ao alterar o modo de trabalho ou o modo de conexão, o dispositivo será reiniciado 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 cartão Wiegand via comunicação Wiegand.

Passos

Nota

Esta função deve ser suportada pelo dispositivo.

1. Entre no módulo de controle de acesso.
 2. Na barra de navegação à esquerda, insira **Função avançada** → **Mais parâmetros**.
 3. Selecione um dispositivo de controle de acesso na lista de dispositivos e clique em **Wiegand** para entrar na página Configurações de Wiegand.
 4. Coloque a chave em on para habilitar a função Wiegand para o dispositivo.
 5. Selecione o nº do canal Wiegand e o modo de comunicação na lista suspensa.
-

Nota

Se você definir a **Direção de comunicação** como **Envio**, será necessário definir o **Modo Wiegand** como **Wiegand 26** ou **Wiegand 34**.

6. Marque **Habilitar Wiegand** para habilitar a função Wiegand.
 7. Clique em **Salvar**.
 - Os parâmetros configurados serão aplicados ao dispositivo automaticamente.
-

- Depois de alterar a direção da comunicação, o dispositivo será reiniciado automaticamente.

7.8 Configurar ações de ligação para controle de acesso

Você pode configurar diferentes ações de vinculação para o evento detectado pelo dispositivo de controle de acesso. Depois disso, as ações de ligação serão acionadas assim que o evento acontecer. Este mecanismo é usado para notificar o pessoal de segurança do evento, ou acionar o controle automático de acesso em tempo real.

Dois tipos de ações de ligação são suportados:

- **Ações do cliente:** Quando o evento é detectado, ele irá disparar as ações no cliente, como o cliente fazendo um aviso sonoro.
- **Ações do dispositivo:** quando o evento for detectado, ele irá desencadear as ações de um dispositivo específico, como zumbido de um leitor de cartão e abertura / fechamento de uma porta,

7.8.1 Configurar ações do cliente para eventos de acesso

Mesmo se você estiver longe de um ponto de acesso, você ainda pode saber o que acontece e quão urgente é o evento, configurando ações vinculadas de evento de acesso no cliente. Você será notificado no cliente assim que um evento for disparado, para que possa responder ao evento instantaneamente. Você também pode configurar ações de cliente de pontos de acesso em um lote por vez.

Passos

Nota

As ações de vinculação aqui se referem à vinculação das próprias ações do software cliente, como aviso sonoro, vinculação de e-mail, etc.

1. Clique em **Gerenciamento de eventos** → **Evento de controle de acesso** .
Os dispositivos de controle de acesso adicionados serão exibidos na lista de dispositivos.
2. Selecione um recurso (incluindo dispositivo, entrada de alarme, porta / elevador e leitor de cartão) na lista de dispositivos.
Os tipos de eventos suportados pelo recurso selecionado serão exibidos.
3. Selecione o (s) evento (s) e clique em **Editar Prioridade** para definir a prioridade do (s) evento (s), que pode ser usado para filtrar eventos no Centro de Eventos.
4. Defina as ações de vinculação do evento.
 - 1) Selecione o (s) evento (s) e clique em **Editar ligação** para definir as ações do cliente quando os eventos forem disparados.

Aviso Audível

O software cliente dá um aviso sonoro quando o alarme é acionado. Você pode selecionar o som do alarme para aviso audível.

Nota

Para definir o som do alarme, consulte *Definir o som do alarme* no manual do usuário do software cliente.

Enviar email

Envie uma notificação por e-mail das informações de alarme para um ou mais destinatários.

Para obter detalhes sobre como definir parâmetros de e-mail, consulte *Definir parâmetros de e-mail* no manual do usuário do software cliente.

2) Clique em **OK** .

5. Habilite o evento para que quando o evento for detectado, um evento seja enviado ao cliente e as ações de vinculação sejam acionadas.
6. Opcional: Clique em **Copiar para ...** para copiar as configurações do evento para outro dispositivo de controle de acesso, entrada de alarme, porta ou leitor de cartão.

7.8.2 Configurar ações do dispositivo para eventos de acesso

Você pode definir as ações de vinculação do dispositivo de controle de acesso para o evento disparado do dispositivo de controle de acesso. Quando o evento é disparado, ele pode disparar a saída de alarme, a campainha do host e outras ações no mesmo dispositivo.

Passos

Nota

Deve ser suportado pelo dispositivo.

1. Clique em **Controle de acesso** → **Configuração de ligação** .
2. Selecione o dispositivo de controle de acesso na lista à esquerda.
3. Clique no botão **Adicionar** para adicionar uma nova ligação.
4. Selecione a origem do evento como **Event Linkage** .
5. selecione o tipo de evento e o evento detalhado para definir a ligação.
6. Na área Linkage Target, defina o destino da propriedade para habilitar esta ação.

Buzzer no controlador

O aviso sonoro do dispositivo de controle de acesso será acionado.

Capturar

A captura em tempo real será acionada.

Ponto de acesso

O status de porta aberta, fechada, permanecer aberta e permanecer fechada será acionado.

Nota

A porta de destino e a porta de origem não podem ser iguais.

7. Clique em **Salvar** .
8. Opcional: depois de adicionar a ligação do dispositivo, você pode fazer um ou mais dos seguintes:

Editar configurações de ligação Selecione as configurações de vinculação definidas na lista de dispositivos e você pode editar seus parâmetros de origem do evento, incluindo origem do evento e destino de vinculação.

Excluir configurações de ligação Selecione as configurações de vinculação definidas na lista de dispositivos e clique em **Excluir** para excluí-lo.

7.8.3 Configurar ações do dispositivo para passagem do cartão

Você pode definir as ações de vinculação do dispositivo de controle de acesso para a passagem de cartão especificada. Quando você passa o cartão especificado, ele pode acionar a campainha do host e outras ações no mesmo dispositivo.

Passos

Nota

Deve ser suportado pelo dispositivo.

1. Clique em **Controle de acesso** → **Configuração de ligação** .
2. Selecione o dispositivo de controle de acesso na lista à esquerda.
3. Clique no botão **Adicionar** para adicionar uma nova ligação.
4. Selecione a origem do evento como **Card Linkage** .
5. Insira o número do cartão ou selecione o cartão na lista suspensa.
6. Selecione o leitor de cartão onde o cartão passa para acionar as ações vinculadas.
7. Na área Linkage Target, defina o destino da propriedade para habilitar esta ação.

Buzzer no controlador

O aviso sonoro do dispositivo de controle de acesso será acionado.

Capturar

A captura em tempo real será acionada.

Ponto de acesso

O status da porta aberta, fechada, permanecer aberta ou permanecer fechada será acionado.

8. Clique em **Salvar** .

Quando o cartão (configurado na Etapa 5) passa no leitor de cartão (configurado na Etapa 6), ele pode acionar as ações vinculadas (configuradas na etapa 7).

9. Opcional: depois de adicionar a ligação do dispositivo, você pode fazer um ou mais dos seguintes:

Excluir configurações de ligação Selecione as configurações de vinculação definidas na lista de dispositivos e clique em **Excluir** para excluí-lo.

Editar configurações de ligação Selecione as configurações de vinculação definidas na lista de dispositivos e você pode editar seus parâmetros de origem do evento, incluindo origem do evento e destino de vinculação.

7.8.4 Configurar ações do dispositivo para ID de pessoa

Você pode definir as ações de vinculação do dispositivo de controle de acesso para a ID de pessoa especificada. Quando o dispositivo de controle de acesso detecta o ID da pessoa especificada, ele pode acionar a campainha no leitor de cartão e outras ações.

Passos

Nota

Deve ser suportado pelo dispositivo.

1. Clique em **Controle de acesso** → **Configuração de ligação** .
2. Selecione o dispositivo de controle de acesso na lista à esquerda.
3. Clique em **Adicionar** para adicionar uma nova ligação.
4. Selecione **Person Linkage** como a fonte do evento.
5. Insira o número do funcionário ou selecione a pessoa na lista suspensa.
6. Selecione o leitor de cartão onde o cartão é passado.
7. Na área Linkage Target, defina o destino da propriedade para habilitar esta ação.

Buzzer no controlador

O aviso sonoro do dispositivo de controle de acesso será acionado.

Buzzer no Reader

O aviso sonoro do leitor de cartão será acionado.

Capturar

Uma imagem relacionada ao evento será capturada quando o evento selecionado acontecer.

Gravação

Uma imagem relacionada ao evento será capturada quando o evento selecionado acontecer.

Nota

O dispositivo deve suportar gravação.

Ponto de acesso

O status da porta aberta, fechada, permanecer aberta ou permanecer fechada será acionado.

8. Clique em **Salvar** .
9. Opcional: depois de adicionar a ligação do dispositivo, você pode fazer um ou mais dos seguintes procedimentos:

Excluir configurações de ligação Selecione as configurações de vinculação definidas na lista de dispositivos e clique em **Excluir** para excluí-lo.

Editar configurações de ligação Selecione as configurações de vinculação definidas na lista de dispositivos e você pode editar seus parâmetros de origem do evento, incluindo origem do evento e destino de vinculação.

7.9 Controle de porta

No módulo de Monitoramento, você pode ver o status em tempo real das portas gerenciadas pelo dispositivo de controle de acesso adicionado. Você também pode controlar as portas, como abrir / fechar a porta, ou manter a porta aberta / fechada através do cliente remotamente. O evento de acesso em tempo real é exibido neste módulo. Você pode ver os detalhes de acesso e detalhes pessoais.

Nota

Para o usuário com permissão de controle de porta, o usuário pode entrar no módulo de Monitoramento e controlar a porta. Ou os ícones usados para controle não serão exibidos. Para definir a permissão do usuário, consulte ***Gerenciamento de pessoas*** .

7.9.1 Status da porta de controle

Você pode controlar o status de uma única porta, incluindo abrir porta, fechar porta, manter a porta aberta e permanecer fechada.

Passos

1. Clique em **Monitoramento** para entrar na página de monitoramento de status.
2. Selecione um grupo de ponto de acesso no canto superior direito.

Nota

Para gerenciar o grupo de pontos de acesso, consulte *Gerenciamento de grupos* no manual do usuário do software cliente.

As portas no grupo de controle de acesso selecionado serão exibidas.

3. Clique no ícone de uma porta para selecionar uma porta ou pressione **Ctrl** e selecione várias portas.
4. Clique nos seguintes botões para controlar a porta.

Porta aberta

Quando a porta estiver trancada, destranque-a e ela será aberta uma vez. Após o período de abertura, a porta será fechada e trancada novamente automaticamente.

Porta fechada

Quando a porta estiver destrancada, tranque-a e ela será fechada. A pessoa que possui autorização de acesso pode acessar a porta com credenciais.

Continua aberto

A porta será destrancada (não importa se está fechada ou aberta). Todas as pessoas podem acessar a porta sem nenhuma credencial necessária.

Permanece Fechado

A porta será fechada e trancada. Nenhuma pessoa pode acessar a porta mesmo que tenha as credenciais autorizadas, exceto os superusuários.

Capturar

Capture uma foto manualmente.

Nota

Face Recognition Terminal User Manual

O botão **Capturar** está disponível quando o dispositivo oferece suporte à função de captura. A imagem é salva no PC que executa o cliente. Para definir o caminho de salvamento, consulte *Definir caminho de salvamento de arquivo* no manual do usuário do software cliente.

Resultado

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

7.9.2 Verificar registros de acesso em tempo real

Os registros de acesso serão exibidos em tempo real, incluindo registros de passagem do cartão, registros de reconhecimento de rosto, registros de comparação, etc. Você pode visualizar as informações da pessoa e visualizar a imagem capturada durante o acesso.

Passos

1. Clique em **Monitoramento** e selecione um grupo na lista suspensa no canto superior direito. Os registros de acesso acionados nas portas do grupo selecionado serão exibidos em tempo real. Você pode ver os detalhes dos registros, incluindo o número do cartão, nome da pessoa, organização, horário do evento, etc.
 2. Opcional: Verifique o tipo de evento e o status do evento para que esses eventos sejam exibidos na lista se forem detectados. Os eventos de tipo ou status desmarcado não serão exibidos na lista.
 3. Opcional: Marque **Mostrar evento mais recente** e o registro de acesso mais recente será selecionado e exibido no topo da lista de registros.
 4. Opcional: Clique no evento para visualizar os detalhes da pessoa acessada, incluindo fotos da pessoa (foto capturada e perfil), número da pessoa, nome da pessoa, organização, telefone, endereço de contato, etc.
-

Nota

Você pode clicar duas vezes na imagem capturada para aumentá-la e ver os detalhes.

5. Opcional: Clique com o botão direito no nome da coluna da tabela de eventos de acesso para mostrar ou ocultar a coluna de acordo com as necessidades reais.

7.10 Centro de Eventos

As informações do evento (por exemplo, dispositivo off-line) recebidas pelo cliente são exibidas. No Event Center, você pode verificar as informações detalhadas dos eventos em

tempo real e históricos, visualizar o vídeo vinculado ao evento, gerenciar os eventos e assim por diante.

Antes que o cliente possa receber as informações do evento do dispositivo, você precisa habilitar os eventos do recurso e armar o dispositivo primeiro. Para obter detalhes, consulte [Ativar recebimento de eventos de dispositivos](#).

7.10.1 Habilitar recebimento de eventos de dispositivos

Antes que o software cliente possa receber notificações de eventos do dispositivo, você precisa primeiro armar o dispositivo.

Passos

1. Clique → **Ferramenta** → **Controle de arme de dispositivo** para abrir a página Controle de arme de dispositivo.
Todos os dispositivos adicionados aparecem nesta página.
2. Na coluna Auto-arme, ligue a chave para habilitar o auto-arme.

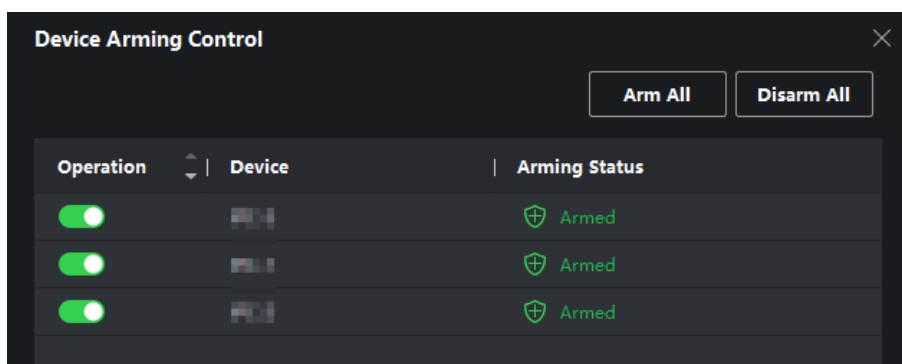


Figura 7-11 Dispositivo de Armar

Depois de ligado, o (s) dispositivo (s) serão armados. E as notificações sobre os eventos disparados pelo (s) dispositivo (s) armado (s) serão enviadas automaticamente para o software cliente em tempo real.

7.10.2 Visualizar eventos em tempo real

As informações de eventos em tempo real recebidas pelo cliente dos recursos conectados são exibidas. Você pode verificar as informações do evento em tempo real, incluindo a fonte do evento, hora do evento, prioridade, etc.

Antes que você comece

Ative o recebimento de eventos de dispositivos antes que o cliente possa receber eventos do dispositivo, consulte [Ativar o recebimento de eventos de dispositivos](#) para obter detalhes.

Face Recognition Terminal User Manual

Passos

1. Clique em **Centro de eventos** → **Evento em tempo real** para entrar na página do evento em tempo real e você pode ver os eventos em tempo real recebidos pelo cliente.

Hora do evento

Para dispositivo de codificação, a hora do evento é a hora do cliente quando ele recebe o evento. Para outros tipos de dispositivos, a hora do evento é a hora em que o evento é disparado.

Prioridade

A prioridade representa o grau de emergência do evento.

2. Filtre os eventos.

Filtrar por tipo de dispositivo e (ou) prioridade Selecione os tipos de dispositivos e (ou) prioridades para filtrar eventos.

Filtrar por palavras-chave Insira as palavras-chave para filtrar os eventos.

3. Opcional: Clique com o botão direito do mouse no cabeçalho da tabela da lista de eventos para customizar os itens relacionados ao evento a serem exibidos na lista de eventos.
4. Visualize os detalhes do evento.
 - 1) Selecione um evento na lista de eventos.
 - 2) Clique em **Expandir** no canto inferior direito da página.
 - 3) Visualize a descrição detalhada e os registros de entrega do evento.
5. Opcional: execute as seguintes operações, se necessário.

Lidar com evento único Clique em **Identificar** para inserir a sugestão de processamento e, em seguida, clique em **Confirmar** .

Nota

Depois que um evento for tratado, o botão **Manipular** se tornará **Adicionar observação** . Clique em **Adicionar** comentário para adicionar mais comentários para este evento manipulado.

Lidar com eventos em lote Selecione os eventos que precisam ser processados e clique em **Tratar em lote** . Insira a sugestão de processamento e clique em **Confirmar** .

Ativar / desativar o áudio do alarme Clique em **Habilitar Áudio** / **Desabilitar Áudio** para habilitar / desabilitar o áudio do evento.

- Selecione o último evento automaticamente** Marque **Seleção automática do último evento** para selecionar o evento mais recente automaticamente e os detalhes das informações do evento são exibidos.
- Limpar eventos** Clique em **Limpar** para limpar todos os eventos na lista de eventos.
- Enviar email** Selecione um evento e clique em **Enviar e-mail**, e os detalhes da informação deste evento serão enviados por e-mail.

Nota

Você deve configurar os parâmetros de e-mail primeiro, consulte para detalhes.

7.10.3 Pesquisar eventos históricos

No módulo Pesquisa de eventos da página do centro de eventos, você pode pesquisar os eventos históricos por tempo, tipo de dispositivo e outras condições de acordo com o tipo de dispositivo especificado e, em seguida, processar os eventos.

Antes que você comece

Ative o recebimento de eventos de dispositivos antes que o cliente possa receber informações de eventos do dispositivo, consulte [**Habilitar o recebimento de eventos de dispositivos**](#) para obter detalhes.

Passos

1. Clique em **Event Center** → **Event Search** para entrar na página de pesquisa de eventos.

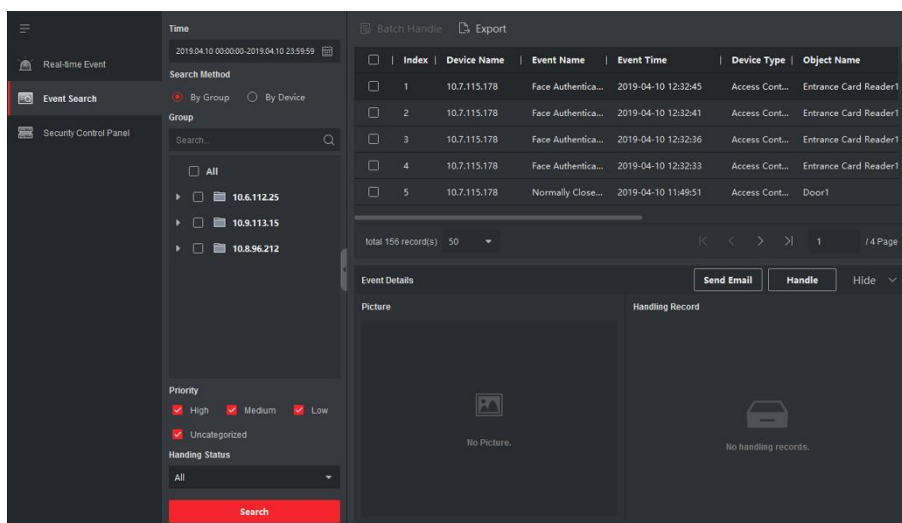


Figura 7-12 Evento de histórico de pesquisa

2. Defina as condições do filtro para exibir apenas os eventos necessários.

Tempo

A hora do cliente quando o evento começa.

Procurar por

Grupo : Pesquise os eventos ocorridos nos recursos do grupo selecionado.

Dispositivo : Pesquise os eventos ocorridos no dispositivo selecionado.

Tipo de dispositivo

O tipo de dispositivo em que ocorreu o evento.

Tudo

Todos os tipos de dispositivos e você pode definir as seguintes condições de filtro: grupo, prioridade e status.

Intercomunicador de vídeo

Para os eventos de intercomunicação de vídeo, você precisa selecionar o escopo de busca: Todas as Gravações e Apenas Desbloqueio.

- Todos os registros
- : Você pode filtrar os eventos de todos os eventos de intercomunicação de vídeo e precisa definir as seguintes condições de filtro: dispositivo, prioridade, status.
- Apenas desbloqueando
- : Você pode filtrar os eventos de todos os eventos de desbloqueio do intercomunicador de vídeo, e você precisa definir as seguintes condições de filtro: dispositivo, tipo de desbloqueio.

Controle de acesso

Para os eventos de controle de acesso, você pode definir as seguintes condições de filtro: dispositivo, prioridade, status, tipo de evento, tipo de leitor de cartão, nome da pessoa, número do cartão, organização.

Nota

Clique em **Mostrar mais** para definir o tipo de evento, tipo de leitor de cartão, nome da pessoa, número do cartão, organização.

Grupo

O grupo do dispositivo em que ocorreu o evento. Você deve definir o grupo como condição apenas quando selecionar o Tipo de dispositivo como **Todos** .

Dispositivo

Face Recognition Terminal User Manual

O dispositivo que ocorreu o evento.

Prioridade

A prioridade incluindo baixa, média, alta e não categorizada que indica o grau de urgência do evento.

Status

O status de tratamento do evento.

3. Clique em **Pesquisar** para pesquisar os eventos de acordo com as condições definidas.
4. Opcional: Clique com o botão direito no cabeçalho da tabela da lista de eventos para personalizar os itens relacionados ao evento a serem exibidos na lista de eventos.

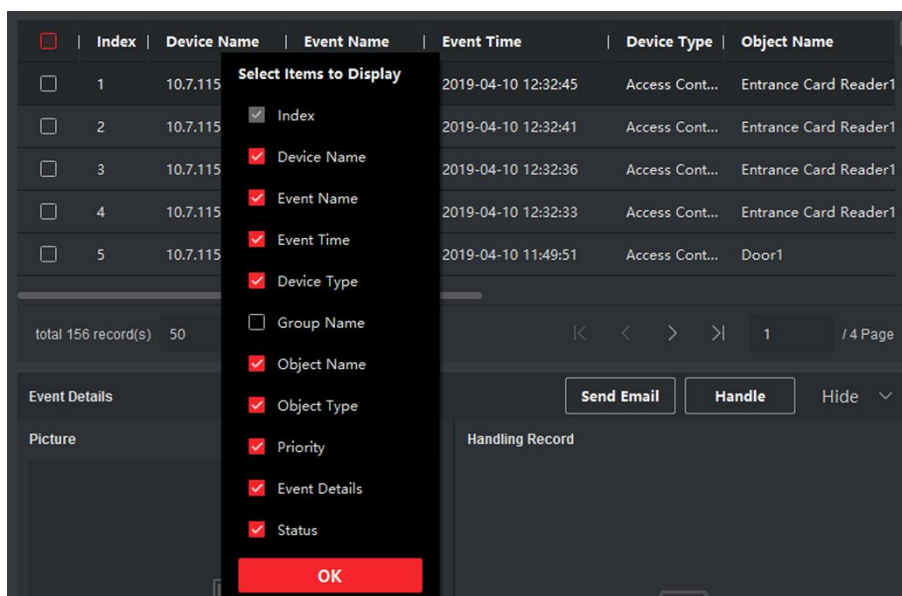


Figura 7-13 Personalizar itens relacionados a eventos a serem exibidos

5. Opcional: manipule o (s) evento (s).
 - Manipular evento único: Selecione um evento que precisa ser processado e clique em **Manipular** na página de detalhes de informações do evento e insira a sugestão de processamento.
 - Tratar eventos em lote: Selecione os eventos que precisam ser processados e, a seguir, clique em **Tratar em lote** e insira a sugestão de processamento.

Nota

Depois que um evento for tratado, o botão **Manipular** se tornará **Adicionar** observação, clique em **Adicionar** observação para adicionar mais observações para este evento manipulado.

6. Opcional: Selecione um evento e clique em **Enviar e-mail**, e os detalhes das informações deste evento serão enviados por e-mail.
-

Nota

Você deve configurar os parâmetros de e-mail primeiro, consulte *Definir parâmetros de e-mail* no manual do usuário do software cliente para obter detalhes.

7. Opcional: Clique em **Exportar** para exportar o log de eventos ou imagens de eventos para o PC local no formato CSV. Você pode definir o caminho de salvamento manualmente.
8. Passe o cursor sobre a imagem relacionada e clique no ícone de download no canto superior direito da imagem para baixá-la para o PC local. Você pode definir o caminho de salvamento manualmente.

7.11 Tempo e Presença

O módulo de Tempo e Presença oferece várias funcionalidades para rastrear e monitorar quando os funcionários começam e param de trabalhar, e controle total das horas de trabalho dos funcionários, como chegadas tardias, saídas antecipadas, tempo de pausas e absenteísmo.

Nota

Nesta seção, apresentamos as configurações para que você possa obter os relatórios de presença. Os registros de acesso registrados após essas configurações serão calculados nas estatísticas.

7.11.1 Configurar os parâmetros de atendimento

Você pode configurar os parâmetros de atendimento, incluindo a regra geral, parâmetros de horas extras, ponto de verificação de presença, feriado, tipo de licença, etc.

Definir fim de semana

Os dias de fim de semana podem variar em diferentes países e regiões. O cliente fornece a função de definição de fins de semana. Você pode selecionar um ou mais dias como fins de semana de acordo com os requisitos reais e definir regras de participação diferentes para fins de semana de dias úteis.

Passos

Nota

Face Recognition Terminal User Manual

Os parâmetros configurados aqui serão definidos como padrão para o período de tempo recém-adicionado. Não afetará o (s) existente (s).

1. Entre no módulo de Tempo e Presença.
2. Clique em **Configurações de participação** → **Regra geral** .
3. Selecione o (s) dia (s) como fim de semana, como sábado e domingo.
4. Clique em **Salvar** .

Configurar parâmetros de horas extras

Você pode configurar os parâmetros de horas extras para dia de trabalho e fim de semana, incluindo nível de horas extras, taxa de horas de trabalho, status de presença para horas extras, etc.

Passos

1. Clique em **Horário e presença** → **Configurações de atendimento** → **Horas extras** .
2. Defina as informações necessárias.

Nível de horas extras para dia de trabalho

Quando você trabalha por um determinado período após o horário de trabalho final no dia de trabalho, você alcançará diferentes níveis de horas extras: horas extras nível 1, horas extras nível 2 e horas extras nível 3. Você pode definir diferentes taxas de horas de trabalho para três níveis de horas extras, respectivamente.

Taxa de horas de trabalho

A Taxa de Horas de Trabalho é usada para calcular as horas de trabalho, multiplicando-as pelas horas extras. Quando você trabalha por um certo período após o horário de término do trabalho no dia útil, você alcançará um nível diferente de horas extras. Você pode definir diferentes taxas de horas de trabalho (1-10, pode ser um decimal) para três níveis de horas extras. Por exemplo, sua hora extra válida é uma hora (em horas extras nível 1), e a taxa de horas de trabalho de horas extras nível 1 é definida como 2, então as horas de trabalho no período serão calculadas como 2 horas.

Regra de horas extras para o fim de semana

Você pode habilitar a regra de horas extras para o fim de semana e definir o modo de cálculo.

3. Clique em **Salvar** .

Configurar Ponto de Verificação de Presença

Você pode definir o (s) leitor (es) de cartão do ponto de acesso como o ponto de verificação de atendimento, de forma que a autenticação nos leitores de cartão seja registrada para atendimento.

Face Recognition Terminal User Manual

Antes que você comece

Você deve adicionar um dispositivo de controle de acesso antes de configurar o ponto de verificação de atendimento. Para obter detalhes, consulte **Adicionar dispositivo** .

Passos

Nota

Por padrão, todos os leitores de cartão dos dispositivos de controle de acesso adicionados são definidos como pontos de verificação de presença.

1. Entre no módulo Horário e Presença.
2. Clique em **Configurações de Presença** → **Ponto de Verificação de Presença** para entrar na página Configurações de Ponto de Verificação de Presença.
3. Opcional: defina a opção **Definir todos os leitores de cartão como pontos de verificação como** desativada.
Apenas os leitores de cartão da lista serão definidos como pontos de verificação de presença.
4. Marque o (s) leitor (es) de cartão desejado (s) na lista de dispositivos como ponto (s) de verificação de presença.
5. Defina a função do ponto de verificação como **Início / Fim do Trabalho** , **Início do Trabalho** ou **Fim do Trabalho** .
6. Clique em **Definir como ponto de verificação** .
O ponto de verificação de presença configurado é exibido na lista da direita.

Configurar feriado

Você pode adicionar o feriado durante o qual o check-in ou check-out não será registrado.

Adicionar feriado regular

Você pode configurar um feriado que terá efeito anualmente em dias normais durante o período de vigência, como dia de Ano Novo, Dia da Independência, Dia de Natal, etc.

Passos

1. Entre no módulo Horário e Presença.
2. Clique em **Configurações de participação** → **Feriado** para entrar na página Configurações de feriado.
3. Marque **Feriado Regular** como o tipo de feriado.
4. Personalize um nome para o feriado.
5. Defina o primeiro dia do feriado.
6. Insira o número de dias de feriado.
7. Defina o status de presença se o funcionário trabalhar nos feriados.
8. Opcional: Marque **Repetir Anualmente** para tornar esta configuração de feriado efetiva todos os anos.


9. Clique em **OK** .

O feriado adicionado será exibido na lista de feriados e no calendário.

Se a data for selecionada como feriados diferentes, ela será registrada como o primeiro feriado adicionado.

10. Opcional: Após adicionar o feriado, execute uma das seguintes operações.

Editar feriado

Clique  para editar as informações do feriado.

Excluir feriado

Selecione um ou mais feriados adicionados e clique em **Excluir** para excluir o (s) feriado (s) da lista de feriados.

Adicionar feriado irregular

Pode configurar um feriado que terá efeito anualmente em dias irregulares durante o período de vigência, como feriado bancário.

Passos

1. Entre no módulo Horário e Presença.
2. Clique em **Configurações de participação** → **Feriado** para entrar na página Configurações de feriado.
3. Clique em **Adicionar** para abrir a página Adicionar feriado.
4. Marque **Feriado irregular** como tipo de feriado.
5. Personalize um nome para o feriado.
6. Defina a data de início do feriado.

Exemplo

Se você deseja definir a quarta quinta-feira de novembro de 2019 como o feriado do Dia de Ação de Graças, deve selecionar 2019, 4 de novembro e quinta-feira nas quatro listas suspensas.


7. Insira o número de dias de feriado.
8. Defina o status de presença se o funcionário trabalhar nos feriados.
9. Opcional: Marque **Repetir Anualmente** para tornar esta configuração de feriado efetiva a cada ano
10. Clique em **OK** .

O feriado adicionado será exibido na lista de feriados e no calendário.

Se a data for selecionada como feriados diferentes, ela será registrada como o primeiro feriado adicionado.

11. Opcional: Após adicionar o feriado, execute uma das seguintes operações.

Editar feriado

Clique  para editar as informações do feriado.

Excluir feriado


Selecione um ou mais feriados adicionados e clique em **Excluir** para excluir o (s) feriado (s) da lista de feriados.

Configurar tipo de licença

Você pode personalizar o tipo de licença (tipo de licença principal e tipo de licença secundária) de acordo com as necessidades reais. Você também pode editar ou excluir o tipo de licença.


Passos

1. Entre no módulo Horário e Presença.
2. Clique em **Configurações de participação** → **Tipo de licença** para entrar na página Configurações de tipo de licença.
3. Clique em **Adicionar** à esquerda para adicionar um tipo de licença principal.
4. Opcional: execute uma das seguintes operações para o tipo de licença principal.

Editar Mova o cursor sobre o tipo de licença principal e clique  para editar o tipo de licença principal.

Excluir Selecione um tipo de licença principal e clique em **Excluir** à esquerda para excluir o tipo de licença principal.

5. Clique em **Adicionar** à direita para adicionar um tipo de licença secundária.
6. Opcional: execute uma das seguintes operações para o tipo de licença secundária.

Editar Mova o cursor sobre o tipo de licença secundária e clique  para editar o tipo de licença secundária.

Excluir Selecione um ou vários tipos de licença principal e clique em **Excluir** à direita para excluir o (s) tipo (s) de licença secundária selecionado (s).

Sincronizar registro de autenticação com banco de dados de terceiros

Os dados de atendimento registrados no software cliente podem ser usados por outro sistema para cálculos ou algumas outras operações. Você pode habilitar a função de sincronização para aplicar o registro de autenticação do software cliente ao banco de dados de terceiros automaticamente.

Passos

1. Entre no módulo de Tempo e Presença.
2. Clique em **Configurações de participação** → **Banco de dados de terceiros** .
3. Defina a opção **Aplicar ao banco de dados** como ativado para ativar a função de sincronização.
4. Selecione o tipo de banco de dados como **SQLServer** ou **MySQL** .

Nota

Se você selecionar **MySQL** , deverá importar o arquivo de configuração (libmysql.dll) do PC local.

5. Defina os outros parâmetros necessários do banco de dados de terceiros, incluindo endereço IP do servidor, nome do banco de dados, nome de usuário e senha.
6. Defina os parâmetros da tabela do banco de dados de acordo com a configuração real.
 - 1) Insira o nome da tabela do banco de dados de terceiros.
 - 2) Defina os campos da tabela mapeada entre o software cliente e o banco de dados de terceiros.
7. Clique em **Salvar** para testar se o banco de dados pode ser conectado e salve as configurações para uma conexão bem-sucedida.
 - Os dados de atendimento serão gravados no banco de dados de terceiros.
 - Durante a sincronização, se o cliente se desconectar do banco de dados de terceiros, o cliente iniciará a reconexão a cada 30 minutos. Depois de ser reconectado, o cliente sincronizará os dados registrados durante o período de desconexão com o banco de dados de terceiros.

Configurar o intervalo

Você pode adicionar o tempo de intervalo e definir a hora de início, fim, duração, modo de cálculo e outros parâmetros para o intervalo. O tempo de pausa adicionado também pode ser editado ou excluído.

Passos

1. Clique em **Horário e presença** → **Horário** .
Os horários adicionados são exibidos na lista.
2. Selecione um horário adicionado ou clique em **Adicionar** para entrar na página de configuração do horário.
3. Clique em **Break Time** para entrar na página Break Time.
4. Clique em **Configurações de intervalo** .
5. Adicione o tempo de intervalo.
 - 1) Clique em **Adicionar** .
 - 2) Digite um nome para o intervalo.
 - 3) Defina os parâmetros relacionados para o tempo de pausa.

Hora de início / hora de término

Defina a hora em que o intervalo começa e termina.

Não antes de / não depois de

Defina a primeira hora de deslizar para iniciar o intervalo e a última hora de deslizar para terminar o intervalo.

Duração do intervalo

A duração do horário de início até o horário de término do intervalo.

Cálculo

Auto Dedução

A duração fixa do intervalo será excluída do horário de trabalho.

Deve verificar

A duração do intervalo será calculada e excluída do horário de trabalho de acordo com o horário real de check-in e check-out.

Nota

Se você selecionar **Deve verificar** como método de cálculo, será necessário definir o status de atendimento para atrasar ou voltar mais cedo do intervalo.

6. Clique em **Salvar** para salvar as configurações.
7. Opcional: Clique em **Adicionar** para continuar adicionando tempo de intervalo.

Configurar exibição de relatório

Você pode configurar o conteúdo de exibição exibido no relatório de presença, como o nome da empresa, logotipo, formato de data, formato de hora e marca.

Passos

1. Entre no módulo de Tempo e Presença.
2. Clique em **Estatísticas de Presença** → **Exibição de Relatório** .
3. Defina as configurações de exibição do relatório de presença.

Nome da empresa

Insira um nome de empresa para exibir o nome no relatório.

Marca de status de atendimento

Insira a marca e selecione a cor. Os campos relacionados ao status de atendimento no relatório serão exibidos com a marca e a cor.

Marco do fim de semana

Insira a marca e selecione a cor. Os campos de fim de semana no relatório serão exibidos com a marca e a cor.

4. Clique em **Salvar** .

7.11.2 Adicionar Cronograma Geral

Na página de horários, você pode adicionar horários gerais para funcionários, o que requer horário fixo de início e fim de trabalho. Além disso, você pode definir um horário válido de check-in / out, horários permitidos para chegar atrasado e sair mais cedo.

Passos

1. Clique em **Horário e presença** → **Horário** para entrar na página de configurações do horário.

Face Recognition Terminal User Manual

2. Clique em **Adicionar** para entrar na página de adicionar calendário.

The screenshot shows a configuration interface for a timetable. It is divided into several sections:

- Basic Settings:** Includes fields for Name (Timetable 1), Timetable Type (General), Calculated by (Each Check-In/Out), Valid Authentication Interval (1 min), and an Enable T&A Status toggle.
- Attendance Time:** Includes Start-Work Time (9:00), End-Work Time (18:00), Valid Check-in Time (8:30 to 9:30), Valid Check-out Time (17:30 to 18:30), Calculated as (540 min), Late Allowable (10 min), and Early Leave Allowable (10 min).
- Configuration Result:** A 24-hour timeline showing the work schedule. A blue bar represents the work time from 9:00 to 18:00. Yellow bars represent the valid check-in/out times from 8:30 to 9:30 and 17:30 to 18:30. A legend below the timeline identifies these colors: yellow for Valid Time of Check-In/Out, blue for Work Time, and light blue for Late/Early Leave Allowable.
- Absence Settings:** A section at the bottom with a red Save button.

Figura 7-14 Adicionar Cronograma

3. Crie um nome para o horário.

Nota

Você pode clicar no ícone de cor ao lado do nome para personalizar a cor do horário válido na barra de tempo na área Resultado da Configuração.

4. Selecione o tipo de horário como geral.

5. Selecione o método de cálculo.

Primeiro a entrar e o último a sair

A hora do primeiro check-in é registrada como hora de início do trabalho e a hora da última check-out é registrada como hora do fim do trabalho.

Cada check-in / out

Cada horário de check-in e check-out é válido e a soma de todos os períodos entre os horários adjacentes de check-in e check-out será registrada como a duração válida de trabalho.

Face Recognition Terminal User Manual

Você precisa definir o **intervalo de autenticação válido** para este método de cálculo. Por exemplo, se o intervalo entre a passagem do cartão do mesmo cartão for inferior ao valor definido, a passagem do cartão é inválida.

6. Opcional: Defina **Ativar o** interruptor de **status T&A** para ligado para calcular de acordo com o status de atendimento do dispositivo.
-

Nota

Esta função deve ser suportada pelo dispositivo.

7. Defina os parâmetros de tempo de atendimento relacionados da seguinte forma:

Horário de início / término do trabalho

Defina a hora de início e fim do trabalho.

Horário válido de check-in / out

Na barra de tempo, ajuste a barra amarela para definir o horário durante o qual o check-in ou check-out é válido.

Calculado como

Defina a duração calculada como a duração real do trabalho.

Licença tardia / antecipada permitida

Defina o horário para saída tardia ou antecipada.

8. Defina os parâmetros relacionados à ausência.

Check-in, tarde para

Você pode definir o tempo de atraso para o funcionário que fez check-in, mas está atrasado para o trabalho. Se o funcionário ultrapassar o período de tempo exigido, seus dados de presença serão marcados como ausente.

Check-out, licença antecipada para

Você pode definir a duração do tempo de licença antecipada para o funcionário que fizer check-out antes do horário normal de licença e seus dados de presença serão marcados como ausente.

Sem check-in

Se o funcionário não fizer o check-in, seus dados de presença podem ser marcados como ausente ou atrasado.

Sem check-out

Caso o funcionário não faça o check-out, seus dados de presença podem ser marcados como ausente ou licença antecipada.

9. Clique em **Salvar** para adicionar o horário.

10. Opcional: execute uma ou mais operações a seguir após adicionar o horário.

Editar Tabela de Horários

Selecione um horário da lista para editar as informações relacionadas.

Apagar Horário

Selecione um horário da lista e clique em **Excluir** para excluí-lo.

7.11.3 Adicionar Turno

Você pode adicionar turno para os funcionários, incluindo a definição do período de turno (dia, semana, mês) e o tempo de atendimento efetivo. De acordo com as necessidades reais, você pode adicionar vários horários em um turno para os funcionários, o que exige que eles façam check-in e check-out para cada horário.

Antes que você comece

Adicione um horário primeiro. Consulte [**Adicionar cronograma geral**](#) para obter detalhes.

Passos

1. Clique em **Horário e presença** → **Turno** para entrar na página de configurações de turno.
2. Clique em **Adicionar** para entrar na página Adicionar turno.
3. Digite o nome do turno.
4. Selecione o período de turno na lista suspensa.
5. Selecione o horário adicionado e clique na barra de tempo para aplicar o horário.

The screenshot displays the 'Shift' configuration page. At the top, there's a 'Name' field with 'Default Shift' and a 'Period' dropdown set to '1'. Below that, there's a 'Week(s)' dropdown. A section titled 'Timetable 1' contains a grid with columns for every 2 hours from 00:00 to 24:00 and rows for days of the week (Mon. to Sun.). Blue bars indicate the shift period from 09:00 to 18:00 for Monday through Saturday. At the bottom, there are 'Save' and 'Assign' buttons.

Figura 7-15 Adicionar turno

Nota

Você pode selecionar mais de um horário. O horário de início e término do trabalho e o horário de entrada e saída válidos em tabelas de horários diferentes não podem ser sobrepostos.

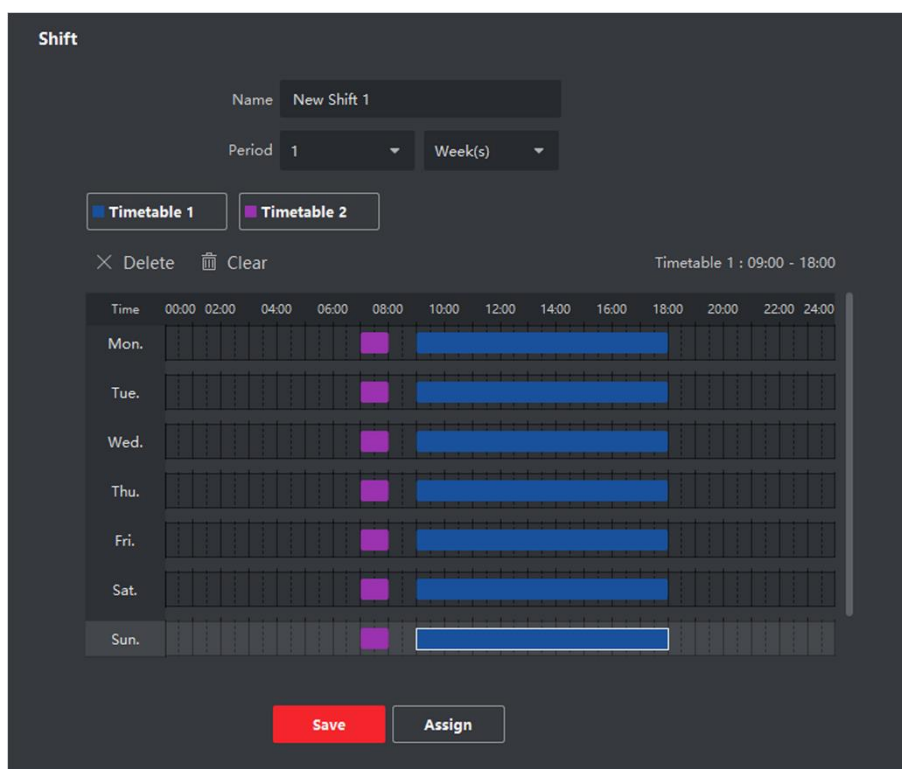


Figura 7-16 Adicionar vários horários

6. Clique em **Salvar** .

As listas de turnos adicionadas no painel esquerdo da página. No máximo 64 turnos podem ser adicionados.

7. Opcional: atribua o turno à organização ou pessoa para uma programação de turnos rápida.

1) Clique em **Atribuir** .

2) Selecione a guia **Organização** ou **Pessoa** e marque a caixa de organização (ões) ou pessoa (s) desejada (s).

As organizações ou pessoas selecionadas serão listadas na página certa.

3) Defina a data de expiração para a programação de turno.

4) Defina outros parâmetros para a programação.

Check-in não obrigatório

As pessoas nesta programação não precisam fazer o check-in quando vierem trabalhar.

Check-out não obrigatório

As pessoas nesta programação não precisam fazer o check-out ao encerrar o trabalho.

Programado para feriados

Nos feriados, esse horário ainda é válido e as pessoas precisam ir trabalhar de acordo com o horário.

Eficaz para horas extras

As horas extras das pessoas serão registradas para esta programação.

5) Clique em **Salvar** para salvar a programação de turno rápido.

7.11.4 Gerenciar Cronograma de Turnos

O trabalho em turnos é uma prática de emprego projetada para fazer uso de todas as 24 horas do relógio todos os dias da semana. A prática normalmente vê o dia dividido em turnos, períodos fixos de tempo durante os quais turnos diferentes executam suas funções.

Você pode definir a programação do departamento, a programação da pessoa e a programação temporária.

Definir cronograma de departamento

Você pode definir a programação de turnos para um departamento e todas as pessoas no departamento serão atribuídas com a programação de turnos.

Antes que você comece

No módulo de Tempo e Presença, a lista de departamentos é a mesma da organização. Você deve adicionar organização e pessoas no módulo Pessoa primeiro. Consulte [**Gerenciamento de pessoas**](#) para obter detalhes.

Passos

1. Clique em **Horário e Presença** → **Programação de Turno** para entrar na página Gerenciamento de Programação de Turno.
2. Clique em **Programação do Departamento** para entrar na página Programação do Departamento.
3. Selecione o departamento na lista de organizações à esquerda.

Nota

Face Recognition Terminal User Manual

Se **Incluir Suborganização** estiver marcada, ao selecionar a organização, suas suborganizações serão selecionadas ao mesmo tempo.

4. Selecione o turno na lista suspensa.
 5. Opcional: ative **Múltiplos horários de turno** e selecione o (s) período (s) de tempo efetivo dos horários adicionados para as pessoas.
-

Nota

Isso está disponível apenas para turnos com apenas um horário.

Múltiplas programações de turnos

Ele contém mais de um horário. A pessoa poderá fazer o check in / out em qualquer um dos horários e o atendimento será efetivo.

Se as programações de vários turnos contiverem três horários: 00:00 às 07:00, 08:00 às 15:00 e 16:00 às 23:00. O atendimento da pessoa que adotar esta programação de múltiplos turnos será efetivo em qualquer um dos três horários. Se a pessoa fizer o check-in às 07h50, será aplicado o horário mais próximo das 08h00 às 15h00 ao atendimento da pessoa.

6. Defina a data de início e a data de término.
7. Defina outros parâmetros para a programação.

Check-in não obrigatório

As pessoas nesta programação não precisam fazer o check-in quando vierem trabalhar.

Check-out não obrigatório

As pessoas nesta programação não precisam fazer o check-out ao encerrar o trabalho.

Programado para feriados

Nos feriados, esse horário ainda é válido e as pessoas precisam ir trabalhar de acordo com o horário.

Eficaz para horas extras

As horas extras das pessoas serão registradas para esta programação.

8. Clique em **Salvar** .

Definir agenda de pessoa

Você pode atribuir a programação de turnos a uma ou mais pessoas. Você também pode visualizar e editar os detalhes da agenda da pessoa.

Antes que você comece

Face Recognition Terminal User Manual

Adicionar departamento e módulo de pessoa em pessoa. Consulte [Gerenciamento de pessoas](#) para obter detalhes.

Passos

Nota

A agenda da pessoa tem maior prioridade do que a agenda do departamento.

1. Clique em **Horário e Presença** → **Programação de Turno** para entrar na página Programação de Turno.
 2. Clique em **Programação de pessoa** para entrar na página Programação de pessoa.
 3. Selecione a organização e selecione a (s) pessoa (s).
 4. Selecione o turno na lista suspensa.
 5. Opcional: ative **Múltiplos horários de turno** e selecione o (s) período (s) de tempo efetivo dos horários adicionados para as pessoas.
-

Nota

Isso está disponível apenas para turnos com apenas um horário.

Múltiplas programações de turnos

Ele contém mais de um horário. A pessoa poderá fazer o check in / out em qualquer um dos horários e o atendimento será efetivo.

Se as programações de vários turnos contiverem três horários: 00:00 às 07:00, 08:00 às 15:00 e 16:00 às 23:00. O atendimento da pessoa que adotar esta programação de múltiplos turnos será efetivo em qualquer um dos três horários. Se a pessoa fizer o check-in às 07h50, será aplicado o horário mais próximo das 08h00 às 15h00 ao atendimento da pessoa.

6. Defina a data de início e a data de término.
7. Defina outros parâmetros para a programação.

Check-in não obrigatório

As pessoas nesta programação não precisam fazer o check-in quando vierem trabalhar.

Check-out não obrigatório

As pessoas nesta programação não precisam fazer o check-out ao encerrar o trabalho.

Programado para feriados

Nos feriados, esse horário ainda é válido e as pessoas precisam ir trabalhar de acordo com o horário.

Eficaz para horas extras

As horas extras das pessoas serão registradas para esta programação.

8. Clique em **Salvar** .

Definir cronograma temporário

Você pode adicionar uma programação temporária para a pessoa e a pessoa será atribuída com a programação de turnos temporariamente. Você também pode visualizar e editar os detalhes da programação temporária.

Antes que você comece

Adicionar departamento e módulo de pessoa em pessoa. Consulte [Gerenciamento de pessoas](#) para obter detalhes.

Passos

Nota

A programação temporária tem maior prioridade do que a programação do departamento e a programação pessoal.

1. Clique em **Horário e Presença** → **Programação de Turno** para entrar na página Gerenciamento de Programação de Turno.
2. Clique em **Programação Temporária** para entrar na página Programação Temporária.
3. Selecione a organização e selecione a (s) pessoa (s).
4. Clique em uma data ou clique e arraste para selecionar várias datas para a programação temporária.
5. Selecione **Dia útil** ou **Dia não útil** na lista suspensa.

Se **Non-Workday** for selecionado, você precisará definir os seguintes parâmetros.

Calculado como

Selecione o nível normal ou de hora extra para marcar o status de atendimento para programação temporária.

Calendário

Selecione um horário na lista suspensa.

Programação de vários turnos

Ele contém mais de um horário. A pessoa poderá fazer o check in / out em qualquer um dos horários e o atendimento será efetivo.

Se as programações de vários turnos contiverem três horários: 00:00 às 07:00, 08:00 às 15:00 e 16:00 às 23:00. O atendimento da pessoa que adotar esta programação de múltiplos turnos será efetivo em qualquer um dos três horários. Se a pessoa fizer o check-in às 07h50, será aplicado o horário mais próximo das 08h00 às 15h00 ao atendimento da pessoa.

Regra



Defina outra regra para a programação, como **Check-in não obrigatório** e **Check-out não obrigatório** .

6. Clique em **Salvar** .

Verifique a programação de turnos

Você pode verificar a programação de turnos no calendário ou modo de lista. Seu CA também edita ou exclui a programação de turnos.

Passos

1. Clique em **Horário e Presença** → **Programação de Turno** para entrar na página Gerenciamento de Programação de Turno.
2. Selecione a organização e a (s) pessoa (s) correspondente (s).
3. Clique  ou  para ver a programação de turnos no calendário ou modo de lista.

Calendário

No modo de calendário, você pode visualizar a programação de turnos para cada dia em um mês. Você pode clicar na programação temporária de um dia para editá-la ou excluí-la.

Lista

No modo de lista, você pode ver os detalhes da programação de turnos sobre uma pessoa ou organização, como nome do turno, tipo, período efetivo e assim por diante. Verifique a (s) programação (ões) de turno e clique em **Excluir** para excluir a (s) programação (ões) de turno selecionada (s).

7.11.5 Registro de check-in / out correto manualmente

Se o status de atendimento não estiver correto, você pode corrigir manualmente o registro de entrada ou saída. Você também pode editar, excluir, pesquisar ou exportar o registro de check-in ou check-out.

Antes que você comece

- Você deve adicionar organizações e pessoas no módulo Pessoa. Para obter detalhes, consulte **Gerenciamento de pessoas** .
- O status de presença da pessoa está incorreto.


Passos

1. Clique em **Tempo e presença** → **Tratamento de presença** para entrar na página de tratamento de presença.
2. Clique em **Check-in / out correto** para adicionar a página de correção de check-in / out.
3. Selecione a pessoa da lista à esquerda para correção.
4. Selecione a data de correção.

Face Recognition Terminal User Manual



- Defina os parâmetros de correção de check-in / out.
Selecione **Check-in** e defina o horário real de início do trabalho. Selecione **Check-out** e defina o horário real de término do trabalho.
-

Nota

Você pode clicar  para adicionar vários itens de check in / out. No máximo 8 itens de check-in / out podem ser suportados.

- Opcional: Insira as informações do comentário conforme desejado.
- Clique em **Salvar** .
- Opcional: Após adicionar a correção de check-in / out, execute uma das seguintes operações.

Visão

Clique  ou  para visualizar as informações de tratamento de presença adicionadas no modo de calendário ou lista.

Nota

No modo de calendário, você precisa clicar em **Calcular** para obter o status de frequência da pessoa em um mês.

Editar

- No modo de calendário, clique no rótulo relacionado na data para editar os detalhes.
- No modo de lista, clique duas vezes no campo relacionado na coluna Data, Tipo de tratamento, Hora ou Observação para editar as informações.

Excluir

Exclua os itens selecionados.

Exportar

Exporte os detalhes de tratamento de presença para o PC local.

Nota

Os detalhes exportados são salvos no formato CSV.

7.11.6 Adicionar Licença e Viagem de Negócios

Você pode adicionar férias e viagem de negócios quando o funcionário deseja pedir licença ou fazer uma viagem de negócios.

Antes que você comece

Face Recognition Terminal User Manual

Você deve adicionar organizações e pessoas no módulo Pessoa. Para obter detalhes, consulte [Gerenciamento de pessoas](#).

Passos



1. Clique em **Tempo e presença** → **Tratamento de presença** para entrar na página de tratamento de presença.
2. Clique em **Inscriver-se para Férias / Viagem de Negócios** para inserir a adição da página de férias / viagem de negócios.
3. Selecione a pessoa na lista da esquerda.
4. Defina a (s) data (s) para sua licença ou viagem de negócios.
5. Selecione o tipo de licença principal e o tipo de licença secundária na lista suspensa.

Nota

Você pode definir o tipo de licença nas configurações de atendimento. Para obter detalhes, consulte [Configurar tipo de licença](#).

6. Defina a hora para a licença.
7. Opcional: Insira as informações do comentário conforme desejado.
8. Clique em **Salvar**.
9. Opcional: Após adicionar a licença e a viagem de negócios, execute uma das seguintes operações.

Visão

Clique  ou  para visualizar as informações de tratamento de presença adicionadas no modo de calendário ou lista.

Nota

No modo de calendário, você precisa clicar em **Calcular** para obter o status de frequência da pessoa em um mês.

Editar

- No modo de calendário, clique no rótulo relacionado na data para editar os detalhes.
- No modo de lista, clique duas vezes no campo na coluna Data, Tipo de tratamento, Hora ou Observação para editar as informações relacionadas.

Excluir

Exclua os itens selecionados.

Exportar

Exporte os detalhes de tratamento de presença para o PC local.

Nota

Os detalhes exportados são salvos no formato CSV.

7.11.7 Calcular Dados de Presença

Você precisa calcular os dados de presença antes de pesquisar e visualizar a visão geral dos dados de presença, dados de presença detalhados dos funcionários, dados de presença anormais dos funcionários, dados de horas extras dos funcionários de trabalho e registro de passagem do cartão.

Calcule Automaticamente os Dados de Presença

Você pode definir uma programação para que o cliente possa calcular automaticamente os dados de atendimento do dia anterior na hora que você configurou todos os dias.

Passos

Nota

1. Entre no módulo Horário e Presença.
2. Clique em **Configurações de participação** → **Regra geral** .
3. Na área Auto-Calculate Attendance, defina a hora que deseja que o cliente calcule os dados.
4. Clique em **Salvar** .
O cliente irá calcular os dados de atendimento do dia anterior a partir do horário que você configurou.

Calcular Dados de Presença Manualmente

Você pode calcular os dados de atendimento manualmente, definindo o intervalo de dados.


Passos

1. Entre no módulo Horário e Presença.
2. Clique em **Estatísticas de participação** → **Cálculo** .
3. Defina o horário de início e término para definir o intervalo de dados de atendimento.
4. Defina outras condições, incluindo departamento, nome, ID da pessoa e status de presença.
5. Clique em **Calcular** .

Nota

Ele só pode calcular os dados de atendimento em três meses.

6. Execute uma das seguintes operações.

Check-in / out correto	Clique em Corrigir check-in / out para adicionar a correção de check-in / out.
Selecione os itens para exibir	Clique  , ou clique com o botão direito nos títulos de diferentes itens para selecionar os itens a serem exibidos no relatório.
Gerar Relatório	Clique em Relatório para gerar o relatório de presença.
Relatório de exportação	Clique em Exportar para exportar os dados de atendimento para o PC local.

Nota

Os detalhes exportados são salvos no formato .CSV.

7.11.8 Estatísticas de Presença

Você pode verificar o registro de presença original, gerar e exportar o relatório de presença com base nos dados de presença calculados.

Obtenha uma visão geral dos dados de comparecimento dos funcionários

Você pode pesquisar e visualizar os registros de presença do funcionário no cliente, incluindo tempo de atendimento, status de atendimento, ponto de verificação, etc.

Antes que você comece

- Você deve adicionar organizações e pessoas no módulo Pessoa e as pessoas têm cartões passados. Para obter detalhes, consulte [***Gerenciamento de pessoas***](#) .
- Calcule os dados de atendimento.

Nota

- O cliente calculará automaticamente os dados de atendimento do dia anterior à 1h00 do dia seguinte.
 - Mantenha o cliente funcionando à 1h da manhã ou ele não poderá calcular os dados de presença do dia anterior automaticamente. Se não for calculado automaticamente, você pode calcular os dados de atendimento manualmente. Para obter detalhes, consulte [***Calcular dados de frequência manualmente***](#) .
-

Passos

Face Recognition Terminal User Manual

1. Entre no módulo Horário e Presença.
2. Clique em **Estatísticas de Presença** → **Registro de Presença** .
3. Defina a hora de início e a hora de término do atendimento que deseja pesquisar.
4. Defina outras condições de pesquisa, incluindo departamento, nome e ID de pessoa.
5. Selecione a fonte de dados como **Registros originais no dispositivo** ou **Registros de tratamento manual** .
6. Opcional: Clique em **Obter eventos do dispositivo** para obter os dados de atendimento do dispositivo.
7. Opcional: Clique em **Redefinir** para redefinir todas as condições de pesquisa e editar as condições de pesquisa novamente.
8. Clique em **Pesquisar** .
O resultado é exibido na página. Você pode visualizar o status de presença obrigatório do empregado e o ponto de verificação.
9. Opcional: Após pesquisar o resultado, execute uma das seguintes operações.

Gerar Relatório Clique em **Relatório** para gerar o relatório de presença.

Relatório de exportação Clique em **Exportar** para exportar os resultados para o PC local.

Exportação Personalizada Para obter detalhes, consulte.

Gerar relatório instantâneo

Suporta gerar uma série de relatórios de presenças manualmente para visualizar os resultados de presenças dos funcionários.

Antes que você comece

Calcule os dados de atendimento.

Nota

Você pode calcular os dados de atendimento manualmente ou definir a programação para que o cliente possa calcular os dados automaticamente todos os dias. Para obter detalhes, consulte **Calcular dados de frequência** .

Passos

1. Entre no módulo Horário e Presença.
2. Clique em **Estatísticas de participação** → **Relatório** .
3. Selecione um tipo de relatório.
4. Selecione o departamento ou pessoa para visualizar o relatório de presença.

5. Defina a hora de início e a hora de término durante as quais os dados de presença serão exibidos no relatório.
6. Clique em **Relatório** para gerar o relatório de estatísticas e abri-lo.

Relatório de Presença Personalizado

O cliente oferece suporte a vários tipos de relatório e você pode pre definir o conteúdo do relatório e enviar o relatório automaticamente para o endereço de e-mail configurado.

Passos

Nota

Defina os parâmetros de e-mail antes de ativar as funções de envio automático de e-mail. Para obter detalhes, consulte *Definir parâmetros de e-mail* no manual do usuário do software cliente.

1. Entre no módulo Horário e Presença.
2. Clique em **Estatísticas de participação** → **Relatório personalizado** .
3. Clique em **Adicionar** para predefinir um relatório.
4. Defina o conteúdo do relatório.

Nome do Relatório

Insira um nome para o relatório.

Tipo de relatório

Selecione um tipo de relatório e este relatório será gerado.

Tempo do Relatório

O tempo a ser selecionado pode variar para diferentes tipos de relatório.

Pessoa

Selecione a (s) pessoa (s) adicionada (s) cujos registros de presença serão gerados para o relatório.

5. Opcional: Defina a programação para enviar o relatório para o (s) endereço (s) de e-mail automaticamente.
 - 1) Marque **Envio automático de e-mail** para habilitar esta função.
 - 2) Defina o período de vigência durante o qual o cliente enviará o relatório na (s) data (s) de envio selecionada (s).
 - 3) Selecione a (s) data (s) em que o cliente enviará o relatório.
 - 4) Defina a hora em que o cliente enviará o relatório.

Exemplo

Face Recognition Terminal User Manual

Se você definir o período de vigência como **10/03/2018 a 10/04/2018** , selecionar **sexta-feira** como a data de envio e definir a hora de envio como **20:00:00** , o cliente enviará o relatório às 20h nas sextas-feiras durante 10/03/2018 a 10/04/2018.

Nota

Certifique-se de que os registros de presença sejam calculados antes da hora de envio. Você pode calcular os dados de atendimento manualmente ou definir a programação para que o cliente possa calcular os dados automaticamente todos os dias. Para obter detalhes, consulte **Calcular dados de frequência** .

5) Digite o (s) endereço (s) de e-mail do destinatário.

Nota

Você pode clicar em + para adicionar um novo endereço de e-mail. São permitidos até 5 endereços de e-mail.

6) Opcional: Clique em **Visualizar** para ver os detalhes do e-mail.

6. Clique em **OK** .

7. Opcional: depois de adicionar o relatório personalizado, você pode fazer um ou mais dos seguintes procedimentos:


Editar Relatório	Selecione um relatório adicionado e clique em Editar para editar suas configurações.
Apagar Relatório	Selecione um relatório adicionado e clique em Excluir para excluí-lo.
Gerar Relatório	Selecione um relatório adicionado e clique em Relatório para gerar o relatório instantaneamente e você pode visualizar os detalhes do relatório.

7.12 Configuração Remota (Web)

Configure os parâmetros do dispositivo remotamente.

7.12.1 Ver informações do dispositivo

Visualize e defina o nome do dispositivo, visualize o tipo de dispositivo, número de série, versão, número do relé e número de bloqueio.

Selecione um dispositivo na guia Dispositivo para gerenciamento e clique em  → **Sistema** → **Informações do dispositivo** para entrar na página Informações do dispositivo.

Face Recognition Terminal User Manual

Device Name

Device Type:

Serial No.

Firmware Version:

Web Version

Hardware Version:

Local Zone Number: 4

Local Relay Number: 4

Lock Number 4

Local RS-485 Number: 8

Figura 7-17 Exibir informações do dispositivo

Você pode definir o nome do dispositivo, visualizar o tipo do dispositivo, número de série, versão, número do relé e número do bloqueio. Clique em **Salvar** para salvar as configurações.

7.12.2 Alterar senha do dispositivo

Você pode alterar a senha do dispositivo.

Antes que você comece

Certifique-se de que o dispositivo esteja ativado. Para obter detalhes, consulte *Ativação*.

Passos

1. Na página Device for Management, clique em **Sistema** → **Sistema** → **Usuário** para acessar a guia Usuário.
2. Selecione um usuário e clique em **Editar** para entrar na página Editar.
3. Insira a senha antiga, crie uma nova senha e confirme a nova senha.

Cuidado

A força da senha do dispositivo pode ser verificada automaticamente. É altamente recomendável que você altere a senha de sua escolha (usando no mínimo 8 caracteres, incluindo pelo menos três tipos das seguintes categorias: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança de sua produtos. E recomendamos que você altere sua senha regularmente, principalmente no sistema de alta segurança, alterando a senha mensal 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.

4. Clique em **OK** .

Resultado

A senha do dispositivo é alterada. Você deve inserir a nova senha na página Device for Management para reconectar o dispositivo.

7.12.3 Gerenciamento de Tempo

Gerenciar o fuso horário, a sincronização de horário e os parâmetros de horário de verão do dispositivo.

Fuso Horário e Sincronização de Horário

Na página Dispositivo para Gerenciamento, selecione um dispositivo e clique em → **Sistema** → **Hora** para entrar na guia Hora.

Você pode selecionar um fuso horário, definir parâmetros NTP ou sincronizar manualmente o horário.

Fuso horário

Selecione um fuso horário na lista suspensa.

NTP

O dispositivo irá sincronizar a hora com NTP automaticamente. Depois de habilitar o **NTP** , você deve definir o endereço do servidor NTP, a porta NTP e o intervalo de sincronização.

Sincronização de Horário Manual

Depois de ativar a **Sincronização manual de hora** , você pode definir manualmente a hora do dispositivo.

Se você marcar **Sincronizar com a hora do computador** , **Definir hora** exibirá a hora atual do computador. Neste momento, desmarque **Sincronizar com hora do computador** e clique em , você pode editar a hora do dispositivo manualmente.

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

DST

Na página Device for Management, clique em **Remote Configuration** → **System** → **Time** → **DST** para entrar na guia DST.

Habilite o DST e você pode editar o tempo de polarização do DST, o horário de início e término do DST.

Clique em **Salvar** .

7.12.4 Manutenção do Sistema

Você pode reiniciar o dispositivo remotamente, restaurar as configurações padrão do dispositivo, importar o arquivo de configuração, atualizar o dispositivo, etc.

Reiniciar

Na página Device for Management, clique em  → **Sistema** → **Manutenção do sistema** para entrar na guia Manutenção do sistema.

Clique em **Reinicializar** e o dispositivo começa a reiniciar.

Restaurar configurações

Na página Dispositivo para gerenciamento, clique em **Configuração remota** → **Sistema** → **Manutenção do sistema** para entrar na guia Manutenção do sistema.

Restaurar padrão

Os parâmetros serão restaurados aos padrões, excluindo o endereço IP.

Restaurar parte das configurações

Restaurar todas as configurações, exceto as configurações de comunicação e as configurações do usuário remoto para os padrões.

Restaurar tudo

Todos os parâmetros do dispositivo serão restaurados aos padrões. O dispositivo deve ser ativado após a restauração.

Importar e exportar

Na página Dispositivo para gerenciamento, clique em **Configuração remota** → **Sistema** → **Manutenção do sistema** para entrar na guia Manutenção do sistema.

Importe ou exporte o arquivo de configuração.

Importar arquivo de configuração

Face Recognition Terminal User Manual

Importe o arquivo de configuração do PC local para o dispositivo.

Nota

O arquivo de configuração contém os parâmetros do dispositivo.

Exportar arquivo de configuração

Exporte o arquivo de configuração do dispositivo para o PC local.

Nota

O arquivo de configuração contém os parâmetros do dispositivo.

Melhoria

Na página Dispositivo para gerenciamento, clique em **Configuração remota** → **Sistema** → **Manutenção do sistema** para entrar na guia Manutenção do sistema.

Selecione um tipo de dispositivo na lista suspensa, clique em **Navegar** e selecione um arquivo de atualização no computador local e clique em **Atualizar**.


Nota

- Se você selecionar Leitor de cartão como o tipo de dispositivo, também deverá selecionar um número de leitor de cartão na lista suspensa.
 - A atualização vai durar cerca de 2 minutos. Não desligue durante a atualização. Após a atualização, o dispositivo será reiniciado automaticamente.
-

7.12.5 Configurar Parâmetros RS-485

Você pode definir os parâmetros RS-485, incluindo a taxa de transmissão, bit de dados, bit de parada, tipo de paridade, modo de comunicação, modo de trabalho e modo de conexão.

Passos


1. Clique em **Manutenção e gerenciamento** → **Dispositivo** para entrar na lista de dispositivos.
2. Clique  para entrar na página de configuração remota.
3. Clique em **Sistema** → **Configurações RS-485** para entrar na guia Configurando os Parâmetros RS-485.
4. Selecione o número de série da porta na lista suspensa para definir os parâmetros RS-485.
5. Defina a taxa de transmissão, o bit de dados, o bit de parada, a paridade, o controle de fluxo, o modo de comunicação, o modo de trabalho e o modo de conexão na lista suspensa.
6. Clique em **Salvar** e os parâmetros configurados serão aplicados ao dispositivo automaticamente.

Nota

Depois de mudar o modo de trabalho, o dispositivo será reiniciado. Um prompt será exibido após alterar o modo de trabalho.

7.12.6 Configurações do modo de segurança

Defina o modo de segurança para fazer login no software cliente.

Na página Device for Management, clique em  → **Sistema** → **Segurança** para entrar na guia Modo de segurança.

Selecione um modo de segurança na lista suspensa e clique em **Salvar**.

Você também pode habilitar o **SSH** para obter uma rede mais segura.

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 fazer o login.

7.12.7 Configurações de parâmetros de rede

Defina os parâmetros de rede do dispositivo, incluindo o tipo de NIC, DHCP e HTTP.

Na página Device for Management, clique em  → **Rede** → **Parâmetros de rede** para acessar a guia Configurações de parâmetros de rede.

Tipo de NIC

Selecione um tipo de NIC na lista suspensa. Você pode selecionar Auto-adaptável, 10M ou 100M.

DHCP

Se você desativar a função, deverá definir manualmente o endereço IPv4 do dispositivo, a máscara de sub-rede IPv4, o gateway padrão IPv4, a MTU e a porta.


Se você ativar a função, o sistema atribuirá automaticamente o endereço IPv4, a máscara de sub-rede IPv4 e o gateway padrão IPv4 para o dispositivo.

HTTP

Defina a porta HTTP, o endereço do servidor DNS1 e o endereço do servidor DNS2.

7.12.8 Configurações de estratégia de relatório

Você pode definir o grupo central para enviar o registro por meio do protocolo EHome.

Na página Device for Management, clique em  → **Rede** → **Estratégia de relatório** para entrar na guia Configurações de estratégia de relatório.

Você pode definir o grupo central e o sistema irá transferir os registros via protocolo EHome. Clique em **Salvar** para salvar as configurações.

Grupo Central

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.

7.12.9 Configurações de Parâmetros do Centro de Rede

Você pode definir o centro de vigilância de notificação, endereço IP do centro, o número da porta, o protocolo (EHome), o nome de usuário da conta EHome, etc. para transmitir dados via protocolo EHome.

Na página Device for Management, clique em  → **Rede** → **Parâmetros do Centro de Rede** para acessar a guia Configurações dos Parâmetros do Centro de Rede.

Selecione um centro na lista suspensa.

Depois de habilitar a função, você pode definir o tipo de endereço do centro, endereço IP / nome de domínio, número da porta, nome de usuário EHome, etc.

Clique em **Salvar** .

7.12.10 Configurar Parâmetros SIP

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

Nota

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

Clique em **Manutenção e gerenciamento** → **Dispositivo** para entrar na lista de dispositivos.

Clique  para entrar na página de configuração remota.


Clique em **Rede** → **Configuração de rede vinculada** e defina o endereço IP da estação mestre e o endereço IP do servidor SIP.

Clique em **Salvar** .

7.12.11 Definir os Parâmetros do Relé


Clique em **Manutenção e gerenciamento** → **Dispositivo** para entrar na lista de dispositivos.

Clique  para entrar na página de configuração remota.

Clique em **Alarme** → **Relé** . Selecione um relé e clique em  e defina o nome do relé e o tempo de atraso de saída. Clique em **OK** para salvar as configurações.

7.12.12 Definir parâmetros de controle de acesso

Passos

1. Na página Device for Management, clique em  → **Outros** → **Parâmetros de controle de acesso** para acessar a guia **Parâmetros de controle de acesso** .
2. Marque a caixa de seleção para habilitar a função.

Prompt de áudio (prompt de voz)

Se você ativar esta função, o prompt de voz será ativado no dispositivo. Você pode ouvir o prompt de voz ao operar no dispositivo.

Carregar imagens após a captura

Se você habilitar esta função, as imagens capturadas serão enviadas para o software cliente.

Salvar fotos capturadas

Se você ativar esta função, as imagens capturadas serão salvas.

Medição de temperatura apenas

Ao habilitar a função, o aparelho não irá autenticar as permissões, apenas medirá a temperatura. Ao desabilitar a função, o aparelho irá autenticar as permissões e ao mesmo tempo medir a temperatura.

Capturar imagem de luz branca

Ao habilitar a função, as imagens capturadas pela câmera de luz branca serão enviadas para a plataforma. Se desabilitar a função, o aparelho só fará upload de fotos capturadas pela câmera termográfica para a plataforma.

Porta não aberta ao detectar temperatura anormal

Ao habilitar a função, a porta não abrirá quando a temperatura detectada for superior ou inferior ao limite de temperatura configurado. Por padrão, a temperatura está habilitada.

Deve usar máscara facial

Após habilitar esta função, a pessoa autenticada deve usar uma máscara facial, caso contrário, a autenticação falhará.

Alarme de temperatura excessiva

Edite o limite de acordo com a situação real. Se a temperatura detectada for superior aos parâmetros configurados, um alarme será acionado. O valor deve estar entre 35,1 °C e 44,9 °C .

3. Clique em **Salvar** .

7.12.13 Definir os parâmetros do terminal de reconhecimento facial

Clique em **Manutenção e gerenciamento** → **Dispositivo** para entrar na lista de dispositivos.

Pressione **CTRL** e clique  para entrar na página de configuração remota.

Clique em **Outro** → **Parâmetros do terminal de reconhecimento facial** e você pode configurar os parâmetros do dispositivo.

Banco de dados de imagens de rosto

Selecione **Deep Learning** como banco de dados de imagens faciais.

Salvar foto de rosto de autenticação

Se ativado, a imagem do rosto capturada durante a autenticação será salva no dispositivo.

Leitura de cartão CPU

Selecione para ler o nº do cartão ou arquivo.

Modo de trabalho

Defina o modo de trabalho do dispositivo como **Modo Normal** . Você deve autenticar sua credencial para acesso.

Modo Eco

Após ativar o modo ECO, o dispositivo usará a câmera infravermelha para autenticar rostos em ambientes com pouca luz ou escuro. E você pode definir o limite do modo ECO, modo ECO (1: N) e modo ECO (1: 1).

Modo ECO (1: 1)

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

Modo ECO (1: N)

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


Limiar do modo ECO

Ao habilitar o modo ECO, você pode definir o limite do modo ECO. Quanto maior o valor, mais fácil será o dispositivo entrar no modo ECO. Faixa disponível: 0 a 8.

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

7.12.14 Configurar os parâmetros da imagem do rosto

Passos

1. Clique em **Manutenção e gerenciamento** → **Dispositivo** para entrar na lista de dispositivos.
2. Clique  para entrar na página de configuração remota.
3. Clique em **Other** → **Face Picture Parameters** para entrar na página Configuring Face Picture Parameters.

Ângulo de inclinação

O ângulo de inclinação máximo durante a autenticação facial.

Ângulo de guinada

O ângulo máximo de guinada durante a autenticação facial.

Margem (esquerda)

A porcentagem da distância do lado esquerdo do rosto até a margem esquerda na área de reconhecimento.

A porcentagem de distância real deve ser maior do que o valor configurado durante a autenticação da imagem facial. Outras porcentagens, distâncias e ângulos também devem atender às suas condições.

Margem (direita)

A porcentagem da distância do lado direito do rosto até a margem direita na área de reconhecimento.

A porcentagem de distância real deve ser maior do que o valor configurado durante a autenticação da imagem facial. Outras porcentagens, distâncias e ângulos também devem atender às suas condições.

Margem (superior)

A porcentagem de distância do lado superior da face até a margem superior na área de reconhecimento.

A porcentagem de distância real deve ser maior do que o valor configurado durante a autenticação da imagem facial. Outras porcentagens, distâncias e ângulos também devem atender às suas condições.

Margem (inferior)

A porcentagem de distância do lado inferior da face até a margem inferior na área de reconhecimento.

A porcentagem de distância real deve ser maior do que o valor configurado durante a autenticação da imagem facial. Outras porcentagens, distâncias e ângulos também devem atender às suas condições.

Distância Pupilar

A resolução mínima entre dois alunos no reconhecimento de rosto.

A resolução real deve ser maior que o valor configurado.

Ponto

O dispositivo pontuará 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.


Você pode definir os parâmetros da imagem do rosto ao autenticar.

4. Clique em **Salvar** .

7.12.15 Configurar parâmetros de luz de suplemento

Você pode ligar ou desligar a luz suplementar. Você também pode ajustar o brilho da luz suplementar.

Passos

1. Clique em **Manutenção e gerenciamento** → **Dispositivo** para entrar na lista de dispositivos.
2. Clique  para entrar na página de configuração remota.
3. Clique em **Other** → **Supplement Light Parameters** para entrar na página Configuring Supplement Light Parameters.
4. Selecione um tipo de luz suplementar na lista suspensa.
5. Selecione um modo de luz suplementar na lista suspensa.
6. Opcional: Defina o brilho da luz suplementar.
7. Clique em **Salvar** para salvar as configurações.

7.12.16 Definir nº do dispositivo

Defina o tipo de dispositivo, nº da comunidade, nº do prédio, nº do andar, nº da unidade e nº da sala

Clique em **Manutenção e gerenciamento** → **Dispositivo** para entrar na lista de dispositivos.


Clique  para entrar na página de configuração remota.

Clique em **Outro** → **Nº. Configurações** e defina o tipo de dispositivo, nº da comunidade, nº do prédio, nº do andar, nº da unidade e nº

7.12.17 Configurar os parâmetros de vídeo e áudio


Você pode definir a qualidade da imagem da câmera do dispositivo, resolução e outros parâmetros.

Passos

1. Clique em **Manutenção e gerenciamento** → **Dispositivo** para entrar na lista de dispositivos.
2. Clique  para entrar na página de configuração remota.
3. Clique em **Imagem** → **Vídeo e Áudio** para entrar na página de configurações.
4. Defina os parâmetros da câmera do dispositivo, incluindo o tipo de fluxo, o tipo de taxa de bits, a qualidade do vídeo, a taxa de quadros, o tipo de codificação de áudio, o tipo de vídeo, a taxa de bits, a resolução e o intervalo de quadros I.
5. Clique em **Salvar** .


7.12.18 Configurar entrada ou saída de volume

Passos

1. Na página Device for Management, clique em  → **Imagem** → **Entrada ou Saída de Áudio** para entrar na guia **Entrada ou Saída de Áudio** .
2. Mova o bloco para ajustar o volume de entrada e saída do dispositivo.
3. Clique em **Salvar** .

7.12.19 Operar relé

Passos

1. Clique em **Manutenção e gerenciamento** → **Dispositivo** para entrar na lista de dispositivos.
2. Clique  para entrar na página de configuração remota.
3. Clique em **Operação** → **Relé** .
4. Habilite ou desabilite o relé.

7.12.20 Ver Status do Relé

Clique em **Manutenção e gerenciamento** → **Dispositivo** para entrar na lista de dispositivos.

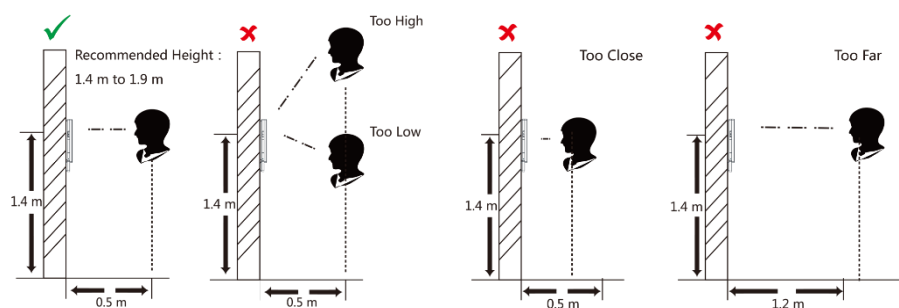
Clique  para entrar na página de configuração remota.

Clique em **Status** → **Relay** e você pode visualizar o status do relé.

A. Dicas para coletar / comparar imagens de rostos

A posição ao coletar ou comparar a imagem do rosto é a seguinte:

Posições (distância recomendada: 0,5 m)



Expressão

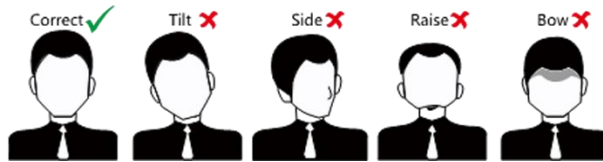
- Mantenha sua expressão naturalmente ao coletar ou comparar fotos de rostos, assim como a expressão na imagem abaixo.



- Não use chapéu, óculos de sol ou outros acessórios que possam afetar a função de reconhecimento facial.
- Não faça seu cabelo cobrir os olhos, orelhas, etc. e maquiagem pesada não é permitida.

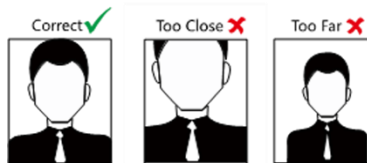
Postura

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



Tamanho

Certifique-se de que seu rosto esteja no meio da janela de coleta.



B. Dicas para o ambiente de instalação

1. Valor de referência de iluminação da fonte de luz



Vela: 10Lux



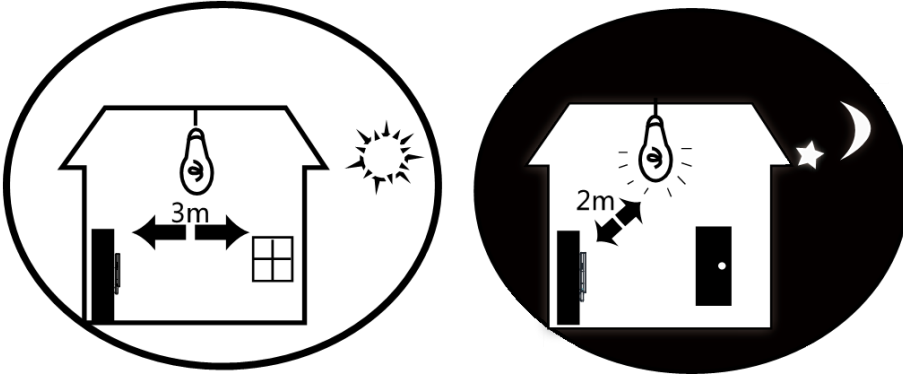
Bulbo: 100 ~ 850Lux



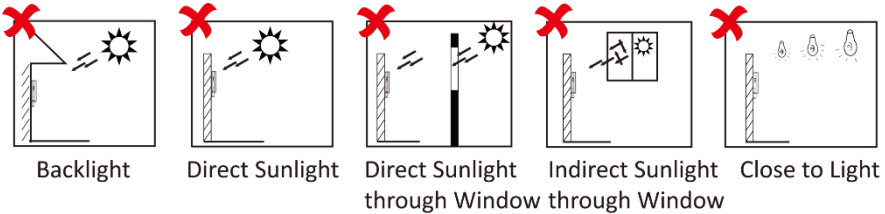
Luz solar: mais de 1200 lux

Face Recognition Terminal User Manual

2. Instale o dispositivo a pelo menos 2 metros de distância da luz e a pelo menos 3 metros de distância da janela ou porta.

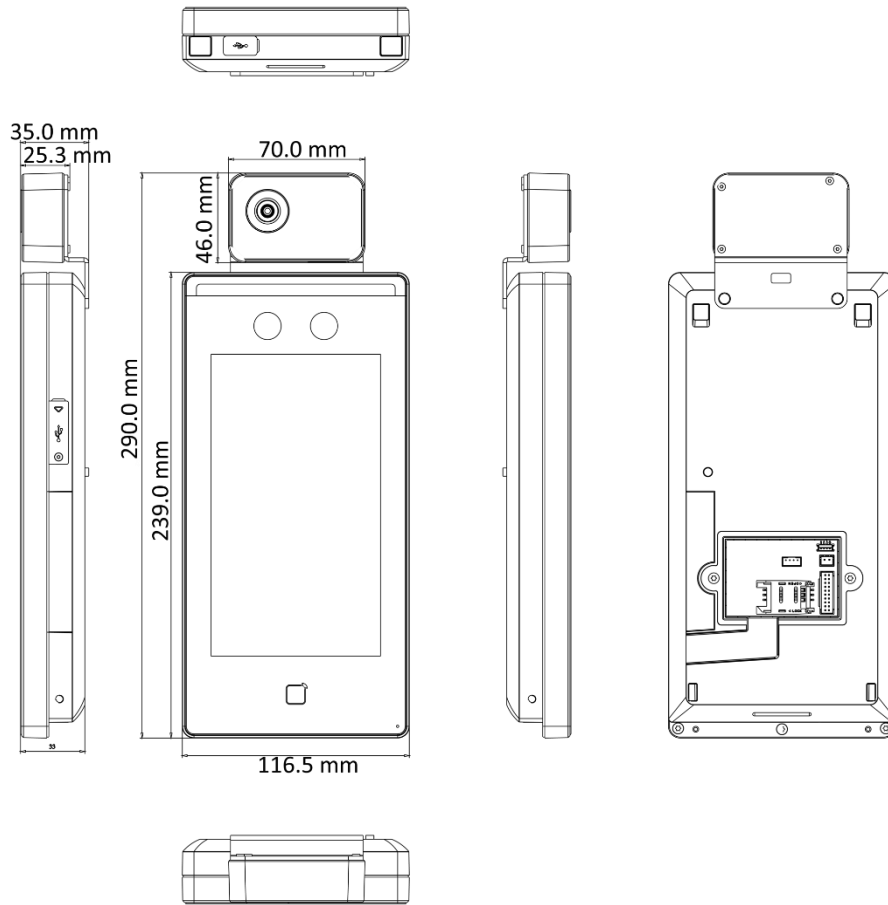


3. Evite luz de fundo, luz solar direta e indireta

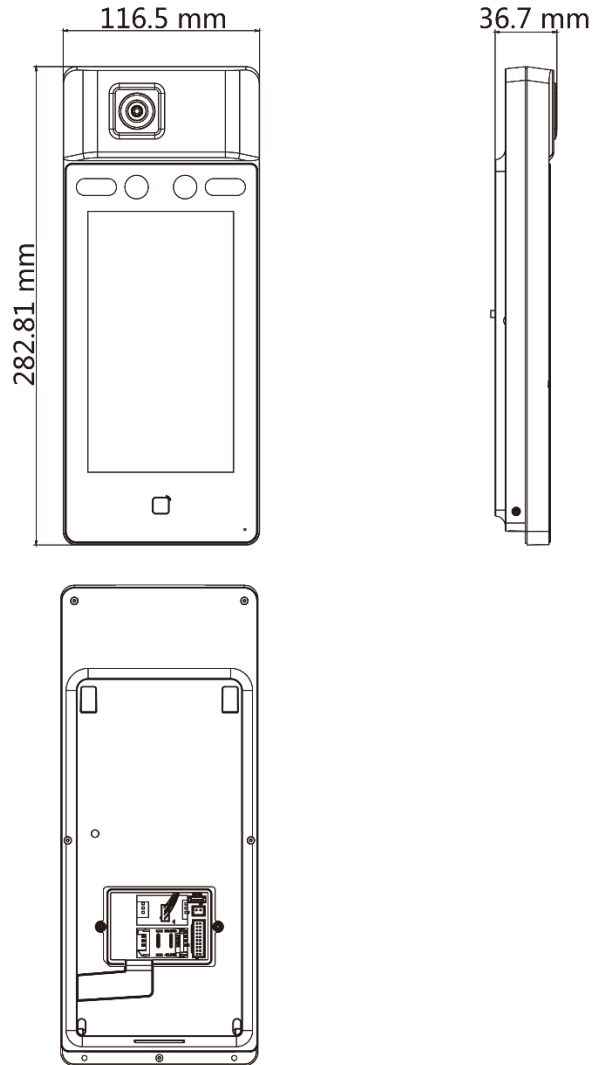


C. Dimensão

Face Recognition Terminal User Manual



Face Recognition Terminal User Manual



1

Face Recognition Terminal User Manual

UD19520B-A