

Manual do Usuário

TERMINAL FACIAL CORE WA04C-W-10

Obrigado por escolher nosso produto. Leia atentamente as instruções antes de utilizá-lo. Siga estas instruções para garantir o funcionamento correto do produto. As imagens apresentadas neste manual são meramente ilustrativas.



Para mais detalhes, visite o site da nossa empresa
www.weg.net/weghome.

Convenções do Documento

Convenções usadas neste manual são listadas abaixo:

Convenções da GUI

Para Software	
Convenção	Descrição
Negrito	Usado para identificar nomes de interfaces de software, por exemplo, OK , Confirmar , Cancelar .
>	Menus de vários níveis são separados por estes colchetes. Por exemplo, Arquivo > Criar > Pasta.
Para Dispositivo	
Convenção	Descrição
< >	Nomes de botões ou teclas para dispositivos. Por exemplo, pressione <OK>.
[]	Nomes de janelas, itens de menu, tabelas de dados e nomes de campos estão entre colchetes. Por exemplo, abra a janela [Novo Usuário]..
/	Menus de vários níveis são separados por barras. Por exemplo, [Arquivo/Criar/Pasta].

Símbolos

Convenção	Descrição
	Isso representa uma nota que precisa de mais atenção.
	As informações gerais que ajudam a realizar as operações mais rapidamente.
	A informação que é significativa.
	Cuidado tomado para evitar perigo ou erros.
	A declaração ou evento que adverte sobre algo ou que serve como exemplo de advertência.

SUMÁRIO

1. MEDIDAS DE SEGURANÇA	5
2. SEGURANÇA ELÉTRICA.....	6
3. SEGURANÇA OPERACIONAL.....	6
4. INSTRUÇÃO DE USO	7
4.1 POSIÇÃO EM PÉ, POSTURA E EXPRESSÃO FACIAL.....	7
4.2 REGISTRO DE MODELO DE ROSTO.....	8
4.3 INTERFACE DE ESPERA.....	9
4.4 TECLADO VIRTUAL	9
4.5 MODO DE VERIFICAÇÃO	10
4.5.1 VERIFICAÇÃO POR CARTÃO	10
4.5.2 VERIFICAÇÃO FACIAL.....	11
4.5.3 VERIFICAÇÃO DE SENHA	13
4.5.4 VERIFICAÇÃO COMBINADA.....	15
5 MENU PRINCIPAL.....	16
6 GERENCIAMENTO DE USUÁRIOS.....	18
6.1.2 FUNÇÃO DE USUÁRIO.....	19
6.1.3 REGISTRAR FACE.....	19
6.1.4 CARTÃO	20
6.1.5 SENHA.....	20
6.1.6 FOTO DO USUÁRIO.....	21
6.1.7 FUNÇÃO DE CONTROLE DE ACESSO.....	21
6.2 TODOS OS USUÁRIOS	22
6.3 EDITAR USUÁRIO.....	22
6.4 EXCLUIR USUÁRIO.....	23
6.5 ESTILO DE EXIBIÇÃO.....	23
7 PRIVILÉGIOS DO USUÁRIO	25
8 COMUNICAÇÃO	27
8.1 TCP/IP	27
8.2 COMUNICAÇÃO SERIAL	28
8.3 CONFIGURAÇÃO DE COMUNICAÇÃO	29
8.4 CONFIGURAÇÕES DE WI-FI.....	30
8.5 CONFIGURAÇÕES DO SERVIDOR EM NUVEM.....	31
8.6 CONFIGURAÇÃO WIEGAND.....	32
8.6.1 ENTRADA WIEGAND.....	32
8.6.2 SAÍDA WIEGAND.....	34
8.7 DIAGNÓSTICO DE REDE	35
9 CONFIGURAÇÕES DO SISTEMA	36
9.1 DATA E HORA.....	36
9.2 CONFIGURAÇÕES DE REGRAS DE ACESSO	37
9.3 PARÂMETROS DE FACE	38
9.4 CONFIGURAÇÃO DE SEGURANÇA.....	40
9.5 ATUALIZAÇÃO USB.....	41

9.6	ATUALIZAR FIRMWARE ONLINE.....	42
9.7	RESET DE FÁBRICA.....	42
10	PERSONALIZAÇÃO.....	43
10.1	CONFIGURAÇÕES DA INTERFACE DO USUÁRIO.....	43
10.2	CONFIGURAÇÕES DE VOZ.....	44
10.3	ALARME.....	45
10.4	MODO STATUS DE PONTO.....	46
10.5	MAPEAMENTOS DE TECLAS DE ATALHO.....	47
11	GERENCIAMENTO DE DADOS.....	48
11.1	EXCLUIR DADOS.....	48
12	INTERFONE.....	50
12.1	CONFIGURAÇÕES SIP.....	50
12.1.1	CONFIGURAÇÕES LOCAIS.....	50
12.1.2	OPÇÕES DE ÁUDIO.....	52
12.1.3	OPÇÕES DE VÍDEO.....	52
12.1.4	OPÇÕES DE COMPRA.....	53
12.1.5	LISTA DE CONTATOS.....	54
12.1.6	CONFIGURAÇÕES DE ATALHO DE CHAMADA.....	55
12.1.7	CONFIGURAÇÕES AVANÇADAS.....	56
12.2	CONFIGURAÇÃO DA CAMPAINHA.....	56
12.3	CONFIGURAÇÕES DO ONVIF.....	57
13	CONTROLE DE ACESSO.....	59
13.1	OPÇÕES DE CONTROLE DE ACESSO.....	59
13.2	CONFIGURAÇÃO DE REGRA DE TEMPO.....	61
13.3	FERIADOS.....	62
13.4	ACESSO COMBINADO.....	63
13.5	CONFIGURAÇÃO ANTI-PASSBACK.....	64
13.6	OPÇÕES DE COAÇÃO.....	65
14	GERENCIADOR USB.....	66
14.1	BAIXAR USB.....	66
14.2	USB UPLOAD.....	67
15	REGISTROS.....	68
16	AUTO TESTE.....	70
17	INFORMAÇÃO DO SISTEMA.....	71
18	INTERFACE WEB.....	72
19	INSTALAÇÃO.....	74
20	PORTAS UTILIZADAS.....	79
21	COMO ADICIONAR O TERMINAL FACIAL NO WEG BIOGUARD.....	80

1. Medidas de Segurança

As instruções abaixo têm como objetivo garantir que o usuário possa usar o produto corretamente para evitar perigos ou perda de bens. As precauções a seguir visam manter os usuários seguros e prevenir danos. Leia atentamente antes da instalação.

 O não cumprimento das instruções pode levar a danos ao produto ou ferimentos físicos (podendo até causar a morte).

1. **Leia, siga e retenha as instruções** - Todas as instruções de segurança e operacionais devem ser lidas e seguidas corretamente antes de colocar o dispositivo em serviço.
2. **Não ignore os avisos** - Atenha-se a todos os avisos na unidade e nas instruções de operação.
3. **Acessórios** - Use apenas acessórios recomendados pelo fabricante ou vendidos com o produto. Por favor, não utilize nenhum outro componente que não seja o material sugerido pelo fabricante.
4. **Precauções para a instalação** - Não coloque este dispositivo em um suporte ou estrutura instável. Ele pode cair e causar ferimentos graves a pessoas e danos ao dispositivo.
5. **Serviço** - Não tente consertar esta unidade sozinho. Abrir ou remover as tampas pode expô-lo a tensões perigosas ou outros riscos.
6. **Danos que exigem serviço** - Desconecte o sistema da fonte de alimentação CA ou CC da rede elétrica e chame um técnico de serviço nas seguintes condições:
 - Quando o controle do cabo ou da conexão for afetado.
 - Quando o líquido foi derramado ou um item caiu no sistema.
 - Se o sistema é exposto à água ou a intempéries condições (chuva, neve e mais).
 - Se o sistema não estiver funcionando normalmente, siga as instruções de operação.

Apenas altere os controles definidos nas instruções de operação. O ajuste incorreto dos controles pode resultar em danos e exigir a intervenção de um técnico qualificado para retornar o dispositivo à operação normal.

E não conecte vários dispositivos a um único adaptador de energia, pois a sobrecarga do adaptador pode causar superaquecimento ou risco de incêndio.

7. **Peças de reposição** - Quando peças de reposição forem necessárias, os técnicos de serviço devem usar apenas peças de reposição fornecidas pelo fornecedor. Substitutos não autorizados podem resultar em queimaduras, choques ou outros perigos.
8. **Verificação de segurança** - Após a conclusão dos serviços ou reparos na unidade, peça ao técnico de serviço que realize verificações de segurança para garantir o funcionamento adequado do dispositivo.
9. **Fontes de alimentação** - Opere o sistema somente com a fonte de alimentação indicada no rótulo. Se o tipo de fonte de alimentação a ser utilizada não estiver claro, ligue para o seu revendedor.
10. **Raio** - Pode instalar para-raios externos para proteção contra tempestades elétricas. Impede que picos de energia destruam o sistema.

Recomenda-se instalar os dispositivos em áreas com acesso limitado.

2. Segurança Elétrica

- Antes de conectar um cabo externo ao dispositivo, complete o aterramento corretamente e configure a proteção contra surtos; caso contrário, a eletricidade estática danificará a placa principal.
- Certifique-se de que a energia esteja desligada antes de conectar, instalar ou desmontar o dispositivo.
- Certifique-se de que o sinal conectado ao dispositivo seja um sinal de baixa corrente (chave); caso contrário, os componentes do dispositivo serão danificados.
- Certifique-se de que a tensão padrão aplicável ao seu país ou região esteja sendo aplicada. Se você não tiver certeza sobre a tensão padrão aprovada, consulte a sua companhia de energia elétrica local. Desconformidade de potência pode causar curto-circuito ou danos ao dispositivo.
- Em caso de danos na fonte de alimentação, devolva o dispositivo a pessoal técnico profissional ou ao seu revendedor para reparo.
- Para evitar interferências, mantenha o dispositivo longe de dispositivos com alta radiação eletromagnética, como geradores (incluindo geradores elétricos), rádios, televisores, monitores (especialmente CRT) ou alto-falantes.

3. Segurança Operacional

- Se fumaça, odor ou ruído saírem do aparelho, desligue-o imediatamente e desconecte o cabo de alimentação. Em seguida, entre em contato com a assistência técnica.
- O transporte e outras causas imprevisíveis podem danificar o hardware do dispositivo. Verifique se o dispositivo apresenta algum dano intenso antes da instalação.
- Se o dispositivo apresentar defeitos graves que você não consiga resolver, entre em contato com seu revendedor o mais breve possível.
- Poeira, umidade e mudanças bruscas de temperatura podem afetar a vida útil do dispositivo. Recomenda-se não manter o dispositivo nessas condições.
- Não guarde o dispositivo em local que vibre. Manuseie o dispositivo com cuidado. Não coloque objetos pesados sobre o dispositivo.
- Não aplique resina, álcool, benzeno, pesticidas e outras substâncias voláteis que possam danificar a caixa do dispositivo. Limpe os acessórios do dispositivo com um pano macio ou uma pequena quantidade de agente de limpeza.
- Se você tiver alguma dúvida técnica sobre o uso, entre em contato com pessoal técnico certificado ou experiente.



Nota:

- Certifique-se de que a polaridade positiva e a polaridade negativa da fonte de alimentação DC 12V estejam conectadas corretamente. Uma conexão reversa pode danificar o dispositivo. Não é aconselhável conectar a fonte de alimentação AC 24V à porta de entrada DC 12V.
- Certifique-se de conectar os fios seguindo a polaridade positiva e negativa mostradas na placa de identificação do dispositivo.

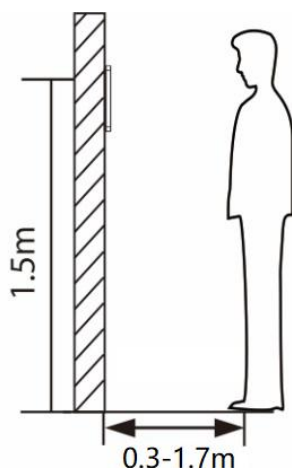
- O serviço de garantia não cobre danos acidentais, danos causados por má operação, e danos causados por instalação ou reparo independente do produto pelo usuário.

4. Instrução de uso

Antes de entrar nos recursos e funções do dispositivo, é recomendável estar familiarizado com os fundamentos abaixo.

4.1 Posição em pé, postura e expressão facial

- A distância recomendada



A distância entre o dispositivo e o usuário, que varia de 1,55 m a 1,85 m, é recomendada entre 0,3 m e 2 m. Os usuários podem se mover ligeiramente para frente ou para trás para melhorar a qualidade das imagens faciais capturadas.

- Postura e Expressão Facial Recomendadas:



Postura em pé



Expressão Facial



Nota: Por favor, mantenha sua expressão facial e postura em pé naturais durante a inscrição ou verificação.

4.2 Registro de Modelo de Rosto

Tente manter o rosto no centro da tela durante o registro. Por favor, olhe para a câmera e fique parado durante o registro do modelo de rosto. A tela deve ficar assim:



Método correto de registro e autenticação facial

- **Recomendação para registro facial**

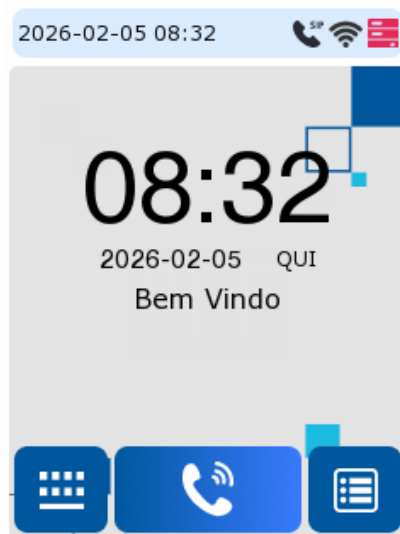
- Ao registrar o rosto modelo, mantenha uma distância de 40 cm a 80 cm entre o dispositivo e o rosto.
- Cuidado para não mudar sua expressão facial. (Cara sorridente, cara séria, piscada, etc.)
- Se você não seguir as instruções na tela, o reconhecimento facial modelo registro pode demorar mais ou falhar.
- Cuidado para não cobrir os olhos ou as sobrancelhas.
- Não use chapéus, máscaras, óculos escuros ou óculos de grau.
- Cuidado para não exibir dois rostos na tela. Cadastre uma pessoa por vez.
- Recomenda-se que o usuário que usa óculos registre ambos os rostos, com e sem óculos.

- **Recomendação para autenticação de um rosto modelo**

- Certifique-se de que o rosto apareça dentro da guia exibida na tela do dispositivo.
- Se os óculos foram trocados, a autenticação pode falhar. Se o rosto sem óculos foi registrado, autentique o rosto modelo sem óculos. Se o rosto com óculos foi registrado, autentique o rosto com os óculos usados anteriormente.
- Se parte do rosto estiver coberta por um chapéu, máscara, tapa-olho ou óculos escuros, a autenticação poderá falhar. Não cubra o rosto, permita que o dispositivo reconheça tanto as sobrancelhas quanto o rosto.

4.3 Interface de espera

Depois de conectar a fonte de alimentação, o seguinte modelo de interface de espera é exibido:



- Clique no  ícone para inserir o modelo de interface de entrada do ID do usuário.
- Quando não houver um Superadministrador definido no dispositivo, toque no  ícone para ir para o menu.
- Depois de definir o Super Administrador no dispositivo, é necessária a verificação do Superadministrador antes de entrar nas funções do menu.
- **Observação:** Para a segurança do dispositivo, recomenda-se registrar um Super Administrador na primeira vez que o dispositivo for usado.
- No modelo de interface em standby, as opções de estado de punção também podem ser mostradas e usadas diretamente. Clique em qualquer lugar da tela além dos ícones, e seis teclas de atalho aparecem na tela, conforme mostrado na figura abaixo:

4.4 Teclado virtual



4.5 Modo de verificação

4.5.1 Verificação por cartão

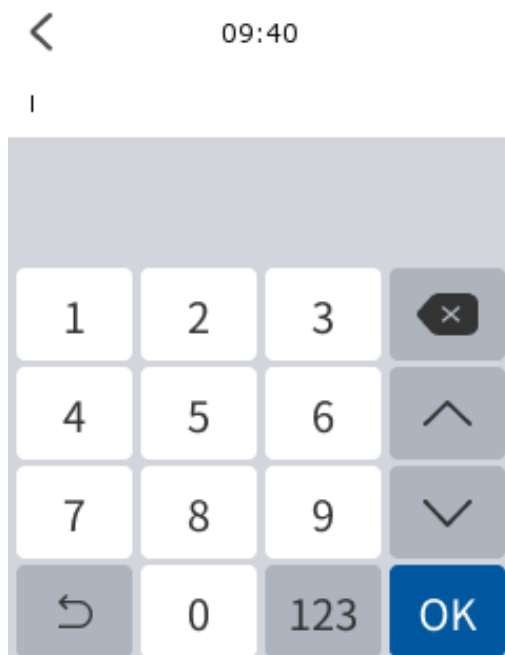
Modo de Verificação de cartão 1:N

- O Modo de Verificação de Cartão 1:N compara o número do cartão na área de indução do cartão com todos os dados do número do cartão registrados no dispositivo. A seguinte tela é exibida na tela de verificação do cartão.



Verificação de cartão 1:1

O modo de Verificação de Cartão 1:1 compara o número do cartão na área de indução do cartão com o número associado ao ID de usuário do funcionário registrado no dispositivo. Pressione  no modelo de interface principal para abrir o modo de verificação de cartão 1:1. Insira o ID do usuário e clique em OK.



Se um funcionário registrar uma impressão digital, rosto e senha além do cartão, a seguinte tela aparecerá. Selecione Cartão para entrar no modo de verificação do cartão.



4.5.2 Verificação Facial

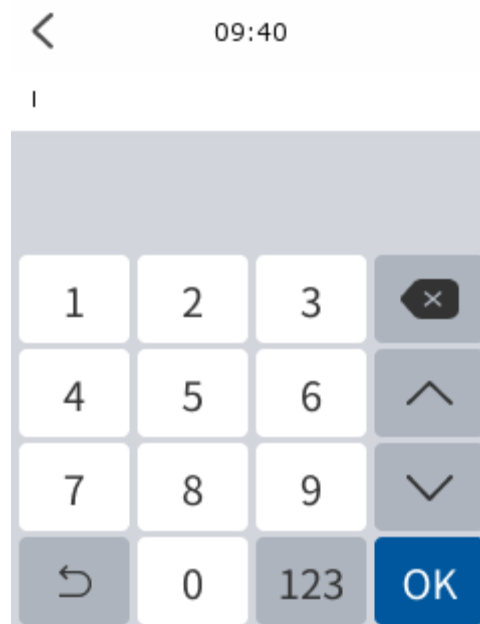
- **Verificação Facial 1:N**

Neste modo de verificação, o dispositivo compara as imagens faciais coletadas com todos os dados faciais registrados no dispositivo. A seguir, está a amostra de um resultado de comparação bem-sucedido.

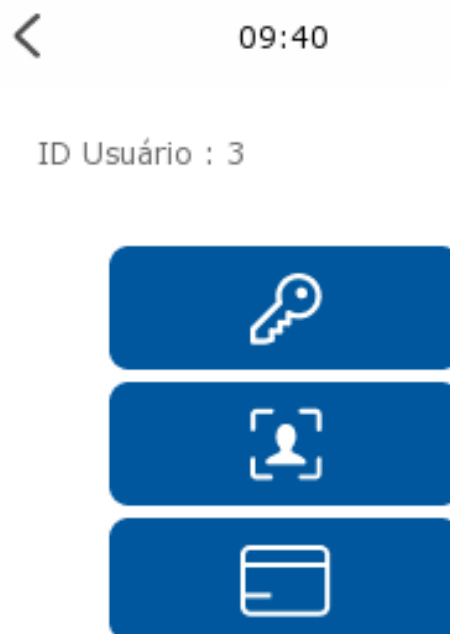


- **Verificação facial 1:1**

Neste modo de verificação, o dispositivo compara o rosto capturado pela câmera com o modelo facial relacionado ao ID do usuário inserido. Pressione o ícone  na interface principal e entre no modo de verificação facial 1:1 e insira o ID de usuário e clique em **OK**.



Se um funcionário registrar uma impressão digital, rosto e senha além do cartão, a seguinte tela aparecerá. Selecione Cartão para entrar no modo de verificação do cartão. Selecione o  ícone para entrar no modo de verificação do modelo de face.

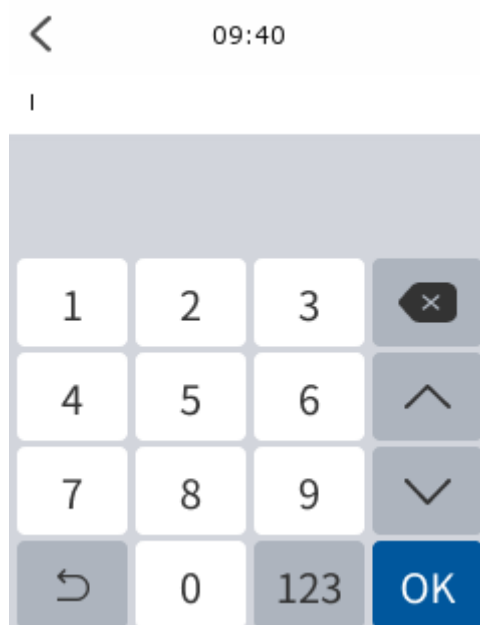


Após a verificação bem-sucedida, a caixa de prompt exibe **Verificado com sucesso**, conforme mostrado abaixo:

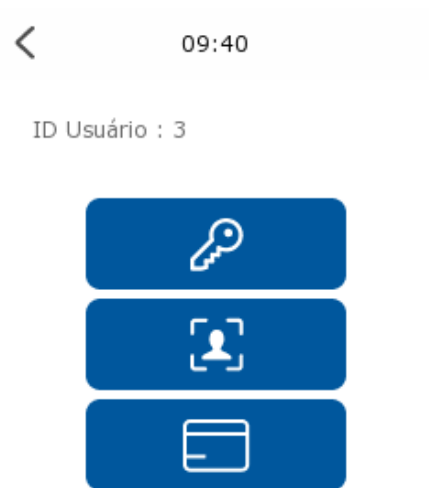


4.5.3 Verificação de senha

O dispositivo compara a senha digitada com a senha registrada pelo ID de usuário fornecido. Clique no  botão na tela principal para entrar no modo de verificação de senha 1:1. Em seguida, insira o ID do usuário e pressione OK.



Se um funcionário registrar uma digital, rosto e cartão além da senha, a seguinte tela aparecerá. Selecione Senha para entrar no modo de verificação de senha. Selecione o  ícone para entrar no modo de verificação de senha.



Insira a senha e pressione OK.



A tela a seguir é exibida, após inserir uma senha correta e uma senha errada, respectivamente.

A verificação foi bem-sucedida:



A verificação falhou:



4.5.4 Verificação combinada

Este dispositivo permite que você use diferentes tipos de métodos de verificação para aumentar a segurança. Há um total de 21 diferentes combinações de verificação que podem ser implementadas.

Símbolo	Definição	Explicação
/	ou	Este método compara a verificação inserida de uma pessoa com o modelo de verificação relacionado previamente armazenado para aquele ID de Pessoal no Dispositivo.
+	e	Este método compara a verificação inserida de uma pessoa com todos os modelos de verificação previamente armazenados para aquele ID de Pessoal no Dispositivo.



Procedimento de configuração do Modo de Verificação Combinada:

- A verificação combinada exige que o pessoal registre todos os diferentes métodos de verificação. Caso contrário, os funcionários não conseguirão verificar com sucesso o processo de verificação combinada.
- Por exemplo, se um funcionário registrou apenas os dados da senha, mas o modo de verificação do dispositivo está definido como "Senha + Cartão", o funcionário não conseguirá concluir o procedimento de verificação com sucesso.

Razão:

- Isso ocorre porque o Dispositivo compara o modelo de senha da pessoa com o modelo de verificação registrado (tanto o Cartão quanto a Senha) previamente armazenado para aquele ID de Pessoal no Dispositivo.
- Mas, como o funcionário registrou apenas sua senha e não seu cartão, o processo de verificação não será bem-sucedido, e o dispositivo exibirá "Verificação Falhou."

5 Menu Principal

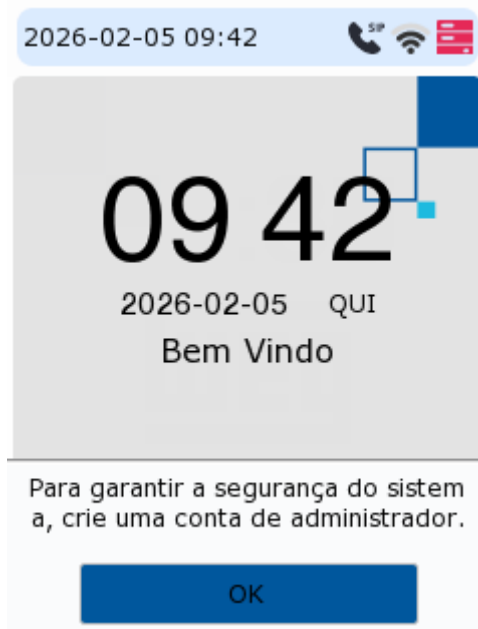
Pressione  na interface de espera para entrar no **menu principal**, a seguinte tela será exibida:



Descrição da função

Menu	Descrição
Usuarios	Para adicionar, editar, visualizar e excluir informações de um usuário.
Priv. usuário	Para definir o escopo de permissão da função personalizada e do cadastrador para os usuários, por exemplo, os direitos operacionais do sistema.
Conf. Com.	Para configurar os parâmetros relevantes de Rede, Conexão de PC, Wi-Fi, Servidor em nuvem e Diagnóstico de Rede.
Sistema	Para definir parâmetros relacionados ao sistema, incluindo data e hora, Configurações de Logs de Acesso/Frequência, Impressão digital, Configurações do Tipo de Dispositivo, Configurações de Segurança, Atualização, USB, Atualizar Firmware Online e Redefinir as configurações de fábrica.
Personalização	Para personalizar as configurações de Interface do Usuário, Voz, Horários do Alarme, Opções de Estado de Registro de Ponto e Atalhos de Teclado.
Ger. dados	Para excluir os dados.
Interfone	Para definir os parâmetros relevantes de interfone, incluindo Configurações SIP, campainha e ONVIF.
Controle acesso	Para definir os parâmetros da fechadura e do dispositivo de controle de acesso correspondente, incluindo opções como Horário, Regra, Feriado, Configurações, Combinar verificação e Configurações da Opção de Coação.
Ger. pen drive	Para carregar ou baixar os dados específicos por um pen drive.
Proc. registros	Para consultar os registros de evento, verificar fotos de presença e Lista de fotos de bloqueados.
Auto teste	Para testar automaticamente se cada módulo funciona corretamente, incluindo a tela LCD e o áudio, Microfone, Teclado, sensor de impressão digital, câmera e Relógio de Tempo Real.
Info. sistema	Para visualizar a Política de Privacidade, a capacidade de dados e as informações do dispositivo e do firmware do dispositivo atual.

Observação: quando os usuários usam o produto pela primeira vez, eles devem operá-lo após definir os privilégios de administrador. Toque em **Gerenciamento de usuário** para adicionar um administrador ou editar as permissões de usuário como superadministrador. Se o produto não tiver uma configuração de administrador, o sistema mostrará um prompt de comando de configuração de administrador toda vez que você entrar no menu do dispositivo.



6 Gerenciamento de usuários

6.1 Novo Cadastro de Usuário

Clique em **Usuário** no menu principal e clique em **Novo**.



6.1.1 Registre um ID de usuário e Nome

Toque em **Novo usuário**. Insira o ID de usuário e o nome.

A imagem mostra um formulário de registro de usuário. No topo, há uma barra de navegação com o título "Editar : 3" e ícones de seta para trás e para frente. O formulário contém os seguintes campos: "ID Usuário" com o valor "3", "Nome" com o valor "Mike", "Tipo de Usuário" com o valor "Comum", "Face" com o valor "1", "Cartão" com o valor "1", e "Senha" com o valor "*****".

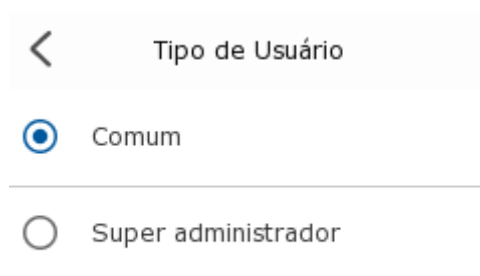
Anotações:

- Um nome de usuário pode conter no máximo 34 caracteres.
- O ID do usuário pode conter de 1 a 14 dígitos por padrão.
- Durante o registro inicial, você pode modificar seu ID, que não pode ser modificado após o registro.
- Se uma mensagem "**Duplicado!**" aparecer, você deve escolher outro ID, pois o ID de usuário inserido já existe.

6.1.2 Função de usuário

Na interface do novo usuário, toque em **Função do usuário** para definir a função do usuário como **Usuário normal** ou **Superadministrador**.

- **Super Admin:** O Super Administrador possui todos os privilégios de gerenciamento no Dispositivo.
- **Usuário Comum:** Se o Super Administrador já estiver registrado no dispositivo, os Usuários Comuns não terão privilégio para gerenciar o sistema e só poderão acessar as verificações de autenticação.
- **Funções Definidas pelo Usuário:** O Usuário Comum também pode receber funções personalizadas com Função Definida pelo Usuário. O usuário pode ter permissão para acessar várias opções de menu conforme necessário.



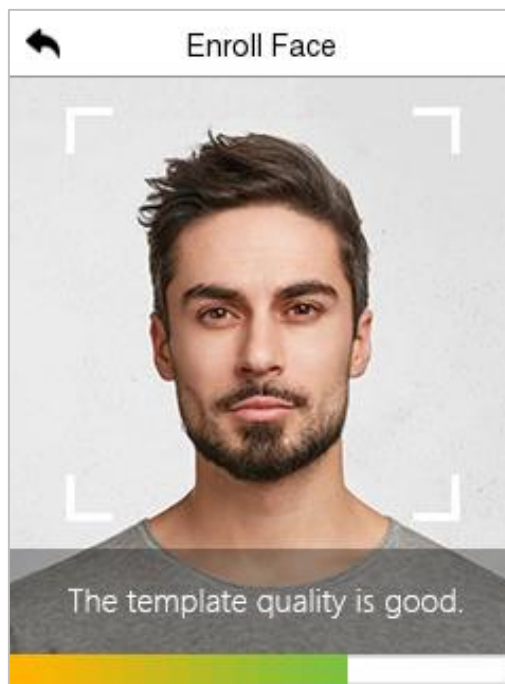
A imagem mostra uma interface de usuário com o título "Tipo de Usuário". Há uma seta de retorno no canto superior esquerdo. Abaixo do título, há duas opções de seleção: "Comum" com um botão de rádio selecionado (um círculo azul com um ponto branco) e "Super administrador" com um botão de rádio não selecionado (um círculo cinza). Há uma linha horizontal separando as duas opções.

Observação: Se a função de usuário selecionada for Super Admin, o usuário deverá passar pela autenticação de identidade para acessar o menu principal. A autenticação é baseada no(s) método(s) de autenticação que o super administrador registrou.

6.1.3 Registrar face

Selecione **Face** na interface **Novo Usuário** para entrar na página de registro facial.

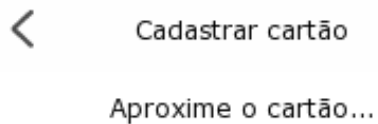
- Por favor, posicione-se de frente para a câmera de forma que sua imagem facial caiba dentro da caixa guia branca e permaneça imóvel durante o registro facial.
- Uma barra de progresso aparece enquanto o rosto é registrado e então "**Inscrito com sucesso**" é exibido assim que a barra de progresso é concluída.
- Se o rosto já estiver registrado, então, a mensagem "**Rosto Duplicado**" aparece. A interface de registro é a seguinte:



6.1.4 Cartão

Selecione **Cartão** na interface **Novo Usuário** para inserir a página de registro do cartão.

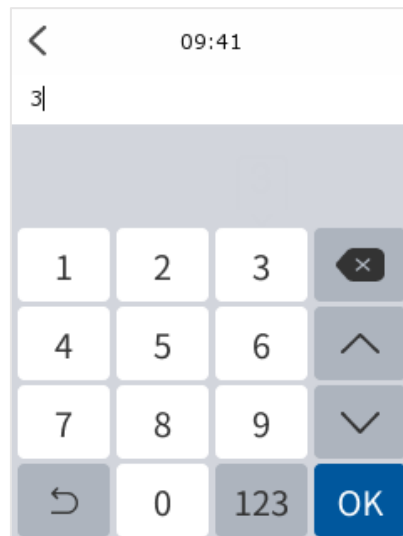
- Na interface do cartão, passe o cartão sob a área de leitura. O registro do cartão será concluído com sucesso.
- Se o cartão já foi registrado, a mensagem "Erro! Cartão já cadastrado" aparece. A interface de registro aparece da seguinte forma:



6.1.5 Senha

Toque em **Senha** na interface do **novo usuário** para entrar na página de registro de senha.

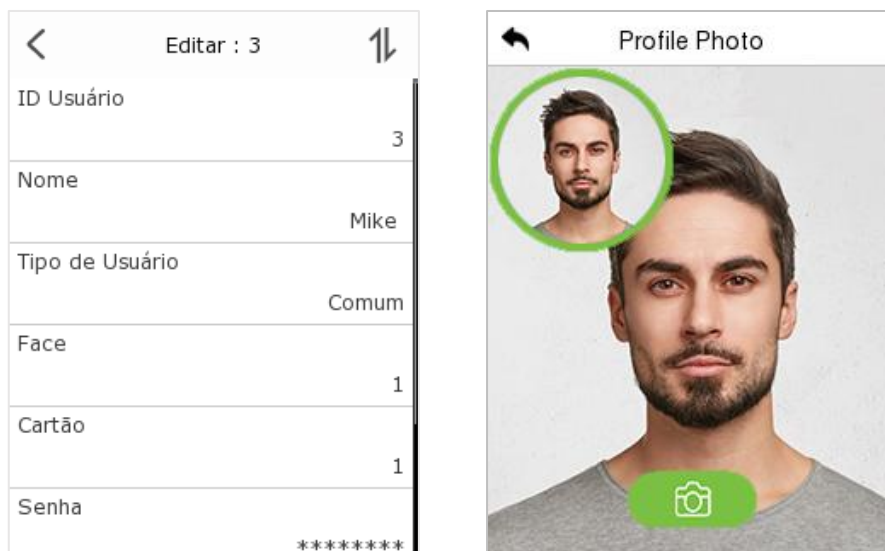
- Na interface Senha, digite a senha necessária e digite novamente para confirmá-la e toque em **OK**.
- Se a senha digitada novamente for diferente da senha digitada inicialmente, o dispositivo exibirá a mensagem como "**A senha não corresponde!**", onde o usuário precisa reconfirmar a senha novamente.



Nota: A senha pode conter de 6 a 8 dígitos por padrão.

6.1.6 Foto do usuário

Selecione face na interface de usuário para ir à página de registro de foto de perfil.



- Quando um usuário registrado com uma foto passa na autenticação, a foto registrada será exibida.
- Toque em **Foto** do perfil, a câmera do dispositivo será aberta e toque no ícone da câmera para tirar uma foto. A foto capturada é exibida no canto superior esquerdo da tela e a câmera abre novamente para tirar uma nova foto, depois de tirar a foto inicial.

6.1.7 Função de controle de acesso

A **Função de Controle de Acesso** define o privilégio de acesso à porta para cada usuário. Isso inclui o grupo de acesso e facilita a definição do período de tempo de acesso ao grupo.

- Toque em **Priv. controle de acesso** > **Grupo de acesso** para atribuir os usuários registrados a diferentes grupos para melhor gerenciamento. Novos usuários pertencem ao Grupo 1 por padrão e podem ser reatribuídos a outros grupos. O dispositivo suporta até 99 grupos de controle de acesso.
- Toque em **Horário** para selecionar o período de tempo a ser usado.

Controle acesso	
No. Grupo	Desabilitado
Horário	

6.2 Todos os Usuários

No **Menu Principal**, toque em **Usuário** e, em seguida, toque em **Todos os Usuários** para pesquisar um Usuário.

- Na interface **Todos os usuários**, toque na barra de pesquisa na lista de usuários para inserir a palavra-chave de recuperação necessária (onde a palavra-chave pode ser o ID do usuário, sobrenome ou nome completo) e o sistema pesquisará as informações do usuário relacionadas.

Usuários

Novo Usr

Todos usr

Estilo do display

Todos usr

3 Mike

6.3 Editar usuário

Na interface **Todos os usuários**, toque no usuário necessário na lista e toque em **Editar** para editar as informações do usuário.

 User : 1	 Editar : 3 
Edit	ID Usuário 3
Delete	Nome Mike
	Tipo de Usuário Comum
	Face 1
	Cartão 1
	Senha *****

Observação: O processo de edição das informações do usuário é o mesmo que adicionar um novo usuário, exceto que o ID do usuário não pode ser modificado durante a edição de um usuário.

6.4 Excluir usuário

Na interface **Todos Usuários**, toque no usuário necessário na lista e toque **Apagar** para excluir o usuário ou informações específicas do usuário do dispositivo. Na interface **Apagar**, toque na operação desejada, e então pressione **OK** para confirmar a exclusão.

Operações de exclusão:

- **Excluir usuário:** Todas as informações do usuário serão excluídas (exclui o usuário selecionado como um todo) do dispositivo.
- **Excluir somente face:** Exclui as informações do modelo de face do usuário selecionado.
- **Excluir somente senha:** Exclui as informações de senha do usuário selecionado.
- **Excluir apenas o número do cartão:** Exclui as informações do cartão do usuário selecionado.
- **Excluir somente foto do perfil:** Exclui a foto do perfil do usuário selecionado.

6.5 Estilo de exibição

Toque em **Gerenciamento de usuário > Estilo de exibição** para escolher o estilo da lista da interface **Todos os usuários**.



Estilo do display



Múltiplas linhas



Linhas mistas

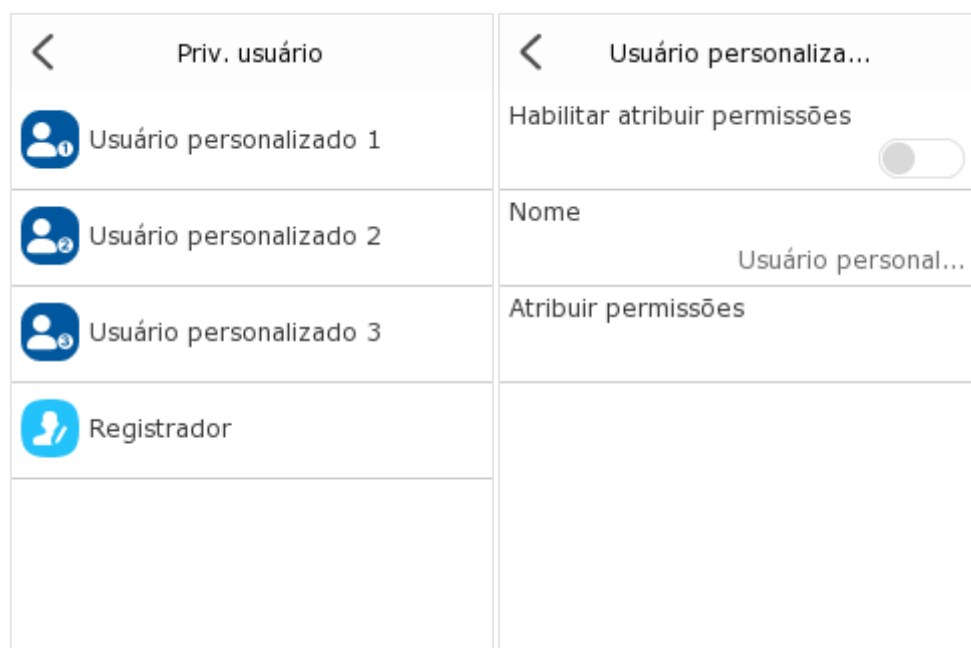
7 Privilégios do Usuário

Permite atribuir permissões específicas a determinados usuários com base em suas necessidades.

- No menu **Principal**, toque em **Priv. usuário** e, em seguida, toque em **Usuário personalizado 1** para definir as permissões definidas pelo usuário.
- O escopo de permissão da função personalizada pode ser configurado para até 3 funções, ou seja, o escopo operacional personalizado das funções de menu do usuário.



- Na interface **Usuário Personalizado**, alterne **Habilitar atribuir permissões** para habilitar ou desabilitar a função pelo usuário.
- Toque em **Nome** e insira o nome personalizado da função.



- Em seguida, selecione os privilégios necessários para atribuir à nova função e, em seguida, toque no **botão Retornar**.

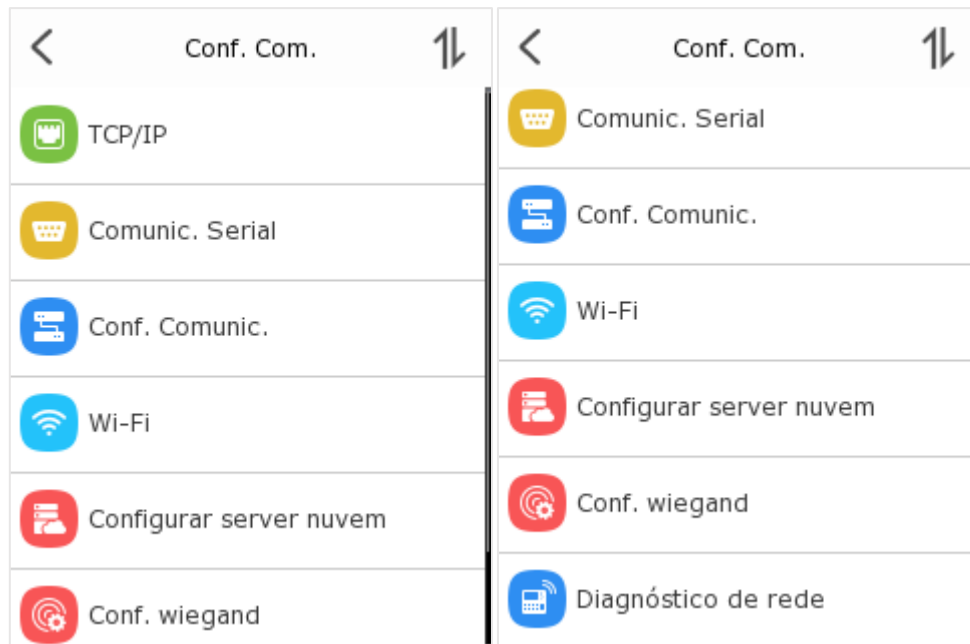
- Durante a atribuição de privilégios, os nomes das funções do menu principal serão exibidos à esquerda e seus submenus serão listados à direita.
- Primeiro toque no nome da função do **Menu Principal** desejado e, em seguida, selecione os submenus necessários na lista.

< Usuário personal... ⇅	< Usuário personal... ⇅
☒ Usuários	☒ Interfone
☒ Conf. Com.	☒ Acesso
☒ Sistema	☐ Pen Drive
☐ Personalização	☐ Registros
☐ Ger. dados	☐ Auto teste
☒ Interfone	☐ Info. sistema

Observação: Se o Privilégio do Usuário estiver habilitado para o Dispositivo, inserir [UsuarioAdm] > [Novo Usr] > [Tipo de Usuário] para atribuir os papéis criados aos usuários necessários. Mas se não houver um Super administrador registrado no dispositivo, ele exibirá a mensagem **cadastre super administrador primeiro** ao habilitar a função de Usuário personalizado.

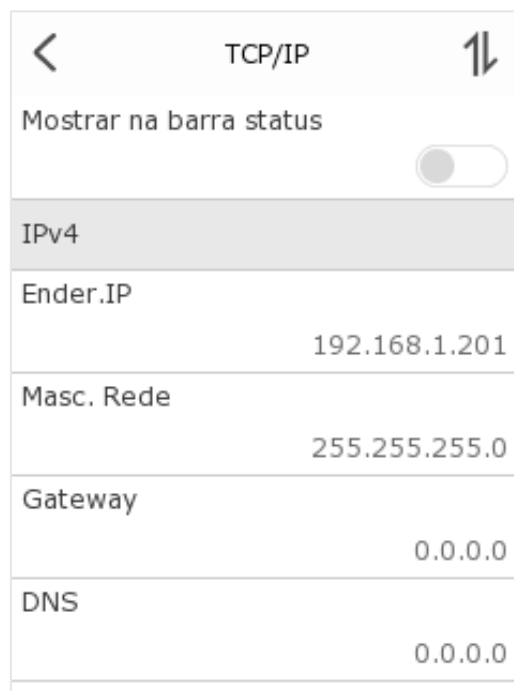
8 Comunicação

As configurações de comunicação são usadas para definir os parâmetros da Rede, Conexão de PC e Wi-Fi, servidor em nuvem e diagnóstico de rede.



8.1 TCP/IP

Quando o dispositivo precisa se comunicar com um PC via Ethernet, você precisa configurar as configurações de rede e garantir que o dispositivo e o PC estejam conectados ao mesmo segmento de rede. Selecione a interface [Conf. Com.] > [TCP/IP] para definir as configurações.



Descrição da função

Nome da Função	Descrição
Mostrar na barra status	Alternar para definir se o ícone da rede deve ser exibido na barra de status.
Ender.IP	O endereço IP padrão é 192.168.1.201. Ele pode ser modificado de acordo com a disponibilidade da rede.
Masc. Rede	A máscara de sub-rede padrão é 255.255.255.0. Pode ser modificada de acordo com a disponibilidade da rede.
Gateway	O endereço do Gateway Padrão é 0.0.0.0. Ele pode ser modificado de acordo com a disponibilidade da rede.
DNS	O endereço DNS padrão é 0.0.0.0. Ele pode ser modificado de acordo com a disponibilidade da rede.
DHCP	Protocolo de Configuração Dinâmica de Host aloca dinamicamente endereços IP para clientes via servidor.

8.2 Comunicação Serial

A função Comunicação Serial facilita o estabelecimento de comunicação com o dispositivo através de uma porta serial (RS485 / Master Unit). Toque em Comunicação serial. Na interface de configurações de comunicação.

<

Comunic. Serial

Porta serial

Não utilizado

Tx. de comunicação

115200

<

Porta serial

☒ Não utilizado

☐ RS485(PC)

☐ Dispositivo mestre

☐ Unidade Escrava OSDP

Descrição da função

Nome da função	Descrições
Porta serial	sem uso: Não se comunique com o dispositivo através da porta serial. RS485 (PC): Comunica-se com o dispositivo através da porta serial RS485. Unidade mestre: Quando o RS485 é usado como função de "unidade mestre", o dispositivo atuará como uma unidade mestre e poderá ser conectado ao leitor de cartão RS485.

Taxa de transmissão	A taxa na qual os dados são comunicados com o PC, existem 4 opções de taxa de transmissão: 115200 (padrão), 57600, 38400 e 19200. Quanto maior for a taxa de transmissão, mais rápida será a velocidade de comunicação, mas também menos confiável. Portanto, uma taxa de transmissão mais alta pode ser usada quando a distância de comunicação é curta; Quando a distância de comunicação é longa, escolher uma taxa de transmissão mais baixa seria mais confiável.
----------------------------	---

8.3 Configuração de Comunicação

Selecione [Conf. Comunic.] na interface para definir as configurações de comunicação.

Descrição da função

Nome da função	Descrições
Chave de comunicação	A senha padrão é 0 e pode ser alterada. A chave de comunicação deve ter 6 dígitos.
ID do dispositivo	É o número de identificação do dispositivo que varia entre 1 e 254.
Porta de comu. TCP	O valor padrão de fábrica é 4370. Ajuste o valor conforme necessário.
HTTPS	Para aumentar a segurança de software, os usuários podem habilitar o protocolo HTTPS para criar uma transmissão de rede segura e criptografada e garantir a segurança dos dados enviados por meio de autenticação de identidade e comunicação criptografada. Esta função está ativada por padrão. Essa função pode ser ativada ou desativada através da interface do menu, e ao alterar o status HTTPS, o dispositivo exibirá um prompt de segurança e reiniciará após a confirmação.

8.4 Configurações de Wi-Fi

O dispositivo fornece um módulo Wi-Fi integrado ao módulo do dispositivo.

O módulo Wi-Fi permite a transmissão de dados via Wi-Fi (Wireless Fidelity) e estabelece um ambiente de rede sem fio. O Wi-Fi está ativado por padrão no dispositivo. Se você não precisar usar a rede Wi-Fi, pode alternar o Wi-Fi para desativar o botão.

Selecione **[Wi-Fi]** na interface de configurações para definir as configurações de Wi-Fi.



- **Pesquise a rede Wi-Fi**

- O WIFI está ativado no dispositivo por padrão. Ative  o botão para ativar ou desativar o WIFI.
- Assim que o Wi-Fi for ligado, o dispositivo procurará o Wi-Fi disponível dentro do alcance da rede.
- Escolha o nome de Wi-Fi apropriado na lista disponível, insira a senha correta na interface de senha e toque em **Conectar ao Wi-Fi (OK)**.
- Quando o Wi-Fi for conectado com sucesso, a interface inicial exibirá o logotipo do Wi-Fi .



- Adicionar rede WIFI manualmente.
- O Wi-Fi também pode ser adicionado manualmente se o Wi-Fi necessário não aparecer na lista.

Observação: Depois de adicionar o WIFI manualmente, siga o mesmo processo para pesquisar o nome do WIFI adicionado. Clique aqui para ver o processo de pesquisa na rede WIFI.

- **Configuração avançada**

Na interface de rede sem fio, toque em **Avançado** para definir os parâmetros relevantes conforme necessário.

Nome da função	Descrição
DHCP	O Protocolo de Configuração Dinâmica de Host (DHCP) aloca dinamicamente endereços IP para clientes de rede. Se o DHCP estiver habilitado, o IP não poderá ser definido manualmente.
Endereço IP	O endereço IP da rede Wi-Fi, o padrão é 0.0.0.0. Pode ser modificado de acordo com a disponibilidade da rede.
Máscara de sub-rede	A máscara de sub-rede padrão da rede Wi-Fi é 255.255.255.0. Ela pode ser modificada de acordo com a disponibilidade da rede.
Gateway	O endereço do Gateway Padrão é 0.0.0.0. Ele pode ser modificado de acordo com a disponibilidade da rede.
DNS	O padrão é 0.0.0.0. Pode ser modificado de acordo com a disponibilidade da rede.

8.5 Configurações do Servidor em Nuvem

Toque em Configuração do servidor em nuvem na interface de configurações de comunicação para se conectar ao servidor ADMS.


Configurar server n...

Tipo de servidor

ADMS

Habilitar domínio

☐

End. Servidor

192.168.31.32

Porta servidor

8088

Proxy

☐

Descrição da Função

Nome da Função		Descrição
Habilitar domínio	End. Servidor	Uma vez que este modo estiver ativado, o modo de nome de domínio será usado, como http://www.XYZ.com, sendo que "XYZ" denota o nome de domínio.
Desativar domínio	End. Servidor	O endereço IP do servidor ADMS.
	Porta servidor	Porta usada pelo servidor ADMS.
Proxy		O endereço IP e a porta do servidor proxy são definidos manualmente quando o proxy está ativado.

8.6 Configuração Wiegand

Para definir os parâmetros de entrada ou saída do Wiegand.

Toque em Conf. Wiegand para definir os parâmetros de entrada ou saída Wiegand.

Nota: A interface Wiegand é compartilhada e o usuário pode optar por usar a função de entrada Wiegand ou saída Wiegand para interagir com diferentes dispositivos Wiegand.

8.6.1 Entrada Wiegand

Toque em Tipo de ID na Configuração do Wiegand, selecione Entrada do Wiegand e, em seguida, toque em Opções do Wiegand na Configuração do Wiegand.

Descrição da função

Nome da função	Descrições
Formato Wiegand	Os valores variam de 26 bits, 32 bits, 34 bits, 36 bits, 37 bits, 50 bits e 64 bits.
Wiegand Bits	Número de bits de dados Wiegand.
Largura de pulso (us)	O valor da largura de pulso enviada pelo Wiegand é de 100 microssegundos por padrão, que pode ser ajustado dentro do intervalo de 20 a 400 microssegundos.
Intervalo de pulso (us)	O valor padrão é 1000 microssegundos, que pode ser ajustado dentro do intervalo de 200 a 20000 microssegundos.
Tipo de ID	Selecione entre ID de usuário e número do cartão.

Várias descrições comuns do formato Wiegand

Formato Wiegand	Descrição
Wiegand26	EEEEEEEEEEEEEEEEEEEEEEEEEEEE Consiste em 26 bits de código binário. O 1º bit é o bit de paridade par do 2º ao 13º bits, enquanto o 26º bit é o bit de paridade ímpar do 14º ao 25º bits. O 2º ao 25º bits são os números das cartas.
Wiegand26a	ESSSSSSSSSSSSSSSSSSSSSSSSSS Consiste em 26 bits de código binário. O 1º bit é o bit de paridade par do 2º ao 13º bits, enquanto o 26º bit é o bit de paridade ímpar do 14º ao 25º bits. O 2º ao 9º bits são os códigos do site, enquanto o 10º ao 25º bits são os números do cartão.
Wiegand34	EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE Consiste em 34 bits de código binário. O 1º bit é o bit de paridade par do 2º ao 17º bits, enquanto o 34º bit é o bit de paridade ímpar do 18º ao 33º bits. O 2º ao 25º bits são os números das cartas.
Wiegand34a	ESSSSSSSSSSSSSSSSSSSSSSSSSSSS Consiste em 34 bits de código binário. O 1º bit é o bit de paridade par do 2º ao 17º bits, enquanto o 34º bit é o bit de paridade ímpar do 18º ao 33º bits. O 2º ao 9º bits são os códigos do site, enquanto o 10º ao 25º bits são os números do cartão.
Wiegand36	OFFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCMME Consiste em 36 bits de código binário. O 1º bit é o bit de paridade ímpar do 2º ao 18º bit, enquanto o 36º bit é o bit de paridade par do 19º ao 35º bits. O 2º ao 17º bits são os códigos do dispositivo. O 18º ao 33º bits são os números do cartão e o 34º ao 35º bits são os códigos do fabricante.
Wiegand36a	EEEEEEEEEEEEEEEEEEEEFFCCCCCCCCCCCCCCCC Consiste em 36 bits de código binário. O 1º bit é o bit de paridade par do 2º ao 18º bits, enquanto o 36º bit é o bit de paridade ímpar do 19º ao 35º bits. O 2º ao 19º bits são os códigos do dispositivo e o 20º ao 35º bits são os números do cartão.
Wiegand37	OMMMMMSSSSSSSSSSSSSSSSSSSSSSSSSSSS Consiste em 37 bits de código binário. O 1º bit é o bit de paridade ímpar do 2º ao 18º bit, enquanto o 37º bit é o bit de paridade par do 19º ao 36º bits. O 2º ao 4º bits são os códigos do fabricante. O 5º ao 16º bits são os códigos do site e o 21º ao 36º bits são os números do cartão.

Wiegand37a	EMMMFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCCO Consiste em 37 bits de código binário. O 1º bit é o bit de paridade par do 2º ao 18º bits, enquanto o 37º bit é o bit de paridade ímpar do 19º ao 36º bits. O 2º ao 4º bits são os códigos do fabricante. O 5º ao 14º bits são os códigos do dispositivo, e o 15º ao 20º bits são os códigos do site e o 21º ao 36º bits são os números do cartão.
Wiegand50	ESSSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consiste em 50 bits de código binário. O 1º bit é o bit de paridade par do 2º ao 25º bits, enquanto o 50º bit é o bit de paridade ímpar do 26º ao 49º bits. O 2º ao 17º bits são os códigos do site e o 18º ao 49º bits são os números dos cartões.
"C" denota o número do cartão; "E" denota o bit de paridade par; "O" denota o bit de paridade ímpar; "F" indica o código da instalação; "M" indica o código do fabricante; "P" denota o bit de paridade; e "S" denota o código do site.	

8.6.2 Saída Wiegand

Toque em Tipo de ID na Configuração do Wiegand, selecione Saída do Wiegand e, em seguida, toque em Opções do Wiegand na Configuração do Wiegand.

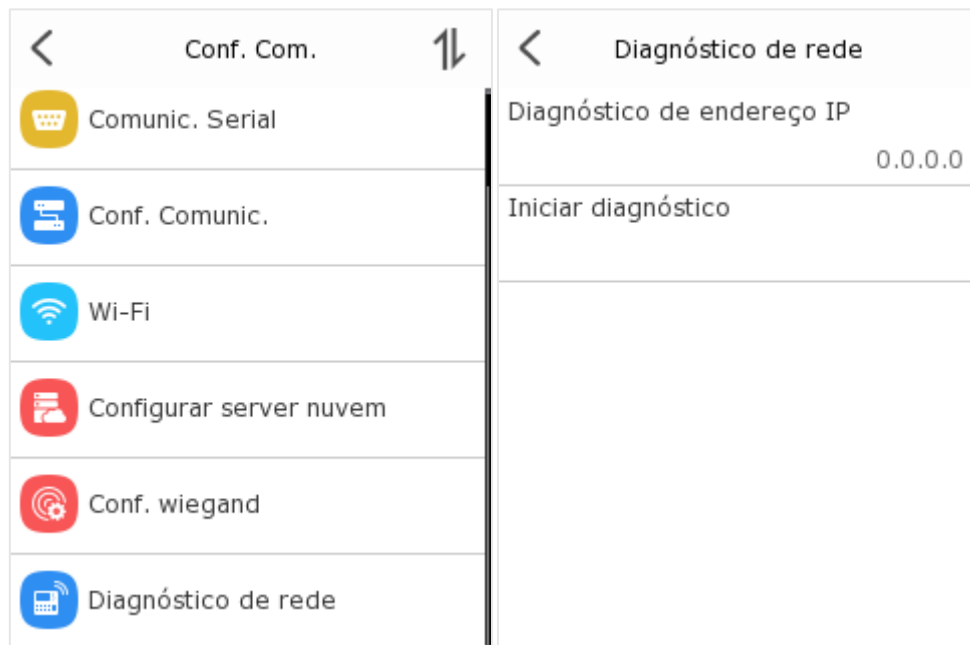
Descrição da função

Nome da função	Descrições
Formato Wiegand	Os valores variam de 26 bits, 32 bits, 34 bits, 36 bits, 37 bits e 50 bits.
Bits de saída Wiegand	Depois de selecionar o formato Wiegand necessário, selecione os dígitos de bits de saída correspondentes do formato Wiegand.
Falha ID	Se a verificação falhar, o sistema enviará o ID com falha para o dispositivo e substituirá o número do cartão ou ID pessoal pelo novo.
Site Code	É semelhante ao ID do dispositivo. A diferença é que um código de site pode ser definido manualmente e pode ser repetido em um dispositivo diferente. O valor válido varia de 0 a 256 por padrão.
Largura de pulso (us)	A largura de tempo representa as mudanças da quantidade de carga elétrica com capacitância regular de alta frequência dentro de um tempo especificado.
Intervalo de pulso (us)	O intervalo de tempo entre os pulsos.
Tipo de ID	Selecione os tipos de ID como ID de usuário ou número do cartão.

8.7 Diagnóstico de rede

Ajuda a definir os parâmetros de diagnóstico de rede.

Selecione Diagnóstico de Rede na interface Conf Com de Configurações. Insira o endereço IP que precisa ser diagnosticado e toque Iniciar diagnóstico para verificar se a rede consegue se conectar ao dispositivo.



9 Configurações do sistema

Defina os parâmetros do sistema relacionados para otimizar o desempenho do dispositivo. Toque em **Sistema** na interface do **Menu Principal** para definir os parâmetros do sistema.



9.1 Data e hora

Selecione Data e Hora na interface de Sistema para definir a data e hora.



- Toque **Servidor NTP** para habilitar a sincronização automática de horário com base no endereço de serviço que você inserir.
- Toque **Data e Hora manual** para definir manualmente a data e hora e, em seguida, toque em **Confirmar** e salvar.
- Toque em **Fuso Horário** para selecionar manualmente o fuso horário onde o dispositivo está localizado.

- Ative ou desative este formato tocando em "Formato 24 horas". Se ativado, então toque em **Formato data** para defini-la de acordo com sua necessidade.

9.2 Configurações de Regras de Acesso

Clique em **Conf. reg. de acesso** na interface do sistema.

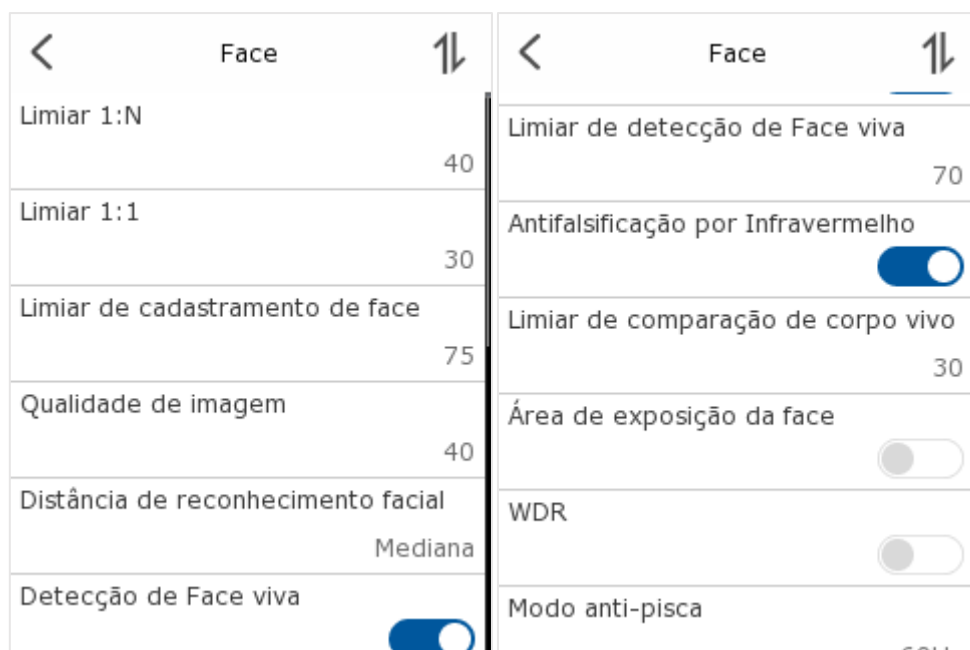
Descrição da função

Nome da Função	Descrição
Modo Câmera	Esta função está desabilitada por padrão. Quando habilitada, um prompt de segurança será exibido. Existem 5 modos: Sem Foto: Nenhuma foto é tirada durante a verificação do usuário. Capturar, não salvar: Foto tirada, mas não salva durante a verificação. Capturar e salvar: Todas as fotos tiradas durante a verificação são salvas. Salva após verificação OK: Foto tirada e salva para cada verificação bem-sucedida. Salva após verificação inválida: Foto tirada e salva apenas para cada verificação que falhou.
Mostrar foto usuário	Exibir a foto do usuário quando o Usuário passa na verificação.
ID usuário alfanumérico	Ativar/Desativar o alfanumérico como ID de usuário.

Config. reg. excessão	Quando o espaço de registro do acesso de ponto atingir o valor máximo de limite, o dispositivo exibirá automaticamente o aviso de espaço de memória. Os usuários podem desabilitar a função ou definir um valor válido entre 1 e 9999.
Ciclo apg. reg. acesso	Quando os logs de acesso atingem sua capacidade máxima, o dispositivo exclui automaticamente um conjunto de logs de acesso antigos. Os usuários podem desabilitar a função ou definir um valor válido entre 1 e 999.
Ciclo de exclusão de fotos	Quando as fotos de presença atingirem sua capacidade máxima, o dispositivo automaticamente excluirá um conjunto de fotos antigas de presença. Os usuários podem desabilitar a função ou definir um valor válido entre 1 e 99.
Ciclo P/ apg. Fotos .L. bloqueados	Quando o número máximo de fotos na lista de bloqueadas for atingido, o dispositivo automaticamente excluirá um conjunto de fotos antigas bloqueadas. Os usuários podem desabilitar a função ou definir um valor válido entre 1 e 99.
Atraso de tela (s)	O tempo gasto para exibir uma mensagem de verificação bem-sucedida. Valor válido: 1 a 9 segundos.
Intervalo (s) de Reconhecimento	Após o intervalo identificação é clicado (selecionado), por exemplo, se o intervalo de comparação for definido para 5 segundos, o reconhecimento facial verificará o rosto a cada 5 segundos. Valor válido: 0 a 9 segundos. 0 significa identificação contínua, 1 a 9 significa identificação em intervalos.

9.3 Parâmetros de face

Toque em Face na interface do sistema para ir para as configurações de parâmetros de face.



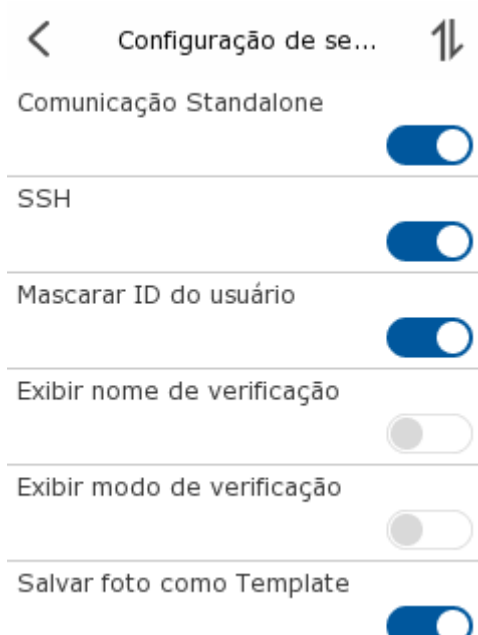
Descrição da função

Nome da Função	Descrição
Limiar 1:N	No modo de verificação 1:N, a verificação só será bem-sucedida quando a similaridade entre a imagem facial adquirida e todos os modelos faciais registrados for maior que o valor definido. Os valores válidos variam de 0 a 100. Quanto maiores os limiares, menores as taxas de falso verdadeiro e maiores as taxas de rejeição e vice-versa. Recomenda-se definir o valor padrão de 47.
Limiar 1:1	No modo de verificação 1:1, a verificação só será bem-sucedida quando a similaridade entre a imagem facial adquirida e os modelos faciais do usuário registrados no dispositivo for maior que o valor definido. Os valores válidos variam de 0 a 100. Quanto maiores os limiares, menores as taxas de falso verdadeiro e maiores as taxas de rejeição e vice-versa. Recomenda-se definir o valor padrão de 63.
Limiar de cadastramento de face	Durante o cadastramento facial, 1:N a comparação é usada para determinar se o usuário já se registrou antes. Quando a similaridade entre a imagem facial adquirida e todos os modelos faciais registrados for maior que o limite definido, ela indica que o rosto já foi registrado.
Qualidade de imagem	É a qualidade da imagem para registro e comparação facial. Quanto maior o valor, mais nítida a imagem precisa ser.
Distância de reconhecimento facial	Quanto mais distante o indivíduo estiver, menor o rosto, menor o número de pixels do rosto obtido pelo algoritmo. Portanto, ajustar

	este parâmetro pode ajustar a distância de comparação mais distante dos rostos.
Detecção de Face viva	Este valor controla o ligar e desligar da luz LED. Quanto maior o valor, mais frequentemente a luz LED ligará e desligará.
Limiar de detecção de Face viva	Usando imagens de espectros de infravermelho próximo para identificar e prevenir ataques com fotos e vídeos falsos.
Antifalsificação por Infravermelho	É conveniente julgar se a imagem espectral de infravermelho próximo é foto e vídeo falsos. Quanto maior o valor, melhor o desempenho anti-spoofing da imagem espectral de infravermelho próximo.
Área de exposição da face	Quando o rosto está na frente da câmera no modo Face, o brilho da área do rosto aumenta, enquanto outras áreas ficam mais escuras.
WDR	Wide Dynamic Range (WDR) equilibra a luz e amplia a visibilidade da imagem em vídeos de vigilância em cenas com iluminação de alto contraste e melhora a identificação de objetos em ambientes claros e escuros.
Modo anti-pisca	É usado quando o WDR está desligado. Ajuda a reduzir o flicker quando a tela do dispositivo pisca na mesma frequência da luz.
Algoritmo Face	Possui informações relacionadas ao algoritmo facial e pausa a atualização do modelo facial.

9.4 Configuração de segurança

Toque em Configuração de segurança na interface do sistema.

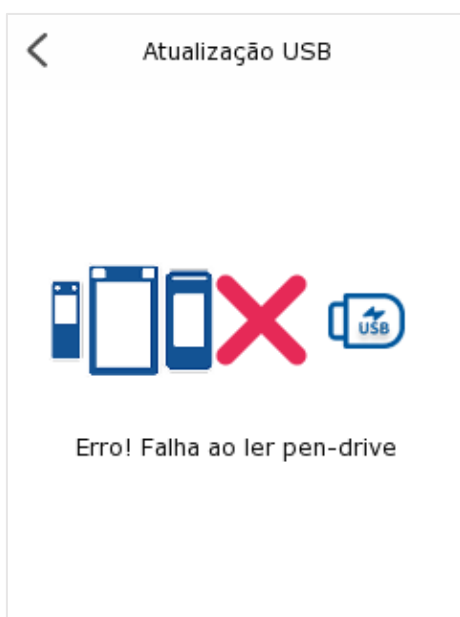


Descrição da função

Nome da Função	Descrição
Comunicação Standalone	Permite utilização do dispositivo sem necessidade de conexão com o servidor. Desativado por padrão!
SSH	SSH é usado para acessar o background do dispositivo para manutenção. Desativado por padrão!
Mascarar ID do usuário	Quando habilitado, e o usuário for comparado e verificado com sucesso, o ID do Usuário no resultado de verificação exibido será substituído por um * para garantir a proteção segura de dados privados sensíveis.
Exibir nome de verificação	Definir se o nome de usuário será exibido na interface de resultado de verificação.
Exibir modo de verificação	Definir se o modo de verificação deve ser exibido na interface de resultado de verificação.
Salvar foto como Template	Após desabilitar esta função, é necessário o recadastramento facial após uma atualização de algoritmo.
Comunicação do servidor web	Quando habilitado, libera a porta 1443 para parametrização do equipamento via interface web

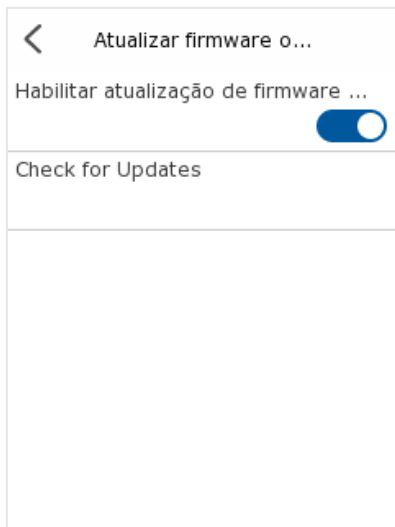
9.5 Atualização USB

Toque em **Atualização USB** na interface do sistema. O firmware do dispositivo pode ser atualizado com o arquivo de atualização em uma unidade USB. Antes de realizar esta operação, certifique-se de que a unidade USB contém o arquivo de atualização correto e está inserido corretamente no dispositivo. Se nenhum disco USB estiver inserido, o sistema fornecerá o seguinte aviso depois que você tocar **em Atualização USB** na interface do sistema.



9.6 Atualizar firmware online

Clique em **Atualizar firmware online** na interface do sistema. Clique em **Ativar função online de atualização de firmware**, o dispositivo avisará que a atualização pode trazer alguns riscos de segurança de dados, o que requer confirmação manual pelo usuário (se a função de configuração de segurança estiver desativada, o aviso de risco não será exibido quando a atualização online for ativada).

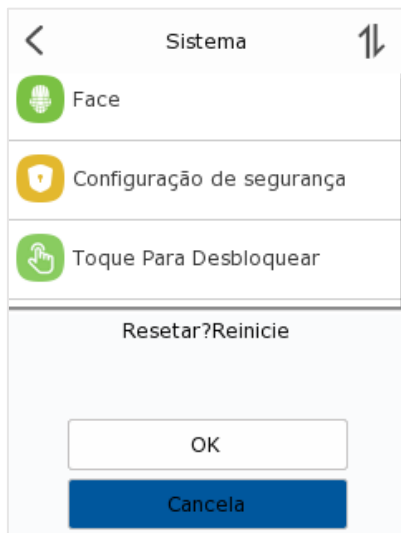


Clique em **Verificar atualizações**, ele pode ter os 3 cenários a seguir:

- Se a consulta falhar, a interface solicitará "Falha na consulta".
- Se a versão do firmware do dispositivo for a mais recente, ele mostrará que a versão atual do firmware é a mais recente.
- Se a versão do firmware do dispositivo não for a mais recente, o número da versão e o log de alterações da versão mais recente serão exibidos. Os usuários podem escolher se desejam atualizar para a versão mais recente do firmware.

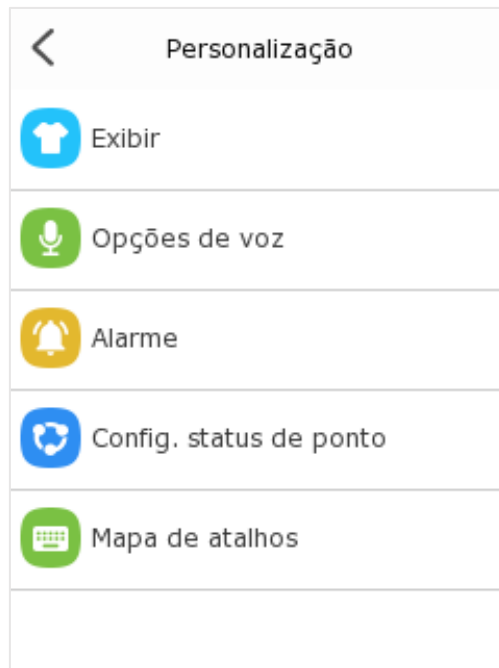
9.7 Reset de fábrica

A função Factory Reset restaura as configurações do dispositivo, como configurações de comunicação e configurações do sistema, para as configurações padrão de fábrica (esta função não limpa os dados do usuário registrado). Toque em **Resetar** na interface do sistema e, em seguida, toque em **OK** para restaurar as configurações padrão de fábrica.



10 Personalização

Toque em **Personalização** na interface do **Menu Principal** para personalizar as configurações da interface, voz, alarme, configuração status de ponto e mapa de atalhos.



10.1 Configurações da interface do usuário

Toque em **Exibir** na interface de **Personalizar** para personalizar o estilo de exibição da interface principal.

 Exibir 	 Exibir 
Papel de parede	Idioma Português Brasil
Idioma Português Brasil	Tempo. Limite tela de Menu(s) 60
Tempo. Limite tela de Menu(s) 60	Tp ocioso espera(s) 60
Tp ocioso espera(s) 60	Intervalo apresentação(s) 30
Intervalo apresentação(s) 30	Tempo inatividade(m) 30
Tempo inatividade(m) 30	Estilo tela principal Estilo 1

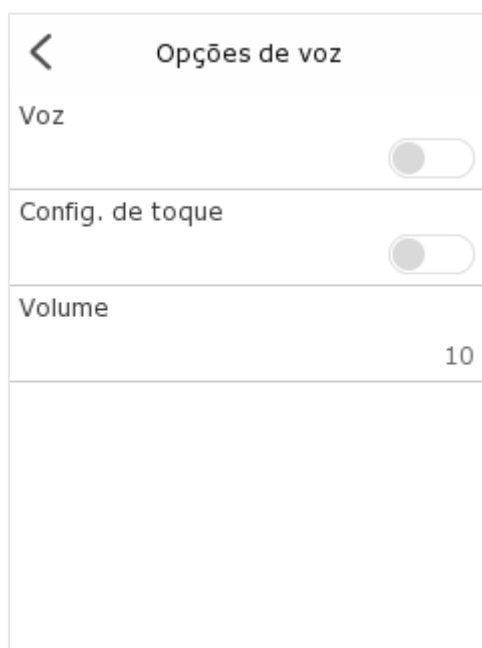
Descrição da função

Nome da Função	Descrição
Papel de parede	Ajuda a selecionar o papel de parede da tela principal de acordo com a preferência do usuário.

Idioma	Ajuda selecionar o idioma do dispositivo.
Tempo. Limite tela de Menu(s)	Quando não houver operação e o tempo exceder o valor definido, o dispositivo retornará automaticamente à interface inicial. A função pode ser desabilitada ou configurada com o valor necessário entre 60 e 99999 segundos.
Tempo ocioso espera(s)	Quando não houver operação e o tempo exceder o valor definido, um slideshow será exibido. A função pode ser desabilitada, ou você pode definir o valor entre 3 e 999 segundos.
Intervalo apresentação(s)	É o intervalo de tempo na troca entre diferentes imagens do slide show. A função pode ser desabilitada, ou você pode definir o intervalo entre 3 e 999 segundos.
Tempo inatividade(m)	Se o modo de suspensão estiver ativado e não houver operação no dispositivo, ele entrará no modo de espera. Esta função pode ser desabilitada ou configurada com um valor entre 1 e 999 minutos.
Estilo tela principal	O estilo da tela principal pode ser selecionado de acordo com a preferência do usuário.

10.2 Configurações de voz

Toque em **Opções de Voz** na interface **Personalizar** para definir as configurações de voz.

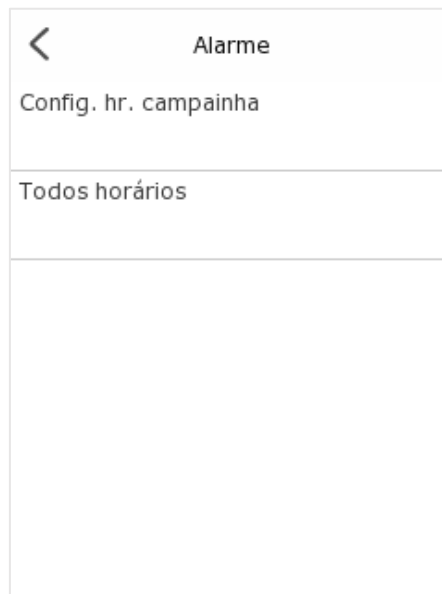


Descrição da função

Nome da Função	Descrição
Voz	Ativar ou desativar as mensagens de voz durante as operações da função.
Config. de toque	Ativar ou desativar os sons do teclado.
Volume	Ajuste o volume do dispositivo, que pode ser configurado entre 0 e 100.

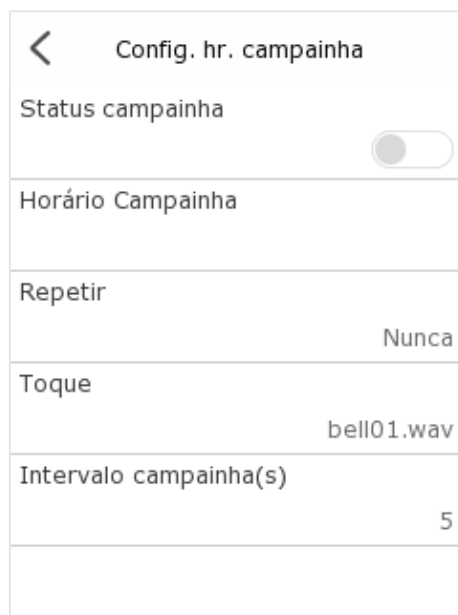
10.3 Alarme

Toque em **Alarme** na interface **Personalizar** para definir as configurações de campainha.



- **Config. Hr. campainha**

Toque em **Config. Hr. campainha** na interface **Programação de alarme** para adicionar uma nova programação de campainha.



Descrição da função

Nome da Função	Descrição
Status campainha	Ativar ou desativar o status do alarme.
Horário Campainha	Uma vez definido o tempo necessário, o dispositivo dispara automaticamente para tocar o alarme durante esse tempo.
Repetir	Defina o número necessário de contagens para repetir o toque programado.
Toque	Selecione um toque.
Intervalo campainha(s)	Defina o tempo de repetição do alarme interno. Os valores válidos variam de 1 a 999 segundos.

- **Todos os horários dos sinos:**

Depois que a campanha estiver agendada, na interface **Alarme**, toque em **Todos horários** para exibir a campanha recém-agendada.

- **Edite o alarme programado:**

Na interface **Todos horários**, toque na programação de campanha necessária e toque em **Editar** para editar a programação de campanha selecionada. O método de edição é o mesmo que as operações de adicionar uma nova tabela de campanha.

- **Excluir um alarme:**

Na interface **Todos horários**, toque na agenda de campanha necessária, toque em **Excluir** e, em seguida, toque em **Sim** para excluir a campanha selecionada.

10.4 Modo status de ponto

Toque em **Modo status de ponto** na interface **Personalizar** para definir as configurações de estado de funcionamento.

Config. status de p...

Modo status de ponto

Modo manual

Tp limite status ponto(s)

10

Exigir status de ponto

Descrição da função

Nome da função	Descrição
Modo status de ponto	Desativado: Desative a função de estado de ponto. Portanto, a chave de estado de ponto definida no menu Mapeamentos de teclas de atalho se tornará inválida. Modo manual: Alterne a chave de estado de ponto manualmente e a chave de estado de ponto desaparecerá após o tempo limite. Modo automático: A tecla de estado de ponto mudará automaticamente para um status de ponto específico de acordo com o cronograma predefinido que pode ser definido nos mapeamentos de teclas de atalho. Modo manual e automático: A interface principal exibirá a chave de estado de ponto de comutação automática. No entanto, os usuários ainda poderão selecionar uma alternativa que seja o status de presença manual. Após o tempo

	limite, a chave de estado de ponto de comutação manual se tornará a chave de estado de ponto de comutação automática. Modo fixo manual: Depois que a tecla de estado de ponto for definida manualmente para um status de ponto específico, a função permanecerá inalterada até ser comutada manualmente novamente. Modo fixo: Somente a chave de estado de ponto corrigida manualmente será mostrada. Os usuários não podem alterar o status pressionando outras teclas.
--	---

10.5 Mapeamentos de teclas de atalho

Os usuários podem definir teclas de atalho para o status de atendimento e para as teclas funcionais que serão definidas na interface principal. Assim, na interface principal, quando as teclas de atalho são pressionadas, o status de atendimento correspondente ou a interface de função será exibido diretamente. Toque em **Mapa de atalhos** na interface **Personalizar** para definir as teclas de atalho necessárias.

Mapa de atalhos	
F1	Entrada
F2	Saída
F3	Saí-intervalo
F4	Ent-intervalo
F5	Ent-extra
F6	Saí-extra

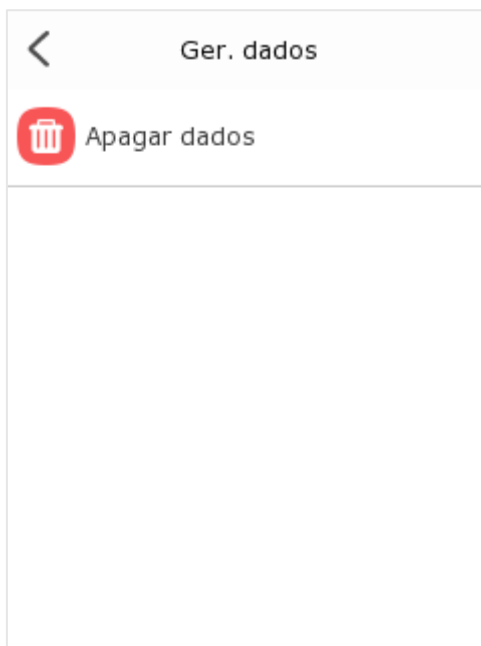
- Na interface **Mapa de atalhos**, toque na tecla de atalho necessária para definir as configurações das teclas de atalho.
- Na interface da **tecla de atalho** (ou seja, "F1"), toque em **função** para definir o processo funcional da tecla de atalho como tecla de estado de ponto ou tecla de função.

Observação: Quando a função é definida como Indefinida, o dispositivo não habilita a chave de estado de ponto.

- **Defina o tempo de troca**
 - O tempo de comutação é definido de acordo com as opções de estado de ponto.
 - Na **interface** Opções de estados de ponto, quando o **modo de estado de ponto** é definido como **modo automático**, o tempo de comutação deve ser definido.
 - Na interface da **tecla de atalho**, toque em **Definir hora da troca** para definir a hora da troca.
 - Na interface **Switch Cycle**, selecione o ciclo de comutação (segunda, terça-feira etc.).

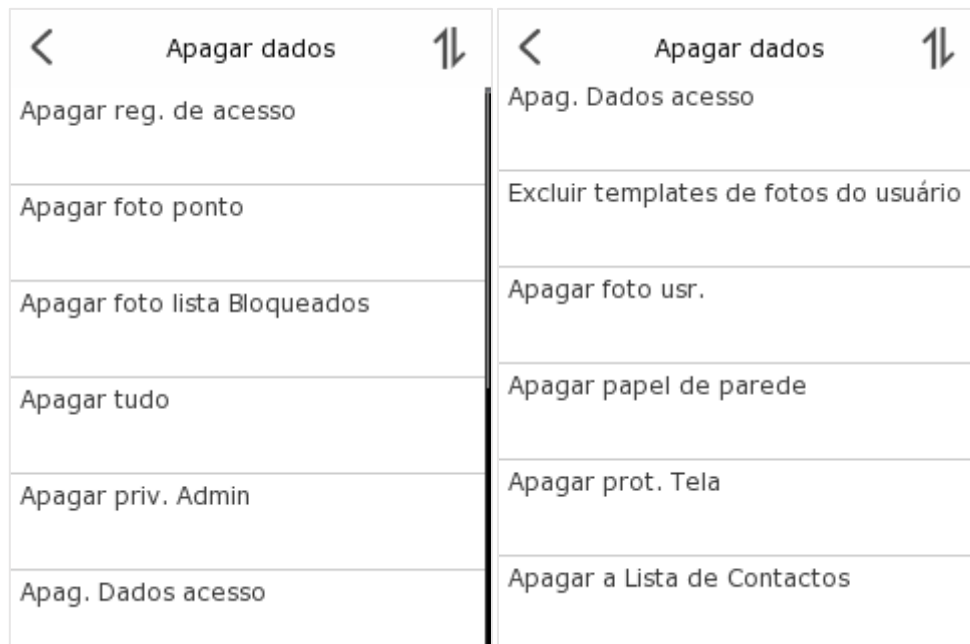
11 Gerenciamento de dados

No **Menu Principal**, toque em **Gerenciamento de Dados**. para excluir os dados relevantes no dispositivo.



11.1 Excluir dados

Toque em **Excluir dados** no **Gerenciador de dados** para excluir os dados necessários.



Descrição da função

Nome da Função	Descrição
Apagar reg. de aceso	Para excluir os registros de acesso e dados de frequência condicionalmente.
Apagar foto ponto	Para excluir fotos de ponto de pessoal designado.

Apagar foto lista Bloqueados	Para excluir as fotos tiradas durante verificações mal sucedidas.
Apagar tudo	Para excluir as informações e os registros de acesso e dados de frequência de todos os usuários registrados.
Apagar priv. Admin	Para remover todos os privilégios de administrador.
Apag. Dados acesso	Para excluir todos os dados de acesso.
Excluir templates de fotos do usuário	Para excluir modelos de fotos de usuário no dispositivo. Ao excluir fotos de modelos, há um lembrete de risco: "O recadastramento facial é necessário após uma atualização do algoritmo."
Apagar foto usr.	Para excluir todas as fotos de perfil do dispositivo.
Apagar papel de parede	Para excluir todos os papéis de parede do dispositivo.
Apagar prot. Tela	Para excluir todos os protetores de tela do dispositivo.
Apagar a Lista de Contatos	Para excluir todos os contatos da lista de vídeo porteiro do dispositivo.

- O usuário pode selecionar Excluir tudo ou Excluir por intervalo de tempo ao excluir os registros de acesso, fotos de presença ou bloquear fotos listadas. Selecionando Excluir por intervalo de tempo, você precisa definir um intervalo de tempo específico para excluir todos os dados dentro de um período específico.

12 Interfone

Clique em **Interfone** no menu principal.



12.1 Configurações SIP

Toque em **Configurações SIP** na interface de Interfone para acessar as configurações SIP.



12.1.1 Configurações locais

Toque em **Configurações locais** na interface Configurações SIP.

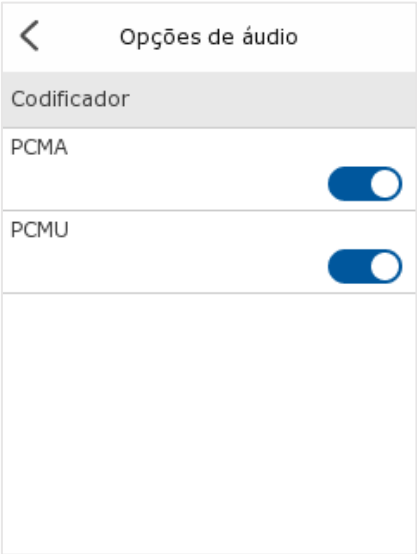


Descrição da função

Nome da Função	Descrição
Servidor SIP	Selecione se deseja habilitar o servidor SIP. Quando estiver ativado, a conta precisa ser configurada. Nota: Toda vez que este recurso for ativado ou desativado, a lista de contatos será redefinida.
Config. Conta Principal	Depois de atribuir a conta SIP para o dispositivo no WEG BioGuard, as informações da conta serão sincronizadas automaticamente com o dispositivo. Você não precisa configurá-lo manualmente.
Config. Conta de Backup	Habilitar o backup de configurações da conta.
Número do Quarto	Ao usar uma rede local para interfone, digite o número do quarto.
Informações Local	Tipo de Equipamento: Defina o tipo de dispositivo como Estação de entrada ou Terminal de Portão . Nota: A lista de contatos será limpa após a alteração do tipo de dispositivo.
Protocolo de transmissão	Defina o protocolo de transporte entre o dispositivo e o servidor.
Chamar Lista de Contatos	Habilitar a lista de contatos na página de chamada. Quando estiver ativado, você poderá pressionar a Tecla para cima para abrir a lista de contatos na página de chamada.
Tipo de Número de Chamada	Número do Quarto: O dispositivo pode chamar o número de ramal. (número curto) ou número do quarto. Número da Conta SIP: O dispositivo só pode ligar para a conta SIP.

12.1.2 Opções de áudio

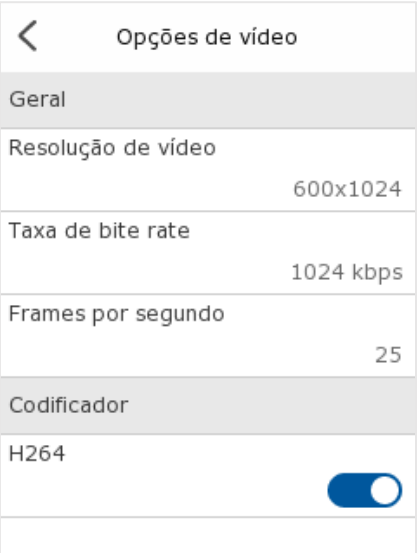
Toque em **Opções de áudio** na **interface** de configurações SIP.



Selecione o codificador de áudio para interfone. Tanto o PCMU quanto o PCMA oferecem melhor qualidade de voz, mas ocupam mais largura de banda, exigindo 64 kbps.

12.1.3 Opções de vídeo

Toque em **Opções de vídeo** na **interface** de configurações do SIP.



Descrição da função

Nome da Função	Descrição
Resolução de vídeo	Selecione a resolução de vídeo do interfone 1024 x 576 ou 600 x 1024.

Taxa de bite rate	Selecione o a taxa de fluxo de informação do interfone, quanto maior o valor, maior a qualidade de imagem e som do vídeo, e maiores as exigências de rede.
Frames por segundo	Refere-se ao número de quadros por segundo do visor de vídeo do interfone; quanto maior o valor, mais suave a imagem. O dispositivo utiliza 25 por padrão e não suporta modificação.
Codificador	Ativar o codificador H264.

12.1.4 Opções de compra

Toque em **Opções de chamada** na interface de configurações SIP.



Descrição da função

Nome da Função	Descrição
Atraso (s) de chamada	Defina o tempo da chamada, valor válido de 30 a 60 segundos.
Atraso (s) para falar	Defina o tempo do interfone, valor válido de 60 a 120 segundos. Sugere-se definir como 60s.
Config. Vol. Chamada	Defina o volume da chamada, com valor válido variando de 0 a 100.
Tipo de chamada	Defina o tipo de chamada para somente Voz ou Voz+Vídeo.
Config. Resposta Auto.	Selecionar para habilitar a função de resposta automática. Quando ativada, o dispositivo atenderá automaticamente se monitor interno chamar.
Atraso da Resposta Auto.	O dispositivo atenderá automaticamente após o tempo de atraso definido se monitor interno chamar, valor válido de 0 a 10 segundos.
Criptografia	Está desabilitado por padrão.

12.1.5 Lista de Contatos

Selecione Lista de Contatos na interface Configurações SIP.

No modo Servidor SIP, a lista de contatos é sincronizada pelo WEG BioGuard para o dispositivo. A lista de contatos só pode ser visualizada, não pode ser editada. Quando o servidor SIP estiver desabilitado, o número do quarto e o endereço de chamada dos monitores internos podem ser adicionados aqui.

Selecione Adicionar para entrar na interface Adicionar Lista de Contatos.

Contact List	Add
Add	Room Number
101 192.168.1.101	Call Address
102 192.168.1.102	
103 192.168.1.103	
104 192.168.1.104	

- **Número da sala:** Personalize o número do monitor interno.
- Quando o tipo de dispositivo estiver definido como **Portaria**, o número do quarto pode ter de 1 a 4 dígitos. Quando o tipo de dispositivo está definido como **Terminal de Cerca**, você precisa inserir o número do bloco, unidade e quarto. Por exemplo, se o monitor interno estiver no Bloco 3, Unidade 2, Quarto 2601, então insira "03.02.2601".

Room Number	Room Number
102	00 . 00 . 0000
1234567890 OK	1234567890 OK

Terminal de vedação da estação de entrada

- **Endereço de chamada:** É o endereço IP do monitor interno.

12.1.6 Configurações de atalho de chamada

Selecione Configurações de atalho de chamada na interface Configurações SIP.

< Configurações de a...	
Central de gerenciamento	Desabilitar
Modo de Chamada	Modo Padrão
ROOM1	Desabilitar
ROOM2	Desabilitar

Central de Gerenciamento: Selecione se deseja habilitar a Central de Gerenciamento e defina o seu número. Após a ativação, você pode pressionar a tecla  para chamar diretamente o administrador na página de chamada.

Modo de Chamada: Pode ser definido como **Modo Padrão** ou **Modo de Chamada Direta**.

- No modo padrão, aqui estão 4 atalhos que podem ser ativados e definidos no dispositivo: **ROOM1**, **ROOM2**, **ROOM3** e **ROOM4**. Você pode definir uma tecla de atalho para chamar o monitor interno rapidamente sem precisar digitar o número do monitor interno cada vez.

Nome: Personalize o nome das teclas de atalho.

Número: Selecione o número do quarto definido no menu **Lista de Contatos**.

↩ Number : 102	
Enable	☒
Name	ROOM1
Number	102

- No modo de Chamada Direta, o usuário pode chamar vários monitores internos diretamente. Entre em **Modo de Chamada > Modo de Chamada Direta > Adicionar**, selecione os monitores internos que você deseja chamar, então os monitores internos serão exibidos na lista.

12.1.7 Configurações avançadas

Toque em Configurações avançadas na interface de configurações SIP.

Configurações Avan...	
Configuração DTMF	
Tipo DTMF	AUTO
DTMF	1234

Descrição da função

Nome da Função	Descrição
Tipo DTMF	Defina o tipo DTMF como AUTO, SIP INFO ou RFC2833.
DTMF	O valor deve ser definido como igual ao valor de DTMF no monitor interno.

12.2 Configuração da campainha

Selecione Configuração da campainha na interface do terminal facial para configurar a campainha.

Doorbell Setting	
☐	Disabled
☒	Video Intercom Only

Descrição da função

Nome da Função	Descrição
Configuração da campainha	Desabilitado: O botão da campainha está desativado. Apenas Vídeo porteiro: Quando o usuário pressiona o botão da campainha, apenas o dispositivo faz uma chamada.

12.3 Configurações do ONVIF



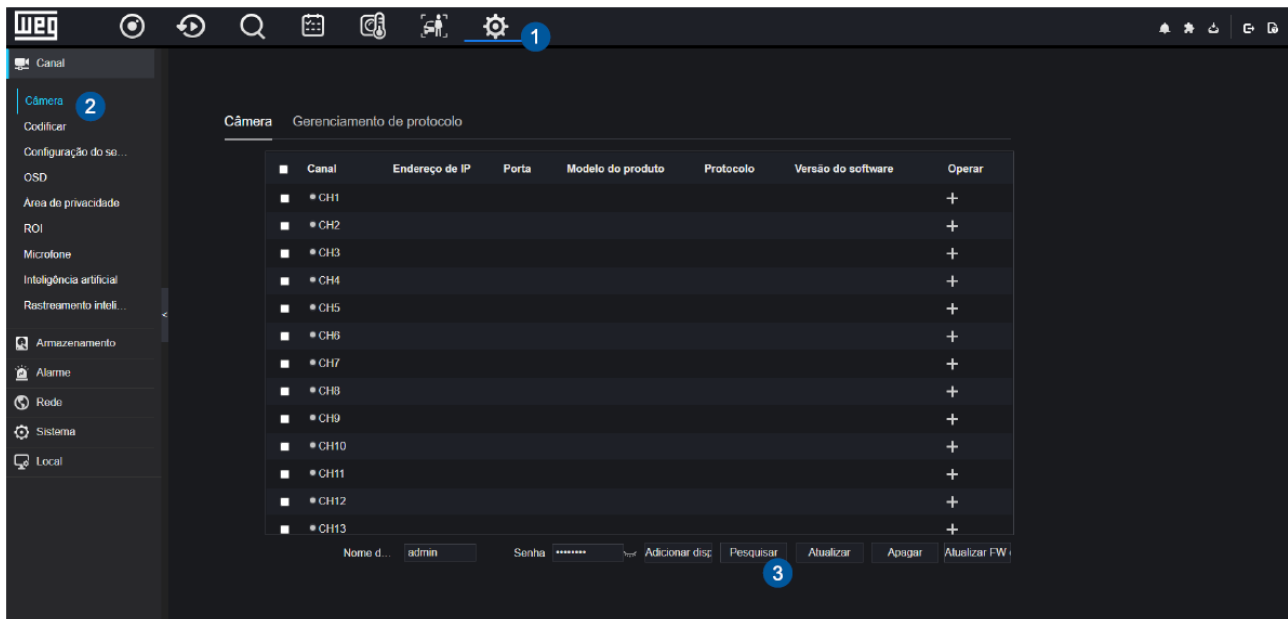
Observação: Esta função precisa ser usada com o gravador de vídeo em rede (NVR).

1. Configure o dispositivo para o mesmo segmento de rede que o NVR.
2. Selecione **Configurações ONVIF** na interface **Interfone**.

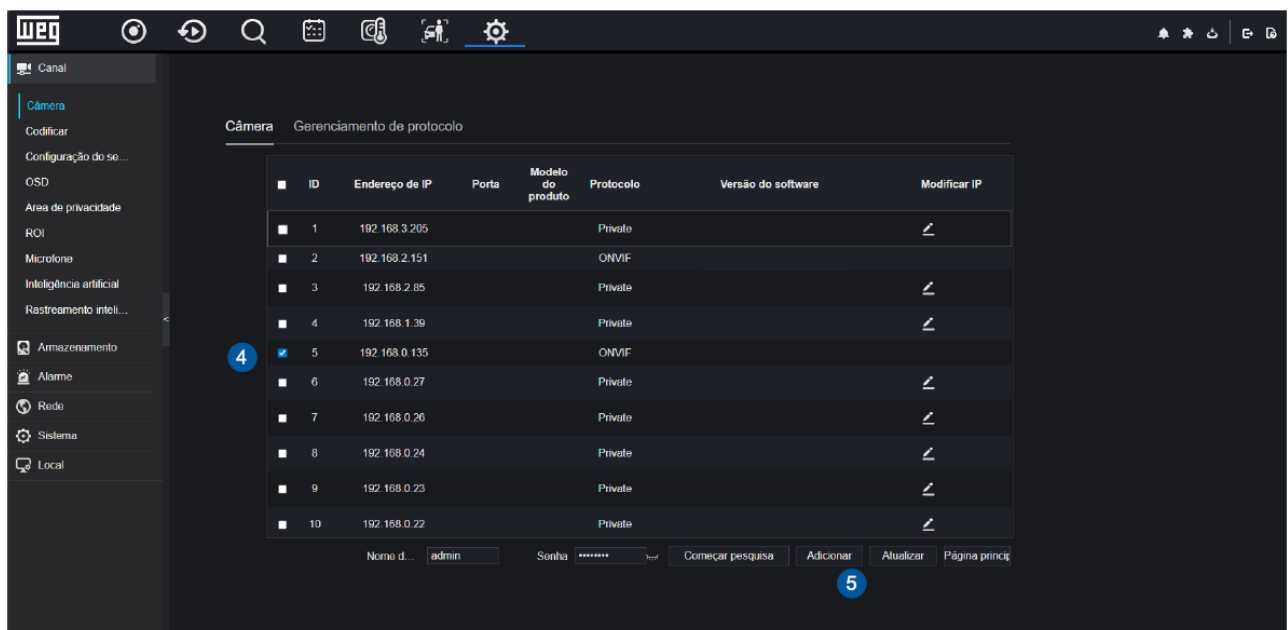
Descrição da função

Nome da Função	Descrição
Habilitar autenticação	Ativar/Desativar a função de autenticação. Quando for desabilitado não há necessidade de inserir o nome de usuário e a senha ao adicionar o dispositivo ao NVR.
Usuário	Defina o nome de usuário. O padrão é admin.
Senha	Defina a senha. A senha padrão é admin.
Porta servidor	O padrão é 8000 e não pode ser modificado.

3. No sistema NVR, clique em [Configuração] > [Canal] > [Câmera] e depois em Pesquisar. Depois clique em Começar Pesquisa e encontre o IP do dispositivo que deseja adicionar.



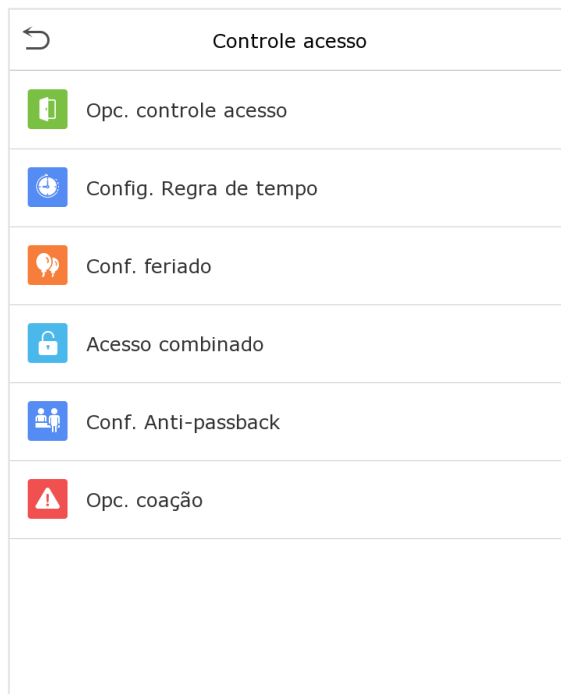
4. Selecione o dispositivo desejado e clique em adicionar.



5. Após a adição bem sucedida você poderá visualizar a imagem do dispositivo no gravador. Para mais detalhes, consulte o *Manual do Usuário do NVR*.

13 Controle de acesso

Quando o dispositivo estiver na interface inicial, selecione Controle acesso para definir a programação da abertura da porta, o controle de travas e configurar outras configurações de parâmetros relacionadas ao controle de acesso.

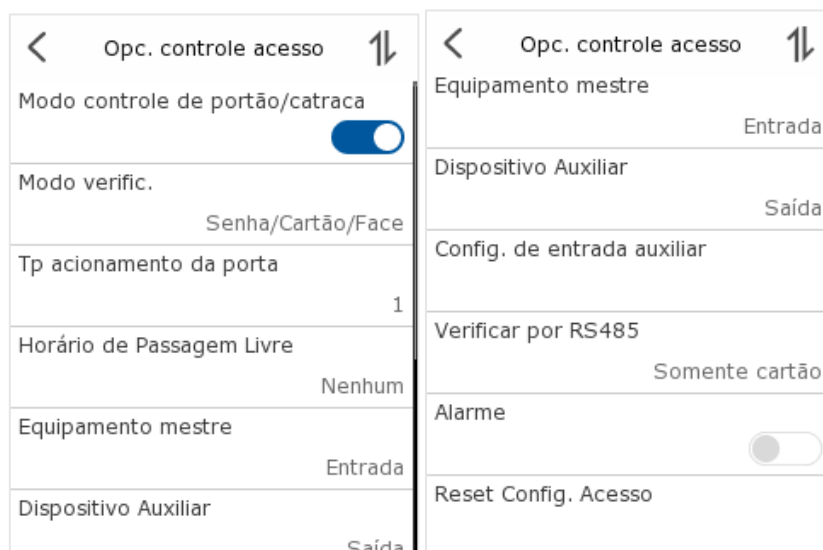


Para obter acesso, o usuário registrado deve atender às seguintes condições:

1. O horário de desbloqueio atual da porta relevante deve estar dentro de qualquer fuso horário válido do período do usuário.
2. O grupo do usuário correspondente deve estar previamente definido na combinação de desbloqueio da porta (e, se houver outros grupos definidos na mesma combinação de acesso, a verificação dos membros desses grupos também é necessária para desbloquear a porta).
3. Nas configurações padrão, novos usuários são alocados no primeiro grupo com o fuso horário padrão do grupo/zona, onde a combinação de acesso é "1" e está definida como desbloqueada por padrão.

13.1 Opções de controle de acesso

Selecione Opc. controle acesso na interface Controle Acesso para definir os parâmetros do bloqueio de controle do terminal e equipamentos relacionados.



Descrição da função

Função	Descrição
Modo controle de portão/catraca	Alterna entre ligado ou desligado para entrar ou não no modo de controle de portão. Quando definido como ligado a interface remove as opções de Tempo do Relé, Atraso do Sensor(s) e Tipo de sensor.
Tempo do Relé	O tempo que o dispositivo controla a fechadura elétrica no estado desbloqueado. Valor válido: 1 a 99 segundos.
Atraso do Sensor(s)	Se a porta não estiver trancada e for deixada aberta para uma certa duração (Atraso do Sensor de Porta), um alarme será disparado. O valor válido do Atraso do Sensor de Porta varia de 1 a 255 segundos.
Tipo de sensor	Existem três tipos de sensores: Nenhum, Normal aberto(NA) e Normal fechado(NF). Nenhum: Significa que o sensor da porta não está em uso. Normal aberto: Isso significa que a porta fica sempre aberta quando a energia elétrica está ligada. Normal fechado: Isso significa que a porta fica sempre fechada quando a energia elétrica está ligada.
Modo verific.	Os modos de verificação suportados incluem: Senha/Cartão/Face, Somente ID Usr., Senha, Somente cartão, Senha+Cartão, Senha ou Cartão, Somente face, Face+Senha e Face+Cartão.
Tp acionamento da porta	Ele define o horário da porta para que ela seja acessível apenas durante esse período.
Horário de Passagem Livre	É o período de tempo programado para o modo "Passagem Livre", de forma que a porta esteja sempre aberta durante esse período.
Alarme	Transmite um alarme sonoro ou alarme de desarmamento do local. Quando a porta é fechada ou a verificação é bem-sucedida, o sistema cancela o alarme do local.

Reset Config. Acesso	Os parâmetros de redefinição de controle de acesso incluem tempo do relé, atraso do sensor, tipo de sensor da porta, modo de verificação, período de tempo disponível da porta, período de horário de passagem livre e alarme. No entanto, os dados de controle de acesso apagados em Gerenciamento de Dados não serão excluídos.
-----------------------------	---

13.2 Configuração de regra de tempo

Selecione **Config. Regra de tempo** na interface **Controle acesso** para configurar as definições de tempo.

- O sistema inteiro pode definir até 50 regras de tempo.
- Cada período de tempo-regra representa **10 Fusos Horários**, ou seja, **1 semana e 3 feriados**, e cada fuso horário é um período padrão de 24 horas por dia, e o usuário só pode verificar dentro do período de tempo válido.
- É possível definir no máximo 3 períodos de tempo para cada fuso horário. O relacionamento entre esses períodos de tempo é **OU**. Assim, quando o horário de verificação cair em qualquer um desses períodos, a verificação será válida.
- O formato do fuso horário de cada período é **HH MM-HH MM**, que é preciso em minutos de acordo com o relógio de 24 horas.

Toque na caixa cinza para pesquisar a Regra de Tempo e especifique a Regra de Tempo necessária (máximo de 50 regras).

Na interface da Regra de tempo selecionada, toque no dia necessário (segunda-feira, terça-feira, etc.) para definir o horário.

← Faixa horária 1

00:00 23:59

▲	▲	▲	▲
00	00	23	59
▼	▼	▼	▼
HH	MM	HH	MM

Confirma(OK) Cancela(ESC)

Especifique o horário de início e o horário de término, e então selecione OK.

Nota:

- A porta fica inacessível o dia todo quando o Horário de Término ocorre antes do Horário de Início (como 23:57 às 23:56).
- É o intervalo de tempo para acesso válido quando o Horário de Término ocorre após o Horário de Início (como 08:00 às 23:59).
- A porta fica acessível o dia todo quando o Horário de Término ocorre após o Horário de Início (de modo que o Horário de Início seja 00:00 e o Horário de Término é 23:59).
- O fuso horário padrão 1 indica que a porta fica aberta o dia todo.

13.3 Feriados

Quando houver um feriado, pode ser necessário um horário de acesso diferente; no entanto, alterar o horário de acesso de todos individualmente é extremamente demorado. Assim, um horário de acesso para feriados, que se aplica a todos os trabalhadores, pode ser definido, e o usuário poderá abrir a porta durante os feriados. Selecione Conf. feriado na interface Controle acesso para definir o acesso em feriados.

← Conf. feriado

Adic. feriado

Todos feriados

- **Adicionar um novo feriado:**

Toque em **Adic. feriado** na interface **Conf. Feriados** e defina os parâmetros do feriado.

Conf. feriado	
No.	1
Data	Indefinido
Tipo de feriado	Feriado tipo 1
Recorrente	☒

- **Editar um feriado:**

Na interface **Conf. feriado**, selecione um item de feriado para ser modificado. Toque em **Editar** para modificar os parâmetros do feriado.

- **Excluir um feriado:**

Na interface **Conf. feriado**, selecione um item de feriado a ser excluído e toque em **Apagar**. Selecione **OK** para confirmar a exclusão. Após a exclusão, este feriado não será exibido na interface **Todos feriados**.

13.4 Acesso combinado

Grupos de acesso são organizados em diferentes combinações de desbloqueio de portas para alcançar múltiplas verificações e fortalecer a segurança. Em uma combinação de abertura de porta, a faixa do número combinado N é $0 \leq N \leq 5$ e o número de membros N pode pertencer a um único grupo de acesso ou a cinco grupos de acesso diferentes. Selecione a interface **Acesso combinado** para configurar a definição de verificação combinada

Acesso combinado	
1	01 00 00 00 00
2	00 00 00 00 00
3	00 00 00 00 00
4	00 00 00 00 00
5	00 00 00 00 00

Na interface de verificação combinada, toque na combinação desbloqueio da porta a ser definida e toque nas **setas para cima e para baixo** para inserir o número da combinação e pressione **OK**.

Por exemplo:

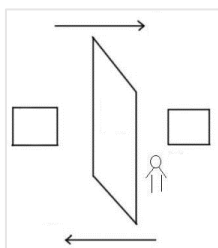
- Se a **Combinação de desbloqueio da porta 1** é definida como **(01 03 05 06 08)**, isso indica que a combinação de desbloqueio 1 consiste em 5 pessoas e que todos os 5 indivíduos são de 5 grupos, a saber, Grupo AC 1, Grupo AC 3, Grupo AC 5, Grupo AC 6 e Grupo AC 8, respectivamente.
- Se a **Combinação de desbloqueio de porta 2** é definida como **(02 02 04 04 07)**, isso indica que a combinação de desbloqueio 2 consiste em 5 pessoas; as duas primeiras são do Grupo AC 2, as duas seguintes são do Grupo AC 4, e a última pessoa é do Grupo AC 7.
- Se a **Combinação de desbloqueio da porta 3** for definida como **(09 09 09 09 09)**, isso indica que há 5 pessoas nessa combinação; todas do Grupo AC 9.
- Se a **Combinação de desbloqueio da porta 4** for definida como **(03 05 08 00 00)**, isso indica que a combinação de desbloqueio 4 consiste em apenas três pessoas. A primeira pessoa é do Grupo AC 3, a segunda pessoa é do Grupo AC 5 e a terceira pessoa é do Grupo AC 8.

Nota: Para apagar a combinação de desbloqueio da porta, defina todas as combinações de desbloqueio da porta para 0.

13.5 Configuração Anti-passback

Para evitar que usuários entrem sem verificação seguindo alguém autorizado — uma prática conhecida como 'carona' ou tailgating — desenvolvemos a função Anti-Passback. Ao habilitar este recurso, o registro de saída só é liberado se houver um registro de entrada correspondente.

A função exige dois dispositivos operando em conjunto via protocolo Wiegand: um instalado na saída (mestre) e outro na entrada (escravo). Para o funcionamento correto, o formato Wiegand e o tipo de saída (ID de usuário ou número do cartão) devem ser idênticos em ambos os equipamentos.



Toque em Configuração anti-passback na interface de controle de acesso.

A captura de tela mostra a interface de configuração do sistema de acesso. No topo, há um ícone de seta para trás e o título "Conf. Anti-passback". Abaixo, há o texto "Sentido Anti-passback" e uma opção "Sem Anti-passback" que está selecionada. A interface é simples e funcional, com uma barra de navegação no topo e uma área de configuração principal.

Descrição da função

Nome da função	Descrição
Direção anti-passback	Sem anti-passback: A função anti-passback está desativada, o que significa que a verificação bem-sucedida através do dispositivo mestre ou do dispositivo escravo pode destravar a porta. O estado de atendimento não é salvo nesta opção. Anti-passback de saída: Depois que um usuário fizer check-out, somente se o último registro for um registro de check-in, o usuário poderá fazer check-out novamente; caso contrário, o alarme será acionado. No entanto, o usuário pode fazer o check-in livremente. Anti-passback entrada: Depois que um usuário fizer check-in, somente se o último registro for um registro de check-out, o usuário poderá fazer check-in novamente; caso contrário, o alarme será acionado. No entanto, o usuário pode fazer check-out livremente. Anti-passback ent/saí: Depois que um usuário faz check-in/out, somente se o último registro for um registro de check-out, o usuário pode fazer check-in novamente; ou se for um registro de check-in, o usuário pode fazer check-out novamente; caso contrário, o alarme será acionado.

13.6 Opções de coação

Uma vez que um usuário ativa a função de verificação de coação com um(ns) método(s) de autenticação específico(s), e quando ele/ela estiver sob coação e se autenticar usando a verificação de coação, o dispositivo destranca a porta como de costume. Ao mesmo tempo, um sinal é enviado para ativar o alarme também. Na interface de Controle de Acesso, selecionar Opc. coação para configurar as definições de emergência.

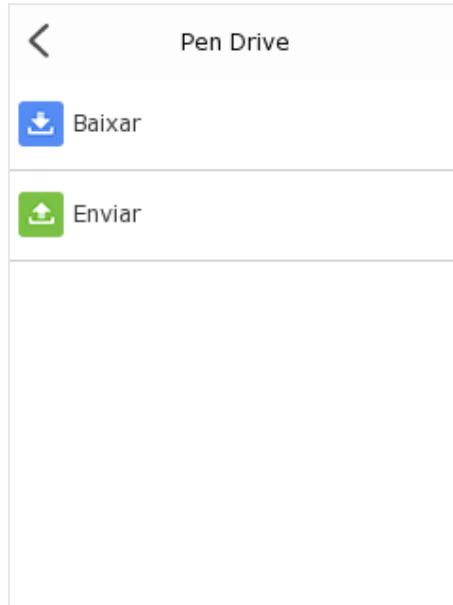
A imagem mostra a interface de configuração 'Opc. coação' em um aplicativo. No topo, há um ícone de seta para trás e o título 'Opc. coação'. Abaixo, há uma seção 'Senha de alarme' com um botão de alternância desativado. Segue-se o campo 'Atraso alarme(s)' com o valor '10' exibido. Abaixo disso, há o campo 'Senha de coação' com o valor 'Nenhum' exibido. O fundo da interface é branco com elementos cinza.

Descrição da função

Nome da Função	Descrição
Senha de alarme	Quando um usuário usa o método de verificação de senha, um sinal de alarme será gerado, caso contrário, não haverá sinal de alarme.
Atraso alarme(s)	O sinal de alarme não será transmitido até que o tempo de atraso do alarme tenha decorrido. O valor varia de 1 a 999 segundos.

14 Gerenciador USB

Você pode importar informações do usuário, acessar dados e outros dados de um drive USB para um computador ou outros dispositivos. Antes de carregar/baixar dados de/para o disco USB, insira primeiro o disco USB na porta USB. Selecione a interface Ger. pen drive no menu principal.



Nota: Apenas o formato FAT32 é suportado quando baixando dados usando disco USB.

14.1 Baixar USB

Na interface Ger. pen drive, toque em **Baixar**.



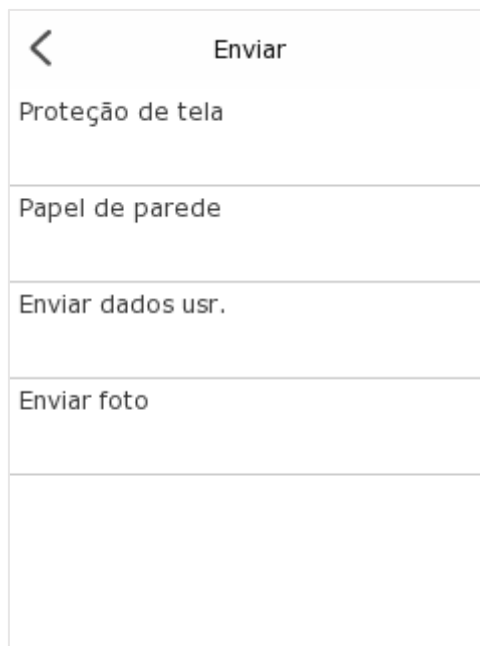
Descrição da função

Menu	Descrição
Baixar reg. Ponto	Para baixar o acesso gravado em um período de tempo especificado em um disco USB.

Baixar usuários	Para baixar todas as informações do usuário do dispositivo para um disco USB.
Baixar fotos usr.	Para baixar todas as fotos do dispositivo para um disco USB.
Baixar fotos Autorizados	Para baixar todas as fotos autorizadas do dispositivo para o disco USB.
Baixar fotos lista bloqueados	Para baixar todas as fotos não autorizadas do dispositivo para o disco USB.

14.2 USB Upload

Na interface do Gerenciador USB , toque em **Download**.

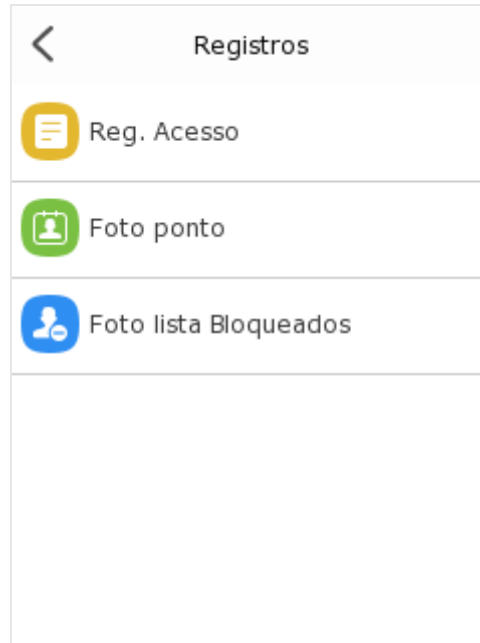


Descrição da função

Menu	Descrição
Proteção de tela	Para carregar todos os protetores de tela do disco USB para o dispositivo. Você pode escolher Carregar foto selecionada ou Carregar todas as fotos. As imagens serão exibidas na interface principal do dispositivo após o carregamento.
Papel de parede	Para carregar todos os papéis de parede do disco USB para o dispositivo. Você pode escolher Carregar foto selecionada ou Carregar todas as fotos. As imagens serão exibidas na tela após o carregamento.
Enviar dados usr.	Para carregar todas as informações do usuário do disco USB para o dispositivo.
Enviar foto	Para carregar todos os retratos de usuários do disco USB para o dispositivo.

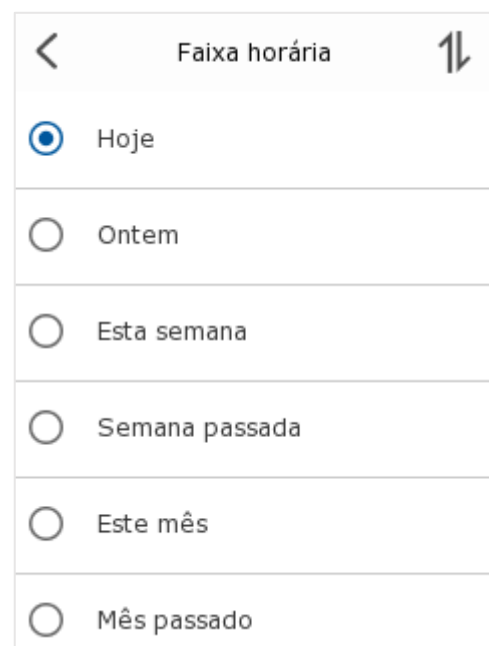
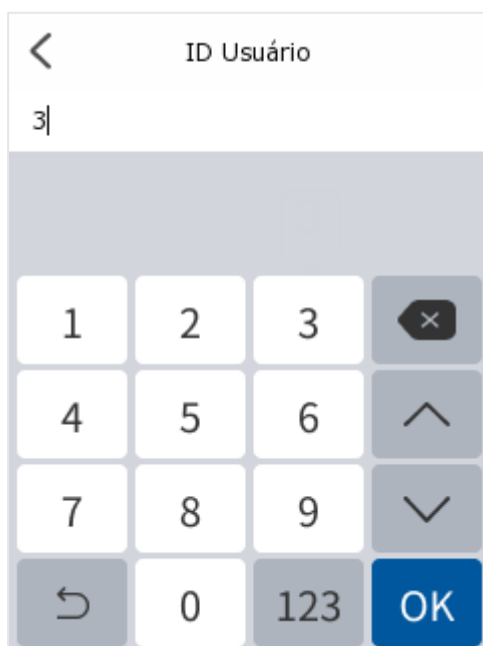
15 Registros

Uma vez verificada a identidade do usuário, o registro de acesso é salvo no dispositivo. Essa função permite que os usuários verifiquem seus logs de eventos. Quando o dispositivo estiver na interface inicial, selecione Registros para pesquisar os logs de eventos necessários.



O processo de busca por fotos de presença e lista de fotos bloqueadas é semelhante à busca por registros de eventos. A seguir, há um exemplo de busca de registro de presença. Na interface Registros, selecionar Reg. Acesso para pesquisar o registro necessário.

1. Insira o ID do usuário a ser pesquisado e clique em OK. Se você quiser pesquisar logs de todos os usuários, clique em OK sem inserir nenhum ID de usuário.
2. Selecione o intervalo de tempo em que os logs serão pesquisados.

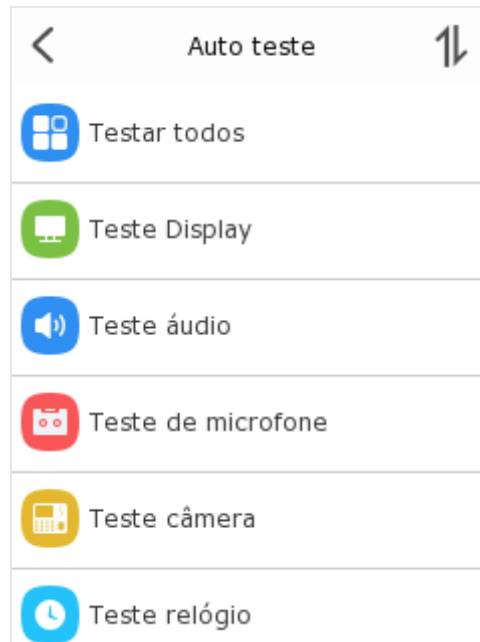


3. Assim que a pesquisa de log for bem-sucedida. Toque no login destacado em verde para ver seus detalhes.

Registros pessoais		
Data	ID Usuário	Tempo
02-05		Total r...:9
	3	11:30 09:39
		09:39 09:38
		09:38 09:37
		09:37 09:36
		09:36

16 Auto teste

Quando o dispositivo estiver na interface inicial, selecione Auto teste, ele permite que o sistema teste automaticamente se as funções de vários módulos estão funcionando normalmente, incluindo o Display, Voz, Microfone, Câmera e Relógio de tempo real (RTC).

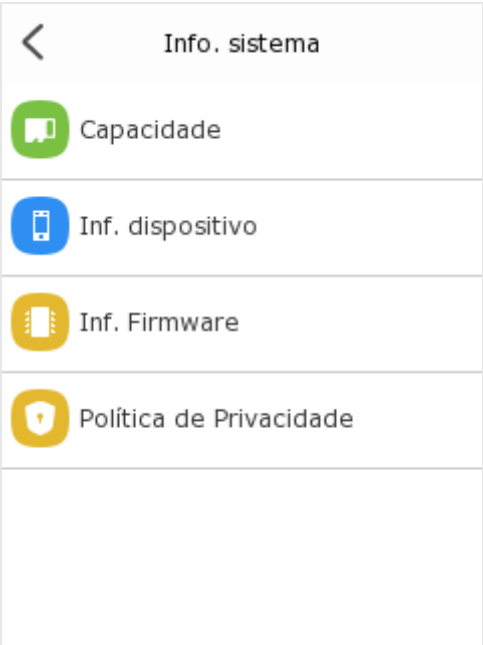


Descrição da função

Nome da Função	Descrição
Testar todos	Para testar automaticamente se o Display, a Voz, o Microfone, Câmera e Relógio de tempo real (RTC) estão normais.
Teste Display	Para testar automaticamente o efeito de exibição do Display exibindo totalmente cor, puro branco e puro preto para verificar se a tela exibe cores normalmente.
Teste áudio	Para testar automaticamente se os arquivos de áudio armazenados no dispositivo estão completos e se a qualidade de voz é boa.
Teste de microfone	Para testar se o microfone está funcionando corretamente, fale nele.
Teste câmera	Para testar se a câmera funciona corretamente.
Teste relógio	Para testar o RTC. O dispositivo testa se o relógio funciona normalmente e com precisão usando um cronômetro. Toque na tela para começar a contar e pressione novamente para parar de contar.

17 Informação do sistema

Quando o dispositivo estiver na interface inicial, pressione M/OK e selecione Info. Sistema para visualizar o status do armazenamento, as informações de versão do dispositivo, as informações de firmware e a política de privacidade.



Descrição da função

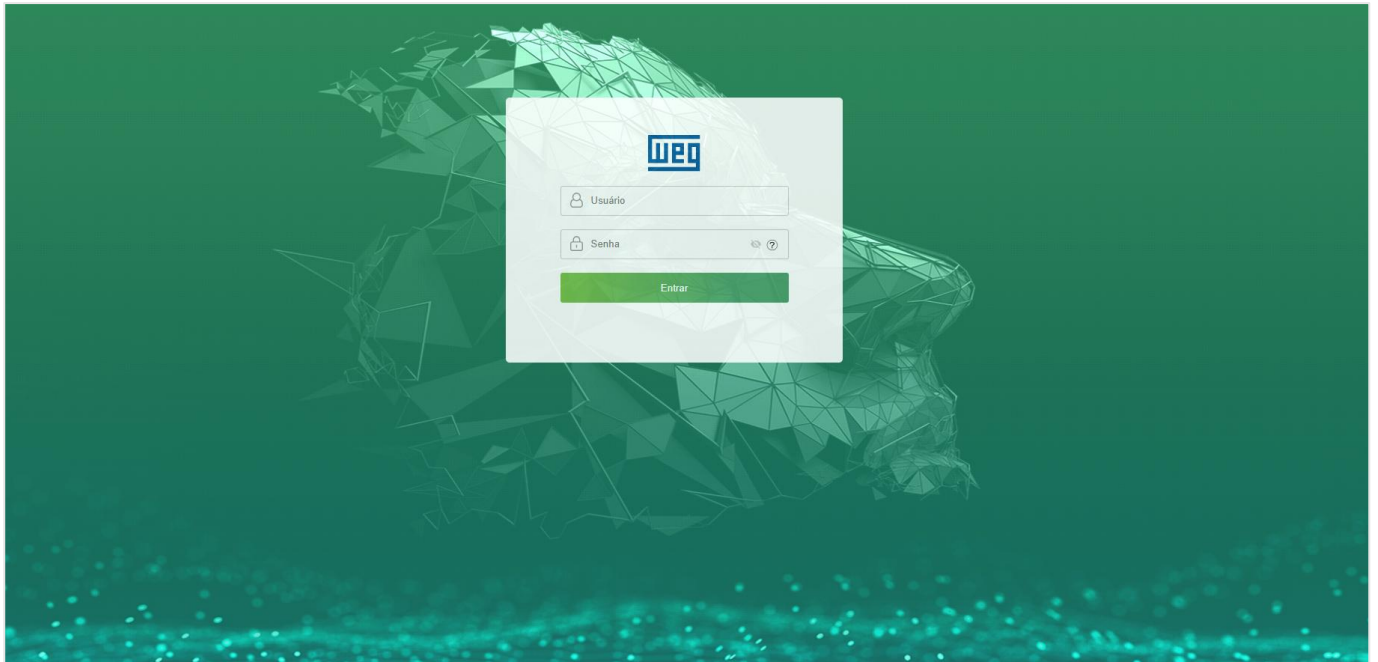
Nome da Função	Descrição
Capacidade	Exibe o armazenamento do usuário do dispositivo atual, Face, Impressão digital, Armazenamento de cartão e senha administradores, registros, frequência, lista de bloqueio e perfil fotos.
Inf. dispositivo	Exibe o nome do dispositivo, o número de série e o endereço MAC. Algoritmo de impressão digital, Algoritmo facial, Informações da plataforma, Versão da MCU e Fabricante.
Inf. Firmware	Exibe a versão do firmware e outras informações de versão do dispositivo.
Política de Privacidade	Exibir a política de privacidade do dispositivo.

18 Interface WEB

Para gerenciar o seu terminal facial via navegador, siga os passos abaixo:

1. Certifique-se de que o computador esteja na mesma rede que o terminal.
2. Abra o seu navegador web de preferência.
3. Na barra de endereços, digite o endereço IP do dispositivo seguido da porta :1443.

Exemplo: <https://192.168.1.201:1443>



AVISO DE SEGURANÇA: Primeiro Acesso

Para garantir a proteção do seu dispositivo e da sua rede, o terminal facial possui credenciais de acesso padrão configuradas de fábrica:

- **Usuário:** admin
- **Senha:** admin@123

⚠ IMPORTANTE: Por questões de segurança, a **alteração desta senha é obrigatória no primeiro acesso** à interface web. Você não conseguirá prosseguir com a configuração do dispositivo sem definir uma nova senha pessoal e segura.

A interface web do terminal facial funciona como o painel central de gerenciamento do dispositivo. Ela permite configurar parâmetros de rede (IP, Wi-Fi), ajustar as definições do serviço em nuvem e realizar a sincronização de data e hora.

Além da gestão de sistema (idioma, volume, segurança HTTPS/SSH), a interface oferece controle total sobre as funcionalidades biométricas, incluindo o ajuste de configurações de face, calibração Wiegand e gestão de protocolos de comunicação como SIP e ONVIF. Por fim, o painel possibilita a visualização do status do hardware, consulta de capacidade de armazenamento, atualização de firmware e auditoria através dos registros de logs (logs de acesso).



Info. sistema

Inf. dispositivo

Capacidade

Inf. Firmware

Configurações Avançadas

Conf. Com.

Configurações de conexão

Configuração do serviço em nuvem

Wi-Fi

Configuração de data

Sistema

Configurações SIP

Configurações ONVIF

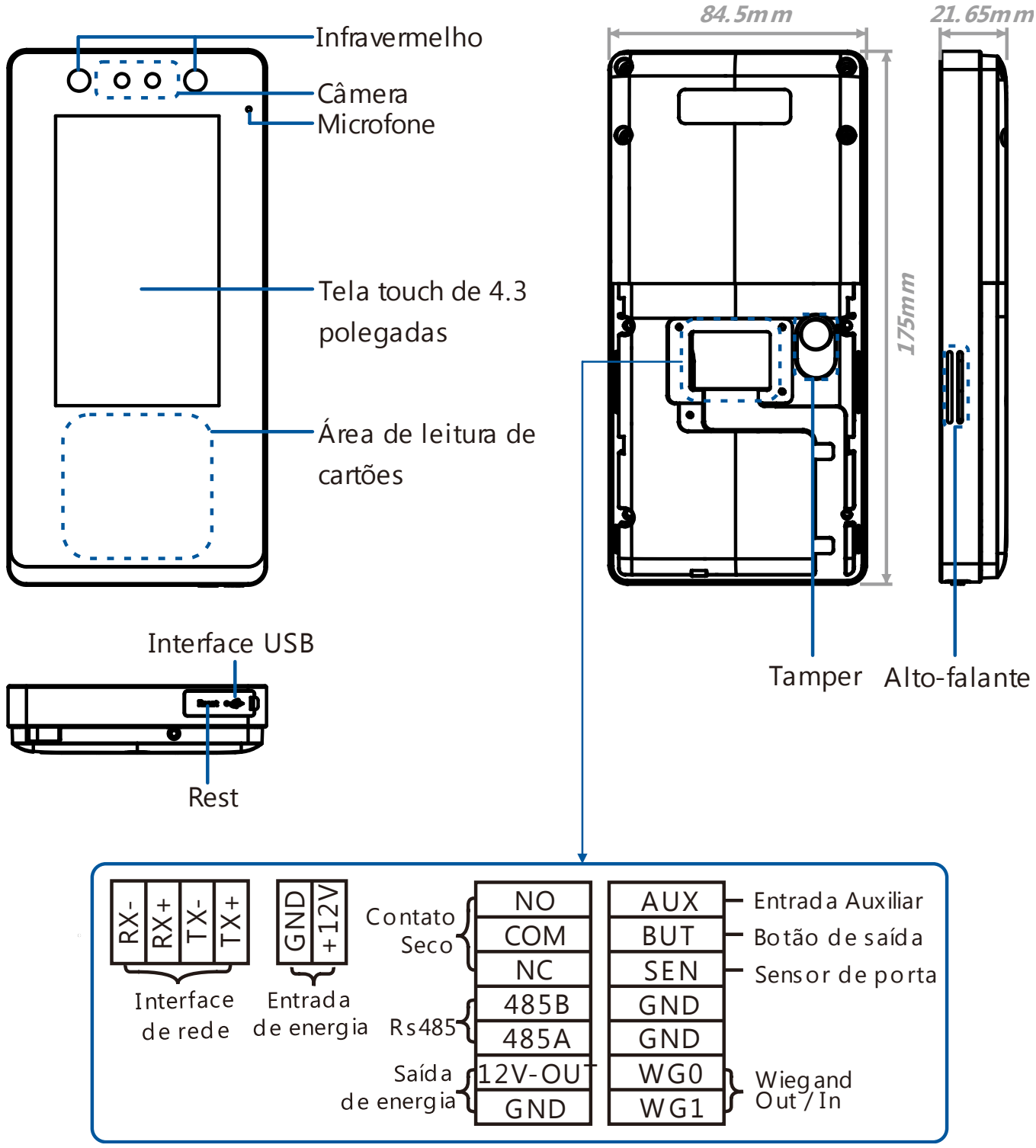
Comunic. Serial

Inf. dispositivo

Nome dispositivo	WA03C-W-10
No. série	NAU2253600892
Versão MCU	212
Endereço de MAC	00:17:61:12:3d:d8
Algoritmo Face	WEG Face VX4.0
Inf. plataforma	ZAM70_TFT
Fabricante	WEG S.A.

Copyright © 2016-2021 All Right Reserved

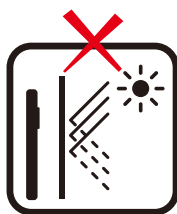
1 Visão Geral



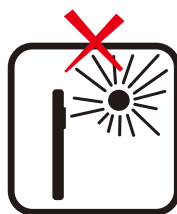
2 Ambiente de Instalação



INSTALAR
APENAS EM
INTERIORES



EVITAR A
INSTALAÇÃO
PERTO DE
JANELAS DE VIDRO



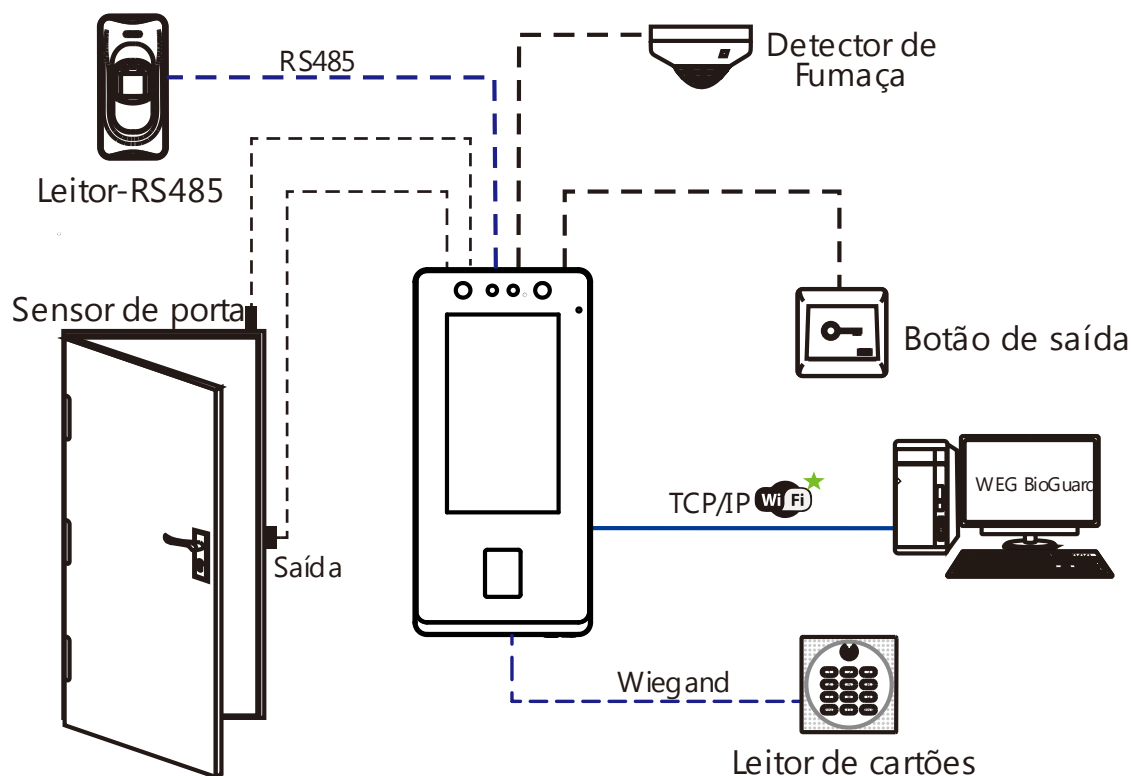
EVITAR A
EXPOSIÇÃO
DIRETA À
LUZ SOLAR



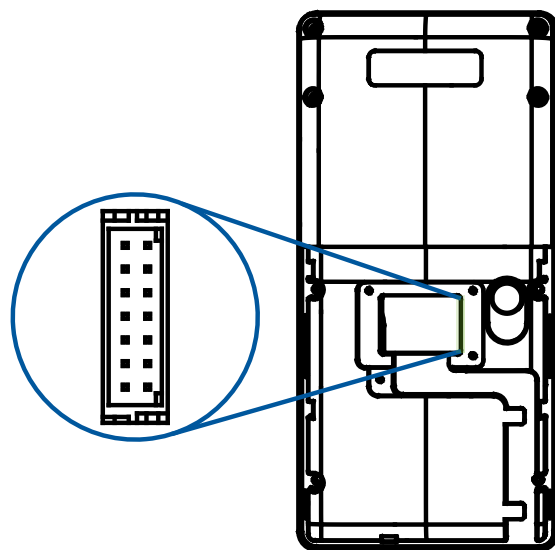
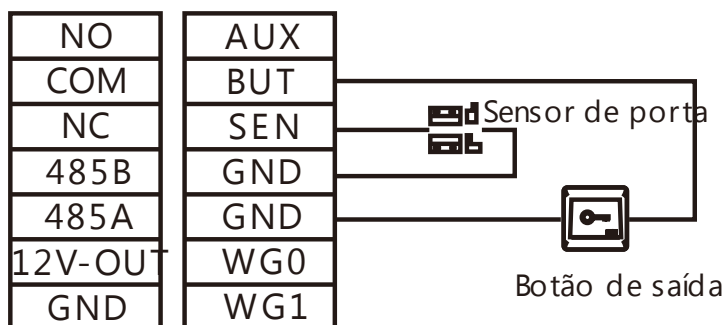
EVITAR O USO DE
QUALQUER FONTE
DE CALOR PERTO
DO DISPOSITIVO

- Evite o contato direto com a luz solar por longos períodos
- Proteja o dispositivo contra umidade, água e chuva.
- Manuseie o dispositivo com cuidado.
- Certifique-se de que o dispositivo não seja instalado próximo ao mar ou a outros ambientes onde a oxidação e a ferrugem do metal possam ocorrer o dispositivo for exposto por longos períodos.
- Proteja o dispositivo contra raios.
- Certifique-se de que o dispositivo não seja utilizado em ambientes ácidos e alcalinos por longos períodos.

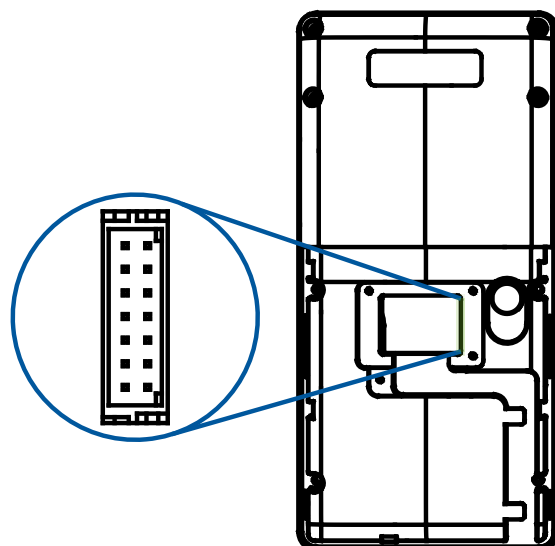
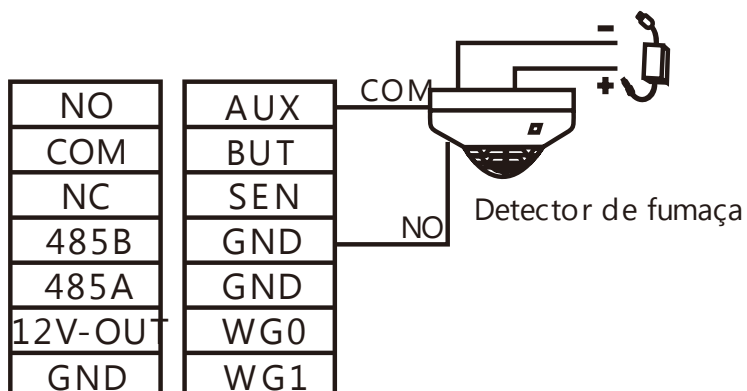
3 Instalação do dispositivo



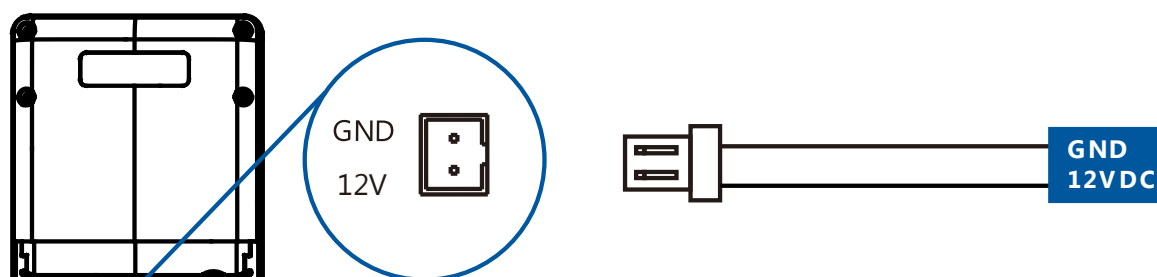
4 Conexão do botão de saída e sensor de porta



5 Conexão do sensor de fumaça

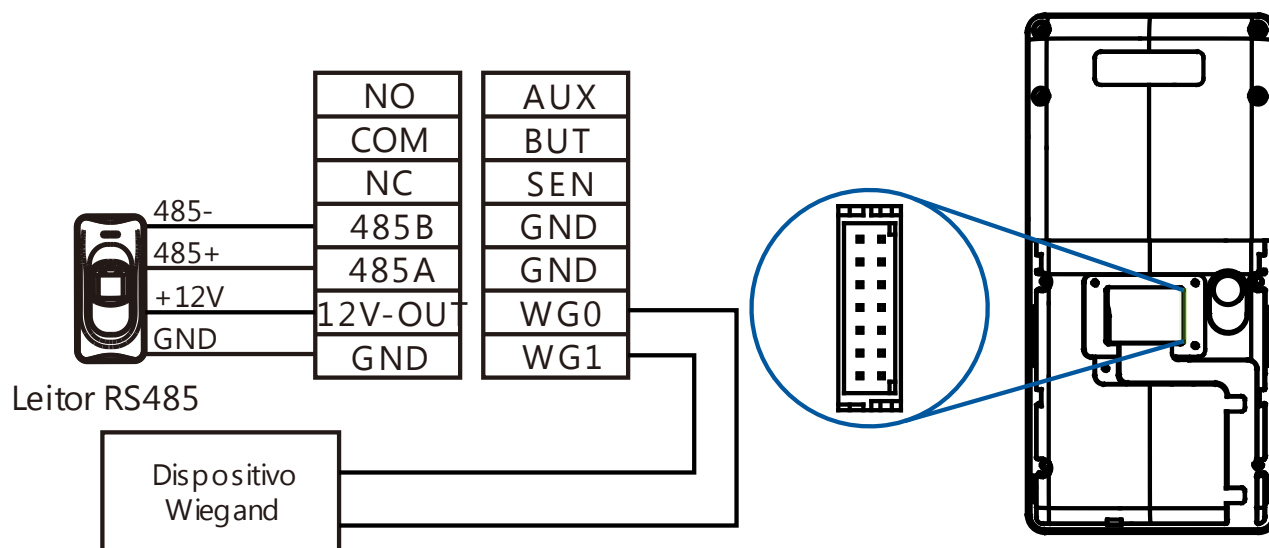


6 Conexão de energia



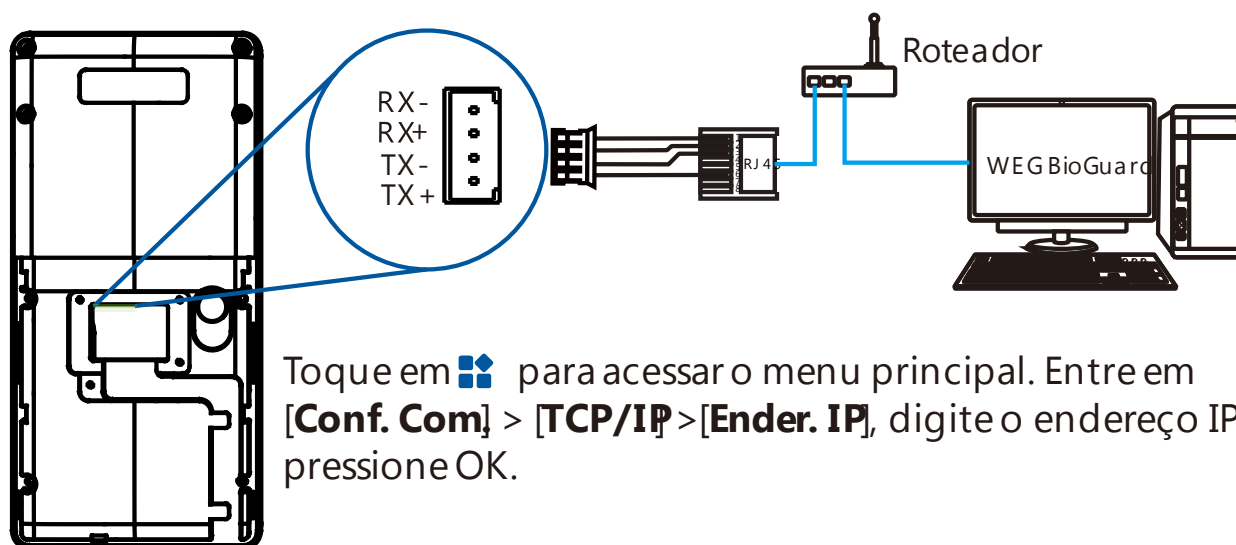
- Fonte de alimentação recomendada: 12V, 3A
- Para compartilhar a energia com outros dispositivos, use uma fonte com capacidade de corrente mais alta.

7 Conexão RS485 e leitor Wiegand



Nota: A interface Wiegand é partilhada e o utilizador pode optar por utilizar a função de entrada ou de saída Wiegand para estabelecer a interface com diferentes dispositivos Wiegand.

8 Conexão Ethernet



Toque em  para acessar o menu principal. Entre em **[Conf. Com] > [TCP/IP] > [Ender. IP]**, digite o endereço IP e pressione OK.

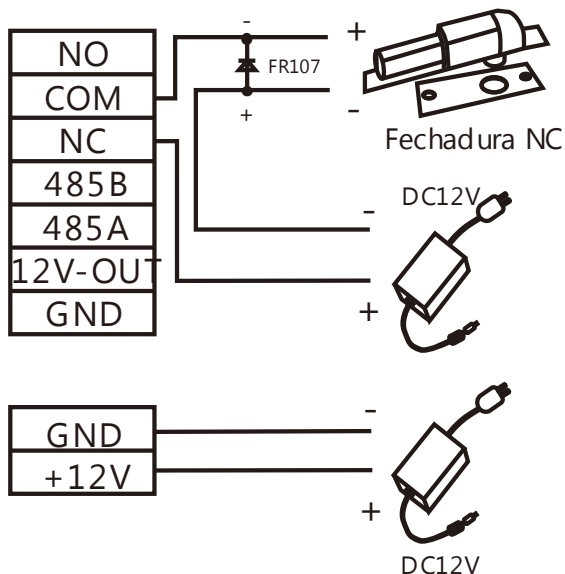
Observação: Na LAN, o endereço IP do servidor (PC) e o dispositivo devem estar no mesmo segmento de rede ao se conectar ao software.

9 Ligação do relé de bloqueio

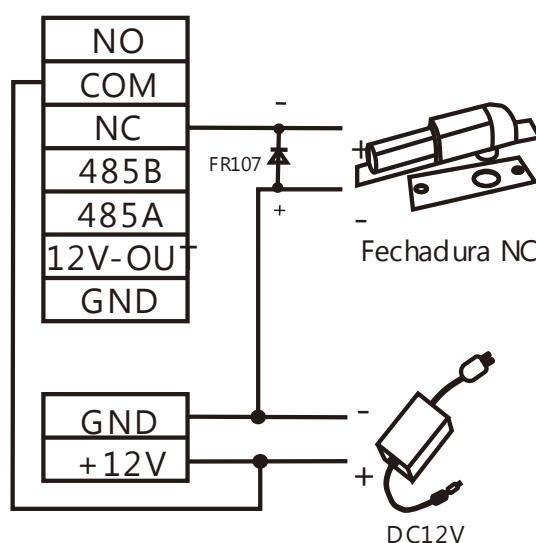
O sistema suporta fechadura normalmente aberta e normalmente fechada. O bloqueio **NO** é conectado aos terminais "**NO**" e "**COM**", e o bloqueio **NC** é conectado aos terminais "**NC**" e "**COM**".

Veja abaixo um exemplo de bloqueio pelo **NC**:

O dispositivo não compartilha energia com a fechadura:



O dispositivo compartilhando energia com a fechadura:



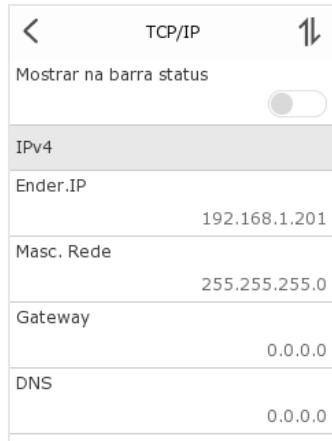
20 Portas Utilizadas

A tabela a seguir apresenta as portas utilizadas pelo terminal:

Porta	Protocolo	Padrão de Fábrica	Função
1443	TCP	Habilitado	Interface WEB
3718	TCP	Desabilitado	Acesso as configurações de manutenção do equipamento
4370	TCP	Desabilitado	Comunicação Standalone
5060	UDP	Desabilitado	SIP padrão não criptografado
5061	TCP	Desabilitado	SIP com TLS
8000	TCP	Habilitado	HTTP
8554	TCP	Habilitado	RTSP

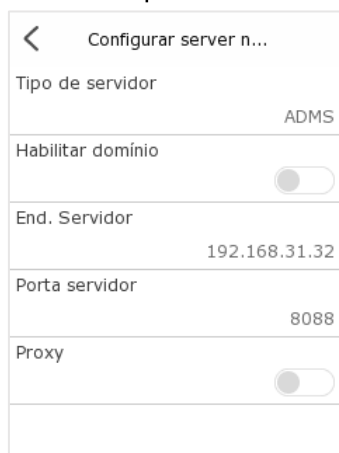
21 Como adicionar o Terminal Facial no WEG BioGuard

1. No terminal facial em [Conf. Com] > [TCP/IP] defina os parâmetros de rede. Se a comunicação TCP/IP do dispositivo for bem-sucedida, o ícone  será exibido no canto superior da tela inicial.



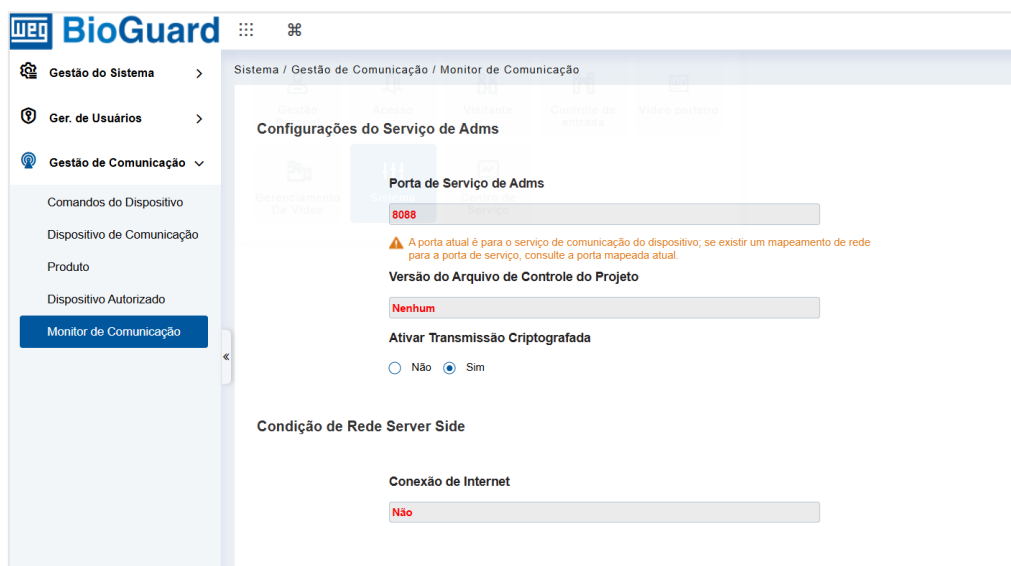
The screenshot shows the 'TCP/IP' configuration screen. At the top, there is a back arrow, the title 'TCP/IP', and a refresh icon. Below the title is a toggle switch for 'Mostrar na barra status'. The main section is titled 'IPv4' and contains the following fields: 'Ender.IP' with the value '192.168.1.201', 'Masc. Rede' with the value '255.255.255.0', 'Gateway' with the value '0.0.0.0', and 'DNS' with the value '0.0.0.0'.

2. Acesse [Conf. Com] > [Configurar Server Nuvem] para definir o endereço e a porta do servidor. Por exemplo, defina o endereço IP e o número da porta do servidor após a instalação do software.



The screenshot shows the 'Configurar server n...' screen. It has a back arrow and the title 'Configurar server n...'. The fields include: 'Tipo de servidor' set to 'ADMS', 'Habilitar domínio' with a toggle switch, 'End. Servidor' with the value '192.168.31.32', 'Porta servidor' with the value '8088', and 'Proxy' with a toggle switch.

3. Para saber qual a porta do servidor, acesse no BioGuard: Sistema > Gestão de Comunicação > Monitor de Comunicação e verifique qual a porta ADMS utilizada. (Por padrão de fábrica 8088)



The screenshot shows the BioGuard web interface. The left sidebar contains the following menu items: 'Gestão do Sistema', 'Ger. de Usuários', 'Gestão de Comunicação' (expanded), 'Comandos do Dispositivo', 'Dispositivo de Comunicação', 'Produto', 'Dispositivo Autorizado', and 'Monitor de Comunicação' (highlighted). The main content area is titled 'Sistema / Gestão de Comunicação / Monitor de Comunicação'. It displays 'Configurações do Serviço de Adms' with the following details: 'Porta de Serviço de Adms' set to '8088', a warning message 'A porta atual é para o serviço de comunicação do dispositivo, se existir um mapeamento de rede para a porta de serviço, consulte a porta mapeada atual.', 'Versão do Arquivo de Controle do Projeto' set to 'Nenhum', and 'Ativar Transmissão Criptografada' with radio buttons for 'Não' and 'Sim' (selected). At the bottom, it shows 'Condição de Rede Server Side' with 'Conexão de Internet' set to 'Não'.

4. Caso durante a instalação do BioGuard foi selecionado a opção de “Use HTTPS”, no terminal facial em [Conf. Com] > [Conf. Comunic] habilite a opção HTTPS. Caso contrário, desabilite a opção.

Conf. Comunic.

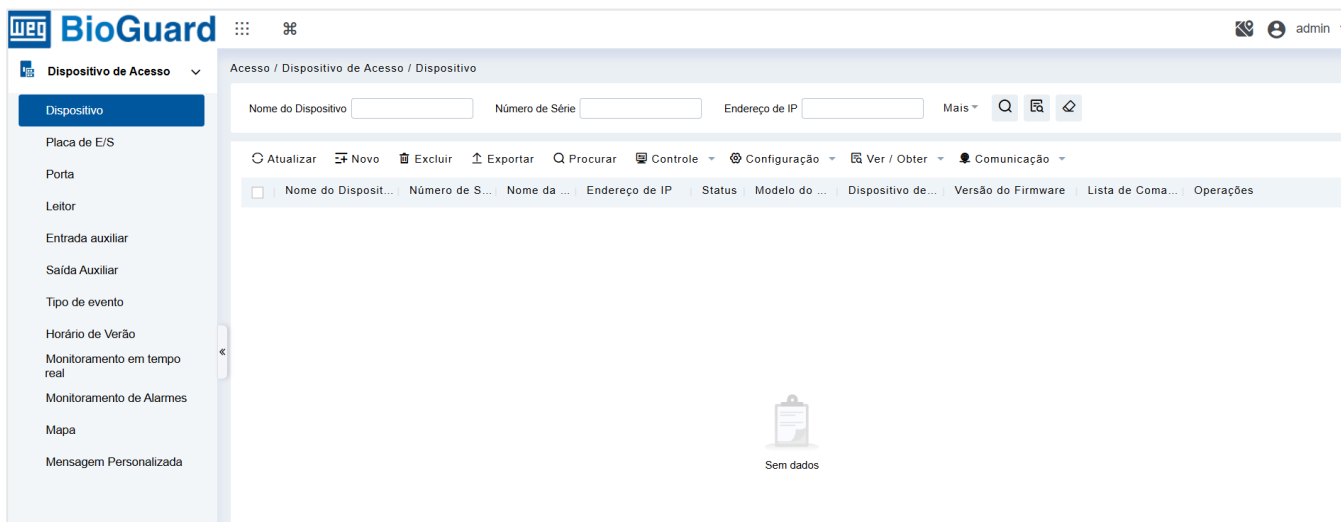
Senha com. *****

ID Equip. 1

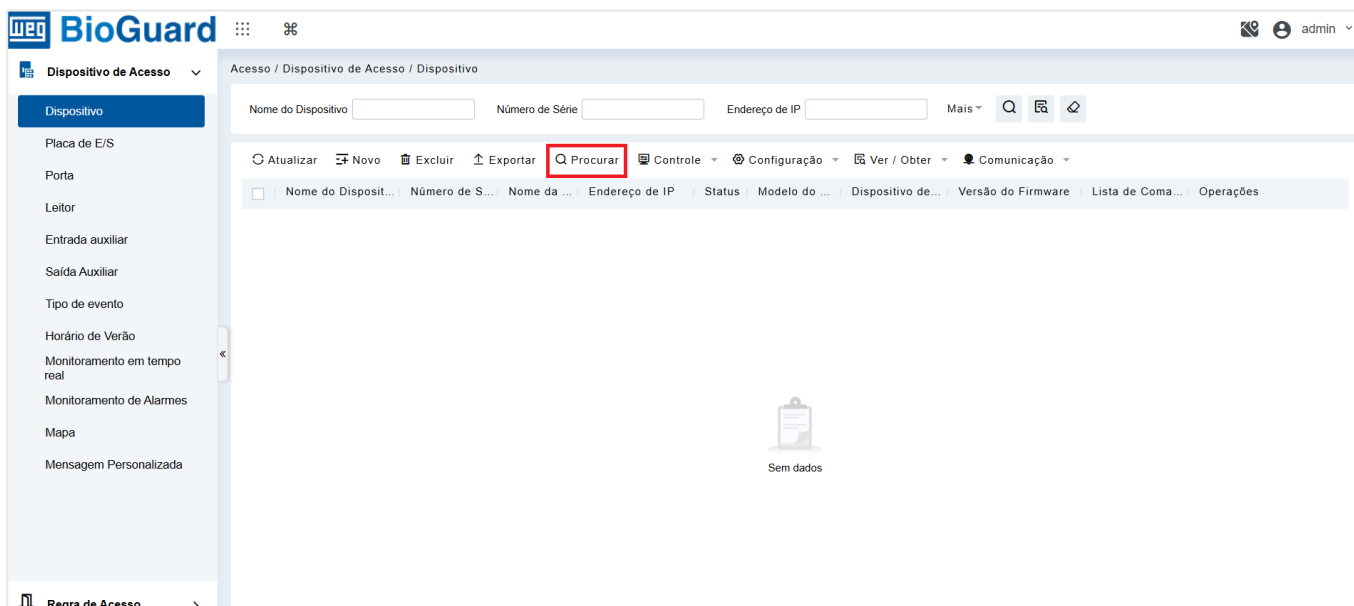
Porta de comu.TCP 4370

HTTPS ☐

5. No software WEG BioGuard para adicionar o terminal facial, acesse Acesso > Dispositivo de Acesso > Dispositivo.



6. Selecione a opção Procurar.



7. Selecione **Buscar** e em seguida na coluna de operações selecione **Adicionar**.

The screenshot displays the BioGuard web application interface. A search modal titled "Procurar" is open, showing a search for devices. The modal includes a "Buscar" button and a message: "Nenhum dispositivo encontrado Baixe as Ferramentas de Pesquisa no Disco Local". Below this, a progress bar shows "Progresso Total" at 100% and "Contagem de dispositivos buscados: 1". Search filters for "Endereço de IP", "Tipo de Dispositivo", and "Número de Série" are present. A table lists the search results:

Endereço de IP	Endereço MAC	Máscara de ...	Endereço de...	Número de S...	Tipo de Dis...	Definir Servidor	Operações
192.168.1.201	255.255.255.0	0.0.0.0	PDA5253601226	WA04C-W-10			Adicionar

At the bottom of the modal, a warning message states: "A porta de comunicação atual do sistema é 8088, verifique se o dispositivo está definido corretamente." and a "Fechar" button is located.

The background interface shows the "Dispositivo de Acesso" section with a sidebar menu containing options like "Placa de E/S", "Porta", "Leitor", "Entrada auxiliar", "Saída Auxiliar", "Tipo de evento", "Horário de Verão", "Monitoramento em tempo real", "Monitoramento de Alarmes", "Mapa", and "Mensagem Personalizada". The bottom status bar indicates "50 linhas por página", "Pular Para 1 / 0 Página", and "Total de 0 registros".