Controlador de acessos

Manual do utilizador

Informações Legais

Sobre este manual

O Manual inclui instruções para utilizar e gerir o Produto. As fotos, gráficos, imagens e todas as outras informações que se seguem são apenas para descrição e explicação. As informações contidas no Manual estão sujeitas a alterações, sem aviso prévio, devido a atualizações de firmware ou outros motivos. Encontre a versão mais recente deste manual no site da Hikvision (***https://www.hikvision.com/***).

Utilize este Manual com a orientação e assistência de profissionais com formação no suporte ao Produto.

Marcas registadas

HIKVISION e outras marcas registadas e logótipos da Hikvision são propriedades da Hikvision em várias jurisdições.

Outras marcas registadas e logótipos mencionados são propriedade dos seus respetivos proprietários.

Isenção de responsabilidade

NA MEDIDA MÁXIMA PERMITIDA PELA LEI APLICÁVEL, ESTE MANUAL E O PRODUTO DESCRITO, COM O SEU HARDWARE, SOFTWARE E FIRMWARE, SÃO FORNECIDOS "TAL COMO ESTÃO" E "COM TODAS AS FALHAS E ERROS". A HIKVISION NÃO OFERECE GARANTIAS, EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÃO, COMERCIALIZAÇÃO, QUALIDADE SATISFATÓRIA OU ADEQUAÇÃO A UM DETERMINADO FIM. A UTILIZAÇÃO DO PRODUTO POR SI É POR SUA CONTA E RISCO. EM HIPÓTESE ALGUMA A HIKVISION SERÁ RESPONSÁVEL PERANTE SI POR QUAISQUER DANOS ESPECIAIS, CONSEQUENCIAIS, ACIDENTAIS OU INDIRETOS, INCLUINDO, ENTRE OUTROS, DANOS POR PERDA DE LUCROS COMERCIAIS, INTERRUPÇÃO DE NEGÓCIO OU PERDA DE DADOS, CORRUPÇÃO DE SISTEMAS OU PERDA DE DOCUMENTAÇÃO, SEJA BASEADO EM QUEBRA DE CONTRATO, ATO ILÍCITO (INCLUINDO NEGLIGÊNCIA), RESPONSABILIDADE DO PRODUTO OU DE OUTRA FORMA, EM RELAÇÃO À UTILIZAÇÃO DO PRODUTO, MESMO QUE A HIKVISION TENHA SIDO AVISADA DA POSSIBILIDADE DE TAIS DANOS OU PERDAS.
RECONHECE QUE A NATUREZA DA INTERNET PROPORCIONA RISCOS DE SEGURANÇA INERENTES, E A HIKVISION NÃO ASSUMIRÁ QUALQUER RESPONSABILIDADE POR OPERAÇÃO ANORMAL, FUGAS DE PRIVACIDADE OU OUTROS DANOS RESULTANTES DE ATAQUE CIBERNÉTICO, ATAQUE DE HACKER, INFECÇÃO POR VÍRUS OU OUTROS RISCOS DE SEGURANÇA NA INTERNET; NO ENTANTO, A HIKVISION FORNECERÁ UM APOIO TÉCNICO OPORTUNO, SE NECESSÁRIO.
CONCORDA EM UTILIZAR ESTE PRODUTO EM CONFORMIDADE COM TODAS AS LEIS APLICÁVEIS E É O ÚNICO RESPONSÁVEL POR GARANTIR QUE A SUA UTILIZAÇÃO ESTÁ EM CONFORMIDADE COM A LEI APLICÁVEL. ESPECIALMENTE, É RESPONSÁVEL POR UTILIZAR ESTE PRODUTO DE UMA 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. NÃO DEVE UTILIZAR ESTE PRODUTO PARA QUAISQUER UTILIZAÇÕES FINAIS PROIBIDAS, INCLUINDO O

DESENVOLVIMENTO OU PRODUÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA, DESENVOLVIMENTO OU PRODUÇÃO DE ARMAS QUÍMICAS OU BIOLÓGICAS, QUAISQUER ATIVIDADES NO CONTEXTO RELACIONADO COM QUALQUER EXPLOSIVO NUCLEAR OU CICLO DE COMBUSTÍVEL NUCLEAR INSEGURO, OU EM APOIO A ABUSOS DOS DIREITOS HUMANOS.

EM CASO DE QUALQUER CONFLITO ENTRE ESTE MANUAL E A LEI APLICÁVEL, PREVALECERÁ ESTA ÚLTIMA.

Proteção de Dados

Durante a utilização do dispositivo, os dados pessoais serão recolhidos, armazenados e tratados. Para proteger os dados, o desenvolvimento de dispositivos Hikvision incorpora princípios de privacidade desde o design. Por exemplo, para dispositivos com capacidades de reconhecimento facial, os dados biométricos são armazenados no seu dispositivo com um método de encriptação; para o dispositivo de impressão digital, apenas o modelo de impressão digital será guardado, o que é impossível de reconstruir uma imagem de impressão digital.

Como responsável pelo tratamento de dados, é aconselhado a recolher, armazenar, processar e transferir dados de acordo com as leis e regulamentos de proteção de dados aplicáveis, incluindo, sem limitação, a realização de controlos de segurança para proteger os dados pessoais, tais como, a implementação de controlos de segurança administrativos e físicos razoáveis, realizar revisões e avaliações periódicas da eficácia dos seus controlos de segurança.

Modelo disponível

Nome do produto	Modelo
Controlador de acessos	Controlador de acesso série DS-K2601T
	Controlador de acesso série DS-K2602T
	Controlador de acesso série DS-K2604T
	Controlador de acesso DS-K2601-G
	Controlador de acesso DS-K2602-G
	Controlador de acessos DS-K2604-G

Informações Regulatórias

Informações da FCC

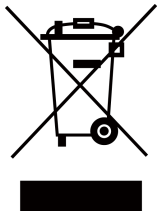
Tenha em atenção que alterações ou modificações não aprovadas expressamente pela parte responsável pela conformidade podem anular a autoridade do utilizador para operar o equipamento.
Conformidade com a FCC: Este equipamento foi testado e está em conformidade com os limites para um dispositivo digital de Classe B, de acordo com a parte 15 das Regras da FCC. Estes limites foram concebidos para proporcionar uma proteção razoável contra interferências prejudiciais numa instalação residencial. Este equipamento gera, utiliza e pode irradiar energia de radiofrequência e, se não for instalado e utilizado de acordo com as instruções, pode causar interferências prejudiciais nas comunicações rádio. Contudo, não há garantia de que não ocorrerão interferências numa instalação específica. Se este equipamento causar interferências prejudiciais à receção de rádio ou televisão, o que pode ser determinado desligando e ligando o equipamento, o utilizador é encorajado a tentar corrigir a interferência através de uma ou mais das seguintes medidas:

— Reoriente ou reposicione a antena recetora.
— Aumentar a separação entre o equipamento e o receptor.
— Ligue o equipamento a uma tomada de um circuito diferente daquele ao qual o receptor está ligado.
— Consulte o revendedor ou um técnico de rádio/TV experiente para obter ajuda
Este equipamento deve ser instalado e operado com uma distância mínima de 20cm entre o radiador e o seu corpo.
Condições da FCC
Este dispositivo está em conformidade com a parte 15 das Regras da FCC. A operação está sujeita às duas condições seguintes:
1. Este dispositivo não pode causar interferências prejudiciais.
2. Este dispositivo deve aceitar qualquer interferência recebida, incluindo interferências que possam causar um funcionamento indesejado.

Declaração de conformidade da UE

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

ao abrigo da Diretiva EMC 2014/30/UE, da Diretiva RE 2014/53/UE, da Diretiva RoHS 2011/65/UE



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

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

Conformidade da Indústria Canadá com o ICES-003

Este dispositivo cumpre os requisitos das normas CAN ICES-3 (B)/NMB-3(B).

Este dispositivo está em conformidade com as normas RSS isentas de licença da Industry Canada. A operação está sujeita às duas condições seguintes:

1. este dispositivo não pode causar interferências e
2. este dispositivo deve aceitar qualquer interferência, incluindo interferências que possam causar um funcionamento indesejado do dispositivo.

O presente aparelho está em conformidade com o CNR da Indústria do Canadá, aplicável aos aparelhos isentos de licença de rádio. A exploração é autorizada nas seguintes condições:

1. O aparelho não deve ser feito de brouillage, et
2. O utilizador do aparelho deve aceitar todas as brouillage radioelectrique subi, mesmo que a brouillage seja susceptível de comprometer o funcionamento.

De acordo com os regulamentos da Industry Canada, este transmissor de rádio só pode operar utilizando uma antena de tipo e ganho máximo (ou inferior) aprovada para o transmissor pela Industry Canada. Para reduzir a potencial interferência rádio para outros utilizadores, o tipo de antena e o seu ganho devem ser escolhidos de modo a que a potência isotropicamente irradiada equivalente (EIRP) não seja superior à necessária para uma comunicação bem-sucedida.

De acordo com o regulamento da Indústria do Canadá, o atual emissor de rádio pode funcionar com uma antena de um tipo e um ganho máximo (ou inferior) aprovado para o gravador da Indústria do Canadá. Além disso, para reduzir os riscos de queima radioelétrica na intenção de outros utilizadores, deve escolher o tipo de antena e ganhar a sorte de que a potência isotrópica de raio de raio equivalente (pire) não ultrapasse a intensidade necessária para o estabelecimento de uma comunicação satisfatória.

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

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

Instrução de segurança

Estas instruções têm como objetivo garantir que o utilizador pode utilizar o produto corretamente para evitar perigos ou perda de propriedade.

A medida de precaução divide-se 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 no equipamento.

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

⚠ Perigo:

- Um dispositivo de desconexão apropriado deverá ser fornecido como parte da instalação.

  Nota

  Os dispositivos de desconexão externos não serão necessariamente fornecidos com o equipamento.
- Toda a operação eletrónica deve estar em estrita conformidade com os regulamentos de segurança elétrica, regulamentos de prevenção de incêndios e outros regulamentos relacionados na sua região local.
- Utilize o adaptador de alimentação fornecido pela empresa normal. O consumo de energia não pode ser inferior ao valor requerido.
- Não ligue vários dispositivos a um adaptador de alimentação, pois a sobrecarga do adaptador pode causar sobreaquecimento ou risco de incêndio.
- Certifique-se de que a alimentação foi desligada antes de ligar, instalar ou desmontar o dispositivo.
- Quando o produto é instalado na parede ou no teto, o dispositivo deve estar firmemente fixo.
- Se houver fumo, odores ou ruído proveniente do dispositivo, desligue imediatamente a alimentação e desligue o cabo de alimentação e, em seguida, contacte o centro de assistência.
- Não ingira bateria, risco de queimadura química.
  Este produto contém uma bateria tipo moeda/botão. Se a bateria tipo moeda/botão for engolida, pode causar queimaduras internas graves em apenas 2 horas e levar à morte.
  Mantenha as pilhas novas e usadas longe do alcance das crianças. Se o compartimento da bateria não fechar bem, pare de utilizar o produto e mantenha-o longe do alcance das crianças. Se acha que as pilhas podem ter sido engolidas ou colocadas dentro de qualquer parte do corpo, procure assistência médica imediata.
- Se o produto não funcionar corretamente, contacte o seu revendedor ou centro de assistência mais próximo. Nunca tente desmontar o dispositivo sozinho. (Não assumiremos qualquer responsabilidade por problemas causados por reparações ou manutenção não autorizadas.)

⚠ Cuidados:

- Não deixe cair o dispositivo nem o sujeite a choques físicos e não o exponha a elevadas radiações eletromagnéticas. Evite a instalação do equipamento em superfícies vibratórias ou locais sujeitos a choques (o desconhecimento pode provocar danos no equipamento).
- Não coloque o dispositivo em locais extremamente quentes (consulte as especificações do dispositivo para obter a temperatura de funcionamento detalhada), locais frios, poeirentos ou húmidos, e não o exponha a radiações eletromagnéticas elevadas.
- A tampa do dispositivo para utilização no interior deve ser protegida da chuva e da humidade.
- É proibido expor o equipamento a luz solar direta, baixa ventilação ou fonte de calor como aquecedor ou radiador (a ignorância pode causar perigo de incêndio).
- Não aponte o dispositivo para o sol ou para locais muito claros. Caso contrário, poderá ocorrer um florescimento ou manchas (o que não é uma avaria) e, ao mesmo tempo, afetar a resistência do sensor.
- Utilize a luva fornecida ao abrir a tampa do dispositivo, evite o contacto direto com a tampa do dispositivo, uma vez que o suor ácido dos dedos pode corroer o revestimento da superfície da tampa do dispositivo.

- Utilize um pano macio e seco para limpar as superfícies internas e externas da tampa do aparelho, não utilize detergentes alcalinos.
- Guarde todas as embalagens depois de as desembalar para uso futuro. Caso ocorra alguma falha, é necessário devolver o aparelho à fábrica com a embalagem original. O transporte sem a embalagem original pode resultar em danos no dispositivo e acarretar custos adicionais.
- A utilização ou substituição inadequada da bateria pode resultar em risco de explosão. Substitua apenas pelo mesmo tipo ou equivalente. Elimine as baterias usadas de acordo com as instruções fornecidas pelo fabricante da bateria.

Conteúdo

Capítulo 1 Dicas preventivas e cautelares

Antes de ligar e operar o seu dispositivo, observe as seguintes dicas:

- Certifique-se de que a unidade está instalada num ambiente bem ventilado e livre de pó.
- Mantenha todos os líquidos afastados do dispositivo.
- Certifique-se de que as condições ambientais cumprem as especificações de fábrica.
- Certifique-se de que a unidade está devidamente fixa a um bastidor ou prateleira. Grandes choques ou solavancos na unidade como resultado de uma queda podem causar danos nos componentes eletrónicos sensíveis dentro da unidade.
- Utilize o dispositivo em conjunto com um UPS, se possível.
- Desligue a unidade antes de ligar e desligar acessórios e periféricos.
- Deve ser utilizado um HDD recomendado pela fábrica para este dispositivo.
- A utilização ou substituição inadequada da bateria pode resultar em risco de explosão. Substitua apenas pelo mesmo tipo ou equivalente. Elimine as baterias usadas de acordo com as instruções fornecidas pelo fabricante.

Capítulo 2 Descrição do Produto

- Processador de alta velocidade de 32 bits
- Suporta comunicação TCP/IP, acesso EHome 5.0, protocolo ISAPI e protocolo OSDP. Os dados de comunicação são especialmente encriptados para aliviar a preocupação com a fuga de privacidade
- Suporta o reconhecimento e armazenamento do número do cartão com um comprimento máximo de 20
- Suporta até 100.000 cartões e 300.000 registos de apresentação de cartões
- Suporta função de encravamento de várias portas, função anti-passback, função de múltiplas autenticações, porta aberta com função de primeiro cartão, função de super cartão e super senha, encriptação de cartão M1, função de atualização online e controlo remoto das portas
- Suporta alarme de violação para o leitor de cartões, alarme para porta não protegida, alarme de porta de abertura forçada, alarme para tempo limite de abertura de porta, cartão de coação e alarme de código, alarme de lista de bloqueio e alarme para tentativas ilegais de passagem de cartão atingindo o limite
- Alarme de tentativas de curto-circuito e alarme de tentativas de circuito aberto
- Detecção de conflito de endereços IP
- Função anti-passback de controlador cruzado (para anti-passback de controlador cruzado baseado em cartão, ligue o leitor de cartões com RS-485. Para anti-passback de controlador cruzado baseado em rede, certifique-se de que o servidor e o dispositivo comunicar entre si corretamente .
- Suporta interface RS-485 e interface Wiegand para acesso ao leitor de cartões. A interface Wiegand suporta W26, W34 e é compatível com leitores de cartões de terceiros com interface Wiegand
- Suporta a adição de vários tipos de pessoas: pessoa normal, visitante e pessoa na lista de bloqueio.
- Suporta vários tipos de cartão: normal/desativado/lista de bloqueio/patrulha/visitante/coação/super cartão, etc.
- Vários indicadores para mostrar diferentes estados
- Suporta sincronização de horário automática e manualmente
- Suporta a função de armazenamento de registos quando o dispositivo está offline e a função de alarme de armazenamento de espaço de armazenamento insuficiente
- Design da bateria de reserva, design de vigilância e função à prova de violação
- Os dados podem ser guardados permanentemente depois de o controlador de acesso ser desligado
- Suporta a ligação de E/S e a ligação de eventos
- Suporta o protocolo EHome para ligação à rede pública
- 500 grupos de palavras-passe no modo de autenticação de cartão ou palavra-passe
- Suporta definições de fuso horário

Capítulo 3 Descrição da Placa Principal

3.1 Descrição da placa principal do controlador de acesso de porta única

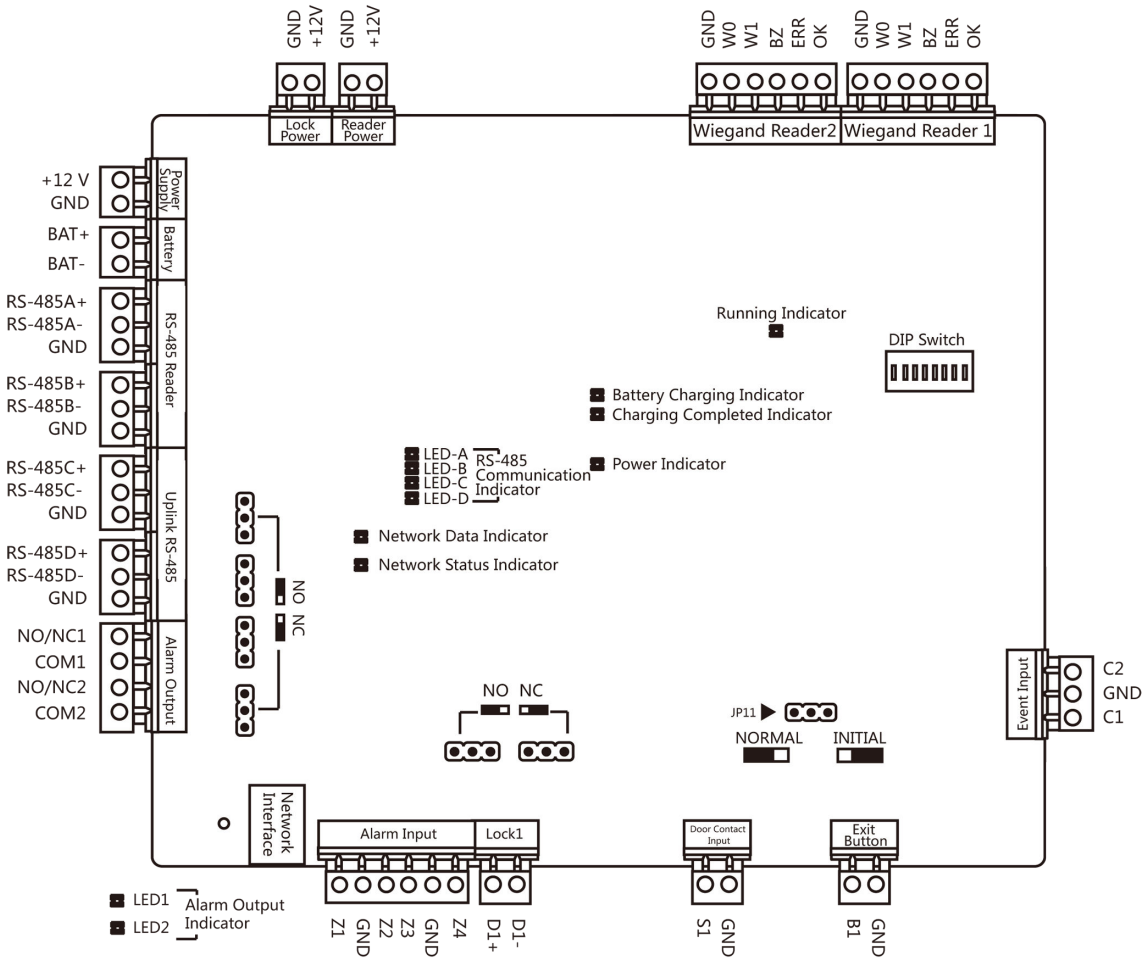


Figura 3-1 Placa principal do controlador de acesso de porta única

3.2 Descrição da placa principal do controlador de acesso de duas portas

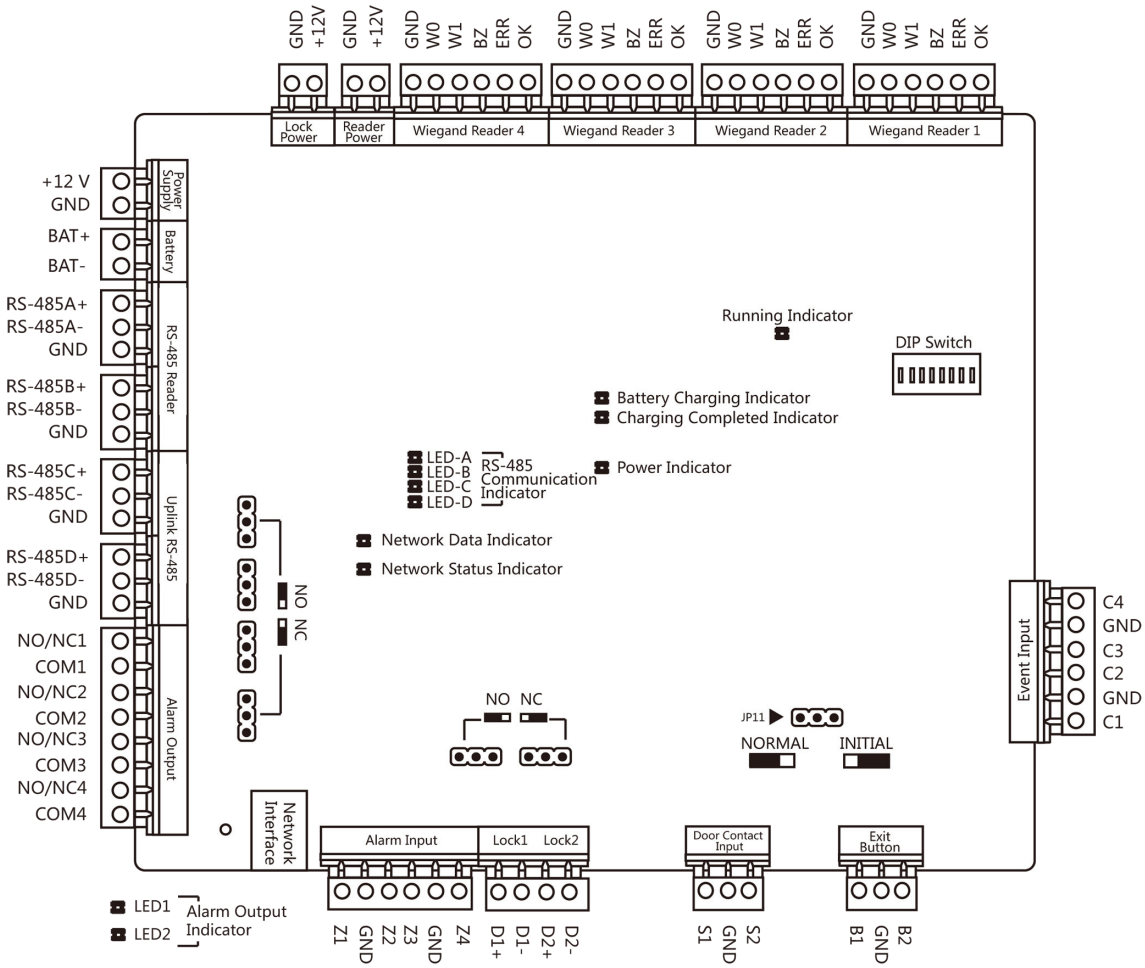


Figura 3-2 Placa principal do controlador de acesso de duas portas

3.3 Descrição da placa principal do controlador de acesso de quatro portas

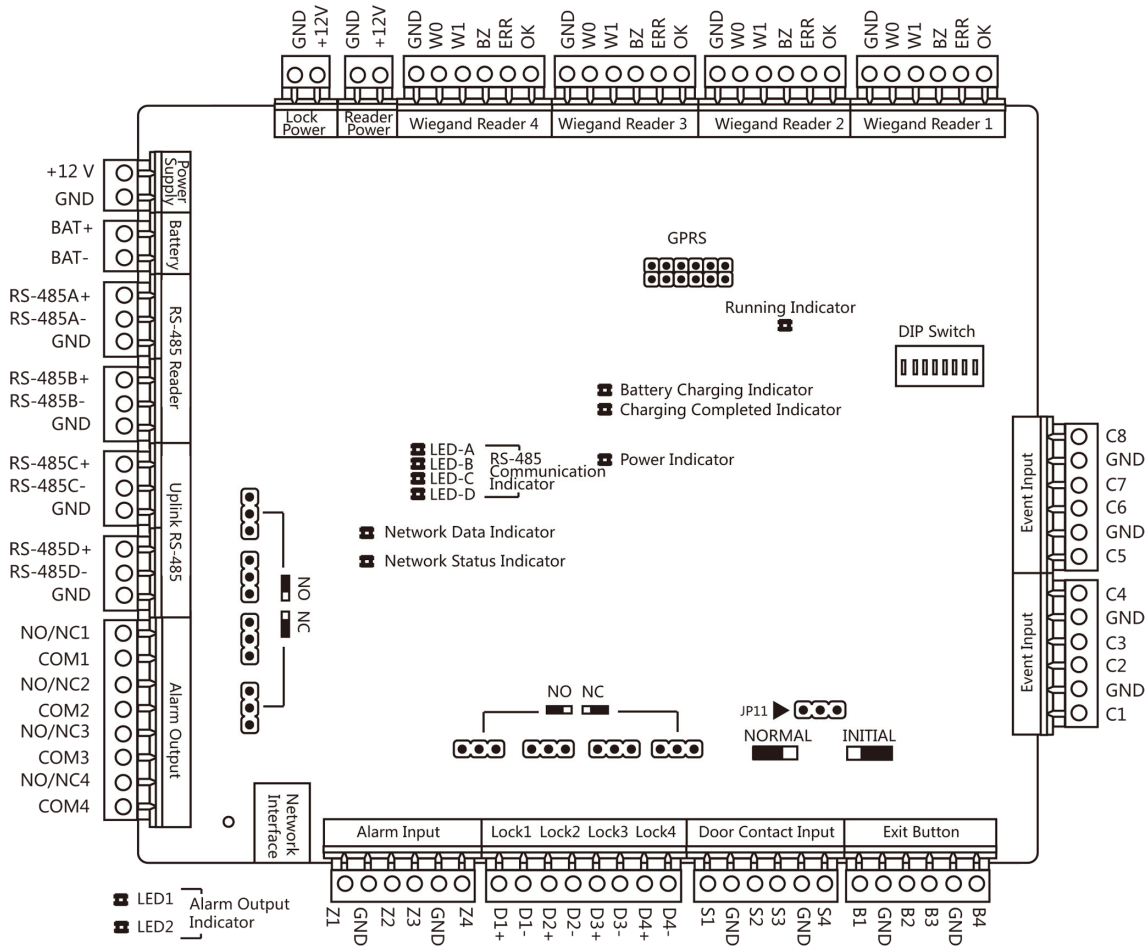


Figura 3-3 Placa principal do controlador de acesso de quatro portas

3.4 Descrição do Componente

Pode visualizar os componentes do dispositivo e as suas descrições.

Tomemos como exemplo o controlador de acesso de quatro portas, o diagrama de componentes é apresentado abaixo.

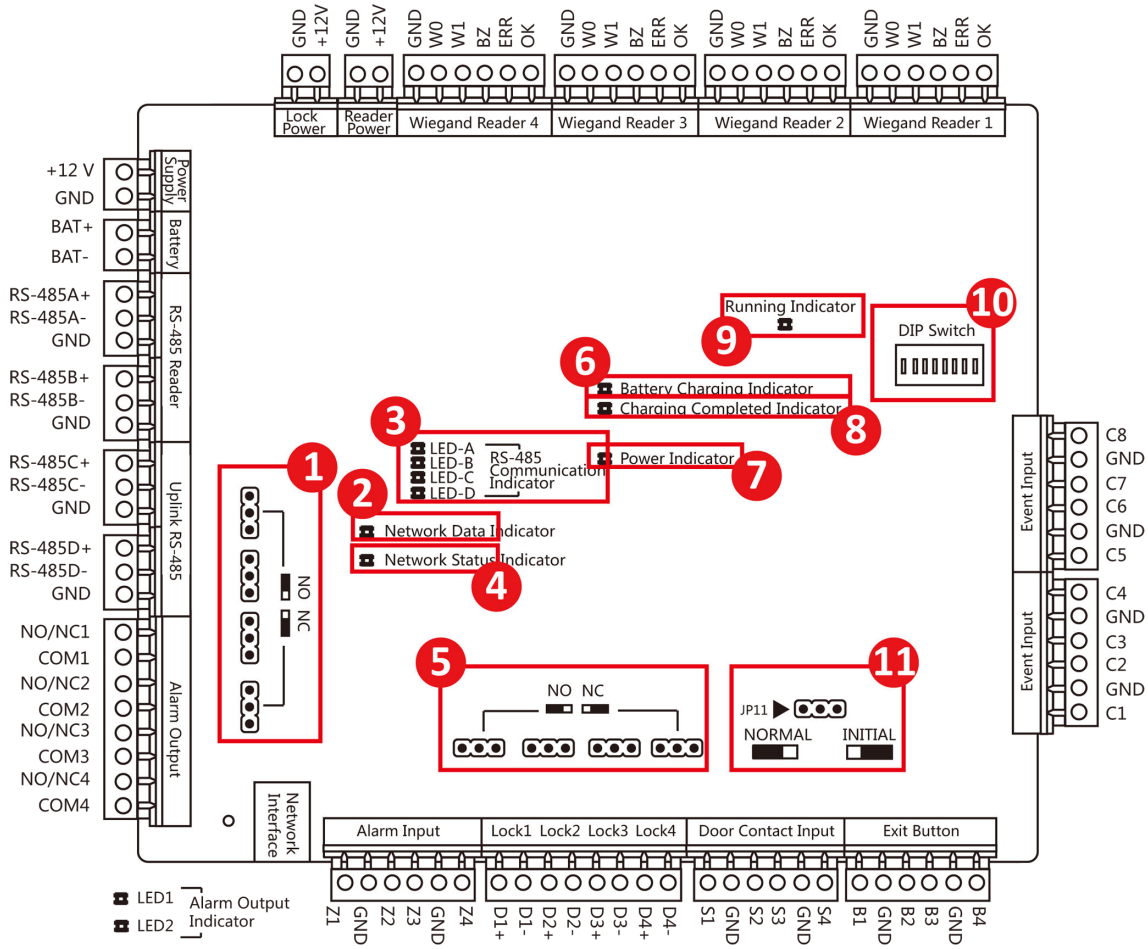


Figura 3-4 Diagrama de Componentes do Controlador de Acesso de Quatro Portas

Tabela 3-1 Descrição do componente do controlador de acesso de quatro portas

Não.	Descrição do Componente		
	Acesso de porta única Controlador	Acesso de duas portas Controlador	Acesso de quatro portas Controlador
1	Estado de saída de relé de alarme (NF/NA)		
2	Indicador de dados de rede		
3	Indicador de comunicação RS-485		
4	Indicador de estado da rede		
5	Escolha do estado da saída do relé da porta (NC/NO)		
6	Indicador de carga da bateria		

7	Indicador de energia
8	Indicador de conclusão do carregamento
9	Indicador de execução
10	Interruptor DIP da placa principal Defina o endereço DIP para o controlador de acesso. Gama disponível: 1 a 63. Exemplo: Se o endereço DIP for 24, coloque o Bit 4 e o Bit 5 em ON. **Nota** ● As definições serão válidas após a reinicialização do dispositivo. ● Para obter detalhes sobre as definições DIP, consulte*Anexo A Descrição do interruptor DIP*.
11	Arranque de hardware e escolha normal de funcionamento

Capítulo 4 Descrição do Terminal

Nota

- Séries 2602 e 2604: A potência nominal para fechadura de porta é de 12 V/2 A, e para fonte de alimentação de leitor de cartões é de 12 V/0,67 A.
- Série 2601: A potência nominal para a fechadura da porta é de 12 V/0,5 A e para a fonte de alimentação do leitor de cartões é de 12 V/0,3 A.

4.1 Descrição do Terminal Controlador de Acessos de Porta Única

Pode visualizar a descrição do terminal do controlador de acesso de porta única.

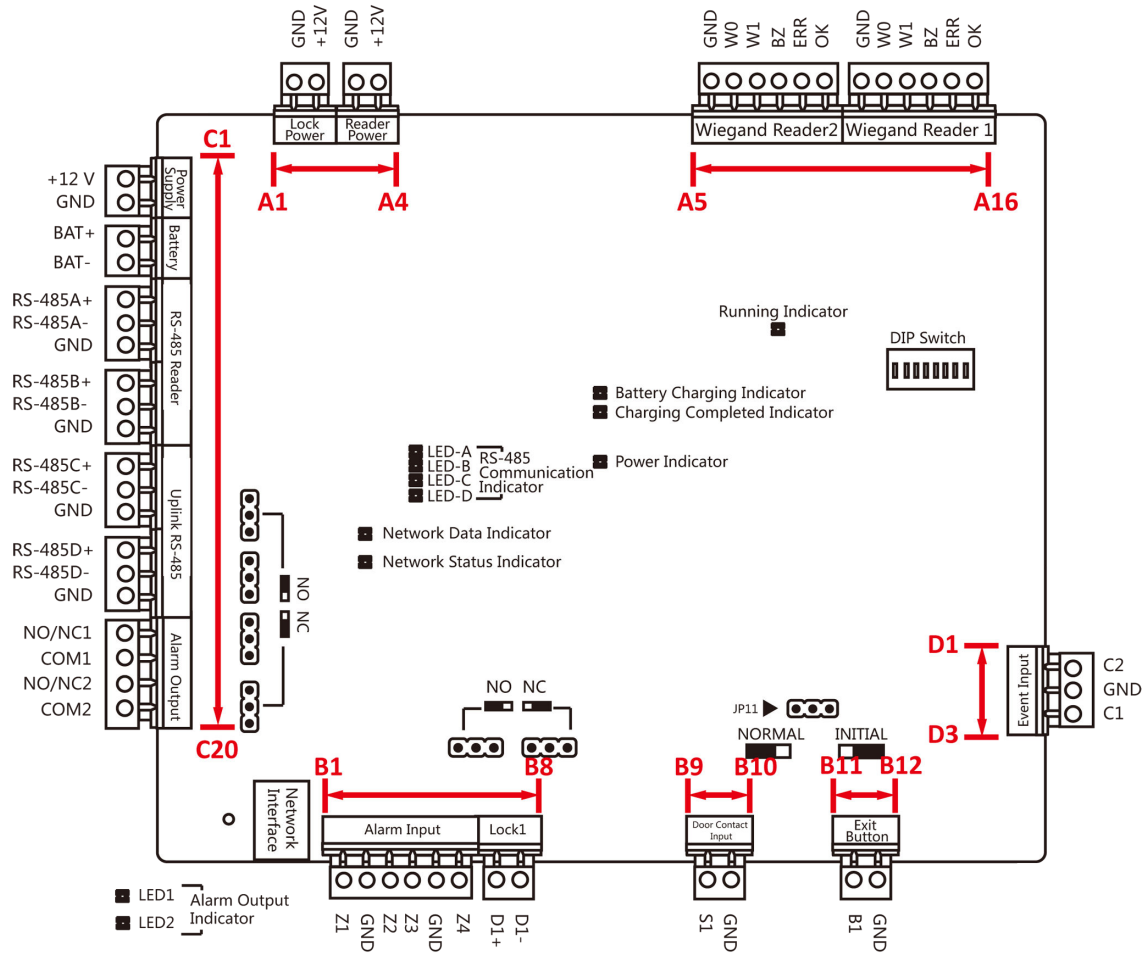


Figura 4-1 Placa principal do controlador de acesso de porta única

Tabela 4-1 Descrição do Terminal do Controlador de Acesso de Porta Única

Não.	Controlador de acesso de porta única		
A1	Fonte de alimentação do E-Lock	GND	Aterramento
A2		+ 12 V	Fonte de alimentação da saída E-Lock
A3	Fonte de alimentação do leitor de cartões	GND	Aterramento
A4		+ 12 V	Fonte de alimentação da saída do leitor de cartões
A5	Leitor de cartões Wiegand 2	GND	Aterramento
A6		W0	Leitor de cartões Wiegand Dados de entrada de dados0
A7		W1	Leitor de cartões Wiegand Dados de entrada de dados1
A8		BZ	Campainha do leitor de cartões Saída de controlo
A9		ERRAR	Indicador do Cartão Saída de controlo do leitor (Saída de cartão inválida)
A10		OK	Indicador do Cartão Saída de controlo do leitor (Saída de cartão válido)
A11	Leitor de cartões Wiegand 1	GND	Aterramento
A12		W0	Leitor de cartões Wiegand Dados de entrada de dados0
A13		W1	Leitor de cartões Wiegand Dados de entrada de dados1
A14		BZ	Campainha do leitor de cartões Saída de controlo
A15		ERRAR	Indicador do Cartão Saída de controlo do leitor (Saída de cartão inválida)
A16		OK	Indicador do Cartão Saída de controlo do leitor (Saída de cartão válido)

Não.	Controlador de acesso de porta única		
B1	Armando entrada de região	Z1	Armando Acesso à Região Terminal 1
B2		GND	Aterramento
B3		Z2	Armando Acesso à Região Terminal 2
B4		Z3	Armando Acesso à Região Terminal 3
B5		GND	Aterramento
B6		Z4	Armando Acesso à Região Terminal 4
B7	Bloqueio eletrónico	D1+	Entrada de relé da porta 1 (contacto seco)
B8		D1-	
B9	Entrada de contacto de porta	S1	Entrada do detector de contacto da porta da porta 1
B10		GND	Aterramento
B11	Botão de abertura de porta	B1	Entrada do botão de abertura da porta 1
B12		GND	Aterramento
C1	Poder	+ 12 V	Cátodo de 12 VCC
C2		GND	Aterramento
C3	Bateria	morcego+	Bateria de 12 VCC Cátodo
C4		BASTÃO-	Ânodo de bateria de 12 VCC
C5	Leitor de cartões RS-485 Interface	RS485A+	Leitor de cartões RS485A+ Acesso
C6		RS485A-	Leitor de cartões RS485A- Acesso
C7		GND	Aterramento
C8		RS485B+	Leitor de cartões RS485B+
C9		RS485B-	Leitor de cartões RS485B-
C10		GND	Aterramento

Não.	Controlador de acesso de porta única		
C11	Controlador de acessos Interface RS485	RS485C+	Ligação ascendente RS485+Comunicação
C12		RS485C-	Uplink RS485- Comunicação
C13		GND	Aterramento
C14		RS485D+	Reservado
C15		RS 485D-	
C16		GND	
Capítulo 17	Saída de alarme	NÃO/NC1	Saída do Relé de Alarme 1 (Contacto Seco)
Capítulo 18		COM1	
Capítulo 19		NÃO/NC2	Saída de relé de alarme 2 (contacto seco)
C20		COM2	
D1	Entrada de Evento	C2	Entrada de alarme de evento 2
D2		GND	Aterramento
D3		C1	Entrada de alarme de evento 1

Nota

- A interface de hardware de entrada de alarme está normalmente aberta por predefinição. Apenas o sinal normalmente aberto é permitido. Pode ser ligado à campainha do leitor de cartões e do controlador de acesso, à saída do relé de alarme e ao relé de abertura e fecho da porta.
- A ligação de entrada de alarme da região de armação é apenas para a ligação de saída de relé de alarme.
- O ID do leitor de cartões RS-485 deve ser definido para 1 a 2. A tabela apresentada abaixo mostra a relação entre o número da porta e o ID.

Porta nº.	ID do leitor de cartões RS-485	Descrição
Porta 1	1	Entrar
	2	Saída

- Para o controlador de acesso de porta única, a relação do leitor de cartões Wiegand e da porta é a seguinte.

Porta nº.	Leitor de cartões Wiegand	Descrição
Porta 1	1	Entrar
	2	Saída

4.2 Descrição do Terminal Controlador de Acessos de Duas Portas

Pode visualizar a descrição do terminal do controlador de acesso de duas portas.

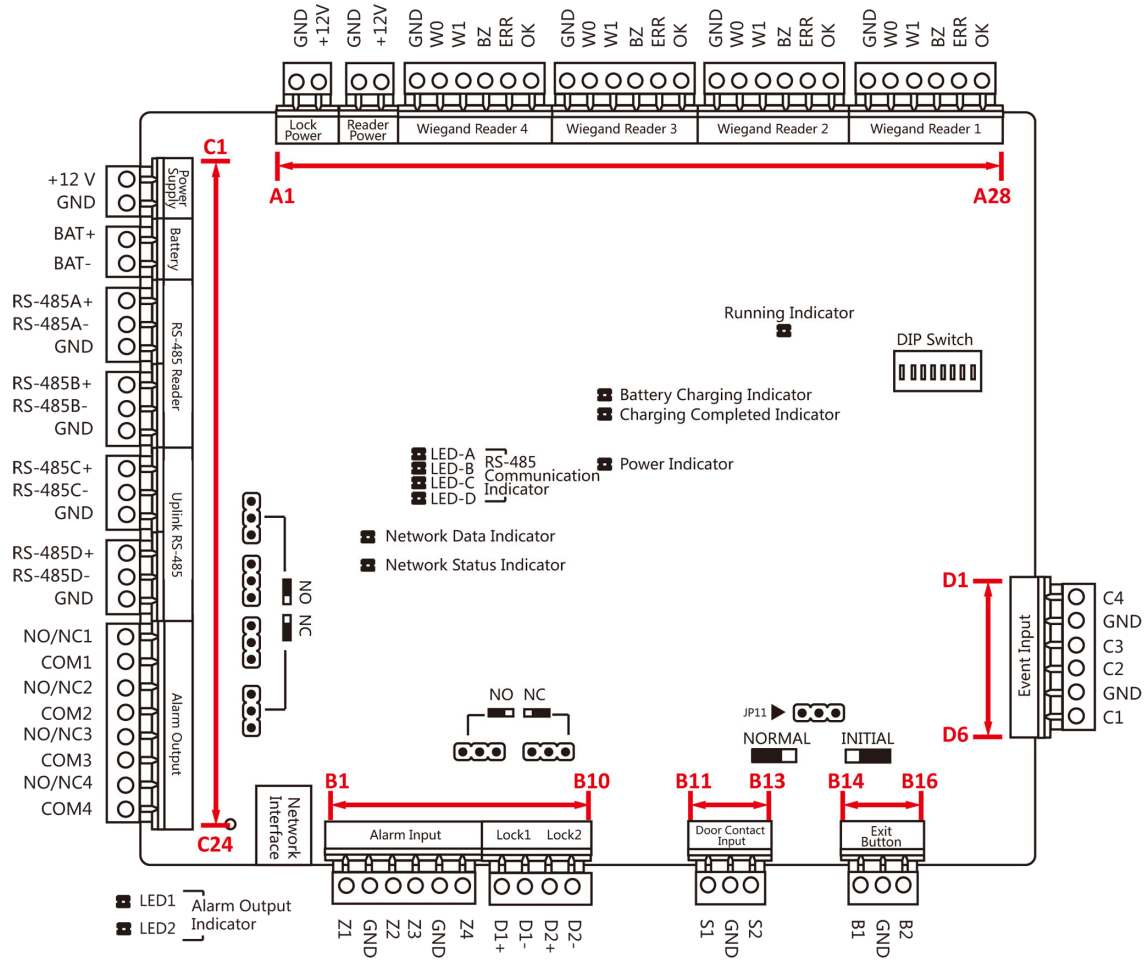


Figura 4-2 Placa principal do controlador de acesso de duas portas

Tabela 4-2 Descrição do terminal do controlador de acesso de duas portas

Não.	Controlador de acessos de duas portas		
A1	Fonte de alimentação do E-Lock	GND	Aterramento
A2		+ 12 V	Fonte de alimentação da saída E-Lock
A3	Fonte de alimentação do leitor de cartões	GND	Aterramento
A4		+ 12 V	Fonte de alimentação da saída do leitor de cartões
A5	Leitor de cartões Wiegand 4	GND	Aterramento
A6		W0	Leitor de cartões Wiegand Dados de entrada de dados0
A7		W1	Leitor de cartões Wiegand Dados de entrada de dados1
A8		BZ	Campainha do leitor de cartões Saída de controlo
A9		ERRAR	Indicador do Cartão Saída de controlo do leitor (Saída de cartão inválida)
A10		OK	Indicador do Cartão Saída de controlo do leitor (Saída de cartão válido)
A11	Leitor de cartões Wiegand 3	GND	Aterramento
A12		W0	Leitor de cartões Wiegand Dados de entrada de dados0
A13		W1	Leitor de cartões Wiegand Dados de entrada de dados1
A14		BZ	Campainha do leitor de cartões Saída de controlo
A15		ERRAR	Indicador do Cartão Saída de controlo do leitor (Saída de cartão inválida)
A16		OK	Indicador do Cartão Saída de controlo do leitor (Saída de cartão válido)

Não.	Controlador de acessos de duas portas		
A17	Leitor de cartões Wiegand 2	GND	Aterramento
A18		W0	Leitor de cartões Wiegand Dados de entrada de dados0
A19		W1	Leitor de cartões Wiegand Dados de entrada de dados1
A20		BZ	Campainha do leitor de cartões Saída de controlo
A21		ERRAR	Indicador do Cartão Saída de controlo do leitor (Saída de cartão inválida)
A22		OK	Indicador do Cartão Saída de controlo do leitor (Saída de cartão válido)
A23	Leitor de cartões Wiegand 1	GND	Aterramento
A24		W0	Leitor de cartões Wiegand Dados de entrada de dados0
A25		W1	Leitor de cartões Wiegand Dados de entrada de dados1
A26		BZ	Campainha do leitor de cartões Saída de controlo
A27		ERRAR	Indicador do Cartão Saída de controlo do leitor (Saída de cartão inválida)
A28		OK	Indicador do Cartão Saída de controlo do leitor (Saída de cartão válido)
B1	Armando entrada de região	Z1	Armando Acesso à Região Terminal 1
B2		GND	Aterramento
B3		Z2	Armando Acesso à Região Terminal 2
B4		Z3	Armando Acesso à Região Terminal 3

Não.	Controlador de acessos de duas portas		
B5		GND	Aterramento
B6		Z4	Armando Acesso à Região Terminal 4
B7	E-Lock1	D1+	Entrada de relé da porta 1 (contacto seco)
B8		D1-	
B9	E-Lock2	D2+	Entrada de relé da porta 2 (contacto seco)
B10		D2-	
B11	Porta Magnética Detector	S1	Porta 1 Magnética Entrada do detector
B12		GND	Aterramento
B13		S2	Porta 2 Magnética Entrada do detector
B14	Botão da porta	B1	Entrada do botão da porta da porta 1
B15		GND	Aterramento
B16		B2	Entrada do botão da porta 2
C1	Poder	+ 12 V	Cátodo de 12 VCC
C2		GND	Aterramento
C3	Bateria	morcego+	Bateria de 12 VCC Cátodo
C4		BASTÃO-	Ânodo de bateria de 12 VCC
C5	Leitor de cartões RS485 Interface	RS485A+	Leitor de cartões RS485A+ Acesso
C6		RS485A-	Leitor de cartões RS485A- Acesso
C7		GND	Aterramento
C8		RS485B+	Leitor de cartões RS485B+
C9		RS485B-	Leitor de cartões RS485B-
C10		GND	Aterramento

Não.	Controlador de acessos de duas portas		
C11	Controlador de acessos Interface RS485	RS485C+	Ligação ascendente RS485+Comunicação
C12		RS485C-	Uplink RS485- Comunicação
C13		GND	Aterramento
C14		RS485D+	Reservado
C15		RS 485D-	
C16		GND	
Capítulo 17	Saída de alarme	NÃO/NC1	Saída do Relé de Alarme 1 (Contacto Seco)
Capítulo 18		COM1	
Capítulo 19		NÃO/NC2	Saída de relé de alarme 2 (contacto seco)
C20		COM2	
Capítulo 21		NÃO/NC3	Saída do Relé de Alarme 3 (Contacto Seco)
C22		COM3	
Capítulo 23		NÃO/NC4	Saída de relé de alarme 4 (contacto seco)
Capítulo 24		COM4	
D1	Entrada de Evento	C4	Entrada de alarme de evento 4
D2		GND	Aterramento
D3		C3	Entrada de alarme de evento 3
D4		C2	Entrada de alarme de evento 2
D5		GND	Aterramento
D6		C1	Entrada de alarme de evento 1

Nota

- A interface de hardware de entrada de alarme está normalmente aberta por predefinição. Portanto, apenas o sinal normalmente aberto é permitido. Pode ser ligado à campainha do leitor de cartões e do controlador de acesso, à saída do relé de alarme e ao relé de abertura e fecho da porta.
- A ligação de entrada de alarme da região de armação é apenas para a ligação de saída de relé de alarme.
- O ID do leitor de cartões RS-485 deve ser definido para 1 a 8.

Porta nº.	ID do leitor de cartões RS-485	Descrição
Porta 1	1	Entrar
	2	Saída
Porta 2	3	Entrar
	4	Saída

- Para o controlador de acesso de duas portas, a relação do leitor de cartões Wiegand e da porta é a seguinte.

Porta nº.	Leitor de cartões Wiegand	Descrição
Porta 1	1	Entrar
	2	Saída
Porta 2	3	Entrar
	4	Saída

4.3 Descrição do Terminal Controlador de Acessos de Quatro Portas

Pode visualizar a descrição do terminal do controlador de acesso de quatro portas.

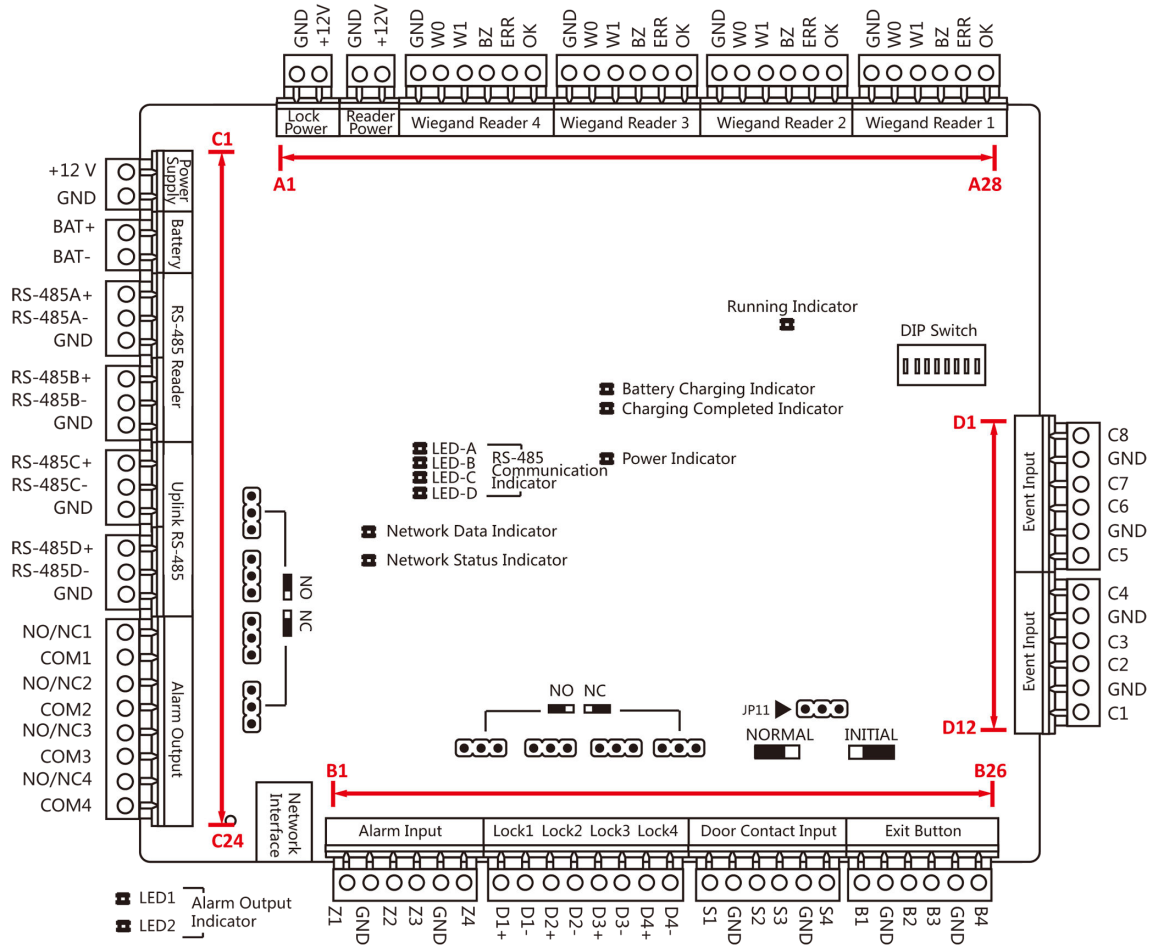


Figura 4-3 Placa principal do controlador de acesso de quatro portas

Tabela 4-3 Descrição do Terminal do Controlador de Acesso de Quatro Portas

Não.	Controlador de acessos de quatro portas		
A1	Fonte de alimentação do E-Lock	GND	Aterramento
A2		+ 12 V	Fonte de alimentação da saída E-Lock
A3	Fonte de alimentação do leitor de cartões	GND	Aterramento
A4		+ 12 V	Fonte de alimentação da saída do leitor de cartões
A5	Leitor de cartões Wiegand 4	GND	Aterramento
A6		W0	Leitor de cartões Wiegand Dados de entrada de dados0

Não.	Controlador de acessos de quatro portas		
A7		W1	Leitor de cartões Wiegand Dados de entrada de dados1
A8		BZ	Campainha do leitor de cartões Saída de controlo
A9		ERRAR	Indicador do Cartão Saída de controlo do leitor (Saída de cartão inválida)
A10		OK	Indicador do Cartão Saída de controlo do leitor (Saída de cartão válido)
A11	Leitor de cartões Wiegand 3	GND	Aterramento
A12		W0	Leitor de cartões Wiegand Dados de entrada de dados0
A13		W1	Leitor de cartões Wiegand Dados de entrada de dados1
A14		BZ	Campainha do leitor de cartões Saída de controlo
A15		ERRAR	Indicador do Cartão Saída de controlo do leitor (Saída de cartão inválida)
A16		OK	Indicador do Cartão Saída de controlo do leitor (Saída de cartão válido)
A17	Leitor de cartões Wiegand 2	GND	Aterramento
A18		W0	Leitor de cartões Wiegand Dados de entrada de dados0
A19		W1	Leitor de cartões Wiegand Dados de entrada de dados1
A20		BZ	Campainha do leitor de cartões Saída de controlo
A21		ERRAR	Indicador do Cartão Saída de controlo do leitor (Saída de cartão inválida)

Não.	Controlador de acessos de quatro portas		
A22		OK	Indicador do Cartão Saída de controlo do leitor (Saída de cartão válido)
A23	Leitor de cartões Wiegand 1	GND	Aterramento
A24		W0	Leitor de cartões Wiegand Dados de entrada de dados0
A25		W1	Leitor de cartões Wiegand Dados de entrada de dados1
A26		BZ	Campainha do leitor de cartões Saída de controlo
A27		ERRAR	Indicador do Cartão Saída de controlo do leitor (Saída de cartão inválida)
A28		OK	Indicador do Cartão Saída de controlo do leitor (Saída de cartão válido)
B1	Armando entrada de região	Z1	Armando Acesso à Região Terminal 1
B2		GND	Aterramento
B3		Z2	Armando Acesso à Região Terminal 2
B4		Z3	Armando Acesso à Região Terminal 3
B5		GND	Aterramento
B6		Z4	Armando Acesso à Região Terminal 4
B7	E-Lock1	D1+	Entrada de relé da porta 1 (contacto seco)
B8		D1-	
B9	E-Lock2	D2+	Entrada de relé da porta 2 (contacto seco)
B10		D2-	
B11	E-Lock3	D3+	Entrada de relé da porta 3 (contacto seco)
B12		D3-	

Não.	Controlador de acessos de quatro portas		
B13	E-Lock4	D4+	Entrada de relé de porta 4 portas (contacto seco)
B14		D4-	
B15	Porta Magnética Detector	S1	Porta 1 Magnética Entrada do detector
B16		GND	Aterramento
B17		S2	Porta 2 Magnética Entrada do detector
B18		S3	Porta 3 Magnética Entrada do detector
B19		GND	Aterramento
B20		S4	Porta 4 Magnética Entrada do detector
B21	Botão da porta	B1	Entrada do botão da porta da porta 1
B22		GND	Aterramento
B23		B2	Entrada do botão da porta 2
B24		B3	Entrada do botão da porta 3
B25		GND	Aterramento
B26		B4	Entrada de botão de porta 4 portas
C1	Poder	+ 12 V	Cátodo de 12 VCC
C2		GND	Aterramento
C3	Bateria	morcego+	Bateria de 12 VCC Cátodo
C4		BASTÃO-	Ânodo de bateria de 12 VCC
C5	Leitor de cartões RS485 Interface	RS485A+	Leitor de cartões RS485A+ Acesso
C6		RS485A-	Leitor de cartões RS485A- Acesso
C7		GND	Aterramento

Não.	Controlador de acessos de quatro portas		
C8		RS485B+	Leitor de cartões RS485B+
C9		RS485B-	Leitor de cartões RS485B-
C10		GND	Aterramento
C11	Controlador de acessos Interface RS485	RS485C+	Ligação ascendente RS485+Comunicação
C12		RS485C-	Uplink RS485- Comunicação
C13		GND	Aterramento
C14		RS485D+	Reservado
C15		RS 485D-	
C16		GND	
Capítulo 17	Saída de alarme	NÃO/NC1	Saída do Relé de Alarme 1 (Contacto Seco)
Capítulo 18		COM1	
Capítulo 19		NÃO/NC2	Saída de relé de alarme 2 (contacto seco)
C20		COM2	
Capítulo 21		NÃO/NC3	Saída do Relé de Alarme 3 (Contacto Seco)
C22		COM3	
Capítulo 23		NÃO/NC4	Saída de relé de alarme 4 (contacto seco)
Capítulo 24		COM4	
D1	Entrada de Evento	C8	Entrada de alarme de evento 8
D2		GND	Aterramento
D3		C7	Entrada de Alarme de Evento 7
D4		C6	Entrada de Alarme de Evento 6
D5		GND	Aterramento
D6		C5	Entrada de alarme de evento 5
D7		C4	Entrada de alarme de evento 4
D8		GND	Aterramento
D9		C3	Entrada de alarme de evento 3
D10		C2	Entrada de alarme de evento 2

Não.	Controlador de acessos de quatro portas		
D11		GND	Aterramento
D12		C1	Entrada de alarme de evento 1

Nota

- A interface de hardware de entrada de alarme está normalmente aberta por predefinição. Portanto, apenas o sinal normalmente aberto é permitido. Pode ser ligado à campainha do leitor de cartões e do controlador de acesso, e à saída do relé de alarme e ao relé da porta para abrir e fechar.
- A ligação de entrada de alarme da região de armação é apenas para a ligação de saída de relé de alarme.
- O ID do cartão RS-485 deve ser definido para 1 a 8.

Porta nº.	ID do leitor de cartões RS-485	Descrição
Porta 1	1	Entrar
	2	Saída
Porta 2	3	Entrar
	4	Saída
Porta 3	5	Entrar
	6	Saída
Porta4	7	Entrar
	8	Saída

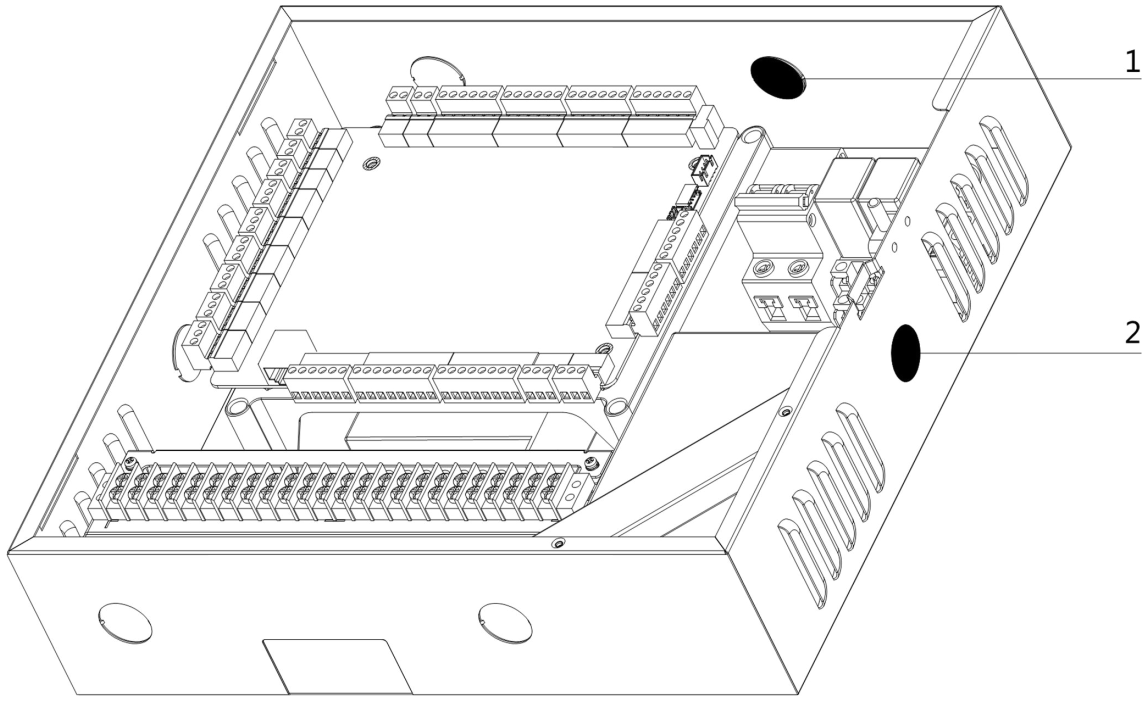
- Para o controlador de acesso de quatro portas, a relação do leitor de cartões Wiegand e da porta é a seguinte.

Porta nº.	Leitor de cartões Wiegand	Descrição
Porta 1	1	Entrar
	/	Saída
Porta 2	2	Entrar
	/	Saída
Porta 3	3	Entrar
	/	Saída
Porta 4	4	Entrar
	/	Saída

Capítulo 5 Cablagem do Terminal

Aviso

O cabo de alta tensão deve ser passado através do Furo 1 e do Furo 2. O Furo 1 e o Furo 2 devem ser instalados com um anel de borracha para evitar que o gume afiado corte o cabo e evitar o choque elétrico.



5.1 Terminal Externo

5.1.1 Descrição do Terminal Controlador de Acessos de Porta Única

Pode visualizar o diagrama de terminais do controlador de acesso de porta única.

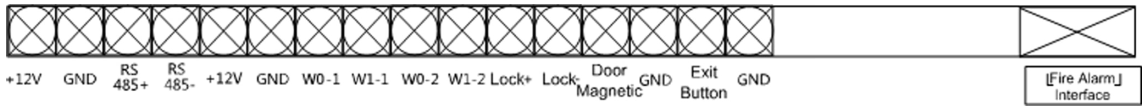


Figura 5-1 Terminais do Controlador de Acesso de Porta Única

5.1.2 Descrição do Terminal Controlador de Acessos de Duas Portas

Pode visualizar o diagrama de terminais do controlador de acesso de duas portas.

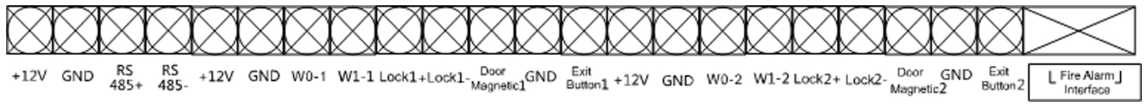


Figura 5-2 Terminais do Controlador de Acesso de Duas Portas

5.1.3 Descrição do Terminal Controlador de Acessos de Quatro Portas

Pode visualizar o diagrama de terminais do controlador de acesso de quatro portas.

Figura 5-3 Terminal Controlador de Acesso de Quatro Portas

5.2 Cablagem do leitor de cartões Wiegand

Pode visualizar o esquema de cablagem do leitor de cartões Wiegand.

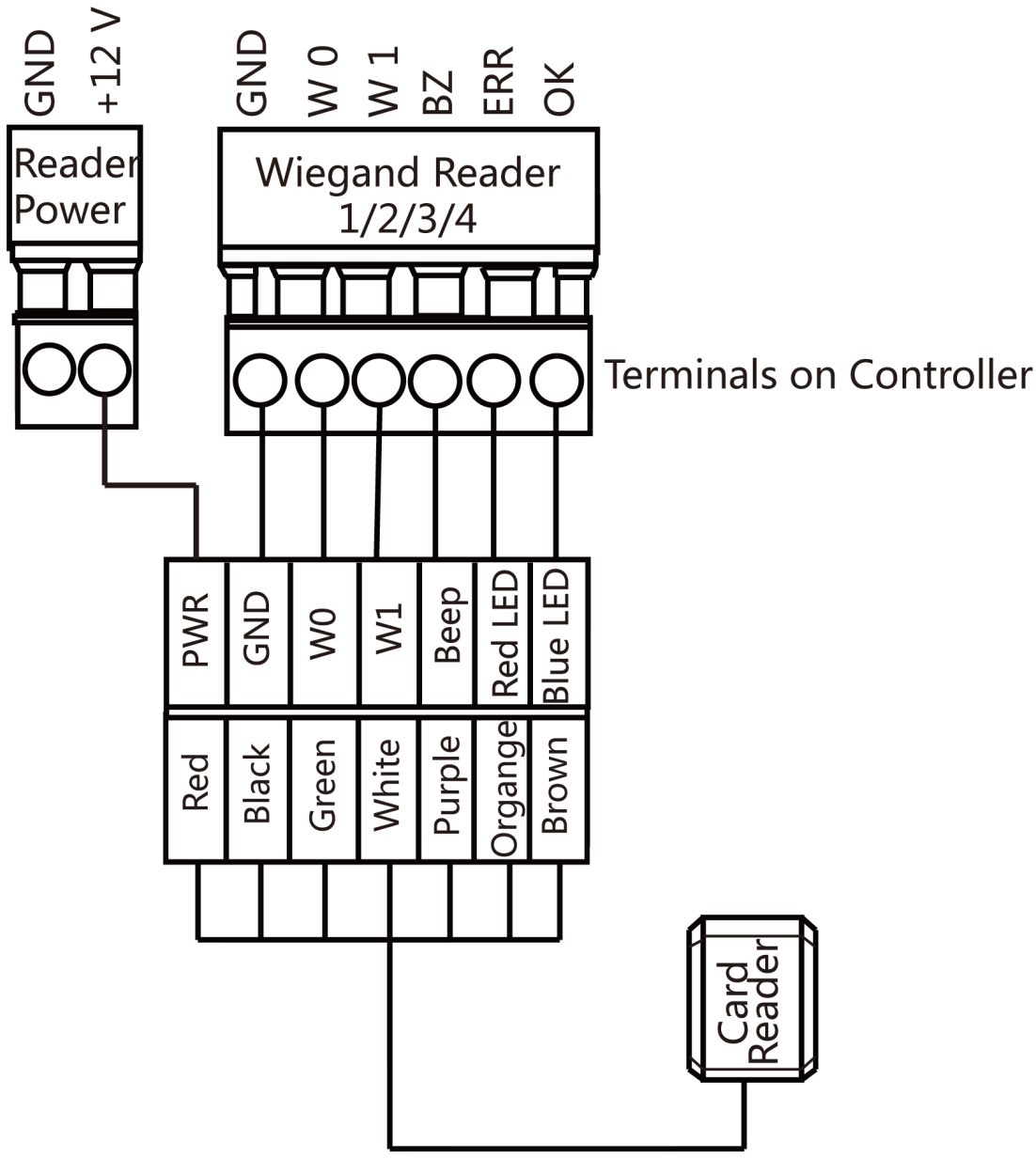


Figura 5-4 Esquema de cablagem do leitor de cartões Wiegand

Nota

Deve ligar o OK/ERR/BZ, se estiver a utilizar controlador de acesso para controlar o LED e a campainha do leitor de cartões Wiegand.

5.3 Cablagem do leitor de cartões RS-485

Pode visualizar o esquema de cablagem do leitor de cartões RS-485.

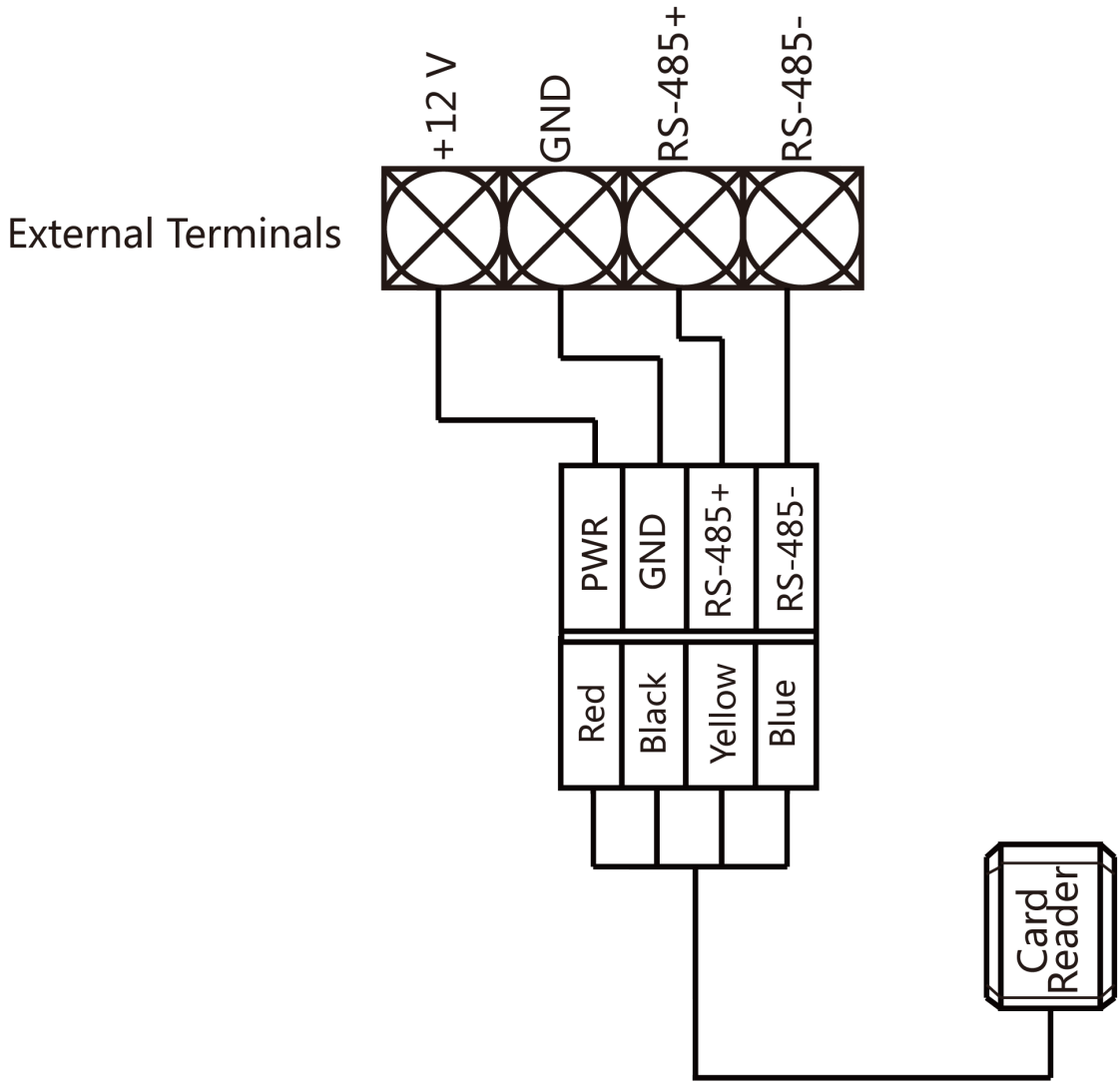


Figura 5-5 Esquema de cablagem do leitor de cartões RS-485

Nota

Se o leitor de cartões estiver instalado muito longe do controlador de acesso, pode utilizar uma fonte de alimentação externa.

5.4 Cablagem da trava catódica

Pode visualizar o esquema de cablagem da fechadura catódica.

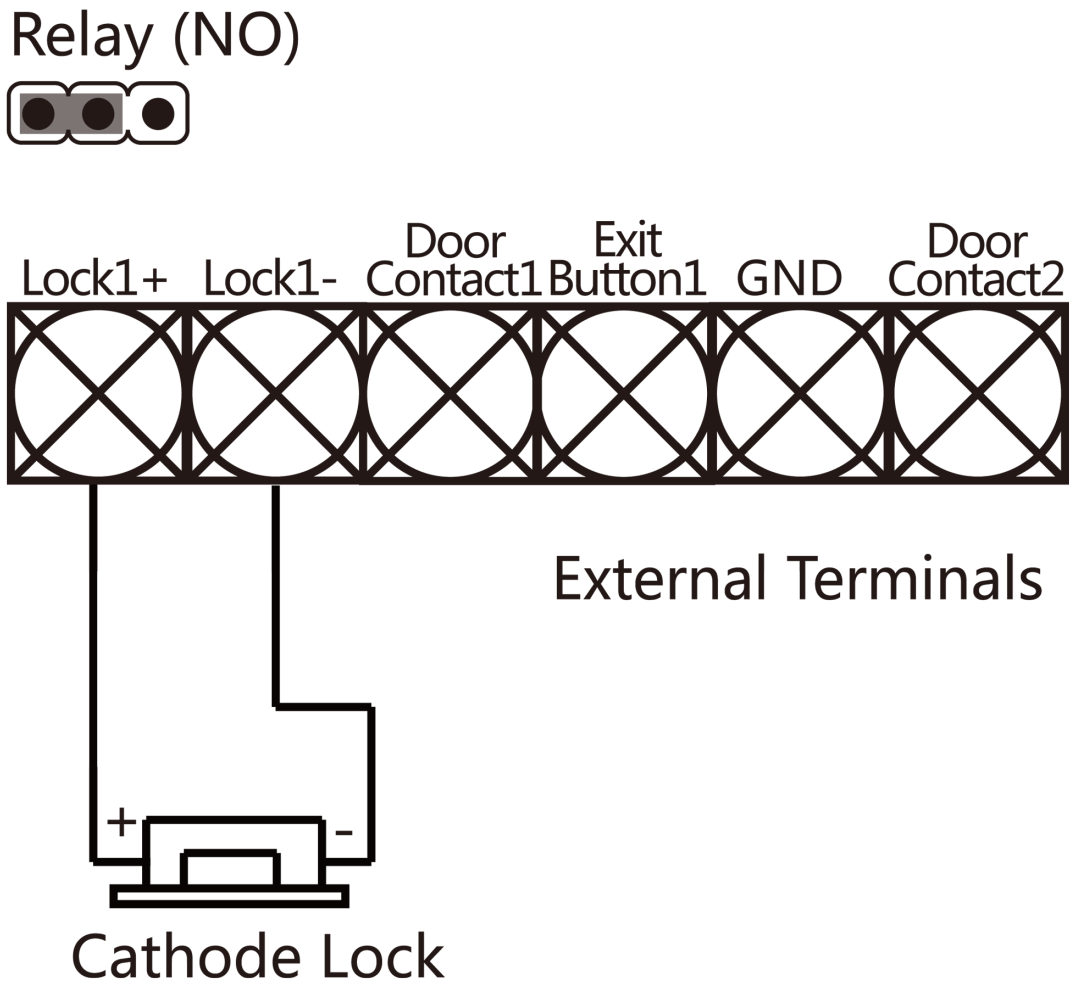


Figura 5-6 Esquema de cablagem da trava catódica

5.5 Cablagem de bloqueio do ânodo

Pode visualizar o esquema de cablagem da fechadura anódica.

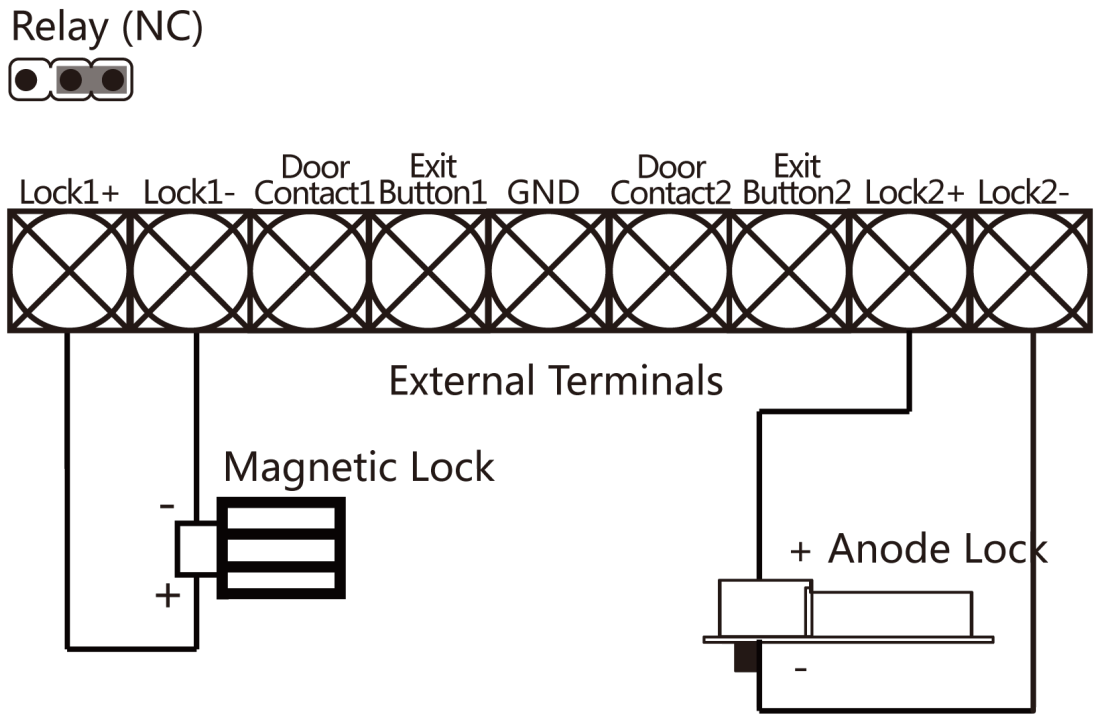


Figura 5-7 Diagrama de cablagem do fecho do ânodo

5.6 Cablagem do Dispositivo de Alarme Externo

Pode visualizar o esquema de cablagem do dispositivo de alarme externo.

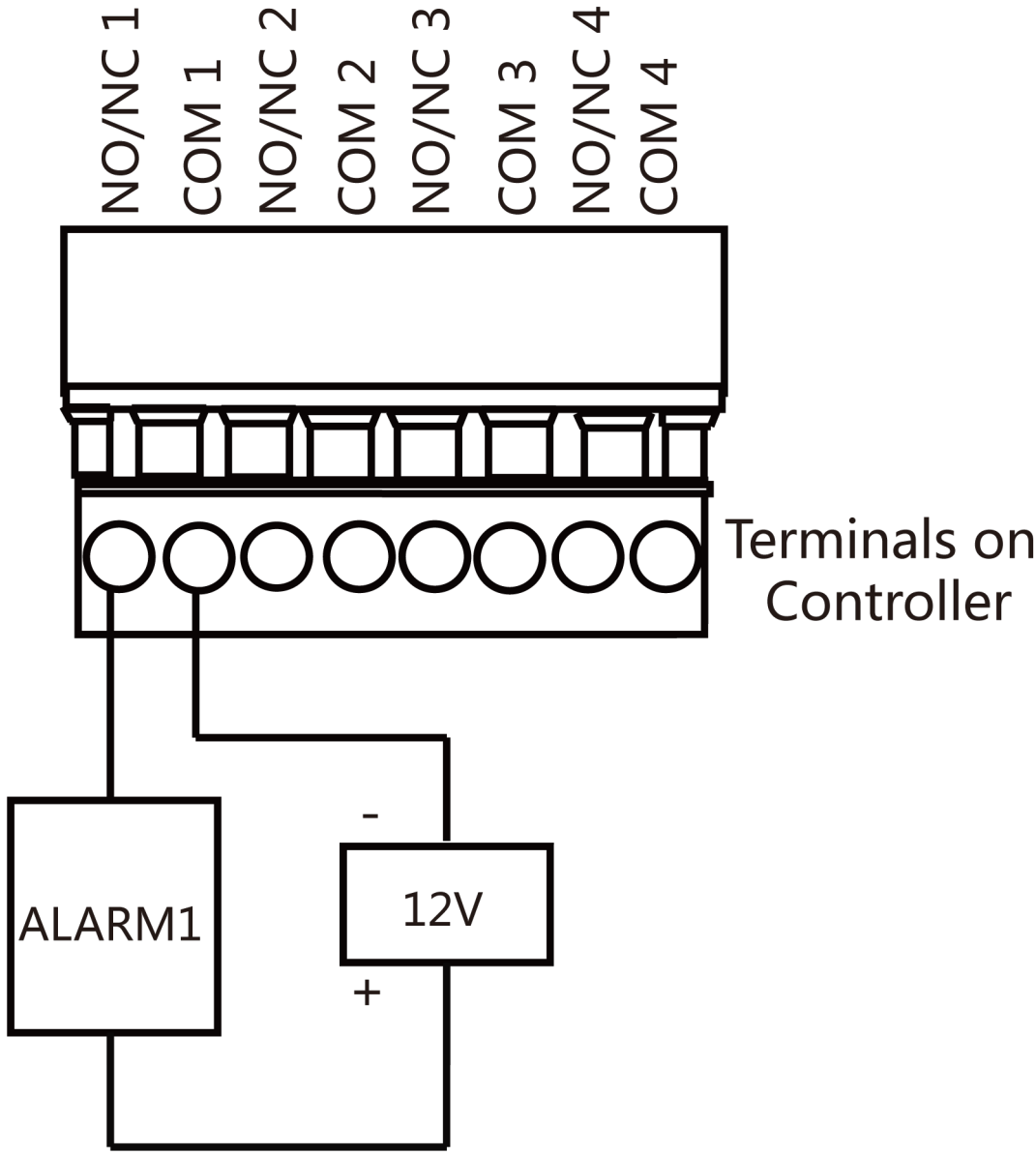


Figura 5-8 Cablagem do Dispositivo de Alarme Externo

5.7 Cablagem do botão de saída

Pode ver o esquema de cablagem do botão de saída

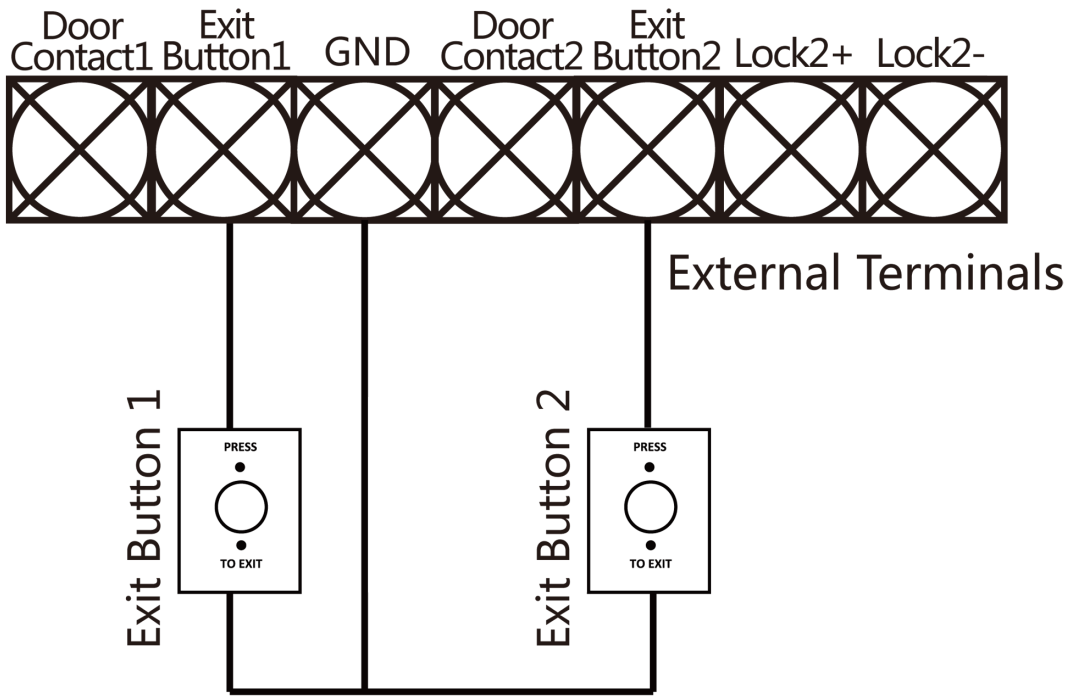


Figura 5-9 Cablagem do botão de saída

5.8 Cablagem de contacto de porta

Pode visualizar o esquema de cablagem do contacto da porta.

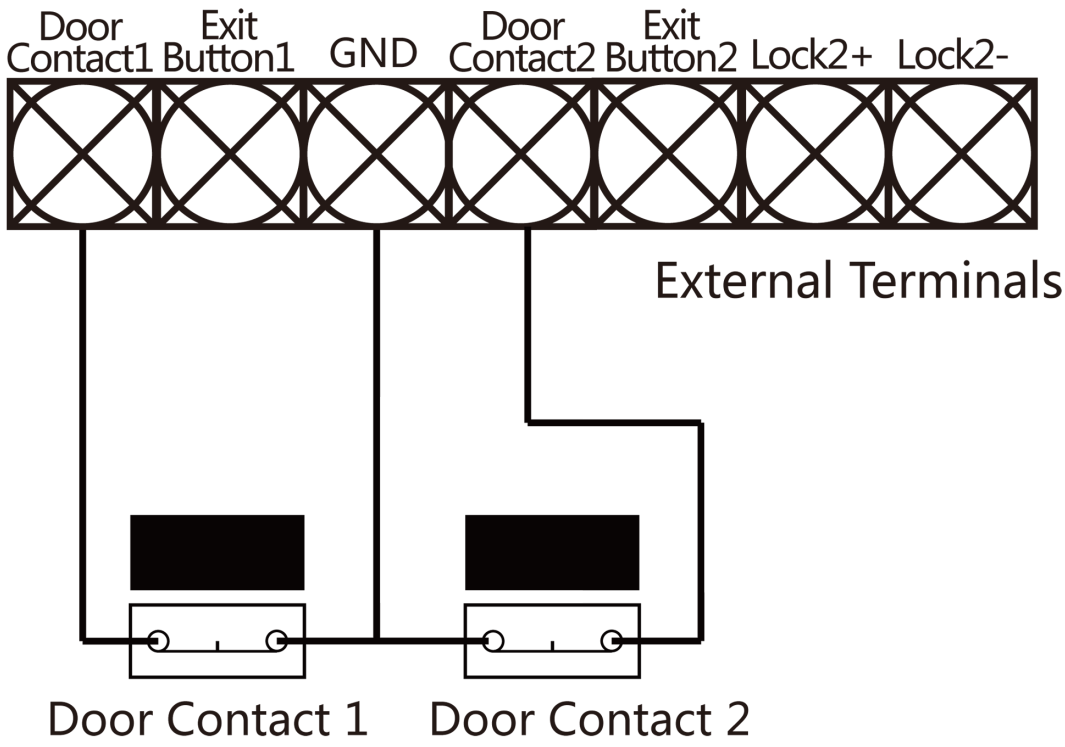


Figura 5-10 Cablagem do contacto da porta

5.9 Cablagem da Fonte de Alimentação

Pode visualizar o esquema de cablagem da fonte de alimentação.

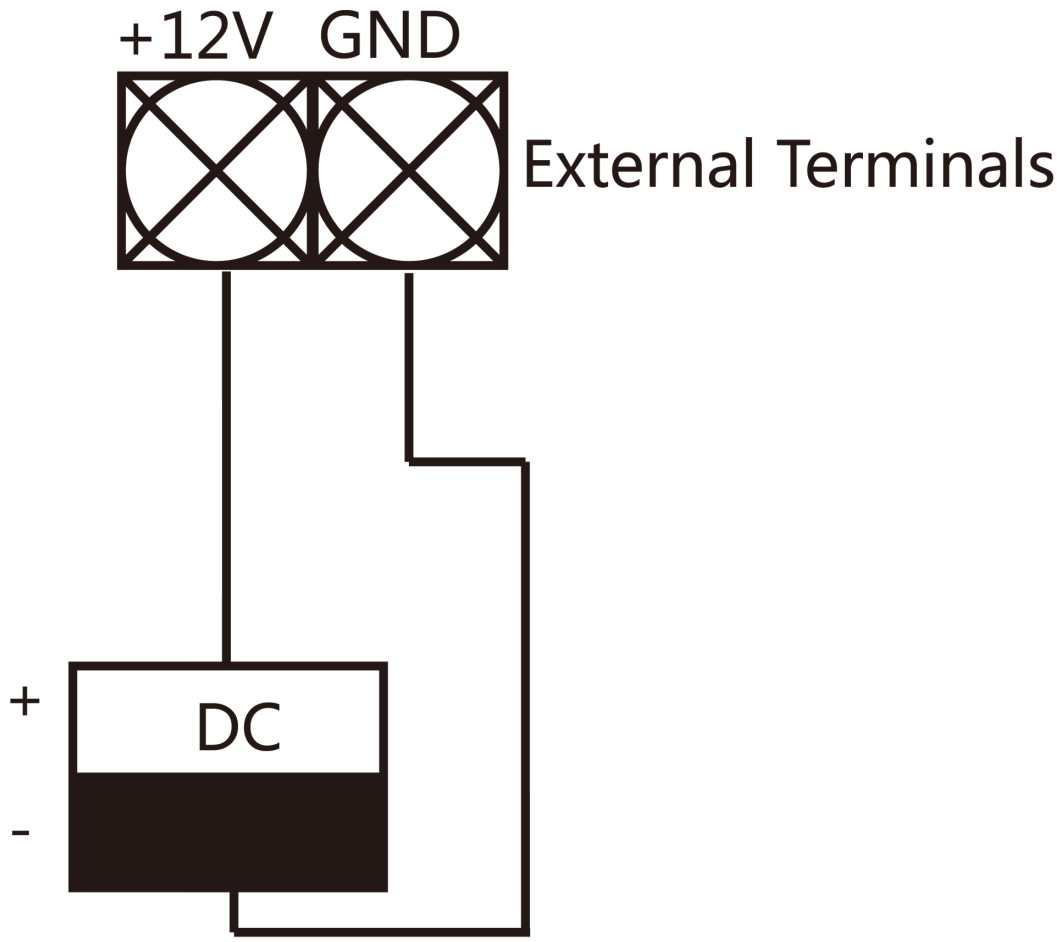


Figura 5-11 Cablagem da Fonte de Alimentação

5.10 Cablagem de Entrada da Região Armada

5.10.1 SEM Cablagem da Entrada da Região Armada

Pode visualizar a entrada da região armada da cablagem NO.

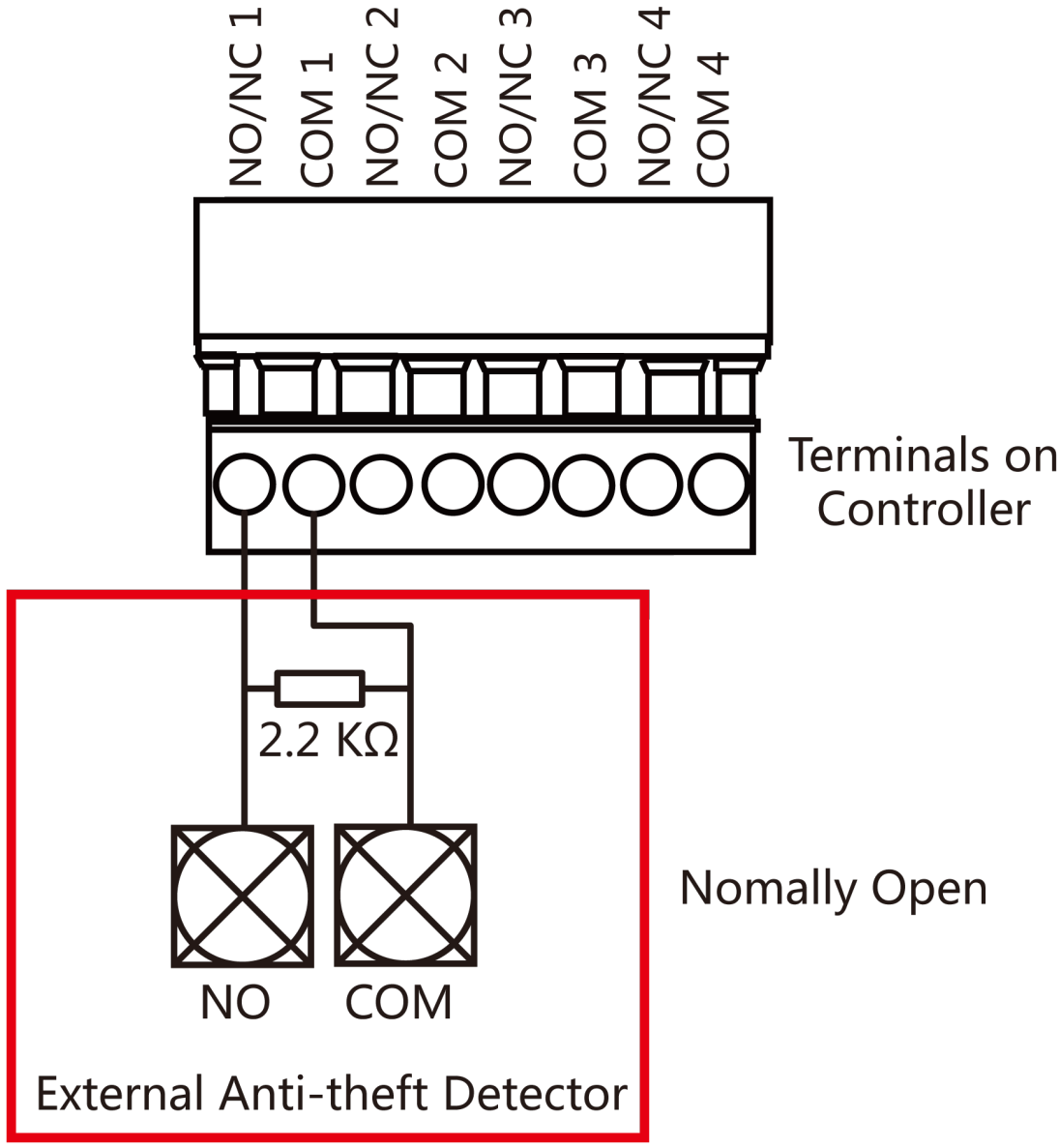


Figura 5-12 SEM Cablagem

5.10.2 Cablagem NC da Entrada da Região Armada

Pode visualizar a entrada da região armada da cablagem NC.

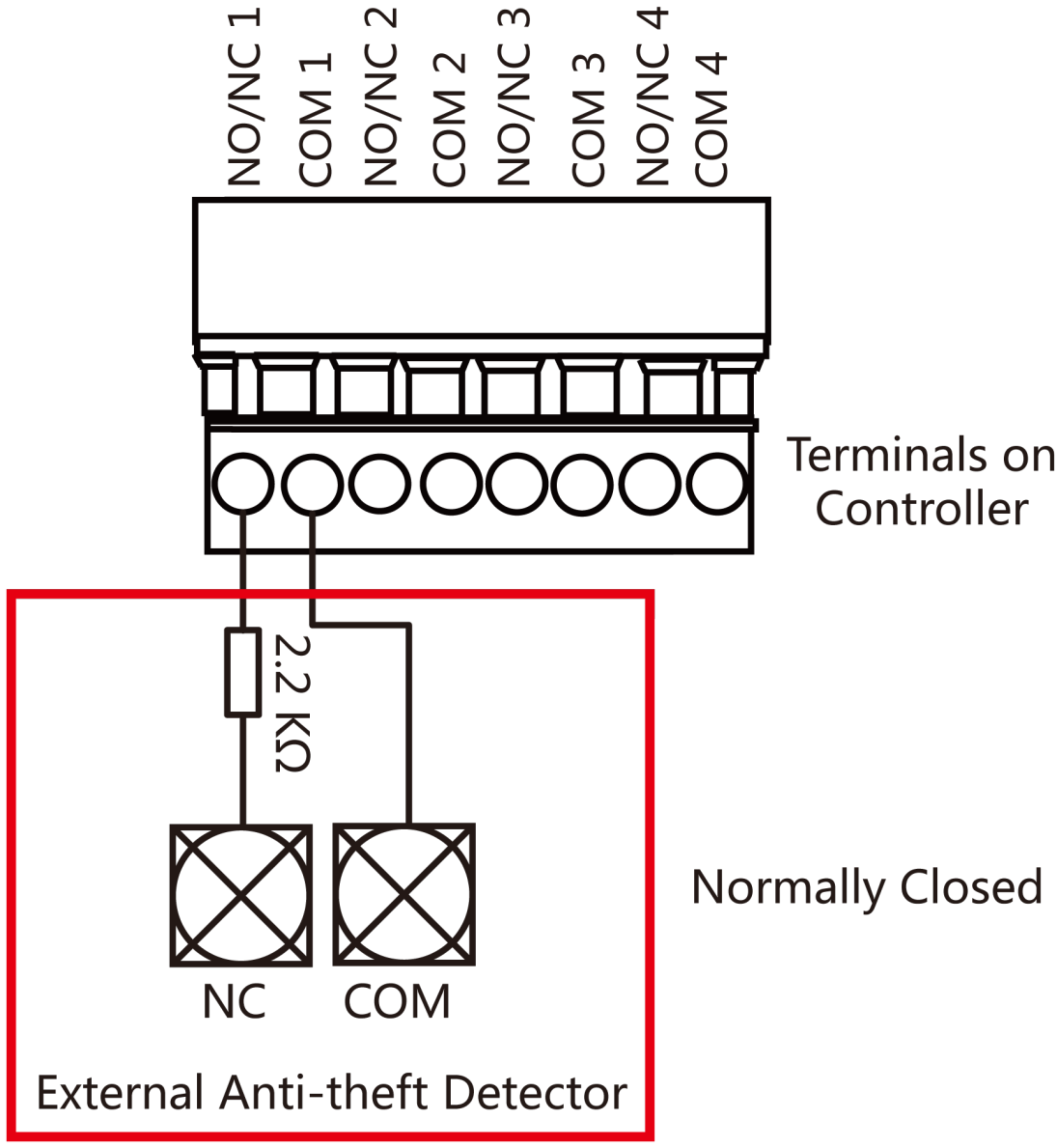


Figura 5-13 Cablagem Normalmente Fechada

5.11 Cablagem do Módulo de Alarme de Incêndio

Pode visualizar o esquema de cablagem do módulo de alarme de incêndio.

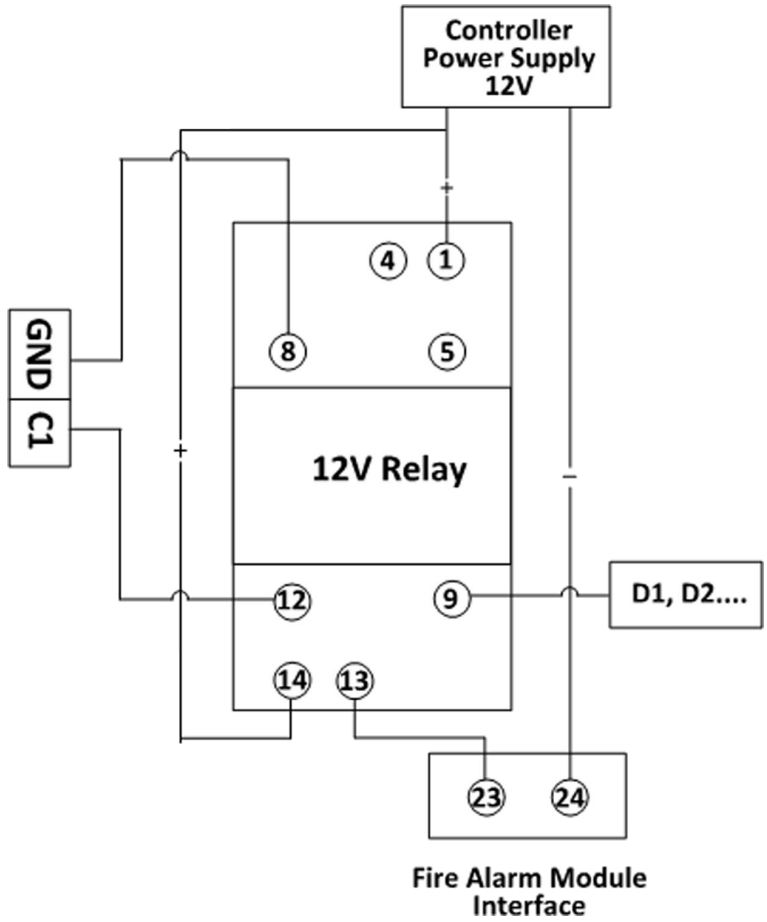


Figura 5-14 Cablagem do Módulo de Alarme de Incêndio

Capítulo 6 Configurações

6.1 Inicialização (Opção 1)

Pode inicializar o dispositivo com o jumper.

Passos

1.Retire a tampa do jumper do terminal Normal.

2.Desligue a alimentação e reinicie o controlador de acesso.

A campainha do controlador emite um sinal sonoro longo.

3.Quando o sinal sonoro parar, volte a ligar a tampa do jumper ao Normal.

4.Desligue a alimentação e reinicie o controlador de acesso.

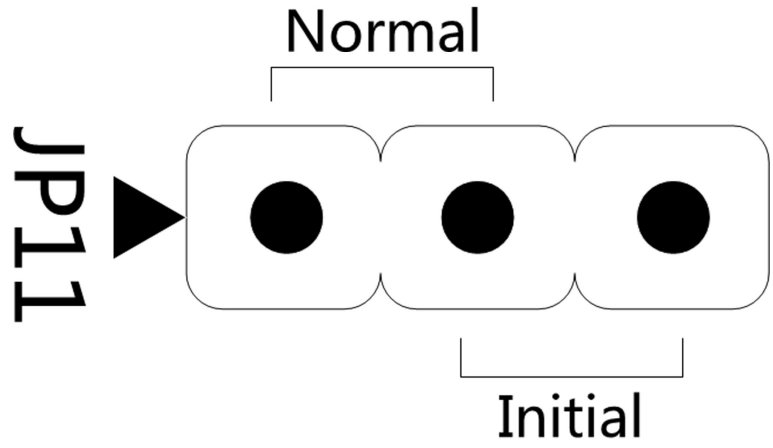


Figura 6-1 Jumper de arranque

Nota

A inicialização do dispositivo irá restaurar todos os parâmetros para as definições padrão e todos os registos de eventos do dispositivo serão eliminados.

6.2 Inicialização (Opção 2)

Pode inicializar o dispositivo com o jumper.

Passos

1.Mova a tampa do jumper de Normal para Inicial.

2.Desligue a alimentação e reinicie o controlador de acesso.

A campainha do controlador emite um sinal sonoro longo.

3.Quando o sinal sonoro parar, mova a tampa do jumper de volta para Normal.

4.Desligue a alimentação e reinicie o controlador de acesso.

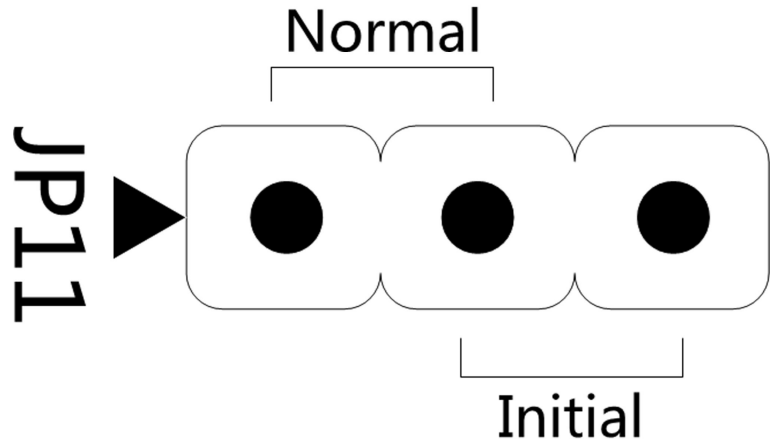


Figura 6-2 Jumper de arranque

Nota

A inicialização do dispositivo irá restaurar todos os parâmetros para as definições padrão e todos os registos de eventos do dispositivo serão eliminados.

6.3 Definições de saída de relé NO/NC

6.3.1 Bloquear as definições de saída de relé

Pode visualizar o estado NO/NC do relé de bloqueio.

Relé de bloqueio SEM estado

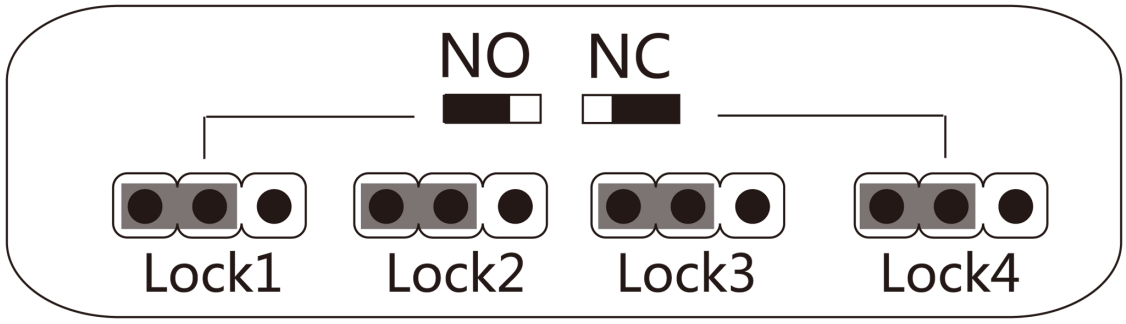


Figura 6-3 Estado NÃO

Estado NC do relé de bloqueio

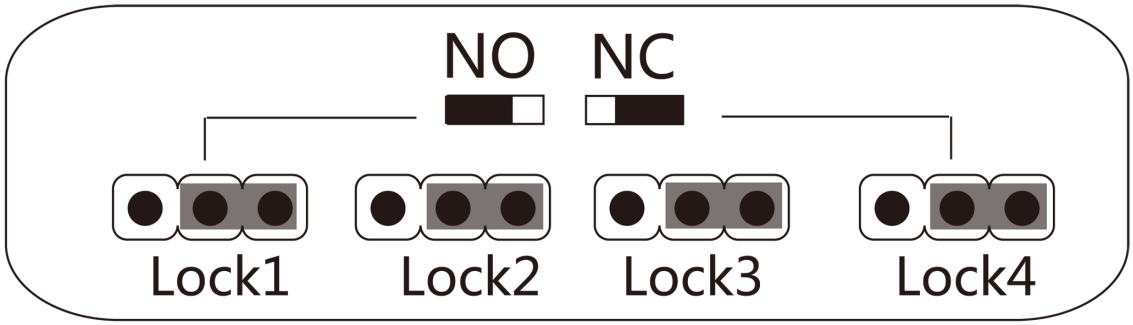


Figura 6-4 Estado NC

6.3.2 Configurações de saída do relé de alarme

Pode visualizar o estado NO/NC do relé de alarme.

Saída de relé de alarme SEM estado

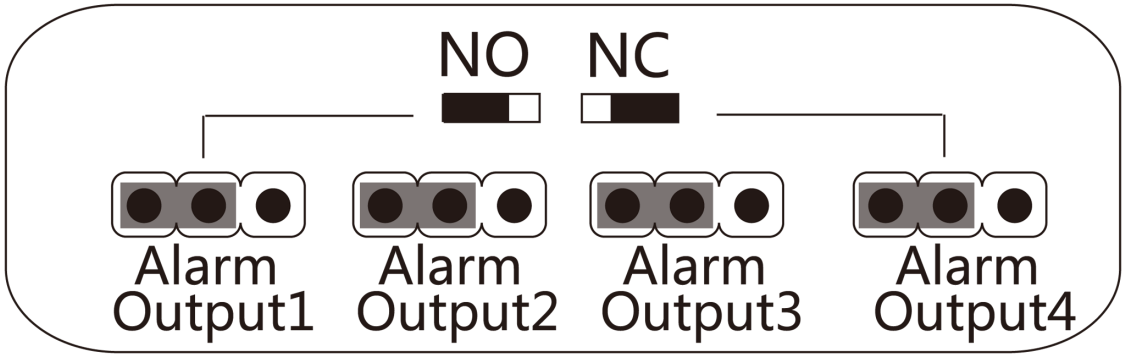


Figura 6-5 Estado NÃO

Estado NC da saída de relé de alarme

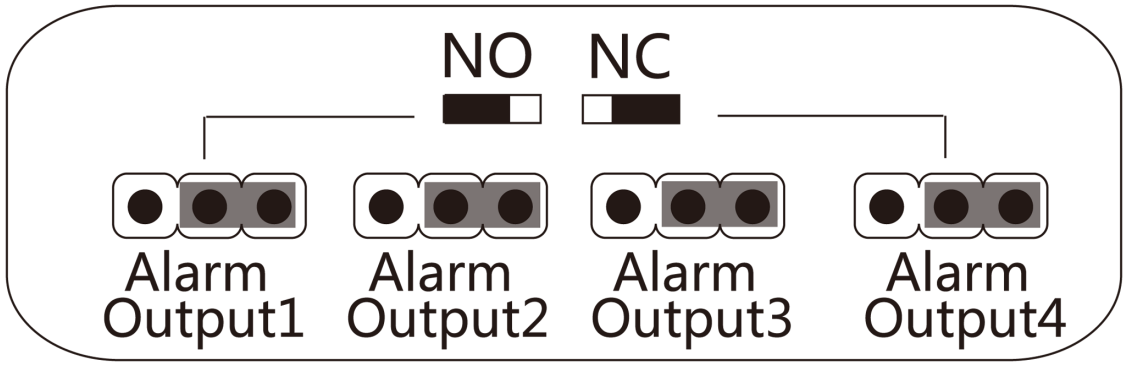


Figura 6-6 Estado NC

Capítulo 7 Ativação

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, da ferramenta SADP e do software cliente é suportada.

Os valores padrão do dispositivo são os seguintes:

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

7.1 Ativar via SADP

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

Antes de começar

- 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.

Os passos seguintes mostram como ativar um dispositivo e modificar o seu endereço IP. Para ativação em lote e modificação de endereços IP, consulte*Manual do utilizador do SADP*para obter detalhes.

Passos

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

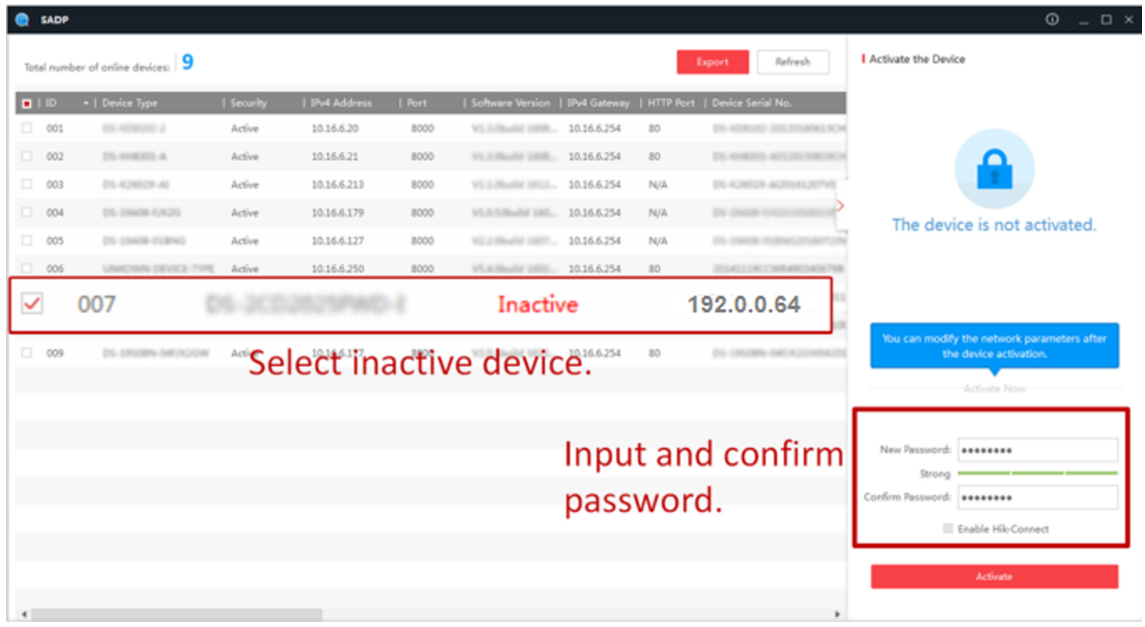
2.Encontre e selecione o seu dispositivo na lista de dispositivos online.

3.Introduza a nova palavra-passe (password de administrador) e confirme a palavra-passe.

Cuidado

PASSWORD FORTE RECOMENDADA - É altamente recomendável que crie uma password forte à sua escolha (utilizando um mínimo de 8 caracteres, incluindo letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. E recomendamos que redefina a sua palavra-passe regularmente, especialmente no sistema de alta segurança, redefinir a palavra-passe mensalmente ou semanalmente pode proteger melhor o seu produto.

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



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

5.Modifique o endereço IP do dispositivo.

1) Selecione o dispositivo.

2) Altere o endereço IP do dispositivo para a mesma sub-rede do seu computador, modificando o endereço IP manualmente ou verificando**Ativar DHCP**.

3) Introduza a palavra-passe do administrador e clique em**Modificar**para ativar a modificação do seu endereço IP.

7.2 Ativar dispositivo através de software cliente

Para alguns dispositivos, é necessário criar uma palavra-passe para os ativar antes que possam ser adicionados ao software e funcionar corretamente.

Passos

Nota

Esta função deve ser suportada pelo dispositivo.

1.Entre na página Gestão de dispositivos.

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

3.Clique**Dispositivo on-line**para mostrar a área do dispositivo online.

Os dispositivos online pesquisados são apresentados na lista.

4.Verifique o estado do dispositivo (apresentado em**Nível de segurança**coluna) e selecione um dispositivo inativo.

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

6.Crie uma palavra-passe no campo da palavra-passe e confirme a palavra-passe.

Cuidado

A força da palavra-passe do dispositivo pode ser verificada automaticamente. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your produto. E recomendamos que redefina a sua palavra-passe regularmente, principalmente no sistema de alta segurança, redefinir a palavra-passe mensalmente ou semanalmente pode proteger melhor o seu produto.

A configuração adequada de todas as palavras-passe e outras definições de segurança é da responsabilidade do instalador e/ou utilizador final.

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

Capítulo 8 Configuração do software cliente

8.1 Operação em Software Cliente

O módulo de Controlo de Acessos oferece múltiplas funcionalidades, incluindo gestão de pessoas e cartões, configuração de permissões e outras funções avançadas.

Nota

Para o utilizador com permissões do módulo de controlo de acesso, o utilizador pode entrar no módulo de Controlo de Acesso e definir as definições de controlo de acesso. Para definir a permissão do utilizador do módulo de controlo de acesso, consulte *Gestão de contas* em *Manual do utilizador do software cliente iVMS-4200*.

8.1.1 Adicionar dispositivo

Depois de executar o cliente, os dispositivos devem ser adicionados ao cliente para configuração e gestão remotas.

Depois de adicionar dispositivos, pode selecionar um dispositivo e clicar **Configuração remota** para configurar outros parâmetros do dispositivo selecionado, se necessário. Você também pode

Nota

Para alguns modelos de dispositivos, pode abrir a sua janela de configuração de parâmetros gerais ou avançados. Para abrir a janela de configuração remota original, prima **CTRL** e clique **Configuração remota**.

Depois de adicionar dispositivos de controlo de acesso, pode selecionar o dispositivo de controlo de acesso na lista e clicar **Estado do dispositivo** para visualizar o estado do dispositivo.

Adicionar dispositivo online

Os dispositivos online ativos na mesma sub-rede local do software cliente serão apresentados no **Dispositivo on-line** área. Pode clicar **Atualizar a cada 60 anos** para atualizar as informações dos dispositivos online.

Adicionar um único dispositivo online

Pode adicionar um único dispositivo online ao software cliente. Execute esta tarefa

para adicionar um único dispositivo online ao software cliente.

Passos

1. Entre no módulo Gestão de dispositivos.

2.Clique**Dispositivo**separador e selecione**Dispositivo Hikvision**como o tipo de dispositivo para exibir o**Dispositivo on-line** área.

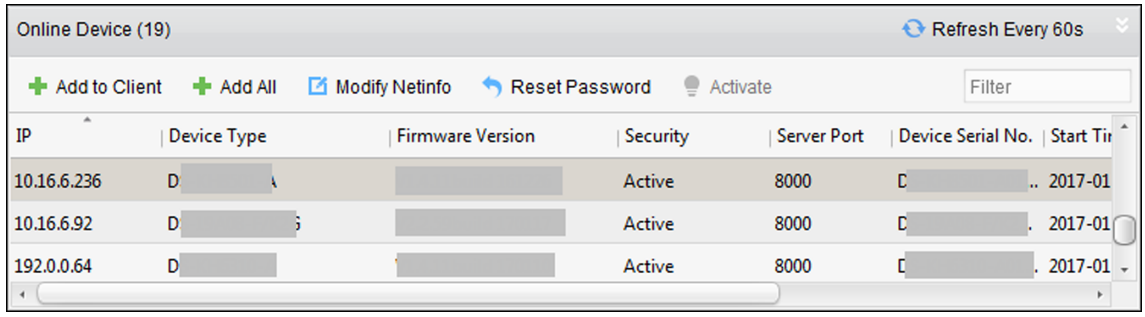


Figura 8-1 Dispositivo On-line

3.Selecione um dispositivo online no**Dispositivo on-line**área.

Nota

Para o dispositivo inativo, precisa de criar uma palavra-passe antes de poder adicionar o dispositivo corretamente. Para obter os passos detalhados, consulte***Ativação*** .

4.Clique**Adicionar ao cliente**para abrir a janela de adição de dispositivos.

5.Introduza as informações necessárias.

Morada

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

Porto

O valor predefinido é 8.000. **Nome**

de utilizador

Por predefinição, o nome de utilizador é admin.

Palavra-passe

Introduza a palavra-passe do dispositivo.

Cuidado

A força da palavra-passe do dispositivo pode ser verificada automaticamente. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your produto. E recomendamos que redefina a sua palavra-passe regularmente, principalmente no sistema de alta segurança, redefinir a palavra-passe mensalmente ou semanalmente pode proteger melhor o seu produto.

A configuração adequada de todas as palavras-passe e outras definições de segurança é da responsabilidade do instalador e/ou utilizador final.

6.º Opcional: Verificação**Sincronizar hora do dispositivo**para sincronizar a hora do dispositivo com o PC que executa o cliente após a adição do dispositivo ao cliente.

7.º Opcional: Verificação**Exportar para grupo**para criar um grupo pelo nome do dispositivo.

Nota

Pode importar todos os canais do dispositivo para o grupo correspondente por predefinição.

8.º Opcional: Adicione os dispositivos offline.

1) Verifique**Adicionar dispositivo offline**.

2) Introduza as informações necessárias, incluindo o número do canal do dispositivo e o número da entrada de alarme.

3) Clique**Adicionar**.

Quando o dispositivo offline ficar online, o software irá ligá-lo automaticamente.

9.Clique**Adicionar**para adicionar o dispositivo.

Adicionar vários dispositivos online

Pode adicionar vários dispositivos online ao software cliente.

Execute esta tarefa se precisar de adicionar vários dispositivos online ao software cliente.

Passos

1.Entre no módulo Gestão de dispositivos.

2.Clique**Dispositivo**separador e selecione**Dispositivo Hikvision**como o tipo de dispositivo para exibir o**Dispositivo on-line** área.

3.Clique e mantenha**Ctrl**tecla para selecionar vários dispositivos.

Nota

Para o dispositivo inativo, precisa de criar uma palavra-passe antes de poder adicionar o dispositivo corretamente. Para obter os passos detalhados, consulte***Ativação*** .

4.Clique**Adicionar ao cliente**para abrir a janela de adição de dispositivos.

5.Introduza as informações necessárias.

Nome de utilizador

Por predefinição, o nome de utilizador é admin.

Palavra-passe

Introduza a palavra-passe do dispositivo.

Cuidado

A força da palavra-passe do dispositivo pode ser verificada automaticamente. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your produto. E recomendamos que redefina a sua palavra-passe regularmente, principalmente no sistema de alta segurança, redefinir a palavra-passe mensalmente ou semanalmente pode proteger melhor o seu produto.

A configuração adequada de todas as palavras-passe e outras definições de segurança é da responsabilidade do instalador e/ou utilizador final.

6.º Opcional: Verificação**Sincronizar hora do dispositivo**para sincronizar a hora dos dispositivos com o PC que executa o cliente após a adição dos dispositivos ao cliente.

7.º Opcional: Verificação**Exportar para grupo**para criar um grupo pelo nome do dispositivo.

Nota

Pode importar todos os canais do dispositivo para o grupo correspondente por predefinição.

8.Clique**Adicionar**para adicionar os dispositivos.

Adicionar todos os dispositivos online

Pode adicionar todos os dispositivos online ao software cliente.

Execute esta tarefa se necessitar de adicionar todos os dispositivos online ao software cliente.

Passos

1.Entre na página Gestão de dispositivos.

2.Clique**Dispositivo**separador e selecione**Dispositivo Hikvision**como o tipo de dispositivo para exibir o**Dispositivo on-line** área.

3.Clique**Adicionar tudo**para abrir a janela de adição de dispositivos.

Nota

Para o dispositivo inativo, precisa de criar uma palavra-passe antes de poder adicionar o dispositivo corretamente. Para obter os passos detalhados, consulte***Ativação*** .

4.Introduza o nome de utilizador e a palavra-passe. **Nome de utilizador**

Por predefinição, o nome de utilizador é admin.

Palavra-passe

Introduza a palavra-passe do dispositivo.

Cuidado

A força da palavra-passe do dispositivo pode ser verificada automaticamente. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your produto. E recomendamos que redefina a sua palavra-passe regularmente, principalmente no sistema de alta segurança, redefinir a palavra-passe mensalmente ou semanalmente pode proteger melhor o seu produto.

A configuração adequada de todas as palavras-passe e outras definições de segurança é da responsabilidade do instalador e/ou utilizador final.

5.º Opcional: Verificação**Sincronizar hora do dispositivo**para sincronizar a hora dos dispositivos com o PC que executa o cliente após a adição dos dispositivos ao cliente.

6.º Opcional: Verificação**Exportar para grupo**para criar um grupo pelo nome do dispositivo.

Nota

Pode importar todos os canais do dispositivo para o grupo correspondente por predefinição.

7.Clique**Adicionar**para adicionar os dispositivos.

Adicionar dispositivo por endereço IP ou nome de domínio

Pode adicionar dispositivos por endereço IP ou nome de domínio.

Execute esta tarefa se necessitar de adicionar um dispositivo por endereço IP ou nome de domínio.

Passos

1.Abra o módulo Gestão de dispositivos.

2.Clique**Dispositivo**separador e selecione**Dispositivo Hikvision**como o tipo de dispositivo.

3.Clique**Adicionar**para abrir a janela Adicionar.

4.Selecionar**IP/Domínio**como o modo de adição.

5.Introduza as informações necessárias, incluindo o apelido, o endereço IP, o número da porta, o nome de utilizador e a palavra-passe.

Morada

Introduza os endereços IP do dispositivo ou o nome de domínio.

Porto

Introduza o número da porta do dispositivo.

Nome de utilizador

Introduza o nome de utilizador do dispositivo. Por predefinição, o nome de utilizador é admin.

Palavra-passe

Introduza a palavra-passe do dispositivo.

Cuidado

A força da palavra-passe do dispositivo pode ser verificada automaticamente. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your produto. E recomendamos que redefina a sua palavra-passe regularmente, principalmente no sistema de alta segurança, redefinir a palavra-passe mensalmente ou semanalmente pode proteger melhor o seu produto.

A configuração adequada de todas as palavras-passe e outras definições de segurança é da responsabilidade do instalador e/ou utilizador final.

6.º Opcional: Verificação**Sincronizar hora do dispositivo**para sincronizar a hora do dispositivo com o PC que executa o cliente após a adição do dispositivo ao cliente.

7.º Opcional: Verificação**Exportar para grupo**para criar um grupo pelo nome do dispositivo.

Nota

Pode importar todos os canais do dispositivo para o grupo correspondente por predefinição.

8.º Opcional: Adicione os dispositivos offline.

1) Verifique**Adicionar dispositivo offline**.

2) Introduza as informações necessárias, incluindo o número do canal do dispositivo e o número da entrada de alarme.

3) Clique**Adicionar**.

Quando o dispositivo offline ficar online, o software irá ligá-lo automaticamente.

9.Clique**Adicionar**para adicionar o dispositivo.

Adicionar dispositivos por segmento IP

Se pretender adicionar dispositivos cujos endereços IP se encontrem dentro de um segmento IP, pode especificar o endereço IP inicial e o endereço IP final, o nome de utilizador, a palavra-passe e outros parâmetros para os adicionar.

Execute esta tarefa quando necessitar de adicionar dispositivos ao cliente por segmento IP.

Passos

1.Entre no módulo Gestão de dispositivos.

2.Clique**Dispositivo**separador e selecione**Dispositivo Hikvision**como o tipo de dispositivo.

3.Clique**Adicionar**para abrir a janela Adicionar.

4.Selecionar**Segmento IP**como o modo de adição.

5.Introduza as informações necessárias.

Iniciar IP

Introduza um endereço IP inicial.

IP final

Introduza um endereço IP final no mesmo segmento de rede do IP inicial. **Porto**

Introduza o número da porta do dispositivo. **Nome de utilizador**

Por predefinição, o nome de utilizador é admin.

Palavra-passe

Introduza a palavra-passe do dispositivo.

Cuidado

A força da palavra-passe do dispositivo pode ser verificada automaticamente. É altamente recomendável que altere a palavra-passe da sua preferência (utilizando um mínimo de 8 caracteres, incluindo pelo menos três tipos das seguintes categorias: letras maiúsculas, letras minúsculas, números,

e caracteres especiais) para aumentar a segurança do seu produto. E recomendamos que redefina a sua palavra-passe regularmente, especialmente no sistema de alta segurança, redefinir a palavra-passe mensalmente ou semanalmente pode proteger melhor o seu produto.

A configuração adequada de todas as palavras-passe e outras definições de segurança é da responsabilidade do instalador e/ou utilizador final.

6.º Opcional: Verificação**Sincronizar hora do dispositivo**para sincronizar a hora do dispositivo com o PC que executa o cliente após a adição do dispositivo ao cliente.

7.º Opcional: Verificação**Exportar para grupo**para criar um grupo pelo nome do dispositivo.

Nota

Pode importar todos os canais do dispositivo para o grupo correspondente por predefinição.

8.º Opcional: Adicione dispositivos offline ao cliente.

1) Verifique**Adicionar dispositivo offline**.

2) Introduza as informações necessárias, incluindo o número do canal do dispositivo e o número da entrada de alarme.

3) Clique**Adicionar**.

Quando o dispositivo offline ficar online, o software irá ligá-lo automaticamente.

9.Clique**Adicionar**para adicionar o dispositivo.

Adicionar dispositivo por conta EHome

Pode adicionar um dispositivo de controlo de acesso ligado através do protocolo EHome, inserindo a conta EHome.

Antes de começar

Defina primeiro o parâmetro do centro de rede. Para obter detalhes, consulte***Definir parâmetros de rede*** .

Execute esta tarefa se necessitar de adicionar dispositivos por conta EHome.

Passos

1.Entre no módulo Gestão de dispositivos.

2.Clique**Dispositivo**separador e selecione**Dispositivo Hikvision**como o tipo de dispositivo.

3.Clique**Adicionar**para abrir a janela Adicionar.

4.Selecionar**ECasa**como o modo de adição.

5.Introduza as informações necessárias.

Conta

Introduza o nome da conta registada no protocolo EHome.

6.º Opcional: Verificação**Sincronizar hora do dispositivo**para sincronizar a hora do dispositivo com o PC que executa o cliente após a adição do dispositivo ao cliente.

7.º Opcional: Verificação**Exportar para grupo**para criar um grupo pelo nome do dispositivo.

8.º Opcional: Adicione os dispositivos offline.

1) Verifique**Adicionar dispositivo offline**.

2) Introduza as informações necessárias, incluindo o número do canal do dispositivo e o número da entrada de alarme.

3) Clique**Adicionar**.

Nota

Quando o dispositivo offline ficar online, o software irá ligá-lo automaticamente.

9.Clique**Adicionar**para adicionar o dispositivo.

Importar dispositivos em batch

Os dispositivos podem ser adicionados ao software em lote, inserindo as informações do dispositivo no ficheiro CSV predefinido.

Execute esta tarefa para importar dispositivos em batch.

Passos

1.Entre na página Gestão de dispositivos

2.Clique**Dispositivo → Dispositivo Hikvision → Adicionar**para abrir a janela de adição de dispositivos.

3.Selecionar**Importação em lote**como o modo de adição.

4.Clique**Exportar modelo**e guarde o modelo predefinido (ficheiro CSV) no seu PC.

5.Abra o ficheiro do modelo exportado e introduza as informações necessárias dos dispositivos a adicionar na coluna correspondente.

Modo de adição

Pode inserir***0***,***2***,***3***,***4***,***5***, ou***6***que indicou diferentes modos de adição.***0***indica que o dispositivo é adicionado por endereço IP ou nome de domínio;***2***indica que o dispositivo foi adicionado através do servidor IP;***3***indica que o dispositivo foi adicionado via HiDDNS;***4***indica que o dispositivo foi adicionado através do protocolo EHome;***5***indica que o dispositivo é adicionado pela porta série;***6***indica que o dispositivo foi adicionado através do Hik-Connect.

Morada

Edite o endereço do dispositivo. Se definir***0***como modo de adição, deve introduzir o endereço IP ou o nome de domínio do dispositivo; se definir***2***como modo de adição, deve ser introduzido o endereço IP do PC que instala o IP Server; se definir***3***como modo de adição, deve introduzir ***www.hik-online.com***.

Porto

Introduza o número da porta do dispositivo.

Informações do dispositivo

Se definir***0***tal como o modo de adição, este campo não é de preenchimento obrigatório; se definir***2***como modo de adição, introduza o ID do dispositivo registado no Servidor IP; se definir***3***como modo de adição, introduza o nome de domínio do dispositivo registado no servidor HiDDNS; se definir***4***como modo de adição, introduza a conta EHome; se definir***6***como modo de adição, introduza o número de série do dispositivo.

Nome de utilizador

Introduza o nome de utilizador do dispositivo. Por predefinição, o nome de utilizador é admin.

Palavra-passe

Introduza a palavra-passe do dispositivo.

Cuidado

A força da palavra-passe do dispositivo pode ser verificada automaticamente. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your produto. E recomendamos que redefina a sua palavra-passe regularmente, principalmente no sistema de alta segurança, redefinir a palavra-passe mensalmente ou semanalmente pode proteger melhor o seu produto.

A configuração adequada de todas as palavras-passe e outras definições de segurança é da responsabilidade do instalador e/ou utilizador final.

Adicionar dispositivo offline

Pode inserir ***1*** para permitir a adição do dispositivo offline e, em seguida, o software irá ligá-lo automaticamente quando o dispositivo offline ficar online. ***0*** indica a desativação desta função.

Exportar para grupo

Pode inserir ***1*** para criar um grupo pelo nome do dispositivo (nickname). Todos os canais do dispositivo serão importados para o grupo correspondente por predefinição. ***0*** indica a desativação desta função.

Número do canal

Se definir ***1*** para Adicionar dispositivo offline, introduza o número do canal do dispositivo. Se definir ***0*** para Adicionar dispositivo offline, este campo não é obrigatório.

Número de entrada de alarme

Se definir ***1*** para Adicionar dispositivo offline, introduza o número de entrada de alarme do dispositivo. Se definir ***0*** para Adicionar dispositivo offline, este campo não é obrigatório.

Número da porta série

Se definir ***5*** como modo de adição, introduza o número da porta série para o dispositivo de controlo de acesso.

Taxa de transmissão

Se definir ***5*** como modo de adição, introduza a taxa de transmissão do dispositivo de controlo de acesso.

MERGULHO

Se definir ***5*** como modo de adição, introduza o endereço DIP do dispositivo de controlo de acesso.

Conta Hik-Connect

Se definir ***6*** como modo de adição, introduza a conta Hik-Connect.

Palavra-passe Hik-Connect

Se definir ***6*** como modo de adição, introduza a palavra-passe da conta Hik-Connect.

6. Clique e selecione o ficheiro do modelo.

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

8.1.2 Selecionar cenário de aplicação

Ao entrar pela primeira vez no módulo de Controlo de Acessos, é necessário selecionar o cenário de aplicação do controlo de acessos como residencial ou não residencial de acordo com as necessidades reais.

Execute esta tarefa se necessitar de selecionar o cenário de aplicação do controlo de acessos quando entrar no módulo de Controlo de Acessos pela primeira vez.

Passos

Nota

Depois de a cena estar configurada, não poderá alterá-la.

1.Entre no módulo de controlo de acessos. A

janela Selecionar cena será apresentada.

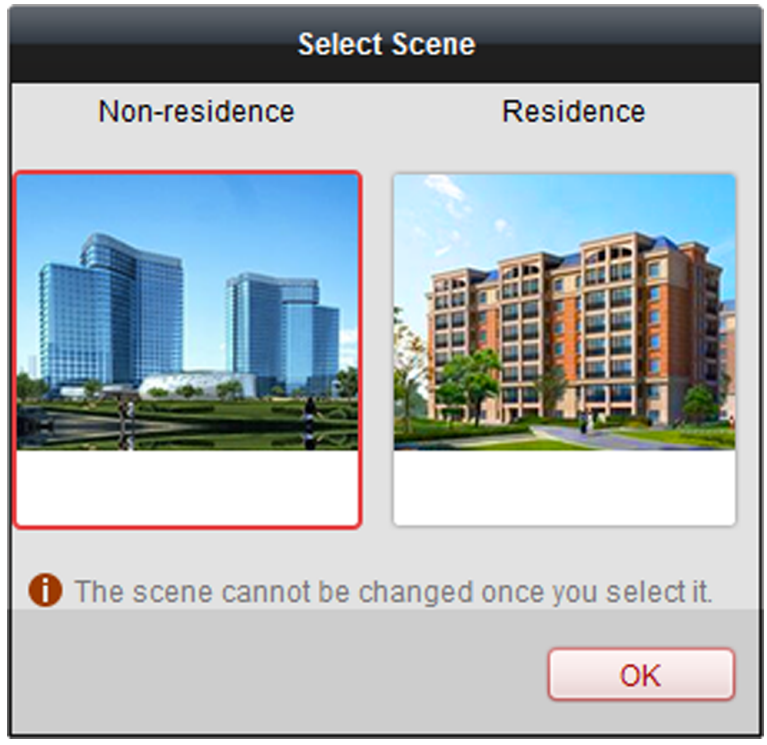


Figura 8-2 Selecione o cenário da aplicação de controlo de acesso

2.Selecione o cenário como residencial ou não residencial de acordo com as reais necessidades.

Nota

Se selecionar**Residência**modo, não pode configurar a regra de presença da pessoa ao adicionar uma pessoa.

3.Clique**OK**.

8.1.3 Configurar outros parâmetros

Após adicionar o dispositivo de controlo de acesso, pode definir os seus parâmetros como parâmetros de rede, parâmetros de captura, parâmetros RS-485, parâmetros Wiegand, etc.

Definir parâmetros de rede

Depois de adicionar o dispositivo de controlo de acesso, pode definir o modo de carregamento de registos do dispositivo e criar uma conta EHome através de uma rede com ou sem fios.

Definir modo de carregamento de registos

Pode definir o modo de upload de registos através do protocolo EHome.

Execute esta tarefa quando necessitar de definir o modo de carregamento de registos do dispositivo de controlo de acesso.

Passos

1.Clique**Controlo de acesso → Gestão de dispositivos**para entrar na página Gestão de dispositivos.

2.Selecione o dispositivo na lista de dispositivos e clique em**Modificar**.

3.Clique**Definições de rede → Modo de upload**para entrar na página Modo de carregamento.

4.Selecione o grupo central na lista pendente.

5.Verificação**Ativar**para ativar a configuração do modo de carregamento.

6.Selecione o modo de carregamento na lista pendente.

- Ativar**N1**ou**G1**para o canal principal e o canal de cópia de segurança.
- Selecionar**Perto**para desativar o canal principal ou o canal de cópia de segurança

Nota

- O canal principal e o canal de cópia de segurança não podem ativar N1 ou G1 ao mesmo tempo.
- N1 refere-se à rede cablada e G1 refere-se ao GPRS.
- Apenas os dispositivos com função 3G/4G suportam a configuração do canal como G1.
- Para definições de rede com fios, consulte***Crie uma conta EHome no modo de comunicação por fios*** .
- Para definições de rede sem fios, consulte***Crie uma conta EHome no modo de comunicação sem fios*** .

7.Clique**Guardar**.

Crie uma conta EHome no modo de comunicação por fios

Pode definir a conta para o protocolo EHome no modo de comunicação com fios. Depois pode adicionar dispositivos através do protocolo EHome.

Execute esta tarefa quando necessitar de criar uma conta EHome no modo de comunicação com fios para o dispositivo de controlo de acesso.

Passos

Nota

Esta função deve ser suportada pelo dispositivo

1.Clique**Controlo de acesso → Gestão de dispositivos**para entrar na página Gestão de dispositivos.

2.Selecione o dispositivo na lista de dispositivos e clique em**Modificar**.

3.Clique**Definições de rede → Central de rede**para entrar na página do Centro de Rede.

4.Selecione o grupo central na lista pendente.

5.Selecione o**Tipo de endereço**como**Endereço IP**ou**Nome de domínio**.

6.Introduza o endereço IP ou o nome de domínio de acordo com o tipo de endereço.

7.Introduza o número da porta do protocolo.

Nota

O número da porta da rede sem fios e da rede com fios deve ser consistente com o número da porta do EHome.

8.Selecione o**Tipo de protocolo**como**ECasa**e selecione a versão EHome.

Nota

Se definir a versão EHome como**5,0**, deve criar uma chave EHome para a conta EHome.

9.Defina um nome de conta para o centro de rede.

10. Clique**Guardar**.

Crie uma conta EHome no modo de comunicação sem fios

Pode definir a conta para o protocolo EHome no modo de comunicação sem fios. Depois pode adicionar dispositivos através do protocolo EHome.

Execute esta tarefa quando necessitar de criar uma conta EHome no modo de comunicação sem fios para o dispositivo de controlo de acesso.

Passos

Nota

Esta função deve ser suportada pelo dispositivo

1.Clique**Controlo de acesso → Gestão de dispositivos**para entrar na página Gestão de dispositivos.

2.Selecione o dispositivo na lista de dispositivos e clique em**Modificar**.

3.Clique**Definições de rede → Centro de comunicação sem fios**para entrar na página do Centro de comunicação sem fios.

4.Selecione o grupo central na lista pendente.

5.Introduza o endereço IP e o número da porta.

Nota

- Por predefinição, o número da porta do EHome é 7660.
- O número da porta da rede sem fios e da rede com fios deve ser consistente com o número da porta do EHome.

6.Selecione o**Tipo de protocolo**como**ECasa**.

7.Defina um nome de conta para o centro de rede.

8.Clique**Guardar**.

Autenticar encriptação de cartão M1

A encriptação do cartão M1 pode melhorar o nível de segurança da autenticação. Após emitir o cartão, pode ativar a função de encriptação do cartão M1 no software cliente.

Antes de começar

Utilize a estação de registo de cartões especificada para emitir o cartão. Ver***Emitir um cartão geral para pessoa*** para obter detalhes.

Execute esta tarefa quando necessitar de ativar a função de encriptação do cartão M1.

Nota

A função deve ser suportada pelo dispositivo de controlo de acessos e pelo leitor de cartões.

Passos

1.Clique**Controlo de acesso → Gestão de dispositivos**para entrar na página de gestão do dispositivo de controlo de acesso.

2.Selecione o dispositivo na lista de dispositivos e clique em**Modificar**para abrir a janela Modificar.

3.Clique**Encriptação de cartão M1**separador para entrar na página Encriptação do cartão M1.

4.Verificação**Ativar**para ativar a função de encriptação do cartão M1.

5.Defina o ID do setor.

O ID do setor varia de 1 a 100.

6.Clique**Guardar**para guardar as configurações.

Nota

Depois de ativar a função de encriptação do cartão M1, deve definir aqui o ID do setor do cartão adicionado como o ID do setor configurado.

8.1.4 Gerir Organização

Pode gerir a organização conforme desejado, como adicionar, editar ou eliminar a organização. Execute esta tarefa quando necessitar de gerir a organização.

Passos

1.Clique**Controlo de Acessos → Pessoa e Cartão**para entrar na página de gestão de pessoas e cartões.

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

3.Crie um nome para a organização.

4.Clique**OK**.

Nota

Podem ser adicionados até 10 níveis de organizações.

5.º Opcional: Depois de adicionar a organização, poderá realizar uma ou mais das operações seguintes.

Editar Organização	Selecione a organização adicionada e clique em**Modificar**para modificar o seu nome.
Eliminar Organização	Selecione a organização adicionada e clique em**Eliminar**para o eliminar. **Nota** • As organizações de nível inferior também serão eliminadas se eliminar uma organização. • Certifique-se de que não há nenhuma pessoa adicionada à organização ou a organização não poderá ser eliminada.

8.1.5 Gerir informações pessoais

Depois de adicionar a organização, pode adicionar uma pessoa à organização e geri-la, como emitir cartões em lote, importar e exportar informações pessoais em lote, etc.

Nota

Podem ser adicionadas até 10.000 pessoas ou cartões.

Adicionar uma única pessoa

Pode adicionar uma pessoa ao software cliente, uma a uma, e introduzir as informações da pessoa, tais como informações básicas, informações detalhadas, permissão de controlo de acesso, cartão ligado, imagem facial ligada, impressão digital ligada e regra de presença.

Configurar informações básicas da pessoa

Pode adicionar uma pessoa ao software cliente, uma a uma, e configurar as informações básicas da pessoa, como o nome, o número de telefone, etc.

Execute esta tarefa quando necessitar de configurar as informações básicas da pessoa ao adicionar uma pessoa.

Passos

1.Entrar**Controlo de Acessos → Pessoa e Cartão**.

2.Selecione uma organização na lista de organizações para adicionar a pessoa.

3.Clique**Adicionar**para abrir a janela de adição de pessoa.

O número da pessoa será gerado automaticamente e não é editável.

4.Introduza as informações básicas, incluindo o nome da pessoa, a duração válida e a palavra-passe.

5.Defina o tipo de pessoa e privilégio.

Normal

Pode definir privilégios para a pessoa normal, incluindo**Gerir back-end do dispositivo**e**Atraso de fecho ativado**.

Visitante

Caso a pessoa seja visitante, deverá definir os horários máximos para que o visitante abra a porta. Após o valor configurado o visitante não poderá voltar a abrir a porta.

Lista de bloqueio

Adicione a pessoa na lista de bloqueio. Se a pessoa se autenticar no dispositivo, o dispositivo carregará um evento no software cliente.

Gerir back-end do dispositivo

Defina a pessoa como administrador. Assim que a permissão for aplicada ao dispositivo, a pessoa poderá iniciar sessão no dispositivo e configurar parâmetros no dispositivo.

Atraso de fecho ativado

Se a função estiver ativada, o tempo de abertura da porta será prolongado. Pode definir a duração alargada de abertura em*Configurar parâmetros de porta*.

6.º Opcional: Defina a fotografia da pessoa.

- Clique**Carregar imagem**para selecionar a imagem da pessoa no PC local para a carregar no cliente.
- Clique**Tirar foto**para tirar a fotografia da pessoa com a câmara do PC.

7.Confirme a adição da pessoa.

- Clique**OK**para adicionar a pessoa e fechar a janela Adicionar Pessoa.
- Clique**Guardar e continuar**para adicionar a pessoa e continuar a adicionar outras pessoas.

Configurar informações detalhadas

Ao adicionar uma pessoa, pode configurar as informações detalhadas da pessoa, como o tipo de identificação da pessoa, o número de identificação, o país, etc., de acordo com as necessidades reais.

Execute esta tarefa quando necessitar de configurar as informações detalhadas da pessoa.

Passos

1.Entrar**Controlo de Acessos → Pessoa e Cartão**.

2.Selecione uma organização da lista de organizações para adicionar a pessoa e clique em**Adicionar**.

Nota

Introduza primeiro as informações básicas da pessoa. Para obter detalhes sobre como configurar as informações básicas da pessoa, consulte***Configurar informações básicas da pessoa*** .

3.Clique**Detalhes**guia.

4.Introduza as informações detalhadas da pessoa, incluindo o tipo de identificação da pessoa, o número de identificação, o país, etc., de acordo com as necessidades reais.

Dispositivo vinculado

ligar a estação interna à pessoa.

Nota

Se selecionar**Estação interna analógica**, o**Estação de porta**O campo será apresentado e deverá selecionar a estação externa para comunicar com a estação interna analógica.

5.Confirme para adicionar a pessoa.

- Clique**OK**para adicionar a pessoa e fechar a janela Adicionar Pessoa.
- Clique**Guardar e continuar**para adicionar a pessoa e continuar a adicionar outras pessoas.

Atribuir permissão à pessoa

Ao adicionar uma pessoa, pode atribuir as permissões (incluindo as permissões de operação do dispositivo de controlo de acesso e as permissões de controlo de acesso) à pessoa.

Execute esta tarefa quando necessitar de atribuir a permissão de controlo de acesso à pessoa.

Passos

Nota

Para definir a permissão de controlo de acesso, consulte***Atribuir permissão à pessoa*** .

1.Entrar**Controlo de Acessos → Pessoa e Cartão**.

2.Selecione uma organização na lista de organizações para adicionar a pessoa.

3.Clique**Adicionar**.

4.Introduza informações básicas da pessoa.

Nota

Para obter detalhes sobre como configurar as informações básicas da pessoa, consulte***Configurar informações básicas da pessoa*** .

5.Clique**Permissão**guia.

6.Na lista Permissões para selecionar, marque as caixas de seleção das permissões e clique em**>**para adicionar à lista Permissões selecionadas.

7.Confirme para adicionar a pessoa.

- Clique**OK**para adicionar a pessoa e fechar a janela Adicionar Pessoa.
- Clique**Guardar e continuar**para adicionar a pessoa e continuar a adicionar outras pessoas.

Emitir um cartão geral para pessoa

Ao adicionar uma pessoa, pode emitir um cartão geral com um número de cartão único para a pessoa.

Execute esta tarefa quando necessitar de emitir um cartão geral para a pessoa.

Passos

1.Entrar**Controlo de Acessos → Pessoa e Cartão**.

2.Selecione uma organização da lista de organizações para adicionar a pessoa e clique em**Adicionar**.

Nota

Introduza primeiro as informações básicas da pessoa. Para obter detalhes sobre como configurar as informações básicas da pessoa, consulte*Configurar informações básicas*.

3.Clique**Credencial → Cartão**separador para entrar na página de definições de credenciais do cartão.

4.Clique**Adicionar**e selecione**Cartão Geral**separador para entrar na página de configuração geral da placa.

5.Defina os parâmetros do cartão.

1) Selecione um tipo de cartão para o cartão geral.

Cartão normal

Por defeito, o cartão é um cartão normal, que não tem funções adicionais. **Cartão de patrulha**

A ação de passar o cartão pode ser utilizada para verificar o estado de trabalho da equipa de inspeção. A permissão de acesso da equipa de inspeção é configurável.

Cartão de coação

A porta pode ser aberta passando o cartão de coação quando existe coação. Ao mesmo tempo, o cliente pode denunciar o evento de coação.

Supercartão

O cartão é válido para todas as portas do controlador durante o horário configurado.

2)**Opcional:**No campo Observação, introduza as informações da observação para o cartão, se necessário.

Nota

São permitidos até 32 caracteres no campo Observação.

3) Defina o tempo de vigência e o prazo de validade do cartão.

6.Selecione o modo de leitura do cartão e introduza o número do cartão.

- Leitor de controlador de acesso

  1. Coloque o cartão no leitor do Controlador de Acesso.

  2.º Clique**Ler**para obter o número do cartão.

- Estação de Registo de Cartões

  1. Ligue a estação de registo de cartões ao PC que executa o cliente.

  2.º Clique**Definir Estação de Registo de Cartões**para definir os parâmetros da estação de registo de cartões.

  3.º Selecione o tipo de Estação Registo de Cartões.

  Nota

  Atualmente, os tipos de leitores de cartões suportados incluem o DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E e DS-K1F180-D8E.

4.º Defina o número da porta série, a taxa de transmissão, o valor do tempo limite, o zumbido ou o tipo de número do cartão.

5. Opcional: Se o cartão for M1 e se necessitar de ativar a função M1 Card Encryption, verifique **Ativar**da encriptação do cartão M1 e clique em**Modificar**para selecionar o setor.

Nota

A função de encriptação de cartão M1 é suportada pelo DS-K1F100-D8, DS-K1F100-D8E e DS-K1F180-D8E.

6.º Clique**Guardar**.

7. Coloque o cartão na estação de registo de cartões.

8.º Clique**Ler**para obter o número do cartão.

- Inserir manualmente

1.º Introduza o número do cartão manualmente.

2.º Clique**Entrar**para introduzir o número do cartão.

7.Clique**OK**.

O(s) cartão(ões) serão emitidos para a pessoa.

8.Confirme para adicionar a pessoa.

- Clique**OK**para adicionar a pessoa e fechar a janela Adicionar Pessoa.
- Clique**Guardar e continuar**para adicionar a pessoa e continuar a adicionar outras pessoas.

Recolha a impressão digital da pessoa localmente

Ao adicionar uma pessoa, pode recolher as informações de impressão digital da pessoa através do gravador de impressões digitais ligado ao PC que executa o cliente.

Execute esta tarefa quando necessitar de recolher a impressão digital da pessoa através do gravador de impressões digitais ligado ao PC que executa o cliente.

Passos

1.Entrar**Controlo de Acessos → Pessoa e Cartão**.

2.Selecione uma organização da lista de organizações para adicionar a pessoa e clique em**Adicionar**.

Nota

Introduza primeiro as informações básicas da pessoa. Para obter detalhes sobre como configurar as informações básicas da pessoa, consulte*Configurar informações básicas da pessoa*.

3.Clique**Credencial → Impressão digital**separador para entrar na página de definições de credenciais do cartão.

4.Selecione o modo de recolha como**Coleção Local**.

5.Ligue o gravador de impressões digitais ao PC e defina os seus parâmetros.

1) Clique**Definir máquina de impressão digital**para abrir a janela de configuração da máquina de impressão digital.

2) Selecione o tipo de dispositivo.

Nota

Atualmente, os tipos de gravadores de impressões digitais suportados incluem o DS-K1F800-F, DS-K1F300-F, DS-K1F810-F e DS-K1F820-F.

3)**Opcional:**Para o gravador de impressões digitais do tipo DS-K1F800-F, pode definir o número da porta série, a taxa de transmissão e os parâmetros de horas extraordinárias do gravador de impressões digitais.

Nota

- O número da porta série deve corresponder ao número da porta série do PC.
- A taxa de transmissão deve ser definida de acordo com o leitor de cartões de impressões digitais externo. O valor predefinido é 19200.
- **Tempo limite após**campo refere-se ao horário válido de recolha de impressões digitais. Se o utilizador não introduzir uma impressão digital ou introduzir uma impressão digital sem sucesso, o dispositivo indicará que a recolha de impressões digitais terminou.

4) Clique**Guardar**.

6.Recolha a impressão digital.

1) Clique**Iniciar**.

2) Selecione uma impressão digital na fotografia da mão para começar a recolher.

3) Levante e coloque a impressão digital correspondente no leitor de impressões digitais duas vezes para recolher a impressão digital.

1) Selecione um tipo de impressão digital.

Nota

Quando são recolhidas as mesmas impressões digitais de uma pessoa, aparece o aviso com repetição de ID. Quando são recolhidas impressões digitais semelhantes para pessoas diferentes, aparece um aviso com o ID repetido e o nome da pessoa.

7.Confirme a adição da pessoa.

- Clique**OK**para adicionar a pessoa e fechar a janela Adicionar Pessoa.
- Clique**Guardar e continuar**para adicionar a pessoa e continuar a adicionar outras pessoas.

Recolher a impressão digital da pessoa remotamente

Ao adicionar uma pessoa, pode recolher as informações de impressão digital da pessoa através do módulo de impressão digital do dispositivo de controlo de acesso remoto.

Execute esta tarefa quando necessitar de recolher a impressão digital da pessoa através do módulo de impressão digital do dispositivo de controlo de acessos.

Passos

1.Entrar**Controlo de Acessos → Pessoa e Cartão**.

2.Selecione uma organização da lista de organizações para adicionar a pessoa e clique em**Adicionar**.

Nota

Introduza primeiro as informações básicas da pessoa. Para obter detalhes sobre como configurar as informações básicas da pessoa, consulte*Configurar informações básicas da pessoa*.

3.Clique**Credencial → Impressão digital**separador para entrar na página de definições de credenciais do cartão.

4.Selecione o modo de recolha como**Recolha Remota**.

5.Clique**Iniciar**e selecione um dispositivo de controlo de acessos para recolher a impressão digital.

Nota

A função deve ser suportada pelo dispositivo.

6.Recolha a impressão digital.

1) Selecione uma impressão digital na fotografia da mão para começar a recolher.

2) Levante e coloque a impressão digital correspondente no módulo de impressão digital do dispositivo para recolher a impressão digital.

3) Selecione um tipo de impressão digital.

4) Clique**Parar**.

7.Confirme a adição da pessoa.

- Clique**OK**para adicionar a pessoa e fechar a janela Adicionar Pessoa.
- Clique**Guardar e continuar**para adicionar a pessoa e continuar a adicionar outras pessoas.

Configurar regra de presença

Ao adicionar pessoa, pode configurar a regra de presença da pessoa caso o cenário da aplicação seja modo não residencial e a pessoa adira no horário e presença.

Execute esta tarefa quando necessitar de configurar a regra de presença da pessoa ao adicionar uma pessoa.

Passos

Nota

Para obter detalhes sobre as definições de frequência e aplicação, consulte***Tempo e presença*** .

1.Entrar**Controlo de Acessos → Pessoa e Cartão**.

2.Selecione uma organização da lista de organizações para adicionar a pessoa e clique em**Adicionar**.

3.Introduza as informações básicas da pessoa.

Nota

Para obter detalhes sobre como configurar as informações básicas da pessoa, consulte***Configurar informações básicas da pessoa*** .

4.Clique**Regra da Presença**guia.

Nota

Esta página do separador será apresentada quando selecionar**Não Residência**modo como a cena da aplicação ao executar o software pela primeira vez. Para obter detalhes, consulte***Selecione o cenário da aplicação*** .

5.Se a pessoa aderir no horário e presença, verifique**Tempo e presença**para habilitar esta função para a pessoa.

Os registos de passagem do cartão da pessoa serão registados e analisados quanto ao tempo e à presença.

6.Defina regra de presença para a pessoa.

Nota

Para obter detalhes sobre o Tempo e a Presença, clique**Mais**para ir para o módulo Tempo e Presença.

7.Confirme para adicionar a pessoa.

- Clique**OK**para adicionar a pessoa e fechar a janela Adicionar Pessoa.
- Clique**Guardar e continuar**para adicionar a pessoa e continuar a adicionar outras pessoas.

Informação de identificação de pessoa de importação e exportação

Pode importar informações e fotografias de várias pessoas para o software cliente em lote. Entretanto, também pode exportar as informações e fotografias da pessoa e guardá-las no seu PC.

Importar informações pessoais

Pode importar as informações de várias pessoas (incluindo informações de identidade, dados de impressão digital e número de cartão ligado à impressão digital) para o software cliente em lote, importando um ficheiro Excel do PC local.

Execute esta tarefa quando necessitar de importar as informações pessoais para o cliente em batch.

Passos

1.Entrar**Controlo de Acessos → Pessoa e Cartão**.

2.Clique**Importar Pessoas**e selecione**Informações Pessoais**como o conteúdo a importar.

3.Na janela pop-up, clique em**Download modelo para pessoa importadora**para descarregar o modelo primeiro.

4.Introduza as informações da pessoa no modelo descarregado.

f1 a f10

Os dados da impressão digital da

pessoa. **f1card para f10card**

O número do cartão ligado à impressão digital. Se não estiver ligado a nenhum cartão, deixe-o em branco.

Nota

Se a pessoa tiver vários cartões, separe o número do cartão com ponto e vírgula.

5.Entrar**Controlo de Acessos → Pessoa e Cartão**,clique**Pessoa de importação**e selecione o ficheiro Excel com informações pessoais.

6.Clique**OK**para começar a importar.

Nota

Se o número da pessoa já existir na base de dados do software cliente, substituirá as informações da pessoa automaticamente após a importação.

Exportar informações pessoais

Pode exportar as informações das pessoas adicionadas para o PC local num ficheiro Excel. Execute esta

tarefa quando necessitar de exportar as informações da pessoa adicionada num lote.

Passos

1.Entrar**Controlo de Acessos → Pessoa e Cartão**módulo.

2.Clique**Pessoa de exportação**e selecione**Informações Pessoais**como o conteúdo a exportar.

3.Selecione o caminho para guardar o ficheiro Excel exportado.

4.Selecione os itens de informação pessoal a exportar.

5.Clique**OK**para começar a exportar.

f1 a f10

Os dados da impressão digital da

pessoa. **f1card para f10card**

O número do cartão ligado à impressão digital. Se não estiver ligado a nenhum cartão, deixe-o em branco.

Obter informações pessoais do dispositivo de controlo de acesso

Se o dispositivo de controlo de acessos adicionado tiver sido configurado com informações pessoais (incluindo dados da pessoa, impressão digital, informações do cartão emitido), pode obter as informações pessoais do dispositivo e importá-las para o cliente para operação posterior.

Execute esta tarefa quando necessitar de obter as informações da pessoa configurada no dispositivo de controlo de acessos.

Passos

Nota

- Esta função só é suportada pelo dispositivo cujo método de ligação é TCP/IP quando se adiciona o dispositivo.
- Se o nome da pessoa armazenado no dispositivo estiver vazio, o nome da pessoa será preenchido com o número do cartão emitido após a importação para o cliente.

1.Entrar**Controlo de Acessos → Pessoa e Cartão**.

2.Selecione uma organização para importar as pessoas.

3.Clique**Obter pessoa**para abrir a janela de seleção do dispositivo.

O dispositivo de controlo de acesso adicionado será apresentado.

4.Comece a obter as informações da pessoa.

- Selecione o dispositivo e clique em**OK**para começar a obter as informações da pessoa no dispositivo.
- Clique duas vezes no nome do dispositivo para começar a obter as informações da pessoa.

As informações da pessoa, incluindo os dados da pessoa, as informações de impressão digital da pessoa (se configuradas) e o cartão ligado (se configurado), serão importadas para a organização selecionada.

Emitir cartões para pessoa em lote

Pode emitir vários cartões para uma pessoa em lote.

Execute esta tarefa quando necessitar de emitir vários cartões para uma pessoa.

Passos

1.Entrar**Controlo de Acessos → Pessoa e Cartão**.

2.Clique**Cartão de emissão em lote**.

Todas as pessoas adicionadas sem cartão emitido serão apresentadas na lista Pessoa(s) sem cartão emitido.

3.Defina os parâmetros dos cartões.

1) Selecione o tipo de cartão de acordo com as necessidades reais.

Nota

Para obter detalhes sobre o tipo de cartão, consulte*Emitir um cartão geral para pessoa.*.

2) No campo Senha do Cartão, crie uma senha (4 a 8 dígitos) para o próprio cartão.

Nota

A palavra-passe será exigida quando o titular do cartão passar o cartão para entrar ou sair da porta se o modo de autenticação do leitor de cartões exigir uma palavra-passe. Para obter detalhes, consulte*Configurar o modo e a programação de autenticação do leitor de cartões*.

3) Introduza o número de cartões emitidos para cada pessoa.

Exemplo

Se a quantidade do cartão for 3, pode ler ou introduzir três números de cartão para cada pessoa.

4) Defina o tempo de vigência e o prazo de validade do cartão.

4.Na lista Pessoa(s) sem cartão emitido à esquerda, selecione a pessoa para emitir os cartões.

5.Selecione o modo de leitura do cartão e introduza o número do cartão.

Leitor de controlador de acesso

Coloque o cartão no leitor do Controlador de Acesso e clique**Ler**para obter o número do cartão. **Estação de Registo de Cartões**

Coloque o cartão na Estação de Registo de Cartões e clique**Ler**para obter o número do cartão.

Nota

A Card Enrollment Station deve ligar-se ao PC que executa o cliente. Pode clicar**Definir Estação de Registo de Cartões**para definir os parâmetros da estação de registo de cartões. Para obter detalhes, consulte *Emitir um cartão geral para pessoa*.

Inserir manualmente

Introduza o número do cartão manualmente e clique**Entrar**para introduzir o número do cartão.

Depois de emitir os cartões à pessoa, as informações da pessoa e do cartão serão apresentadas na lista Pessoa(s) com Cartão Emitido.

6.Clique**OK**.

Pesquisar informações da pessoa

Depois de adicionar as informações da pessoa ao cliente, pode pesquisar a pessoa definindo as condições de pesquisa.

Fornece pesquisa normal e pesquisa avançada para pesquisar a pessoa.

Pesquisa normal

Depois de adicionar as informações da pessoa ao cliente, pode pesquisar a pessoa pelo nome ou número do cartão.

Execute esta tarefa se pretender pesquisar as informações da pessoa por nome da pessoa ou número de cartão.

Passos

1.Entrar**Controlo de Acessos → Pessoa e Cartão**módulo.

2.Defina a condição de pesquisa.

- Para pesquisar a pessoa pelo nome da pessoa, introduza a palavra-chave do nome da pessoa no campo de pesquisa.
- Para pesquisar a pessoa pelo número do cartão, introduza manualmente a palavra-chave do número do cartão no campo de pesquisa ou clique em**Ler**para ler o número do cartão de um determinado cartão por estação de registo de cartões.

Nota

Antes de ler por estação de registo de cartões, precisa primeiro de ligar a estação de registo de cartões ao PC que executa o cliente. Pode clicar**Ler → Definir Estação de Registo de Cartões**para definir os seus parâmetros. Para obter detalhes, consulte***Emitir um cartão geral para pessoa*** .

3.Clique**Pesquisa**.

Os resultados da pesquisa serão apresentados na lista de pessoas.

Pesquisa Avançada

Depois de adicionar as informações da pessoa ao cliente, pode pesquisar a pessoa alvo definindo condições de pesquisa mais precisas, incluindo o número do cartão, o nome da pessoa e o número da pessoa.

Execute esta tarefa se precisar de pesquisar a pessoa alvo com condições de pesquisa mais precisas.

Passos

1.Entrar**Controlo de Acessos → Pessoa e Cartão**módulo.

2.Clique**Pesquisa Avançada**para visualizar as condições de pesquisa.

3.Defina a condição de pesquisa.

Número do cartão

Introduza a palavra-chave do número do cartão ou clique em**Ler**para ler o número do cartão de um determinado cartão por estação de registo de cartões.

Nota

Antes de ler por estação de registo de cartões, precisa primeiro de ligar a estação de registo de cartões ao PC que executa o cliente. Pode clicar**Ler → Definir Estação de Registo de Cartões**para definir os seus parâmetros. Para obter detalhes, consulte***Emitir um cartão geral para pessoa*** .

Pessoa Não.

Introduza a palavra-chave do número da pessoa.

Nome da pessoa

Introduza a palavra-chave do nome da pessoa.

Nota

O nome da pessoa é sensível a maiúsculas e minúsculas.

4.Clique**Pesquisa**.

Os resultados da pesquisa serão apresentados na lista de pessoas.

5.º Opcional: Clique**Reiniciar**para limpar as condições de pesquisa.

Perda de Boletim

Se a pessoa perdeu o seu cartão, pode comunicar a perda do cartão para que a permissão de controlo de acesso relacionada seja eliminada.

Execute esta tarefa se precisar de comunicar a perda do cartão à pessoa que perdeu o cartão.

Passos

1.Entrar**Controlo de Acessos → Pessoa e Cartão**módulo.

2.º Opcional: Pesquise a pessoa a quem pretende comunicar a perda do cartão.

Nota

Para pesquisar a pessoa, consulte***Pesquisar informações da pessoa*** .

3.Selecione a pessoa e clique**Modificar**para abrir a janela Editar Pessoa.

4.Clique**Credencial → Cartão**guia para mostrar as informações do cartão da pessoa

5.Selecione o cartão perdido e clique**Perda de Boletim**.

O estado do cartão mudará para perdido.

6.º Opcional: Se o cartão perdido for encontrado, pode selecioná-lo e clicar**Cancelar perda do cartão**para cancelar a perda.

O estado do cartão voltará ao normal.

7.º Opcional: Se tiver atribuído permissão de acesso à pessoa, será apresentada uma janela para o notificar para aplicar a permissão ao dispositivo novamente para entrar em vigor. Pode clicar**Inscreva-se já**ou**Aplicar mais tarde**para aplicar as alterações de permissões ao dispositivo.

Definir Estação de Registo de Cartões

A estação de registo do cartão pode ler o número do cartão colocado nela e mostrar o número do cartão ao cliente. Depois de ligar uma estação de registo de cartões ao PC que executa o cliente por interface USB ou COM, é necessário definir os parâmetros da estação de registo de cartões antes de a utilizar para ler o número do cartão.

Ao adicionar um cartão a uma pessoa, clique em**Definir Estação de Registo de Cartões**para abrir a janela Estação de Registo de Cartões.

Os seguintes parâmetros estão disponíveis:

Tipo

Selecione o modelo da estação de registo de cartões ligada

Nota

Atualmente, os modelos de estações de registo de cartões suportados incluem o DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E e DS-K1F180-D8E.

Tipo de cartão

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

Se o cartão contiver chips EM e IC, também pode selecionar**Tudo**para ler os números dos chips EM e IC.

Número da porta série e taxa de transmissão

Estes dois campos só estão disponíveis quando o modelo é DS-K1F100-M. Selecione o COM ao qual a estação de registo do cartão se liga e defina a taxa de transmissão. **Tempo limite após**

Especifique os milissegundos após os quais o número do cartão lido atingirá o tempo limite.

Zumbido

Active ou desactive o zumbido quando o número do cartão for lido com sucesso. **Nº do**

cartão Tipo

O tipo do número do cartão.

Encriptação de cartão M1

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

Se o cartão for M1 e necessitar de ativar a função M1 Card Encryption, verifique**Ativar**da encriptação do cartão M1 e clique em**Modificar**para selecionar o setor do cartão a encriptar.

8.1.6 Configurar o agendamento e o modelo

Pode configurar o modelo incluindo a programação semanal e a programação de feriados. Depois de definir os modelos, pode adotar os modelos configurados para as permissões de controlo de acesso ao definir a permissão, para que a permissão de controlo de acesso entre em vigor nos períodos de tempo do modelo.

Nota

Para as definições de permissão de controlo de acesso, consulte***Atribuir permissão à pessoa*** .

Adicionar programação semanal

Pode adicionar uma programação semanal personalizada para tornar a permissão de controlo de acesso válida ou inválida na programação semanal configurada.

Execute esta tarefa quando pretender adicionar uma programação semanal personalizada.

Passos

1.Clique**Controlo de Acessos → Cronograma e Modelo → Cronograma Semanal**para entrar na página Gestão da programação semanal.

Nota

Existem duas programações semanais padrão: Programação da semana inteira e Programação em branco, e não podem ser editadas ou eliminadas.

Programação da semana completa

A passagem do cartão é válida em todos os dias da semana.

Agenda em branco

A passagem do cartão é inválida em todos os dias da semana.

2.Adicione uma programação semanal.

1) Clique**Adicionar programação semanal**para abrir a caixa de diálogo Adicionar programação semanal.

2) Introduza o nome pretendido no**Nome da programação semanal**campo.

3) Clique**OK**para adicionar a programação da semana.

3.Clique na programação semanal adicionada na lista da esquerda para mostrar a sua propriedade à direita.

4.Selecione um dia da semana e desenhe períodos na barra da linha do tempo.

Nota

Podem ser definidos até 8 períodos de tempo para cada dia da programação semanal.

5.º Opcional: Execute uma das seguintes operações para editar os períodos sorteados.

- Mova o cursor para o período de tempo e arraste o período na barra da linha de tempo para a posição pretendida quando o cursor virar para .
- Clique no período de tempo e edite diretamente a hora de início/fim na caixa de diálogo apresentada.
- Mova o cursor para o fim do período de tempo e arraste para aumentar ou diminuir o período de tempo quando o cursor muda para .

6.º Opcional: Depois de definir o horário, pode realizar uma ou mais das seguintes operações.

Apagar programação diária	Selecione um dia e clique**Apagar duração**para eliminar a programação do dia selecionado.
Programação da semana clara	Clique**Claro**para excluir toda a programação da semana.
Copiar para a semana inteira	Clique**Copiar para a semana**para copiar a programação deste dia para toda a semana.

7.Clique**Guardar**para guardar as definições e terminar de adicionar a programação semanal.

Adicionar horário de feriados

Pode criar um horário para feriados e definir os dias no horário de feriados, incluindo a data de início, a data de fim e a duração dos feriados num dia.

Execute esta tarefa quando precisar de adicionar um horário de feriados para predefinir os feriados.

Passos

1.Clique**Controlo de Acessos → Cronograma e Modelo → Cronograma Semanal**para entrar na página Gestão de grupos de feriados.

2.Adicione um grupo de feriados.

1) Clique**Adicionar grupo de feriados**à esquerda para abrir a janela de adição de grupo de feriados.

2) Crie um nome para o grupo de feriados.

3) Clique**OK**.

3.Adicione um período de feriados ao grupo de feriados e configure a duração dos feriados.

Nota

Podem ser adicionados até 16 períodos de feriados a um grupo de feriados.

1) Clique**Adicionar feriado**.

2) Arraste para desenhar o período, ou seja, neste período de tempo a permissão configurada está ativada.

Nota

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

3)**Opcional:**Quando o cursor muda para , pode mover a barra de tempo selecionada que acabou de editar. Também pode editar o ponto no tempo apresentado para definir o período de tempo preciso.

4)**Opcional:**Quando o cursor muda para , pode aumentar ou diminuir a barra de tempo selecionada.

4.Clique**Guardar**.

Adicionar modelo

Depois de definir o horário semanal e o grupo de feriados, pode adicionar e configurar o modelo que contém o horário semanal e o horário do grupo de feriados.

Execute esta tarefa se pretender adicionar e configurar o modelo.

Passos

1.Clique**Controlo de Acessos → Cronograma e Modelo → Modelo**para entrar na página Gestão de modelos.

Nota

Existem dois modelos padrão: Modelo de semana inteira e Modelo em branco, e não podem ser editados ou eliminados.

Modelo de semana inteira

O bilhete do cartão é válido em todos os dias da semana e não tem horário de grupo de feriados. **Modelo em branco**

A passagem do cartão é inválida em todos os dias da semana e não tem programação de grupos de feriados.

2.Adicione um modelo.

1) Clique**Adicionar modelo**para abrir a janela Adicionar modelo.

2) Introduza um nome no**Nome do modelo**arquivado.

3) Clique**OK**para adicionar o modelo.

3.Clique no modelo adicionado na lista da esquerda para mostrar a sua propriedade à direita.

4.Adicione uma programação semanal para aplicar ao modelo.

1) Clique**Programação semanal**guia à direita.

2) No campo Programação Semanal, selecione uma programação semanal configurada.

3)**Opcional:**Clique**Adicionar programação semanal**para adicionar uma nova programação semanal.

Nota

Para obter detalhes sobre como adicionar uma programação semanal, consulte***Adicionar programação semanal*** .

5.Adicione uma programação de grupo de feriados para aplicar ao modelo.

Nota

Até quatro grupos de feriados podem ser adicionados a um modelo.

1) Clique**Grupo de férias**guia.

2) Selecione um grupo de feriados da lista.

3)**Opcional:**Clique**Adicionar grupo de feriados**para adicionar uma nova programação de grupo de feriados.

Nota

Para obter detalhes sobre como adicionar um grupo de feriados, consulte***Adicionar horário de feriados*** .

4) Clique**Adicionar**para adicionar a programação do grupo de feriados selecionado à lista certa.

5)**Opcional:**Selecione um grupo de feriados selecionado na lista à direita e clique em**Eliminar**para remover o selecionado.

6.Clique**Guardar**para guardar as definições e terminar de adicionar o modelo.

8.1.7 Gerir permissão

Após adicionar a pessoa e configurar as credenciais da pessoa, pode criar as permissões de acesso para definir o nível de acesso de que pessoas podem ter acesso a que portas.

Atribuir permissão à pessoa

Pode atribuir permissão às pessoas para que possam entrar ou sair dos pontos de controlo de acesso (portas) de acordo com a permissão atribuída.

Execute esta tarefa se necessitar de atribuir permissões de acesso a pessoas.

Passos

- Pode adicionar até 4 permissões a um ponto de controlo de acesso de um dispositivo.
- Pode adicionar até 128 permissões no total.
- Quando as definições de permissões são alteradas, é necessário aplicar as permissões aos dispositivos novamente para que tenham efeito. As alterações de permissões incluem alterações de programação e de modelo, definições de permissões, definições de permissões da pessoa e dados da pessoa relacionada (incluindo número do cartão, impressão digital, ligação entre o número do cartão e a impressão digital, ligação entre o número do cartão e a impressão digital, senha do cartão, período de vigência do cartão, etc.

1.Clique**Controlo de acesso → Permissão**para entrar na interface de gestão de permissões.

2.Clique**Adicionar**para abrir a janela de permissão de adição.

3.No**Nome da permissão**campo de texto, crie um nome para a permissão que pretende.

4.Selecione um modelo de agendamento para a permissão.

Nota

Deve configurar o modelo antes das definições de permissão. Pode clicar**Adicionar modelo**para adicionar o modelo. Consulte*Configurar agendamento e modelo*para obter detalhes.

5.Na lista Pessoa, selecione a(s) pessoa(s) a quem atribuir a permissão e clique em**>**para adicionar à lista Pessoa Selecionada.

6.Na lista Ponto/dispositivo de controlo de acesso, selecione porta(s) ou estação(s) de porta para as pessoas selecionadas acederem e clique em**>**para adicionar à lista selecionada.

7.Clique**OK**.

As pessoas selecionadas terão permissão para entrar/sair das portas/postos exteriores selecionados com os seus cartões ou impressões digitais vinculados.

8.Depois de adicionar as permissões de acesso, precisa de as aplicar ao dispositivo de controlo de acesso para que tenham efeito.

1) Selecione as permissões a aplicar ao dispositivo de controlo de acessos.

Para selecionar múltiplas permissões, pode segurar o**Ctrl**ou**Turno**chave e selecione permissões.

2) Clique**Aplicar todos os**para começar a aplicar todas as permissões selecionadas ao dispositivo de controlo de acesso ou à estação externa.

Nota

Também pode clicar**Aplicar alterações**para aplicar a parte alterada das permissões selecionadas ao(s) dispositivo(s).

Permissão atribuída para pesquisa

Depois de adicionar as permissões de acesso, pode pesquisar as permissões existentes definindo as condições de pesquisa.

Execute esta tarefa se necessitar de pesquisar a permissão de acesso atribuída.

Passos

1.Clique**Controlo de acesso → Permissão**para entrar na interface de gestão de permissões.

2.Clique**Pesquisa Avançada**para abrir a janela de pesquisa.

3.Defina a condição de pesquisa.

Pessoa Não.

Introduza a palavra-chave do número da pessoa.

Nome da pessoa

Introduza a palavra-chave do nome da pessoa.

Nota

O nome da pessoa é sensível a maiúsculas e minúsculas.

Número do cartão

Introduza a palavra-chave do número do cartão.

Nome da permissão

O nome da permissão é sensível a maiúsculas e minúsculas.

4.Clique**Pesquisa**.

Os resultados da pesquisa serão apresentados abaixo.

5.Clique**Reiniciar**para limpar as condições de pesquisa.

8.1.8 Configurar funções avançadas

Após configurar a pessoa, o modelo e a permissão de acesso, pode configurar as funções avançadas da aplicação de controlo de acesso, como os parâmetros de controlo de acesso, a palavra-passe de autenticação e a abertura de porta com o primeiro cartão, anti-passback, etc.

Por predefinição, são apresentadas três funções nas funções avançadas: parâmetros de controlo de acesso, autenticação do leitor de cartões e autenticações múltiplas. Pode clicar**Adicionar**na barra de separadores para selecionar as funções que pretende visualizar.

Nota

As funções avançadas devem ser suportadas pelo dispositivo.

Configurar os parâmetros de controlo de acesso

Após adicionar o dispositivo de controlo de acessos, pode configurar os parâmetros dos pontos de controlo de acessos (porta ou piso), entradas de alarme, saídas de alarme e leitores de cartões.

Configurar os parâmetros do dispositivo de controlo de acesso

Após adicionar o dispositivo de controlo de acesso, pode configurar os seus parâmetros.

Execute esta tarefa quando pretender configurar parâmetros do dispositivo de controlo de acesso.

Passos

1.Clique**Controlo de acessos → Função avançada → Parâmetros de controlo de acessos**para entrar na página de definições de parâmetros.

2.Selecione um controlador de acesso para mostrar os seus parâmetros à direita.

3.Marque a caixa de seleção para ativar as funções correspondentes.

Nota

Os parâmetros apresentados podem variar para diferentes dispositivos de controlo de acesso.

Redundância de comunicação do leitor de cartões RS-485

Deve marcar a caixa de selecção se ligar o leitor de cartões RS-485 ao dispositivo de controlo de acesso de forma redundante.

Prima a tecla para introduzir o número do cartão.

Se marcar a caixa de selecção, pode introduzir o número do cartão premindo a tecla .

4.Clique**Guardar**.

5.º Opcional: Clique**Copiar para**e selecione o dispositivo de controlo de acessos para copiar os parâmetros para outros dispositivos.

Configurar parâmetros de porta

Depois de adicionar o dispositivo de controlo de acesso, pode configurar os parâmetros do ponto de controlo de acesso (porta).

Execute esta tarefa quando pretender configurar os parâmetros da porta (piso) para o dispositivo de controlo de acessos.

Passos

1.Clique**Controlo de acessos → Função avançada → Parâmetros de controlo de acessos**para entrar na página de definições de parâmetros.

2.Selecione um controlador de acesso e clique para mostrar as portas ou pisos do dispositivo de controlo de acesso selecionado.

3.Selecione uma porta ou um piso para mostrar os seus parâmetros à direita.

4.Edite os parâmetros da porta ou do piso.

Sensor magnético de porta

Selecione o estado do contacto da porta Permanecer Fechado ou Permanecer Aberto.

Tipo de botão de saída

Selecione o estado do botão de saída Permanecer Fechado ou Permanecer Aberto.

Tempo de porta trancada

Após passar o cartão normal e retransmitir a ação, o temporizador para trancar a porta começa a funcionar.

Duração Aberta Prolongada

O magnético da porta pode ser ativado com o atraso apropriado após a pessoa passar o cartão. **Alarme de tempo limite de abertura de porta**

O alarme pode ser acionado caso a porta não tenha sido fechada no período de tempo configurado. **Código de coação**

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

Supersenha

A pessoa específica pode abrir a porta inserindo a super palavra-passe. **Código de dispensa**

Crie um código de dispensa que possa ser utilizado para parar a campainha do leitor de cartões (introduzindo o código de dispensa no teclado).

Nota

- O código de coação, o supercódigo e o código de dispensa devem ser diferentes.
- O código de coação, a supersenha e o código de dispensa devem ser diferentes da senha de autenticação.
- O código de coação, a super-senha e o código de dispensa devem conter 4 a 8 dígitos.

5.Clique**Definições de duração do estado**para definir a duração do estado da porta. Para obter detalhes, consulte*Configurar o cronograma de duração para o estado da porta*.

6.Clique**Guardar**.

7.º Opcional: Clique**Copiar para**e selecione a(s) porta(s)/piso(s) para copiar os parâmetros para outras portas/piso(s).

Nota

As definições de duração do estado da porta ou do piso também serão copiadas para as portas/pisos selecionados.

Configurar o cronograma de duração para o estado da porta

Pode configurar a programação de duração semanal para que o ponto de controlo de acesso (porta) do dispositivo de controlo de acesso permaneça aberto ou fechado.

Execute esta tarefa quando necessitar de configurar a programação da duração do estado da porta.

Passos

1.Clique**Controlo de acessos → Função avançada → Parâmetros de controlo de acessos**para entrar na página de definições de parâmetros.

2.Selecione uma porta para mostrar os seus parâmetros à direita.

3.Clique**Definições de duração do estado**para abrir a janela Duração do estado.

4.Selecione um pincel de estado da porta como**Permaneça aberto**ou**Permanecer Fechado**.

- **Permanecer aberto:**A porta permanecerá desbloqueada durante o período configurado. O pincel está marcado como .
- **Permanecer Encerrado:**A porta permanecerá trancada durante o período configurado. O pincel está marcado como .

5.Arraste na linha do tempo para desenhar uma barra colorida na programação para definir a duração.

6.º Opcional: Selecione a barra de horário de agendamento e clique em**Copiar para a semana inteira**para copiar as definições da barra horária para os outros dias da semana.

7.Clique**Guardar**para guardar a programação de duração do estado.

8.Clique**Guardar**para guardar os parâmetros da porta.

Configurar os parâmetros do leitor de cartões

Após adicionar o dispositivo de controlo de acessos, pode configurar os parâmetros do leitor de cartões.

Execute esta tarefa quando pretender configurar os parâmetros do leitor de cartões para o dispositivo de controlo de acessos.

Passos

1.Clique**Controlo de acessos → Função avançada → Parâmetros de controlo de acessos**para entrar na página de definições de parâmetros.

2.Selecione um controlador de acesso e clique para mostrar os leitores de cartões do controlador de acesso selecionado.

3.Selecione um leitor de cartões para mostrar os seus parâmetros à direita.

4.Edite os parâmetros do leitor de cartões.

Nota

Os parâmetros apresentados podem variar para diferentes dispositivos de controlo de acesso. Há parte dos parâmetros listados abaixo. Consulte o manual do utilizador do dispositivo para obter mais detalhes.

Apelido

Edite o nome do leitor de cartões conforme pretendido.

Ativar leitor de cartão

Selecionar**Sim**para ativar o leitor de cartões para passar o cartão. **Polaridade**

do LED OK/Erro Polaridade do LED/Polaridade da Campainha

Defina a polaridade do LED OK/Polaridade do LED de erro/Polaridade do LED da campainha da placa principal de acordo com os parâmetros do leitor de cartões. Geralmente, adota as definições padrão.

Intervalo mínimo de passagem do cartão

Se o intervalo entre a passagem do mesmo cartão for inferior ao valor definido, a passagem do cartão é inválida. Pode configurá-lo para 0 a 255.

Máx. Intervalo ao introduzir a palavra-passe

Ao introduzir a palavra-passe no leitor de cartões, se o intervalo entre a pressão de dois dígitos for superior ao valor definido, os dígitos que premiu antes serão automaticamente apagados.

Ativar limite de tentativas mal sucedidas de leitura de cartão

Active para reportar alarme quando as tentativas de leitura do cartão atingirem o valor configurado.

Máx. Tempos de falha na passagem do cartão

Defina o máximo. tentativas falhadas de leitura do cartão.

Ativar deteção de adulteração

Active a deteção anti-adulteração para o leitor de cartões. **Detetar**

quando o leitor de cartões está offline para

Quando o dispositivo de controlo de acessos não consegue ligar-se ao leitor de cartões durante mais tempo do que o definido, o leitor de cartões ficará automaticamente offline.

Tempo de zumbido

Defina o tempo de zumbido do leitor de cartões. O tempo disponível varia de 0 a 5.999s. 0 representa zumbido contínuo.

Tipo de leitor de cartões/descrição do leitor de cartões

Obtenha o tipo e a descrição do leitor de cartões. São somente leitura. **Nível de**

reconhecimento de impressões digitais

Selecione o nível de reconhecimento de impressões digitais na lista pendente.

Modo de autenticação do leitor de cartões padrão

Pode visualizar o modo de autenticação padrão do leitor de cartões nesta parte.

5.Clique**Guardar**.

6.º Opcional: Clique**Copiar para**e selecione o(s) leitor(es) de cartões para copiar os parâmetros para outros leitores de cartões.

Configurar os parâmetros de entrada de alarme

Após adicionar o dispositivo de controlo de acesso, pode configurar os parâmetros para as suas entradas de alarme. Execute esta tarefa se necessitar de definir os parâmetros de entrada de alarme do dispositivo de controlo de acesso. **Passos**

Nota

Se a entrada de alarme estiver armada, não será possível editar os seus parâmetros. Desarme-o primeiro.

1.Clique**Controlo de acessos → Função avançada → Parâmetros de controlo de acessos**para entrar na página de definições de parâmetros.

2.Selecione um dispositivo e clique para mostrar as entradas de alarme do dispositivo de controlo de acesso selecionado.

3.Defina os parâmetros de entrada de alarme.

Apelido

Edite o nome da entrada de alarme conforme pretendido.

Tipo de detector

O tipo de detector da entrada de alarme.

Tipo de zona

Defina o tipo de zona para a entrada de alarme.

Sensibilidade

Só quando a duração do sinal detetado pelo detetor atinge o tempo definido é que a entrada de alarme é acionada. Por exemplo, definiu a sensibilidade para 10ms, apenas quando a duração do sinal detectado pelo detector atingir 10ms é que esta entrada de alarme será activada.

Acionar saída de alarme

Selecione a(s) saída(s) de alarme a acionar.

4.Clique**Guardar**.

5.º Opcional: Clique no botão no canto superior direito para armar ou desarmar a entrada de alarme.

Configurar os parâmetros de saída de alarme

Depois de adicionar o dispositivo de controlo de acesso, se o dispositivo estiver ligado a saídas de alarme, pode configurar os parâmetros.

Execute esta tarefa se necessitar de definir os parâmetros de entrada de alarme do dispositivo de controlo de acesso.

Passos

1.Clique**Controlo de acessos → Função avançada → Parâmetros de controlo de acessos**para entrar na página de definições de parâmetros.

2.Selecione um dispositivo e clique para mostrar as saídas de alarme do dispositivo de controlo de acesso selecionado.

3.Defina os parâmetros de saída de alarme.

Atraso de saída

O tempo de atraso para que a saída do alarme seja acionada.

4.Clique**Guardar**.

5.º Opcional: Coloque a chave no canto superior direito para**EM**para acionar a saída de alarme.

Configurar a autenticação individual

Defina o modo de autenticação do indivíduo.

Antes de começar

Adicione uma pessoa e aplique-a no dispositivo. Para obter detalhes, consulte*Gerir informações pessoais* e *Gerir permissão*.

Passos

1.Clique**Controlo de acessos → Função avançada → Autenticação do leitor de cartões**para entrar na página de configuração de autenticação do leitor de cartões.

2.Clique no nome de um dispositivo para entrar na página Autenticação Avançada Individual.

3.Clique**Adicionar**e selecione as pessoas e o seu modo de autenticação.

4.Clique**OK**para guardar as configurações.

Nota

A autenticação individual configurada tem uma prioridade mais elevada do que outros modos de autenticação.

O modo de aplicação individual será aplicado automaticamente ao dispositivo.

5.º Opcional: Selecione uma pessoa na página Autenticação Individual e clique em**Modificar**para alterar o modo de autenticação individual da pessoa.

6.º Opcional: Se a aplicação do modo de autenticação individual falhar, clique em**Falha no aplicativo**para ver detalhes. Selecione um estado de inscrição na lista e clique em**Inscreva-se novamente**para aplicar o modo de autenticação da pessoa novamente ao dispositivo.

Configurar o modo e a programação de autenticação do leitor de cartões

Pode definir as regras de passagem para o leitor de cartões do dispositivo de controlo de acessos de acordo com as suas necessidades reais.

Execute esta tarefa se necessitar de configurar o modo e a programação de autenticação do leitor de cartões.

Passos

1.Clique**Controlo de acessos → Função avançada → Autenticação do leitor de cartões**para entrar na página de configuração de autenticação do leitor de cartões.

2.Selecione um leitor de cartões à esquerda para configurar.

3.Defina o modo de autenticação do leitor de cartões.

1) Clique**Configuração**.

Nota

- Palavra-passe refere-se à palavra-passe do cartão definida ao emitir o cartão para a pessoa. Para obter detalhes, consulte *Adicionar uma única pessoa*.
- A palavra-passe de autenticação refere-se à palavra-passe definida para abrir a porta. Consulte Configurar palavra-passe de autenticação.
- O modo de autenticação do leitor de cartões suportado varia de acordo com os diferentes dispositivos. Para obter detalhes, consulte o produto real.

2) Selecione os modos e clique para adicionar à lista de modos selecionados.

3)**Opcional:**Clique ou para ajustar a ordem de apresentação.

4) Clique**OK**.

Depois de selecionar os modos, os modos selecionados serão apresentados como ícones.

4.Clique no ícone para selecionar um modo de autenticação do leitor de cartões e arraste o dia para desenhar uma barra colorida na programação, o que significa que durante esse período de tempo a autenticação do leitor de cartões é válida.

5.Repita o passo acima para definir outros períodos de tempo.

6.º Opcional: Selecione um dia configurado e clique em**Copiar para a semana**para copiar as mesmas definições para toda a semana.

7.º Opcional: Clique**Copiar para**para copiar as definições para outros leitores de cartões.

8.Clique**Guardar**.

Configurar autenticação múltipla

Pode gerir os cartões por grupo e definir a autenticação para vários cartões a partir de um ponto de controlo de acesso (porta).

Antes de começar

Defina a permissão do cartão e aplique as definições de permissão ao dispositivo de controlo de acesso. Para obter detalhes, consulte***Atribuir permissão à pessoa*** .

Execute esta tarefa quando pretender definir autenticações para vários cartões a partir de um ponto de controlo de acesso (porta).

Passos

1.Clique**Controlo de Acesso → Função Avançada → Autenticação Múltipla**para entrar na página Autenticação Múltipla.

2.Selecione um dispositivo de controlo de acessos na lista do painel Controller List.

3.Adicione um grupo de cartões para o dispositivo de controlo de acesso.

1) Clique**Adicionar**no painel Definir grupo de cartões.

2) Crie um nome para o grupo conforme pretendido.

3) Especifique a hora de início e de fim do período de vigência do grupo de cartões.

4) Selecione os cartões a adicionar ao grupo de cartões.

5) Clique**OK**.

4.Selecione um ponto de controlo de acesso (porta) do dispositivo selecionado no painel Definir grupo de autenticação.

5.Introduza o intervalo de tempo para a passagem do cartão.

6.Adicione um grupo de autenticação para o ponto de controlo de acesso selecionado.

1) Clique**Adicionar**no painel Definir grupo de autenticação.

2) Selecione um modelo configurado para o grupo de autenticação na lista pendente.

Nota

Para definir o modelo, consulte***Configurar agendamento e modelo*** .

3) Selecione o tipo de autenticação como**Autenticação local**,**Autenticação local e porta aberta remotamente**, ou**Autenticação local e super password**na lista pendente.

Autenticação local

Autenticação pelo dispositivo de controlo de acessos.

Autenticação local e porta aberta remotamente

Autenticação pelo dispositivo de controlo de acessos e pelo cliente. Quando a pessoa passa o cartão no dispositivo, irá aparecer uma janela. Pode destrancar a porta através do cliente.

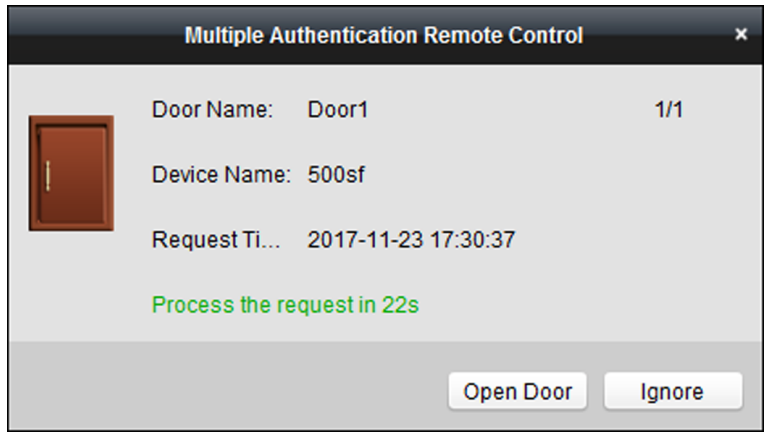


Figura 8-3 Porta aberta remotamente

Nota

Pode verificar**Autenticação offline**para ativar a autenticação por super palavra-passe quando o dispositivo de controlo de acesso estiver desligado do cliente.

Autenticação local e super password

Autenticação pelo dispositivo de controlo de acessos e pela super password.

4) Selecione o grupo de cartões adicionado na lista esquerda abaixo e clique para adicionar o grupo de cartões selecionado à lista direita como grupo de autenticação.

5)**Opcional:**Clique ou para definir a ordem de passagem do cartão.

6) Clique no grupo de autenticação adicionado na lista da direita para definir os tempos de passagem do cartão.

Nota

- Os tempos de passagem do cartão devem ser superiores a 0 e inferiores à quantidade de cartões adicionados no grupo de cartões.
- O valor máximo dos tempos de passagem do cartão é 16.

7) Clique**OK**.

Nota

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

7.Clique**Guardar**.

Configurar porta de abertura com primeiro cartão

Pode definir vários primeiros cartões para um ponto de controlo de acesso. Após a primeira passagem do cartão, permite que várias pessoas acedam à porta ou a outras ações de autenticação.

Antes de começar

Defina a permissão do cartão e aplique a definição de permissão ao dispositivo de controlo de acesso. Para obter detalhes, consulte***Atribuir permissão à pessoa*** .

Execute esta tarefa quando pretender configurar a abertura da porta com o primeiro cartão.

Passos

1.Clique**Controlo de Acessos → Função Avançada → Porta Aberta com Primeiro Cartão**para entrar na página Porta Aberta com Primeiro Cartão.

2.Selecione um dispositivo de controlo de acessos na lista do painel Controller List.

3.Selecione o primeiro modo de cartão como**Permaneça aberto com o primeiro cartão**,**Desativar Permanecer Aberto com o Primeiro Cartão**, ou**Autorização do primeiro cartão**na lista pendente para cada ponto de controlo de acesso do dispositivo selecionado.

Permaneça aberto com o primeiro cartão

A porta permanece aberta durante o tempo configurado após a primeira passagem do cartão até que o período de permanência aberta termine. Se selecionar este modo, deverá definir a duração da permanência aberta.

Nota

A duração da permanência aberta deve situar-se entre 0 e 1440 minutos. Por predefinição, a duração da permanência aberta é de 10 minutos.

Desativar Permanecer Aberto com o Primeiro Cartão

Desative a função de permanecer aberto com o primeiro cartão.

Autorização do primeiro cartão

Todas as autenticações (exceto as autenticações de super cartão, super senha, super impressão digital, cartão de coação, código de coação e impressão digital de coação) são permitidas somente após a primeira autorização do cartão.

Nota

O**Autorização do primeiro cartão**entra em vigor apenas no dia atual. A autorização expirará após as 24h do dia atual.

Nota

Pode passar novamente o primeiro cartão para desativar o modo do primeiro cartão.

4.Clique**Adicionar**no painel Lista de Primeiras Cartas.

5.Selecione um cartão da lista e clique em**OK**para adicionar o cartão selecionado como o primeiro cartão das portas.

O primeiro cartão adicionado será listado no painel Lista de primeiros cartões.

6.º Opcional: Selecione um primeiro cartão da lista e clique em**Eliminar**para remover o cartão da primeira lista de cartões.

7.Clique**Guardar**.

Configurar anti-passback

Pode configurar para passar apenas pelo ponto de controlo de acesso de acordo com o caminho especificado e apenas uma pessoa poderá passar pelo ponto de controlo de acesso após passar o cartão.

Antes de começar

Active a função anti-passback do dispositivo de controlo de acesso.

Execute esta tarefa quando pretender configurar o anti-passback para o dispositivo de controlo de acesso.

Passos

Nota

Tanto a função anti-retorno como a função de encravamento de múltiplas portas podem ser configuradas para um dispositivo de controlo de acessos ao mesmo tempo. Para a configuração do encravamento multiportas, consulte ***Configurar encravamento multiportas*** .

1.Clique**Controlo de Acessos → Função Avançada → Anti-Passback**para entrar na página de configuração anti-passback.

2.Selecione um dispositivo de controlo de acessos na lista.

3.Selecione um leitor de cartões como início do percurso na**Primeiro leitor de cartões**campo.

4.Clique no campo de texto do primeiro leitor de cartões selecionado na**Leitor de cartões depois**coluna para abrir a caixa de diálogo Selecionar leitor de cartões.

5.Selecione os seguintes leitores de cartões para o primeiro leitor de cartões.

Nota

Até quatro leitores de cartões posteriores podem ser adicionados a um leitor de cartões.

6.Clique**OK**na caixa de diálogo para guardar as seleções.

7.Clique**Guardar**no canto superior direito da página Anti-Passback para guardar as definições e entrar em vigor.

Nota

As supercredenciais, como o super cartão, a super palavra-passe, a super impressão digital e assim por diante, têm o privilégio de não seguir as regras anti-passback.

Exemplo

Definir caminho de passagem do cartão

Se selecionar Reader In_01 como início e selecionar Reader In_02, Reader Out_04 como leitores de cartões ligados. Depois, só poderá passar pelo ponto de controlo de acesso passando o cartão pela ordem como Reader In_01, Reader In_02 e Reader Out_04.

Configurar anti-passagem de controlador cruzado

Pode definir o anti-passback para leitores de cartões em vários dispositivos de controlo de acesso. Deve passar o cartão de acordo com a rota configurada para passar o cartão. E apenas uma pessoa podia passar pelo ponto de controlo de acesso após passar o cartão.

Nota

Deve ser suportado pelo dispositivo.

Configurar anti-passagem de rota com base no cartão

A rota anti-passagem depende da rota de passagem do cartão. Deve configurar o primeiro leitor de cartões e os leitores de cartões posteriormente. Este julgará o anti-retorno de acordo com os registos de entrada e saída do cartão.

Execute esta tarefa se precisar de configurar o anti-retorno da rota e julgar o anti-retorno de acordo com os registos de entrada e saída no cartão.

Passos

Nota

Atualmente suporta cartão M1 e o setor não pode ser encriptado. Para obter detalhes sobre a encriptação de setor, consulte***Autenticar encriptação de cartão M1*** .

1.Clique**Controlo de acesso → Função avançada → Anti-passagem de retorno do controlador cruzado**para entrar na página de configuração anti-passagem do controlador cruzado.

2.Verificação**Ativar Anti-passagem de Controlador Cruzado**para ativar a função.

3.Selecionar**Baseado no cartão**como o modo anti-passagem de volta.

4.Selecionar**Rota anti-passagem de regresso**como regra.

5.Defina o ID do setor.

6.Clique**Selecione controlador de acesso**para selecionar um dispositivo para antirretorno.

Nota

Podem ser adicionados até 64 dispositivos com função anti-passback.

7.Configure o primeiro leitor de cartões e os leitores de cartões posteriores.

1) Na área Leitor de cartões, clique no ícone à esquerda da coluna do leitor de cartões para o definir como o primeiro leitor de cartões.

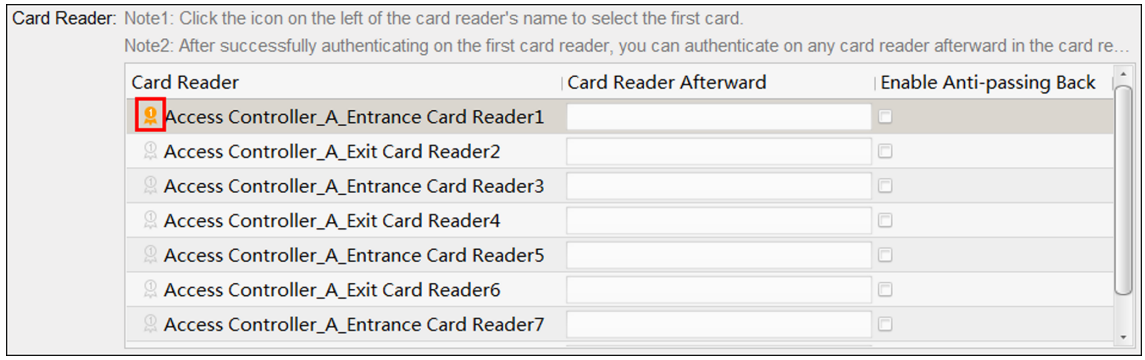


Figura 8-4 Selecione o primeiro cartão

O ícone mudará para .

2) Clique no campo de entrada do leitor de cartões para selecionar os leitores de cartões posteriormente na janela pop-up.

Nota

- Posteriormente, podem ser adicionados até 16 leitores de cartões por cada leitor de cartões.
- Os leitores de cartões apresentados no campo de entrada do leitor de cartões posterior devem estar por ordem de autenticação.

3) Marque a caixa de seleção no**Ativar anti-regresso**coluna vertebral para ativar a função anti-retrocesso.

8.Clique**Guardar**.

Configurar anti-passagem de rota com base na rede

A rota anti-passagem depende da rota de passagem do cartão. Deve configurar o primeiro leitor de cartões e os leitores de cartões posteriormente. Irá autenticar o anti-retorno de acordo com as informações de entrada e saída armazenadas no leitor de cartões.

Execute esta tarefa se necessitar de configurar o antirretorno da rota e autenticar o resultado do antirretorno de acordo com as informações de entrada e saída armazenadas no leitor de cartões.

Passos

1.Clique**Controlo de acesso → Função avançada → Anti-passagem de retorno do controlador cruzado**para entrar na página de configuração anti-passagem do controlador cruzado.

2.Verificação**Ativar Anti-passagem de Controlador Cruzado**para ativar a função.

3.Selecionar**Baseado na rede**como o modo anti-passagem de volta.

4.Selecionar**Rota anti-passagem de regresso**como regra.

5.Selecione um servidor na lista pendente para julgar o anti-repasse.

Nota

- Pode clicar**Apagar registo de passagem de cartão**e selecione o cartão na janela pop-up para eliminar as informações de passagem do cartão em todos os dispositivos.
- Podem ser armazenados até 5.000 registos de passagem de cartões no servidor selecionado.

6.Clique**Selecione controlador de acesso**para selecionar um dispositivo para antirretorno.

Nota

Podem ser adicionados até 64 dispositivos com função anti-passback.

7.Configure o primeiro leitor de cartões e os leitores de cartões posteriores.

1) Na área Leitor de cartões, clique no ícone à esquerda da coluna do leitor de cartões para o definir como o primeiro leitor de cartões.

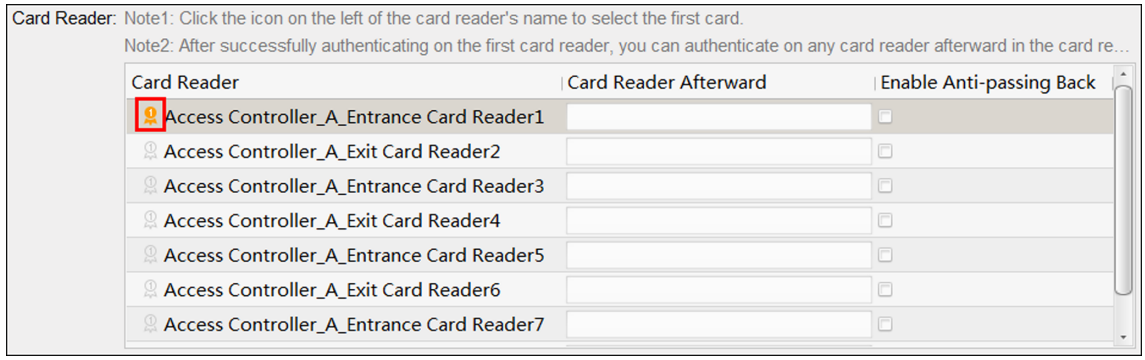


Figura 8-5 Selecione o primeiro cartão

O ícone mudará para .

2) Clique no campo de entrada do leitor de cartões para selecionar os leitores de cartões posteriormente na janela pop-up.

Nota

- Posteriormente, podem ser adicionados até 16 leitores de cartões por cada leitor de cartões.
- Os leitores de cartões apresentados no campo de entrada do leitor de cartões posterior devem estar por ordem de autenticação.

3) Marque a caixa de seleção no**Ativar anti-regresso**coluna vertebral para ativar a função anti-retrocesso.

8.Clique**Guardar**.

Configurar anti-passback de entrada/saída com base no cartão

Pode configurar o leitor de cartões de entrada e o leitor de cartões de saída apenas para entrar e sair, sem configurar o primeiro leitor de cartões e os leitores de cartões posteriormente. Este julgará o anti-retorno de acordo com os registos de entrada e saída do cartão.

Execute esta tarefa se necessitar de configurar o anti-retorno de entrada/saída e julgar o anti-retorno de acordo com os registos de entrada e saída no cartão.

Passos

Nota

Atualmente suporta cartão M1 e o setor não pode ser encriptado. Para obter detalhes sobre a encriptação de setor, consulte***Autenticar encriptação de cartão M1*** .

1.Clique**Controlo de acesso → Função avançada → Anti-passagem de retorno do controlador cruzado**para entrar na página de configuração anti-passagem do controlador cruzado.

2.Verificação**Ativar Anti-passagem de Controlador Cruzado**para ativar a função.

3.Selecionar**Baseado no cartão**como o modo anti-passagem de volta.

4.Selecionar**Entrada/Saída Anti-passagem de Volta**como regra.

5.Defina o ID do setor.

6.Clique**Selecione controlador de acesso**para selecionar um dispositivo para antirretorno.

Nota

Podem ser adicionados até 64 dispositivos com função anti-passback.

7.Na área Leitor de cartões, marque as caixas de selecção no**Ativar anti-regresso**coluna para selecionar o leitor de cartões de entrada e o leitor de cartões de saída.

Nota

Devem ser verificados até um cardador de entrada e um leitor de cartões de saída.

8.Clique**Guardar**.

Configurar anti-passback de entrada/saída com base na rede

Pode configurar o leitor de cartões de entrada e o leitor de cartões de saída apenas para entrar e sair, sem configurar o primeiro leitor de cartões e os leitores de cartões posteriormente. Irá autenticar o anti-retorno de acordo com as informações de entrada e saída do leitor de cartões.

Execute esta tarefa se necessitar de configurar o anti-retorno de entrada/saída e julgar o anti-retorno de acordo com as informações de entrada e saída armazenadas no leitor de cartões.

Passos

1.Clique**Controlo de acesso → Função avançada → Anti-passagem de retorno do controlador cruzado**para entrar na página de configuração anti-passagem do controlador cruzado.

2.Verificação**Ativar Anti-passagem de Controlador Cruzado**para ativar a função.

3.Selecionar**Baseado na rede**como o modo anti-passagem de volta.

4.Selecionar**Entrada/Saída Anti-passagem de Volta**como regra.

5.Selecione um servidor na lista pendente para julgar o anti-repasse.

Nota

- Pode clicar**Apagar registo de passagem de cartão**e selecione o cartão na janela pop-up para eliminar as informações de passagem do cartão em todos os dispositivos.
- Podem ser armazenados até 5.000 registos de passagem de cartões no servidor selecionado.

6.Clique**Selecione controlador de acesso**para selecionar um dispositivo para antirretorno.

Nota

Podem ser adicionados até 64 dispositivos com função anti-passback.

7.Na área Leitor de cartões, marque as caixas de selecção no**Ativar anti-regresso**coluna para selecionar o leitor de cartões de entrada e o leitor de cartões de saída.

Nota

Devem ser verificados até um cardador de entrada e um leitor de cartões de saída.

8.Clique**Guardar**.

Configurar encravamento multiportas

Pode definir o encravamento de múltiplas portas entre várias portas do mesmo dispositivo de controlo de acesso. Para abrir uma das portas, as outras portas devem permanecer fechadas. Isto significa que, no grupo de portas combinadas interligadas, até uma porta pode ser aberta ao mesmo tempo.

Execute esta tarefa quando pretender realizar o encravamento entre múltiplas portas.

Passos

Nota

- A função de encravamento multiportas é suportada apenas pelo dispositivo de controlo de acesso que possui mais do que um ponto de controlo de acesso (portas).
- Tanto a função anti-retorno como a função de encravamento de múltiplas portas podem ser configuradas para um dispositivo de controlo de acessos ao mesmo tempo. Para a configuração da função anti-passback, consulte ***Configurar anti-passback*** .

1.Clique**Controlo de acessos → Função avançada → Encravamento multiportas**para entrar na página Interbloqueio de múltiplas portas.

2.Selecione um dispositivo de controlo de acessos na lista do painel Controller List.

3.Clique**Adicionar**no painel Lista de encravamento de múltiplas portas para abrir a janela Adicionar ponto de controlo de acesso ao encravamento.

4.Selecione ponto(s) de controlo de acesso na lista.

Nota

Podem ser adicionadas até quatro portas numa combinação de encravamento de múltiplas portas.

5.Clique**OK**para adicionar o(s) ponto(s) de controlo de acesso selecionado(s) para encravamento.

A combinação de encravamentos de múltiplas portas configurada será listada no painel Lista de encravamentos de múltiplas portas.

6.º Opcional: Selecione uma combinação de encravamento multiportas adicionada na lista e clique em**Eliminar**para excluir a combinação.

7.Clique**Guardar**.

Configurar a palavra-passe de autenticação

Pode introduzir a palavra-passe de autenticação no teclado do leitor de cartões para abrir a porta após definir a palavra-passe de autenticação.

Execute esta tarefa quando pretender configurar a palavra-passe de autenticação para abrir a porta.

Nota

- A função de palavra-passe de autenticação deve ser suportada pelo dispositivo de controlo de acesso.
- Podem ser adicionados até 500 cartões com palavra-passe de autenticação a um dispositivo de controlo de acesso. A palavra-passe deve ser única e não pode ser igual entre si.

Passos

1.Clique**Controlo de Acessos → Função Avançada → Password de Autenticação**para entrar na página de configuração da palavra-passe de autenticação.

2.Selecione um dispositivo de controlo de acessos na lista do painel Controller List.

Todos os cartões e pessoas aplicados serão apresentados no painel Lista de cartões.

Nota

Para definir e aplicar as permissões ao dispositivo, consulte***Atribuir permissão à pessoa*** .

3.Clique no campo de cada cartão na coluna Palavra-passe para introduzir a palavra-passe de autenticação.

Nota

A palavra-passe de autenticação deve conter 4 a 8 dígitos.

4.Clique**Guardar**no canto superior direito da página Palavra-passe de autenticação para guardar as definições.

A função de palavra-passe de autenticação do cartão será automaticamente ativada. E pode definir o modo de autenticação do leitor de cartões do dispositivo de controlo de acessos como**Cartão ou Palavra-chave de Autenticação**. Consulte ***Configurar o modo e a programação de autenticação do leitor de cartões*** para obter detalhes.

Configurar regra Wiegand personalizada

Com base no conhecimento da regra de carregamento para Wiegand de terceiros, pode definir diversas regras Wiegand personalizadas para a comunicação entre o dispositivo e os leitores de cartões de terceiros.

Antes de começar

Ligue os leitores de cartões de terceiros ao dispositivo.

Execute esta tarefa para configurar a regra Wiegand personalizada para leitores de cartões de terceiros. **Passos**

Nota

- Por predefinição, o dispositivo desativa a função wiegand personalizada. Se o dispositivo ativar a função Wiegand personalizada, todas as interfaces Wiegand no dispositivo utilizarão o protocolo Wiegand personalizado.
- Podem ser configurados até 5 Wiegands personalizados.
- Para obter detalhes sobre o Wiegand personalizado, consulte***Descrições de regras Wiegand personalizadas*** .

1.Clique**Controlo de acessos → Função avançada → Wiegand personalizado**para entrar na página de configuração personalizada do Wiegand.

2.Selecione um Wiegand personalizado à esquerda.

3.Verificação**Ativar**para ativar o Wiegand personalizado.

4.Crie um nome Wiegand.

Nota

São permitidos até 32 caracteres no nome personalizado Wiegand.

5.Clique**Selecione o dispositivo**para selecionar o dispositivo de controlo de acesso para configurar o wiegand personalizado.

6.Defina a paridade de acordo com a propriedade do leitor de cartões de terceiros.

Nota

- São permitidos até 80 bits no comprimento total.
- O bit inicial de paridade ímpar, o comprimento de paridade ímpar, o bit inicial de paridade par e o comprimento de paridade par variam de 1 a 80 bits.
- O bit inicial do ID do cartão, o código do fabricante, o código do site e o OEM devem variar de 1 a 80 bits.

7.Defina a regra de transformação de saída.

1) Clique**Definir regra**para abrir a janela Definir regras de transformação de saída.

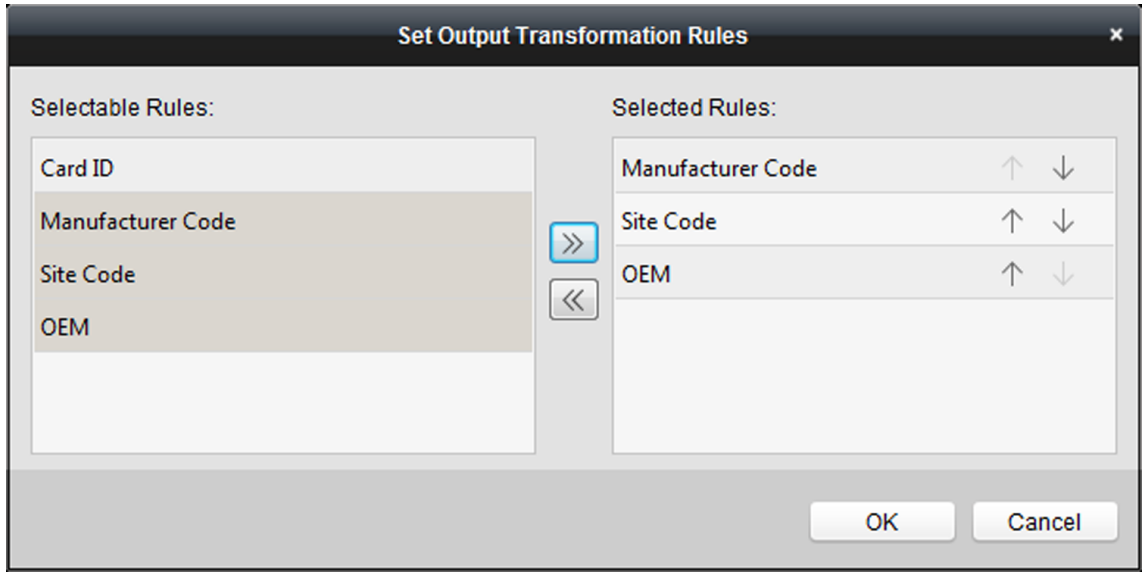


Figura 8-6 Definir regra de transformação de saída

2) Selecione regras na lista da esquerda.

3) Clique para mover as regras selecionadas para a lista da direita.

4)**Opcional:**Clique ou para alterar a ordem das regras.

5) Clique**OK**.

6) No separador Wiegand personalizado, defina o bit de início, o comprimento e o dígito decimal da regra.

8.Clique**Guardar**.

8.1.9 Evento de controlo de acesso de pesquisa

Pode pesquisar os eventos do histórico de controlo de acesso, incluindo eventos remotos e locais, através do cliente.

Pesquisar eventos de controlo de acesso armazenados no cliente local

Pode pesquisar os registos e eventos de acesso ao histórico da base de dados do cliente atual e exportar os registos para o PC local.

Passos

Nota

Pode pesquisar os eventos de controlo de acesso no prazo de três meses.

1.Clique**Controlo de acesso → Pesquisa → Evento de controlo de acesso**para entrar na página de pesquisa do evento de controlo de acesso.

2.Selecione a fonte do evento como**Evento local**.

3.Defina as condições de pesquisa, como dispositivo(s), tipo de evento, hora de ocorrência e assim por diante.

4.Clique**Pesquisa**para começar a pesquisar os eventos de controlo de acesso.

Os eventos de controlo de acesso correspondentes serão apresentados.

5.º Opcional: Depois de pesquisar os eventos, pode executar um ou mais dos seguintes procedimentos.

Ver Pessoa Detalhes	Para o evento de controlo de acessos acionado por pessoa, clique no evento para visualizar os detalhes da pessoa, incluindo o número da pessoa, o nome da pessoa, a organização, o número de telefone, o endereço de contacto e a fotografia.
Ver vinculado Vídeo	Para eventos que contenham vídeo ligado, clique em**Reprodução**coluna para visualizar o ficheiro de vídeo gravado da câmara acionada quando o alarme é acionado.

Nota

Para configurar a câmara acionada, consulte***Configurar ações do cliente para evento de acesso*** .

Evento de exportação Informação	Clique**Exportar**para exportar os resultados da pesquisa para o PC local em ficheiro CSV.

Pesquisar evento de controlo de acesso remoto

Pode pesquisar os registos de eventos de controlo de acesso armazenados no dispositivo de controlo de acesso.

Execute esta tarefa quando necessitar de pesquisar os eventos de controlo de acesso armazenados no dispositivo de controlo de acesso.

Passos

1.Clique**Controlo de acesso → Pesquisa → Evento de controlo de acesso**para entrar na página de pesquisa do evento de controlo de acesso remoto.

2.Selecione a fonte do evento como**Evento Remoto**.

3.Defina as condições de pesquisa conforme pretendido.

4.Clique**Pesquisa**.

Os eventos de controlo de acesso correspondentes serão apresentados.

5.º Opcional: Clique**Exportar**para exportar os resultados da pesquisa para o PC local em ficheiro CSV.

8.1.10 Configurar ligação de alarme de controlo de acesso

Para o dispositivo de controlo de acesso adicionado, pode configurar as ações de ligação, como a ligação de clientes, a ligação de dispositivos ou a ligação entre dispositivos.

Configurar ações do cliente para evento de acesso

Pode atribuir ações de ligação de clientes ao evento configurando uma regra. Por exemplo, quando o evento é detetado, surge um aviso sonoro para notificar o pessoal de segurança.

Passos

Nota

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

1.Clique**Gestão de eventos → Evento de controlo de acesso**.

Os dispositivos de controlo de acesso adicionados serão apresentados na lista de dispositivos.

2.Selecione um recurso na lista de dispositivos.

Os tipos de eventos suportados pelo recurso selecionado serão apresentados.

3.Selecione o(s) evento(s) e clique em**Editar prioridade**para definir a prioridade do(s) evento(s), que pode ser utilizado para filtrar os eventos no Event Center.

4.Defina as ações de ligação do evento.

1) Selecione o(s) evento(s) e clique em**Editar ligação**para definir as ações do cliente quando os eventos são despoletados.

Aviso sonoro

O software cliente emite um aviso sonoro quando o alarme é acionado. Pode selecionar o som do alarme para aviso sonoro.

Nota

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

Vinculação de e-mail

Envie uma notificação por e-mail com as informações do alarme para um ou mais destinatários.

2) Clique**OK**.

5.Ative o evento para que quando o evento for detetado, um evento seja enviado para o cliente e as ações de ligação sejam despoletadas.

6.º Opcional: Clique**Copiar para...**para copiar as definições do evento para outro dispositivo de controlo de acesso, entrada de alarme, porta ou leitor de cartões.

Configurar a ligação de dispositivos para alarme de controlo de acesso

Pode definir as ações de ligação do dispositivo de controlo de acesso para o alarme acionado do dispositivo de controlo de acesso. Quando o alarme é acionado, pode acionar a saída de alarme, a campainha do host e outras ações no mesmo dispositivo.

Execute esta tarefa quando necessitar de configurar a ligação do dispositivo de controlo de acesso ao alarme de controlo de acesso do dispositivo.

Passos

Nota

Deve ser suportado pelo dispositivo.

1.Clique**Gestão de eventos → Vinculação de cartão de evento**.

2.Selecione o dispositivo de controlo de acessos na lista à esquerda.

3.Clique**Adicionar**botão para adicionar uma nova ligação.

4.Selecione a fonte do evento como**Vinculação de eventos**.

5.seleccione o tipo de alarme e o alarme detalhado para definir a ligação.

6.No painel Linkage Target, ative a opção de propriedade para ativar esta ação.

Campainha do anfitrião

O aviso sonoro do dispositivo de controlo de acessos será acionado.

Capturar

A captura em tempo real será acionada.

Gravação

A gravação será acionada.

Nota

O dispositivo deve suportar a gravação.

Campainha do leitor de cartões

O aviso sonoro do leitor de cartões será acionado. **Saída de alarme**

A saída de alarme será acionada para notificação.

Zona

Armar ou desarmar a zona.

Nota

O dispositivo deve suportar a função de zona.

Ponto de controlo de acesso

O estado da porta aberta, fechada, permanece aberta e permanece fechada será acionado.

Nota

- O estado da porta aberta, fechada, permanece aberta e permanece fechada não pode ser acionado ao mesmo tempo.
- A porta alvo e a porta fonte não podem ser a mesma.

Reprodução de áudio

O aviso de áudio será acionado. E o conteúdo de áudio relacionado com o índice de áudio selecionado será reproduzido de acordo com o modo de reprodução configurado.

7.Clique**Guardar**.

8.º Opcional: Depois de adicionar a ligação de dispositivo, pode executar um ou mais dos seguintes procedimentos:

Editar ligação Configurações	Selecione as definições de ligação definidas na lista de dispositivos e poderá editar os seus parâmetros de origem de eventos, incluindo a origem de eventos e o destino de ligação.
Apagar ligação Configurações	Seleccione as definições de ligação definidas na lista de dispositivos e clique em**Eliminar**para o eliminar.

Configurar ações ligadas a dispositivos para passagem de cartão

Pode definir as ações de ligação do dispositivo de controlo de acesso para a passagem do cartão especificada. Quando passa o cartão especificado, pode acionar a saída de alarme, a campainha do host e outras ações no mesmo dispositivo.

Execute esta tarefa quando necessitar de configurar a ligação do dispositivo de controlo de acessos para a ação de passagem do cartão.

Passos

Nota

Deve ser suportado pelo dispositivo.

1.Clique**Gestão de eventos → Vinculação de cartão de evento**.

2.Selecione o dispositivo de controlo de acessos na lista à esquerda.

3.Clique**Adicionar**botão para adicionar uma nova ligação.

4.Selecione a fonte do evento como**Vinculação de cartão**.

5.Introduza o número do cartão ou selecione o cartão na lista pendente.

6.Selecione o leitor de cartões onde o cartão passa para acionar as ações ligadas.

7.No painel Linkage Target, ative a opção de propriedade para ativar esta ação.

Campainha do anfitrião

O aviso sonoro do dispositivo de controlo de acessos será acionado.

Capturar

A captura em tempo real será acionada.

Gravação

A gravação será acionada.

Nota

O dispositivo deve suportar a gravação.

Campainha do leitor de cartões

O aviso sonoro do leitor de cartões será acionado. **Saída de alarme**

A saída de alarme será acionada para notificação.

Zona

Armar ou desarmar a zona.

Nota

O dispositivo deve suportar a função de zona.

Ponto de controlo de acesso

O estado da porta aberta, fechada, permanece aberta e permanece fechada será acionado.

Nota

O estado da porta aberta, fechada, permanece aberta e permanece fechada não pode ser acionado ao mesmo tempo.

Reprodução de áudio

O aviso de áudio será acionado. E o conteúdo de áudio relacionado com o índice de áudio selecionado será reproduzido de acordo com o modo de reprodução configurado.

8.Clique**Guardar**.

Quando o cartão (configurado no Passo 5) passa no leitor de cartões (configurado no Passo 6), pode desencadear as ações ligadas (configuradas no passo 7).

9.º Opcional: Depois de adicionar a ligação de dispositivo, pode executar um ou mais dos seguintes procedimentos:

Apagar ligação **Configurações**	Seleccione as definições de ligação definidas na lista de dispositivos e clique em**Eliminar**para o eliminar.
Editar ligação **Configurações**	Selecione as definições de ligação definidas na lista de dispositivos e poderá editar os seus parâmetros de origem de eventos, incluindo a origem de eventos e o destino de ligação.

Configurar a ligação de ID de funcionário

Quando a pessoa introduz o ID do funcionário no leitor de cartões especificado, pode desencadear ações de ligação a partir de outros dispositivos, como a saída de alarme, a abertura de portas, etc.

Antes de começar

Adicione pessoa. Para obter detalhes, consulte*Gerir informações pessoais*.

Passos

1.Clique**Gestão de eventos → Vinculação de cartão de evento**para entrar na página Vinculação de cartões de evento.

2.Selecione um dispositivo de controlo de acessos na lista à esquerda.

3.Clique**Adicionar**para adicionar uma nova ligação.

4.Selecione a fonte do evento como**Vinculação de ID de funcionário**.

5.Selecione um ID de funcionário na lista pendente.

6.No painel Linkage Target, defina a opção de propriedade para On para ativar a ação de ligação.

Campainha do anfitrião

O aviso sonoro do dispositivo de controlo de acessos será acionado.

Capturar

A captura em tempo real será acionada.

Saída de alarme

A saída de alarme será acionada para notificação. **Ponto de controlo de acesso**

O estado da porta aberta, fechada, permanece aberta e permanece fechada será acionado.

Nota

O estado da porta aberta, fechada, permanece aberta e permanece fechada não pode ser acionado ao mesmo tempo.

7.Clique**Guardar**.

Quando o ID do funcionário for introduzido no leitor de cartões selecionado, este poderá acionar as ações ligadas (configuradas no passo 7).

8.Depois de adicionar a ligação de dispositivo, pode executar um ou mais dos seguintes procedimentos:

Apagar ligação Configurações	Seleccione as definições de ligação definidas na lista de dispositivos e clique em**Eliminar**para o eliminar.
Editar ligação Configurações	Selecione as definições de ligação definidas na lista de dispositivos e poderá editar os seus parâmetros de origem de eventos, incluindo a origem de eventos e o destino de ligação.

Configurar a ligação entre dispositivos

Pode atribuir o acionamento da ação de outro dispositivo de controlo de acesso configurando uma regra quando o evento de controlo de acesso é acionado.

Nota

Deve ser suportado pelo dispositivo.

Configurar a ligação entre dispositivos para evento de controlo de acesso

Quando o evento de controlo de acesso é acionado e detetado, pode acionar ações de ligação de outro dispositivo de controlo de acesso, como a saída de alarme, a abertura de porta, etc. entrada de alarme, evento de porta e evento do leitor de cartões.

Execute esta tarefa quando necessitar de configurar ações de ligação de outro dispositivo de controlo de acesso para evento de controlo de acesso.

Passos

Nota

Os dispositivos devem suportar esta função.

1.Clique**Gestão de eventos → Ligação entre dispositivos**para entrar na interface de configuração de ligação entre dispositivos.

2.Clique**Adicionar**para adicionar uma nova ligação entre dispositivos.

3.Seleccione o tipo de ligação como**Vinculação de eventos**.

4.Defina a origem do evento.

1) Selecione o dispositivo de controlo de acessos como dispositivo de origem do evento.

2) Selecione o tipo de evento de controlo de acesso.

Evento de dispositivo

Selecione o tipo de evento detalhado na lista pendente. **Entrada de alarme**

Selecione o tipo de evento detalhado como evento de zona ou evento de entrada de alarme e selecione o nome da zona ou o nome da entrada de alarme na lista pendente.

Evento de porta

Selecione o tipo de evento detalhado e selecione o ponto de controlo de acesso na lista pendente. **Evento leitor de cartões**

Selecione o tipo de evento detalhado e selecione o leitor de cartões na lista pendente.

5.Defina o dispositivo de controlo de acesso de destino como destino de ligação.

1) Selecione o dispositivo de controlo de acesso na lista pendente como alvo de ligação.

2) Coloque o interruptor em ligado para ativar a ação de ligação.

Saída de alarme

A saída de alarme do dispositivo alvo será acionada para notificação. **Ponto de controlo de acesso**

O estado da porta aberta, fechada, permanece aberta e permanece fechada será acionado.

Nota

O estado da porta aberta, fechada, permanece aberta e permanece fechada não pode ser acionado ao mesmo tempo.

6.Clique**Guardar**.

Configurar a ligação entre dispositivos para passagem de cartão

Quando uma pessoa passa o cartão especificado no leitor de cartões especificado, este pode desencadear ações de ligação a partir de outro dispositivo de controlo de acesso, como a saída de alarme, a abertura de portas, etc.

Execute esta tarefa quando necessitar de configurar outras ações de ligação de dispositivos de controlo de acesso para a passagem de cartão.

Passos

1.Clique**Gestão de eventos → Ligação entre dispositivos**para entrar na interface de configuração de ligação entre dispositivos.

2.Clique**Adicionar**para adicionar uma nova ligação entre dispositivos.

3.Seleccione o tipo de ligação como**Vinculação de cartão**.

4.Defina a origem do evento.

1) Selecione o cartão na lista pendente.

2) Selecione o dispositivo de controlo de acessos como dispositivo de origem do evento.

3) Selecione o leitor de cartões para acionamento.

5.Defina o dispositivo de controlo de acesso de destino como destino de ligação.

1) Selecione o dispositivo de controlo de acesso na lista pendente como alvo de ligação.

2) Coloque o interruptor em ligado para ativar a ação de ligação.

Saída de alarme

A saída de alarme do dispositivo alvo será acionada para notificação. **Ponto de controlo de acesso**

O estado da porta aberta, fechada, permanece aberta e permanece fechada será acionado.

Nota

O estado da porta aberta, fechada, permanece aberta e permanece fechada não pode ser acionado ao mesmo tempo.

6.Clique**Guardar**.

Configurar a ligação entre dispositivos para o ID do funcionário

Quando a pessoa introduz o ID do funcionário no leitor de cartões especificado, pode desencadear ações de ligação a partir de outro dispositivo de controlo de acesso, como a saída de alarme, a abertura de portas, etc.

Execute esta tarefa quando necessitar de configurar outras ações de ligação de dispositivos de controlo de acesso para introduzir o ID do funcionário.

Passos

1.Clique**Gestão de eventos → Ligação entre dispositivos**para entrar na interface de configuração de ligação entre dispositivos.

2.Clique**Adicionar**para adicionar uma nova ligação entre dispositivos.

3.Seleccione o tipo de ligação como**Vinculação de ID de funcionário**.

4.Defina o ID do funcionário.

1) Selecione o dispositivo de controlo de acessos como dispositivo de origem do evento.

2) Selecione o leitor de cartões para acionamento.

5.Defina o dispositivo de controlo de acesso de destino como destino de ligação.

1) Selecione o dispositivo de controlo de acesso na lista pendente como alvo de ligação.

2) Coloque o interruptor em ligado para ativar a ação de ligação.

Saída de alarme

A saída de alarme do dispositivo alvo será acionada para notificação. **Ponto de controlo de acesso**

O estado da porta aberta, fechada, permanece aberta e permanece fechada será acionado.

Nota

O estado da porta aberta, fechada, permanece aberta e permanece fechada não pode ser acionado ao mesmo tempo.

6.Clique**Guardar**.

8.1.11 Gerir o estado do ponto de controlo de acesso

O estado do ponto de controlo de acesso do dispositivo de controlo de acesso adicionado será apresentado em tempo real. Pode verificar o seu estado e os eventos vinculados do ponto de controlo de acesso selecionado. Também pode controlar o estado e definir a duração do estado do ponto de controlo de acesso.

Pontos de controlo de acesso de grupo

Antes de controlar o estado das portas e definir a duração do estado, deve organizar os pontos de controlo de acesso do dispositivo de controlo de acesso em grupos para uma gestão conveniente.

Execute esta tarefa quando necessitar de agrupar os pontos de controlo de acesso para uma gestão conveniente.

Passos

Nota

- Também pode importar as entradas de alarme do dispositivo de controlo de acesso para grupos.
- Para terminal de controlo de acesso de vídeo, pode importar as suas câmaras em grupos.
- Para outras operações detalhadas, consulte*Gestão de Grupo*.

1.Clique**Gestão de dispositivos → Grupo**para entrar na página de gestão do grupo.

2.Adicione um novo grupo.

1) Clique para abrir a janela Adicionar grupo.
2) Crie um nome de grupo.
3)**Opcional:**Verificação**Criar grupo por nome de dispositivo**para criar o novo grupo pelo nome do dispositivo selecionado.
4) Clique**OK**.

3.Importe os pontos de controlo de acesso para o grupo.

1) Clique**Importação**.
2) Clique**Ponto de controlo de acesso**guia.
3) Selecione os pontos de controlo de acesso na lista.
4) Selecione um grupo da lista de grupos.
5) Clique**Importação**para importar os pontos de controlo de acesso selecionados para o grupo.

Estado da porta de controlo

Pode controlar o estado de um único ponto de controlo de acesso (porta), incluindo a abertura de portas, o fecho de portas, a permanência aberta e a permanência fechada.

Execute esta tarefa quando necessitar de controlar o estado da porta.

Passos

1.Clique**Monitor de estado → Estado da porta**para a página de monitorização do estado da porta.

2.Selecione um grupo de controlo de acesso à esquerda.

Nota

Para gerir o grupo de controlo de acesso, consulte*Pontos de controlo de acesso de grupo.*.

Os pontos de controlo de acesso do grupo de controlo de acesso selecionado serão apresentados à direita.

3.Clique no painel Informações de estado para selecionar uma porta.

4.Clique nos seguintes botões listados no painel Informações de estado para controlar a porta.

Porta aberta

Abra a porta uma vez.

Fechar porta

Feche a porta uma vez.

Permaneça aberto

Mantenha a porta aberta.

Permanecer Fechado

Mantenha a porta fechada.

Nota

- Certifique-se de que a porta está ligada a um contacto de porta ou o estado da porta não pode ser apresentado no registo de operação.
- Certifique-se de que o ponto de controlo de acesso não pode ser armado por outro software cliente, ou não conseguirá visualizar as alterações no estado da porta. Apenas um software cliente pode armar o dispositivo e, em seguida, visualizar as alterações do estado da porta, receber as mensagens de alarme do ponto de controlo de acesso.

Verifique os registos de acesso em tempo real

Os registos de acesso de todos os dispositivos de controlo de acesso serão apresentados em tempo real, incluindo registos de passagem de cartões, registos de reconhecimento facial, registos de comparação de impressões digitais, etc.

Passos

1.Clique**Monitor de estado**e pode visualizar os registos de acesso em tempo real.

Os logs dos registos de acesso serão apresentados em tempo real. Pode visualizar os detalhes dos registos, incluindo o número do cartão, o nome da pessoa, a organização, a hora do evento, etc.

2.º Opcional: Verificação**Mostrar registo de acesso mais recente**e o registo de acesso mais recente será selecionado e apresentado no topo da lista de registos.

3.º Opcional: Clique no evento para visualizar os detalhes da pessoa, incluindo fotografias da pessoa captada (fotografia e perfil captados), número da pessoa, nome da pessoa, organização, telefone, endereço de contacto, etc.

Resultado da autenticação

Aceda a resultados como nº de cartão não registado, bem sucedido, etc.

Verifique o alarme de controlo de acesso em tempo real

Os registos de eventos de controlo de acesso serão apresentados em tempo real, incluindo a exceção de dispositivo, evento de porta, evento de leitor de cartões e entrada de alarme.

Execute esta tarefa quando necessitar de verificar os alarmes de controlo de acesso em tempo real.

Passos

1.Clique**Monitor de estado → Alarme de controlo de acesso**para entrar na página de alarme de controlo de acesso em tempo real.

Todos os alarmes de controlo de acesso serão apresentados na lista em tempo real.

2.Clique para visualizar o alarme no E-map.

Nota

Para configurar o ponto de controlo de acesso no E-map, consulte***Exibir ponto de controlo de acesso no Emap*** .

3.º Opcional: Clique em ou para visualizar a visualização em direto ou a imagem captada da câmara acionada quando o alarme é acionado.

Nota

Para configurar a câmara acionada, consulte***Configurar ações do cliente para evento de acesso*** .

4.º Opcional: Selecione o alarme que o cliente pode receber quando o alarme é acionado.

1) Clique**Inscrever-se**.

2) Marque a(s) caixa(s) de seleção para selecionar o(s) alarme(s), incluindo o alarme de exceção do dispositivo, o alarme de evento de porta, o alarme do leitor de cartões e a entrada de alarme.

3) Clique**OK**para guardar as configurações.

8.1.12 Porta de controlo durante a visualização em direto

Durante a visualização em direto, pode controlar o ponto de controlo de acesso ligado à câmara (porta), como abrir, fechar, etc.

Execute esta tarefa quando necessitar de controlar a porta ligada da câmara para abrir ou fechar durante a visualização em direto.

Passos

1.Entrar**Visualização ao vivo**módulo e inicie a visualização em direto de uma câmara.

Nota

Para obter detalhes sobre como iniciar a visualização em direto, consulte para obter detalhes.

2.Ligue a câmara a um ponto de controlo de acesso.

1) Clique com o botão direito do rato na janela de visualização em direto e selecione**Ligação para ponto de controlo de acesso**para abrir a janela Definir ponto de controlo de acesso ligado.

2) Verifique**Ativar**para ativar a ligação.

3) Selecione o ponto de controlo de acesso na lista pendente.

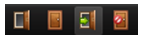
4) Clique**OK**.

Nota

Uma câmara pode ser ligada a apenas um ponto de controlo de acesso; Diferentes câmaras podem ser ligadas ao mesmo ponto de controlo de acesso.

3.Inicie novamente a visualização em direto da câmara para tornar as definições efetivas.

Quatro botões de controlo de porta aparecerão na barra de ferramentas durante a visualização em direto.

4.Clique  para controlar a porta para abrir, fechar, permanecer aberta ou permanecer fechada.

8.1.13 Visualizar ponto de controlo de acesso no mapa eletrónico

Pode adicionar o ponto de controlo de acesso no E-map. Quando o alarme do ponto de controlo de acesso é acionado, pode visualizar a notificação de alarme no E-map, verificar os detalhes do alarme e controlar a porta.

Execute esta tarefa quando necessitar de apresentar o ponto de controlo de acesso no e-map como ponto de acesso.

Passos

Nota

- Para o Terminal de Controlo de Acesso de Vídeo, também pode adicionar a sua câmara ao E-map para visualizar a visualização em direto da câmara.
- Para operações detalhadas do E-map, consulte .

1.Entrar**Mapa eletrónico**módulo.

2.Clique**Editar**na barra de ferramentas do E-map para entrar no modo de edição do mapa.

3.Clique na barra de ferramentas para abrir a janela Adicionar Hot Spot.

4.Selecione o ponto de controlo de acesso a adicionar como ponto de acesso.

5.º Opcional: Edite o nome do hot spot, selecione a cor do nome e selecione o ícone do hot spot clicando duas vezes no campo correspondente.

6.Clique**OK**.

Os ícones das portas são adicionados ao mapa como pontos de acesso e os ícones dos pontos de controlo de acesso adicionados mudam de para na lista de grupos. Pode clicar e arrastar os ícones do ponto de controlo de acesso para mover os pontos de acesso para os locais pretendidos.

7.Depois de adicionar o ponto de controlo de acesso no mapa como ponto de acesso, pode controlar o ponto de controlo de acesso e visualizar o alarme acionado.

1) Clique**Sair do modo de edição**na barra de ferramentas do E-map para entrar no modo de visualização do mapa.

2) Para controlar o ponto de controlo de acesso, pode clicar com o botão direito do rato no ícone do ponto de controlo de acesso no mapa e clicar**Porta aberta**,**Fechar porta**,**Permaneça aberto**, e**Permanecer Fechado**para controlar a porta.

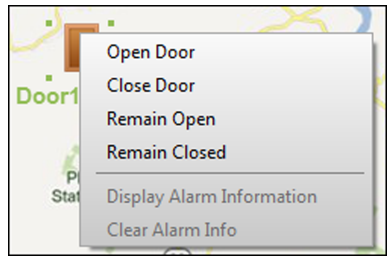


Figura 8-7 Controlo do ponto de controlo de acesso no mapa

3)**Opcional:**Se algum alarme for acionado, um ícone aparecerá e piscará junto ao ponto de acesso (piscará durante 10s). Clique no ícone do alarme para verificar as informações do alarme, incluindo o tipo de alarme e a hora de disparo.

Nota

Para visualizar as informações de alarme no mapa, deve definir a visualização no e-map como a ação de ligação de alarme. Para obter detalhes, consulte***Configurar ações do cliente para evento de acesso*** .

8.2 Configuração Remota (Web)

Configure os parâmetros do dispositivo remotamente.

8.2.1 Gestão de Tempo

Faça a gestão do fuso horário, da sincronização de horários e dos parâmetros de horário de verão do dispositivo.

Fuso horário e sincronização de horário

Na página Dispositivo para gestão, selecione um dispositivo e clique em**Configuração Remota → Sistema → Hora**para entrar no separador Hora.

Pode selecionar um fuso horário, definir parâmetros NTP ou sincronizar a hora manualmente.

Fuso horário

Selecione um fuso horário na lista pendente.

NTP

O dispositivo sincronizará a hora com o NTP automaticamente. Depois de ativar**NTP**, deve definir o endereço do servidor NTP, a porta NTP e o intervalo de sincronização.

Sincronização manual da hora

Depois de ativar**Sincronização manual da hora**, pode definir manualmente a hora do dispositivo.

Se verificar**Sincronizar com a hora do computador**, o**Definir hora**irá apresentar a hora atual do computador. Neste momento, desmarque**Sincronizar com a hora do computador**e clicar em , pode editar a hora do dispositivo manualmente.

Clique**Guardar**para guardar as configurações.

Horário de Verão

Na página Dispositivo para gestão, clique em**Configuração Remota → Sistema → Hora → DST**para entrar no separador DST.

Ative o horário de verão e poderá editar o horário de polarização do horário de verão, o horário de início e o horário de fim do horário de verão. Clique **Guardar**.

8.2.2 Configurações dos parâmetros de rede

Defina os parâmetros de rede do dispositivo, incluindo o tipo de NIC, DHCP e HTTP.

Na página Dispositivo para gestão, clique em**Configuração Remota → Rede → Parâmetros de Rede** para entrar no separador Configurações de parâmetros de rede.

Tipo de placa de rede

Selecione um tipo de NIC na lista pendente. Pode selecionar Autoadaptável, 10M ou 100M.

DHCP

Se desativar a função, tem de definir manualmente o endereço IPv4 do dispositivo, a máscara de sub-rede IPv4, a gateway padrão IPv4, a MTU e a porta.

Se ativar a função, o sistema atribuirá automaticamente o endereço IPv4, a máscara de sub-rede IPv4 e a gateway padrão IPv4 ao dispositivo.

HTTP

Defina a porta HTTP, o endereço do servidor DNS1 e o endereço do servidor DNS2.

8.2.3 Configurações da estratégia de relatório

Pode definir o grupo central para carregar o registo através do protocolo EHome.

Na página Dispositivo para gestão, clique em**Configuração Remota → Rede → Estratégia de Reporte** para entrar no separador Configurações de estratégia de relatório.

Pode definir o grupo central e o sistema transferirá os registos através do protocolo EHome. Clique**Guardar**para guardar as configurações.

Grupo Central

Selecione um grupo central na lista pendente.

Canal principal/canal de reserva

O dispositivo comunicará com a central através do canal principal. Quando ocorre uma exceção no canal principal, o dispositivo e a central comunicarão através do canal de cópia de segurança.

Nota

- N1 refere-se à rede cablada e G1 refere-se ao GPRS.
- Apenas os dispositivos com função 3G/4G suportam a configuração do canal como G1.

8.2.4 Configurações dos parâmetros do centro de rede

Pode definir a central de segurança de notificações, o endereço IP da central, o número da porta, o protocolo (EHome), o nome de utilizador da conta EHome, etc. para transmitir dados através do protocolo EHome.

Na página Dispositivo para gestão, clique em**Configuração remota → Rede → Parâmetros do centro de rede**para entrar no separador Configurações de parâmetros do centro de rede.

Selecione um centro na lista pendente.

Depois de ativar a função, pode definir o tipo de endereço do centro, o endereço IP/nome de domínio e o número da porta, criar um nome de utilizador EHome, etc.

Nota

Se definir o tipo EHome para EHome5.0, também terá de criar uma chave EHome.

Clique**Guardar**.

Após criar as informações do EHome, pode adicionar o dispositivo através do protocolo EHome.

8.2.5 Alterar a palavra-passe do dispositivo

Pode alterar a palavra-passe do dispositivo.

Antes de começar

Certifique-se de que o dispositivo está ativado. Para obter detalhes, consulte*Ativação*.

Passos

1.Na página Dispositivo para gestão, clique em**Configuração Remota → Sistema → Utilizador**para entrar no separador Usuário.

2.Selecione um utilizador e clique em**Editar**para entrar na página Editar.

3.Introduza a palavra-passe antiga, crie uma nova palavra-passe e confirme a nova palavra-passe.

Cuidado

A força da palavra-passe do dispositivo pode ser verificada automaticamente. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your produto. E recomendamos que redefina a sua palavra-passe regularmente, principalmente no sistema de alta segurança, redefinir a palavra-passe mensalmente ou semanalmente pode proteger melhor o seu produto.

A configuração adequada de todas as palavras-passe e outras definições de segurança é da responsabilidade do instalador e/ou utilizador final.

4.Clique**OK**.

Resultado

A palavra-passe do dispositivo foi alterada. Deve introduzir a nova palavra-passe na página Dispositivo para gestão para voltar a ligar o dispositivo.

8.2.6 Definições do modo de segurança

Defina o modo de segurança para iniciar sessão no software cliente.

Na página Dispositivo para gestão, clique em**Configuração Remota → Sistema → Segurança**para entrar no separador Modo de segurança.

Selecione um modo de segurança na lista pendente e clique em**Guardar**. **Modo de segurança**

Elevado nível de segurança para verificação da informação do utilizador ao efetuar login no software cliente.

Modo compatível

A verificação das informações do utilizador é compatível com a versão antiga do software cliente ao iniciar sessão.

8.2.7 Otimizar nome do evento

O sistema carregará o nome do evento otimizado para o software cliente após ativar a função.

Na página Dispositivo para gestão, clique em**Configuração remota → Definições → Evento → Otimizar nome do evento**.

Ativar**Otimizar nome do evento**e clique em**Guardar**.

O sistema pode fazer o upload do nome do evento otimizado para o software cliente.

8.2.8 Definir modo de evento

De acordo com o comprimento do ID do funcionário, pode definir diferentes modos de evento. Diferentes modos de eventos suportam diferentes capacidades de eventos.

Na página Dispositivo para gestão, clique em**Configuração remota → Definições → Evento → Modo de evento**.

Selecione um modo de evento na lista pendente e clique em**Guardar**.

Modo A

Armazenamento de 250.000 eventos do dispositivo. Suporta ID de funcionário de 32 caracteres (combinação entre dígitos e letras minúsculas) ou 16 caracteres (combinação entre letras maiúsculas, letras minúsculas, dígitos e caracteres especiais).

Modo B

Armazenamento de 300.000 eventos do dispositivo. Suporta ID de funcionário de 24 caracteres (combinação entre dígitos e letras minúsculas) ou 12 caracteres (combinação entre letras maiúsculas, letras minúsculas, dígitos e caracteres especiais).

8.2.9 Manutenção do Sistema

Pode reiniciar o dispositivo, restaurá-lo para as definições padrão e atualizá-lo.

Reinício

Na página Dispositivo para gestão, clique em**Configuração Remota → Sistema → Manutenção do Sistema**para entrar no separador Manutenção do sistema. Clique**Reinício**e o dispositivo começa a reiniciar.

Restaurar as definições padrão

Na página Dispositivo para gestão, clique em**Configuração Remota → Sistema → Manutenção do Sistema**para entrar no separador Manutenção do sistema.

Restaurar padrão

Os parâmetros serão restaurados para os padrões, excluindo o endereço IP.

Restaurar tudo

Todos os parâmetros do dispositivo serão restaurados para os valores padrão. O dispositivo deve ser ativado após a restauração.

Atualização

Na página Dispositivo para gestão, clique em**Configuração Remota → Sistema → Manutenção do Sistema**para entrar no separador Manutenção do sistema.

Selecione um tipo de dispositivo na lista pendente e clique em**Navegar**e selecione um ficheiro de atualização do computador local e clique em**Atualização**.

Nota

- Se selecionar Leitor de cartões como tipo de dispositivo, também terá de selecionar um número de leitor de cartões na lista pendente.
- A atualização durará cerca de 2 minutos. Não desligue durante a atualização. Após a atualização, o dispositivo será reiniciado automaticamente.

8.3 Horário e Presença

O módulo Tempo e Presença oferece múltiplas funcionalidades para rastrear e monitorizar quando os colaboradores iniciam e param de trabalhar, e controlo total do horário de trabalho dos colaboradores, como chegadas tardias, saídas antecipadas, tempo de pausa e absentismo.

Nota

Nesta secção apresentamos as configurações antes de obter os relatórios de presença. Os registos de acesso registados após estas configurações serão calculados nas estatísticas.

8.3.1 Gerir agendamento de turnos

O trabalho por turnos é uma prática laboral concebida para aproveitar todas as 24 horas do relógio todos os dias da semana. A prática vê normalmente o dia dividido em turnos, períodos definidos durante os quais diferentes turnos desempenham as suas funções.

Pode definir a programação do departamento, a programação pessoal e a programação temporária.

Adicionar período de tempo

Pode adicionar o período de tempo para a programação de turnos. Execute

esta tarefa quando necessitar de adicionar um período de tempo.

Passos

1.Entre no módulo Tempo e Presença e clique em**Gestão de cronograma de turnos**guia.

2.Clique**Definições de turno → Definições de período de tempo**para entrar na janela Definições do período de tempo.

3.Clique**Adicionar**para entrar na página Adicionar período de tempo.

4.Defina os parâmetros relacionados com o período de tempo.

Participe pelo menos

Defina o tempo mínimo de atendimento.

Nota

Se tiver configurado os diferentes leitores de cartões como pontos de verificação de início e de fim do trabalho, pode verificar**O tempo de ausência não está incluído nas horas de trabalho efetivas**para excluir o tempo de ausência do horário de trabalho.

Check-in/Check-out obrigatório

Marque as caixas de seleção e defina o período válido para o check-in ou check-out. **Marcar como**

atrasado/Marcar como licença antecipada

Defina o período de licença tardia ou antecipada.

Apagar período de pausa da duração do trabalho

Marque a caixa de selecção e defina o período de intervalo eliminado.

Nota

Podem ser definidos até 3 períodos de pausa.

Definir como período de pagamento por tempo

Marque a caixa de seleção e defina a taxa de pagamento e a unidade de tempo mínimo.

5.Clique**Guardar**.

O período de tempo adicionado é listado no painel esquerdo da janela.

Adicionar turno

Pode adicionar o turno à programação de turnos.

Antes de começar

Adicione primeiro um período de tempo. Ver***Adicionar período de tempo*** para obter detalhes.

Execute esta tarefa quando necessitar de adicionar turno.

Passos

1.Entre no módulo Tempo e Presença.

2.Clique**Gestão de agendamento de turno → Configurações de turno → Turno**para entrar na janela Definições de turno.

3.Clique**Adicionar**para entrar na página Adicionar turno.

4.Introduza o nome do turno.

5.Selecione o período de turno na lista pendente.

6.Selecione o período de tempo adicionado e clique na barra de tempo para aplicar o período de tempo.

7.Clique**Guardar**.

As listas de turnos adicionadas no painel esquerdo da janela.

Definir cronograma do departamento

Pode definir o horário de turnos para um departamento e todas as pessoas do departamento receberão o horário de turnos.

Antes de começar

No módulo Ponto e Presença, a lista de departamentos é a mesma da organização no módulo de Controlo de Acessos. Deve primeiro adicionar departamentos e pessoas no módulo de Controlo de Acesso. Ver ***Gerir organização*** e***Gerir informações pessoais*** para obter detalhes.

Execute esta tarefa quando necessitar de definir a programação do departamento.

Passos

1. Clique**Tempo e Presença → Gestão de Agenda de Turnos**para entrar na página Gestão de agendamento de turnos.
2. Selecione um departamento e clique**Cronograma do Departamento**para abrir a janela Agenda do Departamento.
3. Verificação**Tempo e presença**.

   Todas as pessoas do departamento esperam que os excluídos da frequência apliquem o horário de frequência.
4. Selecione o turno na lista pendente.
5. Defina a data de início e a data de fim.
6. Defina outros parâmetros para o horário, incluindo Check-in não obrigatório, Check-out não obrigatório, Em vigor para feriados, Em vigor para horas extraordinárias ou Em vigor para horários de vários turnos.

Nota

Depois de verificar o**Eficaz para horários de múltiplos turnos**, pode selecionar o(s) período(s) efetivo(s) dos períodos adicionados para as pessoas do departamento.

Programações de múltiplos turnos

Contém mais de um período de tempo. A pessoa poderá fazer o check in/out em qualquer um dos horários e o atendimento será eficaz.
Se a escala de turnos múltiplos contiver três períodos de tempo: 00h00 às 07h00, 08h00 às 15h00 e 16h00 às 23h00. A comparência do adotante deste regime de turnos múltiplos será efetiva em qualquer dos três períodos de tempo. Caso a pessoa faça o check-in às 07h50, será aplicado o horário mais próximo das 08h00 às 15h00 para a comparência da pessoa.

7. **Opcional:**Verificação**Definir como padrão para todas as pessoas do departamento**.

   Todas as pessoas do departamento utilizarão esta programação de turnos por defeito.
8. **Opcional:**Se o departamento selecionado contiver subdepartamentos, poderá verificar**Definir como horário de turno para todos os subdepartamentos**para aplicar a programação do departamento aos seus subdepartamentos.
9. Clique**Guardar**.

Definir agendamento pessoal

Pode atribuir a programação de turnos a uma pessoa. Também pode visualizar e exportar os detalhes da programação pessoal.

Antes de começar

Adicione departamento e pessoa no módulo de Controlo de Acessos. Ver ***Gerir organização*** e ***Gerir informações pessoais*** para obter detalhes.

Execute esta tarefa quando necessitar de definir a programação pessoal.

Passos

1. Entre no módulo Tempo e Presença.

2. Clique **Gestão de cronograma de turnos** para entrar na página Gestão de agendamento de turnos.

3. Selecione o departamento e selecione uma pessoa.

4. Clique **Agenda Pessoal** para abrir a janela Agenda Pessoal.

5. Verificação **Tempo e presença**.

A pessoa configurada aplicará o agendamento de atendimento.

6. Selecione o turno na lista pendente.

7. Defina a data de início e a data de fim.

8. Defina outros parâmetros para o horário, incluindo Check-in não obrigatório, Check-out não obrigatório, Efetivo para feriados, Efetivo para horas extraordinárias e Efetivo para horários de vários turnos.

Nota

Depois de verificar o **Eficaz para horários de múltiplos turnos**, pode selecionar o(s) período(s) efetivo(s) dos períodos adicionados para as pessoas do departamento.

Programações de múltiplos turnos

Contém mais de um período de tempo. A pessoa poderá fazer o check in/out em qualquer um dos horários e o atendimento será eficaz.
Se a escala de turnos múltiplos contiver três períodos de tempo: 00h00 às 07h00, 08h00 às 15h00 e 16h00 às 23h00. A comparência do adotante deste regime de turnos múltiplos será efetiva em qualquer dos três períodos de tempo. Caso a pessoa faça o check-in às 07h50, será aplicado o horário mais próximo das 08h00 às 15h00 para a comparência da pessoa.

9. Clique **Guardar**.

Definir programação temporária

Pode adicionar um horário temporário para a pessoa e a pessoa receberá o horário do turno temporariamente. Também pode visualizar e exportar os detalhes da programação temporária.

Antes de começar

Adicione departamento e pessoa no módulo de Controlo de Acessos e defina a regra de presença para a pessoa. Ver ***Gerir organização*** e ***Gerir informações pessoais*** para obter detalhes.

Execute esta tarefa quando necessitar de definir um agendamento temporário.

Passos

Nota

A programação temporária tem maior prioridade do que a programação do departamento e a programação pessoal.

1. Entre no módulo Tempo e Presença.

2. Clique **Gestão de cronograma de turnos** separador para entrar na página Gestão de agendamento de turnos.

3. Selecione o departamento e selecione uma pessoa.

4. Clique **Cronograma Temporário** para abrir a janela Programação temporária.

5. Clique para definir a data do turno.

6. Selecione o período de tempo.

7. Clique na barra de tempo para aplicar o período de tempo à data selecionada.

8.º Opcional: Clique **Configurações avançadas** e selecione regras de frequência avançadas para a programação temporária.

9. Clique **Adicionar**.

Verifique e edite a programação de turnos

Pode verificar os detalhes da programação de turnos e editar a programação. Execute esta

tarefa quando necessitar de verificar e editar a programação de turnos.

Passos

1. Entre no módulo Tempo e Presença.

2. Clique **Gestão de cronograma de turnos** separador para entrar na página Gestão de agendamento de turnos.

3. Selecione o departamento e a(s) pessoa(s) correspondente(s).

4. Clique **Ver** para abrir a janela Detalhes da programação de turnos.

Os detalhes da programação de turno são apresentados.

5. Edite os detalhes normais da programação.

1) Clique **Horário normal** guia.

2) Selecione um turno na lista pendente.

3) Clique **Configurações das regras de presença** para abrir a janela Definições das regras de presença.

4) Selecione as regras de atendimento conforme pretendido e clique **OK**.

5) Clique para definir a data de entrada em vigor.

6) Clique **Guardar**.

6.º Opcional: Clique **Cronograma Temporário** e execute uma das seguintes operações.

Adicionar	Adicione a programação temporária para a pessoa selecionada.
	Edite o período de tempo.
	Apague a programação temporária.

8.3.2 Corrigir manualmente o registo de check-in/out

Se o estado de atendimento não estiver correto, pode corrigir manualmente o registo de check-in ou check-out. Também pode editar, eliminar, pesquisar ou exportar o registo de check-in ou check-out.

Antes de começar

- Deve adicionar organizações e pessoas no módulo de Controlo de Acesso. Para obter detalhes, consulte ***Gerir organização*** e ***Gerir informações pessoais*** .
- O estado de presença da pessoa está incorreto.

Execute os passos seguintes para corrigir o registo de check-in ou check-out.

Passos

1. Entre no módulo Tempo e Presença.

2. Clique **Tratamento de atendimento → Correção de check-in/out** para entrar na página Correção de check-in/out.

3. Clique **Adicionar** para entrar na janela Adicionar correção de check-in/out.

4. Defina os parâmetros de correção de check-in/out.

- Verificação **Check-in** e defina a hora real de início do trabalho.
- Verificação **Confira** e defina o horário real de fim do trabalho.

5. Clique **Nome do funcionário** campo e selecione a pessoa para correção.

6.º Opcional: Introduza as informações da observação conforme pretendido.

7. Clique **Adicionar**.

8.º Opcional: Após adicionar a correção de check-in/out, execute uma das seguintes operações.

Pesquisa	Defina as condições de pesquisa e pesquise a correção.
Modificar	Edite a correção de check-in/out selecionada.
Eliminar	Apague a correção de check-in/out selecionada. Gere e
Relatório	visualize o relatório de correção de check-in/out. Exporte os
Exportar	detalhes de correção de check-in/out para o PC local.

Nota

Os detalhes exportados são guardados no formato CSV.

8.3.3 Adicionar licença e viagem de negócios

Pode adicionar uma aplicação de licença e viagem de negócios quando o colaborador quiser pedir licença ou fazer uma viagem de negócios.

Antes de começar

Deve adicionar organizações e pessoas no módulo de Controlo de Acesso. Para obter detalhes, consulte ***Gerir organização*** e ***Gerir informações pessoais*** .

Execute os passos seguintes quando quiser adicionar um pedido de licença ou de viagem de negócios.

Passos

1.Entre no módulo Tempo e Presença.

2.Clique**Serviço → Saída e Viagem de Negócios**para entrar na página Licença e viagem de negócios.

3.Clique**Adicionar**para abrir a janela Adicionar aplicação de licença e viagem de negócios.

4.Selecione o tipo de licença e de viagem de negócios na lista pendente.

Nota

Pode definir o tipo de licença em Definições avançadas. Para obter detalhes, consulte***Configurar tipo de licença*** .

5.Clique e defina o período da sua licença ou viagem de negócios.

6.Clique**Nome do funcionário**arquivado e selecione a pessoa para a aplicação na janela pop-up Adicionar Pessoa.

7.º Opcional: Introduza as informações da observação conforme pretendido.

8.Clique**Adicionar**.

As férias e viagens de negócios adicionadas são apresentadas na página Licença e viagem de negócios.

9.º Opcional: Após adicionar a aplicação de licença e viagem de negócios, execute uma das seguintes operações.

Modificar	Selecione a licença e a viagem de negócios e clique**Modificar**para editar o pedido de licença ou de negócio.
Eliminar	Selecione a licença e a viagem de negócios e clique**Eliminar**para excluir o pedido de licença ou de viagem de negócios.
Relatório	Clique**Relatório**para gerar o relatório de férias ou viagem de negócios. Clique**Exportar**para
Exportar	exportar os detalhes da licença ou da viagem de negócios para o PC local.

Nota

Os detalhes exportados são guardados no formato CSV.

8.3.4 Calcular os Dados de Presença

É necessário calcular os dados de assiduidade antes de pesquisar e visualizar a visão geral dos dados de assiduidade, dados detalhados de assiduidade dos colaboradores, dados de assiduidade anormal dos colaboradores, dados de horas extraordinárias dos colaboradores e registo de passagem do cartão.

Calcular automaticamente os dados de presença

Pode definir um horário para que o cliente possa calcular os dados de atendimento automaticamente no horário que configurou todos os dias.

Execute esta tarefa se precisar de definir o horário para que o cliente calcule os dados de atendimento automaticamente.

Passos

Nota

Calculará os dados de atendimento até ao dia anterior.

1. Entre no módulo Tempo e Presença.

2. Clique **Tratamento de Presença → Cálculo de Presença** para entrar na página de cálculo do registo de assiduidade.

3. No painel Calcular Presença Automática, defina a hora a que pretende que o cliente calcule os dados todos os dias.

4. Clique **Guardar**.

Calcular manualmente os dados de presença

Pode calcular os dados de frequência manualmente definindo o intervalo de dados.

Execute os passos seguintes para calcular manualmente os dados de frequência.

Passos

1. Entre no módulo Tempo e Presença.

2. Clique **Tratamento de Presença → Cálculo de Presença** para entrar na página de cálculo do registo de assiduidade.

3. No painel Calcular presença manualmente, defina a hora de início e a hora de fim para definir o intervalo de dados de presença.

4. Clique **Calcular**.

Nota

Só pode calcular os dados de atendimento dentro de três meses.

8.3.5 Definir definições avançadas

Pode definir as definições avançadas para a frequência, incluindo as definições básicas de frequência, definições de regra de frequência, definições de ponto de verificação de frequência, definições de feriados e definições de tipo de licença.

Configurar parâmetros básicos

Pode configurar os parâmetros básicos de atendimento, incluindo o dia de início de cada semana, a data de início de cada mês e o dia não útil.

Execute os passos seguintes para configurar os parâmetros básicos de atendimento.

Passos

1.Entre no módulo Tempo e Presença.

2.Clique**Definições avançadas → Definições básicas**para entrar na página Definições básicas.

3.Defina o dia de início de cada semana e a data de início de cada mês na lista pendente.

4.Defina as definições de dia não útil.

Definir como dia não útil

Marque as caixas de seleção para definir as datas como dias não úteis.

Definir a cor do dia não útil no relatório

Selecione a cor na janela Selecionar cor. Os dias não úteis no relatório serão marcados como a cor configurada.

Definir marca de dia não útil no relatório

Introduza a marca e o campo do dia não útil no relatório será apresentado com a marca.

5.Defina o tipo de autenticação, o que significa que o cliente calculará os dados de atendimento registados com base no tipo de autenticação selecionado.

6.Clique**Guardar**.

Configurar regra de presença

Pode configurar a regra de presença para todos os turnos antes de definir o turno. Pode configurar a regra de presença/ausência, check-in/out e horas extra.

Execute os passos seguintes para configurar a regra de presença.

Passos

Nota

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

1.Entre no módulo Tempo e Presença.

2.Clique**Definições avançadas → Definições de regras de presença**para entrar na página Definições das regras de presença.

3.Defina os parâmetros das regras, incluindo os parâmetros de presença/ausência, os parâmetros de check-in/out e os parâmetros de horas extraordinárias.

4.º Opcional: Verificação**Dia de trabalho não programado**e definir a regra das horas extraordinárias para os dias não úteis.

5.Clique**Guardar**.

Configurar ponto de verificação de presença

Pode definir o(s) leitor(es) de cartões do ponto de controlo de acesso como ponto de verificação de atendimento, para que a passagem do cartão no(s) leitor(es) de cartões seja válida para atendimento.

Antes de começar

Deve adicionar um dispositivo de controlo de acesso antes de configurar o ponto de verificação de presença. Para obter detalhes, consulte ***Adicionar dispositivo*** .

Execute os seguintes passos para definir o leitor de cartões do ponto de controlo de acesso como ponto de verificação de presença.

Passos

Nota

Por predefinição, todos os leitores de cartões dos dispositivos de controlo de acesso adicionados estão configurados como ponto de verificação de presença.

1. Entre no módulo Tempo e Presença.

2. Clique **Definições avançadas → Definições de ponto de verificação de presença** para entrar na página Definições do ponto de verificação de presença.

3.º Opcional: Desmarque **Definir todos os leitores de cartões como pontos de verificação**.

Apenas os leitores de cartões da lista serão definidos como pontos de verificação de atendimento.

4. Clique para entrar na janela Adicionar ponto de verificação de presença.

5. Defina os parâmetros relacionados.

Nome do ponto de verificação

Personalize um nome para o ponto de verificação.

Leitor de cartões

Selecione o leitor de cartões na lista pendente como ponto de verificação de presença. **Função de ponto de verificação**

Selecione a função do ponto de verificação na lista pendente. Pode definir o ponto de verificação como ponto de verificação de início/fim de trabalho, ponto de verificação de início de trabalho ou ponto de verificação de fim de trabalho.

Localização da porta

Introduza o nome do local da porta.

Descrição do ponto de verificação

Introduza as descrições do ponto de verificação conforme pretendido.

6. Clique **Adicionar**.

O ponto de verificação de presença adicionado é apresentado na lista.

7.º Opcional: Depois de adicionar o ponto de verificação de presença, execute uma das seguintes operações.

Edite as informações do ponto de verificação de presença.

Apague o ponto de verificação de presença na lista.

Configurar feriado

Pode adicionar o feriado durante o qual o check-in ou check-out não será registado.

Adicionar feriado com data fixa

Pode configurar um feriado que só terá efeito uma vez. Execute esta tarefa se pretender configurar um feriado com data fixa.

Passos

1. Entre no módulo Tempo e Presença.

2. Clique **Definições avançadas → Definições de feriados** para entrar na página Definições de feriados.

3. Clique + para abrir a janela Adicionar feriado.

4. Clique **Data Fixa** guia.

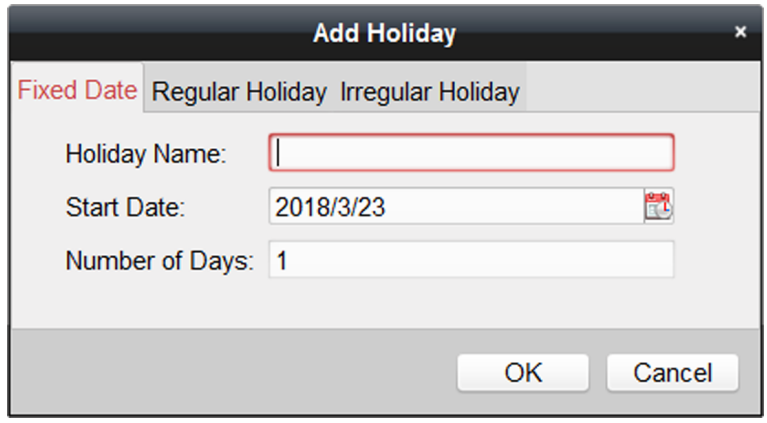


Figura 8-8 Adicionar feriado com data fixa

5. Personalize um nome para o feriado.

6. Defina a data de início como o primeiro dia do feriado.

7. Defina o número de dias do feriado.

8.º Opcional: Após adicionar o feriado, realize uma das seguintes operações.

- Edite as informações do feriado. Apague o feriado da lista de feriados.

Adicionar feriado normal

Pode configurar um feriado que entrará em vigor anualmente em dias normais durante o período de vigência, como o Dia de Ano Novo, o Dia da Independência, o Dia de Natal, etc.

Execute esta tarefa se precisar de adicionar um feriado normal.

Passos

1. Entre no módulo Tempo e Presença.

2. Clique **Definições avançadas → Definições de feriados** para entrar na página Definições de feriados.

3. Clique + para abrir a janela Adicionar feriado.

4. Clique **Feriado normal** guia.

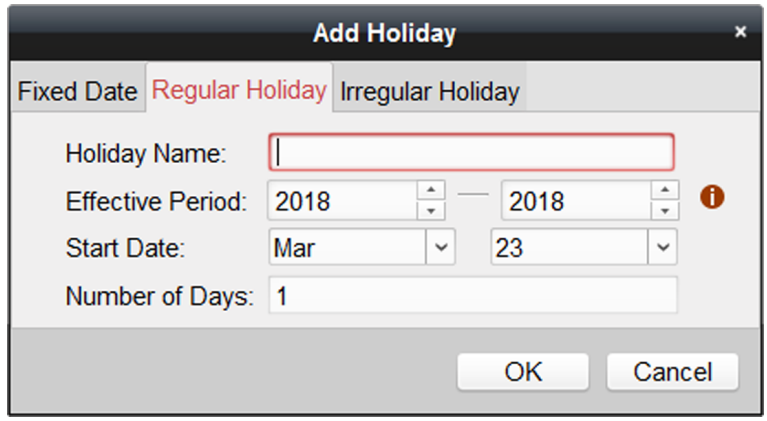


Figura 8-9 Adicionar feriado regular

5.Defina os parâmetros de feriado.

Data de início

O primeiro dia do feriado.

Período Efetivo

Os anos durante os quais a data de início do feriado entrará em vigor. Por exemplo, se o período de vigência do feriado for definido como 2018 a 2019, e a data de início for definida como 31 de dezembro e o número de dias for 3, o feriado será de 31/12/2018 a 02/01/ 2019, 31/12/2019 a 02/01/2020.

6.Clique**OK**.

7.º Opcional: Após adicionar o feriado, realize uma das seguintes operações.

Edite as informações do feriado. Apague o feriado da lista de feriados.

Adicionar feriado irregular

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

Execute esta tarefa se desejar adicionar um feriado irregular.

Passos

1.Entre no módulo Tempo e Presença.

2.Clique**Definições avançadas → Definições de feriados**para entrar na página Definições de feriados.

3.Clique para abrir a janela Adicionar feriado.

4.Clique**Feriado Irregular**guia.

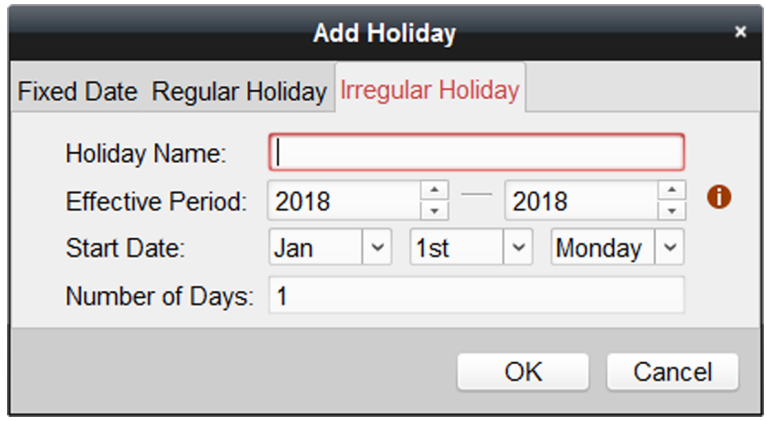


Figura 8-10 Adicionar feriado irregular

5.Defina os parâmetros de feriado.

Data de início

O primeiro dia do feriado.

Período Efetivo

Os anos durante os quais a data de início do feriado entrará em vigor. Por exemplo, se o período de vigência do feriado for definido como 2018 a 2019, e a data de início for definida como 31 de dezembro e o número de dias for 3, o feriado será de 31/12/2018 a 02/01/ 2019, 31/12/2019 a 02/01/2020.

Nota

Se um feriado ultrapassar os dois anos e o período efetivo

6.Clique**OK**.

7.º Opcional: Após adicionar o feriado, realize uma das seguintes operações.

Edite as informações do feriado. Apague o

feriado da lista de feriados.

Configurar tipo de licença

Pode personalizar o tipo de licença de acordo com as necessidades reais. Por predefinição, existem três tipos principais de licença: licença, dia de folga e saída em negócios.

Execute os passos seguintes para adicionar, editar ou eliminar o tipo de licença.

Passos

1.Entre no módulo Tempo e Presença.

2.Clique**Definições avançadas → Sair das definições de tipo**para entrar na página Definições do tipo de licença.

3.Clique para adicionar um tipo de licença principal no painel esquerdo.

4.º Opcional: Execute uma das seguintes operações para o tipo de licença principal.

Edite o tipo de licença principal.

Apague o tipo de licença principal.

5.Clique para adicionar um tipo de licença secundária no painel direito.

6.º Opcional: Execute uma das seguintes operações para o tipo de licença principal.

Edite o tipo de licença secundária.

Apague o tipo de licença secundária.

8.3.6 Visualizar Relatório de Presença

Depois de calcular os dados de frequência, pode verificar o resumo de frequência, os detalhes de frequência, a frequência anormal, as horas extraordinárias, os registos de passagem de cartão e os relatórios com base nos dados de frequência calculados.

Obtenha uma visão geral dos dados de assiduidade dos colaboradores

Pode pesquisar os tempos de presença necessários, os tempos de presença reais, os horários atrasados, os tempos de licença antecipada, os tempos de ausência, os tempos de excesso de trabalho, os tempos de licença, etc. obter uma visão geral dos dados de presença dos colaboradores.

Antes de começar

- Deve adicionar organizações e pessoas no módulo de Controlo de Acesso e as pessoas passaram o cartão. Para obter detalhes, consulte***Gerir organização*** e***Gerir informações pessoais*** .
- Calcule os dados de atendimento.

Nota

- O cliente calculará automaticamente os dados de atendimento do dia anterior à 1h da manhã do dia seguinte.
- Mantenha o cliente a funcionar à 1h ou não conseguirá calcular automaticamente os dados de atendimento do dia anterior. Se não for calculado automaticamente, pode calcular os dados de frequência manualmente. Para obter detalhes, consulte***Calcular manualmente os dados de presença*** .

Execute os passos seguintes para pesquisar todos os dados de assiduidade dos colaboradores num período de tempo.

Passos

1.Entre no módulo Tempo e Presença.

2.Clique**Estatísticas de frequência → Resumo de frequência**para entrar na página Resumo de presença.

3.Selecione um departamento na lista pendente.

4.º Opcional: Introduza o nome da pessoa para pesquisa.

5.Selecione a data de início e a data de fim da frequência que pretende pesquisar.

6.º Opcional: Clique**Reiniciar**para repor todas as condições de pesquisa e editá-las novamente.

7.Clique**Pesquisa**.

O resultado é apresentado na página. Pode visualizar os tempos de assiduidade exigidos ao colaborador, os tempos de assiduidade reais, os horários de atraso, os tempos de licença antecipada, os tempos de ausência, os tempos de excesso de trabalho, os tempos de licença, etc.

8.º Opcional: Após pesquisar o resultado, execute uma das seguintes operações.

Relatório Gere o relatório de assiduidade.

Exportar Exporte os resultados para o PC local.

Pesquisar dados detalhados de assiduidade dos colaboradores

Pode pesquisar todos os dados de presença do funcionário com detalhe, incluindo a data de presença, o turno da pessoa, período de tempo, estado de início do trabalho, estado de término do trabalho, horário de check-in, horário de check-in out, período de atraso, período de licença antecipada, período de presença, período de ausência, período de licença e período de excesso de trabalho.

Antes de começar

- Deve adicionar organizações e pessoas no módulo de Controlo de Acesso e as pessoas passaram o cartão. Para obter detalhes, consulte ***Gerir organização*** e ***Gerir informações pessoais*** .
- Calcule os dados de atendimento.

Nota

- O cliente calculará automaticamente os dados de atendimento do dia anterior à 1h da manhã do dia seguinte.
- Mantenha o cliente a funcionar à 1h ou não conseguirá calcular automaticamente os dados de atendimento do dia anterior. Se não for calculado automaticamente, pode calcular os dados de frequência manualmente. Para obter detalhes, consulte ***Calcular manualmente os dados de presença*** .

Execute os passos seguintes para pesquisar os dados detalhados de assiduidade do funcionário.

Passos

1. Entre no módulo Tempo e Presença.

2. Clique **Estatísticas de frequência → Detalhes de frequência** para entrar na página Detalhes da participação.

3. Selecione um departamento na lista pendente.

4.º Opcional: Introduza o nome da pessoa para pesquisa.

5. Selecione a data de início e a data de fim da frequência que pretende pesquisar.

6.º Opcional: Verifique o estado de atendimento que pretende pesquisar.

7.º Opcional: Clique **Reiniciar** para repor todas as condições de pesquisa e editá-las novamente.

8. Clique **Pesquisa**.

As informações detalhadas dos detalhes do serviço são apresentadas abaixo. Pode visualizar a data de comparência, o turno da pessoa, período de tempo, estado de início do trabalho, estado de término do trabalho, horário de check-in, horário de check-out, período de atraso, período de licença antecipada, período de comparência, período de ausência, período de licença e período de excesso de trabalho.

9.º Opcional: Após pesquisar o resultado, execute uma das seguintes operações.

Relatório Gere o relatório de assiduidade.

ExportarExporte os resultados para o PC local.

Pesquisar dados de frequência anormal de colaboradores

Pode pesquisar e obter as estatísticas dos dados de comparência anormal do funcionário, incluindo o número, nome e departamento dos funcionários, tipo anormal, hora de início/fim e data de comparência.

Antes de começar

- Deve adicionar organizações e pessoas no módulo de Controlo de Acesso e as pessoas passaram o cartão. Para obter detalhes, consulte***Gerir organização*** e***Gerir informações pessoais***
- Calcule os dados de atendimento.

Nota

- O cliente calculará automaticamente os dados de atendimento do dia anterior à 1h da manhã do dia seguinte.
- Mantenha o cliente a funcionar à 1h ou não conseguirá calcular automaticamente os dados de atendimento do dia anterior. Se não for calculado automaticamente, pode calcular os dados de frequência manualmente. Para obter detalhes, consulte***Calcular manualmente os dados de presença*** .

Execute os passos seguintes para pesquisar os dados de frequência anormal do funcionário.

Passos

1.Entre no módulo Tempo e Presença.

2.Clique**Estatísticas de Presença → Presença Anormal**para entrar na página Presença anormal.

3.Selecione um departamento na lista pendente.

4.º Opcional: Introduza o nome da pessoa para pesquisa.

5.Selecione a data de início e a data de fim da frequência que pretende pesquisar.

6.º Opcional: Clique**Reiniciar**para repor todas as condições de pesquisa e editá-las novamente.

7.Clique**Pesquisa**.

O resultado é apresentado abaixo. Pode visualizar o número do funcionário, o nome da pessoa, o departamento a que pertence, o tipo anormal, a hora de início anormal, a hora de fim anormal e a data anormal.

8.º Opcional: Após pesquisar o resultado, execute uma das seguintes operações.

Relatório	Gere o relatório de assiduidade.
Exportar	Exporte os resultados para o PC local.

Pesquisar dados de horas extraordinárias de funcionários

Pode pesquisar e obter estatísticas de estado de horas extraordinárias do funcionário selecionado no período especificado. E pode verificar as informações detalhadas das horas extraordinárias, incluindo o número, nome e departamento dos colaboradores, data de comparência, duração das horas extraordinárias e tipo de horas extraordinárias.

Antes de começar

- Deve adicionar organizações e pessoas no módulo de Controlo de Acesso e as pessoas passaram o cartão. Para obter detalhes, consulte***Gerir organização*** e***Gerir informações pessoais*** .
- Calcule os dados de atendimento.

Nota

- O cliente calculará automaticamente os dados de atendimento do dia anterior à 1h da manhã do dia seguinte.
- Mantenha o cliente a funcionar à 1h ou não conseguirá calcular automaticamente os dados de atendimento do dia anterior. Se não for calculado automaticamente, pode calcular os dados de frequência manualmente. Para obter detalhes, consulte***Calcular manualmente os dados de presença*** .

Execute os passos seguintes para pesquisar os dados de horas de trabalho suplementar.

Passos

1.Entre no módulo Tempo e Presença

2.Clique**Estatísticas de Presença → Pesquisa de Horas Extra**para entrar na página Pesquisa de horas extraordinárias.

3.Selecione um departamento na lista pendente.

4.º Opcional: Introduza o nome da pessoa para pesquisa.

5.Selecione a data de início e a data de fim da frequência que pretende pesquisar.

6.º Opcional: Clique**Reiniciar**para repor todas as condições de pesquisa e editá-las novamente.

7.Clique**Pesquisa**.

As informações detalhadas do resultado do trabalho suplementar são apresentadas abaixo. Pode visualizar o número do funcionário, o nome da pessoa, o departamento a que pertence, a data das horas extraordinárias, a duração das horas extraordinárias e o tipo de horas extraordinárias.

8.º Opcional: Após pesquisar o resultado, execute uma das seguintes operações.

Relatório	Gere o relatório de assiduidade.
Exportar	Exporte os resultados para o PC local.

Verifique os registos de passagem de cartão dos funcionários

Pode pesquisar e visualizar os registos de passagem do cartão dos colaboradores quando quiser verificar os detalhes da passagem do cartão dos colaboradores.

Antes de começar

- Deve adicionar organizações e pessoas no módulo de Controlo de Acesso e as pessoas passaram o cartão. Para obter detalhes, consulte***Gerir organização*** e***Gerir informações pessoais*** .
- Calcule os dados de atendimento.

Nota

- O cliente calculará automaticamente os dados de atendimento do dia anterior à 1h da manhã do dia seguinte.
- Mantenha o cliente a funcionar à 1h ou não conseguirá calcular automaticamente os dados de atendimento do dia anterior. Se não for calculado automaticamente, pode calcular os dados de frequência manualmente. Para obter detalhes, consulte***Calcular manualmente os dados de presença*** .

Execute os passos seguintes para pesquisar e visualizar o registo de passagem do cartão.

Passos

1.Entre no módulo Tempo e presença.

2.Clique**Estatísticas de presença → Registo de passagem de cartão**para entrar na página Registo de passagem de cartão.

3.Configure as condições de pesquisa, incluindo o departamento do funcionário, o nome do funcionário ou a data de presença.

4.º Opcional: Clique**Reiniciar**para repor todas as condições de pesquisa.

5.Clique**Pesquisa**.

As listas de resultados da pesquisa nesta página.

Pode visualizar os detalhes do resultado, incluindo o número do funcionário, o nome do funcionário, o departamento, o horário, o modo de autenticação e o número do cartão.

6.º Opcional: Depois de pesquisar e visualizar o registo de passagem do cartão, execute uma das seguintes operações.

Relatório	Gere o relatório de assiduidade.
Exportar	Exporte os resultados para o PC local.

Gerar relatório de presença

Após o cálculo dos dados de assiduidade, pode gerar relatórios que mostram o estado de assiduidade dos colaboradores no período específico.

Gerar relatório instantâneo

Suporta a geração manual de uma série de relatórios de assiduidade para visualizar os resultados de assiduidade dos colaboradores.

Antes de começar

Calcule os dados de atendimento.

Nota

Pode calcular os dados de atendimento manualmente ou definir o horário para que o cliente possa calcular os dados automaticamente todos os dias. Para obter detalhes, consulte***Calcular os dados de presença*** .

Execute os passos seguintes para gerar o relatório de presença instantaneamente.

Passos

1.Entre no módulo Tempo e Presença.

2.Clique**Estatísticas de frequência → Relatório**para entrar na página do Relatório.

3.No painel Relatório instantâneo, selecione um tipo de relatório na lista pendente.

4.Selecione uma pessoa ou departamento.

5.Defina o período de tempo durante o qual os dados de atendimento serão apresentados no relatório.

6.Clique**Gerar**.

Configurar relatório agendado

Suporta 5 tipos de relatório e pode pré-definir o conteúdo do relatório e enviará o relatório automaticamente para o endereço de e-mail que configurou.

Execute esta tarefa se pretender configurar um relatório agendado.

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*.

1.Entre no módulo Tempo e Presença.

2.Clique**Estatísticas de frequência → Relatório**para entrar na página do Relatório.

3.No painel Relatório agendado, clique em**Adicionar**para pré-definir um relatório e definir o conteúdo do relatório.

4.Defina o conteúdo do relatório.

Pessoa

Selecione a(s) pessoa(s) adicionada(s) e clique em > para adicionar a pessoa.

5.º Opcional: Defina a programação para enviar o relatório para o(s) endereço(s) de e-mail automaticamente.

1) Defina o**Envio automático de e-mail**mude para ON para ativar esta função.

2) Defina o período efetivo 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 irá submeter o relatório.

4) Defina o horário em que o cliente irá enviar o relatório.

Exemplo

Se definir o período efetivo como ***10/03/2018 a 10/04/2018***, selecionar ***Sexta-feira*** como a data de envio e defina a hora de envio como ***20:00:00***, o cliente enviará o relatório às 20h00 de sexta-feira no período 10/03/2018 a 10/04/2018.

Nota

Certifique-se de que os registos de assiduidade são calculados antes do horário de envio. Pode calcular os dados de atendimento manualmente ou definir o horário para que o cliente possa calcular os dados automaticamente todos os dias. Para obter detalhes, consulte ***Calcular os dados de presença*** .

5) Introduza o(s) endereço(s) de e-mail do destinatário.

Nota

Pode clicar para adicionar um novo endereço de e-mail. São permitidos até 5 endereços de e-mail.

6.Clique**Guardar**.

7.º Opcional: Depois de adicionar o relatório programado, pode executar um ou mais dos seguintes procedimentos:

Modificar relatório	Selecione um relatório adicionado e clique em**Modificar**para editar as suas definições.
Apagar relatório	Selecione um relatório adicionado e clique em**Remover**para o eliminar.
Gerar relatório	Selecione um relatório adicionado e clique em**Gerar**para gerar o relatório instantaneamente e pode visualizar os detalhes do relatório.

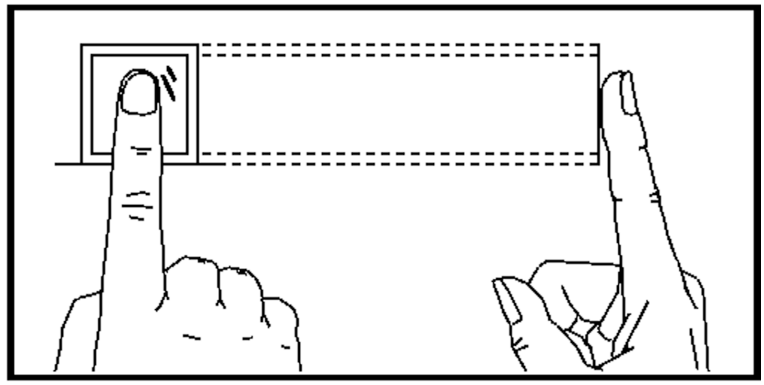
Anexo A. Dicas para digitalizar impressões digitais

Dedo recomendado

Dedo indicador, dedo médio ou terceiro dedo.

Digitalização Correta

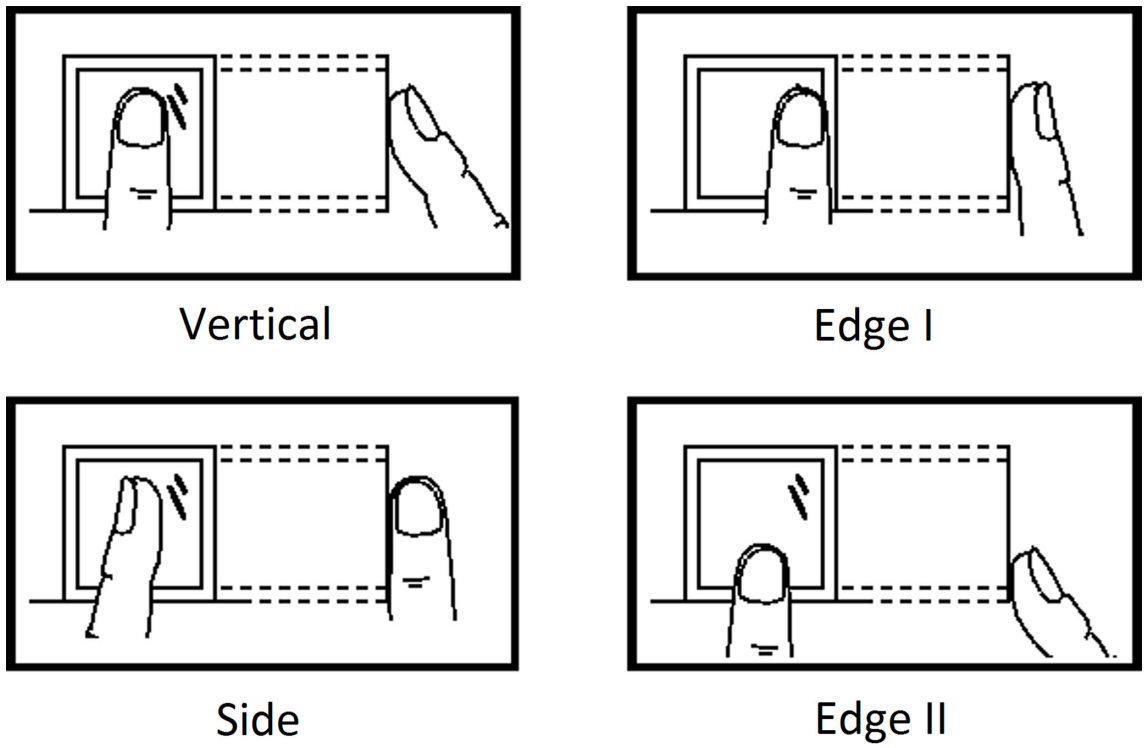
A figura apresentada abaixo é a forma correta de digitalizar o dedo:



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

Digitalização incorreta

Os números de digitalização de impressões digitais apresentados abaixo estão incorretos:



Ambiente

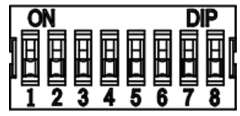
O scanner deve evitar a luz solar direta, altas temperaturas, condições húmidas e chuva. Quando estiver seco, o scanner poderá não reconhecer a sua impressão digital com êxito. Pode soprar o dedo e digitalizar novamente.

Outros

Se a sua impressão digital for superficial ou for difícil digitalizá-la, recomendamos que utilize outros métodos de autenticação.
Se tiver ferimentos no dedo digitalizado, o scanner poderá não reconhecer. Pode mudar outro dedo e tentar novamente.

Anexo B. Descrição da chave DIP

O número 1 ao número 8 vai do bit baixo ao bit alto.



Quando a chave está na posição ON, significa que a chave está habilitada, caso contrário a chave está desligada. Se configurar o interruptor DIP como na figura abaixo, o seu valor binário será 00001100 e o seu valor decimal será 12.

Anexo C. Descrições de regras Wiegand personalizadas

Tomemos como exemplo o Wiegand 44, os valores de configuração no separador Custom Wiegand são os seguintes:

Wiegand personalizado Nome	Wiegand 44				
Comprimento total	44				
Regra de transformação (dígito decimal)	porFormatRule[4]=[1][4][0][0]				
Modo de paridade	Paridade XOR				
Bit inicial de paridade ímpar		Comprimento			
Paridade uniforme inicial		Comprimento			
Bit inicial de paridade XOR	0	Comprimento por grupo	4	Comprimento total	40
Bit inicial do ID do cartão	0	Comprimento	32	Dígito Decimal	10
Bit inicial do código do site		Comprimento		Dígito Decimal	
Bit inicial OEM		Comprimento		Dígito Decimal	
Código do fabricante Começar pouco	32	Comprimento	8	Dígito Decimal	3

Dados Wiegand

Dados Wiegand = Dados Válidos + Dados de Paridade

Comprimento total

Comprimento dos dados Wiegand.

Regra de transporte

4 bytes. Apresente os tipos de combinação de dados válidos. O exemplo apresenta a combinação do ID do cartão e do código do fabricante. Os dados válidos podem ser uma regra única ou uma combinação de várias regras.

Modo de paridade

Paridade válida para dados Wiegand. Pode selecionar paridade ímpar ou par.

Bit inicial e comprimento de paridade ímpar

Se selecionar Paridade ímpar, estes itens estarão disponíveis. Se o bit inicial de paridade ímpar for 1 e o comprimento for 12, o sistema iniciará o cálculo de paridade ímpar a partir do bit 1. Calculará 12 bits. O resultado estará no bit 0. (O bit 0 é o primeiro bit.)

Bit inicial de paridade uniforme e comprimento

Se selecionar Paridade par, estes itens estarão disponíveis. Se o bit inicial de paridade par for 12 e o comprimento for 12, o sistema iniciará o cálculo de paridade par a partir do bit 12. Calculará 12 bits. O resultado estará na última parte.

Bit inicial de paridade XOR, comprimento por grupo e comprimento total

Se selecionar Paridade XOR, estes itens estarão disponíveis. Dependendo da tabela apresentada acima, o bit de início é 0, o comprimento por grupo é 4 e o comprimento total é 40. Isto significa que o sistema irá calcular a partir do bit 0, calcular a cada 4 bits e calcular 40 bits no total (10 grupos no total). O resultado estará nos últimos 4 bits. (O comprimento do resultado é igual ao comprimento por grupo.)

Bit inicial, comprimento e dígito decimal do ID do cartão

Se utilizar a regra de transformação, estes itens estarão disponíveis. Dependendo da tabela apresentada acima, o bit de início do ID do cartão é 0, o comprimento é 32 e o dígito decimal é 10. Representa que a partir do bit 0, existem 32 bits que representam o ID do cartão. (O comprimento aqui é calculado por bit.) E o comprimento do dígito decimal é de 10 bits.

Bit inicial, comprimento e dígito decimal do código do site

Se utilizar a regra de transformação, estes itens estarão disponíveis. Para obter informações detalhadas, consulte a explicação do ID do cartão.

Bit inicial, comprimento e dígito decimal do OEM

Se utilizar a regra de transformação, estes itens estarão disponíveis. Para obter informações detalhadas, consulte a explicação do ID do cartão.

Bit inicial, comprimento e dígito decimal do código do fabricante

Se utilizar a regra de transformação, estes itens estarão disponíveis. Dependendo da tabela apresentada acima, o bit de início do código do fabricante é 32, o comprimento é 8 e o dígito decimal é 3. Isto representa que a partir do bit 32, existem 8 bits no código do fabricante. (O comprimento aqui é calculado por bit.) E o comprimento decimal é 3.


See Far, Go Further