

Controlador de 2 fios

Manual do utilizador



Prefácio

Geral

Este manual apresenta a estrutura, as funções e as operações do controlador de 2 fios (a seguir designado por "Controlador"). Leia com atenção antes de utilizar o dispositivo e guarde o manual para consulta futura.

Instruções de segurança

As seguintes palavras-sinal podem aparecer no manual.

Palavras de sinalização	Significado
 DANGER	Indica um perigo potencial elevado que, se não for evitado, resultará em morte ou ferimentos graves.
 WARNING	Indica um perigo potencial médio ou baixo que, se não for evitado, pode provocar ferimentos ligeiros ou moderados.
 CAUTION	Indica um risco potencial que, se não for evitado, pode resultar em danos materiais, perda de dados, reduções no desempenho ou resultados imprevisíveis.
 NOTE	Fornecer informações adicionais como complemento do texto.

Histórico de revisões

Versão	Conteúdo da revisão	Tempo de libertação
V1.0.1	Diagrama de rede revisto.	setembro de 2024
V1.0.0	Primeiro lançamento.	julho de 2024

Aviso de proteção da privacidade

Como utilizador do dispositivo ou controlador de dados, pode recolher dados pessoais de outras pessoas, como o rosto, o áudio, as impressões digitais e o número da matrícula. É necessário estar em conformidade com as leis e regulamentos locais de proteção da privacidade para proteger os direitos e interesses legítimos de outras pessoas, implementando medidas que incluem, entre outras, as seguintes Fornecer uma identificação clara e visível para informar as pessoas da existência da área de vigilância e fornecer as informações de contacto necessárias.

Sobre o manual

- O manual serve apenas de referência. Podem existir ligeiras diferenças entre o manual e o produto.
- Não nos responsabilizamos por perdas incorridas devido à utilização do produto de formas que não estejam em conformidade com o manual.
- O manual será atualizado de acordo com as leis e regulamentos mais recentes das jurisdições relacionadas. Para obter informações detalhadas, consulte o manual do utilizador em papel, utilize o nosso CD-ROM, leia o código QR ou visite o nosso sítio Web oficial. O manual serve

apenas de referência. Podem existir ligeiras diferenças entre a versão eletrónica e a versão em papel.

- Todos os desenhos e software estão sujeitos a alterações sem aviso prévio por escrito. As actualizações do produto podem resultar no aparecimento de algumas diferenças entre o produto real e o manual. Contacte o serviço de apoio ao cliente para obter o programa e a documentação suplementar mais recentes.
- Podem existir erros na impressão ou desvios na descrição das funções, operações e dados técnicos. Em caso de dúvida ou litígio, reservamo-nos o direito de explicação final.
- Actualize o software de leitura ou experimente outro software de leitura convencional se não for possível abrir o manual (em formato PDF).
- Todas as marcas comerciais, marcas registadas e nomes de empresas no manual são propriedade dos respectivos proprietários.
- Visite o nosso website, contacte o fornecedor ou o serviço de apoio ao cliente se ocorrer algum problema durante a utilização do dispositivo.
- Em caso de incerteza ou controvérsia, reservamo-nos o direito de explicação final.

Avisos e salvaguardas importantes

Esta secção apresenta conteúdos que abrangem o manuseamento correto do dispositivo, a prevenção de perigos e a prevenção de danos materiais. Leia atentamente antes de utilizar o dispositivo e cumpra as diretrizes quando o utilizar.

Requisitos de instalação



- Não ligue o adaptador de corrente ao dispositivo enquanto o adaptador estiver ligado.
- Não ligue o dispositivo a dois ou mais tipos de fontes de alimentação, para evitar danos no dispositivo.
- Siga os requisitos eléctricos para alimentar o dispositivo.
 - ◊ Seguem-se os requisitos para seleccionar um adaptador de corrente.
 - A fonte de alimentação deve estar em conformidade com os requisitos das normas IEC 60950-1 e IEC 62368-1.
 - A tensão deve cumprir os requisitos SELV (Safety Extra Low Voltage) e não exceder as normas ES-1.
 - Quando a potência do dispositivo não excede 100 W, a fonte de alimentação deve cumprir os requisitos LPS e não ser superior a PS2.
 - ◊ Recomendamos a utilização do adaptador de corrente fornecido com o dispositivo.
 - ◊ Ao seleccionar o adaptador de alimentação, os requisitos da fonte de alimentação (como a tensão nominal) estão sujeitos à etiqueta do dispositivo.



- O pessoal que trabalha em altura deve tomar todas as medidas necessárias para garantir a sua segurança pessoal, incluindo a utilização de um capacete e de cintos de segurança.
- Não coloque o dispositivo num local exposto à luz solar ou perto de fontes de calor.
- Mantenha o dispositivo afastado de humidade, pó e fuligem.
- Instale o dispositivo numa superfície estável para evitar que caia.
- Instale o dispositivo num local bem ventilado e não bloqueie a sua ventilação.
- Utilize um adaptador ou uma fonte de alimentação de armário fornecida pelo fabricante.
- Utilize os cabos de alimentação recomendados para a região e que estejam em conformidade com as especificações de potência nominal.
- O dispositivo é um aparelho eléctrico de classe I. Certifique-se de que a fonte de alimentação do dispositivo está ligada a uma tomada de alimentação com ligação à terra de protecção.

Requisitos de funcionamento



Precauções com a bateria

Medidas preventivas (incluindo, mas não se limitando a):

- Não transportar, armazenar ou utilizar as baterias em altitudes elevadas com baixa pressão e ambientes com temperaturas extremamente altas e baixas.

- Não deitar as pilhas ao fogo ou a um forno quente, nem esmagar ou cortar mecanicamente as pilhas para evitar uma explosão.
- Não deixe as baterias em ambientes com temperaturas extremamente elevadas para evitar explosões e fugas de líquidos ou gases inflamáveis.
- Não submeta as baterias a uma pressão de ar extremamente baixa para evitar explosões e fugas de líquidos ou gases inflamáveis.



- Verifique se a fonte de alimentação está correta antes de utilizar.
- Não desligue o cabo de alimentação na parte lateral do dispositivo enquanto o adaptador estiver ligado.
- Utilizar o dispositivo dentro da gama nominal de entrada e saída de energia.
- Transportar, utilizar e armazenar o dispositivo em condições de humidade e temperatura permitidas.
- Se o dispositivo estiver desligado durante mais de um mês, deve ser colocado na sua embalagem original e selado. Certifique-se de que o mantém afastado da humidade e de que o armazena em condições de humidade e temperatura permitidas.
- Não deixe cair nem salpique líquido sobre o dispositivo e certifique-se de que não existe nenhum objeto cheio de líquido sobre o dispositivo para evitar que o líquido entre nele.
- Não desmontar o aparelho sem instrução profissional.

Índice

Prefácio.....	I
Salvaguardas e avisos importantes	III
1 Visão geral.....	1
1.1 Introdução.....	1
1.2 Estrutura.....	1
2 Diagrama de rede	3
3 Funcionamento da página Web	7
3.1 Página inicial.....	7
3.2 Centro de administração	8
3.2.1 Repor a palavra-passe	8
3.2.2 Alterar a mensagem do utilizador.....	9
3.2.3 Restaurar as predefinições de fábrica	10
3.2.4 Reiniciar o dispositivo	10
3.2.5 Terminar a sessão	10
3.3 Centro de segurança	10
3.3.1 Estado da segurança	10
3.3.2 Configuração de HTTPS	11
3.3.3 Defesa de ataque	12
3.3.3.1 Configurar a Firewall.....	12
3.3.3.2 Configurar o bloqueio de conta.....	13
3.3.3.3 Configuração de ataque anti-DoS	14
3.3.4 Instalar o certificado do dispositivo.....	15
3.3.4.1 Criar um certificado	15
3.3.4.2 Solicitar e importar o certificado da AC.....	16
3.3.4.3 Instalação de um certificado existente	18
3.3.5 Instalar o certificado da CA confiável	18
3.3.6 Aviso de segurança	19
3.3.7 Autenticação de segurança	19
3.4 Configuração da VTO.....	20
3.4.1 Gestão do pessoal.....	20
3.4.2 Mapeamento do número da sala VTH	22
3.4.3 Controlo de acesso	23
3.4.3.1 Configuração.....	23
3.4.3.2 RS-485	24
3.4.4 Módulo	24

3.4.5 Manutenção.....	25
3.5 Adicionar pessoa.....	25
3.6 Importação de pessoas em lotes.....	27
3.7 Definições de rede.....	28
3.7.1 Configurar o TCP/IP	28
3.7.2 Configurar os serviços básicos.....	29
3.8 Centro de manutenção	31
3.8.1 Diagnóstico com um clique.....	31
3.8.2 Informações do sistema.....	31
3.8.3 Exportar e importar ficheiros de configuração.....	32
3.8.4 Atualizar o sistema.....	32
3.8.5 Manutenção avançada.....	33
3.8.5.1 Exportação	33
3.8.5.2 Captura de pacotes	33
Apêndice 1 Recomendação de segurança	34

1 Visão geral

1.1 Introdução

O controlador de 2 fios utiliza o material plástico e suporta a instalação em calha deslizante. Podem ser ligados até 100 VTHs analógicos ou 22 VTHs com função Wi-Fi a um controlador de 2 fios. O controlador de 2 fios pode ligar-se a outros controladores de 2 fios no modo em cascata (são suportados até 10 níveis de cascata). Pode iniciar sessão na página Web do controlador para gerir os dispositivos.



- No modo em cascata, configure os dispositivos através de uma página web do controlador de 2 fios ao mesmo tempo.
- Utilize a fonte de alimentação recomendada.

1.2 Estrutura

Figura 1-1 Painel frontal

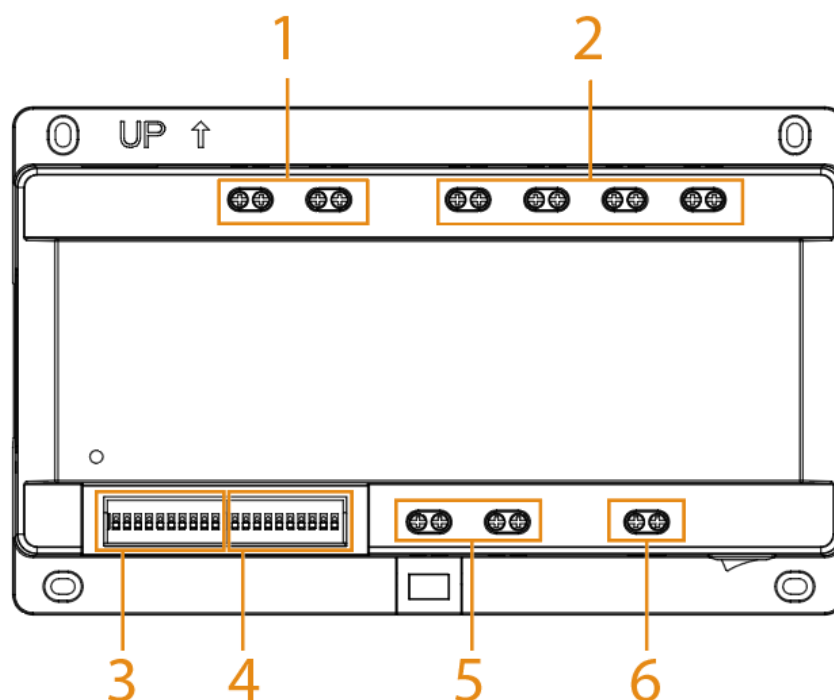
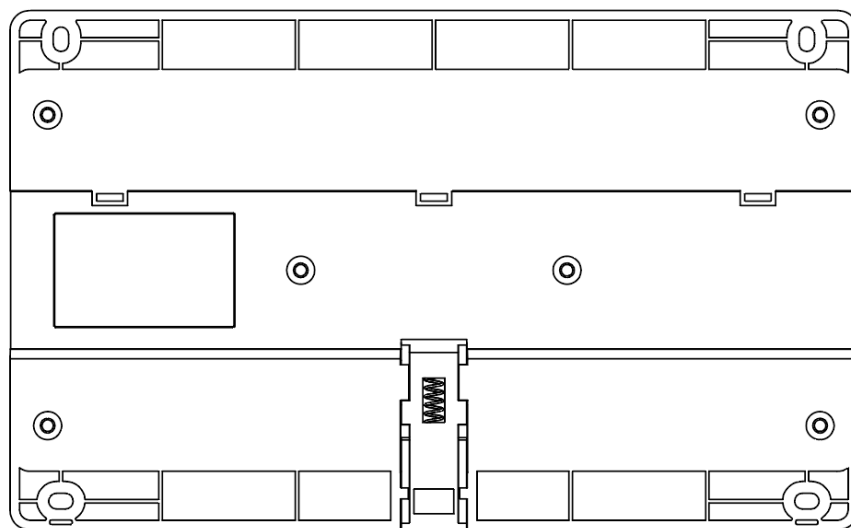


Tabela 1-1 Descrição do painel frontal

Não.	Descrição
1	Ligar à VTO.
2	Ligar a VTH.

Não.	Descrição
3	Depois de ligar aos VTHs, defina o DIP para a ID mínima de todas as IDs de VTH.  Mova o atuador completamente para a posição superior ou inferior. Se o atuador estiver na posição intermédia, é considerado como estando na posição superior.
4	Após a ligação aos VTHs, defina o DIP para a ID máxima de todas as IDs dos VTHs.  Mova o atuador completamente para a posição superior ou inferior. Se o atuador estiver na posição intermédia, é considerado como estando na posição superior.
5	Ligação a outros controladores de 2 fios. A porta UP só pode ser ligada à porta Down de outro controlador. A porta Down só pode ser ligada à porta Up noutro controlador. Para mais informações, consulte o diagrama de ligações.
6	Ligar à fonte de alimentação.

Figura 1-2 Painel traseiro



2 Diagrama de rede



Quando vários monitores interiores estão ligados em modo cascata à porta do terminal de derivação, para reduzir a reflexão do sinal, o 14.º interruptor DIP do monitor interior mais afastado da porta tem de estar ligado.

Consulte a imagem seguinte para configurar o interruptor DIP do dispositivo em cascata. O interruptor DIP do ID deve ser configurado de acordo com a situação atual.

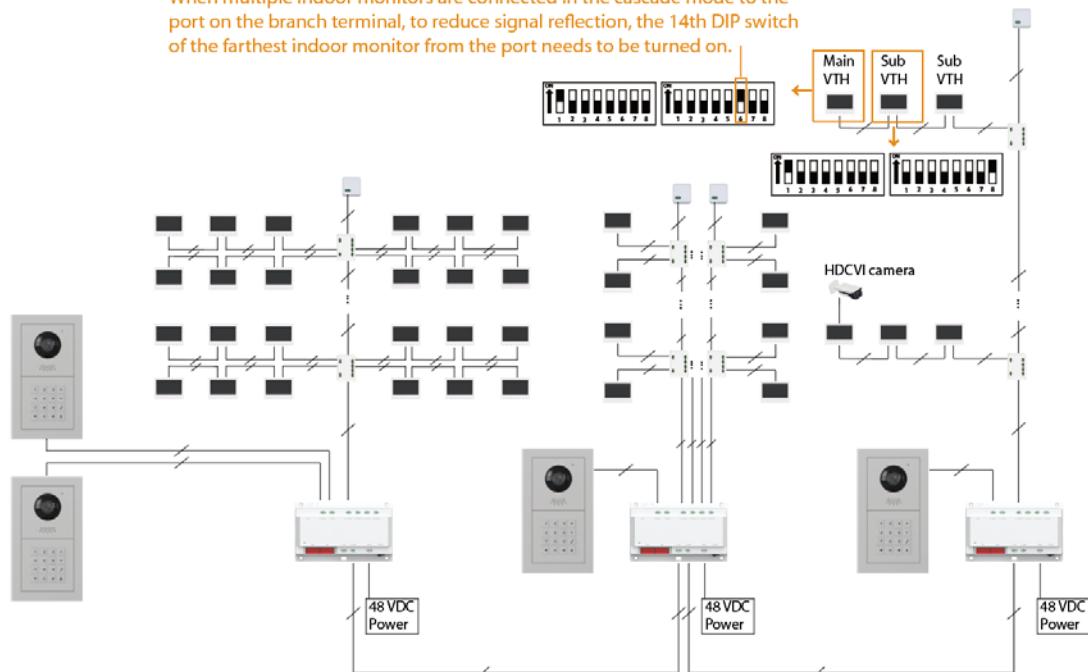


- A fonte de alimentação da câmara HDCVI não pode ser ligada à terra.
- A aparência do produto é apenas para referência.

Diagrama de rede

Figura 2-1 Diagrama de rede

When multiple indoor monitors are connected in the cascade mode to the port on the branch terminal, to reduce signal reflection, the 14th DIP switch of the farthest indoor monitor from the port needs to be turned on.

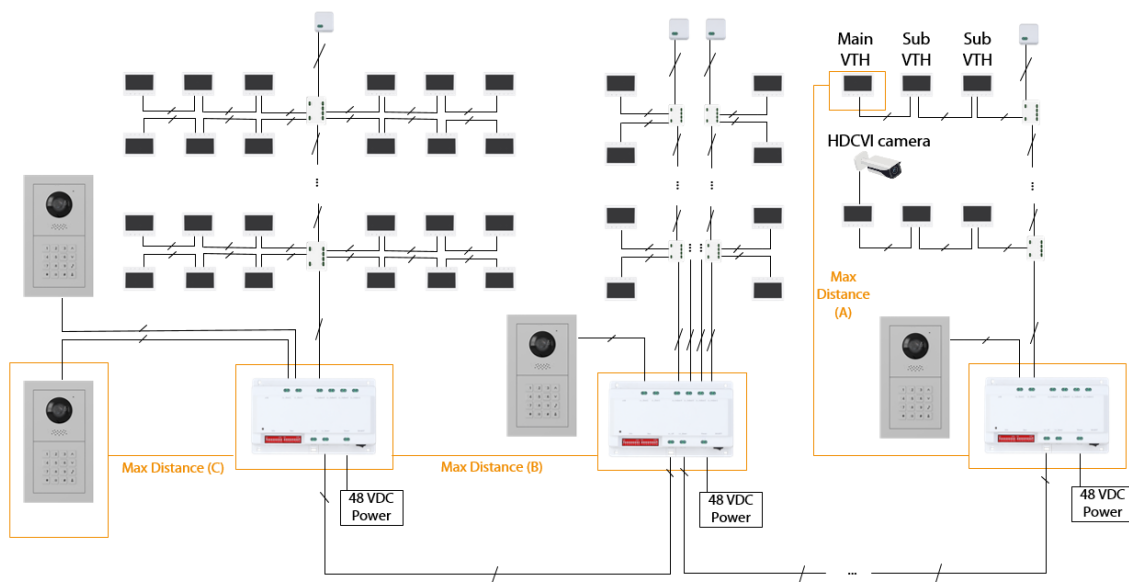


Distância de cablagem entre o controlador, o VTH e o VTO



- A distância máxima (A) refere-se à distância entre o controlador de 2 fios e o VTH. $A \leq 100$ m.
- A distância máxima (B) refere-se à distância entre os controladores de 2 fios em cascata. $B \leq 100$ m.
- A distância máxima (C) refere-se à distância entre o controlador de 2 fios e o VTO. $C \leq 100$ m.
- O número de controladores em cascata deve ser inferior ou igual a 10.

Figura 2-2 Distância máxima



Capacidade de rede para VTH

A capacidade para o VTH indica o número máximo de VTHs que podem ser ligados a uma porta de monitor interior no controlador de 2 fios.

Cada controlador pode ligar até 22 VTHs com função Wi-Fi ou até 100 VTHs sem função Wi-Fi.



- Os VTHs de 2 fios com a função Wi-Fi podem funcionar ao mesmo tempo. O número de VTHs de 2 fios sem a função Wi-Fi que funcionam ao mesmo tempo é de 5% da capacidade máxima de acordo com as diferentes especificações e distâncias dos cabos.
- Os valores de capacidade baseiam-se nas predefinições de voz e brilho do ecrã e nos cabos padrão mencionados na tabela seguinte.
- Na rede, se pretender substituir o VTH com função Wi-Fi pelo VTH sem função Wi-Fi, o rácio de conversão é de 1:8.

Por exemplo, se quiser reduzir 1 VTH com função Wi-Fi na rede, pode ligar-se a 8 VTHs sem função Wi-Fi.



O número máximo de VTHs com função Wi-Fi não pode exceder 22.

O número máximo de VTHs sem função Wi-Fi não pode exceder 100.

Quadro 2-1 Capacidade da rede para VTH

Tipo de cabo	Especificação do cabo	AWG	Tipo de dispositivo	A=0-25 m	A=26-50 m	A=51-75 m	A=76-100 m
Cabo normal	RVV 2 × 1,5 mm ² (Recomendado)	AWG 15	Com Wi-Fi	22	22	22	17
			Sem Wi-Fi	100	100	100	100
	RVV 2 × 1 mm ²	AWG 17	Com Wi-Fi	22	22	18	13
			Sem Wi-Fi	100	100	100	100
	RVV 2 × 0,5 mm ²	AWG 20	Com Wi-Fi	22	17	11	8
			Sem Wi-Fi	100	100	91	68
Cabo de rede	Cabo de rede de par duplo	AWG 21	Com Wi-Fi	22	14	9	7
			Sem Wi-Fi	100	100	75	56
	Cabo de rede de par único	AWG 24	Com Wi-Fi	14	7	4	3
			Sem Wi-Fi	100	56	37	28

Capacidade de rede para o controlador de 2 fios

A capacidade para o controlador de 2 fios indica o número máximo de controladores que podem ser ligados a uma porta correspondente no controlador.



Os valores de capacidade baseiam-se em cabos padrão mencionados na tabela seguinte.

Quadro 2-2 Capacidade de rede do controlador

Tipo de cabo	Especificação do cabo	AWG	B=0-100 m
Cabo normal	RVV 2 × 1,5 mm ²	AWG 15	8
	RVV 2 × 1 mm ²	AWG 17	10
	RVV 2 × 0,5 mm ² (Recomendado)	AWG 20	10
Cabo de rede	Cabo de rede de par duplo	AWG 21	10
	Cabo de rede de par único	AWG 24	10

Capacidade da rede para VTO

A capacidade para o VTO indica o número máximo de VTOs que podem ser ligados a um controlador de 2 fios.

Podem ser ligados até 2 VTOs a um controlador de 2 fios.



Os valores de capacidade baseiam-se em cabos padrão mencionados na tabela seguinte.

Tabela 2-3 Capacidade de rede para a VTO

Tipo de cabo	Especificação do cabo	AWG	C=0-25 m	C=26-50 m	C=51-75 m	C=76-100 m
Cabo normal	RVV 2 × 1,5 mm ² (Recomendado)	AWG 15	2	2	2	2
	RVV 2 × 1 mm ²	AWG 17	2	2	2	2
	RVV 2 × 0,5 mm ²	AWG 20	2	2	2	2
Cabo de rede	Cabo de rede de par duplo	AWG 21	2	2	2	2
	Cabo de rede de par único	AWG 24	2	2	1	1

3 Funcionamento da página Web

Para o primeiro início de sessão, é necessário inicializar o dispositivo na página Web. Inicie sessão na página Web para configurar os parâmetros do Controlador e gerir a VTO ligada ao controlador atual e a VTO ligada aos controladores em cascata.

3.1 Página inicial

O sistema passa automaticamente para a página inicial após o início de sessão.

Figura 3-1 Página inicial

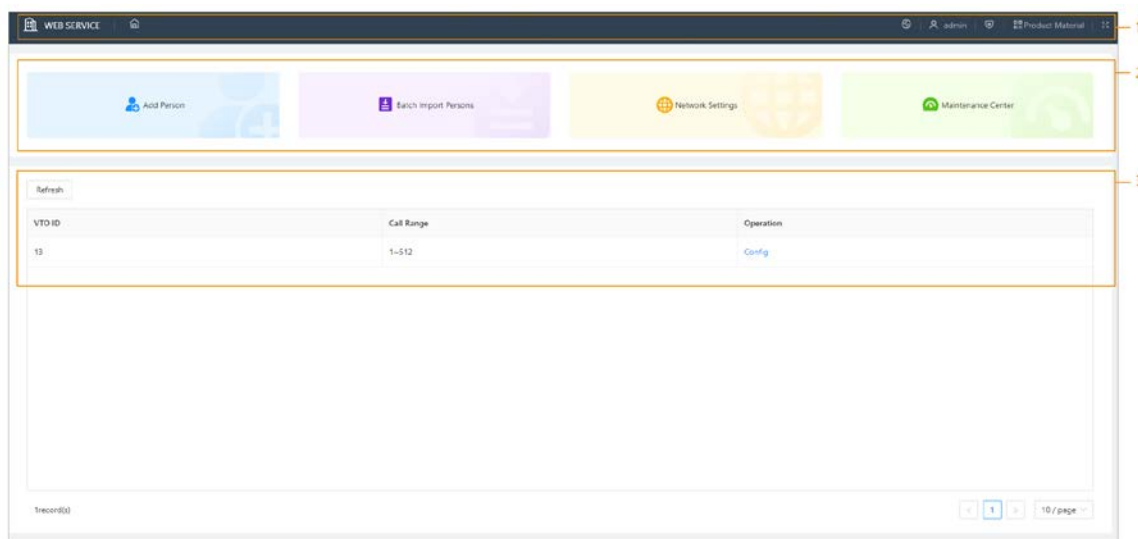


Tabela 3-1 Introdução à página inicial

Não.	Ícone	Função	Descrição	Referência
1		Botão de início	Regressar à página inicial.	-
		Língua	Alterar o idioma da página Web do dispositivo.	-
		Centro de administração	Alterar a palavra-passe, terminar a sessão do dispositivo atual, reiniciar o sistema e repor as definições de fábrica do dispositivo.	"Centro de administração 3.2"
		Centro de segurança	Ver e configurar as definições de segurança.	"Centro de Segurança 3.3"
		Material do produto	Digitalize o código QR para ver o material do produto, como o manual do utilizador.	-

Não.	Ícone	Função	Descrição	Referência
		Ecrã inteiro	Visualizar a página Web no modo de ecrã inteiro. Clique novamente ou prima a tecla Exit para sair do modo de ecrã inteiro.	-
2	-	Adicionar pessoa	Adicionar a pessoa e enviar as informações às VTOs.	"3.5 Adicionar pessoa"
	-	Importação de pessoas em lote	Depois de exportar informações sobre pessoas do VTO, importar pessoas em lotes para outros VTOs.	"3.6 Importação de pessoas em lotes"
	-	Definições de rede	Configurar os parâmetros de rede, tais como TCP/IP e serviços básicos.	"3.7 Definições de rede"
	-	Centro de manutenção	Visualizar as informações do sistema. Exportar e importar ficheiros de configuração. Atualizar o dispositivo e muito mais.	"3.8 Centro de manutenção"
3	-	Configuração do VTO	Gerir as informações pessoais no VTO. Configurar os parâmetros da VTO, incluindo os parâmetros de controlo de acesso, os parâmetros do módulo e muito mais.	"3.4 Configuração de VTO"

3.2 Centro de administração

Alterar a palavra-passe, terminar a sessão, reiniciar o dispositivo, repor as predefinições de fábrica e outras operações na página inicial.

3.2.1 Repor a palavra-passe

Se se esquecer da palavra-passe de início de sessão da conta de administrador, leia o código QR para a repor.

Pré-requisitos

Certifique-se de que activou **a reposição da palavra-passe** em **Definições de rede > Serviços básicos**.



Se não tiver configurado o endereço de correio eletrónico durante a inicialização, o sistema comunicará um erro. Contacte o revendedor local ou o apoio técnico para obter ajuda.

Procedimento

Passo 1 Clique **Esqueceu a senha?** na página de login e, em seguida, clique em **Próximo**.

Passo 2 Obter o **código de segurança** de acordo com as instruções.



- Pode obter até 2 códigos de segurança com o mesmo código QR. Se precisar de mais códigos de segurança, tem de atualizar o código QR e digitalizá-lo novamente.
- O código de segurança será enviado para o seu endereço de correio eletrónico. Tem de o utilizar no prazo de 24 horas. Caso contrário, o código de segurança será inválido.
- A conta será bloqueada durante 5 minutos se introduzir o código de segurança errado 5 vezes seguidas.

Passo 3 Introduza o código de segurança que recebeu e clique em **Seguinte**.

Passo 4 Introduza a nova palavra-passe, confirme a nova palavra-passe e clique em **OK**.

3.2.2 Alterar a mensagem do utilizador

Alterar a palavra-passe de início de sessão e o endereço de correio eletrónico do utilizador.

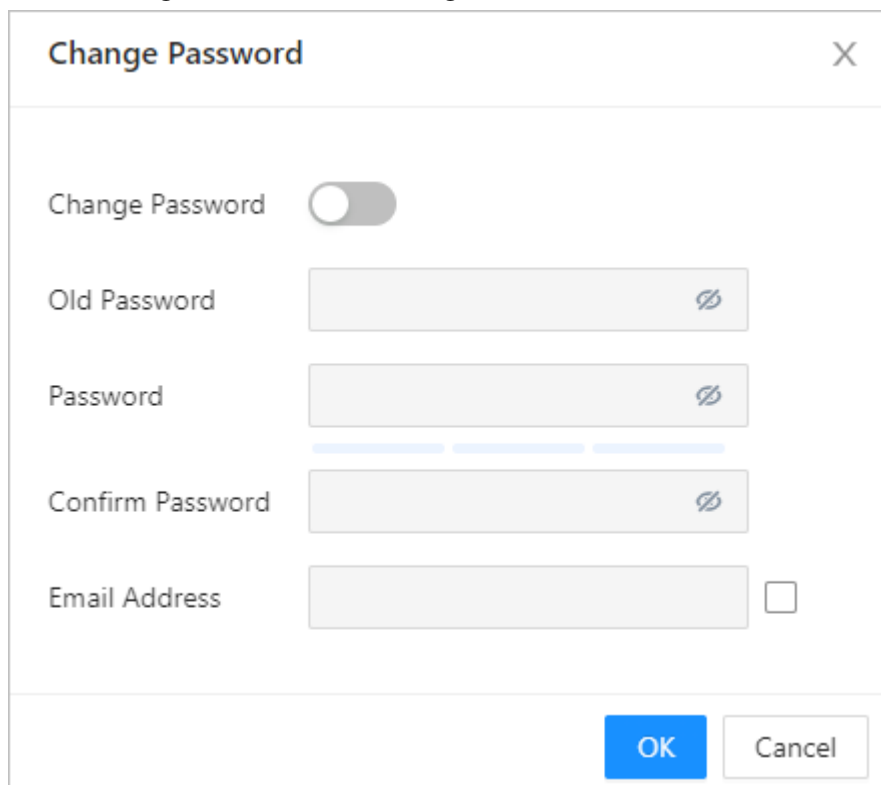
Procedimento

Passo 1 Clique em  **admin** na página inicial.

Passo 2 Clique **Alterar senha**.

Passo 3 Habilite a função, configure os parâmetros e clique em **OK**.

Figura 3-2 Alterar a mensagem do utilizador



3.2.3 Restaurar as predefinições de fábrica

Procedimento

Passo 1 Seleccione  > **Predefinição de fábrica.**



O restauro do controlador para as configurações predefinidas resultará na perda de dados.

Atenção.

Passo 2 Introduza a palavra-passe de início de sessão e clique em **OK**.

Passo 3 Restaure as predefinições de fábrica, se necessário.

3.2.4 Reiniciar o dispositivo

Selecione  > **Reiniciar** e, em seguida, clique em **OK** na janela de contexto. O dispositivo é reiniciado automaticamente e a página Web passa para a página de início de sessão.

3.2.5 Terminar a sessão

Selecione  > **Terminar sessão**. A página Web vai para a página de início de sessão.

3.3 Centro de segurança

3.3.1 Estado de segurança

Analise os utilizadores, o serviço e os módulos de segurança para verificar o estado de segurança do controlador.

Informações de base

- **Deteção de utilizadores e serviços:** Verificar se as configurações actuais estão em conformidade com as recomendações.
- **Verificação dos módulos de segurança:** Verificar o estado de funcionamento dos módulos de segurança, como a proteção de confiança, a encriptação de firmware e a defesa contra ataques.

Procedimento

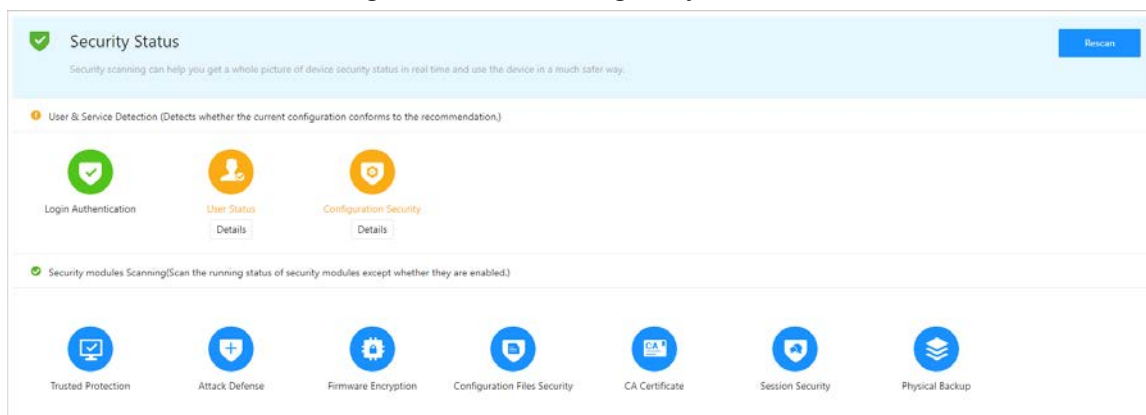
Passo 1 Seleccione  > **Estado da segurança.**

Passo 2 Clique em **Verificar** para efetuar uma verificação de segurança do dispositivo.



- Passe o cursor sobre os ícones dos módulos de segurança para ver o seu estado de funcionamento.
- Se pretender verificar o estado após a primeira verificação, clique em **Verificar novamente**.

Figura 3-3 Estado da segurança



Operações relacionadas

Depois de efetuar a verificação, os resultados serão apresentados em cores diferentes. Amarelo indica que os módulos de segurança estão anormais e verde indica que os módulos de segurança estão normais.

- Clique em **Detalhes** para ver os detalhes sobre os resultados da verificação.
- Clique em **Ignorar** para ignorar a anomalia e esta não será digitalizada. A anomalia que foi ignorada será destacada a cinzento.
- Clique em **Otimizar** para solucionar a anomalia.

3.3.2 Configuração de HTTPS

Crie um certificado ou carregue um certificado autenticado e, em seguida, pode iniciar sessão na página Web através de HTTPS no seu computador. O HTTPS protege a comunicação através de uma rede informática.

Procedimento

Passo 1 Seleccione  > **Serviço de sistema** > **HTTPS**.

Passo 2 **Habilitar** o serviço HTTPS.



Se ativar a opção compatível com TLS v1.1 e versões anteriores, podem ocorrer riscos de segurança. Atenção.

Passo 3 Seleccione o certificado.



Se não existirem certificados na lista, clique em **Gestão de certificados** para carregar um certificado.

Figura 3-4 HTTPS

No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
1		323032	26-01-2054 08:59:00	20:23:12:11:10:00	Device BSC CA	
2		323032	18-02-2054 18:21:31	20:23:12:11:10:00	Device BSC CA	HTTPS, RTSP over TLS

Passo 4 Clique em **Aplicar**.

Introduzir "*https://IP address: httpsport*" num navegador Web. Se o certificado estiver instalado, pode iniciar sessão na página Web com êxito. Caso contrário, a página Web apresentará o certificado como incorreto ou não fiável.

3.3.3 Defesa de ataque

3.3.3.1 Configurar a Firewall

Configurar a firewall para limitar o acesso ao Dispositivo.

Procedimento

Passo 1 Selecione > **Defesa contra ataques** > **Firewall**.

Passo 2 Clique para ativar a função de firewall.

Figura 3-5 Firewall

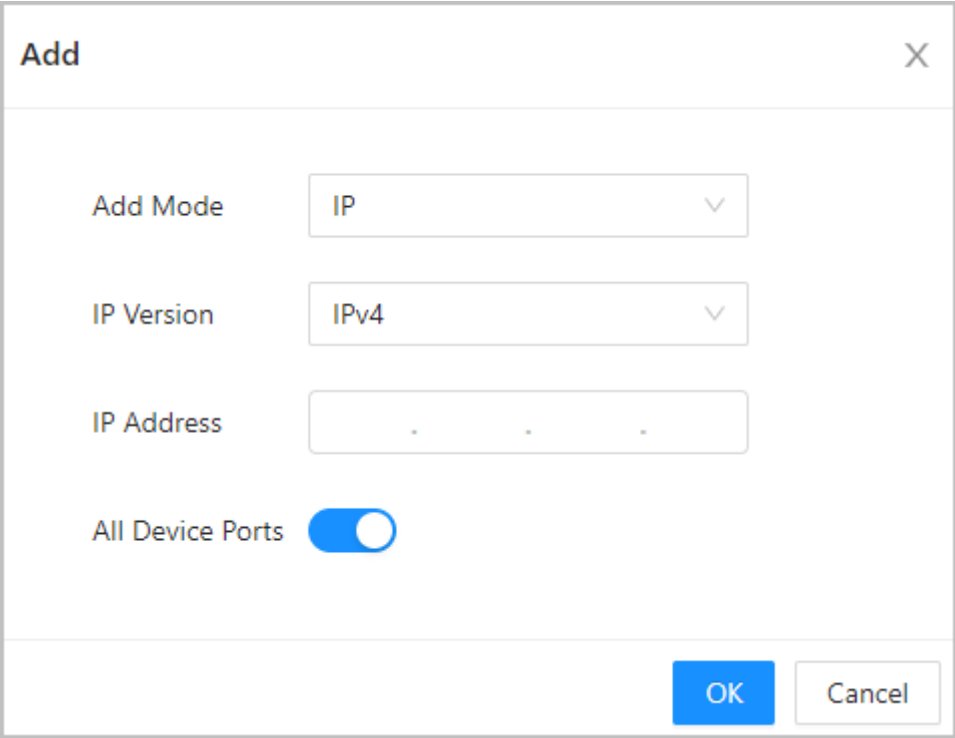
No.	Host IP/MAC	Port	Operation
1	15.0.0.6	All Device Ports	

Passo 3 Seleccione o modo: **Lista de permissões** e **Lista de bloqueios**.

- **Lista de permissões:** Apenas os endereços IP/MAC na lista de permissões podem aceder ao Dispositivo.
- **Lista de bloqueio:** Os endereços IP/MAC na lista de bloqueio não podem aceder ao Dispositivo.

Passo 4 Clique **Adicionar** para introduzir as informações de IP.

Figura 3-6 Adicionar informações de IP



The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. Inside the dialog, there are four configuration options:

- Add Mode:** A dropdown menu currently set to "IP".
- IP Version:** A dropdown menu currently set to "IPv4".
- IP Address:** A text input field containing three dots, indicating a placeholder for an IP address.
- All Device Ports:** A toggle switch that is currently turned on (blue).

At the bottom right of the dialog, there are two buttons: "OK" (blue) and "Cancel" (white with a gray border).

Passo 5 Clique em **OK**.

Operações relacionadas

- Clique em  para editar as informações de IP.
- Clique em  para eliminar o endereço IP.

3.3.3.2 Configurar o bloqueio de conta

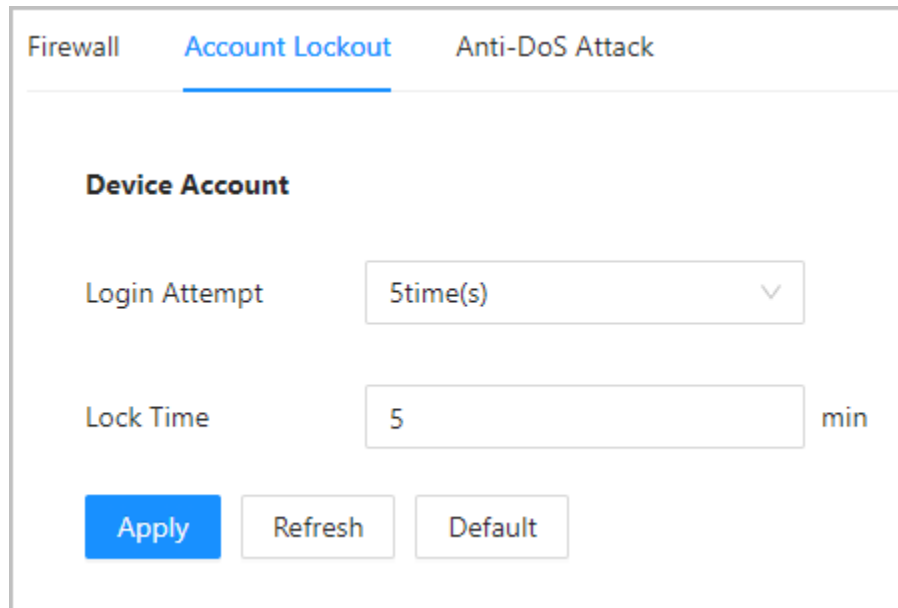
Se for introduzida uma palavra-passe incorrecta durante um determinado número de vezes, a conta será bloqueada.

Procedimento

Passo 1 Seleccionar  > **Defesa contra ataques** > **Bloqueio de conta**.

Passo 2 Introduza o número de tentativas de início de sessão e a duração do bloqueio da conta de administrador e do utilizador ONVIF.

Figura 3-7 Bloqueio de conta



Firewall **Account Lockout** Anti-DoS Attack

Device Account

Login Attempt 5time(s) ▼

Lock Time 5 min

Apply Refresh Default

- Tentativa de início de sessão: O limite de tentativas de início de sessão. Se a palavra-passe incorrecta for introduzida durante um número definido de vezes, a conta será bloqueada.
- Tempo de bloqueio: A duração durante a qual não é possível iniciar sessão depois de a conta ser bloqueada.

Passo 3 Clique em **Aplicar**.

3.3.3.3 Configuração de ataque anti-DoS

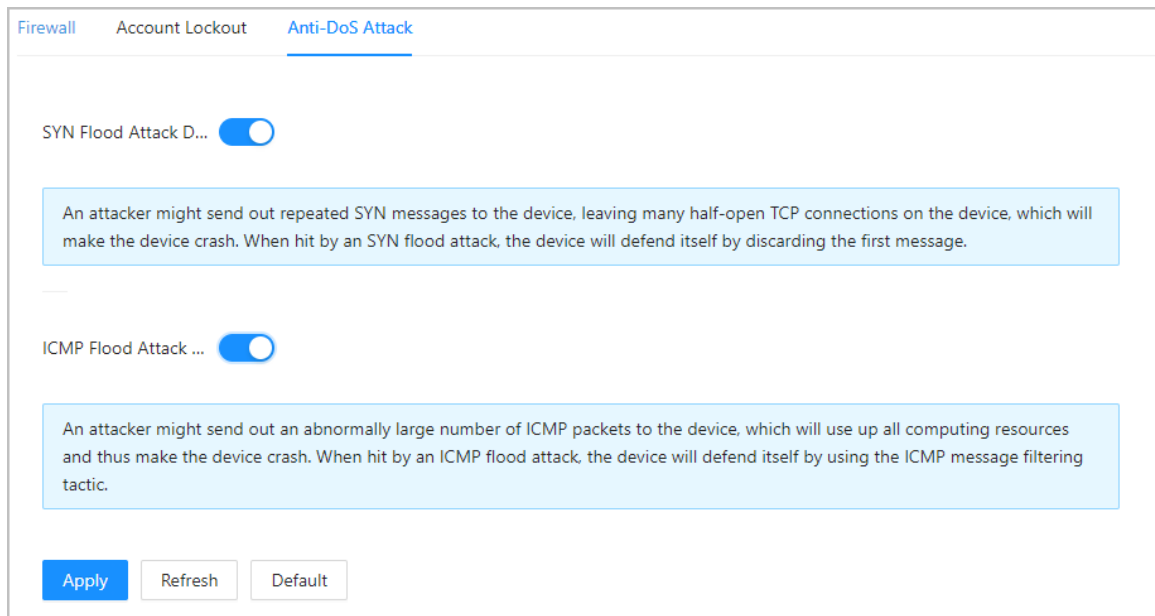
Pode ativar a **Defesa contra Ataques de Inundação SYN** e a **Defesa contra Ataques de Inundação ICMP** para defender o Dispositivo contra ataques Dos.

Procedimento

Passo 1 Seleccione  > **Defesa contra ataques** > **Ataque anti-DoS**.

Passo 2 Ativar **Defesa contra ataque de inundação SYN** ou **Defesa contra ataque de inundação ICMP** para proteger o dispositivo contra ataque Dos.

Figura 3-8 Ataque anti-DoS



Passo 3 Clique em **Aplicar**.

3.3.4 Instalar o certificado do dispositivo

Crie um certificado ou carregue um certificado autenticado e, em seguida, pode iniciar sessão através de HTTPS no seu computador.

3.3.4.1 Criar um certificado

Criar um certificado para o Dispositivo.

Procedimento

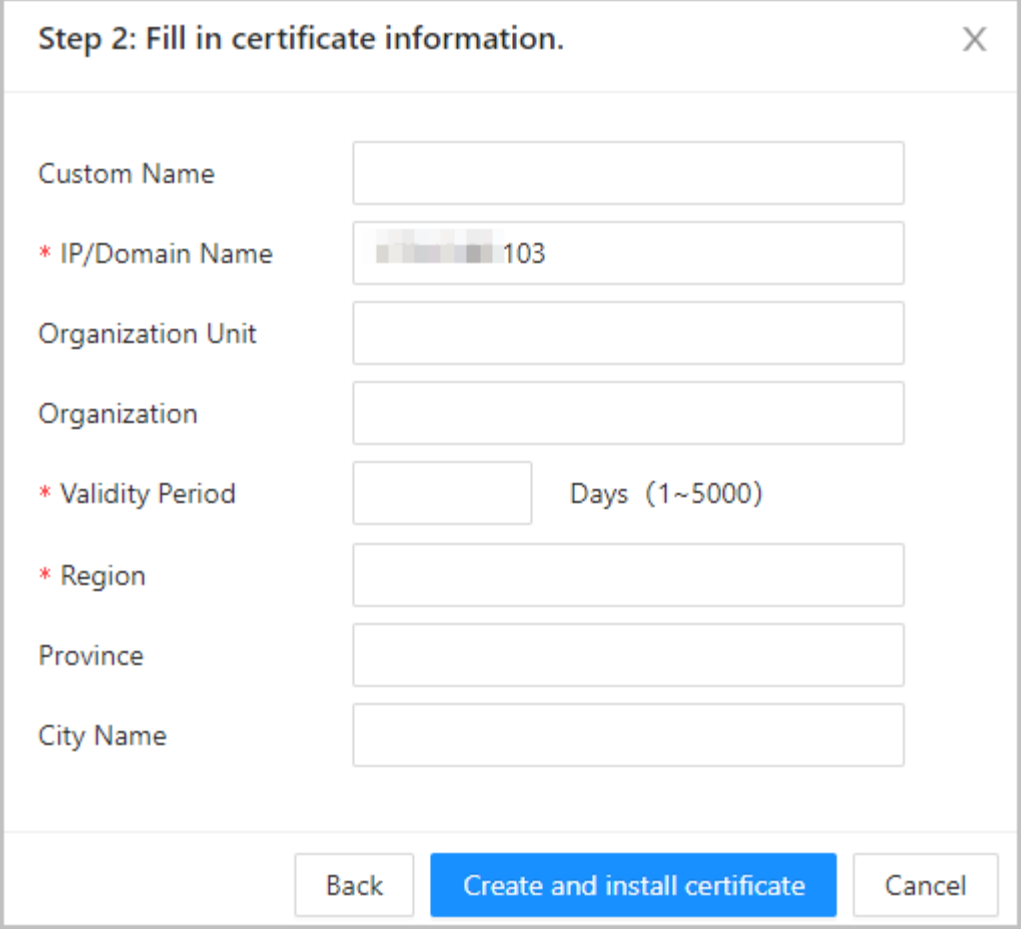
Passo 1 Seleccione  > **Certificado CA** > **Certificado do dispositivo**.

Passo 2 Seleccione **Instalar certificado de dispositivo**.

Passo 3 Seleccione **Criar certificado** e clique em **Seguinte**.

Passo 4 Introduza as informações do certificado.

Figura 3-9 Informações sobre o certificado



Step 2: Fill in certificate information. X

Custom Name

* IP/Domain Name

Organization Unit

Organization

* Validity Period Days (1~5000)

* Region

Province

City Name

Back Create and install certificate Cancel



O nome da região não pode exceder 2 caracteres. Recomendamos que introduza a abreviatura do nome da região.

Passo 5 Clique em **Criar e instalar certificado**.

O certificado recentemente instalado é apresentado na página **Certificado do dispositivo** depois de o certificado ter sido instalado com êxito.

Operações relacionadas

- Clique em **Entrar no modo de edição** na página **Certificado do dispositivo** para editar o nome do certificado.
- Clique em  para transferir o certificado.
- Clique em  para eliminar o certificado.

3.3.4.2 Solicitar e importar o certificado da AC

Importar o certificado CA de terceiros para o Dispositivo.

Procedimento

Passo 1 Seccione  > **Certificado CA** > **Certificado do dispositivo**.

Passo 2 Clique **Instalar certificado do dispositivo**.

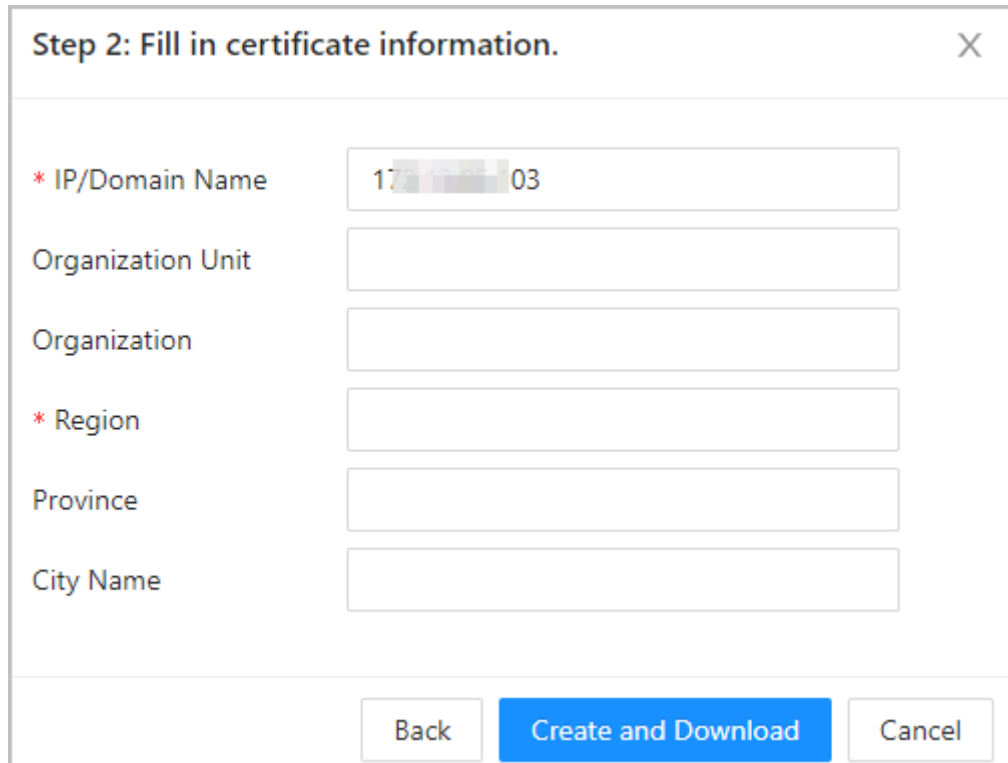
Passo 3 Seccione **Aplicar para certificado CA e Importar (Recomendado)** e clique em

Seguinte.

Passo 4 Introduza as informações do certificado.

- IP/Nome de domínio: o endereço IP ou o nome de domínio do Dispositivo.
- Região: O nome da região não deve exceder 3 caracteres. Recomendamos que introduza a abreviatura do nome da região.

Figura 3-10 Informações sobre o certificado



Step 2: Fill in certificate information. X

* IP/Domain Name 172.16.1.03

Organization Unit

Organization

* Region

Province

City Name

Back Create and Download Cancel

Passo 5 Clique em **Criar e descarregar**.

Guarde o ficheiro do pedido no seu computador.

Passo 6 Aplicar o certificado a uma autoridade CA de terceiros utilizando o ficheiro de pedido.

Passo 7 Importar o certificado CA assinado.

- 1) Guardar o certificado CA no seu computador.
- 2) Clique em **Instalar o certificado do dispositivo**.
- 3) Clique em **Procurar** para seleccionar o certificado CA.
- 4) Clique em **Importar e instalar**.

O certificado recentemente instalado é apresentado na página **Certificado do dispositivo** depois de o certificado ter sido instalado com êxito.

- Clique em **Recriar** para criar novamente o ficheiro de pedido.
- Clique em **Importar mais tarde** para importar o certificado noutra altura.

Operações relacionadas

- Clique em **Entrar no modo de edição** na página **Certificado do dispositivo** para editar o nome do certificado.
- Clique em  para transferir o certificado.
- Clique em  para eliminar o certificado.

3.3.4.3 Instalação de um certificado existente

Se já tiver um certificado e um ficheiro de chave privada, importe o certificado e o ficheiro de chave privada.

Procedimento

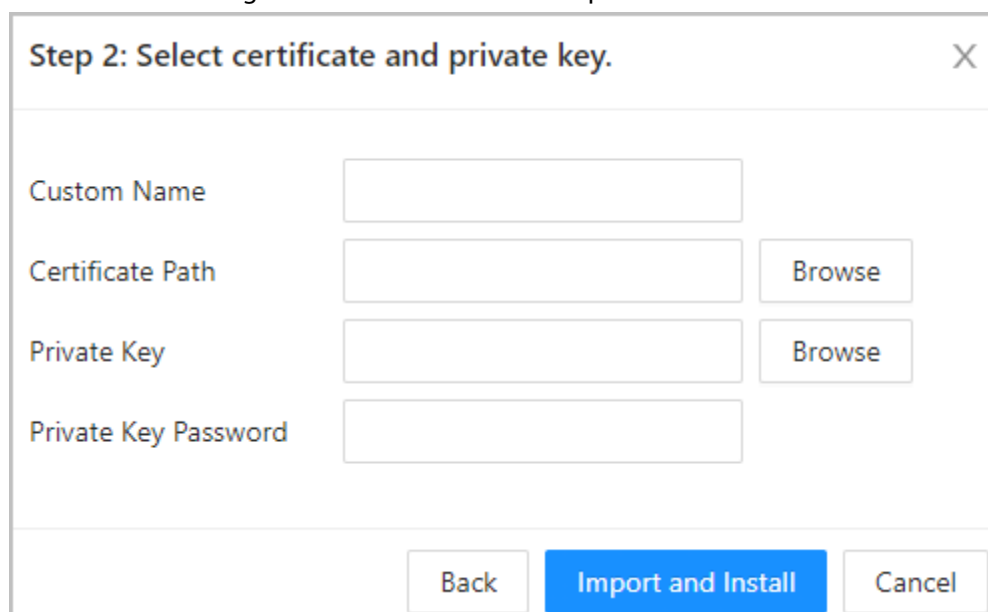
Passo 1 Seleccione **Segurança > Certificado CA > Certificado do dispositivo**.

Passo 2 Clique **Instalar certificado do dispositivo**.

Passo 3 Seccione **Instalar certificado existente** e clique em **Seguinte**.

Passo 4 Clique em **Procurar** para seleccionar o ficheiro do certificado e da chave privada e introduza a palavra-passe da chave privada.

Figura 3-11 Certificado e chave privada



Passo 5 Clique **Importar e instalar**.

O certificado recentemente instalado é apresentado na página **Certificado do dispositivo** depois de o certificado ter sido instalado com êxito.

Operações relacionadas

- Clique em **Entrar no modo de edição** na página **Certificado do dispositivo** para editar o nome do certificado.
- Clique em  para transferir o certificado.
- Clique em  para eliminar o certificado.

3.3.5 Instalar o certificado da CA confiável

Um certificado CA fiável é um certificado digital que é utilizado para validar as identidades de sítios Web e servidores. Por exemplo, quando é utilizado o protocolo 802.1X, o certificado CA dos comutadores é necessário para autenticar a sua identidade.

Informações de base

O 802.1X é um protocolo de autenticação de rede que abre portas para acesso à rede quando uma

organização autentica a identidade de um utilizador e autoriza o acesso do utilizador à rede.

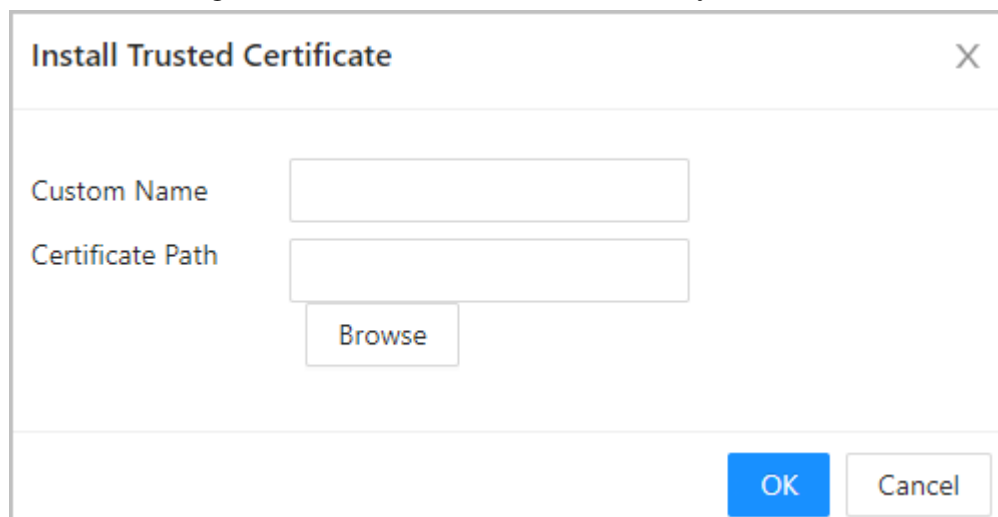
Procedimento

Passo 1 Seleccione  > **Certificado CA** > **Certificados CA fidedignos**.

Passo 2 Seleccione **Instalar certificado confiável**.

Passo 3 Clique em **Procurar** para seleccionar o certificado de confiança.

Figura 3-12 Instalar o certificado de confiança



Passo 4 Clique em **OK**.

O certificado recém-instalado é apresentado na página **Certificados de CA fidedignos** depois de o certificado ser instalado com êxito.

Operações relacionadas

- Clique em **Entrar no modo de edição** na página **Certificado do dispositivo** para editar o nome do certificado.
- Clique em  para transferir o certificado.
- Clique em  para eliminar o certificado.

3.3.6 Aviso de segurança

Procedimento

Passo 1 Seleccione  > **Aviso de segurança**.

Passo 2 Activa a função de aviso de segurança.

Passo 3 Clique em **Aplicar**.

3.3.7 Autenticação de segurança

Procedimento

Passo 1 Seleccione  > **Autenticação de segurança**.

Passo 2 Seleccione um algoritmo de resumo de mensagens.

Passo 3 Clique em **Aplicar**.

Figura 3-13 Autenticação de segurança

Digest Algorithm for Authentication

Digest Algorithm for User Authentication ☒ MD5 ☐ SHA256

3.4 Configuração do VTO

Inicie sessão na página Web do controlador de 2 fios. O sistema apresenta o VTO ligado ao controlador atual e o VTO ligado aos controladores em cascata.

- Clique em **Config** para concluir a configuração detalhada da VTO.
- **Intervalo de chamadas:** O intervalo de números que a VTO pode chamar. Não é possível chamar o número que está para além deste intervalo de chamadas. O intervalo é gerado de acordo com o DIP configurado no controlador de 2 fios. Se o intervalo de chamadas não for gerado e for apresentado a vermelho -, configure novamente o DIP no controlador de 2 fios.

Figura 3-14 VTO

Refresh		
VTO ID	Call Range	Operation
2	1-256	Config
3	1-256	Config

3.4.1 Gestão do pessoal

Gerir e visualizar as informações das pessoas, cartões, palavras-passe e impressões digitais.

Procedimento

Passo 1 Iniciar sessão na página Web.

Passo 2 Clique em **Config** ao lado da VTO correspondente.

Passo 3 Seleccionar **Gestão de pessoas**.

Figura 3-15 Gestão de pessoas

Add Delete Export Import Quick Add						User ID/Name Q
☐	ID	Name	Lock Permission	Authentication Mode	Operation	
☐	14	14	Local Lock, External Lock	0		
☐	15	15	Local Lock, External Lock	0		
☐	16	16	Local Lock, External Lock	0		
☐	17	17	Local Lock, External Lock	0		
☐	18	18	Local Lock, External Lock	0		
☐	19	19	Local Lock, External Lock	0		

Passo 4 Clique **Adicionar**.

Passo 5 Configure os parâmetros e, em seguida, clique em **Adicionar**.

Add

Basic Info

* User ID

* Name

Lock Permission

☒ Local Lock

☒ External Lock

Multi-Door Unlock

☐ After verification is successful, all the locks that the user has permission for will be enabled.

Verification Mode

▼ Password

Not Added



Add

> Card

Not Added

> Fingerprint

Not Added

Add

Add More

Cancel

Quadro 3-2 Descrição dos parâmetros para adicionar uma pessoa

Parâmetro	Descrição
ID do utilizador	Introduzir o ID do utilizador e o nome.
Nome	 O ID de utilizador não pode ser o mesmo que o ID existente.
Permissão de bloqueio	Selecionar a permissão de bloqueio. • Bloqueio local: Bloqueio local. • Bloqueio externo: Bloqueio RS-485.
Desbloqueio de várias portas	Se estiver ativado, após a verificação ser bem sucedida, todos os bloqueios para os quais o utilizador tem permissão serão activados.

Parâmetro	Descrição
Modo de verificação	Adicione a palavra-passe, o cartão ou a impressão digital. - Palavra-passe: Selecione Palavra-passe > Adicionar, introduza a palavra-passe, confirme a palavra-passe e clique em OK. - Cartão: Selecione Cartão > Adicionar, passe o cartão ou introduza o número do cartão e, em seguida, clique em Adicionar.  Clique em Modificar para alterar o dispositivo de leitura de cartões. Se seleccionar Leitor de Matrícula, tem de seleccionar o tipo de cartão entre Cartão IC e Cartão ID. - Impressão digital: Selecione Impressão digital > Adicionar, prima o dedo no scanner 3 vezes continuamente e, em seguida, clique em Adicionar.  Clique em Modificar para alterar o dispositivo de reconhecimento.

Operações relacionadas

- Acrescentar uma pessoa rapidamente.
 1. Clique em **Adição rápida**.
 2. Configurar o número de ID do utilizador a partir do qual pretende começar, introduzir a quantidade total.
 3. Configure a permissão de bloqueio e o desbloqueio de várias portas.
 4. Selecione **Cartão** > **Adicionar**, passe o cartão ou introduza o número do cartão e, em seguida, clique em **Adicionar**.



Clique em **Modificar** para alterar o dispositivo de leitura de cartões. Se seleccionar **Leitor de Matrícula**, tem de seleccionar o tipo de cartão entre Cartão IC e Cartão ID.

5. Clique em **Adicionar**.
- Eliminar, exportar ou importar as informações sobre as pessoas.
Ao exportar as informações sobre as pessoas, é possível configurar a palavra-passe do ficheiro. Introduza a palavra-passe quando importar o ficheiro de informações para outras VTOs.

3.4.2 Mapeamento do número da sala VTH

É possível definir o número de marcação para o ID do VTH correspondente. Após o mapeamento, chamar o VTH apenas através do número configurado.



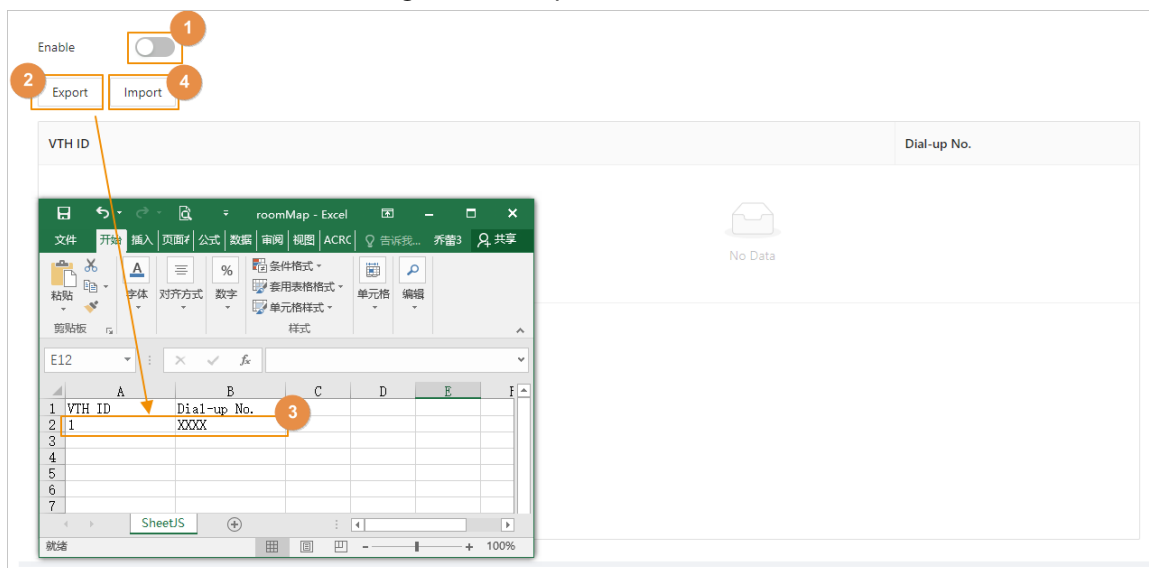
A função de mapeamento do número de divisão VTH só é válida quando o módulo de teclado está ligado

Procedimento

Passo 1 **Iniciar** sessão na página Web.

- Passo** 2 Clique em **Config** ao lado da VTO correspondente.
- Passo** 3 Seleccione **Mapeamento do n.º da sala** e, em seguida, configure o mapeamento.
- 1) Ativar a função.
 - 2) Clique em **Exportar** para descarregar o modelo.
 - 3) Introduza o ID VTH e configure o número de marcação correspondente e, em seguida, guarde o modelo.
 - 4) Clique em **Importar** para carregar o ficheiro.
- Os números de marcação configurados serão apresentados no sistema.

Figura 3-17 Mapeamento



3.4.3 Controlo de acesso

3.4.3.1 Configuração

Procedimento

- Passo 1** Iniciar sessão na página Web.
- Passo** 2 Clique em **Config** ao lado da VTO correspondente.
- Passo** 3 Seleccione **Controlo de acesso > Configuração**.
- Passo 4** Configurar os parâmetros.

Figura 3-18 Controlo de acesso

Quadro 3-3 Descrição dos parâmetros de controlo de acesso

Parâmetro	Descrição
Intervalo entre desbloqueios consecutivos	A porta só pode ser desbloqueada novamente após o intervalo.
Verificar o sinal do detetor de portas antes de bloquear	Ativar a função conforme necessário. Se activada, o estado do detetor de porta será detectado antes do bloqueio para evitar a abertura da porta.
Encriptação de cartões IC	Ativar a função para que a encriptação do cartão IC tenha efeito.
Estado do detetor de portas	• NC: Normalmente fechado. • NA: Normalmente aberto.

Passo 5Clique em **Aplicar**.

3.4.3.2 RS-485

Procedimento

Passo 1Iniciar sessão na página Web.

Passo 2Clique em **Config** ao lado da VTO correspondente.

Passo 3Seleccionar **Controlo de acesso > RS-485**.

Passo 4Configurar os parâmetros do cadeado ligado através da porta RS-485.

Figura 3-19 RS-485

Tabela 3-4 Descrição do RS-485

Parâmetro	Descrição
Tipo de porta	Bloquear por defeito.
Intervalo entre desbloqueios consecutivos	A porta só pode ser desbloqueada novamente após o intervalo.

Passo 5Clique em **Aplicar**.

3.4.4 Módulo

Visualizar a VTO, todos os módulos em cascata e informações sobre a versão. Atualizar a VTO e os módulos.

Procedimento

Passo 1Iniciar sessão na página Web.

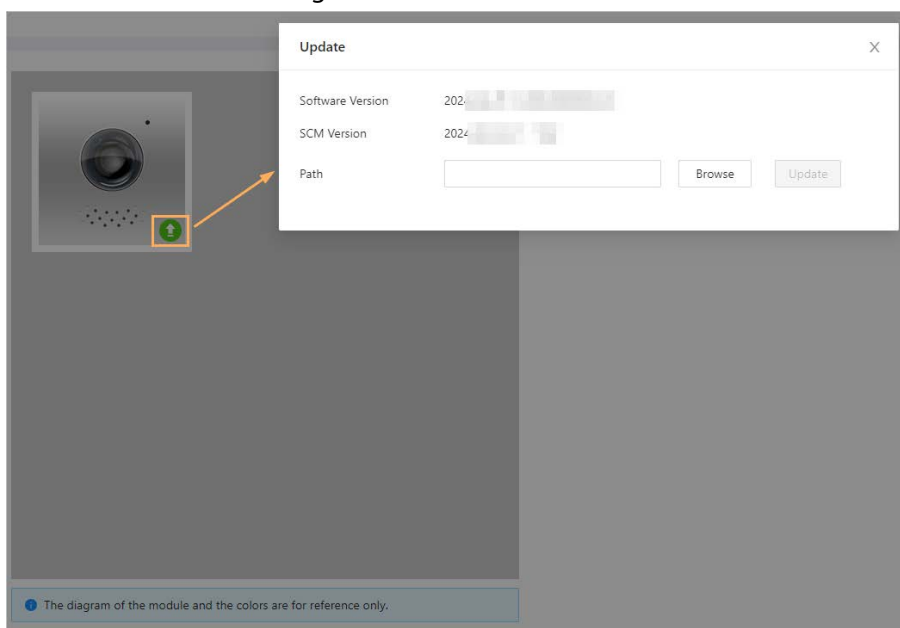
Passo 2Clique em **Config** ao lado da VTO correspondente.

Passo 3Seleccionar **Módulo**.

- Visualizar a VTO e todos os módulos em cascata.

- Clique em  para ver as informações da versão atual.
- Clique em **Procurar** para selecionar o ficheiro de atualização e, em seguida, clique em **Atualizar**.

Figura 3-20 Módulo



3.4.5 Manutenção

Procedimento

Passo 1 Iniciar sessão na página Web.

Passo 2 Clique em **Config** ao lado da VTO correspondente.

Passo 3 Selecione **Manutenção**.

- Clique em **Predefinição de fábrica** para repor as predefinições.
- Clique em **Reiniciar** para reiniciar o controlador.

3.5 Adicionar pessoa

Adicionar a pessoa e enviar as informações para a VTO.

Procedimento

Passo 1 Iniciar sessão na página Web.

Passo 2 Clique **Adicionar pessoa** e, em seguida, configure os parâmetros.

Figura 3-21 Adicionar pessoa

Quadro 3-5 Descrição dos parâmetros para adicionar uma pessoa

Parâmetro	Descrição
ID do utilizador	Introduza o ID do utilizador e o nome.
Nome	 O ID de utilizador não pode ser o mesmo que o ID existente.
Permissão de bloqueio	Selecionar a permissão de bloqueio. - Bloqueio local: Bloqueio local. - Bloqueio externo: Bloqueio RS-485.
Desbloqueio de várias portas	Se estiver ativado, após a verificação ser bem sucedida, todos os bloqueios para os quais o utilizador tem permissão serão activados.

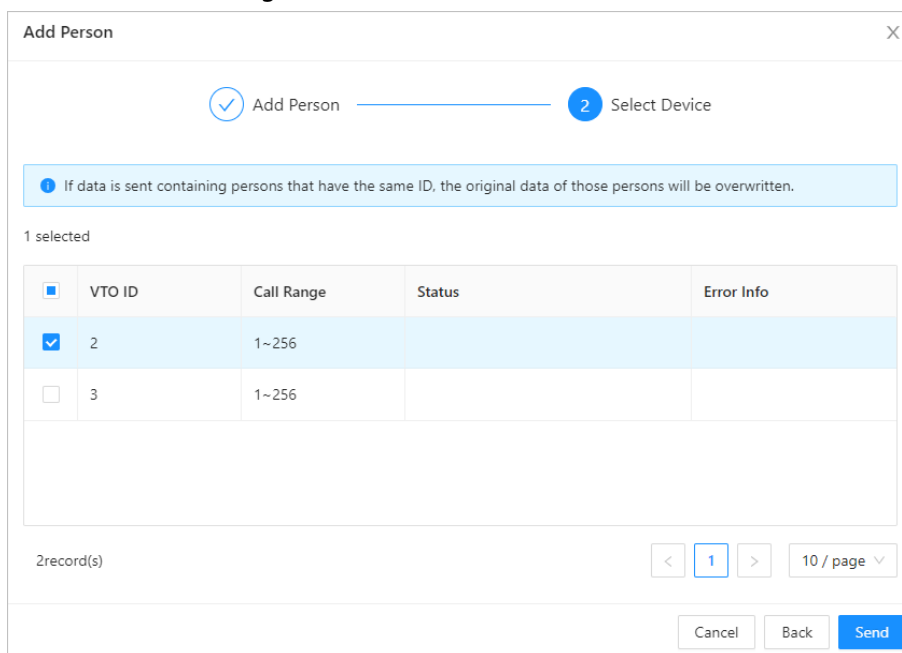
Parâmetro	Descrição
Modo de verificação	Adicione a palavra-passe, o cartão ou a impressão digital. - Palavra-passe: Selecione Palavra-passe > Adicionar, introduza a palavra-passe, confirme a palavra-passe e clique em OK. - Cartão: Selecione Cartão > Adicionar, passe o cartão ou introduza o número do cartão e, em seguida, clique em Adicionar.  Clique em Modificar para alterar o dispositivo de leitura de cartões e o tipo de cartão. - Impressão digital: Selecione Impressão digital > Adicionar, prima o dedo no scanner 3 vezes continuamente e, em seguida, clique em Adicionar.  Clique em Modificar para alterar o dispositivo de reconhecimento.

Passo 3 Clique em **Seguinte**.

Passo 4 Selecione o dispositivo e, em seguida, clique em **Enviar**.

As informações pessoais serão enviadas para o VTO que selecionou.

Figura 3-22 Selecionar a VTO



The screenshot shows a 'Add Person' window with a progress bar indicating 'Add Person' is complete and 'Select Device' is the current step. A message states: 'If data is sent containing persons that have the same ID, the original data of those persons will be overwritten.' Below this, a table lists available VTOs:

	VTO ID	Call Range	Status	Error Info
☒	2	1~256		
☐	3	1~256		

At the bottom, it shows '2 record(s)', navigation arrows, a page indicator '1' of '10 / page', and buttons for 'Cancel', 'Back', and 'Send'.

3.6 Importação de pessoas em lotes

Depois de exportar as informações sobre a pessoa do VTO, pode carregar o ficheiro para importar pessoas em lotes para outros VTOs.

Procedimento

Passo 1 Iniciar sessão na página Web.

Passo 2 Clique **Importação em lote de pessoas**.

Passo 3 Selecione o arquivo, digite a senha que é configurada ao exportar as informações e clique em **Avançar**.

Figura 3-23 Importar pessoas

Batch Import Persons

1 Select File ————— 2 Select Device

File

Password

Passo 4 Selecione o dispositivo e, em seguida, clique em **Enviar**.

As informações pessoais serão enviadas para o VTO que selecionou.

3.7 Definições de rede

3.7.1 Configuração do TCP/IP

É necessário configurar o endereço IP do dispositivo para garantir que este pode comunicar com outros dispositivos.

Procedimento

Passo 1 Iniciar sessão na página Web.

Passo 2 Selecione **Definições de rede > TCP/IP**.

Passo 3 Configurar os parâmetros.

Figura 3-24 TCP/IP

The screenshot displays a network configuration window. At the top, under 'Mode', there are two radio buttons: 'DHCP' and 'Static'. The 'Static' button is selected. Below this, there are several input fields: 'MAC Address', 'IP Address', 'Subnet Mask', 'Default Gateway', 'Preferred DNS', and 'Alternate DNS'. Each field has a small icon to its right, likely for refreshing or clearing the field. At the bottom of the window, there are three buttons: 'Apply' (highlighted in blue), 'Refresh', and 'Default'.

Tabela 3-6 Descrição dos parâmetros TCP/IP

Parâmetro	Descrição
Modo	• DHCP (Protocolo de configuração dinâmica de anfitrião): O Dispositivo será automaticamente atribuído com endereço IP, máscara de sub-rede e gateway. • Estático: Introduzir manualmente o endereço IP, a máscara de sub-rede e o gateway.
Endereço MAC	Endereço MAC do dispositivo.
Endereço IP	Se definir o modo como Estático , configure o endereço IP, a máscara de sub-rede e o gateway.
Máscara de sub-rede	
Gateway predefinido	 • O endereço IPv6 é representado em hexadecimal. • A versão IPv6 não requer a definição de máscaras de sub-rede. • O endereço IP e o gateway predefinido têm de estar no mesmo segmento de rede.
DNS preferido	Definir o endereço IP do servidor DNS preferido.
DNS alternativo	Definir o endereço IP do servidor DNS alternativo.

Passo 4Clique em **Aplicar**.

3.7.2 Configuração dos serviços básicos

Inicie sessão na página Web e, em seguida, selecione **Definições de rede > Serviços básicos**.

Active o protocolo conforme necessário e, em seguida, clique em **Aplicar**.

Figura 3-25 Serviços básicos

SSH ☒

There might be safety risk if this service is enabled.

CGI ☒

Password Reset ☒

Multicast/Broadcast Search ☒

Authentication Mode Security Mode (Recommended) ▼

Emergency Maintenance ☐

For easy access to our after-sales service, enable this function. If the device has any trouble performing functions, such as updating, the system will automatically enable this function.

Password Expires in Never ▼

Private Protocol ☒

*Before enabling private protocol TLS, make sure that the corresponding device or software supports this function.

TLSv1.1 ☐

Apply Refresh Default

Quadro 3-7 Descrição dos serviços de base

Serviço	Descrição
SSH	Se estiver ativado, é possível iniciar sessão na VTO através de SSH.
CGI	A Common Gateway Interface (CGI) oferece um protocolo padrão para os servidores Web executarem programas semelhantes às aplicações de consola executadas num servidor que gera dinamicamente páginas Web. Se estiver ativado, podem ser utilizados comandos CGI. O CGI está ativado por predefinição.
Redefinição da palavra-passe	Ativado por predefinição. Active a função e, em seguida, configure o endereço de correio eletrónico. Após a configuração, pode clicar em Esqueceu-se da palavra-passe? na página de início de sessão para repor a palavra-passe.
Pesquisa Multicast/Broadcast	Active esta função e, em seguida, quando vários utilizadores estiverem a pré-visualizar a imagem de vídeo do dispositivo em simultâneo através da rede, poderão encontrar o seu dispositivo com o protocolo multicast/broadcast.
Modo de autenticação	Modo de segurança (recomendado): O modo não suporta o início de sessão com autenticação Digest, DES e de texto simples. Modo de compatibilidade: O modo suporta o início de sessão com autenticação Digest, DES e de texto simples.
Manutenção de emergência	Quando esta função está activada, se o dispositivo não conseguir reiniciar 5 vezes seguidas, ligará automaticamente uma porta de serviço utilizada pelo apoio técnico para efetuar actualizações e recuperação.
A palavra-passe expira em	Selecione a hora em que a palavra-passe irá expirar.
Protocolo privado	Se estiver ativado, a plataforma pode aceder ao dispositivo com um

Serviço	Descrição
TLsv1.1	protocolo privado.  Existe um risco de segurança se ativar o TLsv1.1.

3.8 Centro de manutenção

3.8.1 Diagnóstico com um clique

O sistema diagnostica automaticamente as configurações e o estado do dispositivo para melhorar o seu desempenho.

Procedimento

Passo 1 Iniciar sessão na página Web.

Passo 2 Seleccionar **Centro de Manutenção > Diagnóstico com um clique**.

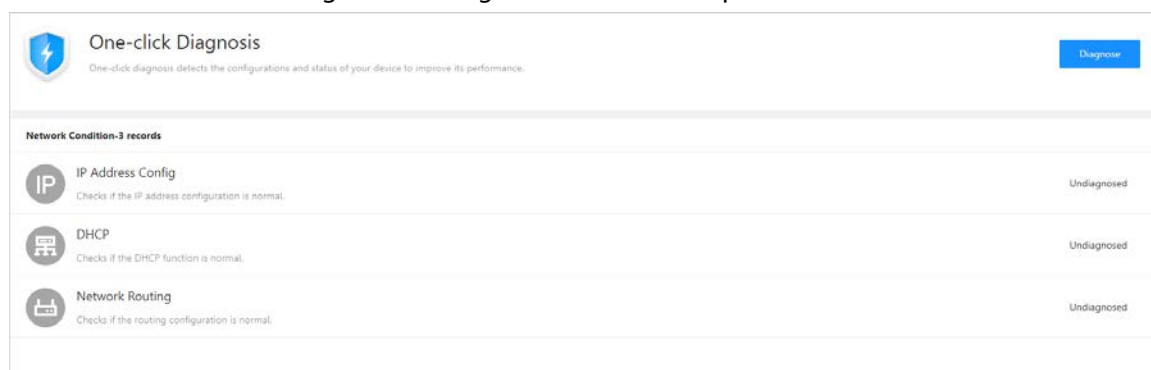
Passo 3 Clique em **Diagnosticar**.

O sistema diagnostica automaticamente as configurações e o estado do dispositivo e apresenta os resultados do diagnóstico após a sua conclusão.

Passo 4 (Opcional) Clique em **Detalhes** para ver os detalhes dos itens anormais.

É possível ignorar a anomalia ou optimizá-la. Também pode clicar em **Diagnosticar novamente** para efetuar novamente o diagnóstico automático.

Figura 3-26 Diagnóstico com um clique



3.8.2 Informações sobre o sistema

Inicie sessão na página Web, selecione **Centro de manutenção > Informações do sistema** e poderá ver o aviso de software de fonte aberta.

Selecione **Informação jurídica** para ver o aviso de software de fonte aberta.

Selecione **Informações do sistema** para ver as informações sobre a versão do controlador.

3.8.3 Exportar e importar ficheiros de configuração

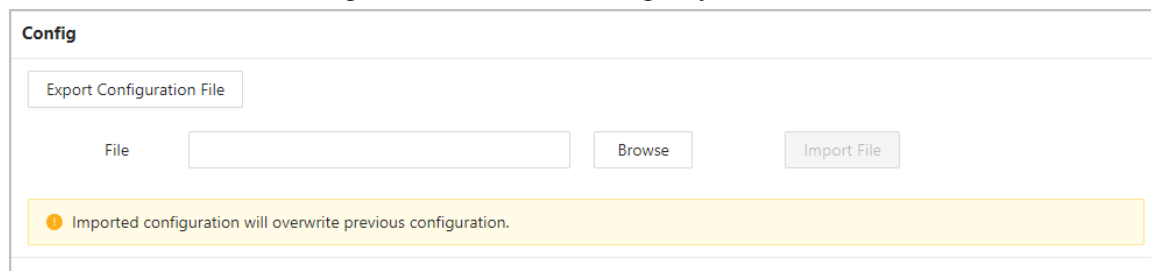
É possível importar e exportar o ficheiro de configuração para o dispositivo. Se pretender aplicar as mesmas configurações a vários dispositivos, pode importar o ficheiro de configuração para os mesmos.

Procedimento

Passo 1 Iniciar sessão na página Web.

Passo 2 Selecione **Centro de manutenção > Config.**

Figura 3-27 Gestão da configuração



The screenshot shows a web interface titled 'Config'. At the top, there is a button labeled 'Export Configuration File'. Below this, there is a 'File' input field, a 'Browse' button, and an 'Import File' button. A yellow warning banner at the bottom states: 'Imported configuration will overwrite previous configuration.'

Passo 3 Exportar ou importar ficheiros de configuração.

- Exportar o ficheiro de configuração.
Clique em **Exportar ficheiro de configuração** para transferir o ficheiro para o computador local.



O IP não será exportado.

- Importar o ficheiro de configuração.
 1. Clique em **Procurar** para selecionar o ficheiro de configuração.
 2. Clique em **Importar configuração**.



Os ficheiros de configuração só podem ser importados para dispositivos que tenham o mesmo modelo.

3.8.4 Atualizar o sistema



- Utilize o ficheiro de atualização correto. Certifique-se de que obtém o ficheiro de atualização correto junto do apoio técnico.
- Não desligue a fonte de alimentação ou a rede, e não reinicie nem desligue o Dispositivo durante a atualização.

Procedimento

Passo 1 Iniciar sessão na página Web.

Passo 2 Seleccione **Centro de manutenção > Atualizar**.

Passo 3 Na área **Atualização de ficheiros**, clique em **Procurar** e, em seguida, carregue o ficheiro de atualização.



O ficheiro de atualização deve ser um ficheiro .bin.

Passo 4 Clique em **Atualizar**.

O controlador de 2 fios será reiniciado após a conclusão da atualização.

Figura 3-28 Atualização de ficheiros

File Update

File

Browse

Update

3.8.5 Manutenção avançada

Adquirir informações sobre o dispositivo e capturar pacotes para facilitar a resolução de problemas pelo pessoal de manutenção.

3.8.5.1 Exportação

Procedimento

Passo 1 Iniciar sessão na página Web.

Passo 2 Selecionar **Centro de manutenção > Manutenção avançada > Exportar**.

Passo 3 Clique em **Exportar** para exportar o número de série, a versão do firmware, os registos de funcionamento do dispositivo e as informações de configuração.

3.8.5.2 Captura de pacotes

Procedimento

Passo 1 Iniciar sessão na página Web.

Passo 2 Selecione **Centro de manutenção > Manutenção avançada > Captura de pacotes**.

Figura 3-29 Captura de pacotes

NIC	Device Address	IP 1: Port 1	IP 2: Port 2	Packet Sniffer Size	Packet Sniffer Backup
eth0	192.168.1.166	Optional	Optional	0.00MB	▶
eth2	192.168.1.101	Optional	Optional	0.00MB	▶

Passo 3 Introduza o endereço IP, clique em ▶

▶ alterações em . ||

Passo 4 Depois de ter adquirido dados suficientes, clique em . ||

Os pacotes capturados são automaticamente descarregados para o seu computador local.

Apêndice 1 Recomendação de segurança

Gestão de contas

1. Utilizar palavras-passe complexas

Consulte as seguintes sugestões para definir as palavras-passe:

- O comprimento não deve ser inferior a 8 caracteres;
- Incluir pelo menos dois tipos de caracteres: letras maiúsculas e minúsculas, números e símbolos;
- Não conter o nome da conta ou o nome da conta na ordem inversa;
- Não utilizar caracteres contínuos, tais como 123, abc, etc;
- Não utilize caracteres repetidos, como 111, aaa, etc.

2. Alterar periodicamente as palavras-passe

Recomenda-se que altere periodicamente a palavra-passe do dispositivo para reduzir o risco de ser adivinhada ou quebrada.

3. Atribuir contas e permissões de forma adequada

Adicionar utilizadores de forma adequada com base nos requisitos de serviço e de gestão e atribuir conjuntos mínimos de permissões aos utilizadores.

4. Ativar a função de bloqueio de conta

A função de bloqueio de conta está activada por predefinição. Aconselha-se que a mantenha activada para proteger a segurança da conta. Após várias tentativas falhadas de introdução da palavra-passe, a conta correspondente e o endereço IP de origem serão bloqueados.

5. Definir e atualizar atempadamente as informações relativas à reposição da palavra-passe

O dispositivo suporta a função de reposição da palavra-passe. Para reduzir o risco de esta função ser utilizada por agentes de ameaças, se houver alguma alteração nas informações, modifique-as atempadamente. Ao definir as perguntas de segurança, recomenda-se que não utilize respostas fáceis de adivinhar.

Configuração do serviço

1. Ativar HTTPS

Recomenda-se que active o HTTPS para aceder a serviços Web através de canais seguros.

2. Transmissão encriptada de áudio e vídeo

Se o conteúdo dos seus dados de áudio e vídeo for muito importante ou sensível, recomenda-se a utilização da função de transmissão encriptada para reduzir o risco de os seus dados de áudio e vídeo serem escutados durante a transmissão.

3. Desativar os serviços não essenciais e utilizar o modo de segurança

Se não for necessário, recomenda-se a desativação de alguns serviços, como SSH, SNMP, SMTP, UPnP, ponto de acesso AP, etc., para reduzir as superfícies de ataque.

Se necessário, é altamente recomendável escolher modos seguros, incluindo, mas não se limitando aos seguintes serviços:

- SNMP: Escolha SNMP v3 e configure encriptação forte e palavras-passe de autenticação.
- SMTP: Escolha TLS para aceder ao servidor da caixa de correio.
- FTP: Escolha SFTP e defina palavras-passe complexas.

- Ponto de acesso AP: Escolha o modo de encriptação WPA2-PSK e defina palavras-passe complexas.
4. **Alterar o HTTP e outras portas de serviço predefinidas**

Recomenda-se que altere a porta predefinida do HTTP e de outros serviços para qualquer porta entre 1024 e 65535 para reduzir o risco de ser adivinhado por agentes de ameaças.

Configuração de rede

1. **Ativar a lista de permissões**

Recomenda-se que active a função de lista de permissões e que apenas permita que os IP da lista de permissões acedam ao dispositivo. Por conseguinte, certifique-se de que adiciona o endereço IP do seu computador e o endereço IP do dispositivo de suporte à lista de permissões.
2. **Vinculação de endereços MAC**

Recomenda-se que associe o endereço IP do gateway ao endereço MAC no dispositivo para reduzir o risco de falsificação de ARP.
3. **Criar um ambiente de rede seguro**

Para melhor garantir a segurança dos dispositivos e reduzir os potenciais riscos cibernéticos, recomenda-se o seguinte

 - Desativar a função de mapeamento de portas do router para evitar o acesso direto aos dispositivos da intranet a partir da rede externa;
 - De acordo com as necessidades reais da rede, particionar a rede: se não houver necessidade de comunicação entre as duas sub-redes, recomenda-se a utilização de VLAN, gateway e outros métodos para particionar a rede de modo a obter o isolamento da rede;
 - Estabelecer um sistema de autenticação de acesso 802.1x para reduzir o risco de acesso ilegal de terminais à rede privada.

Auditoria de segurança

1. **Verificar os utilizadores em linha**

Recomenda-se a verificação regular dos utilizadores em linha para identificar os utilizadores ilegais.
2. **Verificar o registo do dispositivo**

Ao visualizar os registos, pode ficar a conhecer os endereços IP que tentam iniciar sessão no dispositivo e as principais operações dos utilizadores registados.
3. **Configurar o registo de rede**

Devido à capacidade de armazenamento limitada dos dispositivos, o registo armazenado é limitado. Se precisar de guardar o registo durante muito tempo, recomenda-se que active a função de registo de rede para garantir que os registos críticos são sincronizados com o servidor de registo de rede para rastreio.

Segurança de software

1. **Atualizar o firmware atempadamente**

De acordo com as especificações de funcionamento normalizadas da indústria, o firmware dos dispositivos tem de ser atualizado atempadamente para a versão mais recente, de modo a garantir que o dispositivo possui as funções e a segurança mais recentes. Se o dispositivo estiver ligado à rede pública, recomenda-se a ativação da função de deteção automática de atualização em linha, de modo a obter atempadamente as informações de atualização do firmware divulgadas pelo fabricante.

2. **Atualizar atempadamente o software do cliente**

Recomenda-se que descarregue e utilize o software cliente mais recente.

Proteção física

Recomenda-se a proteção física dos dispositivos (especialmente os dispositivos de armazenamento), como a colocação do dispositivo numa sala de máquinas e num armário dedicados, e o controlo de acesso e a gestão de chaves para evitar que pessoal não autorizado danifique o hardware e outro equipamento periférico (por exemplo, disco flash USB, porta série).