

Manual do Usuário

TERMINAL FACIAL GO WA02-FW-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	6
2	SEGURANÇA ELÉTRICA.....	7
3	SEGURANÇA OPERACIONAL.....	7
4	INSTRUÇÃO DE USO	8
4.1	Posição em pé, postura e expressão facial.....	8
4.2	Registro de Modelo de Rosto.....	9
4.3	Posicionamento do Dedo.....	10
4.4	Reserva Interface.....	10
4.5	Modo de Verificação	11
4.5.1	Verificação Facial	11
4.5.2	Verificação de Impressão digital.....	12
4.5.3	Verificação de Senha.....	14
4.5.4	Verificação Combinada.....	14
5	VISÃO GERAL	16
5.1	Aparência.....	16
5.2	Descrição do Terminal e Cabeamento	17
5.2.1	Descrição do Terminal	17
5.3	Descrição da fiação	17
5.3.1	Conexão de Energia.....	17
5.3.2	Sensor de Porta & Conexão do Botão de Saída.....	18
5.3.3	Travar Conexão do Relé.....	18
5.3.4	Conexão Ethernet.....	19
6	INSTALAÇÃO.....	19
6.1	Ambiente de Instalação.....	19
6.2	Instalação do Dispositivo.....	19
7	MENU PRINCIPAL.....	20
8	GERENCIAMENTO DE USUÁRIOS.....	21
8.1	Novo Cadastro de Usuário.....	21
8.1.1	Registre um ID de usuário e Nome	22
8.1.2	Função do Usuário	22
8.1.3	Registrar Impressão Digital	23
8.1.4	Registrar Face	23
8.1.5	Senha.....	24
8.1.6	Foto do usuário.....	24
8.2	Todos os Usuários.....	25
8.2.1	Editar Usuário	25
8.2.2	Excluir Usuário.....	25
8.3	Estilo do display.....	26

9	PRIVILÉGIOS DO USUÁRIO.....	27
10	COMUNICAÇÃO	28
10.1	Ethernet.....	28
10.2	Configuração da comunicação.....	29
10.3	Configurações de Wi-Fi.....	30
10.4	Configurações do Servidor em Nuvem	32
10.5	Diagnóstico de Rede.....	32
11	CONFIGURAÇÕES DO SISTEMA	33
11.1	Data e Hora.....	33
11.2	Configurações de Logs de Acesso/Frequência	34
11.3	Parâmetros de Face.....	35
11.4	Configurações de Segurança	37
11.5	Atualização USB.....	37
11.6	Atualizar Firmware Online.....	38
11.7	Redefinição de fábrica.....	39
12	PERSONALIZAR CONFIGURAÇÕES	40
12.1	Interface do Usuário.....	40
12.2	Opções de Voz	41
12.3	Alarme	41
13	GERENCIAMENTO DE DADOS	43
14	INTERFONE.....	44
14.1.1	Configurações Locais	44
14.1.2	Opções de Áudio	45
14.1.3	Opções de Vídeo.....	45
14.1.4	Opções de Chamada	46
14.1.5	Lista de Contatos	47
14.1.6	Configurações de Atalho de Chamada	47
14.1.7	Configurações Avançadas	48
14.2	Configuração da campanha	49
14.3	Configurações ONVIF	49
15	CONTROLE DE ACESSO.....	51
15.1	Opções de Controle de Acesso.....	52
15.2	Configurações de Regra de Tempo	53
15.3	Feriados	54
15.4	Verificação Combinada.....	55
15.5	Configurações de Opções de Coação.....	56
16	GERENCIADOR USB	57
16.1	Baixar de USB.....	58
16.2	Enviar de USB.....	59

17	PESQUISA DE FREQUÊNCIA.....	59
18	AUTO TESTE	61
19	INFORMAÇÕES DO SISTEMA.....	62
20	INTERFACE WEB.....	63
21	PORTAS UTILIZADAS.....	65
22	COMO ADICIONAR O TERMINAL FACIAL NO WEG BIOGUARD	66

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.

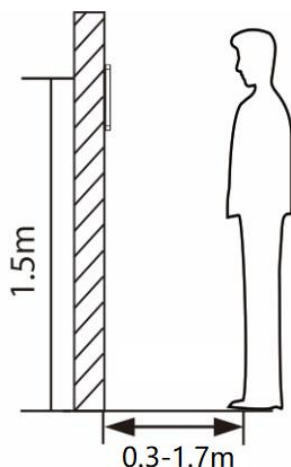
- Certifique-se de conectar os fios seguindo a polaridade positiva e negativa mostradas na placa de identificação do dispositivo.
- O serviço de garantia não cobre danos acidentais, danos causados por má operação, e danos causados por instalação ou reparo independente do produto pelo usuário.

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 Posicionamento do Dedo

Dedos recomendados: O indicador, médio ou anelar e evite usar o polegar ou dedos mindinhos, pois são difíceis de pressionar com precisão no leitor de impressões digitais.



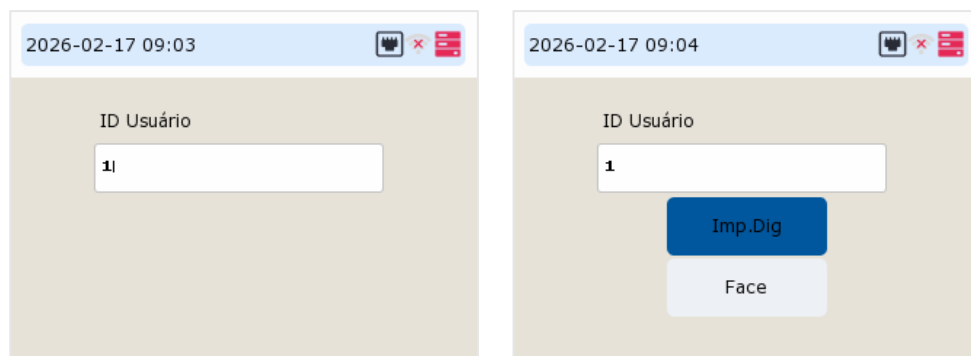
Nota: Por favor, utilize o método correto ao pressionar seus dedos no leitor de impressão digital para registro e identificação. Nossa empresa não se responsabilizará por problemas de reconhecimento que possam resultar do uso incorreto do produto. Reservamo-nos o direito de interpretação e modificação final a respeito deste ponto.

4.4 Reserva Interface

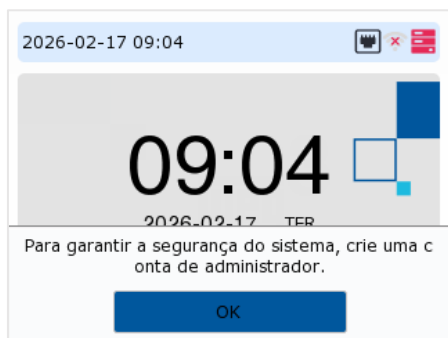
O dispositivo usa uma tela colorida de 2,4 polegadas, na qual todas as operações são realizadas através do teclado. Após conectar a fonte de alimentação, a seguinte interface de espera é exibida:



- Digite qualquer número para acessar a interface de entrada do ID do usuário.



- Quando não houver um Super Administrador definido no dispositivo, pressione **M/OK** para ir ao menu.



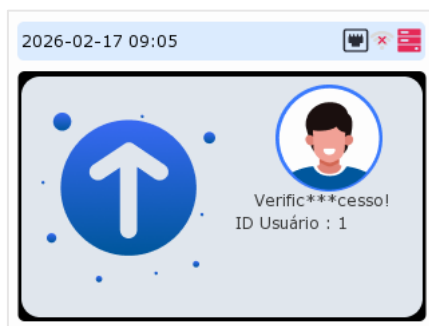
Observação: Para a segurança do dispositivo, recomenda-se registrar um Super Administrador na primeira vez que o dispositivo for usado.

4.5 Modo de Verificação

4.5.1 Verificação Facial

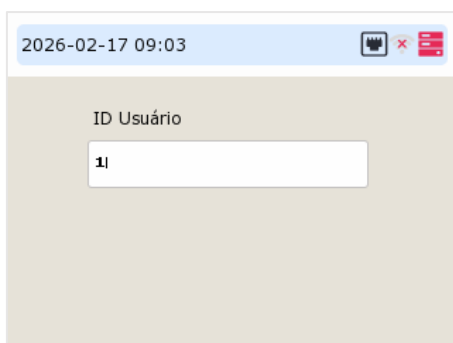
Verificação Facial 1:N

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.

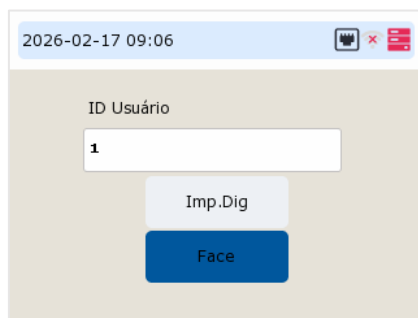


Verificação Facial 1:1

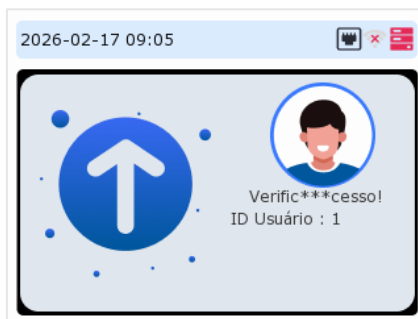
Neste modo de verificação, o dispositivo compara o rosto capturado pela câmera com o modelo facial relacionado ao ID do usuário inserido. Digite o ID do usuário e pressione **M/OK** para a verificação 1:1 do modo de verificação facial.



Se o usuário tiver registrado senha e digital além do rosto, e o método de verificação está definido como Senha/Impressão digital/Face, aparecerá a seguinte tela. Selecione **Face** para entrar no modo de verificação facial.



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



4.5.2 Verificação de Impressão digital

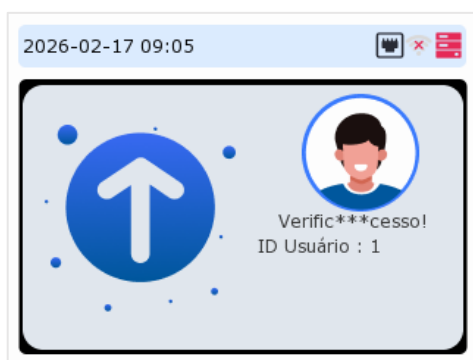
➤ Modo de Verificação por Impressão Digital 1:N

O dispositivo compara a impressão digital atual com os dados de impressão digital disponíveis armazenados em seu banco de dados.

O modo de autenticação por impressão digital é ativado quando um usuário coloca o dedo no leitor de impressão digital.

Por favor, siga a maneira recomendada de colocar o dedo no sensor. Para detalhes, consulte a seção Posicionamento do Dedo.

Verificação bem-sucedida:



Verificação falhou:

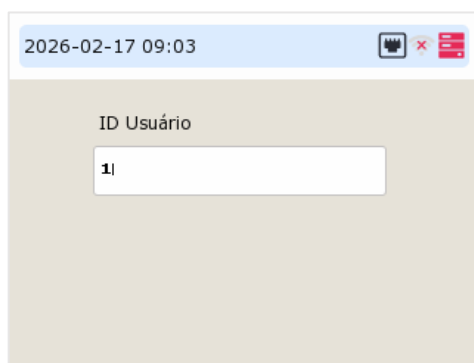


➤ Modo de Verificação de Impressão Digital 1:1

O dispositivo compara a impressão digital atual com as impressões digitais vinculadas ao ID do usuário inserido por meio do teclado virtual.

Caso os usuários não consigam acessar usando o método de autenticação 1:N, eles podem tentar verificar sua identidade usando o modo de verificação 1:1.

Digite o ID do usuário e pressione **M/OK** para iniciar o modo de verificação de impressão digital 1:1.

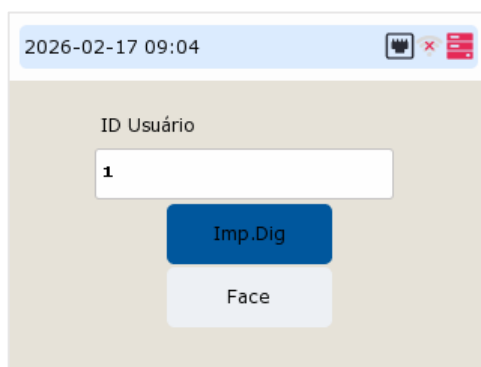


2026-02-17 09:03

ID Usuário

1

Se um funcionário registrar uma senha e face além da impressão digital, a seguinte tela aparecerá. Selecione **Impressão digital** para entrar no modo de verificação de impressão digital.



2026-02-17 09:04

ID Usuário

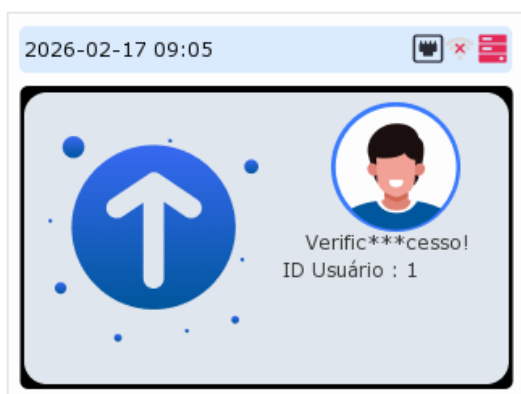
1

Imp.Dig

Face

Pressione a impressão digital para verificar.

Verificação bem-sucedida:



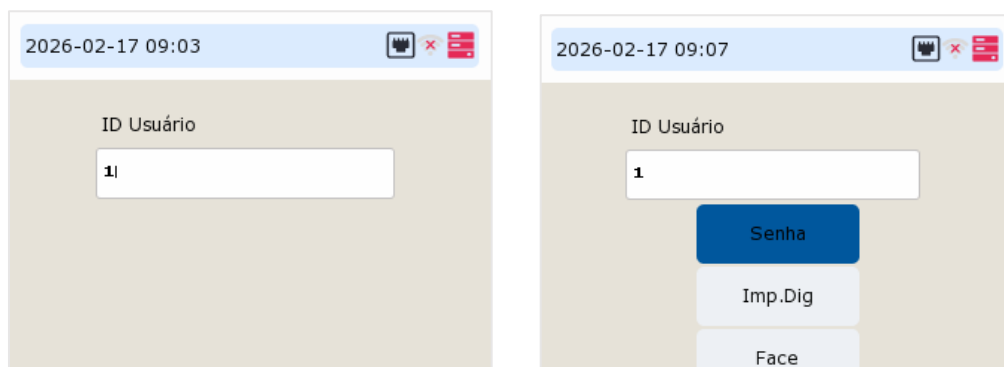
Verificação falhou:



4.5.3 Verificação de Senha

O dispositivo compara a senha inserida com a senha registrada e ID do usuário.

Digite o ID do usuário e pressione **M/OK** para entrar no modo de verificação de senha 1:1. Em seguida, insira o ID do usuário e pressione **M/OK**.



2026-02-17 09:03

ID Usuário

1

2026-02-17 09:07

ID Usuário

1

Senha

Imp.Dig

Face

Se um funcionário registrar uma digital e rosto além da senha, a seguinte tela aparecerá.



2026-02-17 09:07

ID Usuário : 1

Verificação : Senha

2026-02-17 09:05

Verific**cesso!

ID Usuário : 1

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, conforme listado abaixo:

Definição Combinada de Símbolo de Verificação

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.

Modo verific.	
☐	Somente ID Usr.
☒	Senha
☐	ID Usuário+Imp.Dig
☐	Imp.Dig+Senha
☐	ID Usuário+Imp.Dig+Senha

Procedimento de configuração do Modo de Verificação Combinada:

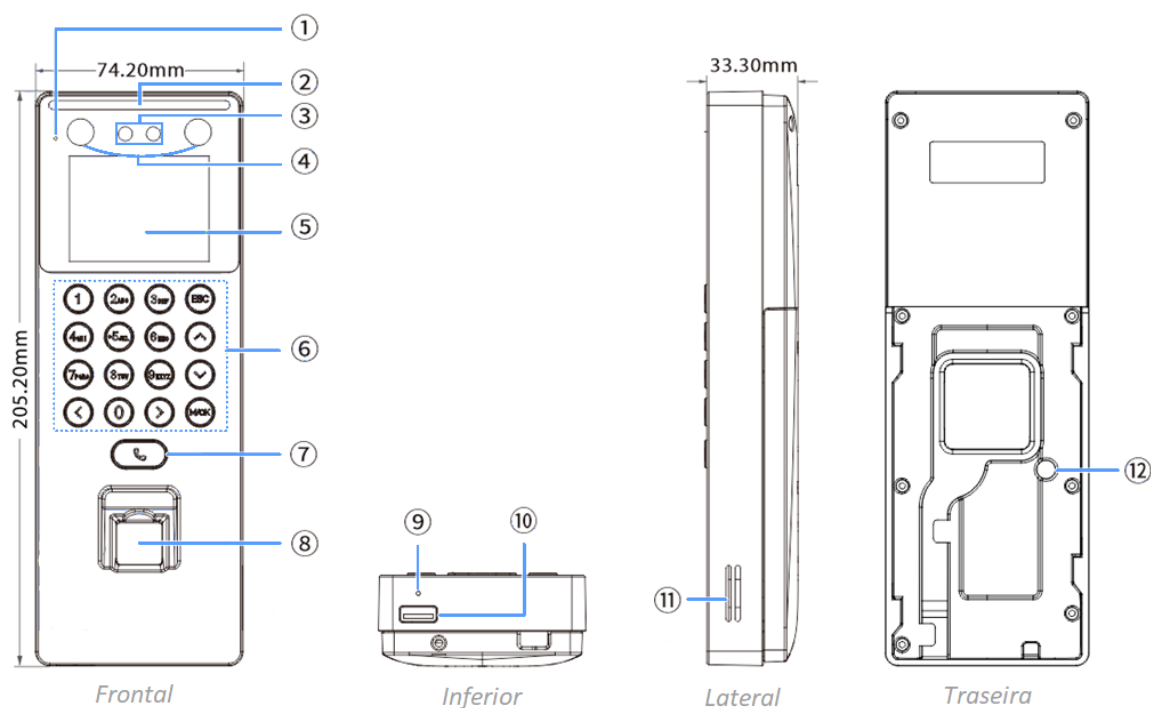
- A verificação combinada exige que o pessoal registre todos os diferentes métodos de verificação. Caso contrário, os funcionários não conseguirão verificar com sucesso o processo de verificação combinada.
- Por exemplo, se um funcionário registrou apenas os dados da senha, mas o modo de verificação do dispositivo está definido como "Imp.Dig+Senha", 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 a impressão digital quanto a Senha) previamente armazenado para aquele ID de Pessoal no Dispositivo.
- Mas, como o funcionário registrou apenas sua senha e não sua impressão digital, o processo de verificação não será bem-sucedido, e o dispositivo exibirá "Verificação Falhou."

5 Visão geral

5.1 Aparência



Não.	Descrição
1	Microfone
2	Led suplementar (disponível em modelos específicos)
3	Câmera de reconhecimento facial
4	Led infravermelho
5	Tela colorida de 2,4 polegadas
6	Teclado
7	Botão da campainha
8	Sensor de digital
9	Reset
10	USB
11	Alto-falante
12	Tamper

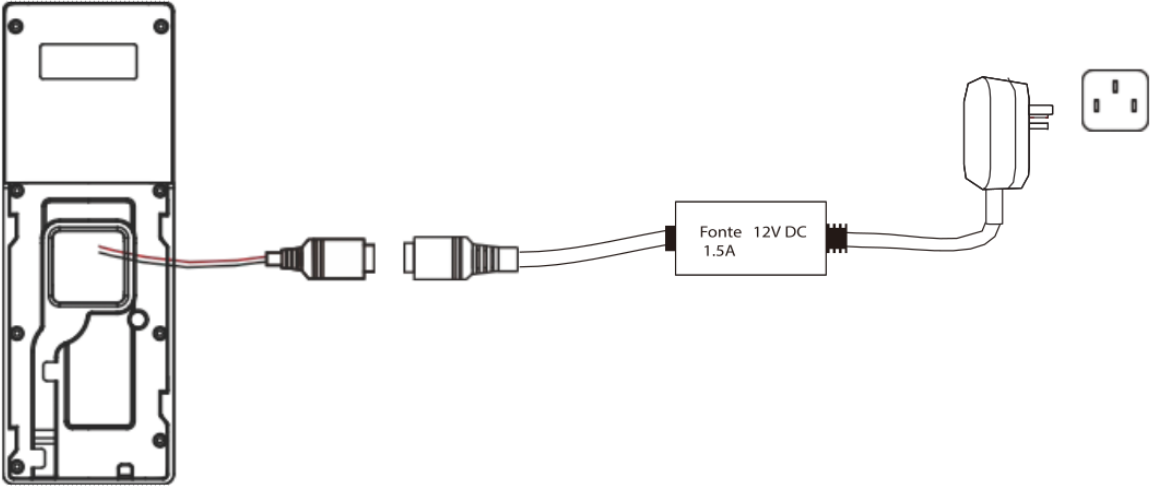
5.2 Descrição do Terminal e Cabeamento

5.2.1 Descrição do Terminal

Interface	Descrição	
	NC	Fechadura
	COM	
	NO	
	SEN	Sensor de porta e Botão de Saída
	GND	
	BUT	
	Entrada de energia	
	Interface de Rede	

5.3 Descrição da fiação

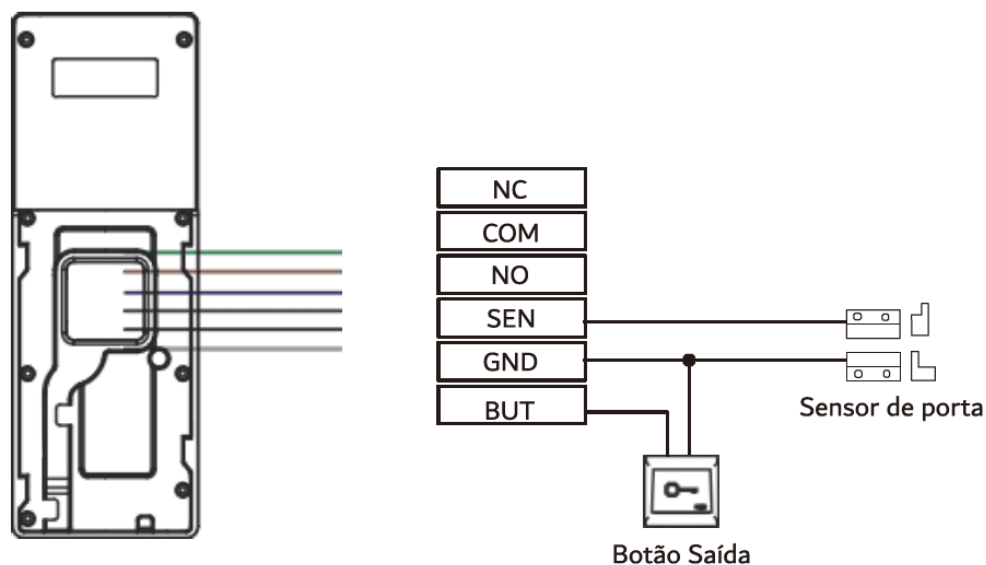
5.3.1 Conexão de Energia



Fonte de alimentação recomendada

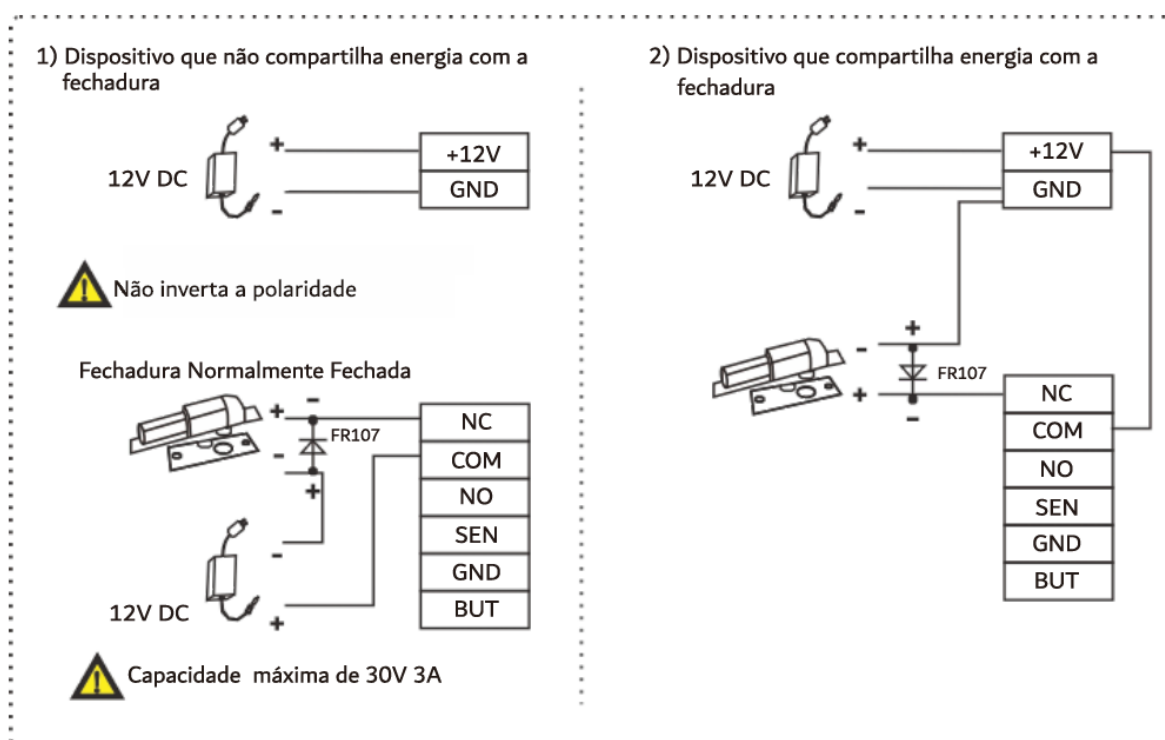
- Classificação de 12V e 1,5 A.
- Para compartilhar a energia do dispositivo com outros dispositivos, use uma fonte de alimentação com classificações de corrente mais altas.

5.3.2 Sensor de Porta & Conexão do Botão de Saída



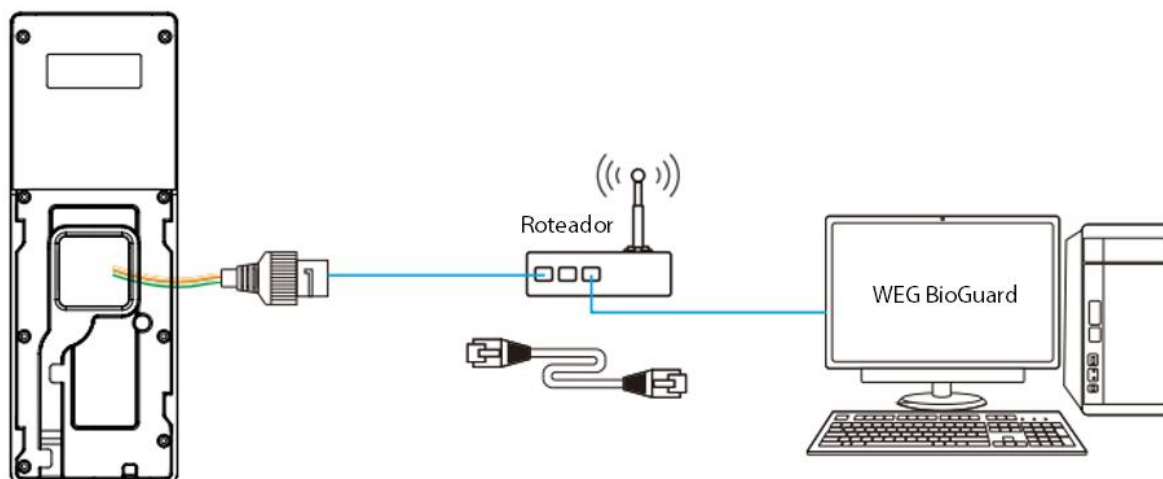
5.3.3 Travar Conexão do Relé

O sistema suporta tanto fechadura normalmente aberta quanto fechadura normalmente fechada. A fechadura NO (normalmente aberta quando energizada) é conectada aos terminais 'NO' e 'COM', e a fechadura NC (normalmente fechada quando energizada) é conectada aos terminais 'NC' e 'COM'. A alimentação pode ser compartilhada com a fechadura ou pode ser usada separadamente para a fechadura, como mostrado no exemplo com a fechadura NC a seguir:



5.3.4 Conexão Ethernet

Conecte o dispositivo ao software de WEG BioGuard usando um cabo Ethernet. Um exemplo é mostrado abaixo:



Entre em [COM.] > [TCP/IP] para definir os parâmetros relevantes da rede.



Note: Em LAN, os endereços IP do servidor (PC) e do dispositivo devem estar no mesmo segmento de rede quando o software realizar a conexão com o dispositivo.

6 Instalação

6.1 Ambiente de Instalação

Por favor, consulte as seguintes recomendações para instalação.



MANTER DISTÂNCIA



EVITAR A REFRAÇÃO
DO VIDRO



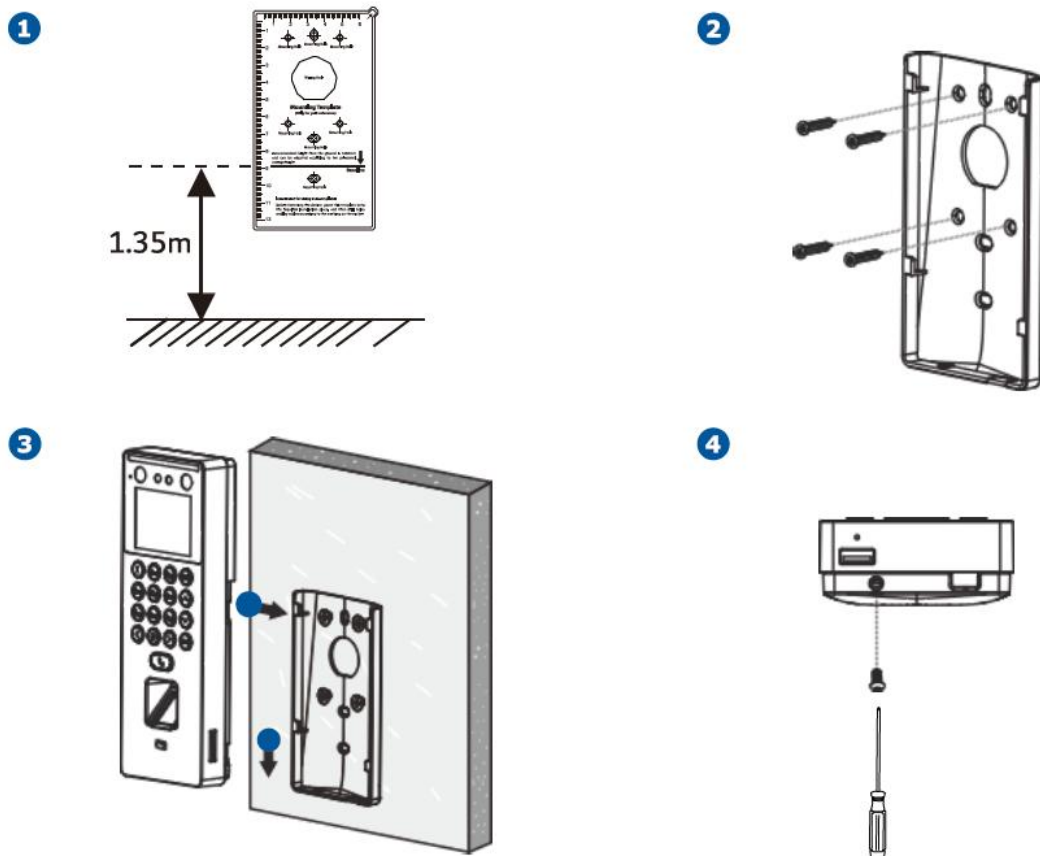
EVITE A EXPOSIÇÃO DIRETA
À LUZ SOLAR



EVITE O USO DE
QUALQUER FONTE
DE CALOR PERTO
DO DISPOSITIVO

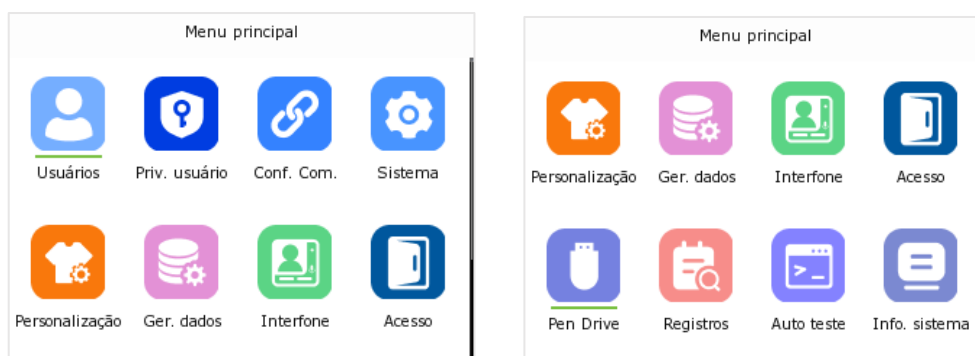
6.2 Instalação do Dispositivo

1. Cole o adesivo do gabarito de montagem na parede e faça os furos.
2. Fixe a placa traseira na parede usando os parafusos.
3. Fixe o dispositivo na placa traseira.
4. Fixe o dispositivo na placa traseira com um parafuso de segurança.



7 Menu Principal

Pressione **M/OK** na interface inicial para acessar o menu principal, conforme mostrado abaixo:



Descrição da Função

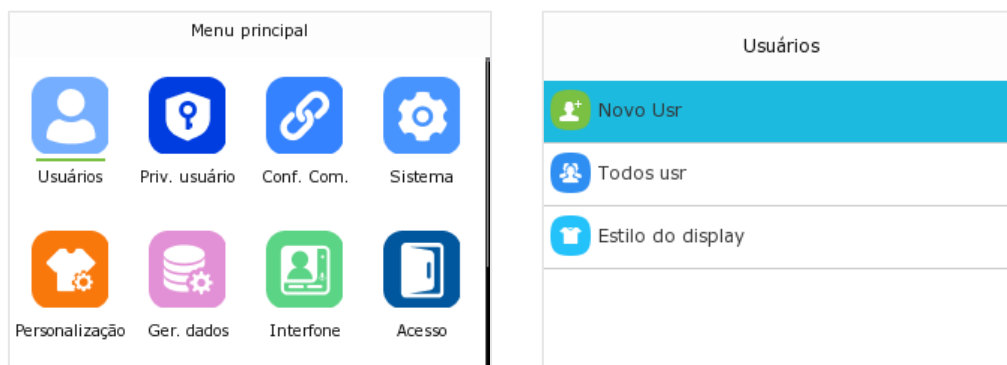
Menu	Descrição
Usuários	Para adicionar, editar, visualizar e excluir informações de um usuário.
Priv. usuário	Para definir o escopo de permissão da função personalizada e do cadastrador para os usuários, por exemplo, os direitos operacionais do sistema.

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.

8 Gerenciamento de Usuários

8.1 Novo Cadastro de Usuário

Quando o dispositivo estiver na interface inicial, pressione **M/OK** e toque em **[UsuarioAdm] > [Novo Usr]**.



8.1.1 Registre um ID de usuário e Nome

Entre com o **ID do Usuário** e **Nome**.

Novo Usr	
ID Usuário	2
Nome	
Tipo de Usuário	Comum
Imp. Dig.	0
Face	

Nota:

1. Um nome pode ter no máximo 36 caracteres.
2. O ID do usuário pode conter de 1 a 14 dígitos por padrão, suporta ambos os caracteres numéricos e alfabéticos.
3. Durante o registro inicial, você pode modificar seu ID, mas não após o registro.
4. Se a mensagem "**Duplicado**" aparecer, você deve escolher um ID de usuário diferente porque o que você inseriu já existe.

8.1.2 Função do Usuário

Na interface **Novo Usr**, selecionar **Tipo de Usuário** para definir o papel do usuário como **Usuário Comum** ou **Super Admin**.

- **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.

Tipo de Usuário	
☒	Comum
☐	Super administrador

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.

8.1.3 Registrar Impressão Digital

Selecione **Impressão digital** na interface **Novo Usr** para entrar na página de registro de impressão digital.

- Selecione o dedo a ser cadastrado.
- Pressione o mesmo dedo no leitor de impressão digital três vezes.
- Verde indica que a impressão digital foi cadastrada com sucesso.



8.1.4 Registrar Face

Selecione **Face** na interface **Novo Usr** 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:



8.1.5 Senha

Selecione **Senha** na interface **Novo Usr** para inserir a página de registro de senha.

- Na interface de Senha, digite a senha exigida, digite novamente para confirmá-la e pressione **OK/M**.
- Se a senha redigitada for diferente da senha digitada inicialmente, então o dispositivo exibe a mensagem como "**Senha não confere**", onde o usuário precisa confirmar a senha novamente.
- A senha pode conter de 6 a 8 dígitos por padrão.

8.1.6 Foto do usuário

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



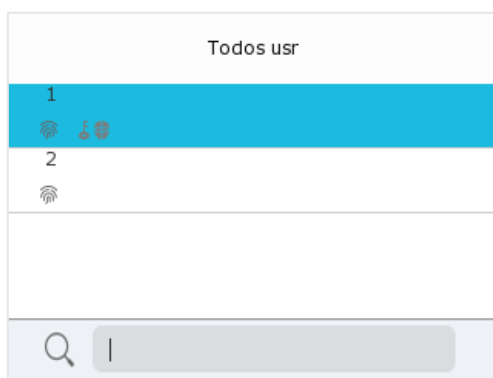
- Toque **Foto usuário**, a câmera do dispositivo será aberta, então pressione **OK/M** para tirar uma foto. A foto tirada é exibida no canto superior esquerdo da tela.

Observação: Durante o registro de um modelo facial, o sistema captura automaticamente uma foto como foto de perfil do usuário. Se você não registrar uma foto de perfil, o sistema define automaticamente a foto tirada durante o registro como foto padrão.

8.2 Todos os Usuários

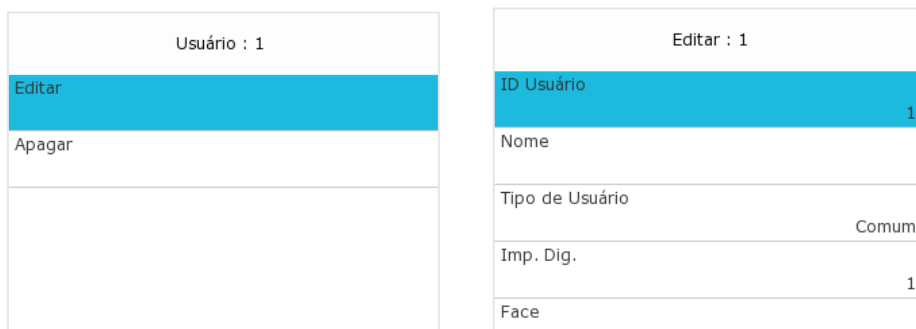
Quando o dispositivo estiver na interface inicial, pressione **M/OK** e digite [**UsuarioAdm**] > [**Todos usr**].

- Na interface **Todos Usr**, 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.



8.2.1 Editar Usuário

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



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. O processo detalhado é descrito em "Novo Cadastro de Usuário".

8.2.2 Excluir Usuário

Na interface **Todos Usr**, 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/Confirmar** para confirmar a exclusão.

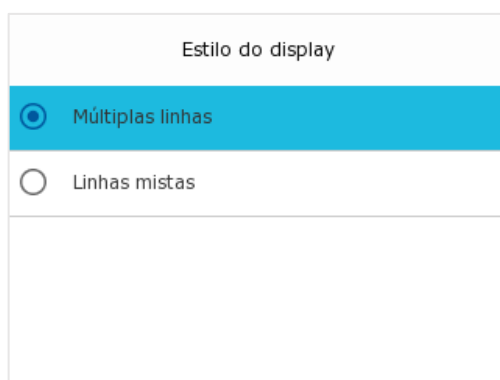
Operações de Exclusão:

- **Apg. Usuário:** Exclui todas as informações do usuário (exclui o Usuário selecionado como um todo) do Dispositivo.
- **Apg. Imp. Dig.:** Exclui a impressão digital do usuário.



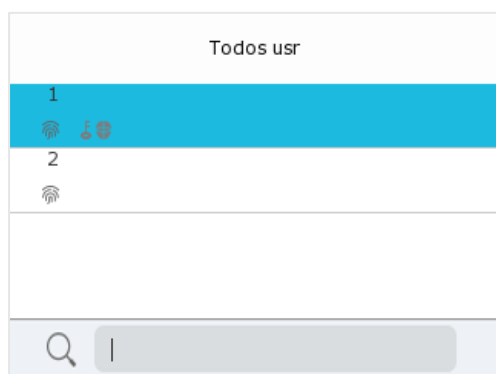
8.3 Estilo do display

Quando o dispositivo estiver na interface inicial, pressione **M/OK** e selecione **[Usuário Adm] > [Estilo do display]**.

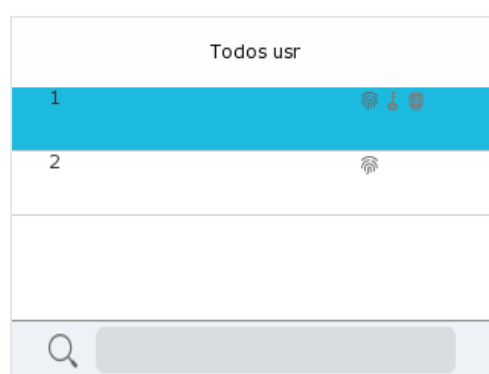


Todos os estilos de exibição são mostrados abaixo:

Múltiplas linhas:



Linhas mistas:



9 Privilégios do Usuário

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

- Quando o dispositivo estiver na interface inicial, pressione **M/OK** e toque em [**Priv. usuário**] para configurar as permissões definidas pelo usuário.
- O escopo de permissão da função personalizada pode ser configurado em 3 funções, ou seja, o escopo de operação personalizada das funções de menu do usuário.

Priv. usuário	
	Usuário personalizado 1
	Usuário personalizado 2
	Usuário personalizado 3
	Registrador

- Na interface **Usuário personalizado**, alternar **Habilitar atribuir permissões** para habilitar ou desabilitar o papel definido pelo usuário.

Usuário personalizado 1	
Habilitar atribuir permissões ☐	
Nome	Usuário personalizado 1
Atribuir permissões	

- Então, selecionando **Atribuir permissões**, selecione os privilégios necessários para a nova função, e então pressione a tecla **M/OK**.
- Primeiro toque nome das funções principais, então pressione **M/OK** e selecione os submenus necessários na lista.

Usuário personalizado 1	
☒	Usuários
☒	Conf. Com.
☒	Sistema
☐	Personalização
☐	Ger. dados

Usuário personalizado 1	
☐	Personalização
☐	Ger. dados
☒	Interfone
☒	Acesso
☐	Pen Drive

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.

10 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.

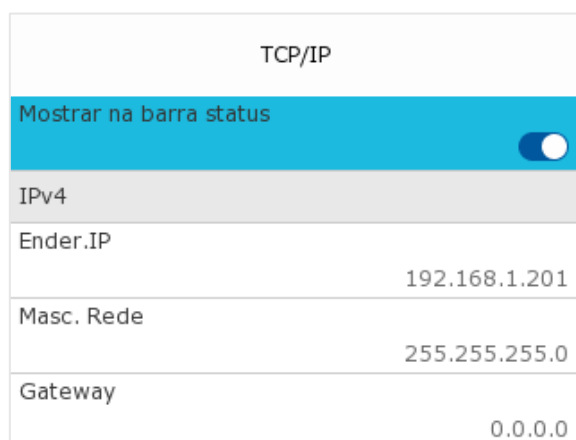
Quando o dispositivo estiver na interface inicial, pressione **M/OK** e selecione **[Conf. Com.]**



10.1 Ethernet

Quando o dispositivo precisa se comunicar com um PC via a 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.

10.2 Configuração da comunicação

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

Conf. Comunic.

Senha com. *****

ID Equip. 1

Porta de comu.TCP 4370

HTTPS ☐

Descrição da Função

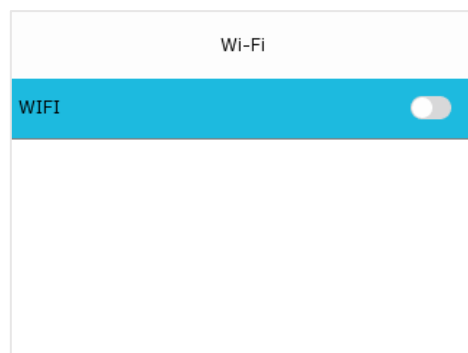
Nome da Função	Descrição
ID Equip.	É o número de identificação do dispositivo que varia entre 1 e 254.
Porta de comu. TCP	O valor padrão de fábrica é 4370. Ajuste o valor conforme necessário.
HTTPS	Para aumentar a segurança de software, os usuários podem habilitar o protocolo HTTPS para criar uma transmissão 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.

10.3 Configurações de Wi-Fi

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

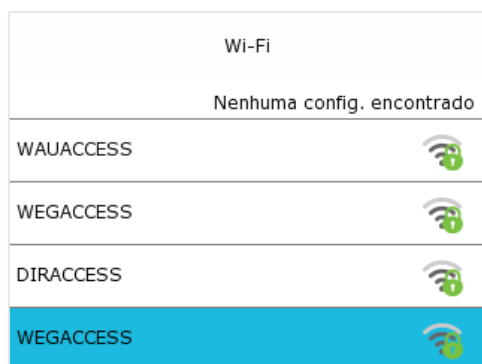
O módulo Wi-Fi permite a transmissão de dados via Wi-Fi (Wireless Fidelity) e estabelece um ambiente de rede sem fio. O Wi-Fi está ativado por padrão no dispositivo. Se você não precisar usar a rede Wi-Fi, pode alternar o Wi-Fi para desativar o botão.

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

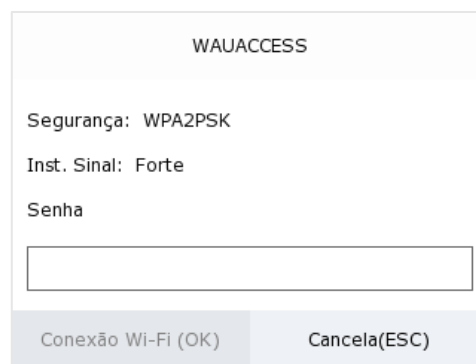


➤ Pesquisando a rede Wi-Fi

- Wi-Fi está ativado no dispositivo por padrão. Ative ou desative o  botão para ativar ou desativar Wi-Fi.
- Assim que o Wi-Fi estiver ligado, o dispositivo pesquisará as redes Wi-Fi disponíveis dentro do alcance da rede.
- Toque no nome da rede Wi-Fi desejada na lista disponível e insira a senha correta na interface de senha, e então pressione **M/OK**.



Wi-Fi habilitado: toque na rede desejada na lista de redes Wi-Fi



Toque no campo de senha para entrar com a senha e pressione **M/OK**.

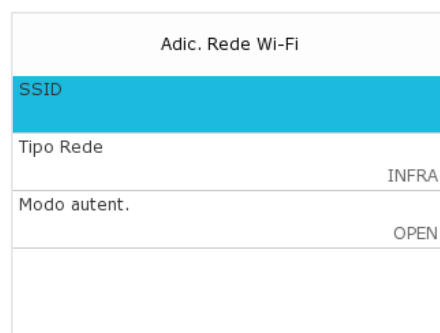
- Quando o Wi-Fi estiver conectado com sucesso, a interface inicial exibirá o logotipo do Wi-Fi .

➤ Adicionando rede Wi-Fi manualmente

A rede Wi-Fi também pode ser adicionada manualmente caso a rede Wi-Fi desejada não apareça na lista.



Toque em **Adic. Rede Wi-Fi** para adicionar manualmente a rede Wi-Fi.

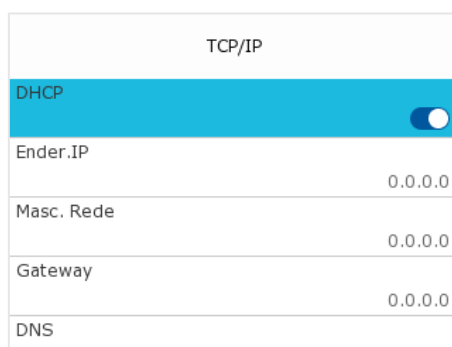


Nesta interface, entre com os parâmetros da rede Wi-Fi. (A rede adicionada precisa existir).

Observação: Após adicionar o Wi-Fi manualmente com sucesso, siga o mesmo processo para pesquisar o nome da rede Wi-Fi adicionada.

➤ Configurações Avançadas

Toque em **Avançado** para definir os parâmetros relevantes conforme necessário.



Descrição da Função

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.
Ender.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.
Masc. 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.

10.4 Configurações do Servidor em Nuvem

Selecione **Configurar server nuvem** na interface **Conf. Com** para conectar-se ao servidor ADMS.

Configurar server nuvem

Tipo de servidor	ADMS
Habilitar domínio	☐
End. Servidor	192.168.1.220
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.

10.5 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.

Diagnóstico de rede

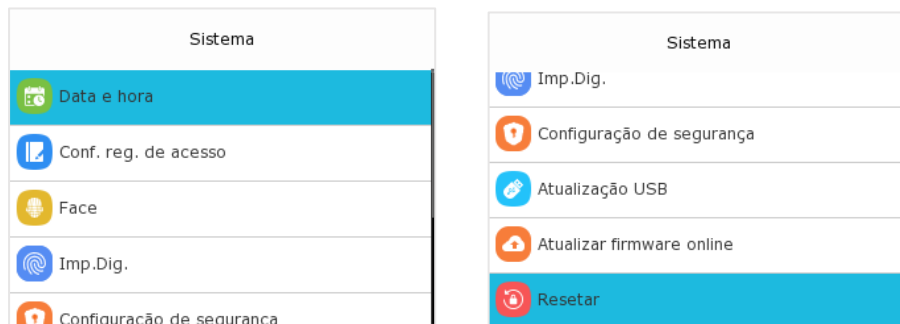
Diagnóstico de endereço IP	192.168.1.220
Iniciar diagnóstico	

11 Configurações do Sistema

Ajuda a definir os parâmetros do sistema relacionados para otimizar a acessibilidade do dispositivo.

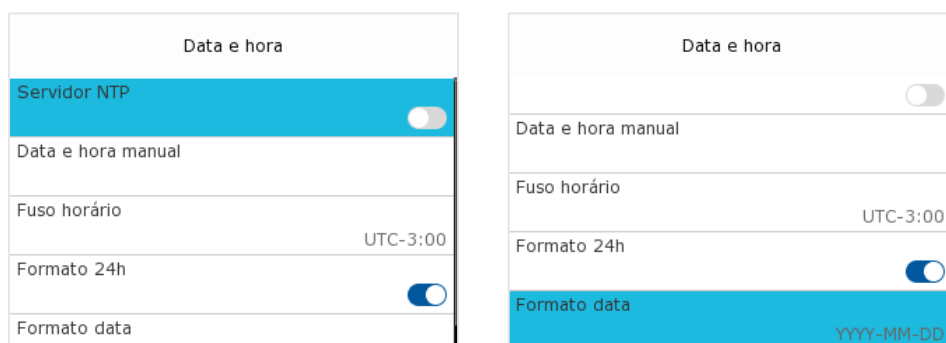
Quando o dispositivo estiver na interface inicial, pressione **M/OK** e selecione **Sistema**.

Terminal de Controle de Acesso:



11.1 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.
- Ao restaurar as configurações de fábrica, o formato de hora (24 horas) e data (AAAA-MM-DD) podem ser restaurados, mas a data e hora do dispositivo não podem ser restauradas.

Observação: Por exemplo, se um usuário definir a hora do dispositivo de 18:35 do dia 15 de março de 2020 para 18:30 do dia 1º de janeiro de 2021. Após a restauração das configurações de fábrica, a hora do dispositivo permanecerá em 18:30 do dia 1º de janeiro de 2021.

11.2 Configurações de Logs de Acesso/Frequência

Selecione a interface **Conf. reg. de acesso**.

Terminal de Controle de Acesso:

Conf. reg. de acesso	
Modo câmera	Sem Foto
Mostra foto usuário	☐
ID usuário alfanumérico	☐
Config. reg. excessão	99
Ciclo apg. reg. acesso	

Descrição da Função do Terminal de Controle de Acesso:

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.

11.3 Parâmetros de Face

Selecione a interface **Face** para acessar as configurações de parâmetros do modelo de face.

Face	
Limiar 1:N	40
Limiar 1:1	30
Limiar de cadastramento de face	75
Qualidade de imagem	40
Distância de reconhecimento facial	

Face	
Sensibilidade para acionamento de luz de LED	80
Detecção de Face viva	☒
Limiar de detecção de Face viva	70
Antifalsificação por Infravermelho	☒
Limiar de comparação de corpo vivo	

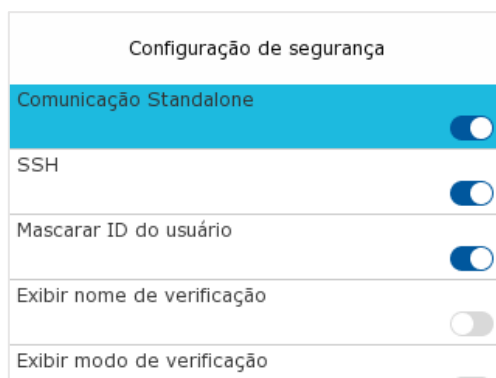
Face	
	30
Área de exposição da face	☐
WDR	☐
Modo anti-pisca	Desabilitar
Algoritmo Face	

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 10. 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 10. 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.
Deteção 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 deteção 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.

11.4 Configurações de Segurança

Selecione **Configuração de Segurança** na interface **Sistema** para acessar as configurações de segurança.



Descrição da Função

Nome da Função	Descrição
Comunicação Standalone	Permite utilização do dispositivo sem necessidade de conexão com o servidor.
SSH	SSH é usado para acessar o background do dispositivo para manutenção.
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 cadastramento facial após uma atualização de algoritmo.

11.5 Atualização USB

O programa de firmware do dispositivo pode ser atualizado com o arquivo de atualização em um drive USB. Antes de realizar esta operação, certifique-se de que o drive USB contenha o arquivo de atualização correto e esteja devidamente inserido no dispositivo.

Se nenhum disco USB estiver inserido, o sistema exibirá a seguinte mensagem após você tocar em Atualização USB na interface do Sistema.

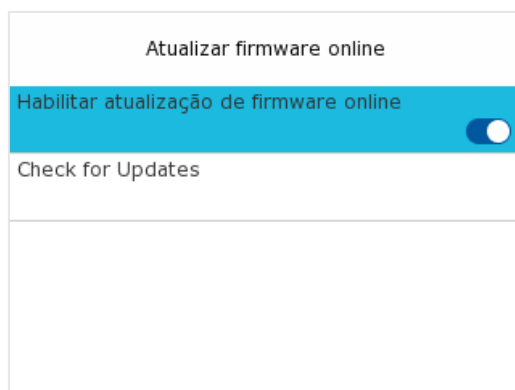
Selecione **Atualização USB** na interface de **Sistema**.



 **Nota:** Se o arquivo de atualização for necessário, entre em contato com nosso suporte técnico. A atualização de firmware não é recomendada em circunstâncias normais.

11.6 Atualizar Firmware Online

Selecione **Atualizar Firmware Online** na interface de **Sistema**.



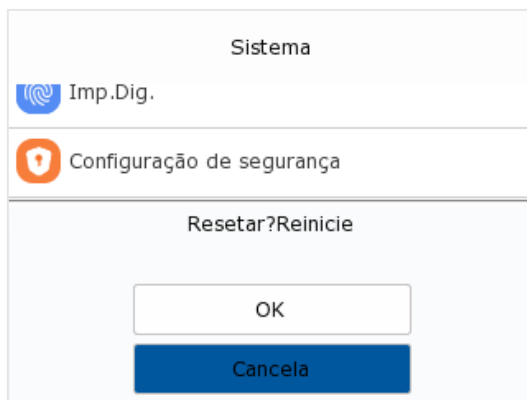
A função de Atualização de Firmware Online está ativada por padrão. Toque **Verificar atualizações** pode apresentar os 3 cenários a seguir:

- Se a consulta falhar, a interface exibirá a mensagem "Falha na consulta".
- Se a versão de firmware do dispositivo for a mais recente, será exibida uma mensagem indicando que a versão de firmware atual já é a mais recente.
- Se a versão de firmware do dispositivo não for a mais recente, o número da versão e o registro de alterações da versão mais recente serão exibidos. Os usuários podem escolher se desejam atualizar para a versão mais recente do firmware.

11.7 Redefinição de fábrica

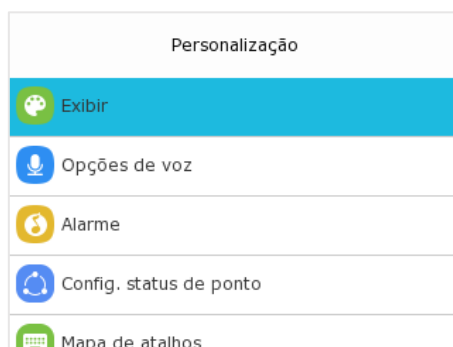
A função de redefinição de fábrica restaura as configurações do dispositivo, como configurações de comunicação e configurações do sistema, para as configurações de fábrica padrão (esta função não limpa os dados do usuário registrado).

Selecione **Resetar** na interface de **Sistema** e, em seguida, toque em **OK** para restaurar as configurações de fábrica padrão.



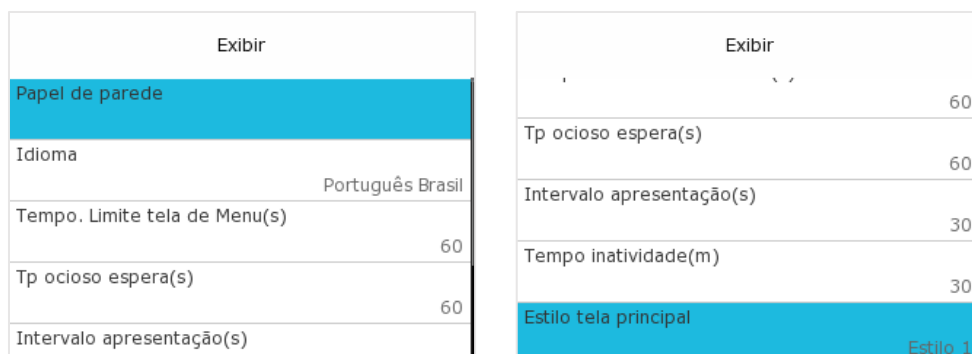
12 Personalizar Configurações

Quando o dispositivo estiver na interface inicial, pressione **M/OK** e selecione **Personalização** para personalizar as configurações da interface, voz e alarme.



12.1 Interface do Usuário

Selecione **Estilo tela principal** na interface **Personalização > Exibir** para personalizar o estilo de exibição da interface principal.



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.
Tp 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.

12.2 Opções de Voz

Selecione **Opções de Voz** na interface **Personalização** para configurar as definições de voz.

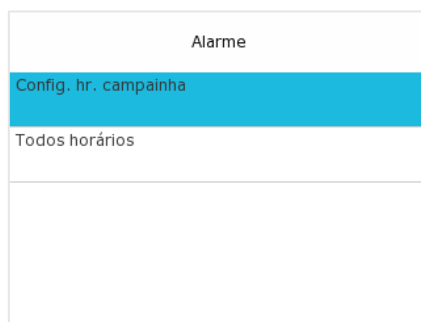


Descrição da Função

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.

12.3 Alarme

Selecione **Alarme** na interface **Personalização** para configurar as definições do sinal.



➤ **Conf. hr. campanha:**

Toque em **Conf. hr. campanha** na interface **Personalização > Alarme** para adicionar um novo horário do sinal.



Descrição da Função

Nome da Função	Descrição
Status campanha	Ativar ou desativar o status do alarme.
Horário Campanha	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 campanha(s)	Defina o tempo de repetição do alarme interno. Os valores válidos variam de 1 a 999 segundos.

➤ **Todos os horários do sinal:**

Assim que o alarme for agendado, na interface **Config. Hr. campanha**, toque em **Todos horários** para visualizar o alarme recém-agendado.

➤ **Editar o Alarme Agendado:**

Na interface **Todos horários**, toque no horário do alarme necessário e toque em **Editar** para editar a programação do sino selecionada. O método de edição é o mesmo que as operações de adicionar uma nova programação de alarme.

➤ **Apagar alarme agendado:**

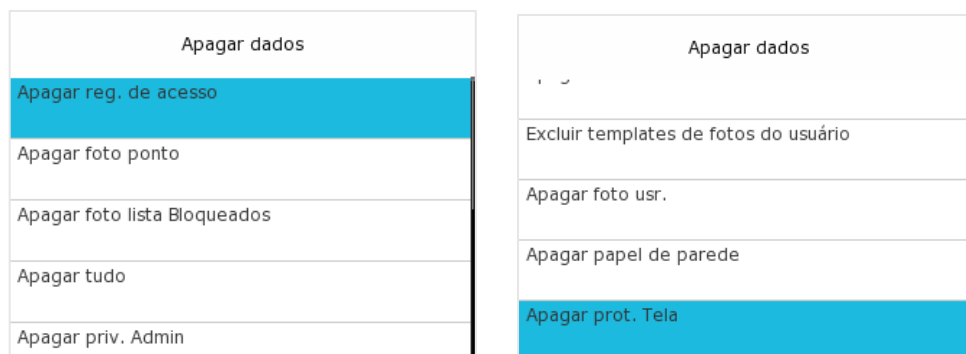
Na interface **Todos Horários**, toque no horário do alarme necessário, toque **Apaga**, e então toque em **Sim** para excluir o horário selecionado.

13 Gerenciamento de Dados

Quando o dispositivo estiver na interface inicial, pressione **M/OK** e selecione **Ger. dados** para gerenciar os dados relevantes no dispositivo.



Selecione **Apagar Dados** na interface **Gerenciamento de Dados** para excluir os dados necessários.



Descrição da Função

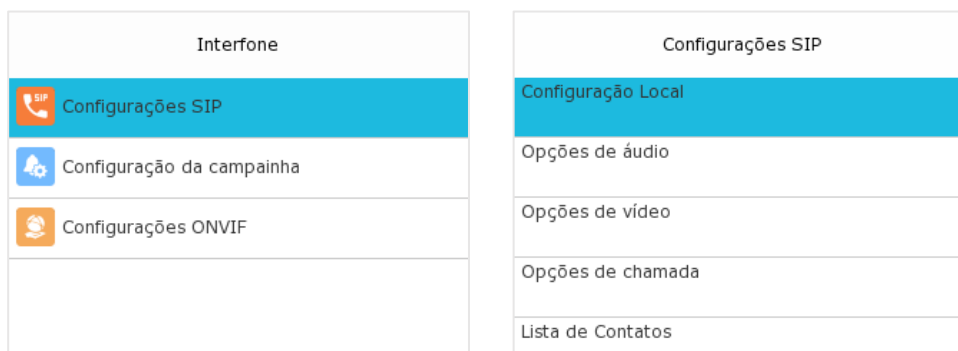
Nome da Função	Descrição
Apagar reg. de aceso	Para excluir os registros de acesso e dados de frequência condicionalmente.
Apagar foto ponto	Para excluir fotos de ponto de pessoal designado.
Apagar foto lista Bloqueados	Para excluir as fotos tiradas durante verificações mal sucedidas.
Apagar tudo	Para 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.

14 Interfone

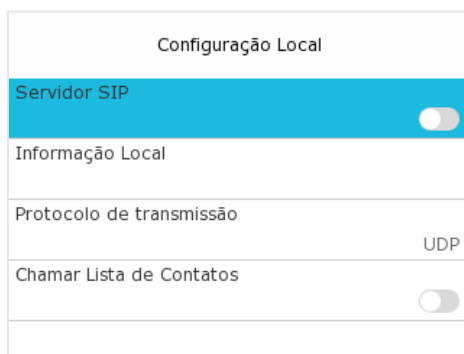
Quando o dispositivo estiver na interface inicial, pressione **M/OK** e selecione **Interfone** para definir os parâmetros relevantes do interfone, incluindo as configurações SIP, campanha e ONVIF.

Selecione **Configurações SIP** na interface **Interfone** para configurar as definições.



14.1.1 Configurações Locais

Selecione **Configurações Local** na interface **Configurações SIP**.



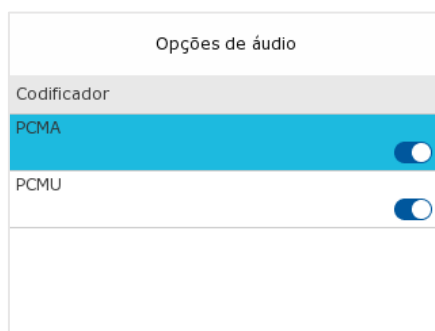
Descrição da Função

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.

14.1.2 Opções de Áudio

Selecione **Opções de áudio** na interface de **Configurações SIP**.



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

14.1.3 Opções de Vídeo

Selecione **Opções de vídeo** na interface de **Configurações SIP**.

Opções de vídeo	
Geral	
Resolução de vídeo	800x600
Taxa de bite rate	1024 kbps
Frames por segundo	25
Codificador	
H264	

Descrição da Função

Nome da Função	Descrição
Resolução de vídeo	Selecione a resolução de vídeo do interfone 1024 x 576 ou 600 x 1024. O dispositivo suporta apenas tela em paisagem. Sugere-se definir como 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 Hz por padrão e não suporta modificação.
Codificador	Ativar o codificador H264.

14.1.4 Opções de Chamada

Selecione **Opções de chamada** na interface **Configurações SIP**.

Opções de chamada	
Geral	
Atraso (s) de chamada	30
Atraso (s) para falar	60
Config. Vol. Chamada	70
Tipo de chamada	Voz+Vídeo

Descrição 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.

14.1.5 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.

Lista de Contatos

Adicionar

101192.168.1.101
102192.168.1.102
103

Q
|

Adicionar

Número do Quarto

Endereço de chamada

14.1.6 Configurações de Atalho de Chamada

Selecione **Configurações de atalho de chamada** na interface **Configurações SIP**.

Configurações de atalho de chamada

Central de gerenciamentoDesabilitar
Modo de ChamadaModo Padrão
ROOM1Desabilitar
ROOM2Desabilitar
ROOM3

Central de Gerenciamento: Selecione se deseja habilitar o Centro 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**.

Número : 102	
Ativar	☒
Nome	ROOM1
Número	102

14.1.7 Configurações Avançadas

Selecione **Configurações Avançadas** na interface **Configurações SIP**.

Configurações Avançadas	
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.

14.2 Configuração da campanha

Selecione **Configuração da campanha** na interface do **interfone** para configurar a campanha.



Descrição da Função:

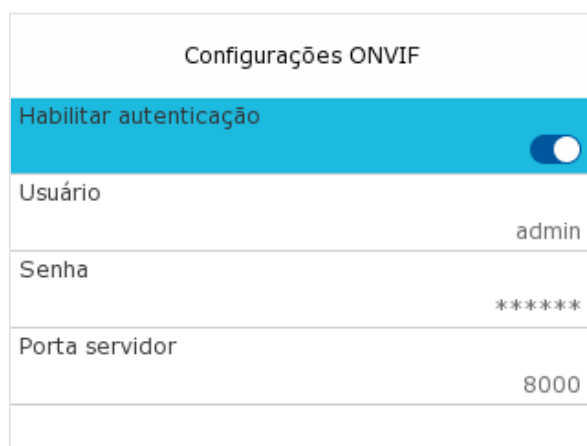
Nome da Função	Descrição
Configuração da campanha	Desabilitado: O botão da campanha está desativado. Apenas Vídeo porteiro: Quando o usuário pressiona o botão da campanha, apenas o dispositivo faz uma chamada.

14.3 Configurações ONVIF



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

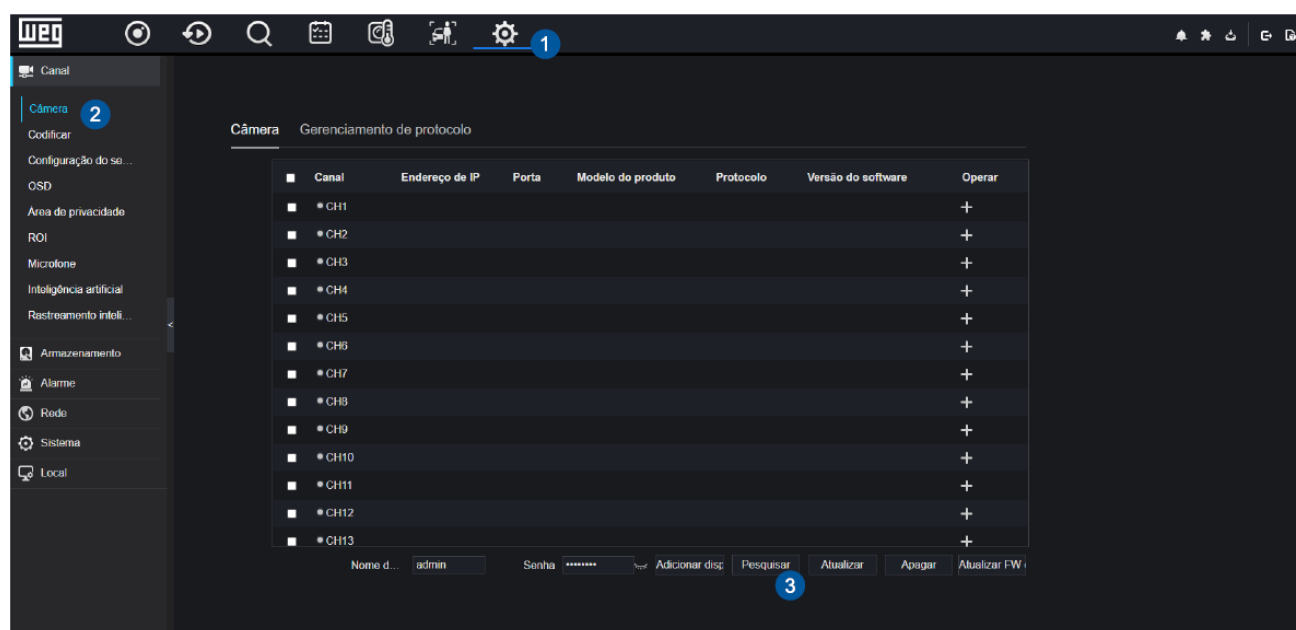
1. Configure o dispositivo para o mesmo segmento de rede que o NVR.
2. Selecione **Configurações ONVIF** na interface **Interfone**.



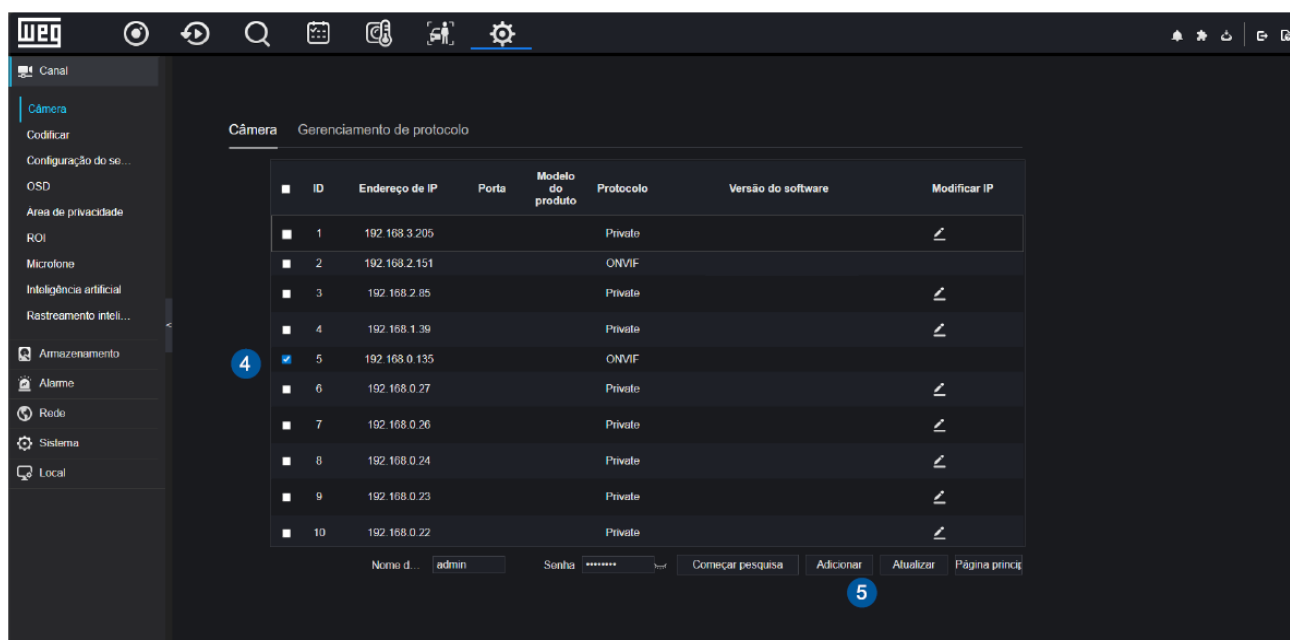
Nome da Função	Descrição
----------------	-----------

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.



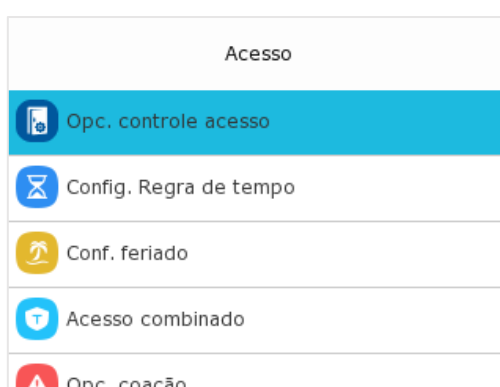
5. Após a adição bem sucedida você poderá visualizar a imagem do dispositivo no gravador.

Para mais detalhes, consulte o *Manual do Usuário do NVR*.

15 Controle de Acesso

Quando o dispositivo estiver na interface inicial, pressione **M/OK** e 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.

Terminal de 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.

15.1 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.

Opc. controle acesso	
Modo controle de portão/catraca	☒
Tempo do Relé	5
Atraso do Sensor(s)	15
Tipo de sensor	Nenhum
Modo verific.	

Opc. controle acesso	
Equipamento mestre	Nenhum
Dispositivo Auxiliar	Entrada
Alarme	Saída
Reset Config. Acesso	☒

Descrição da Função do Terminal de Controle de Acesso:

Nome da 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/Imp.Dig./Face, Somente ID Usr., Senha, Somente Imp.Dig., Senha+Imp.Dig., Senha ou Imp.Dig., Somente face, Face+Senha e Face+Imp.Dig.
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.

15.2 Configurações 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).

The screenshot shows a configuration window with a title bar containing "[2/50]". Below the title bar is a list of days: Domingo, Segunda, Terça, and Quarta. Each day has a corresponding time range "[00:00 23:59]" displayed next to it. The Domingo row is highlighted in blue. At the bottom of the window is a search bar with a magnifying glass icon and a text input field containing the letter "I".

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

The screenshot shows a time selection interface titled "Faixa horária 1". It displays the time "00:00 23:59". Below the time, there are four input fields for HH, MM, HH, and MM. The first HH field is highlighted with a blue border and contains the value "00". Above each input field is a "+" sign and below each is a "-" sign. At the bottom of the interface are two buttons: "Confirma(OK)" and "Cancela(ESC)".

Especifique o horário de início e o horário de término, e então pressione **M/OK**.

Nota:

1. A porta fica inacessível o dia todo quando o Horário de Término ocorre antes do Horário de Início (como **23:57 às 23:56**).
2. 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**).
3. 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**).
4. O fuso horário padrão 1 indica que a porta fica aberta o dia todo.

15.3 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. feriado** 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**. Pressione **OK** para confirmar a exclusão. Após a exclusão, este feriado não será exibido na interface **Todos feriados**.

15.4 Verificação Combinada

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	00 00 00 00 00
2	00 00 00 00 00
3	00 00 00 00 00
4	

🔍 |

Na interface de verificação combinada, toque na combinação de desbloqueio da porta a ser definida, e pressione a tecla **para cima** e **para baixo** para inserir o número da combinação, e então pressione **M/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.

15.5 Configurações de Opções de Coação

Uma vez que um usuário ativa a função de verificação de coerção com um(ns) método(s) de autenticação específico(s), e quando ele/ela estiver sob coação e se autenticar usando a verificação de coerção, 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.

Opc. coação	
Senha de alarme	☐
1:1 Gatilho	☐
1:N Gatilho	☐
Atraso alarme(s)	10
Senha de coação	

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.

16 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.

Pen Drive
 Baixar
 Enviar



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

16.1 Baixar de USB

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

Enviar
Proteção de tela
Papel de parede
Enviar dados usr.
Enviar foto

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	Para baixar todas as fotos não autorizadas do dispositivo para o disco USB.

bloqueados	
-------------------	--

16.2 Enviar de USB

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

Enviar
Proteção de tela
Papel de parede
Enviar dados usr.
Enviar foto

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.

17 Pesquisa de Frequência

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, pressione **M/OK** e selecione **Proc. registros** para pesquisar os logs de eventos necessários.

Registros

Reg. Acesso

Foto ponto

Foto lista Bloqueados

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 **Proc. registros**, selecionar **Registros ponto** para pesquisar o registro necessário.

ID Usuário

Introduza(consultar todos)

Confirma(OK)

Cancela(ESC)

1. Insira o ID do usuário a ser pesquisado e pressione **M/OK**. Se desejar pesquisar registros de todos os usuários, pressione **M/OK** sem inserir nenhum ID de usuário.

Faixa horária

☒ Hoje

☐ Ontem

☐ Esta semana

☐ Semana passada

☐ Este mês

2. Selecione o intervalo de tempo em que os registros precisam ser pesquisados.

Registros pessoais		
Data	ID Usuário	Tempo
02-17		Total registros:1
	1	09:10
Ant : Esquerda Prox : Direita Detalhes : OK		

3. Após a conclusão da busca por registros, toque no registro destacado para visualizar seus detalhes.

Registros pessoais	
ID Usuário	Tempo
1	02-17 09:10
Nome : Status : Entrada Modo verific. : Imp. Dig.	

4. A figura mostra os detalhes do registro selecionado.

18 Auto teste

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



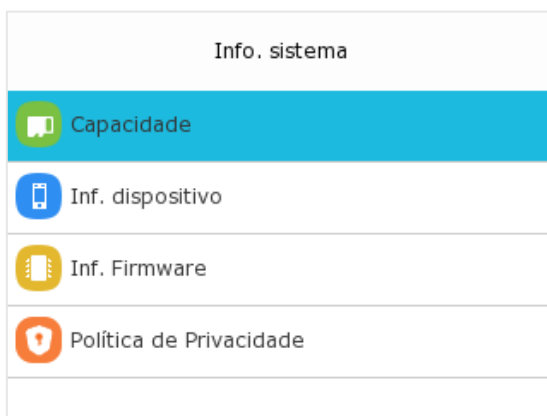
Descrição da Função

Nome da Função	Descrição
Testar todos	Para testar automaticamente se o Display, a Voz, o Microfone, Teclado, Impressão digital, 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 teclado	O terminal testa se todas as teclas do teclado funcionam normalmente. Pressione qualquer tecla na interface de Teste de Teclado para verificar se a tecla pressionada corresponde à tecla exibida na tela. As teclas são exibidas em cinza escuro antes e mudam de cor após pressionadas. Pressione ESC para sair do teste.
Teste do Sensor de Impressão Digital	Para testar o sensor de impressão digital, pressione um dedo no scanner para verificar se a imagem da impressão digital adquirida está nítida. Ao pressionar um dedo no scanner, a imagem da impressão digital será exibida na tela.

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. Pressione M/OK para começar a contar e pressione novamente para parar de contar.

19 Informações 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

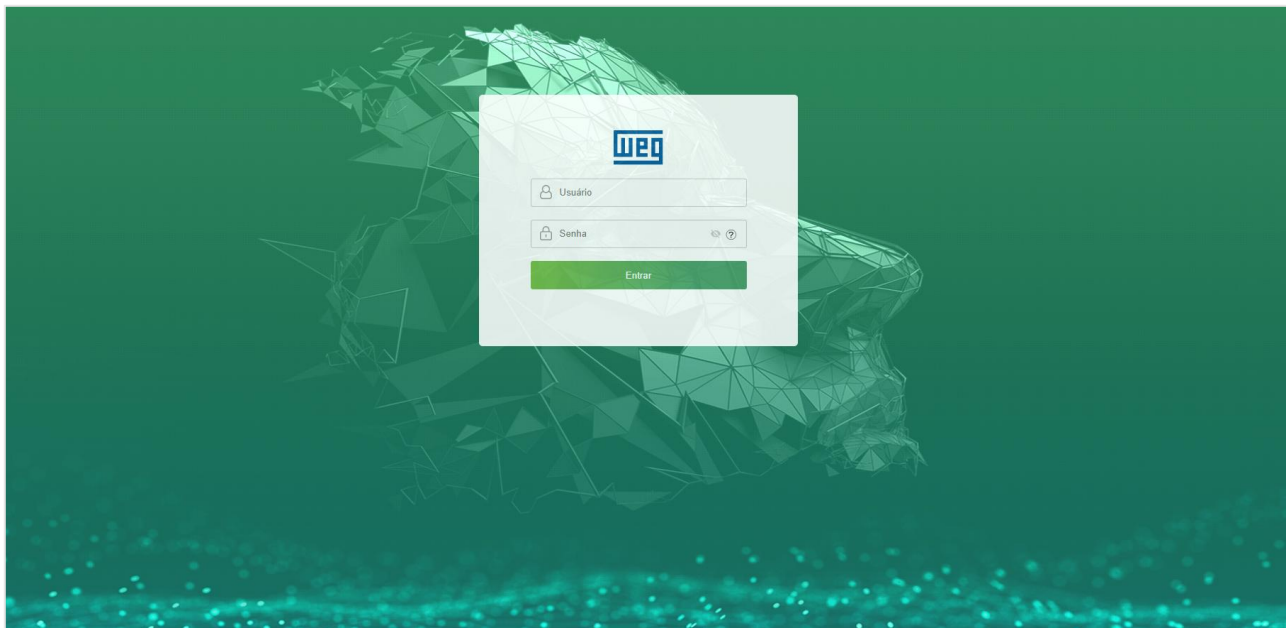
Nome da Função	Descrição
Capacidade	Exibe o armazenamento do usuário do dispositivo atual, Face, Impressão digital, Armazenamento de impressões digitais e senha administradores, registros, frequência, lista de bloqueio e perfil fotos.
Inf. dispositivo	Exibe o nome do dispositivo, o número de série e 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.

20 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 © 2015-2021 All Right Reserved

21 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

22 Como adicionar o Terminal Facial no WEG BioGuard

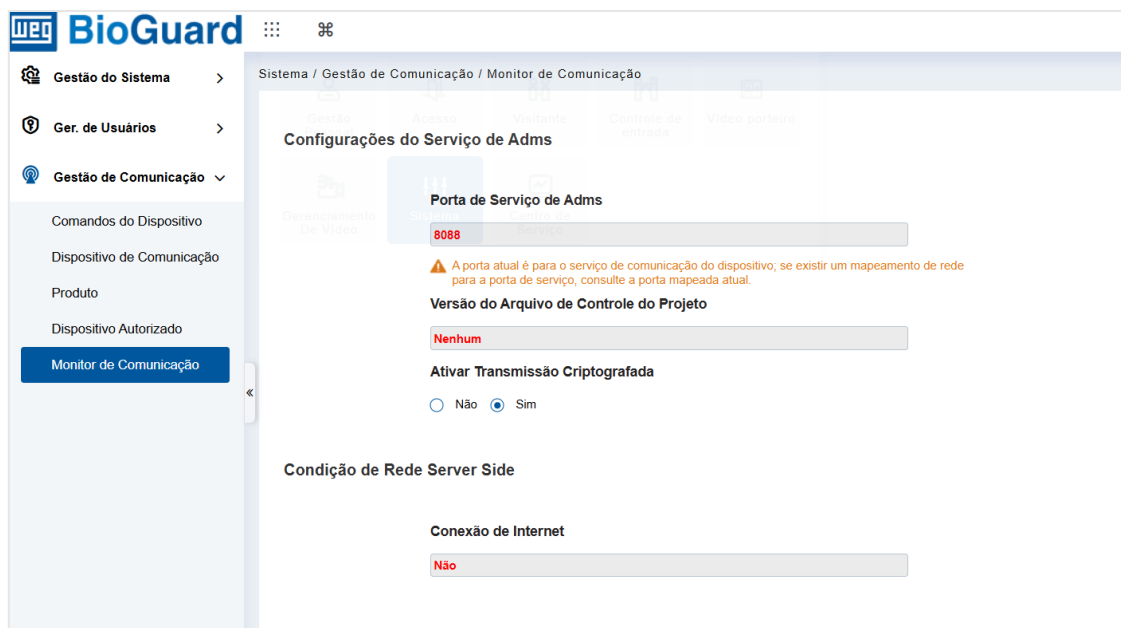
No terminal facial em **[Conf. Com] > [TCP/IP]** defina os parâmetros de rede. Se a comunicação TCP/IP do dispositivo for bem-sucedida, o ícone  será exibido no canto superior da tela inicial.

TCP/IP	
Mostrar na barra status	☐
IPv4	
Ender.IP	192.168.1.201
Masc. Rede	255.255.255.0
Gateway	0.0.0.0
DNS	0.0.0.0

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.

Configurar server n...	
Tipo de servidor	ADMS
Habilitar domínio	☐
End. Servidor	192.168.31.32
Porta servidor	8088
Proxy	☐

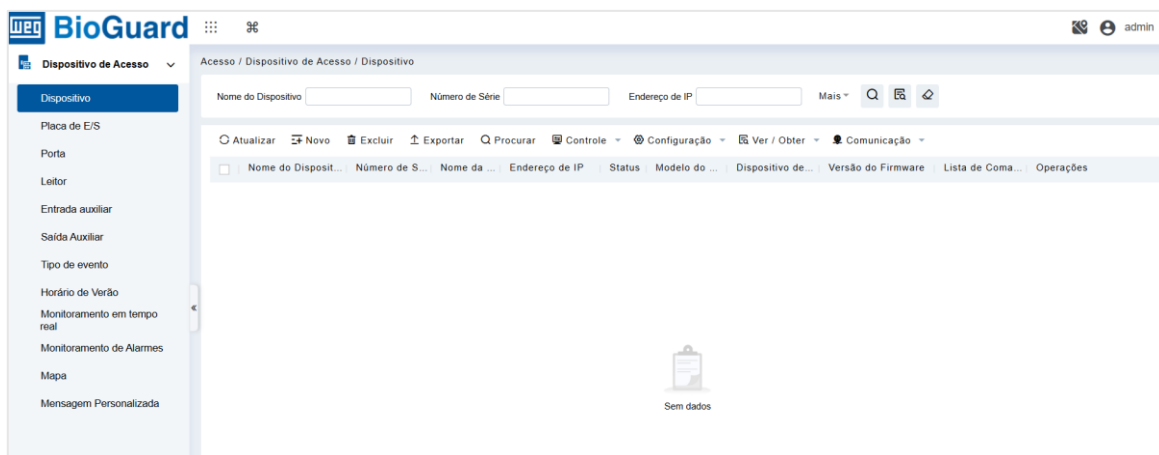
Para saber qual a porta do servidor, acesse no BioGuard: **Sistema > Gestão de Comunicação > Monitor de Comunicação** e verifique qual a porta ADMS utilizada. (Por padrão de fábrica 8088)



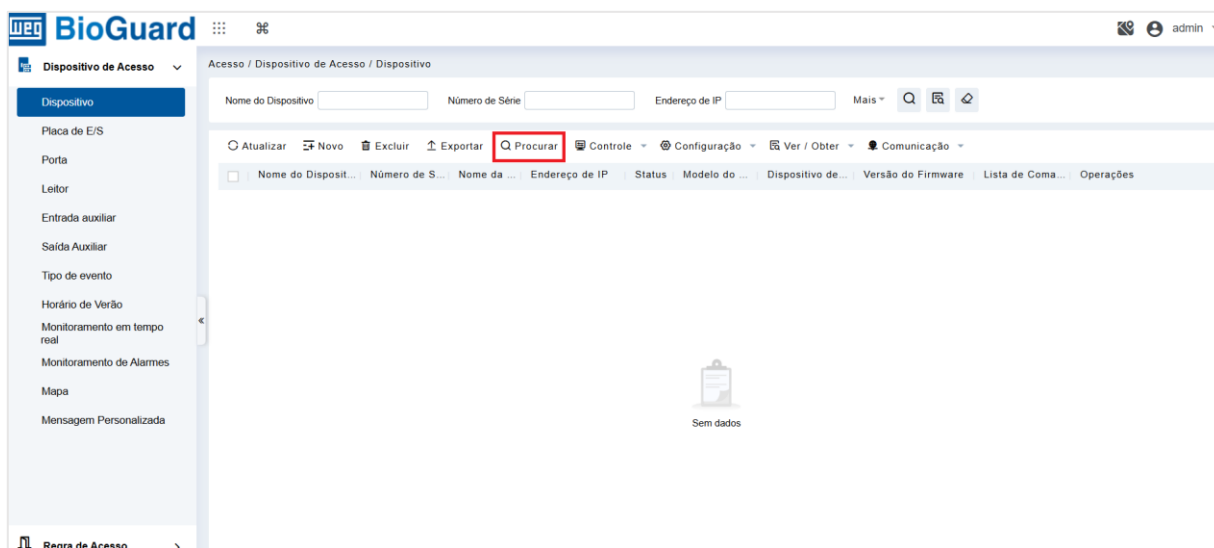
Caso durante a instalação do BioGuard foi selecionado a opção de “Use HTTPS”, no terminal facial em **[Conf. Com] > [Conf. Comunic]** habilite a opção HTTPS. Caso contrário, desabilite a opção.

A screenshot of a terminal screen titled 'Conf. Comunic.'. It has a back arrow icon at the top left. The screen contains four input fields: 'Senha com.' with a masked password '*****', 'ID Equip.' with the value '1', 'Porta de comu.TCP' with the value '4370', and 'HTTPS' with a toggle switch that is currently turned off.

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



Selecione a opção **Procurar**.



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

