Manual do Usuário

ProMA Series

Data: Setembro 2023

Versão do Documento: 2.0

Idioma: Português

Obrigado por escolher nosso produto. Por favor, leia atentamente as instruções antes de iniciar a operação. Siga estas instruções para garantir o bom funcionamento do produto. As imagens apresentadas neste manual são apenas ilustrativas.

Para obter mais detalhes, por favor, visite o site da nossa empresa: www.zkteco.com.br.

Copyright © 2022 ZKTECO CO., LTD. Todos os direitos reservado.

Marca registrada

ZKTeco é uma marca registrada da ZKTeco. Outras marcas mencionadas neste manual são propriedades de seus respectivos proprietários.

Responsabilidade

Este manual contém informações sobre a operação e manutenção dos produtos ZKTeco. Os direitos de propriedade intelectual de todos os documentos, desenhos, etc., em relação aos produtos fornecidos pela ZKTeco são de propriedade da ZKTeco. O conteúdo deste documento não deve ser usado ou compartilhado pelo receptor com terceiros sem a permissão expressa por escrito da ZKTeco.

O conteúdo deste manual deve ser lido na íntegra antes de iniciar a utilização e manutenção do produto adquirido. Se algum dos conteúdos do manual parecer pouco claro ou incompleto, entre em contato com a ZKTeco antes de iniciar a utilização e/ou manutenção do referido produto.

É um pré-requisito essencial para a operação e/ou manutenção corretas/adequadas, que a equipe que irá utilizar e/ou dar manutenção, esteja totalmente familiarizado com o projeto e que esta equipe tenha recebido um treinamento completo da utilização e/ou manutenção da máquina / unidade / produto. É ainda essencial para a utilização segura da máquina / unidade / produto que a equipe tenha lido, compreendido e seguido as instruções de segurança contidas no manual.

Em caso de qualquer conflito entre os termos e condições deste manual e as especificações de fichas-técnicas, desenhos, folhas de instruções ou quaisquer outros documentos acordados entre as partes relacionados ao produto, as condições de tais documentos devem prevalecer em relação ao manual.

A responsabilidade da ZKTeco em relação ao presente manual e ao produto está detalhada nos termos de sua respectiva Garantia.

A ZKTeco reserva-se o direito de adicionar, apagar, alterar ou modificar as informações contidas no manual de tempos em tempos, independente de aviso prévio, por meio de circulares, cartas, notas e/ou novas edições do manual, visando a melhor utilização e/ou segurança do produto. Os mais recentes procedimentos de utilização e documentos relevantes estão disponíveis em http://www.zkteco.com.br sendo de responsabilidade do usuário verificar eventuais atualizações e informes, especialmente se o produto indicar problemas no funcionamento ou se restarem dúvidas sobre sua instalação, manejo, armazenamento, operação e/ou manutenção.

Se houver algum problema relacionado ao produto, entre em contato conosco.

ZKTeco Filial Brasil

Endereço **Vespasiano:** Rodovia MG-010, KM 26 - Loteamento 12 - Bairro Angicos, Vespasiano - MG | CEP: 33.206-240

Telefone (31) 3055-3530

Para questões comerciais, por favor entre em contato conosco pelo e-mail: comercial.brasil@zkteco.com
Para saber mais sobre nossas filiais globais, visite www.zkteco.com

Sobre a Empresa

A ZKTeco é um dos maiores fabricantes do mundo de leitores RFID e biométricos (impressão digital, facial, veia do dedo). A oferta de produtos inclui leitores e painéis de controle de acesso, câmeras de reconhecimento facial de alcance próximo e remoto, controladores de acesso a elevadores/andares, torniquetes, controladores de portões de reconhecimento de placas de veículos (LPR) e produtos de consumo, incluindo fechaduras de porta com bateria operada com leitor de impressão digital e facial. Nossas soluções de segurança são multilíngues e localizadas em mais de 18 idiomas diferentes. Na moderna instalação de fabricação da ZKTeco, certificada pela ISO9001 e com 700.000 pés quadrados, controlamos a fabricação, o design do produto, a montagem de componentes e a logística/ envio, tudo sob um mesmo teto.

Os fundadores da ZKTeco estabeleceram a determinação de pesquisa e desenvolvimento independentes de procedimentos de verificação biométrica e a produção em série de SDK de verificação biométrica, que inicialmente foram amplamente aplicados em segurança de PC e campos de autenticação de identidade. Com o contínuo aprimoramento do desenvolvimento e muitas aplicações de mercado, a equipe gradualmente construiu um ecossistema de autenticação de identidade e um ecossistema de segurança inteligente, que são baseados em técnicas de verificação biométrica. Com anos de experiência na industrialização de verificações biométricas, a ZKTeco foi oficialmente estabelecida em 2007 e agora é uma das principais empresas do mundo na indústria de verificação biométrica, possuindo várias patentes e sendo selecionada como Empresa Nacional de Alta Tecnologia por 6 anos consecutivos. Seus produtos são protegidos por direitos de propriedade intelectual.

Sobre o Manual

Este manual apresenta as operações da Série ProMA .

Todas as imagens exibidas são apenas para fins ilustrativos. As imagens neste manual podem não ser exatamente consistentes com os produtos reais.

Recursos e parâmetros com ★ não estão disponíveis em todos os dispositivos.

Este produto pode conter um ou mais módulos listados abaixo, de acordo com o modelo adquirido por você.

ANATEL
11891-22-11470

Módulo: L287B-SR
"Incorpora produto homologado pela ANATEL sob número 11891-22-11470"

Este equipamento não tem direito à proteção contra interferência prejudicial e não pode causar interferência em sistemas devidamente autorizados.

Convenções do Documento

As convenções utilizadas neste manual estão listadas abaixo:

Convenções de Interface Gráfica do Usuário:

Para o software	
Convenção	**Descrição**
Bold	Utilizado para identificar nomes de interfaces de software, por exemplo, **OK, Confirmar, Cancelar.**
>	Os menus de vários níveis são separados por estes parêntesis. Por exemplo, Ficheiro > Criar > Pasta.
Para o dispositivo	
Convenção	**Descrição**
< >	Nomes de botões ou teclas para dispositivos. Por exemplo, pressione <OK>.
[ ]	Os nomes de janelas, itens de menu, tabelas de dados e nomes de campos estão entre colchetes. Por exemplo, abra a janela [Novo usuário].
/	Os menus de vários níveis são separados por barras inclinadas. Por exemplo, [Arquivo/Criar/Pasta].

Símbolos

Convenção	Descrição
	Isso representa uma nota à qual é preciso dar mais atenção.
	As informações gerais que ajudam a realizar as operações mais rapidamente.
	As informações que são importantes.
	Cuidados a tomar para evitar perigos ou erros.
	A declaração ou o evento que alerta sobre algo ou que serve como exemplo de advertência.

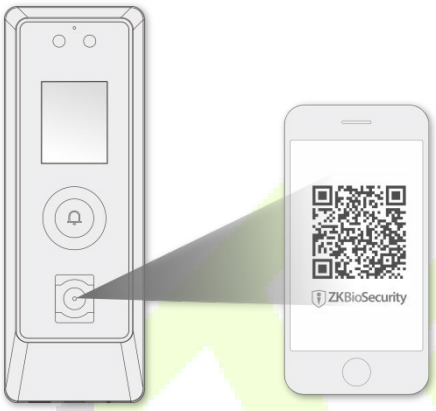
Índice

1 Instruções de Uso

Antes de entrar nas características do dispositivo e suas funções, é recomendado estar familiarizado com os fundamentos abaixo.

1.1 Como escanear o código QR?

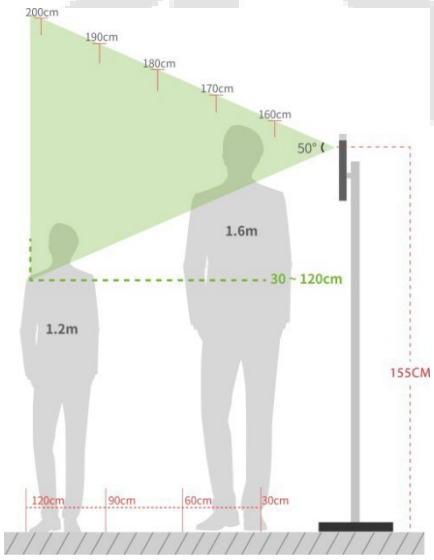
Abra o aplicativo ZKBioSecurity no seu celular e alinhe a tela do telefone com o scanner de código QR do dispositivo.



Observação: Posicione o seu celular a uma distância de 15 a 50cm do dispositivo (a distância depende do tamanho da tela do celular), não obstrua o scanner de código QR do dispositivo e o código QR na tela do celular.

1.2 Posição em Pé, Postura e Expressão Facial

- **A distância recomendada**



A distância recomendada entre o dispositivo e um usuário com altura variando de 1,55m a 1,85m é de 0,3 a 2,5m. Os usuários podem se mover ligeiramente para frente ou para trás para melhorar a qualidade das imagens faciais capturadas.

- **Postura em Pé e Expressão Facial Recomendadas**

Postura em Pé

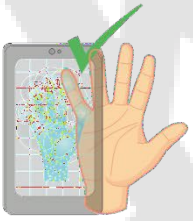
Expressão Facial

Observação: Mantenha sua expressão facial e postura em pé naturais durante o processo de cadastro ou verificação.

1.3 Registro de Palma★

Coloque a palma da sua mão na área de coleta de palma, de modo que a palma fique paralela ao dispositivo. Certifique-se de manter espaço entre os dedos.

Mantenha uma distância efetiva de 30 a 50 cm.



Mantenha espaço entre os dedos.

Não mantenha os dedos próximos.

Não coloque a palma fora da área de coleta.

Não mantenha os dedos enrolados.

Observação:

1. Coloque sua palma a uma distância de 30 a 50 cm do dispositivo.
2. Coloque sua palma na área de coleta de palma, de modo que a palma fique paralela ao dispositivo.
3. Certifique-se de manter espaço entre os dedos.
4. Evite a luz solar direta ao usar a função de palma ao ar livre. De acordo com testes de laboratório, o efeito de reconhecimento de palma é melhor quando a intensidade da luz não ultrapassa 10.000 lux.

1.4 Registro Facial

Tente manter o rosto no centro da tela durante o registro. Por favor, olhe diretamente para a câmera e mantenha-se imóvel durante o registro facial. A tela deve ficar assim:

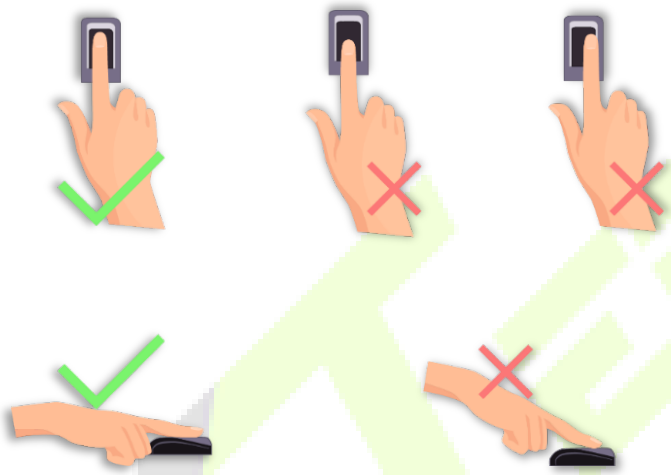
Método correto de registro e autenticação facial

- **Recomendação para registrar uma face**
  - Ao registrar um rosto, mantenha uma distância de 40 cm a 80 cm entre o dispositivo e o rosto.
  - Tenha cuidado para não mudar sua expressão facial (rosto sorridente, rosto contraído, piscar de olhos, etc.).
  - Se não seguir as instruções na tela, o registro facial pode levar mais tempo ou falhar.
  - Tenha cuidado para não cobrir os olhos ou sobrancelhas.
  - Não use bonés, máscaras, óculos de sol ou óculos.
  - Tenha cuidado para não exibir dois rostos na tela. Registre uma pessoa por vez.
  - É recomendado que um usuário que usa óculos registre o rosto tanto com quanto sem óculos.
- **Recomendação para autenticar um rosto**
  - Certifique-se de que o rosto esteja dentro das diretrizes exibidas na tela do dispositivo.
  - Se os óculos forem trocados, a autenticação pode falhar. Se o rosto sem óculos tiver sido registrado, autentique o rosto sem óculos. Se o rosto com óculos tiver sido registrado, autentique o rosto com os óculos previamente usados.

- Se uma parte do rosto estiver coberta por um chapéu, uma máscara, um tapa-olho ou óculos de sol, a autenticação pode falhar. Não cubra o rosto e permita que o dispositivo reconheça tanto as sobrancelhas quanto o rosto.

1.5 Posicionamento dos Dedos★

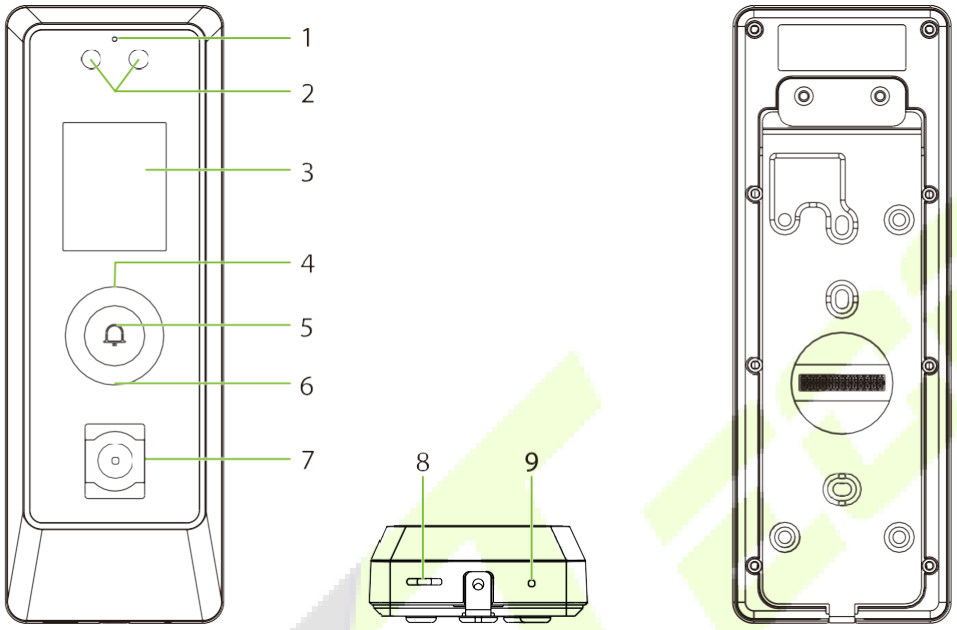
Dedos recomendados: Indicador, médio ou anelar.
Evite usar o polegar ou o dedo mínimo, pois eles são mais difíceis de tocar com precisão no leitor de impressões digitais.



Observação: Por favor, utilize o método correto ao pressionar os dedos sobre o leitor de impressões digitais para registro e identificação.

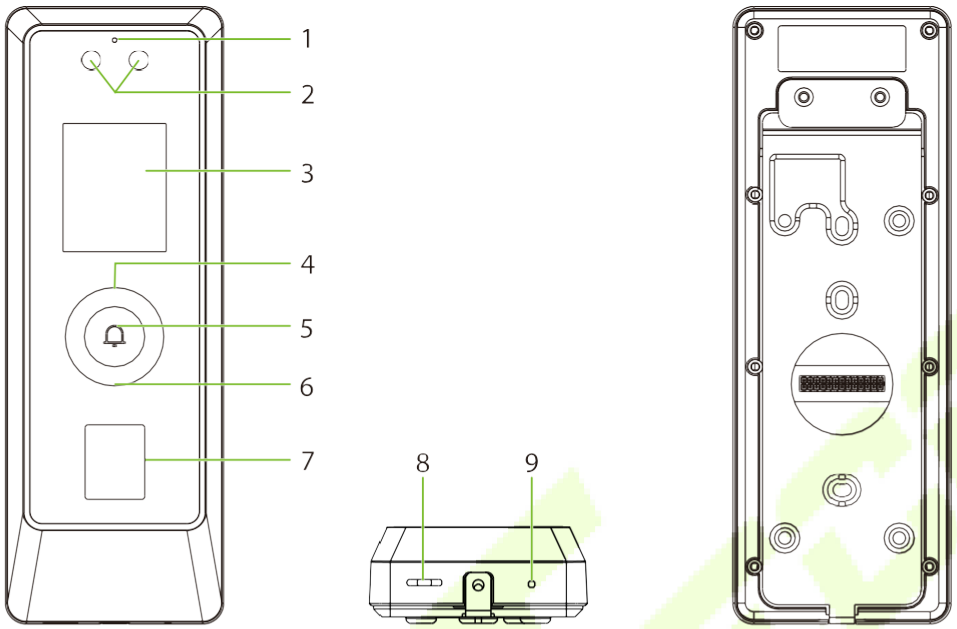
2 Aparência

2.1 ProMA-QR



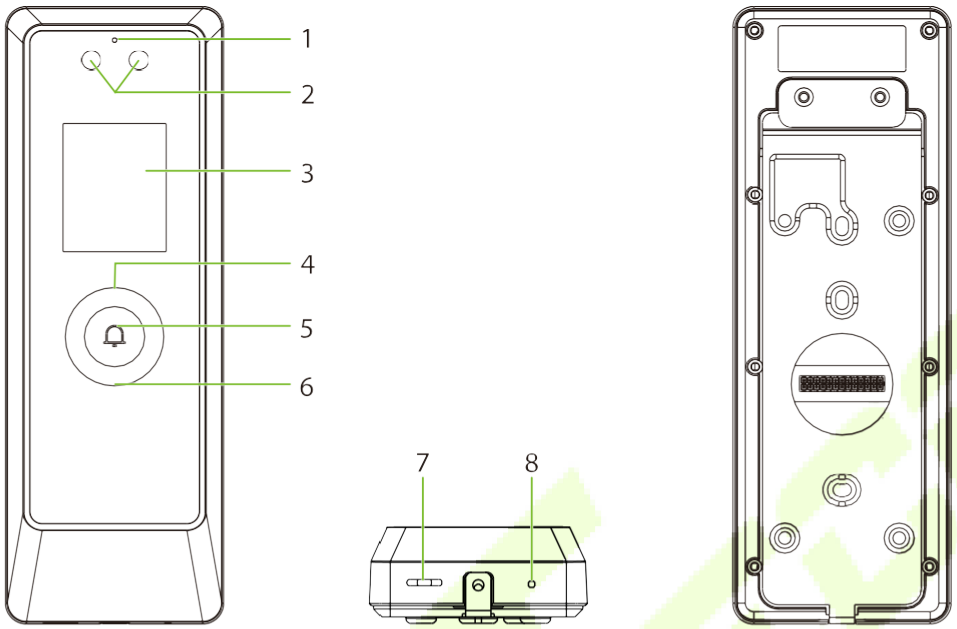
No.	Descrição
1	Microfone
2	Câmera e Detector de Palma
3	Tela de 2 polegadas
4	Área de leitura de cartões
5	Botão da campainha
6	Flash
7	Scanner de QR Code
8	Alto-falante
9	Redefinir

2.2 ProMA



No.	Descrição
1	Microfone
2	Câmera e Detector de Palma
3	Tela de 2 polegadas
4	Área de leitura de cartões
5	Botão da campainha
6	Flash
7	Sensor de impressões digitais
8	Alto-falante
9	Redefinir

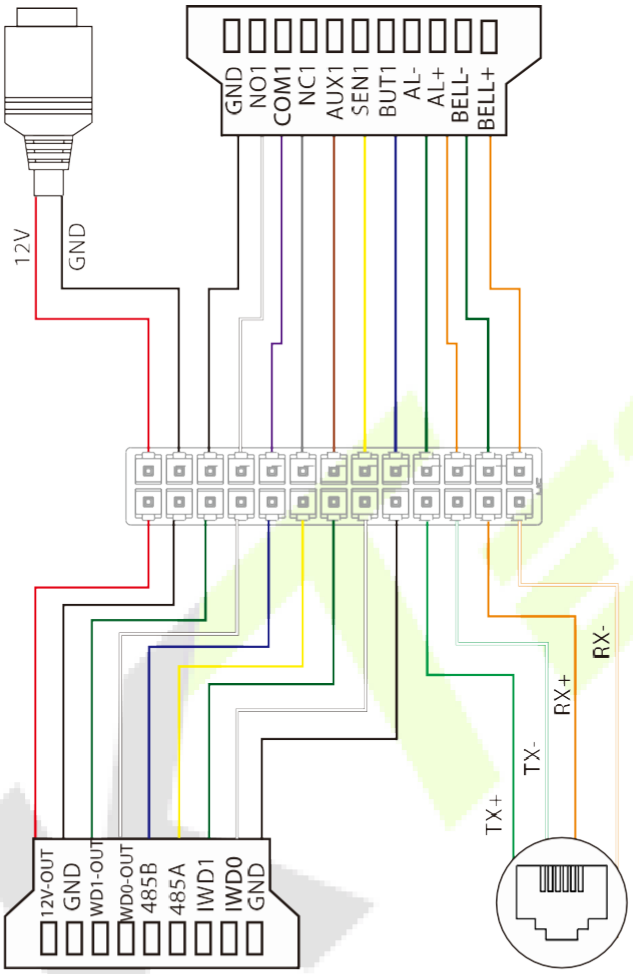
2.3 ProMA-RF



No.	Descrição
1	Microfone
2	Câmera e Detector de Palma
3	Tela de 2 polegadas
4	Área de leitura de cartões
5	Botão da campainha
6	Flash
7	Alto-falante
8	Redefinir

2.4 Descrição do Terminal e da Fiação

2.4.1 Descrição do Terminal

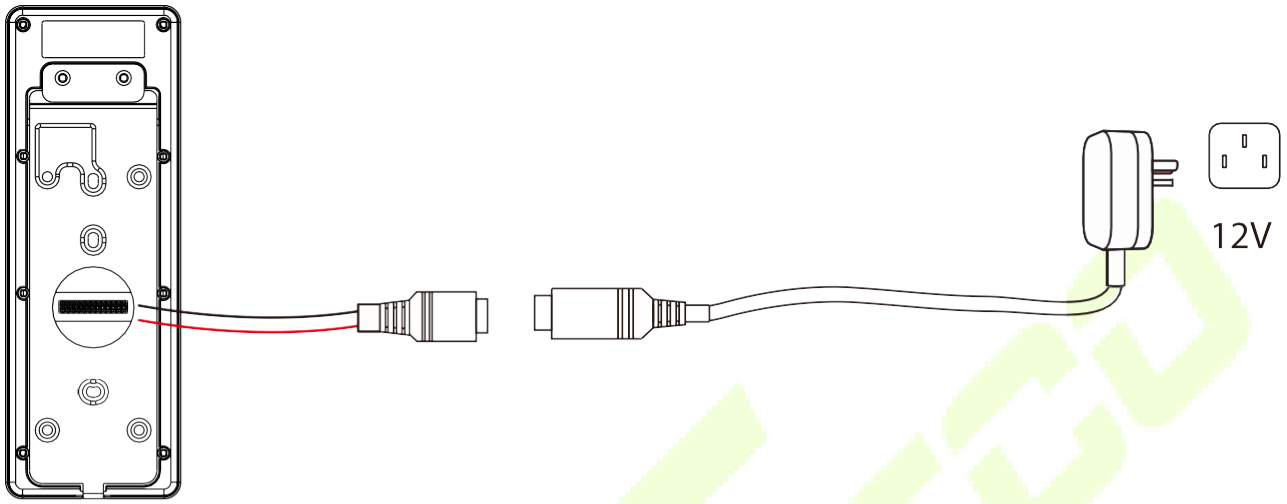


Interface	Descrição
12V	Entrada de Energia 12V
GND	
GND	
NO1	Fechadura
COM1	
NC1	

AUX1	Entrada Auxiliar
SEN1	Sensor
BUT1	Botoeira
AL-	Alarme
AL+	
BELL-	Campainha
BELL+	
12V-OUT	Saída de Energia
GND	
WD1-OUT	Saída Wiegand
WD0-OUT	
485B	RS485
485A	
IWD1	Entrada Wiegand
IWD0	
GND	
TX+	Interface de Rede
TX-	
RX+	
RX-	

2.5 Descrição da Fiação

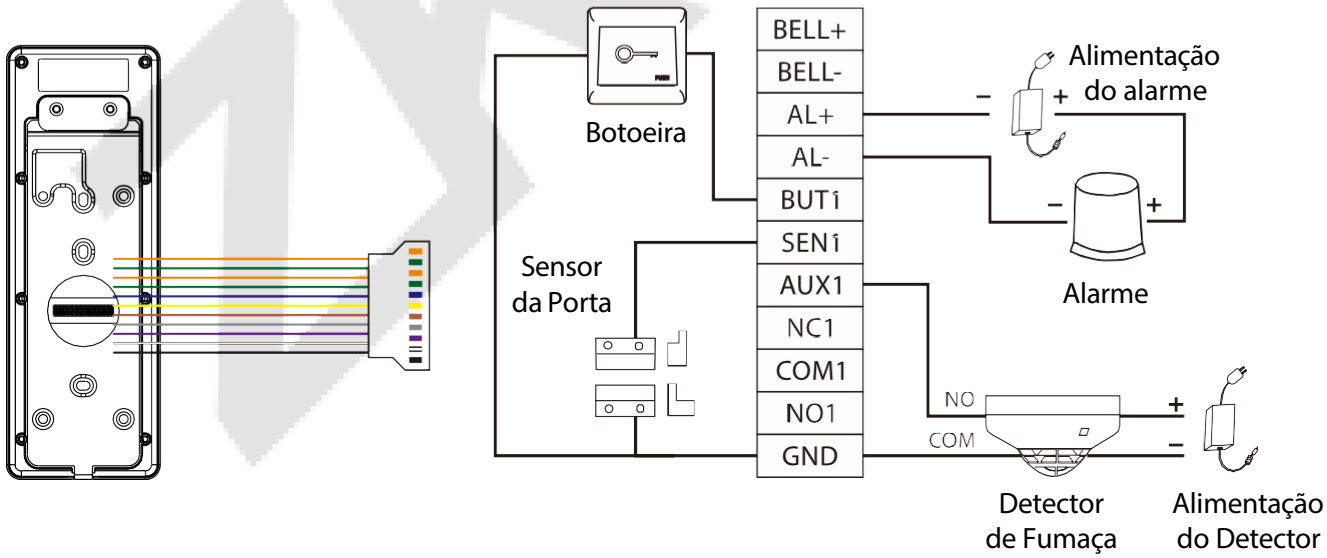
2.5.1 Conexão de Energia



Fonte de energia recomendada

- Classificação de 12V e 3A
- Para compartilhar a energia do dispositivo com outros dispositivos, utilize uma fonte de alimentação com classificação de corrente mais alta.

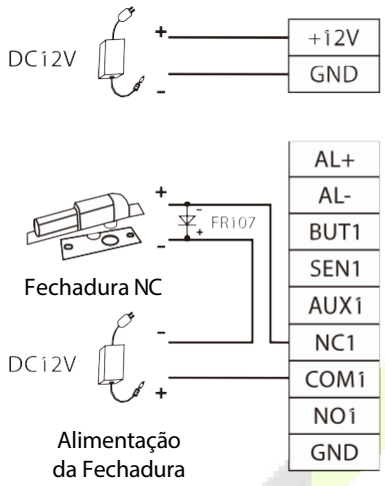
2.5.2 Sensor de Porta, Botão de Saída, Alarme e Conexão Auxiliar



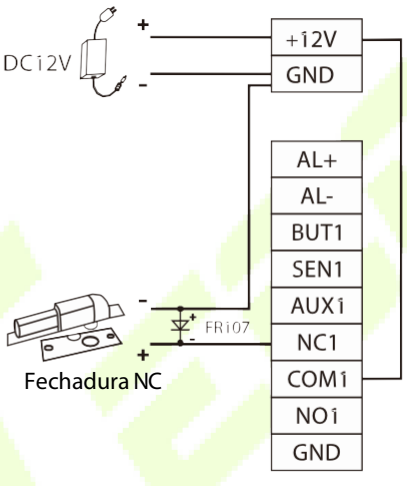
2.5.3 Conexão do Relé de Trava

O sistema suporta tanto a Trava Normalmente Aberta (NO) quanto a Trava Normalmente Fechada (NC). A Trava NO (normalmente aberta quando energizada) é conectada aos terminais 'NO1' e 'COM1', e a Trava NC (normalmente fechada quando energizada) é conectada aos terminais 'NC1' e 'COM1'. A energia pode ser compartilhada com a trava ou pode ser usada separadamente para a trava, conforme mostrado no exemplo abaixo com a Trava NC:

1) Dispositivo não compartilhando energia com a fechadura.

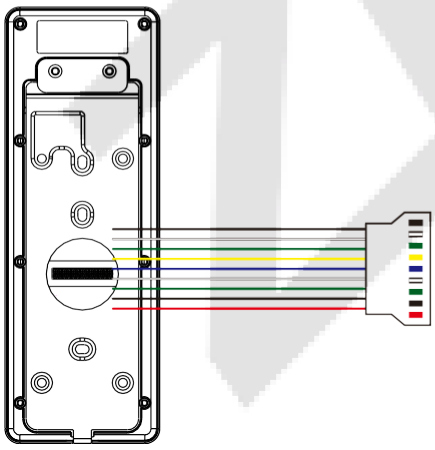


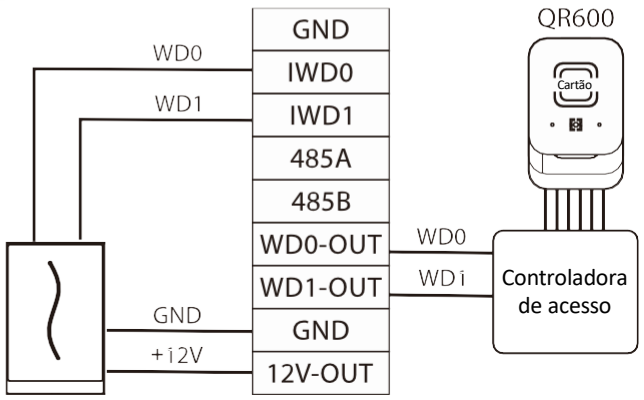
2) Dispositivo compartilhando energia com a fechadura.



2.5.4 Conexão Wiegand

O leitor de cartão Wiegand se conecta aos 4 pinos superiores do terminal Wiegand, e os dois últimos pinos são usados pelo Controlador de Acesso, conforme mostrado na figura a seguir. Ele envia as credenciais para o dispositivo por meio da comunicação Wiegand.



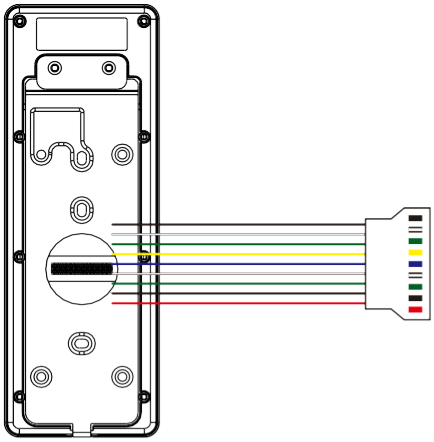


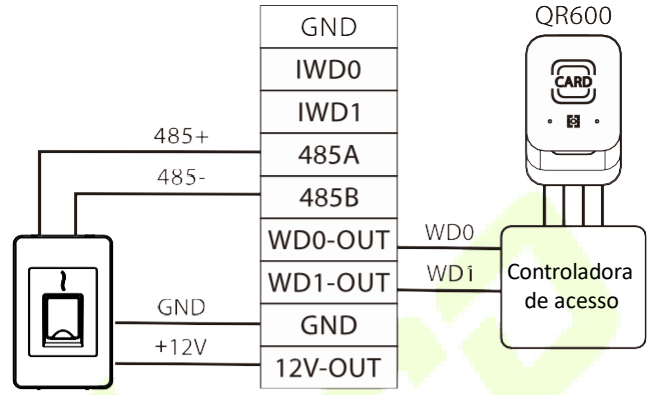
Leitor Wiegand

Observação: O leitor QR600 é um recurso exclusivo do ProMA-QR. Para obter detalhes, por favor consulte o Guia Rápido do Leitor de Código QR600.

2.5.5 Conexão RS485

O RS485 permite que os usuários se conectem a vários leitores ao dispositivo. O RS485 pode ser conectado ao terminal, conforme mostrado na figura abaixo.



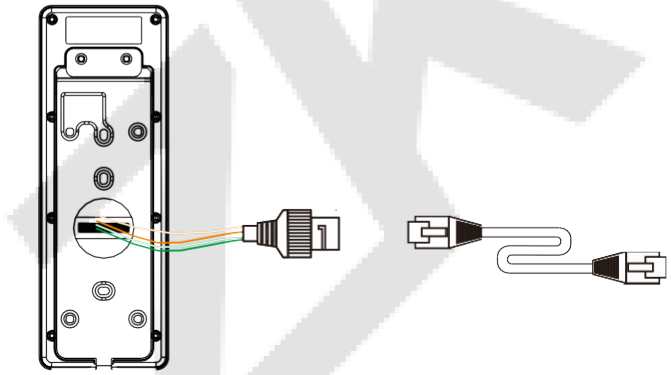


Leitor 485

Observação: O leitor QR600 é um recurso exclusivo do ProMA-QR. Para mais detalhes, por favor consulte o Guia de Início Rápido do Leitor QR600.

2.5.6 Conexão Ethernet

Conecte o dispositivo e o software do computador usando um cabo Ethernet. Um exemplo é mostrado abaixo:



Endereço IP padrão: 192.168.1.201
Máscara de sub-rede: 255.255.255.0

Endereço IP padrão: 192.168.1.130
Máscara de sub-rede: 255.255.255.0

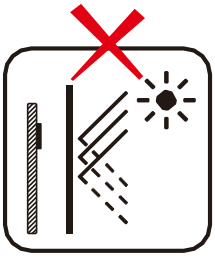
Observação: Na LAN, os endereços IP do servidor (PC) e do dispositivo devem estar no mesmo segmento de rede ao se conectar ao Servidor Web.

3 Instalação

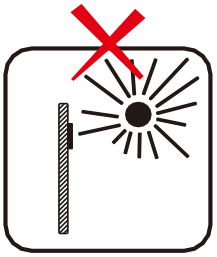
3.1 Ambiente de Instalação

Por favor, consulte as seguintes recomendações para a instalação.

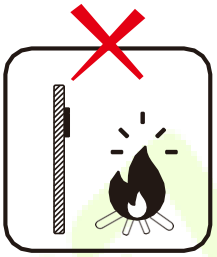
Instale em ambientes internos



Evite instalar perto de janelas de vidro



Evite exposição a luz solar direta

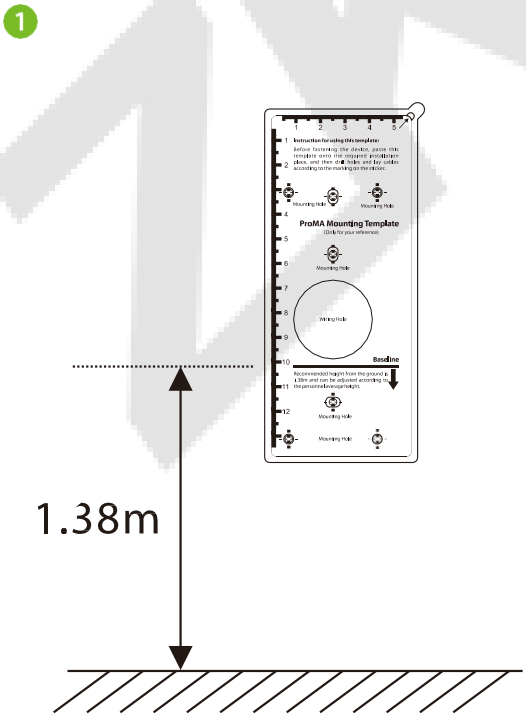


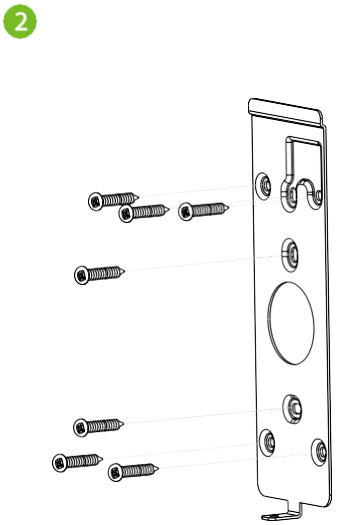
Evite o uso de qualquer fonte de calor perto do dispositivo

3.2 Instalação do Dispositivo

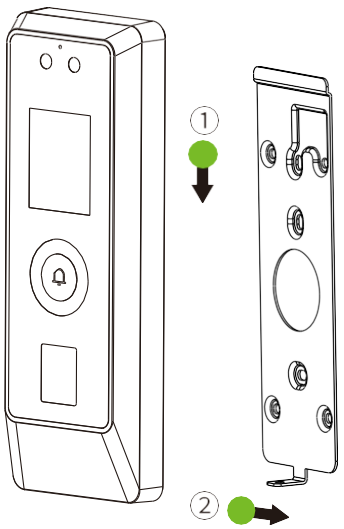
As instalações da série ProMA são iguais, o seguinte é um exemplo do ProMA.

1. Fixe o adesivo do modelo de montagem na parede e faça furos de acordo com o papel de montagem.
2. Fixe a placa traseira na parede usando parafusos de montagem na parede.
3. Fixe o dispositivo à placa traseira.
4. Aperte o dispositivo à placa traseira com um parafuso de segurança.

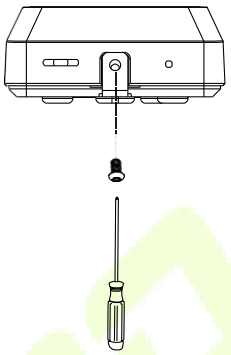




3

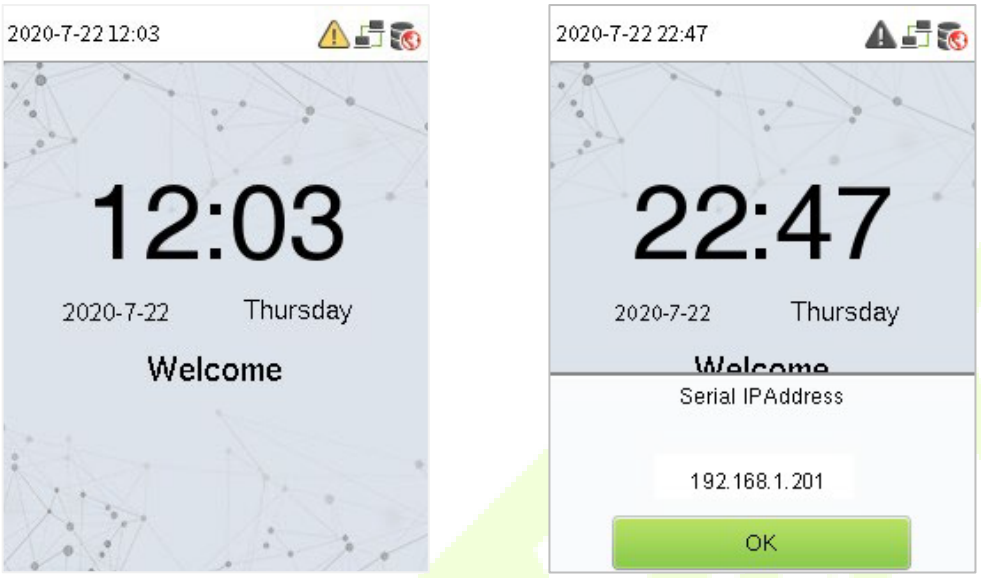


4



4 Interface de Espera

Após conectar a fonte de alimentação, a seguinte interface de espera é exibida:



O dispositivo possui um endereço IP incorporado, que pode ser usado para comunicação do dispositivo, conexão com o Servidor Web e software ZKBio CVSecurity, dentre outros.

Observação: O dispositivo utiliza uma tela de 2 polegadas, que não suporta operação por toque e é utilizada apenas para exibir informações de status e verificação. Todas as operações, como informações do dispositivo, configurações de comunicação, gerenciamento de usuários e configurações do sistema, são realizadas e configuradas no Servidor Web.

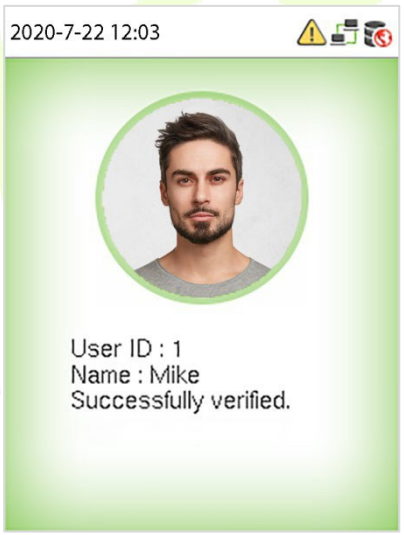
5 Modo de Autenticação

5.1 Autenticação de QR Code ★

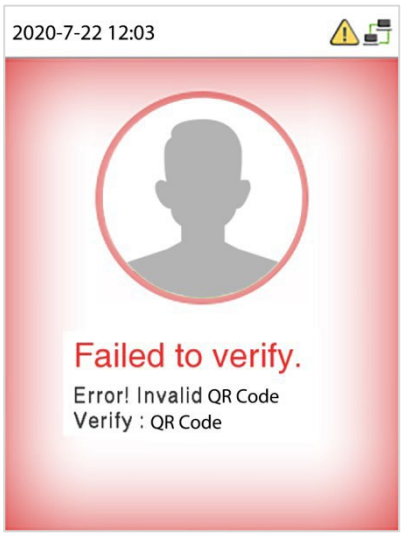
Neste modo de verificação, o dispositivo compara a imagem do código QR coletada pelo coletor de código QR com todos os dados de código QR armazenados no dispositivo.

Toque em [**Credencial Móvel**] no aplicativo ZKBioSecurity e um código QR será exibido, contendo informações como ID do funcionário e número do cartão (o código QR estático contém apenas o número do cartão). O código QR pode substituir um cartão físico em um dispositivo específico para obter autenticação sem contato. Consulte a seção Credencial Móvel★ para mais informações.

Autenticação bem-sucedida



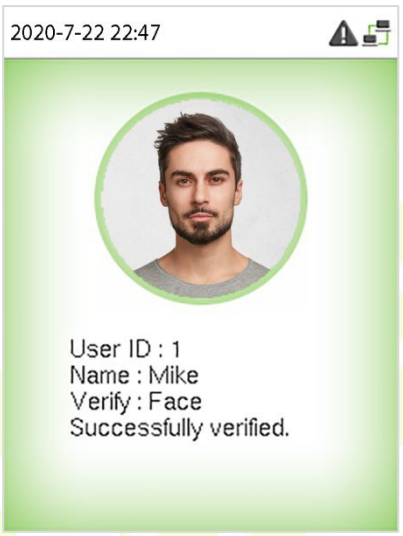
Falha na autenticação:



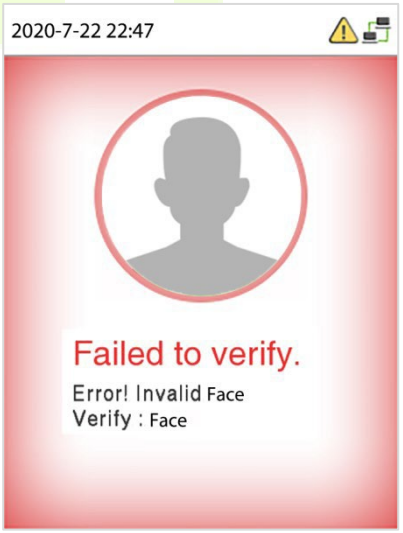
5.2 Autenticação Facial

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

Autenticação bem-sucedida:



Falha na autenticação:

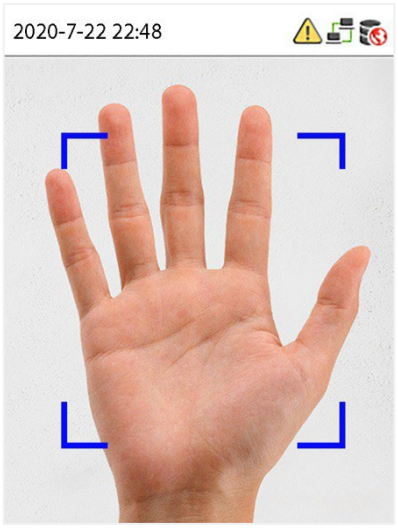


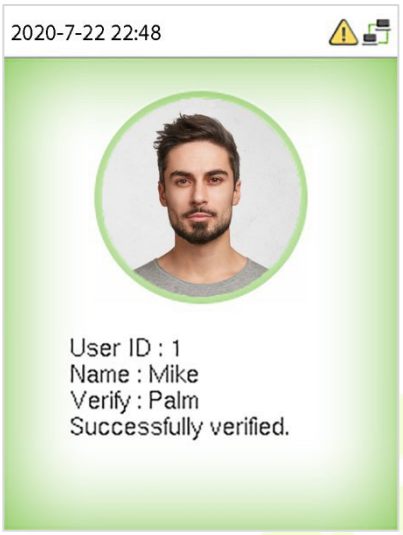
5.3 Autenticação de Palma★

Este modo de autenticação compara a imagem da palma coletada pelo módulo de palma com todos os modelos de dados de palma no dispositivo.

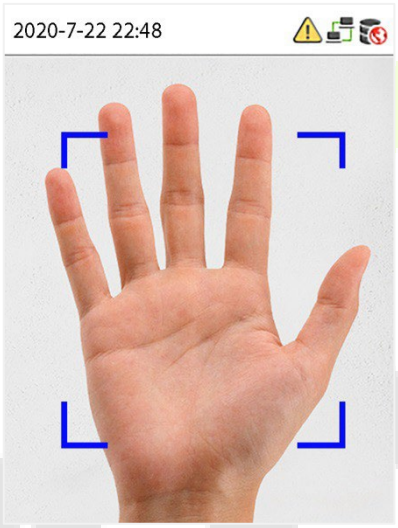
O dispositivo irá distinguir automaticamente entre o modo de autenticação de palma e o modo de autenticação facial. Coloque a palma na área que pode ser capturada pelo módulo de palma, para que o dispositivo possa alternar automaticamente para o modo de autenticação de palma.

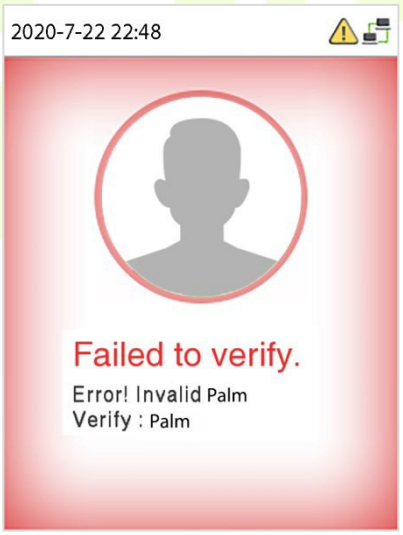
Autenticação bem-sucedida:





Falha na autenticação:



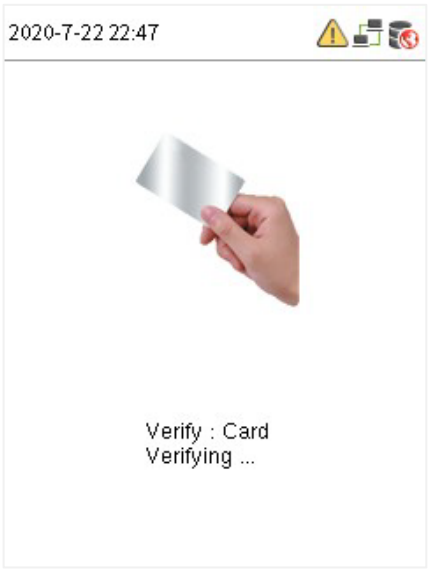


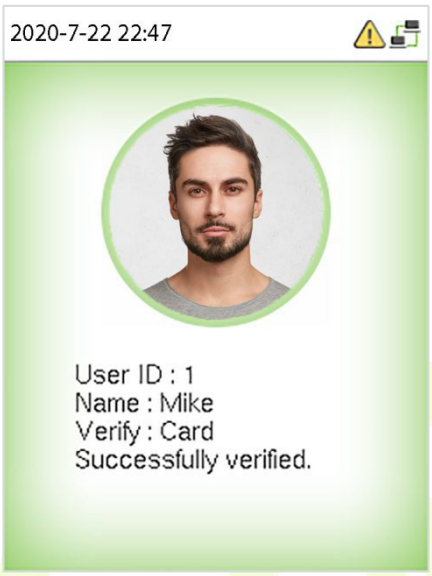
Observação: O reconhecimento de palma requer a configuração de uma câmera especial.

5.4 Autenticação de Cartão

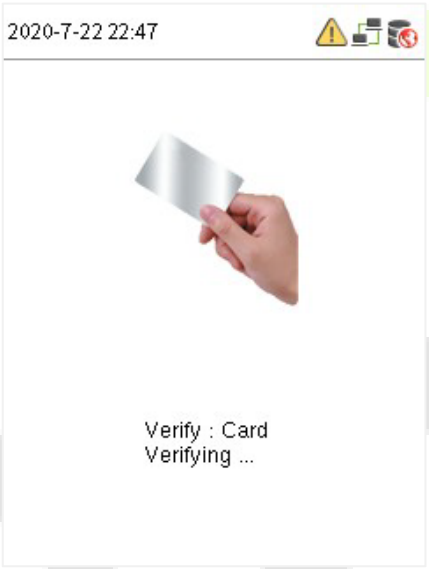
O modo de Autenticação de Cartão compara o número do cartão na área de indução do cartão com todos os dados de número de cartão registrados no dispositivo. A seguir está a tela de autenticação de cartão.

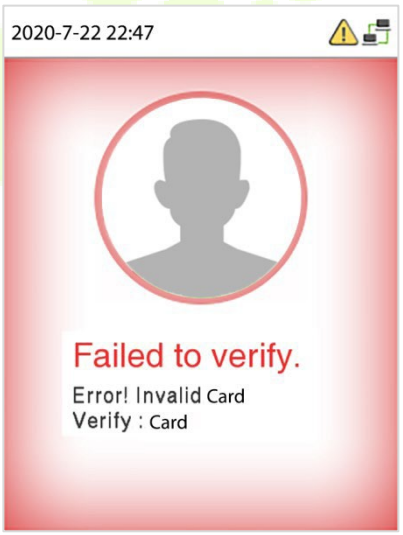
Autenticação bem-sucedida:





Falha na autenticação:





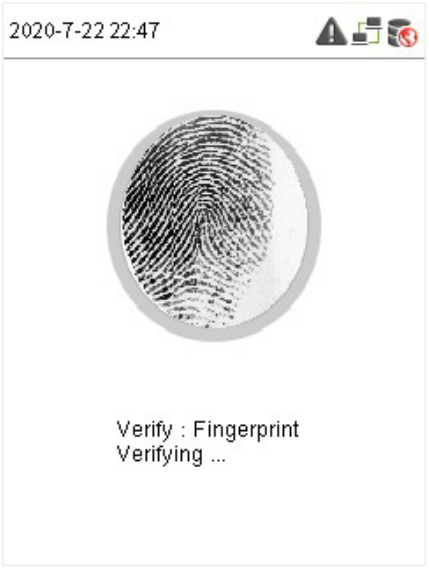
Observação: O ProMA-QR suporta códigos PDF417 de identidade chilena e argentina.

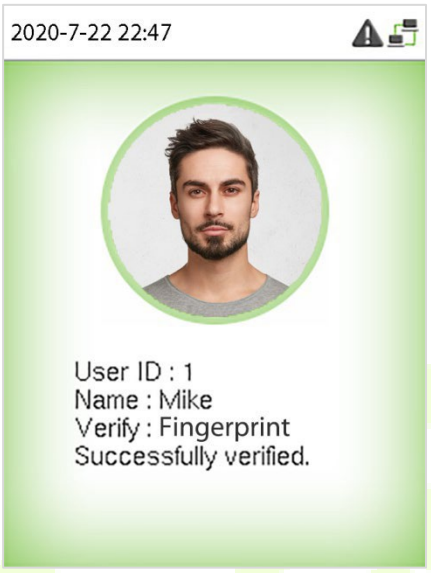
5.5 Autenticação de Impressão Digital ★

Este método compara a impressão digital do usuário que está sendo pressionada no leitor de impressão digital com todos os dados de impressão digital pré-armazenados no dispositivo.

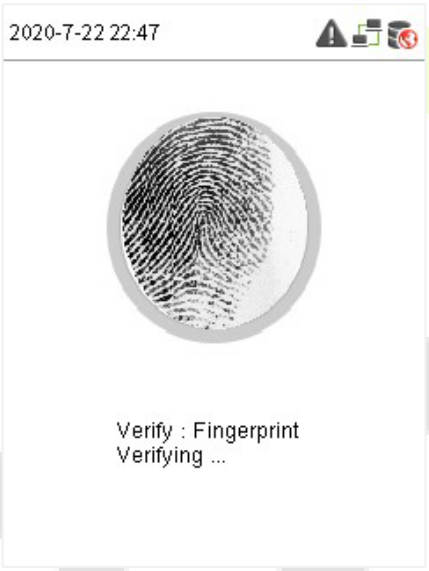
Para entrar no modo de identificação de impressão digital, basta tocar o dedo no leitor de impressão digital.

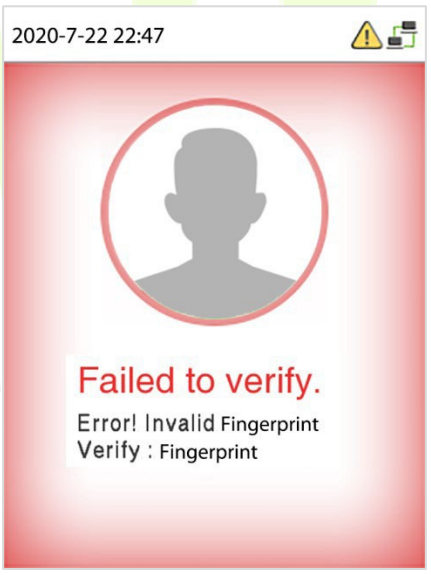
Autenticação bem-sucedida:





Falha na autenticação:

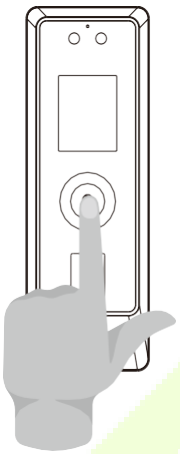




6 Acesso ao Servidor Web

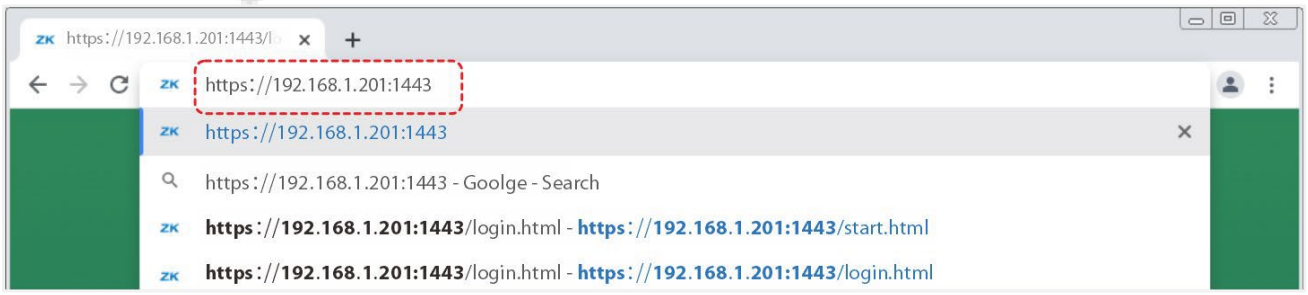
Um usuário pode abrir o aplicativo web para configurar os parâmetros relevantes do dispositivo.

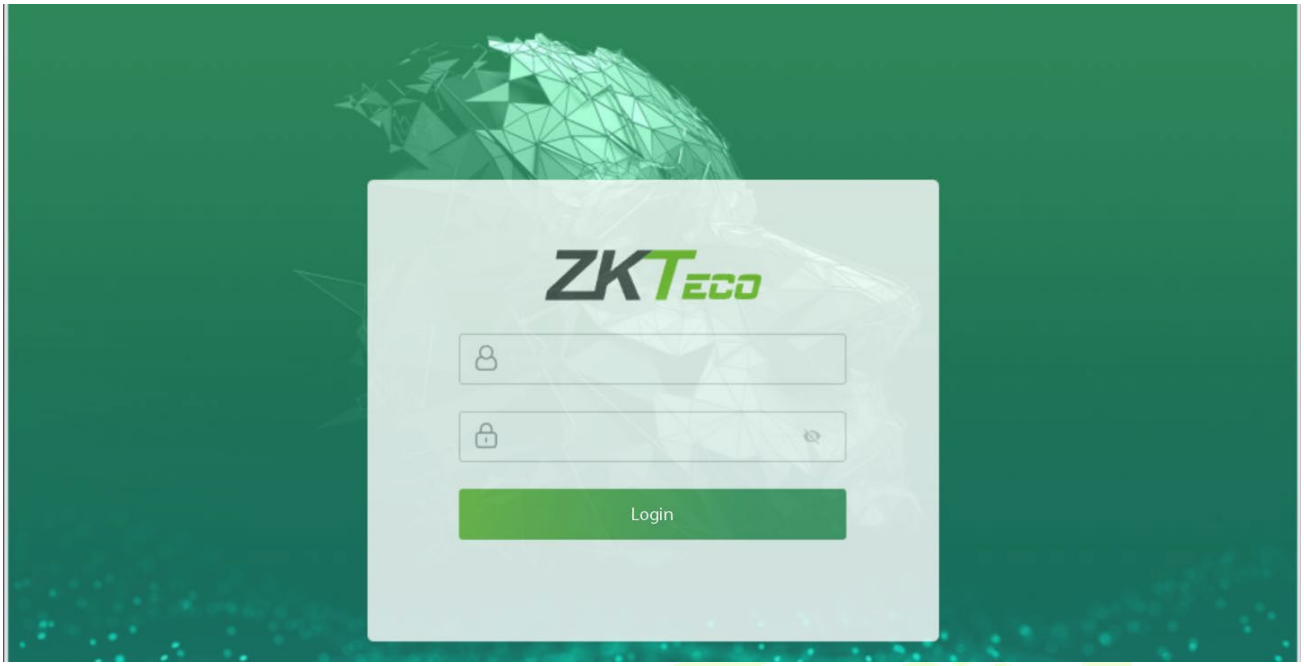
1. Pressione e segure o botão da campainha do dispositivo até que o IP apareça.



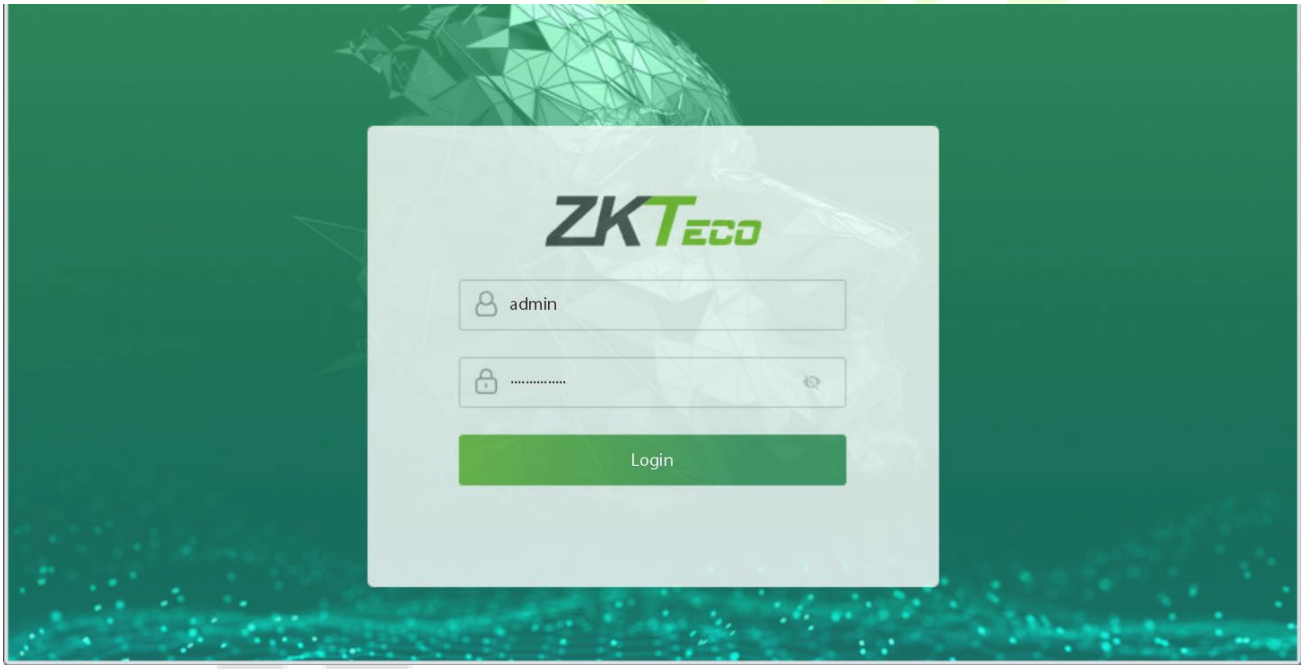
2. Abra um navegador e digite o endereço para fazer login no Servidor Web, o endereço é **https:// Endereço IP Serial:1443.** Por exemplo: **https://192.168.1.201:1443.**

   Observação: O Endereço IP Serial do dispositivo para comunicação pode ser modificado. Para mais detalhes, consulte as Configurações de Comunicação.





3. Insira a conta e senha do Servidor Web, a conta padrão é: **admin**, senha: **admin@123**.



Observação:

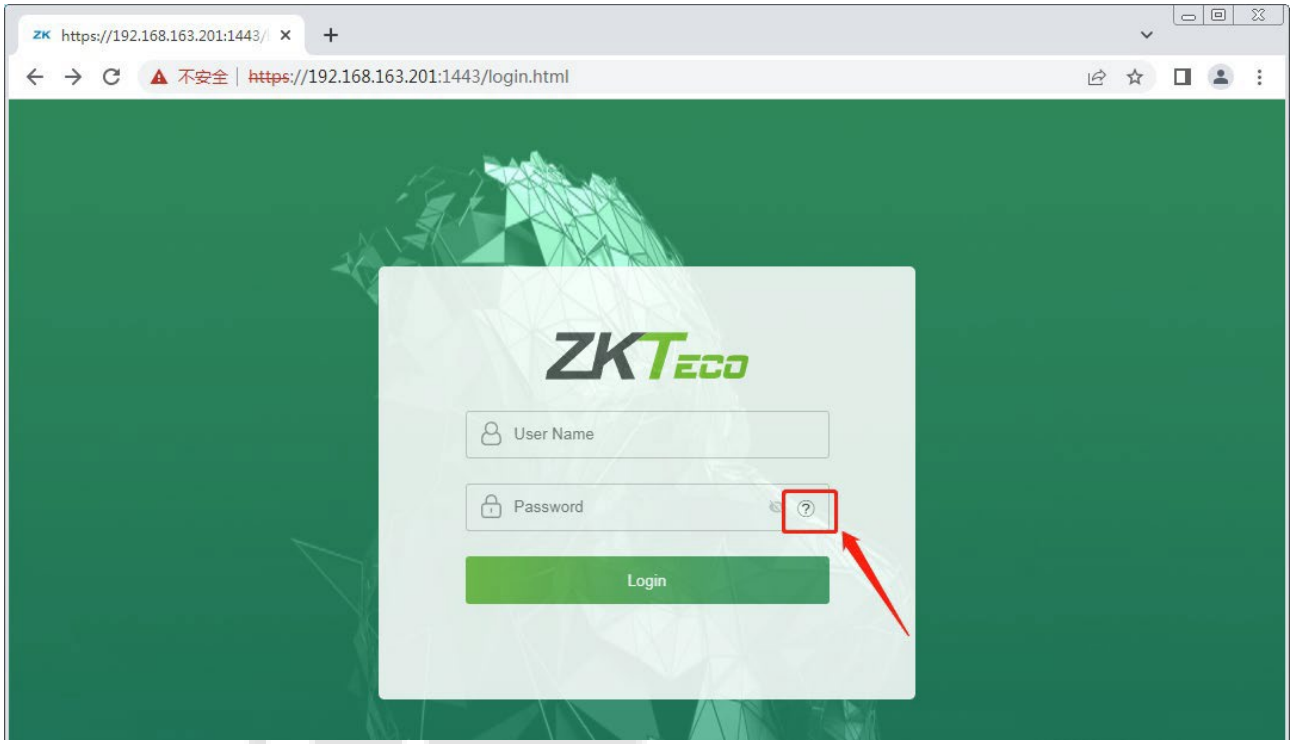
1. Após fazer login pela primeira vez, os usuários precisam alterar a senha original e fazer login novamente antes de poderem utilizá-la. Por favor, consulte as instruções para alterar a senha.
2. Para recuperar a senha facilmente, por favor, registre um super administrador primeiro. Por favor, consulte as instruções para o registro de usuários.

7 Esqueci a senha

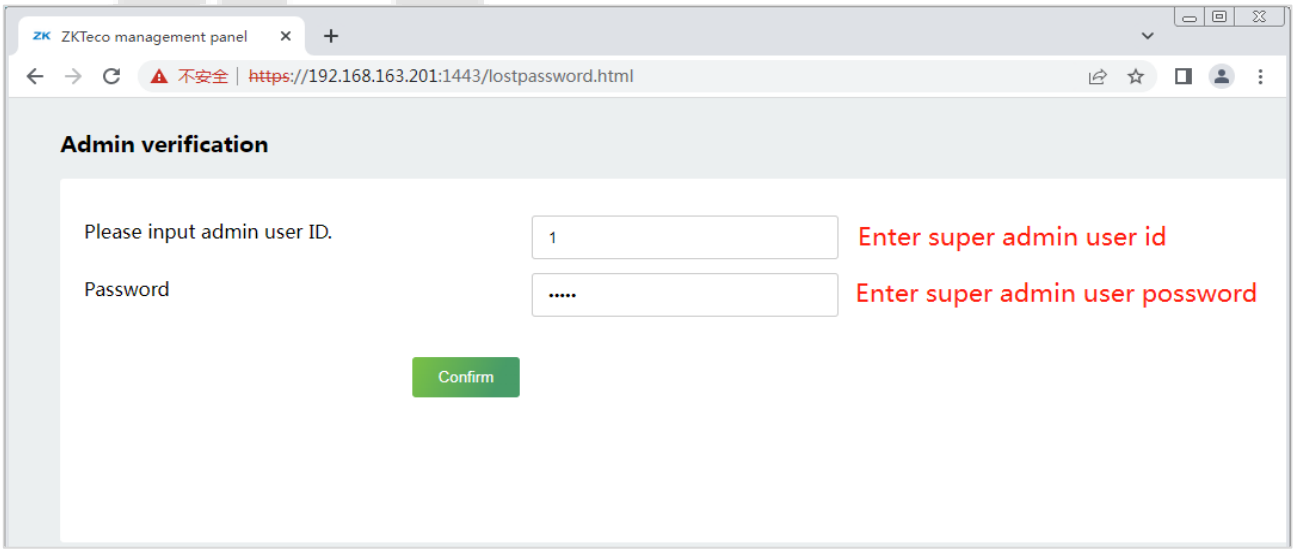
- **Método 1 (Quando há um super administrador):**

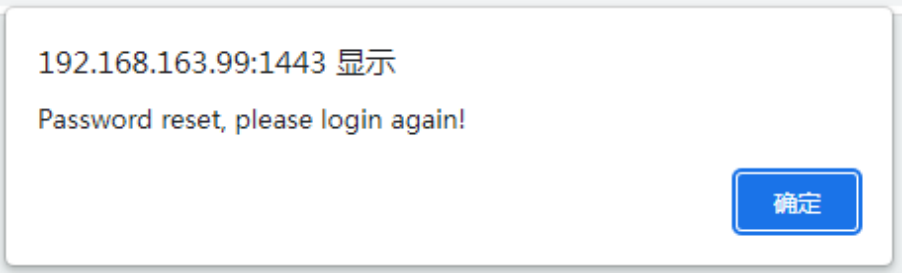
Se você esqueceu a senha do Servidor Web, você pode redefini-la pelo super administrador registrado.
Os passos detalhados são os seguintes:

1. Clique no ícone na interface de login.



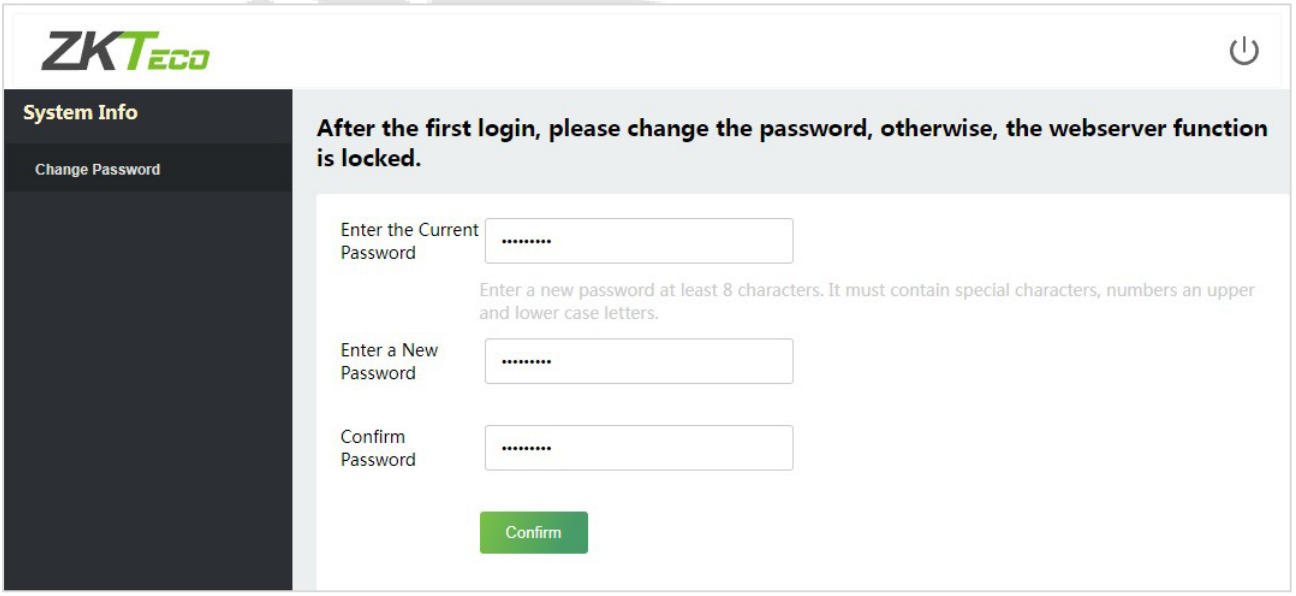
2. Na página pop-up, insira as informações relevantes do usuário super administrador conforme solicitado.





3. Após uma redefinição bem-sucedida, insira a conta e a senha padrão (conta: admin, senha: admin@123) na interface de login para fazer o login.

4. Por motivos de segurança, por favor, altere sua senha após fazer login com sucesso.

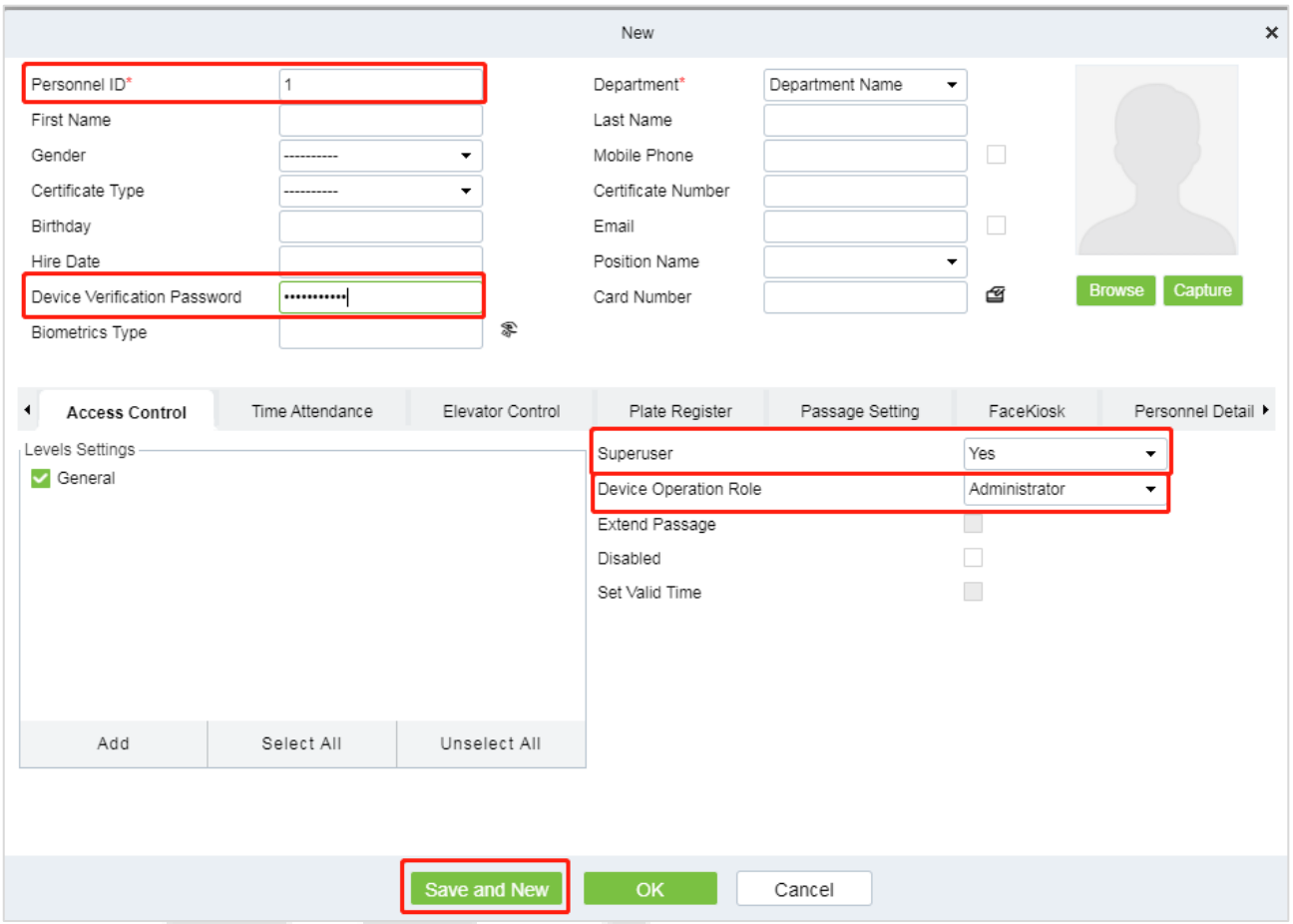


Observação: O super administrador deve existir.

- **Método 2 (Quando não há um super administrador):**

Se a rede do dispositivo estiver funcionando normalmente e o ZKBio CVSecurity estiver conectado, você pode redefinir a senha enviando a conta e a senha do super administrador a partir do servidor.

1. Clique em **Pessoal > Pessoa > Novo** no Servidor ZKBio CVSecurity.



2. Após registrar as informações do super administrador, clique em **Salvar** e **Novo**.

3. Clique em **Acesso > Dispositivo > Controle > Sincronizar Todos os Dados nos Dispositivos** para sincronizar todos os dados no dispositivo, incluindo os novos usuários.

Observação: Para outras operações específicas, consulte o Manual do Usuário ZKBio CVSecurity V6600.

5. Após a sincronização dos dados ser bem-sucedida, você pode redefinir a senha com o super administrador recém-registrado. Os passos de operação são os mesmos do método 1.

- **Método 3:**

Se o dispositivo não tiver registrado um super administrador e não puder se conectar ao servidor, entre em contato com nossos técnicos pós-venda para obter ajuda na recuperação da senha.

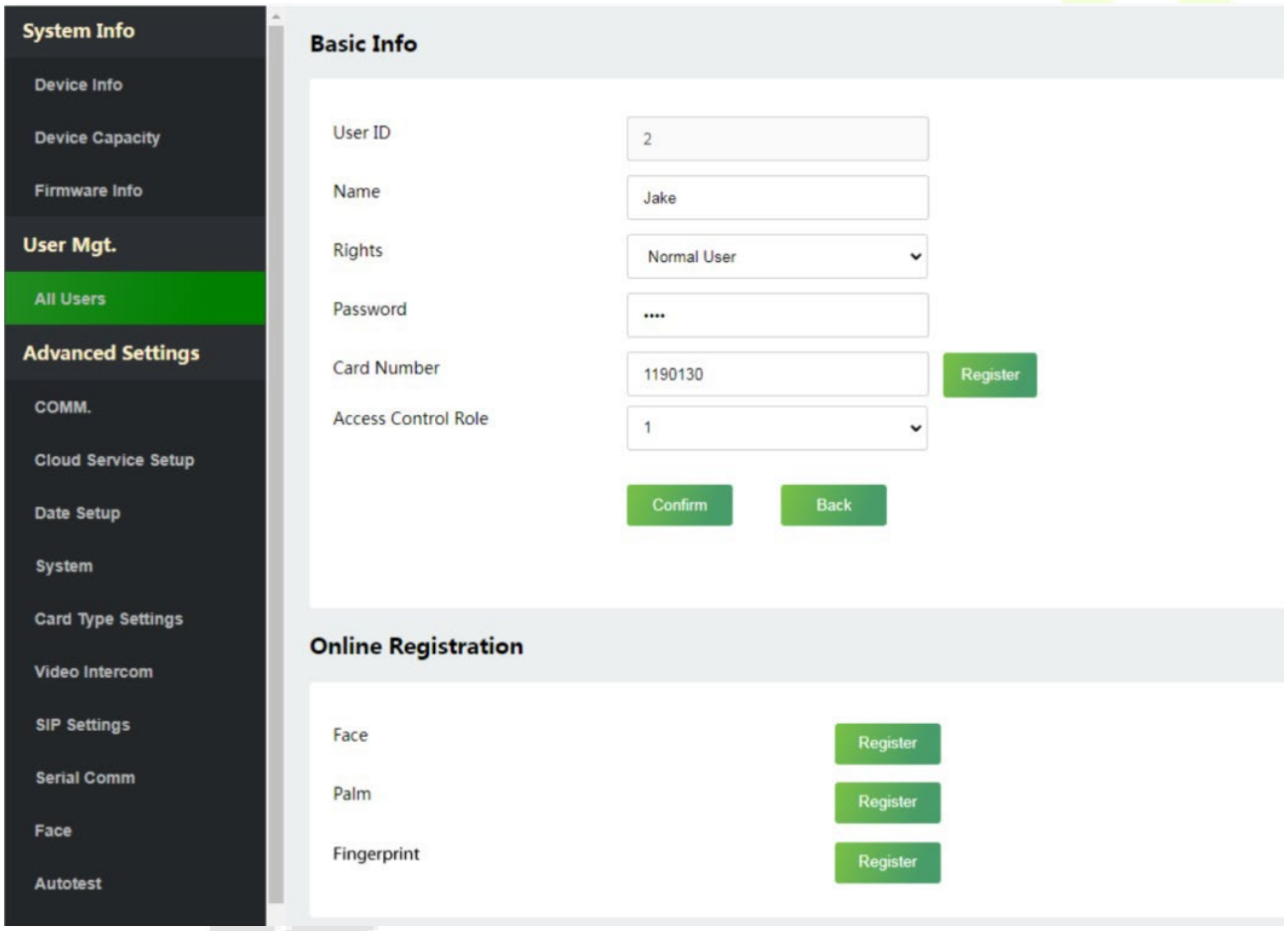
8 Gerenciamento de Usuários

8.1 Registro de Usuário

8.1.1 Informações Básicas

Clique em **Todos os Usuários** no Servidor Web.

Nesta interface, você pode registrar o ID do usuário, nome, direitos, senha, número do cartão e função de controle de acesso do novo usuário. Clique em **Confirmar** para salvar.



Função	Descrição
ID de Usuário	O ID de usuário pode conter de 1 a 14 caracteres por padrão. Pode ser composto por números, letras, símbolos, etc.
Nome	Um nome pode ter até 63 caracteres.

Privilégio	Defina a função do usuário como **Usuário Normal** ou **Super Administrador**. • **Super Administrador:** O Super Administrador possui todos os privilégios de gerenciamento no Servidor Web. • **Usuário Normal:** Se o Super Administrador já estiver registrado no Servidor Web, os Usuários Normais não terão os privilégios para gerenciar o sistema e só poderão acessar autenticações.
Senha	Defina a senha de registro do usuário.
Número do Cartão	Digite o número do cartão manualmente. Após registrar o número do cartão do usuário, o usuário poderá passar o cartão para verificação. Ou, atrás do número do cartão, clique em **Registrar**, e o dispositivo exibirá a interface de registro de cartão em tempo real. Passe o cartão na área de leitura do cartão. O registro do cartão será bem-sucedido. ***Observação:*** O ProMA-QR suporta códigos de ID PDF417 chilenos e argentinos, bem como o leitor auxiliar QR600.
Função de Controle de Acesso	A Função de Controle de Acesso define os privilégios de acesso à porta para cada usuário. Novos usuários serão adicionados ao Grupo 1 por padrão, podendo ser realocados para outros grupos conforme necessário. O sistema suporta até 10 grupos de controle de acesso.

Observação:

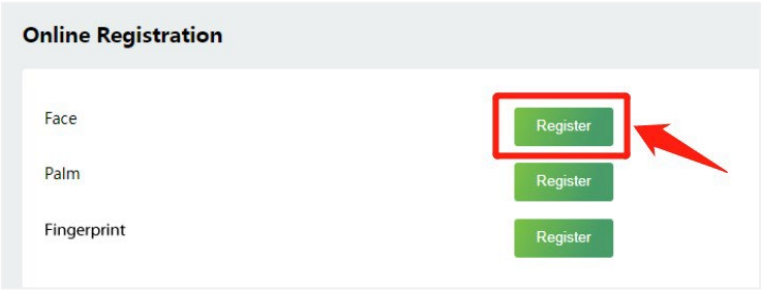
1. Durante o registro inicial, é possível modificar o seu ID; no entanto, após o registro bem-sucedido, não é possível modificar o ID registrado.
2. Se a mensagem "Falha na configuração!" aparecer, você deve escolher um ID de usuário diferente, pois o que você inseriu já existe.

8.1.2 Registro Online

Nesta interface, você pode registrar a Face, Palma ★ e Impressão Digital ★ do usuário. O modo de autenticação só pode ser registrado após a confirmação das informações básicas.

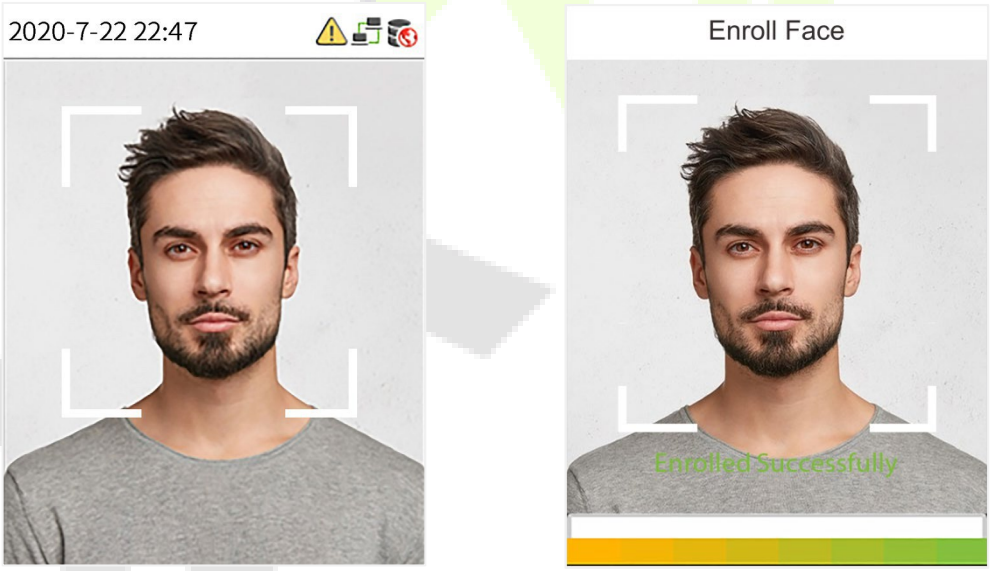
➢ Registrar Face

Na interface atual, atrás da barra de face, clique em **Registrar** e o dispositivo exibirá a interface de registro de face em tempo real.



- Por favor, posicione seu rosto voltado para a câmera e dentro da caixa de orientação branca e mantenha-se imóvel durante o registro da face.
- Uma barra de progresso aparece durante o registro da face e a mensagem "Registrado com sucesso" é exibida até que o registro seja concluído.
- Se a face já estiver registrada, a mensagem "Face Duplicada" será exibida.

A interface de registro é a seguinte:



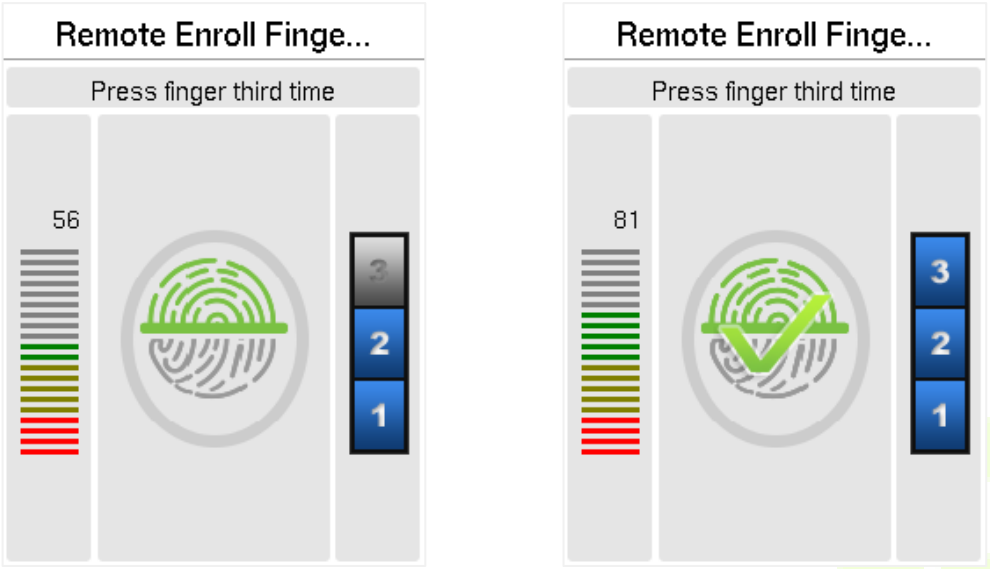
Observação: Durante o registro de uma face, o sistema captura automaticamente uma foto como foto de perfil. Se você não registrar uma foto de perfil, o sistema definirá automaticamente a foto capturada durante o registro como a foto padrão.

➢ Registrar Palma ★

Na interface atual, atrás da barra de palma, clique em **Registrar** e o dispositivo exibirá a interface de registro de palma em tempo real.

➢ **Registrar Impressão Digital ★**

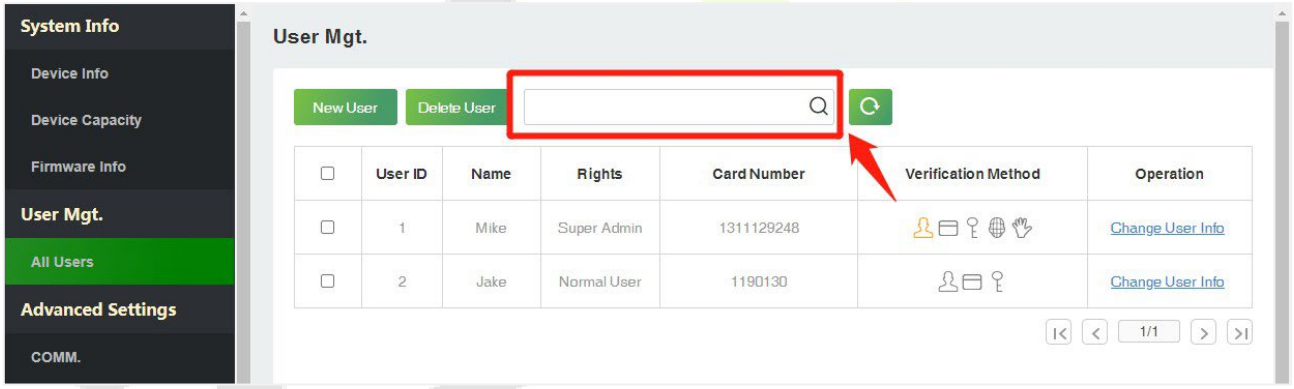
Na interface atual, atrás da barra de impressão digital, clique em **Registrar** e o dispositivo exibirá a interface de registro de impressão digital em tempo real. Pressione o seu dedo no sensor de impressão digital do dispositivo e siga as instruções para completar o registro.



Para a operação de pressionar a impressão digital, por favor, consulte a Posição do dedo.

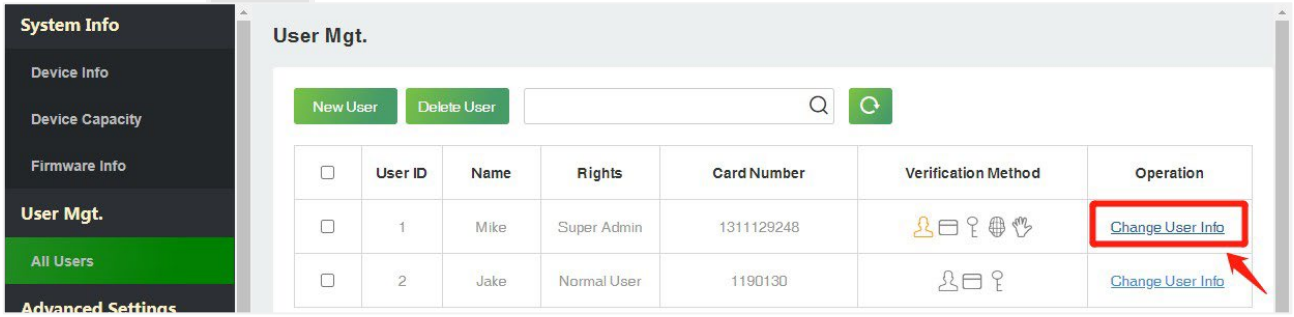
8.2 Buscar Usuários

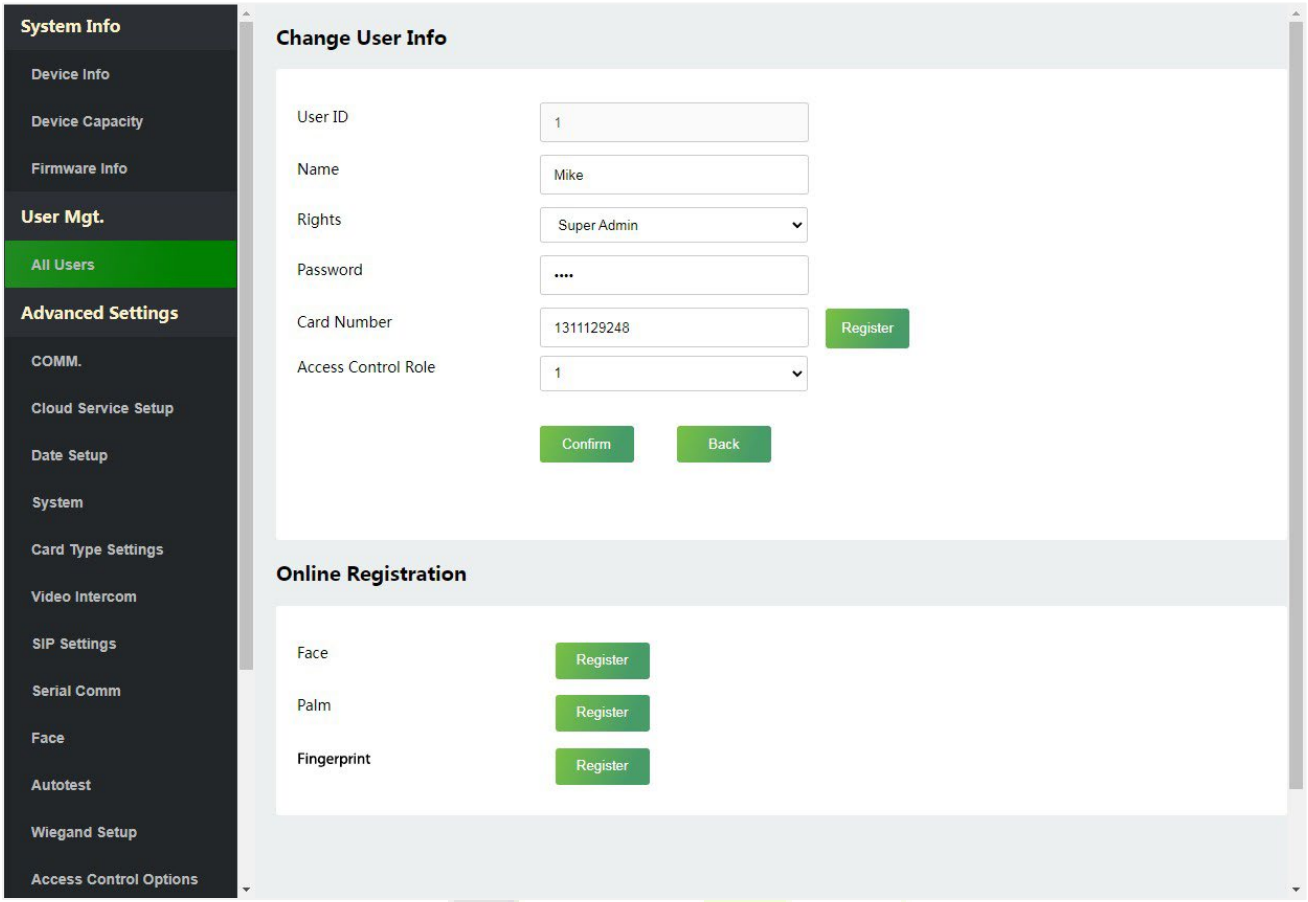
Clique em **Todos os Usuários** no **Servidor Web**, clique na barra de pesquisa para inserir a palavra-chave de busca necessária (onde a palavra-chave pode ser o ID do usuário, sobrenome ou nome completo) e o sistema irá procurar pelas informações do usuário relacionadas.



8.3 Editar Usuário

Na interface **Todos os Usuários**, selecione o usuário necessário da lista e clique em Alterar Informações do Usuário para editar as informações do usuário.

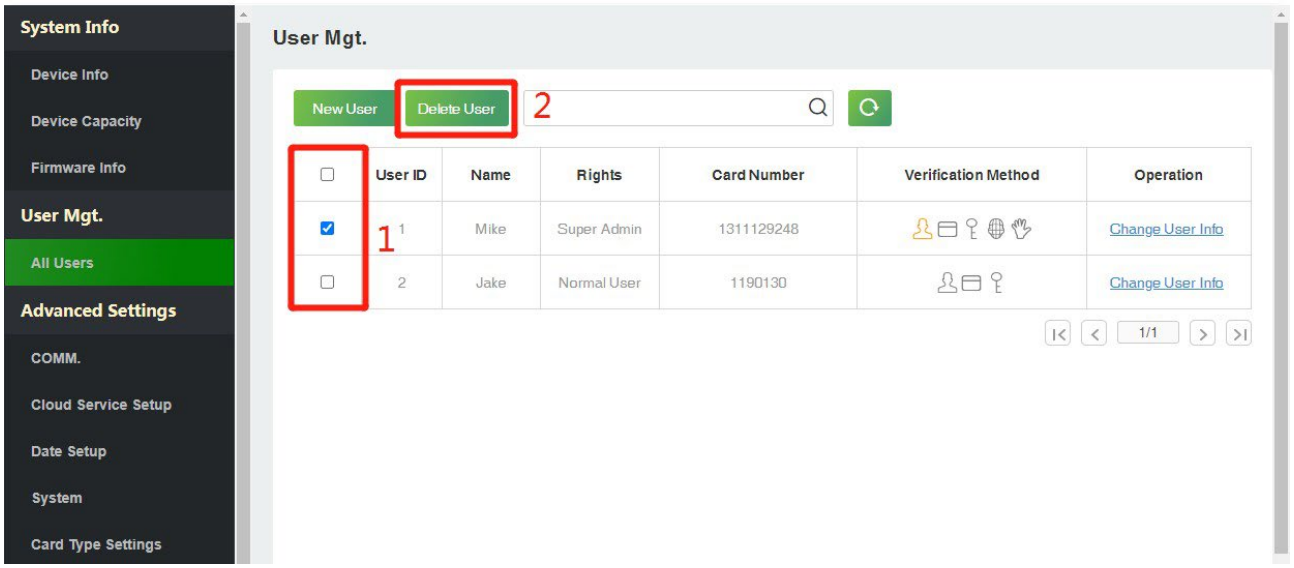




Observação: O processo de edição das informações do usuário é o mesmo que adicionar um novo usuário, exceto que o ID do usuário não pode ser modificado. O processo detalhado pode ser encontrado na seção 8.1 Registro do Usuário.

8.4 Excluir Usuário

Na interface **Todos os Usuários**, selecione o usuário necessário da lista e clique em **Excluir Usuário** para remover o usuário. Aqui, é possível realizar a exclusão individual ou em lote.

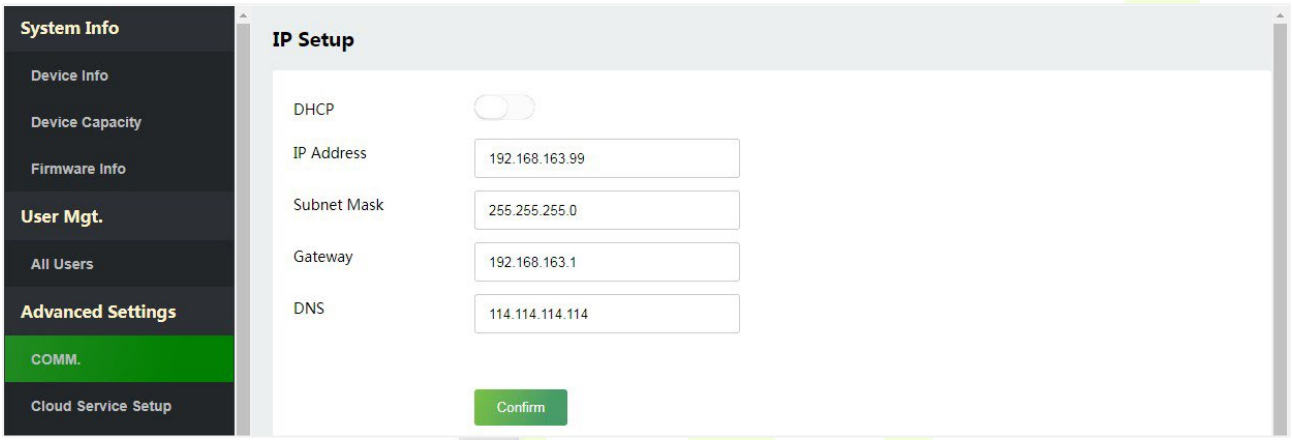


9 Configurações Avançadas

9.1 Configurações de Comunicação

Clique em **Config. Com.** no **Servidor Web**.

Altere o endereço IP do dispositivo conforme necessário, clique em **Confirmar** para salvar e o dispositivo irá sincronizar automaticamente as informações de IP.



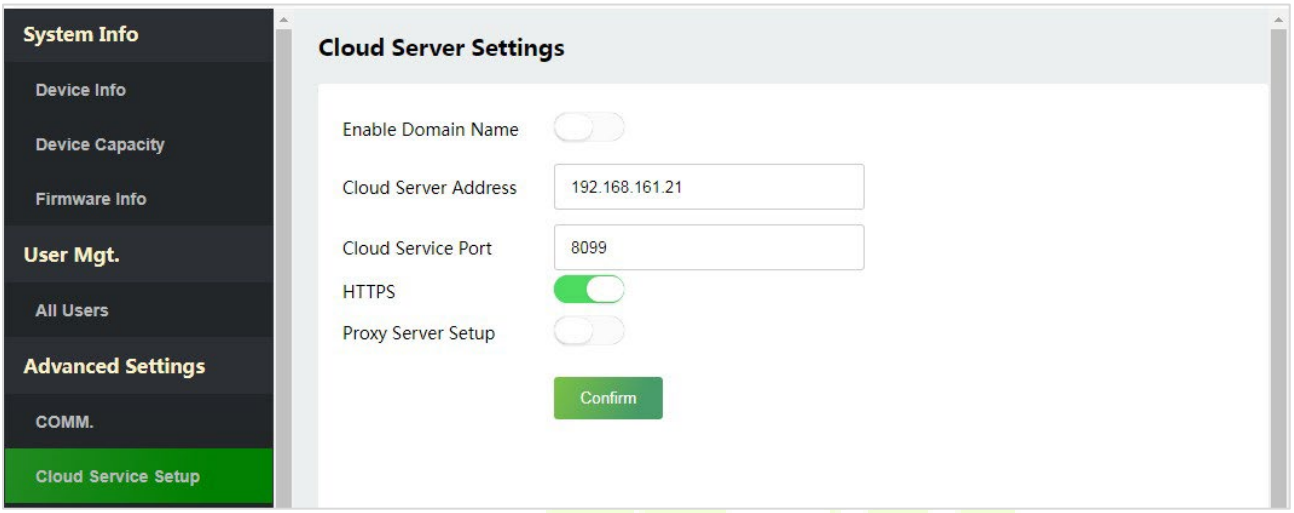
Função	Descrição
DHCP	Selecione se deseja obter o endereço IP automaticamente.
Endereço IP	O endereço IP padrão é 192.168.1.201. Ele pode ser modificado de acordo com a disponibilidade da rede.
Máscara de Sub-rede	A máscara de sub-rede padrão é 255.255.255.0. Ela pode ser modificada de acordo com a disponibilidade da rede.
Gateway	O endereço de 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.

Observação: Após alterar com sucesso o endereço IP do dispositivo, é necessário fazer logout do Servidor Web atual e fazer login novamente no endereço IP recém-modificado para se conectar ao dispositivo. Para obter detalhes de login do Servidor Web, consulte o Login do Servidor Web.

9.2 Configuração do Servidor em Nuvem

Clique em **Configuração do Serviço em Nuvem** no Servidor Web.

A Configuração do Servidor em Nuvem é usada para se conectar ao software ZKBio CVSecurity, por favor, consulte a seção 12.1 Configurar o Endereço de Comunicação.

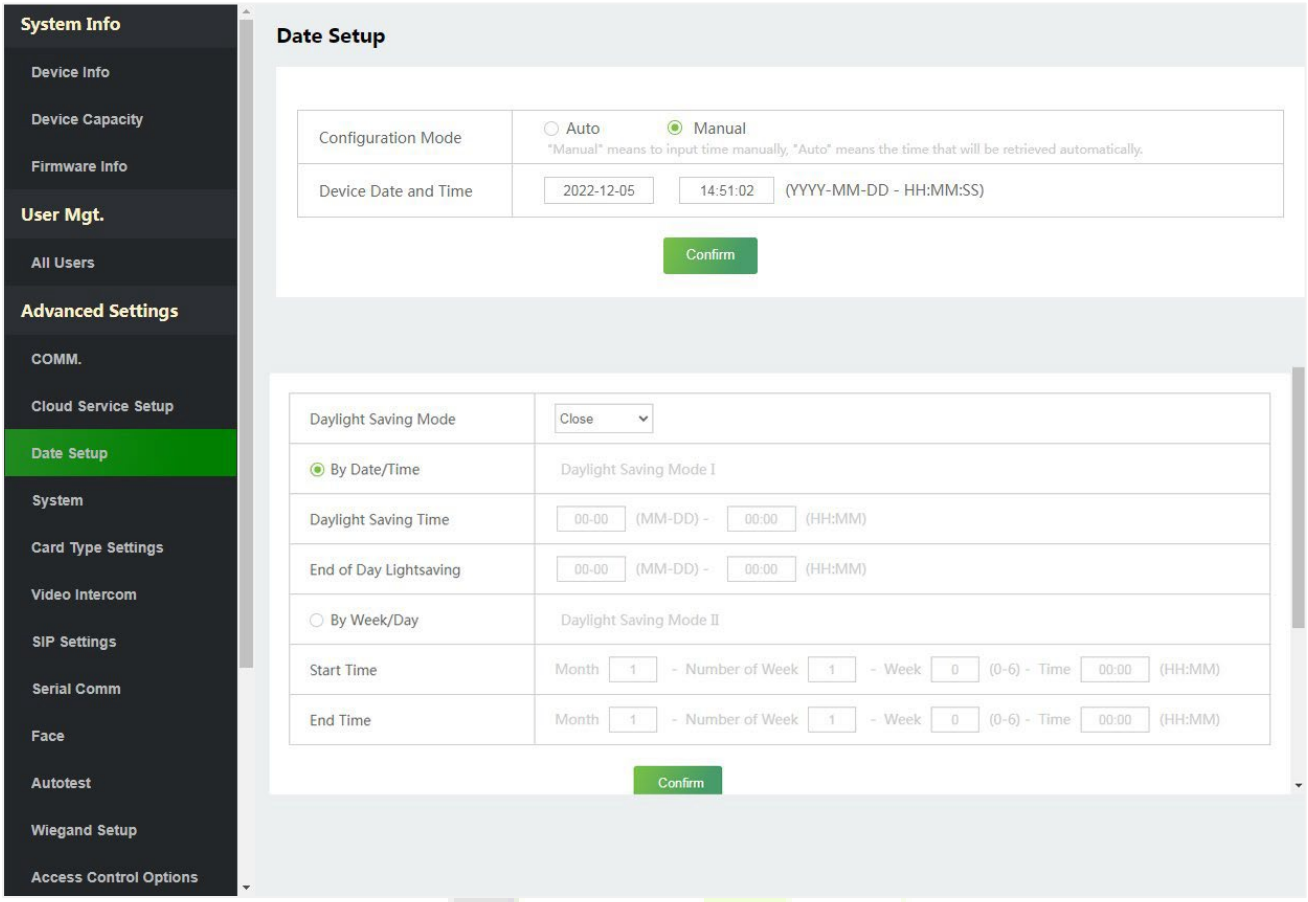


Função		Descrição
Habilitar Nome de Domínio	**Endereço do Servidor**	Uma vez que essa função seja habilitada, o modo de nome de domínio "http://..." será usado, como por exemplo http://www.XYZ.com, onde "XYZ" representa o nome de domínio (quando esse modo estiver ativado).
Desabilitar Nome de Domínio	**Endereço do Servidor**	Endereço IP do servidor ADMS.
	Porta do Servidor	Porta usada pelo servidor ADMS.
HTTPS		Baseado em HTTP, a criptografia da transmissão e a autenticação de identidade garantem a segurança do processo de transmissão.
Configuração do Servidor Proxy		Quando você escolhe habilitar o proxy, é necessário configurar o endereço IP e o número da porta do servidor proxy.

9.3 Configuração de Data

Clique em **Configuração de Data** no Servidor Web.

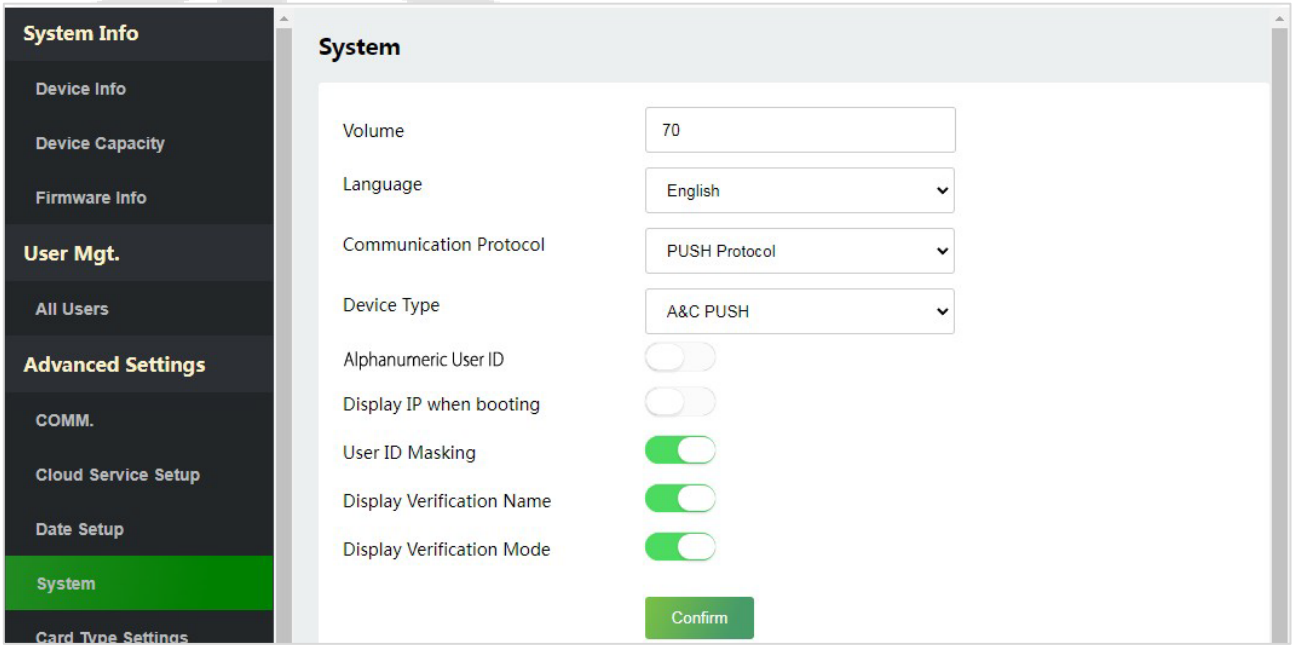
- Clique em **Manual** para configurar manualmente a data e a hora e clique em **Confirmar** para salvar.
- Selecione **Abrir** ou **Fechar** a **função de Horário de Verão.** Se estiver aberto, defina o Horário de Verão e o Fim do Horário de Verão.



9.4 Configurações do Sistema

Clique em **Sistema** no **Servidor Web**.

Isso permite configurar os parâmetros do sistema relacionados para otimizar a acessibilidade do dispositivo.



Função	Descrição
Volume	Ajuste o volume do dispositivo, que pode ser configurado entre 0 e 100.
Idioma	Selecione o idioma do Servidor Web e do dispositivo.
Protocolo de Comunicação	Configure o protocolo de comunicação do dispositivo.
Tipo de Dispositivo	Configure o dispositivo como um terminal de controle de acesso ou terminal de registro de presença. ***Observação:*** Após alterar o tipo de dispositivo, todos os dados do dispositivo serão excluídos e reiniciados, e algumas funções serão ajustadas de acordo.
ID Alfanumérico do Usuário	Habilitar/Desabilitar o uso de ID de usuário alfanumérico.
Exibir endereço IP durante a inicialização	Habilitar/Desabilitar a função de exibir o endereço IP durante a inicialização.
Mascaramento do ID do Usuário	Quando habilitado, e o usuário é 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	Defina se deseja exibir o nome de usuário na interface de resultado de verificação.
Exibir Modo de Verificação	Defina se deseja exibir o modo de verificação na interface de resultado de verificação.

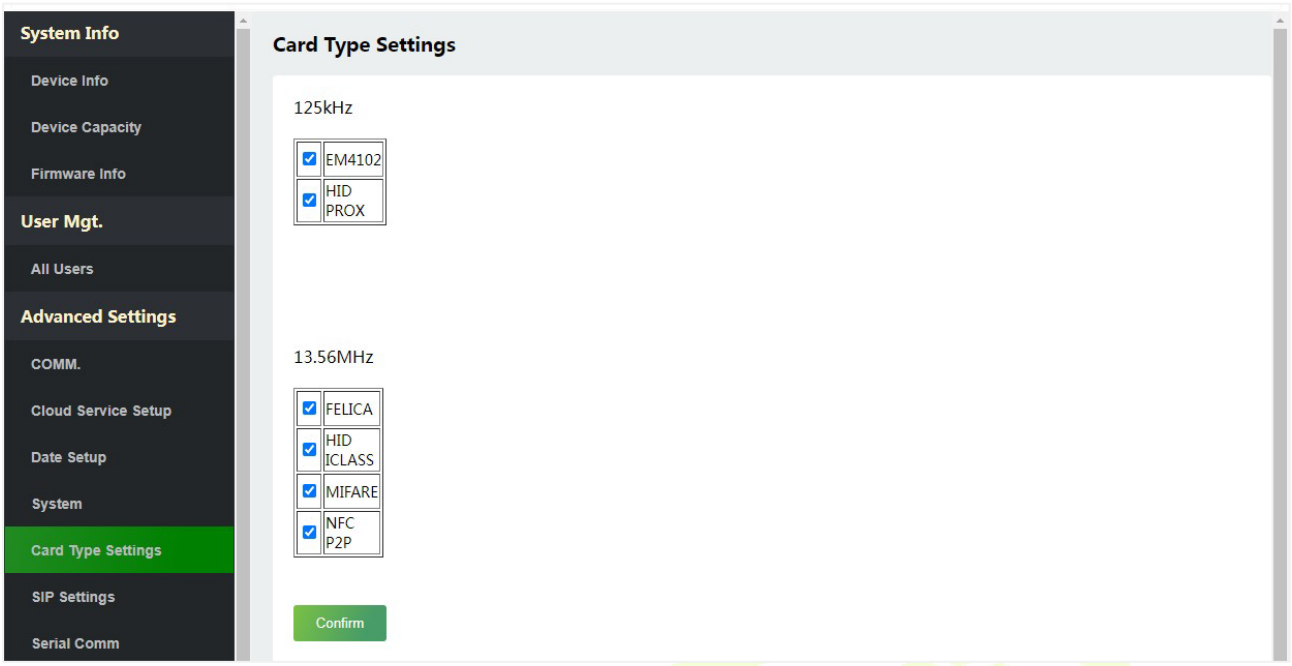
Observação:

1. Após selecionar o idioma e clicar em **Confirmar**, o dispositivo será reiniciado automaticamente e exibirá o idioma alterado.
2. Em seguida, o Servidor Web não exibirá o idioma alterado até que o dispositivo seja reiniciado e faça login novamente.

9.5 Configurações de Tipo de Cartão

Clique em **Configurações de Tipo de Cartão** no Servidor Web.

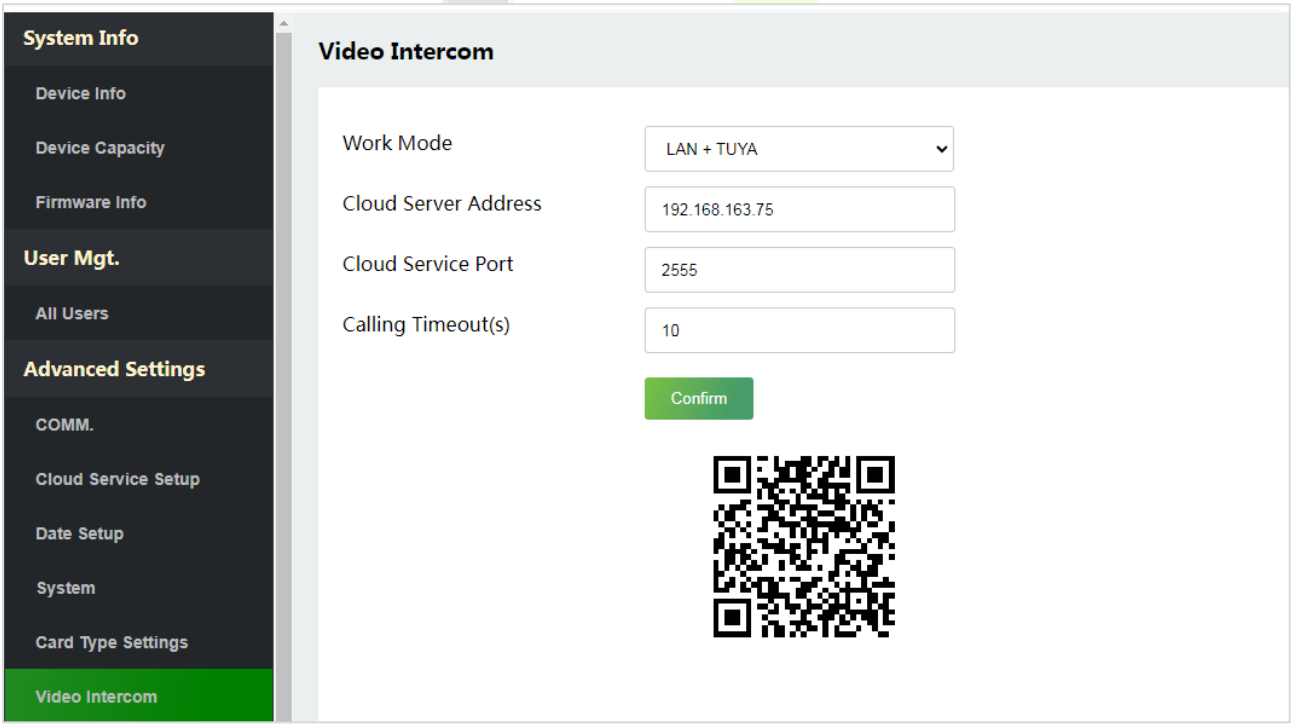
O dispositivo suporta cartões nas frequências de 125kHz e 13.56MHz. Por favor, selecione o tipo de cartão correspondente de acordo com suas necessidades.



9.6 Intercomunicador de Vídeo★

Clique em **Intercomunicador de Vídeo** no **Servidor Web**.

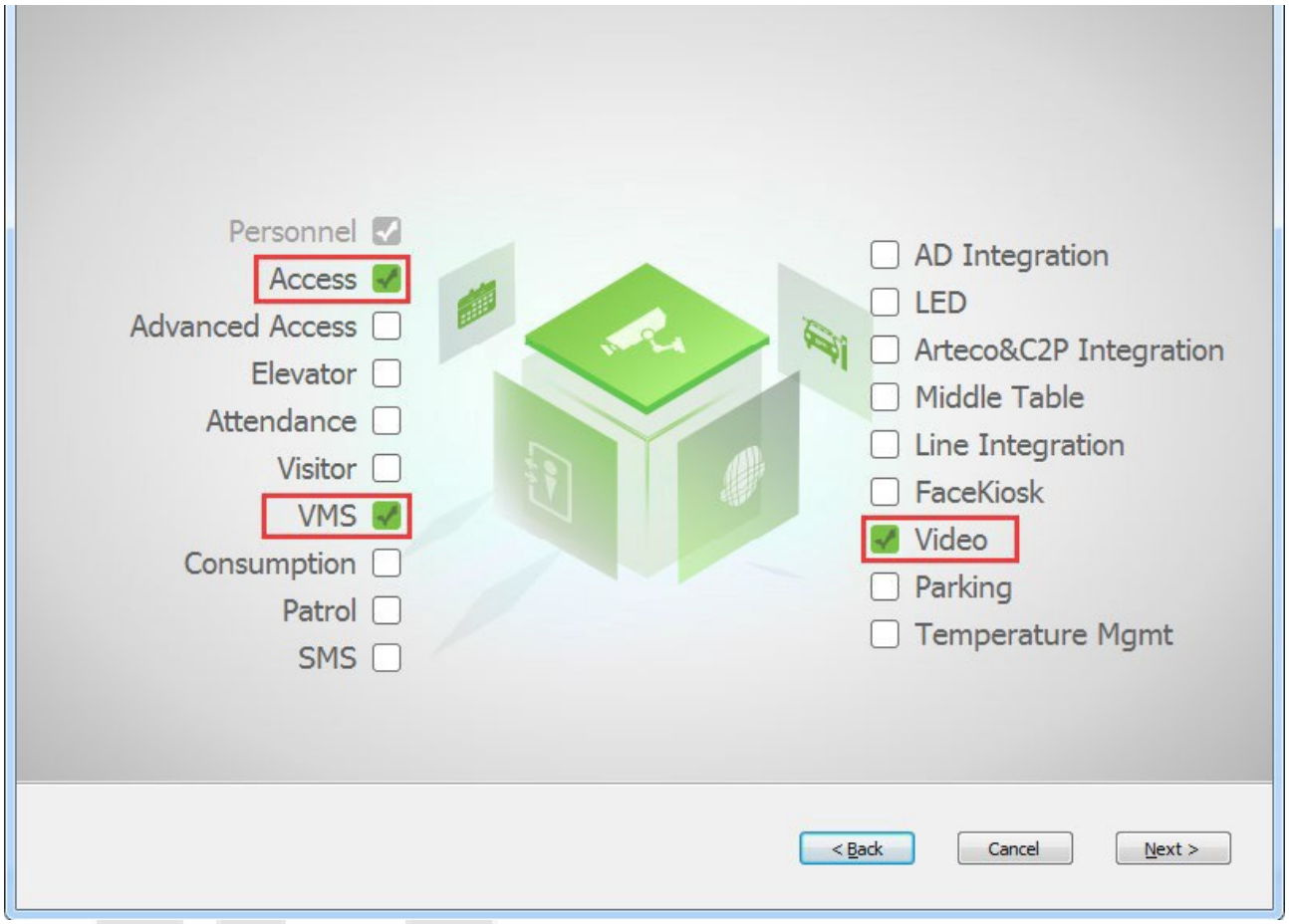
A função de intercomunicador de vídeo suporta LAN e WAN, sendo a LAN adequada para PC e a WAN adequada para celular.



9.6.1 Configurações da Função de Intercomunicador de Vídeo na LAN

1. Instalando o Plugin ZKBio VMS no Software ZKBio CVSecurity

Durante a instalação, selecione o módulo "VMS" do software ZKBio CVSecurity para instalar, conforme mostrado na seguinte interface de instalação.



Observação: O módulo de vídeo e o módulo VMS não podem ser selecionados ao mesmo tempo.

Dê um clique duplo no arquivo fornecido **ZKBioVMSPlugin_sqlite.exe** para instalar o Plugin ZKBio VMS.

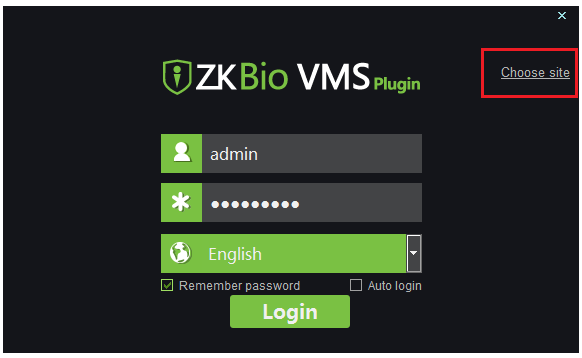
Observação: O software ZKBio CVSecurity e o Plugin ZKBio VMS precisam ser abertos simultaneamente para reconhecer a função de intercomunicador.

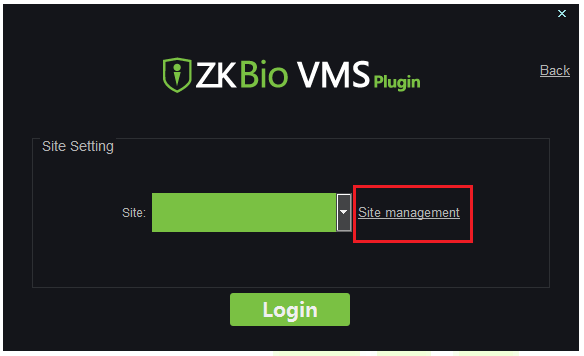
2. Parâmetros de Configuração

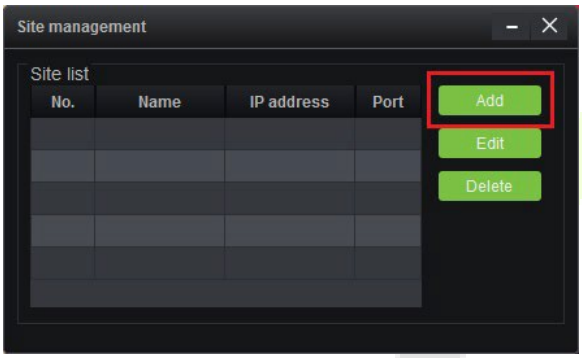
Configure corretamente os parâmetros necessários para garantir uma conexão entre o dispositivo e o software.

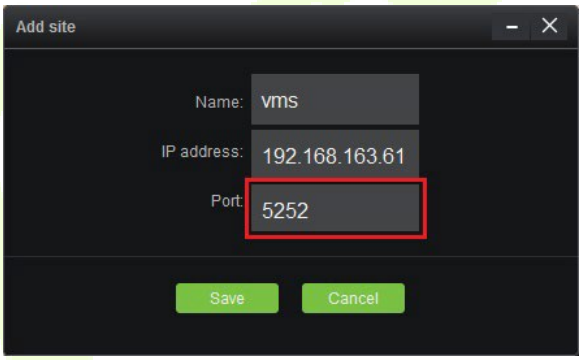
- **Adicione o site no plugin Video-VMS**

1) Clique duas vezes no ícone para abrir o Plugin Video-VMS. Clique em Escolher site > Gerenciamento de site > Adicionar na interface de login. Em seguida, insira o Nome, Endereço IP e Porta para adicionar um site, conforme mostrado na figura a seguir.





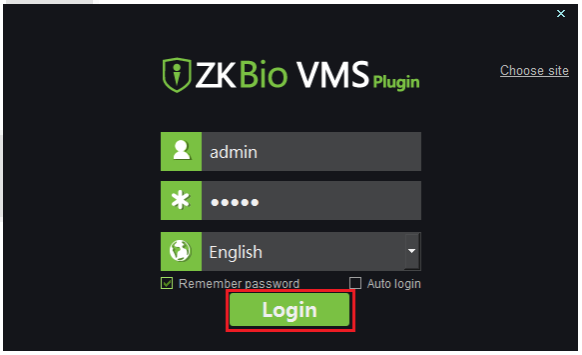




✓ **Endereço IP:** Insira o endereço IP local.

✓ **Porta:** A porta padrão é 5252.

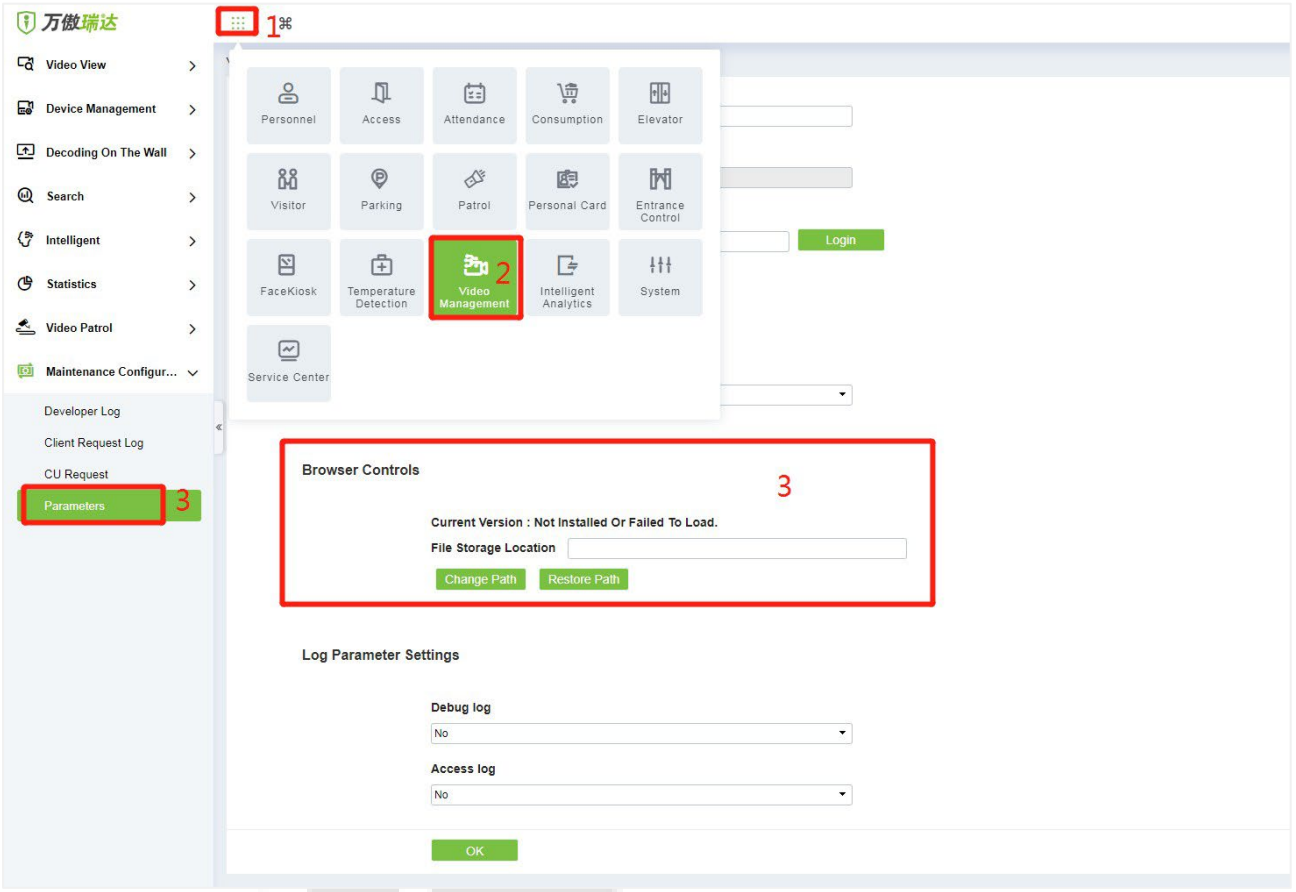
2) Digite o nome de usuário e a senha após adicionar o site e clique em **Login** para acessar o plugin Video-VMS. O nome de usuário e a senha inicial são ambos **admin**.



Observação: Quando o plugin Video-VMS estiver conectado com sucesso ao ZKBio CVSecurity, a senha é alterada sincronamente para a senha do usuário admin do ZKBio CVSecurity.

- **Configurar o caminho de conexão do ZKBio CVSecurity e do plugin VMS**

Clique em **Vídeo** > **Configuração de manutenção** > **Controles do navegador** software ZKBio CVSecurity para alterar o caminho, conforme mostrado na imagem a seguir:



Caminho de Conexão do VMS

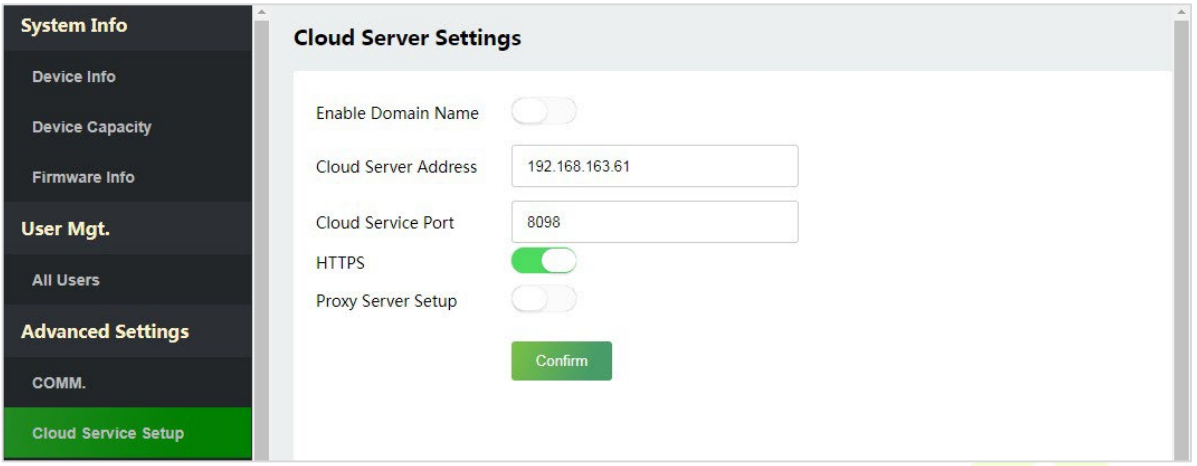
- ✓ **URL:** "http://local IP address: port"
- ✓ **Porta:** Por padrão, é **8489** (por exemplo, http://192.168.163.61:8489).

Caminho do Servidor

- ✓ **URL:** "http://server IP address: port"
- ✓ **Porta:** A porta é a porta de serviço definida durante a instalação (por exemplo, http://192.168.163.61:8098) (não a porta ADMS).

- **Configure os parâmetros no ProMA**

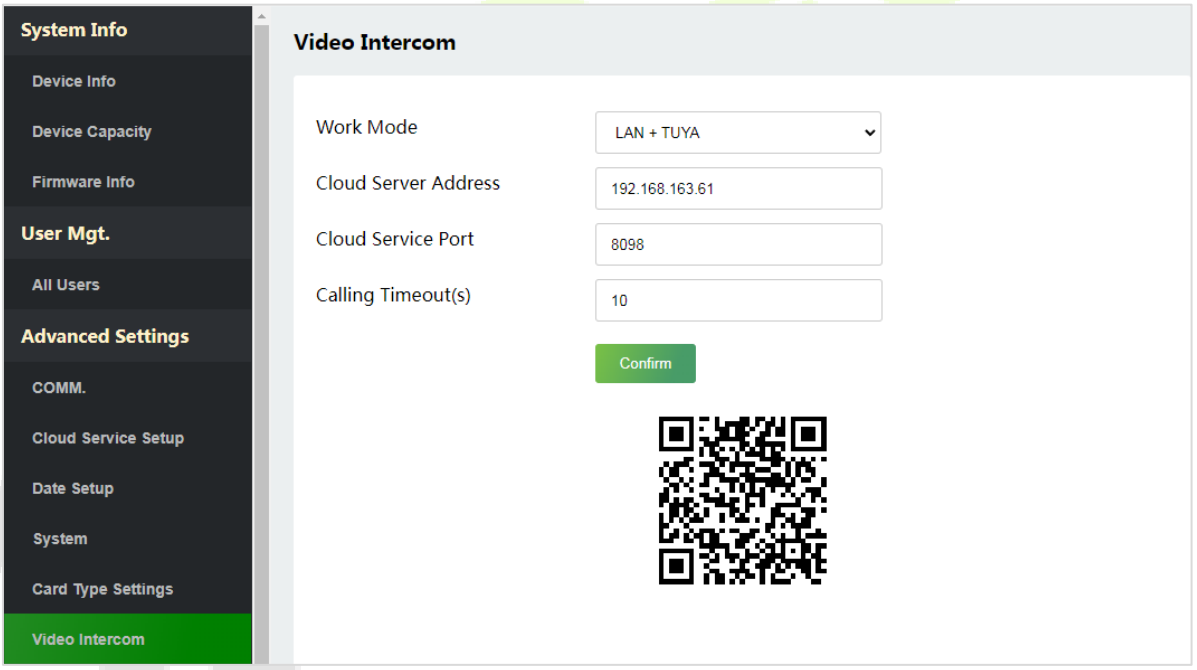
1) Clique em **Configuração do Servidor de Nuvem** no Servidor Web para definir o endereço do servidor e a porta do servidor, ou seja, o endereço IP e o número da porta do servidor após a instalação do software. Se o dispositivo se comunicar com o servidor com sucesso, o ícone será exibido no canto superior direito da interface de espera.



2) Clique em **Intercomunicador de Vídeo** para definir o endereço do servidor e a porta do servidor.

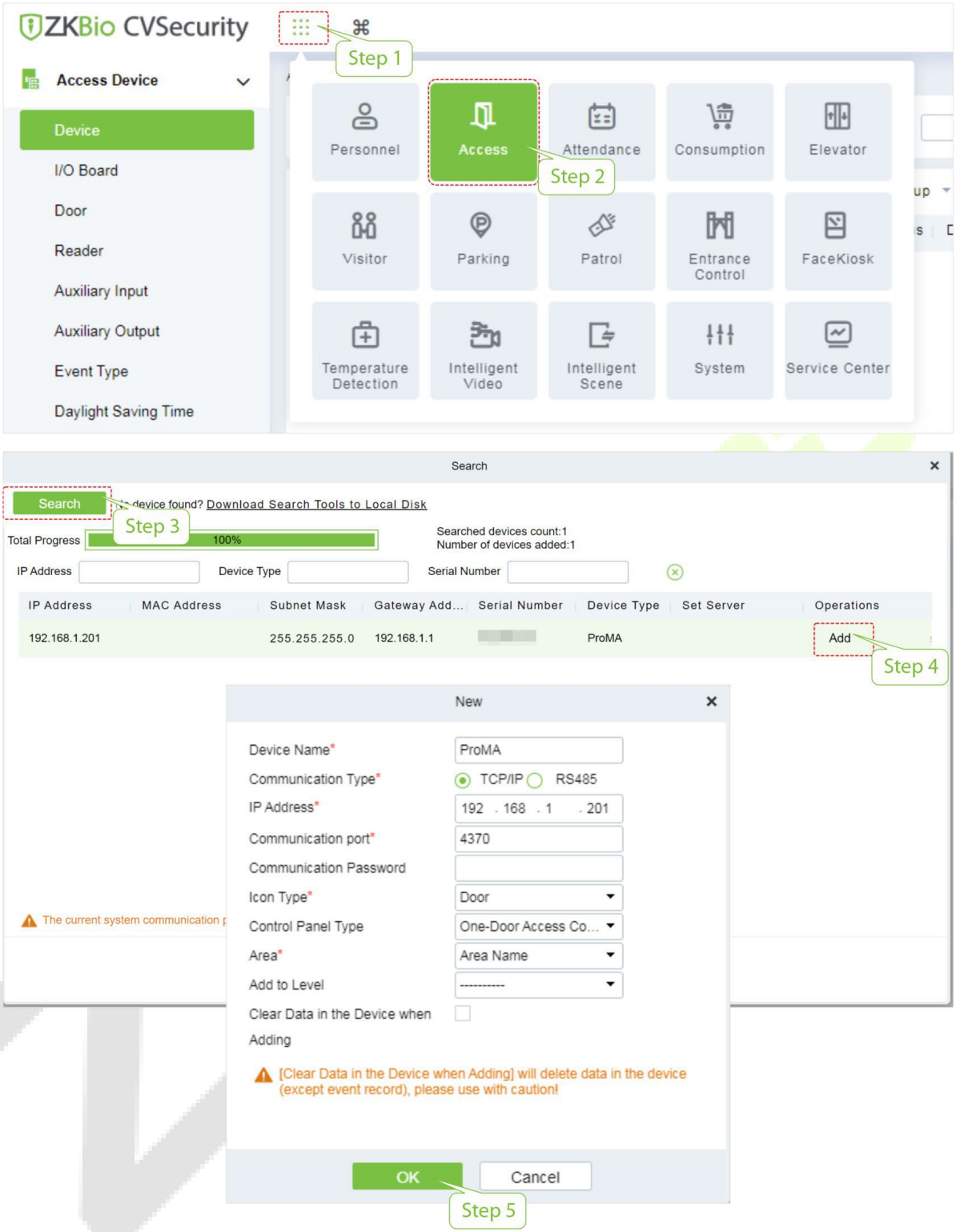
✓ **Endereço do Servidor de Nuvem:** Insira o endereço IP da instalação do ZKBio CVSecurity.

✓ **Porta do Servidor de Nuvem:** A porta é a porta de serviço definida durante a instalação (não a porta ADMS).

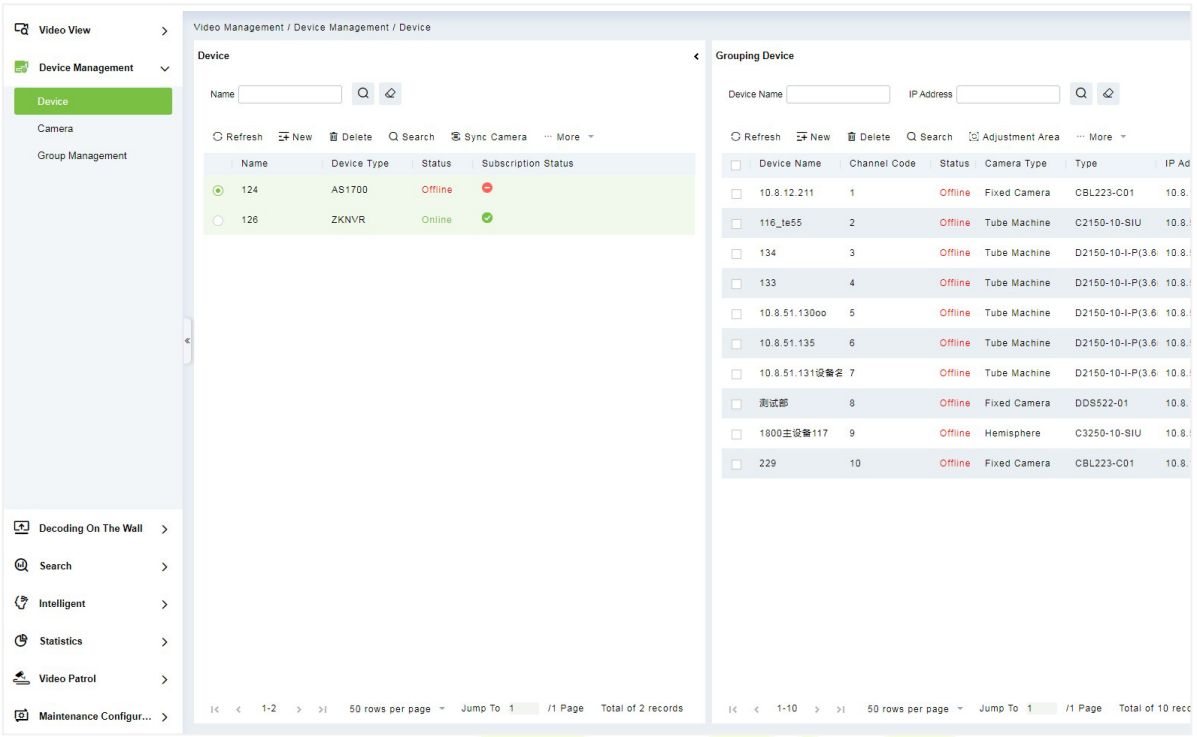


- **Adicionando dispositivo no software ZKBio CVSecurity.**

1) Clique em **Acesso > Dispositivo > Dispositivo > Pesquisar** para adicionar o dispositivo no software ZKBio CVSecurity.



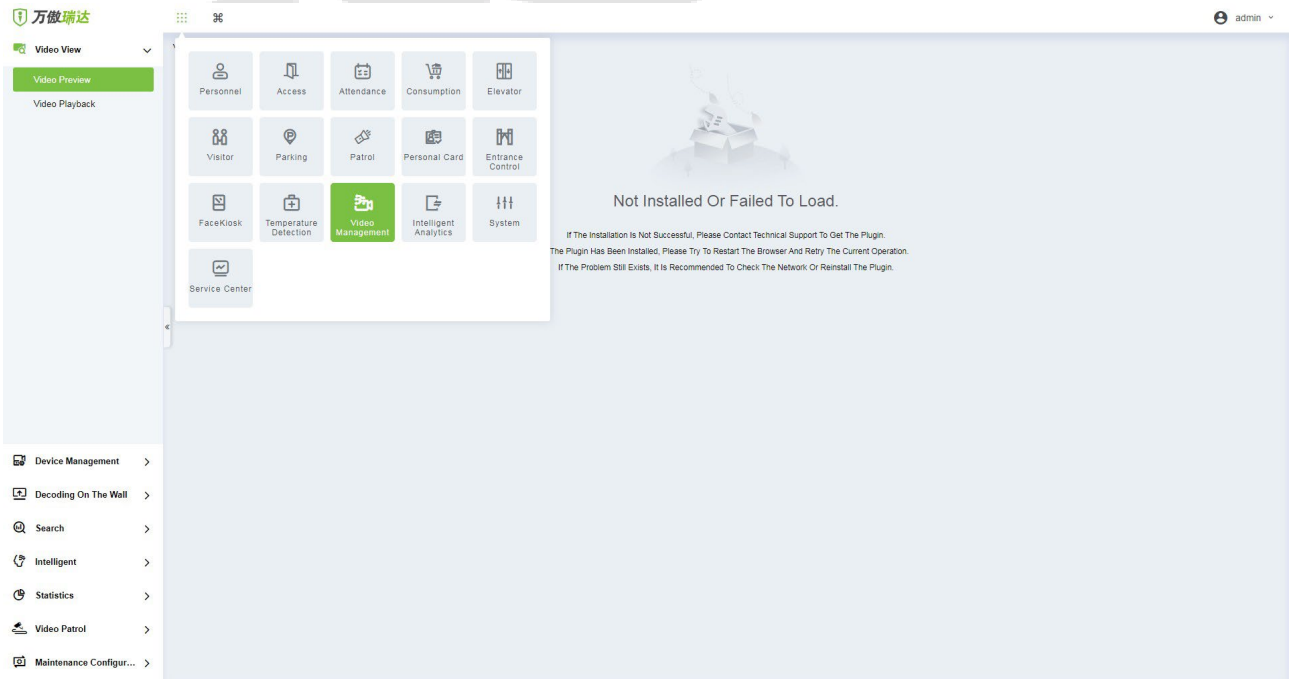
2) Após o dispositivo ser adicionado com sucesso ao módulo de acesso, ele é automaticamente adicionado ao módulo de vídeo. O usuário pode clicar em **Vídeo** > **Dispositivo de Vídeo** > **Pesquisar** para visualizar.



Observação: Se o dispositivo não for adicionado ao módulo de vídeo, verifique se as configurações dos parâmetros estão corretas.

3. Visualização de Vídeo no Software ZKBio CVSecurity.

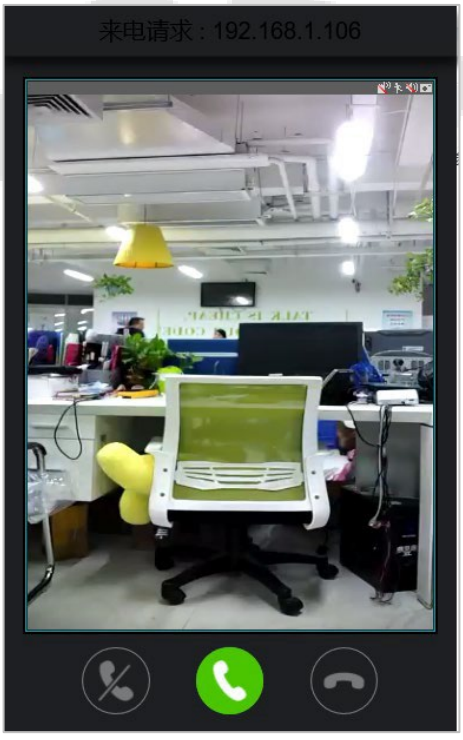
Clique em **Vídeo** > **Visualização de Vídeo** para acessar a interface de visualização do dispositivo.

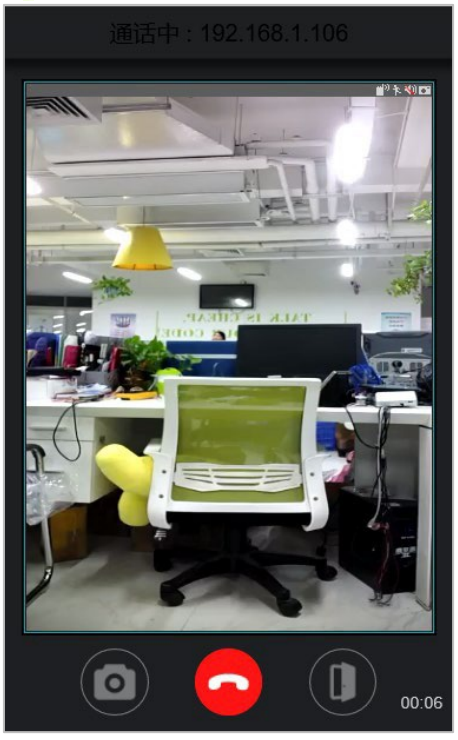


4. Realizar uma Chamada no Dispositivo

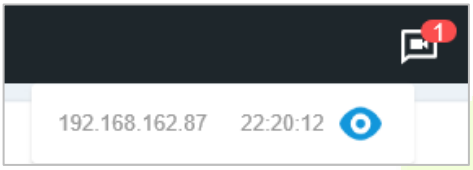
1) Toque no ícone no ProMA para fazer uma chamada.

2) A página do servidor abre automaticamente a janela de chamada por padrão, conforme mostrado na figura a seguir.





Function Description

Função	Descrição
	É a tecla Atender, o usuário pode clicar para atender a chamada atual. Após atender, entre na janela durante a chamada e ligue o áudio e o vídeo por padrão.
	É a tecla Desligar. Após desligar, a chamada é encerrada imediatamente.
	É a tecla Ignorar, usada para ignorar a chamada atual. Clique nela para fechar a janela de chamada, e o ícone  no canto superior direito exibirá o número de chamadas pendentes  . O usuário pode clicar no ícone no menu suspenso para abrir novamente a janela de chamada do dispositivo atual e escolher responder, como mostrado na figura a seguir. 
	É a tecla Desligar, usada para encerrar a chamada atual.
	É a tecla Captura de Instantâneo, usada para tirar uma foto instantânea.
	É a tecla Abrir Remotamente, usada para abrir a porta remotamente. O tempo padrão de acionamento da fechadura é de 5 segundos.

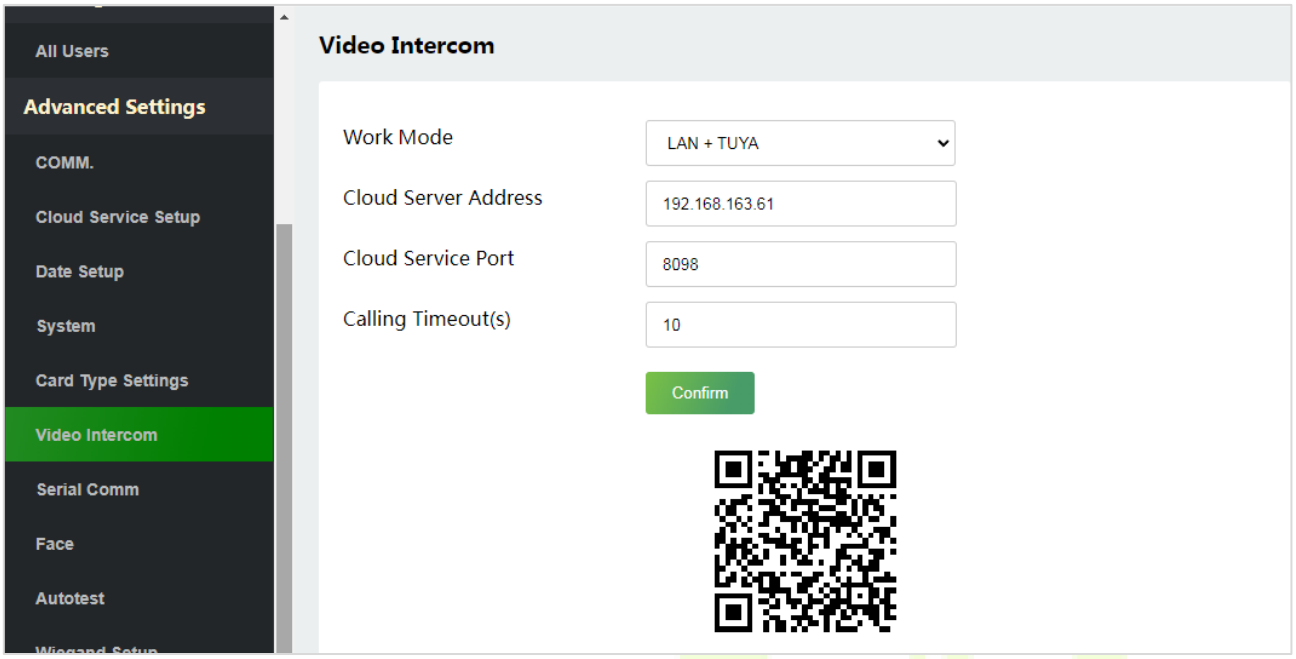
Observação: Se a interface de visualização do dispositivo estiver aberta no software ZKBio CVSecurity, a interface de chamada não será mais exibida nesta janela de chamada.

9.6.2 Conectando ao Software ZKBio Talk

Faça o download e instale o software ZKBio Talk. Em seguida, mantenha as configurações de parâmetros do software ZKBio CVSecurity inalteradas para as configurações relevantes. (Consulte as Configurações de Função de Intercomunicador de Vídeo LAN).

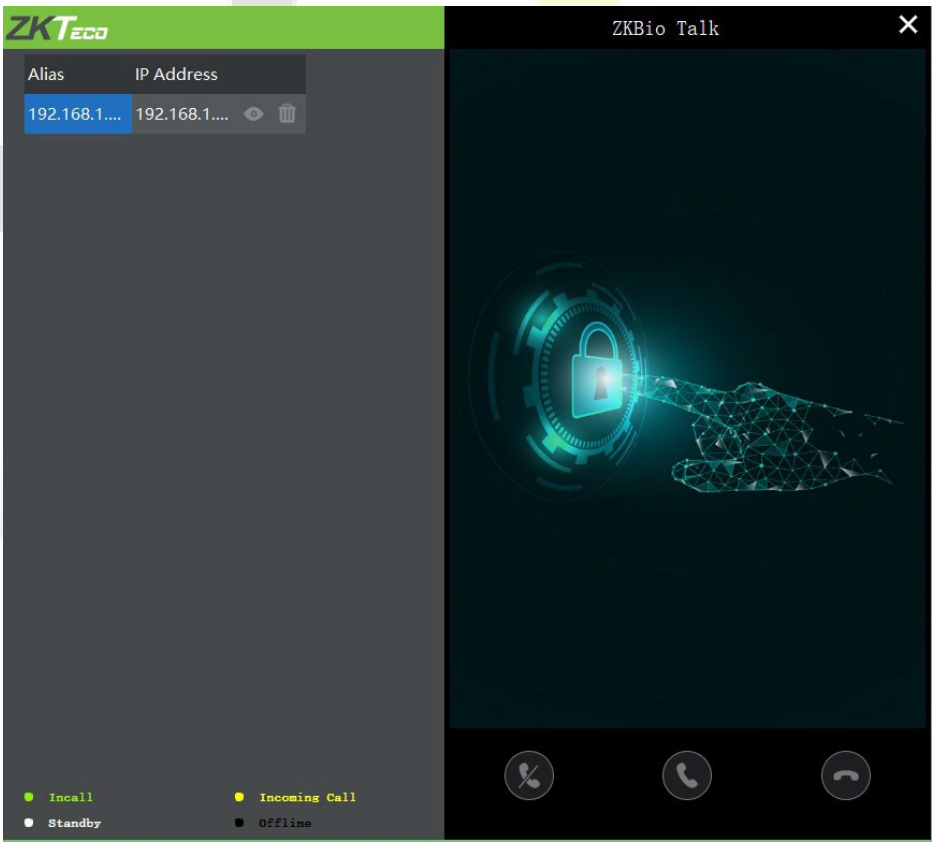
A seguir estão os passos para conectar o ZKBio Talk ao software ZKBio CVSecurity:

1. Primeiramente, altere o parâmetro no ProMA. Clique em Interfone de Vídeo no WebServer para alterar o endereço do servidor e a porta do servidor, conforme mostrado na figura a seguir.

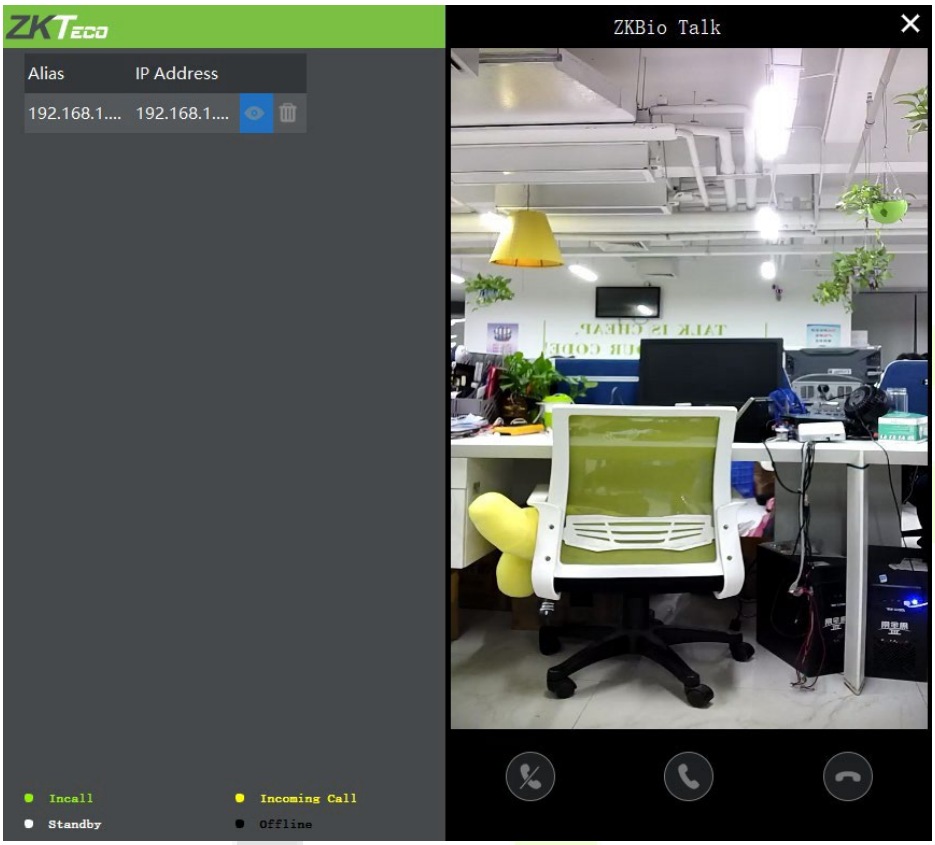


- ✓ **Endereço do Servidor:** Digite o endereço IP atual da instalação do servidor
- ✓ **Porta do Servidor:** A porta padrão do servidor é **25550**.

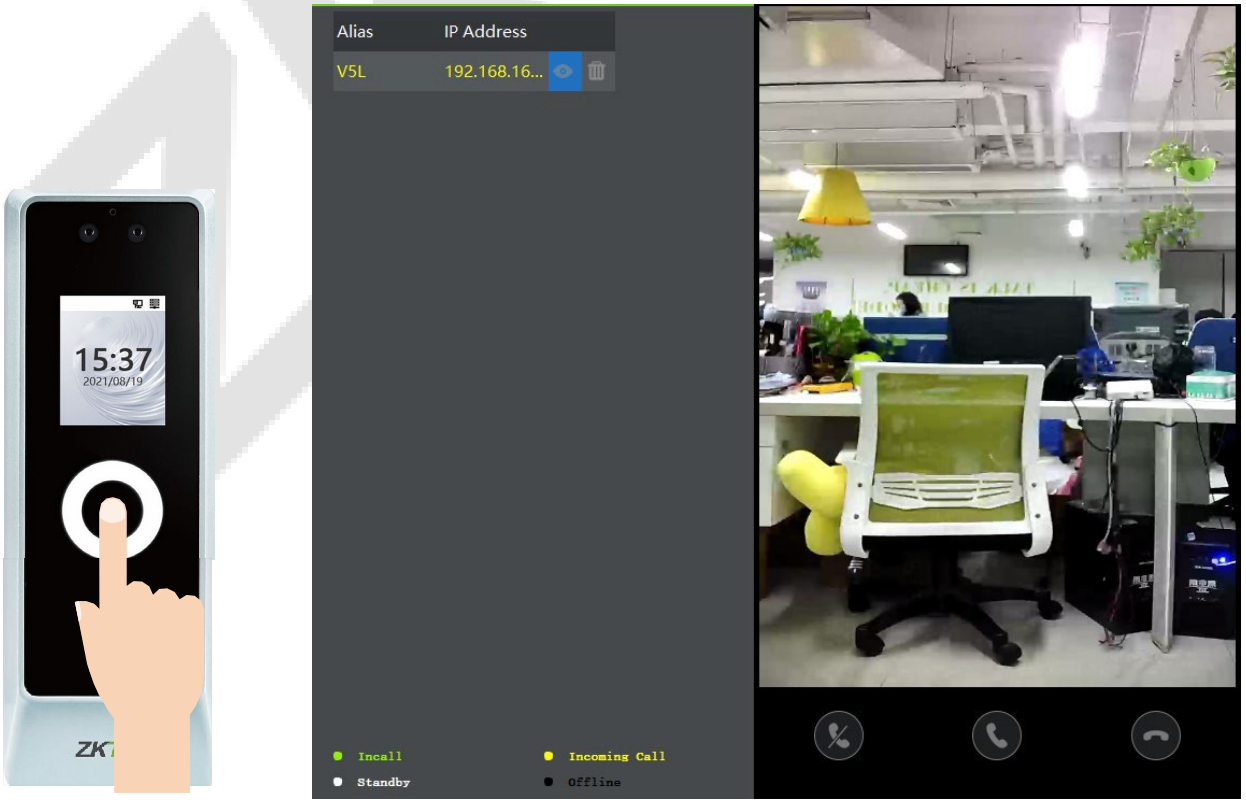
2. Clique duas vezes no ícone para abrir o software ZKBio Talk. Quando os parâmetros de intercomunicador de vídeo do dispositivo estiverem configurados corretamente, o dispositivo automaticamente envia a lista de dispositivos à esquerda, como mostrado na figura a seguir.



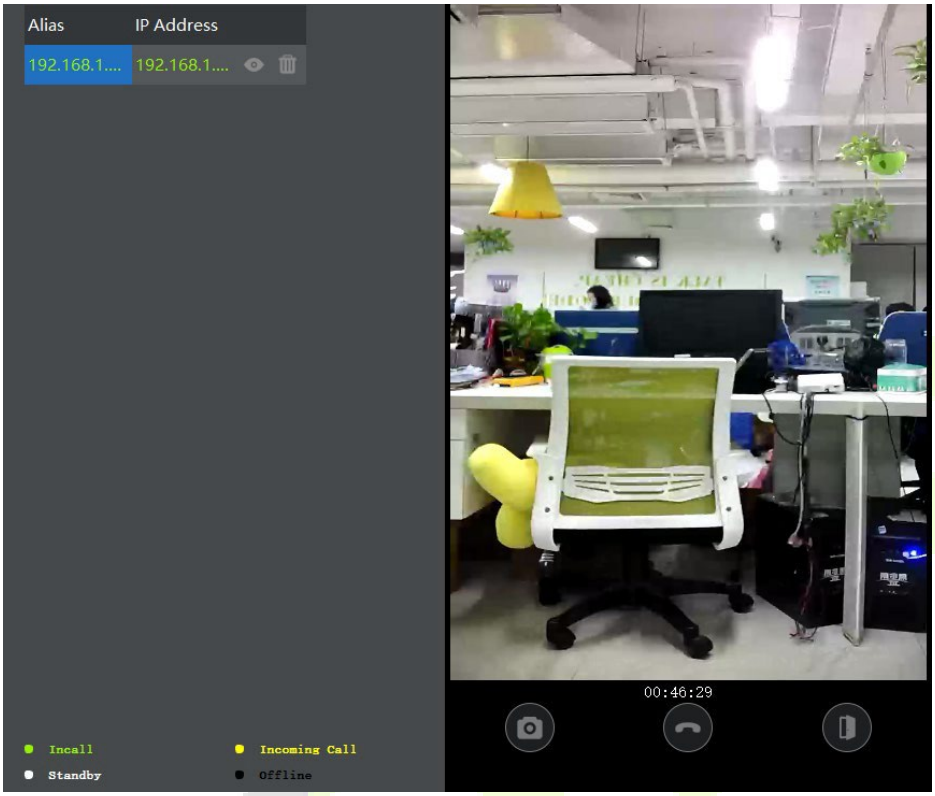
3. Um usuário pode clicar em para visualizar o vídeo à direita. Ao clicar no ícone ou , um usuário pode fechar a tela de visualização. Nenhuma ação é realizada quando é clicado.



4. Quando um usuário toca no ícone no ProMA para fazer uma chamada, a interface do software exibe o endereço IP do dispositivo chamador em amarelo.



5. Quando o usuário clica no ícone para atender a chamada, o endereço IP é exibido em verde durante a chamada. A duração da chamada também é exibida logo acima do ícone.



Descrição da Função

Função	Descrição
	É a tecla de Snapshot, usada para tirar uma foto instantânea.
	É a tecla de Abertura Remota, usada para abrir a porta remotamente. O tempo padrão de acionamento da fechadura é de 5 segundos.

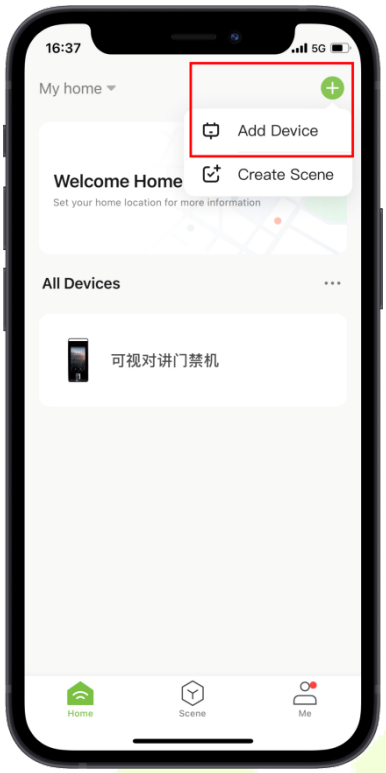
9.6.3 Conectando ao aplicativo ZSmart

- **Adicionando dispositivo no aplicativo ZSmart**

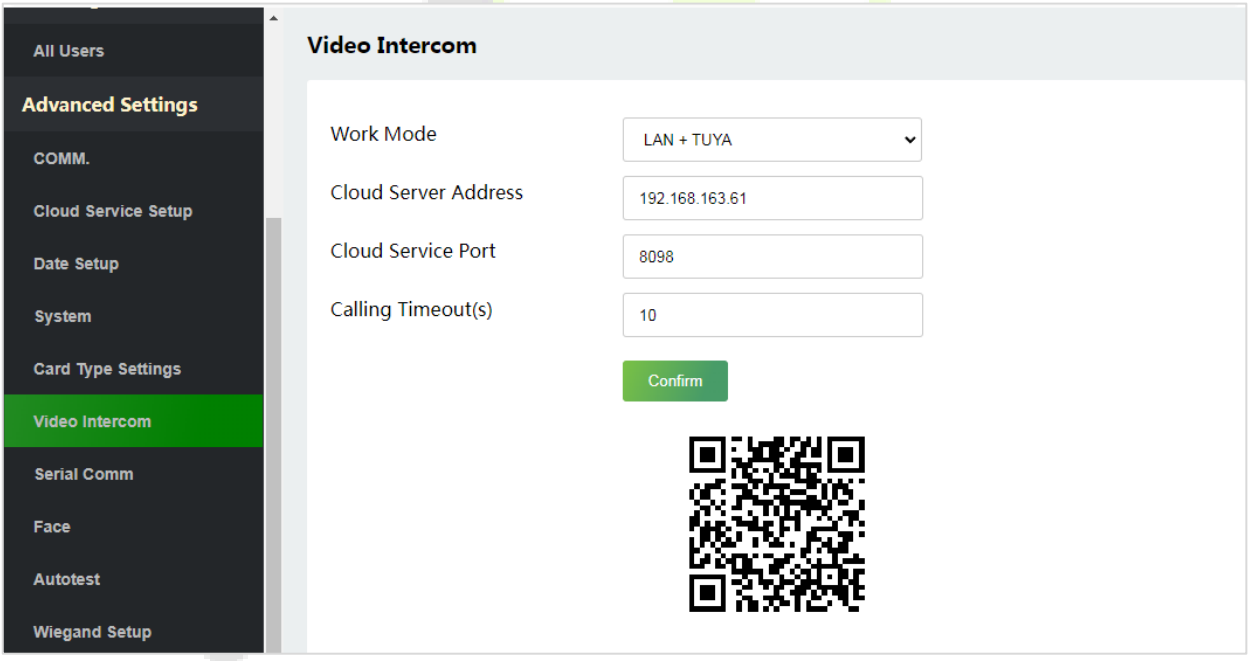
Após baixar e instalar o aplicativo ZSmart em seu telefone, crie uma conta de usuário inicialmente com seu endereço de e-mail. Após criar a conta de usuário, faça login no aplicativo e toque no ícone 

ou  no canto superior direito da tela para adicionar um dispositivo. O processo é o seguinte:

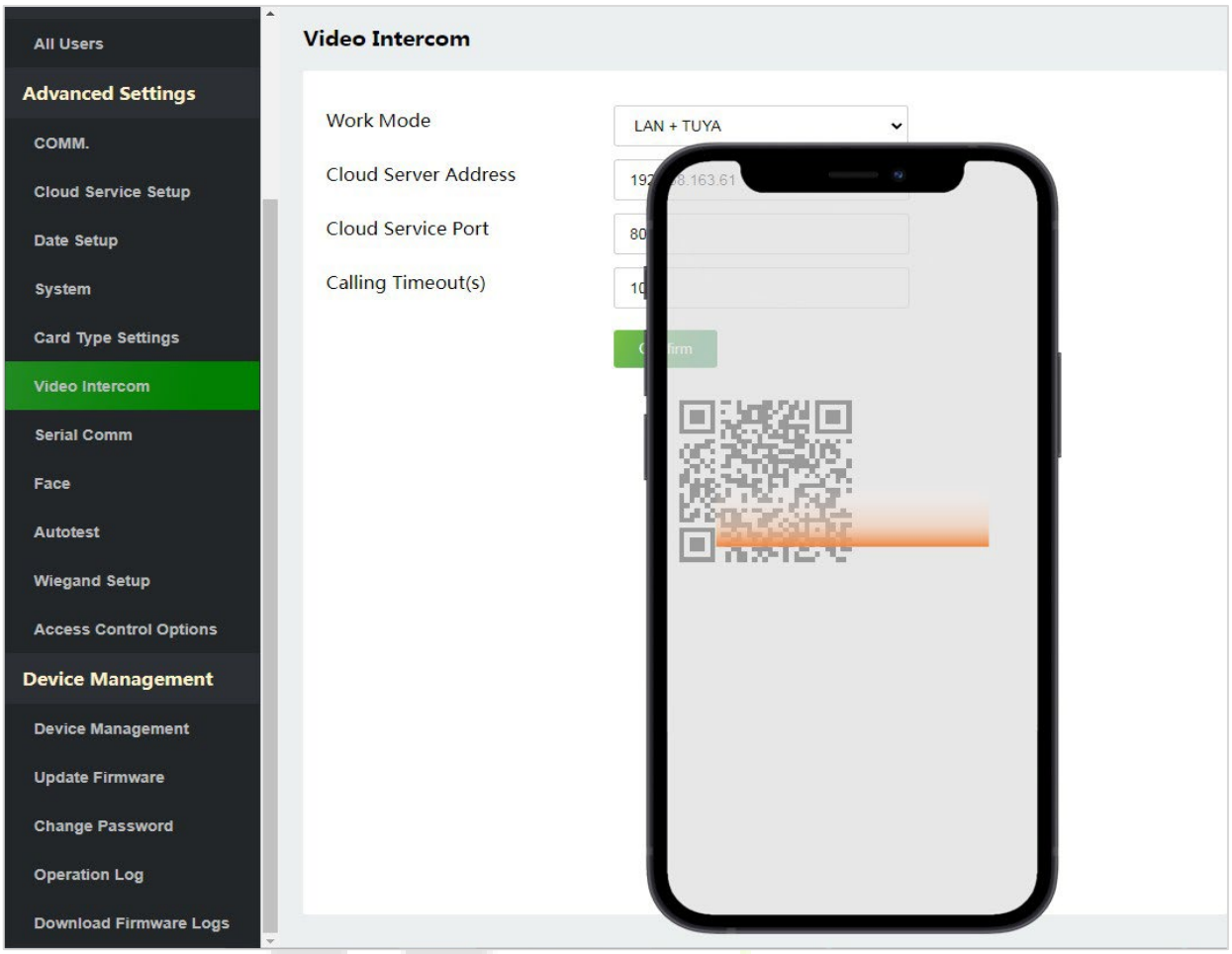
1. Clique em **Adicionar Dispositivo** na página inicial.

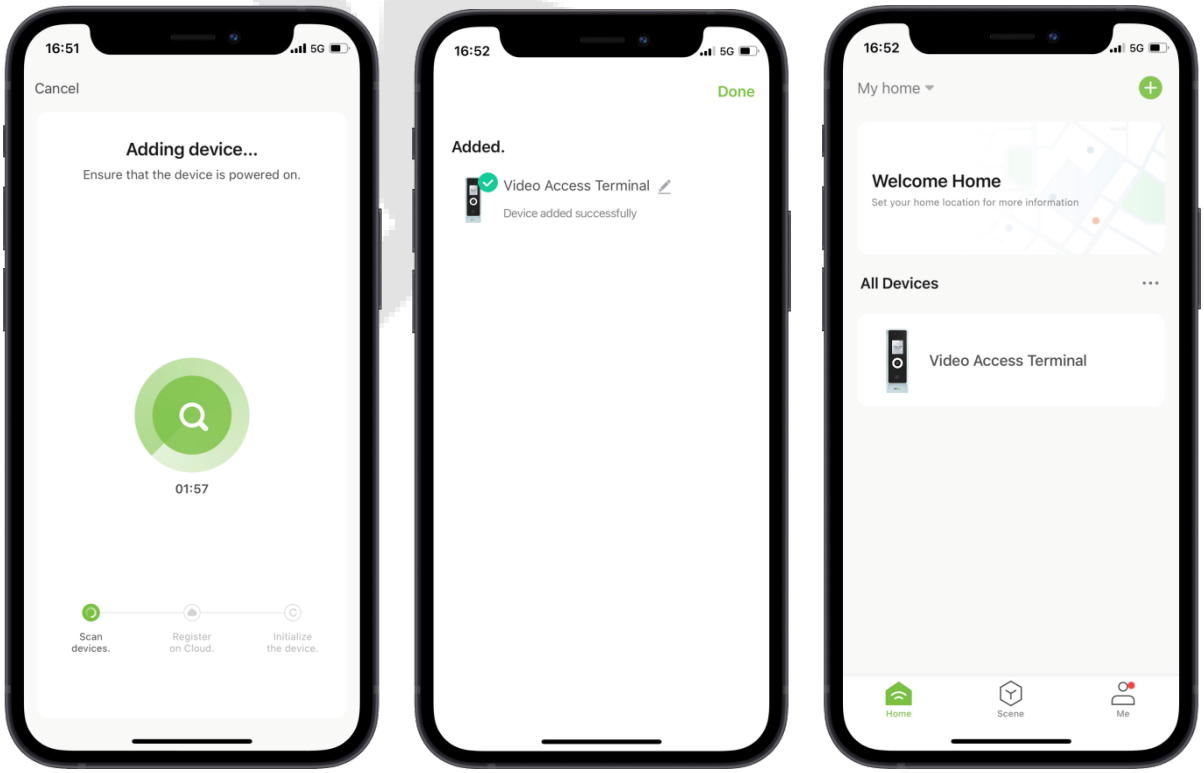


2. Clique em **Intercomunicador de Vídeo** no Servidor Web.



3. Toque no ícone no canto superior direito.



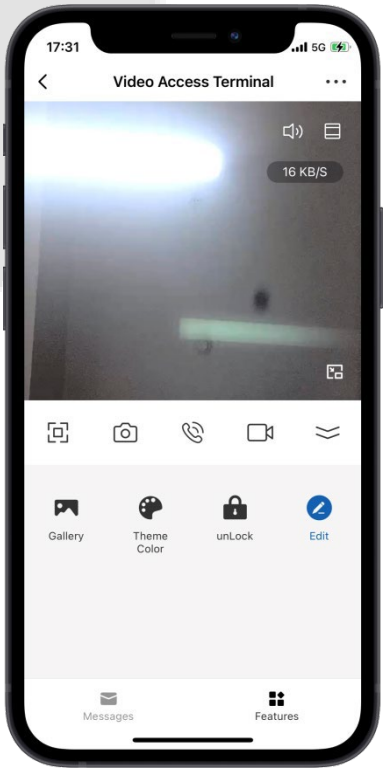


- **Realizar uma chamada no dispositivo**

Toque no ícone no ProMA para fazer uma chamada. Após receber a chamada, deslize para cima para abrir a porta remotamente.

- **Tela de vigilância**

Encontre o ProMA agrupado no aplicativo ZSmart para visualizar a tela em tempo real.

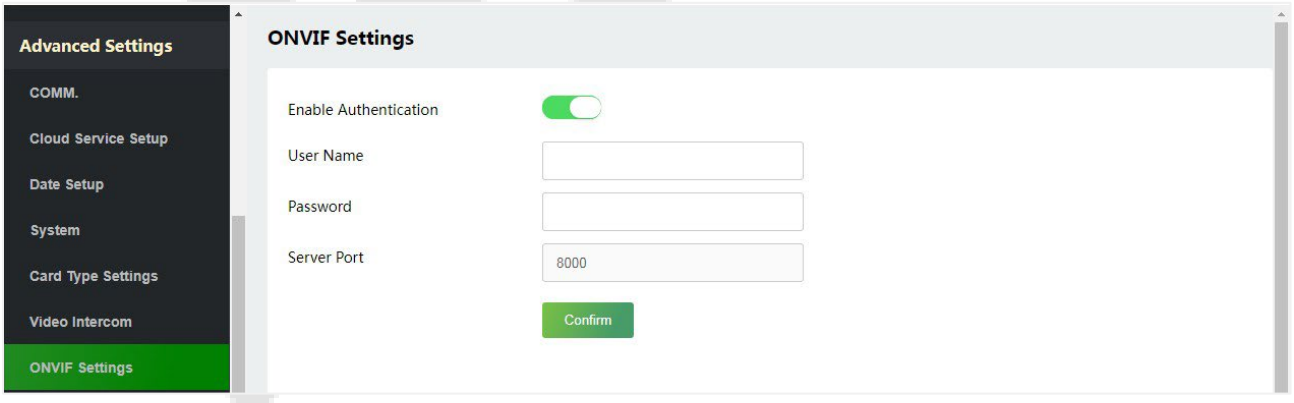


Descrição da Função

Função	Descrição
	Toque nele para alternar para a tela cheia.
	Capture uma foto para o álbum de fotos no aplicativo.
	Toque nele para falar com as pessoas em frente ao dispositivo.
	Grave manualmente um vídeo para o álbum de fotos no aplicativo.
	Para silenciar ou ativar o som do dispositivo.
Galeria	Reveja as fotos gravadas ao detectar o movimento.
Cor do Tema	Alterar o tema da interface para modo claro ou modo escuro.
Destrancar	Abertura remota da porta e visualização dos registros de abertura da porta.

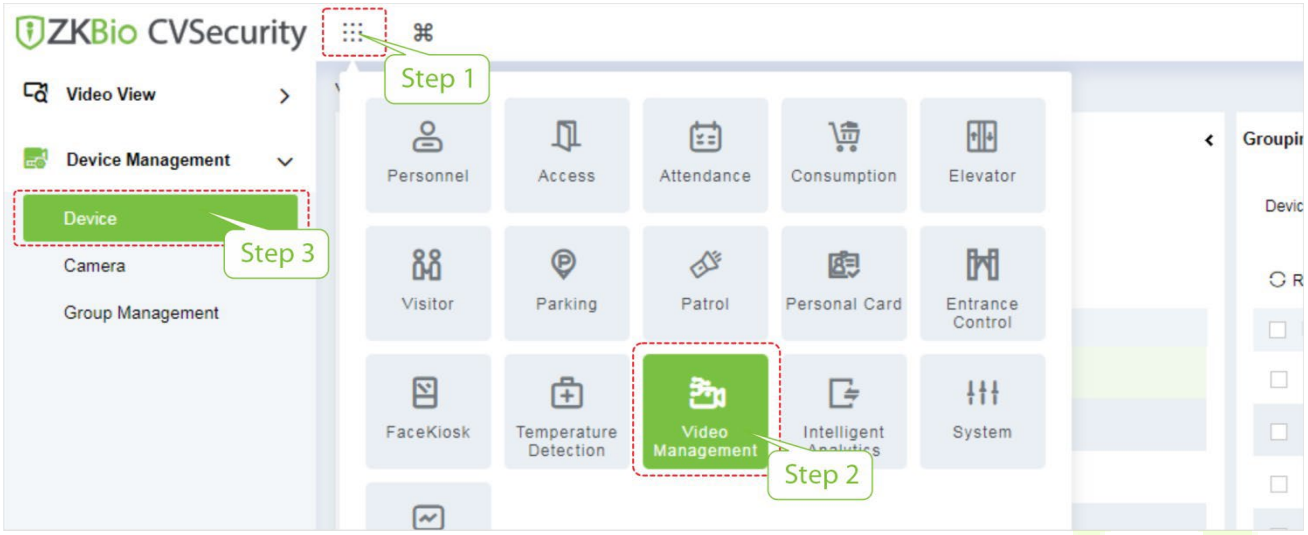
9.7 Configurações Onvif

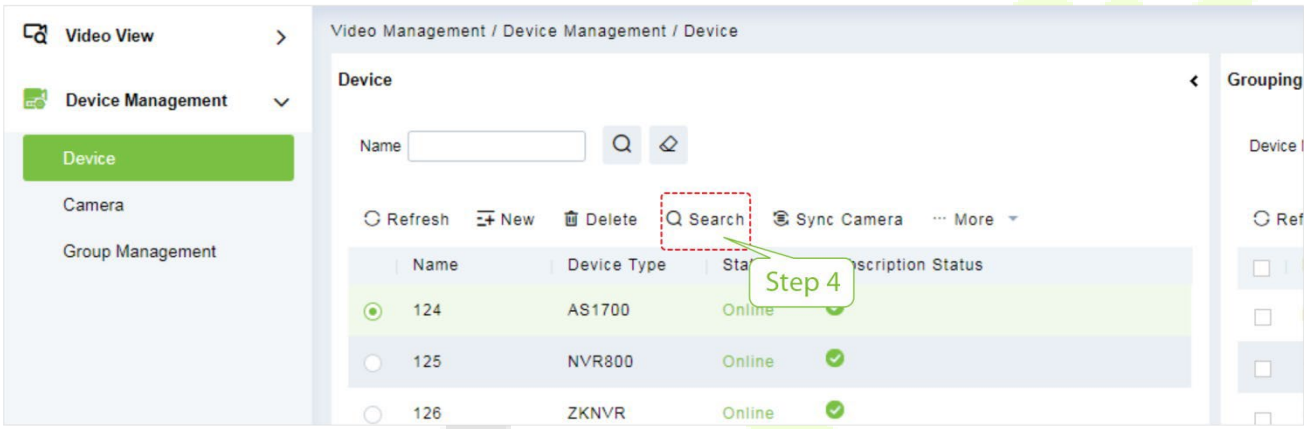
Observação: Essa função precisa ser usada com o gravador de vídeo em rede (NVR) ★. Clique em **Configurações ONVIF** no Servidor Web.

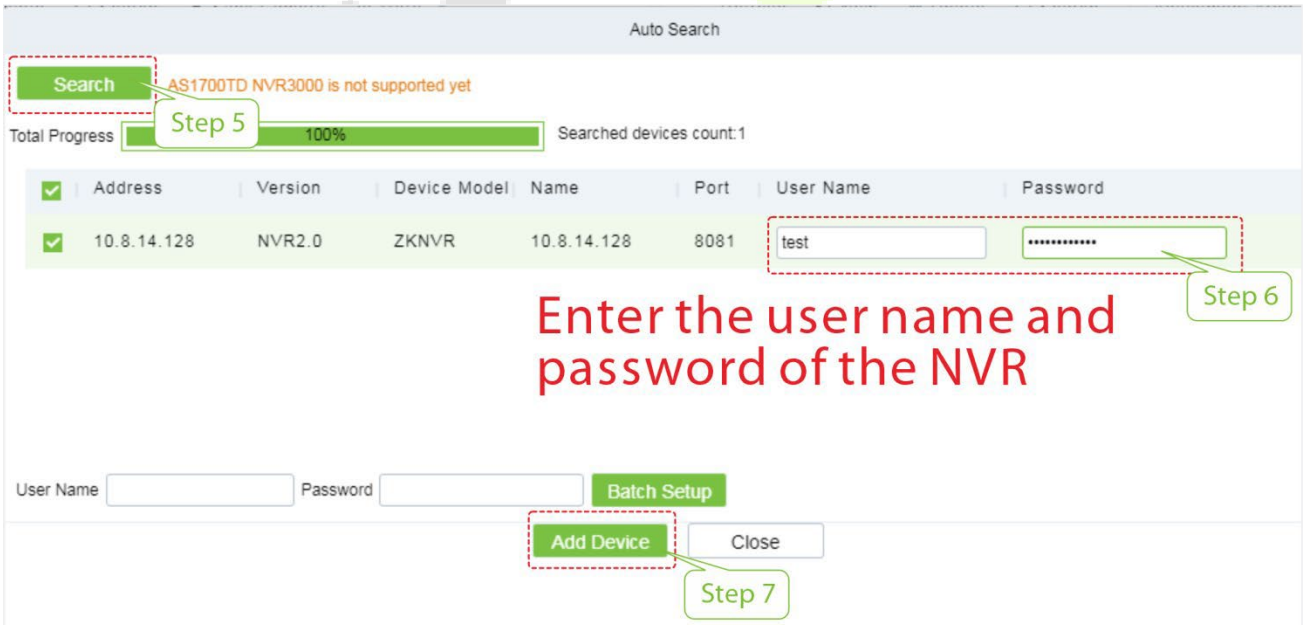


9.7.1 Gravador de Vídeo em Rede (NVR)

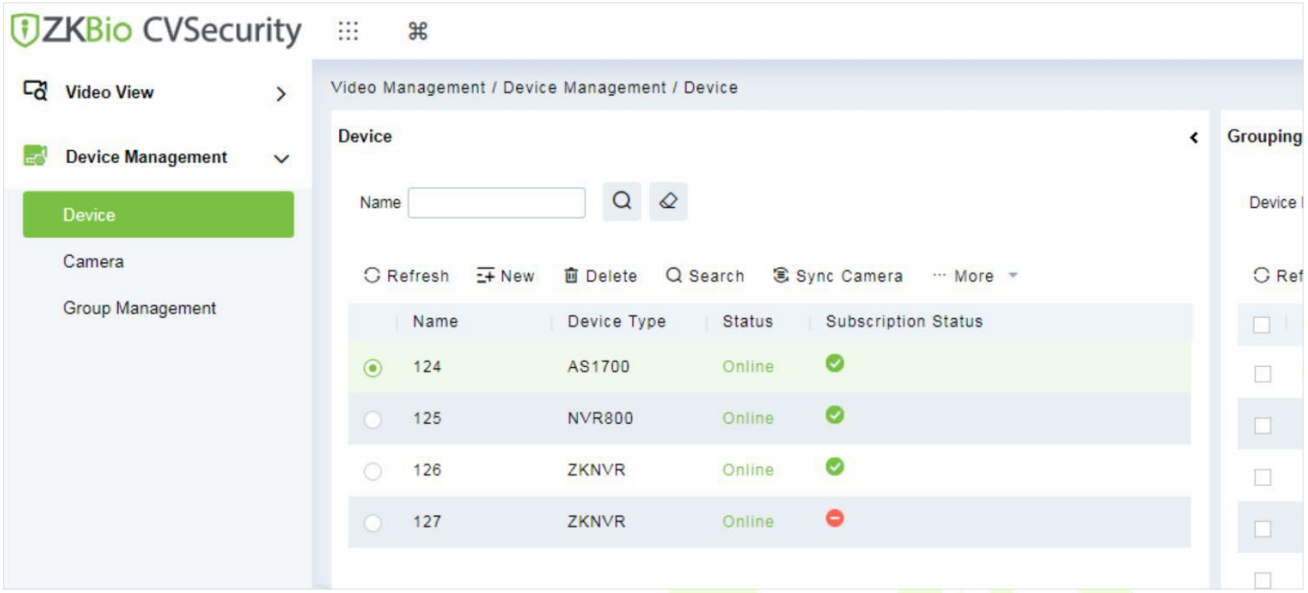
1. Após ligar o dispositivo NVR, conecte a porta de conexão do NVR através de um cabo Ethernet.
2. Clique em **Gerenciamento de Vídeo** > **Dispositivo** > **Pesquisar** no servidor ZKBio CVSecurity para adicionar o NVR.





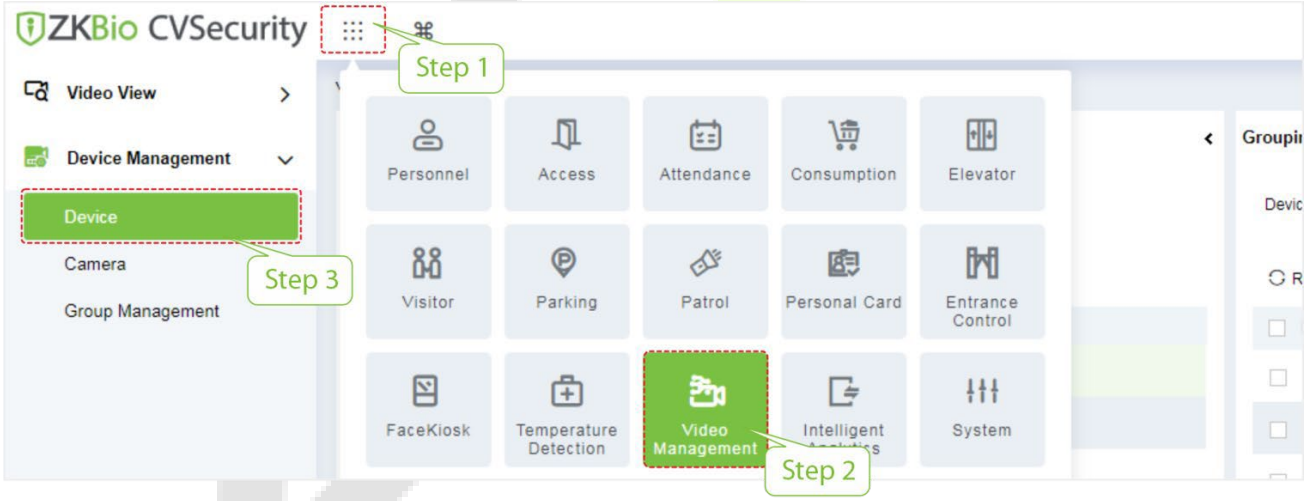


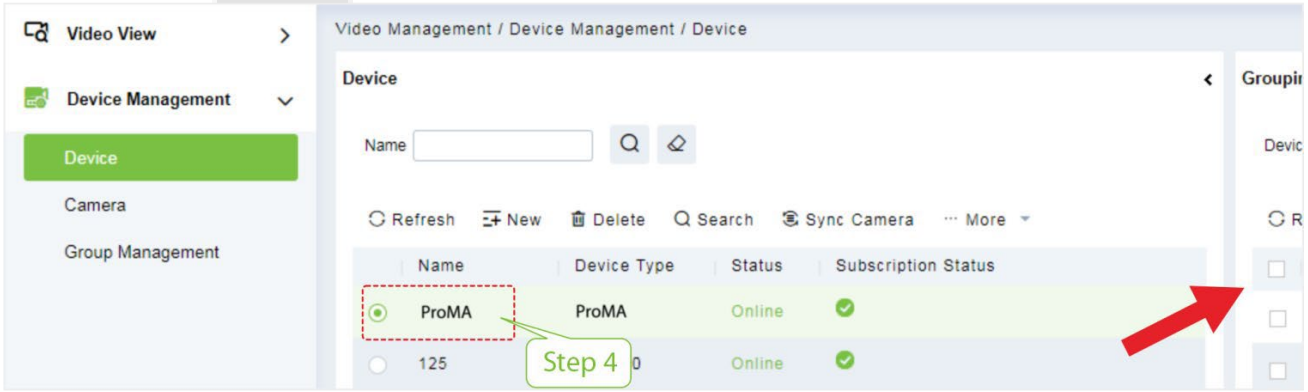
Os NVRs adicionados com sucesso são exibidos na lista de dispositivos, conforme mostrado na figura a seguir.



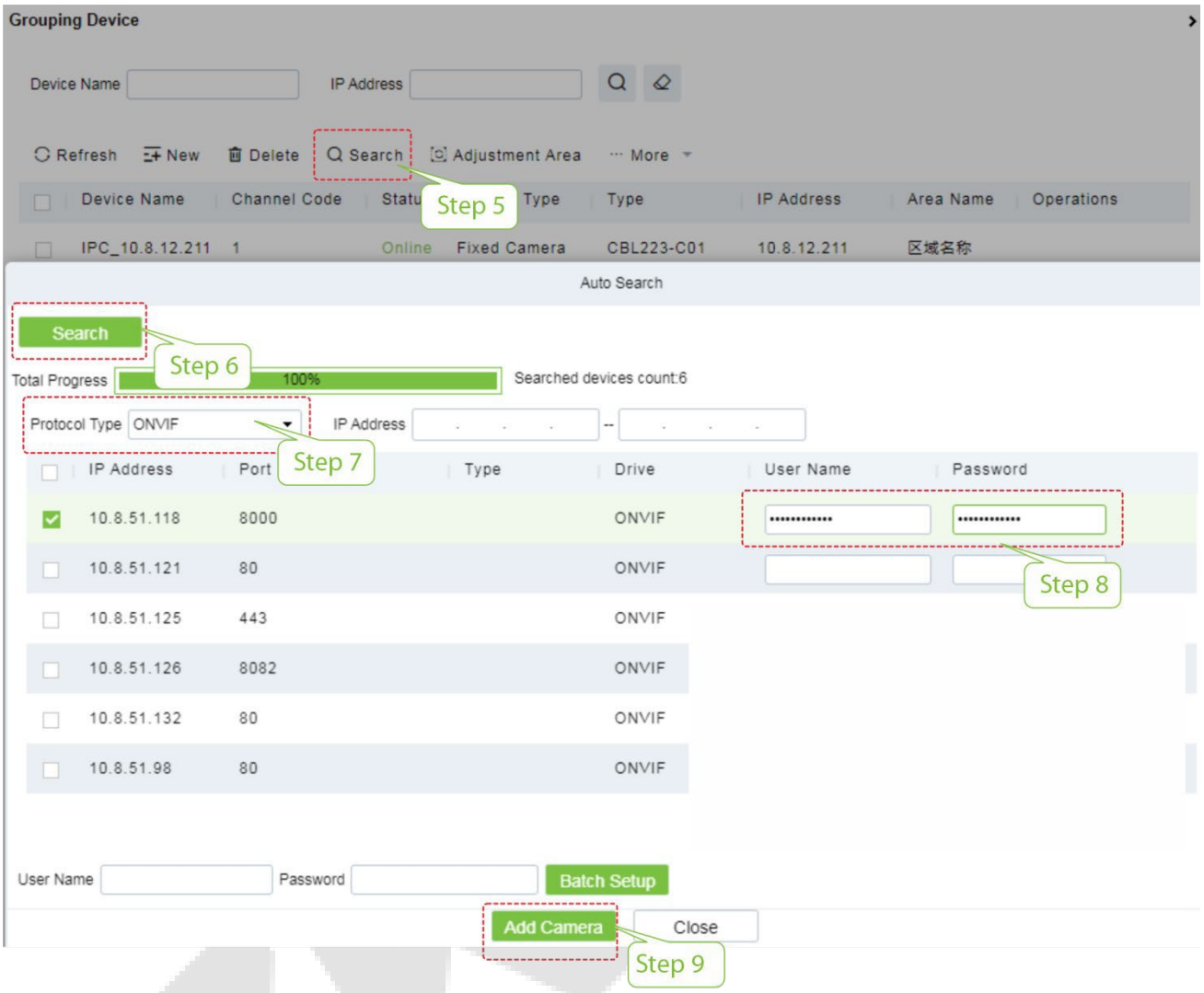
9.7.2 Adicione o ProMA ao NVR

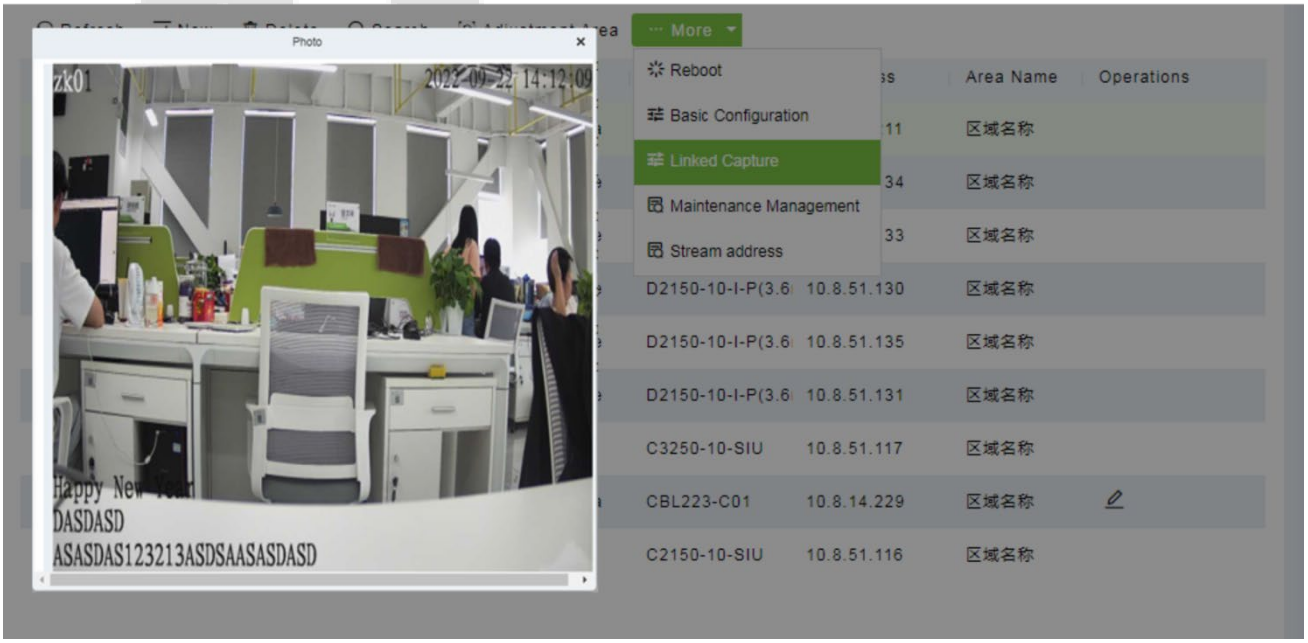
1. Clique em **Gerenciamento de Vídeo** > **Dispositivo** > **Pesquisar** no servidor ZKBio CVSecurity para selecionar o NVR ao qual você precisa adicionar o ProMA na lista de dispositivos.





2. Na lista de dispositivos, clique em **Pesquisar** > **Iniciar Pesquisa**, o NVR irá pesquisar automaticamente as câmeras IPC na mesma rede local (LAN) através do cabo de rede e adicioná-las.

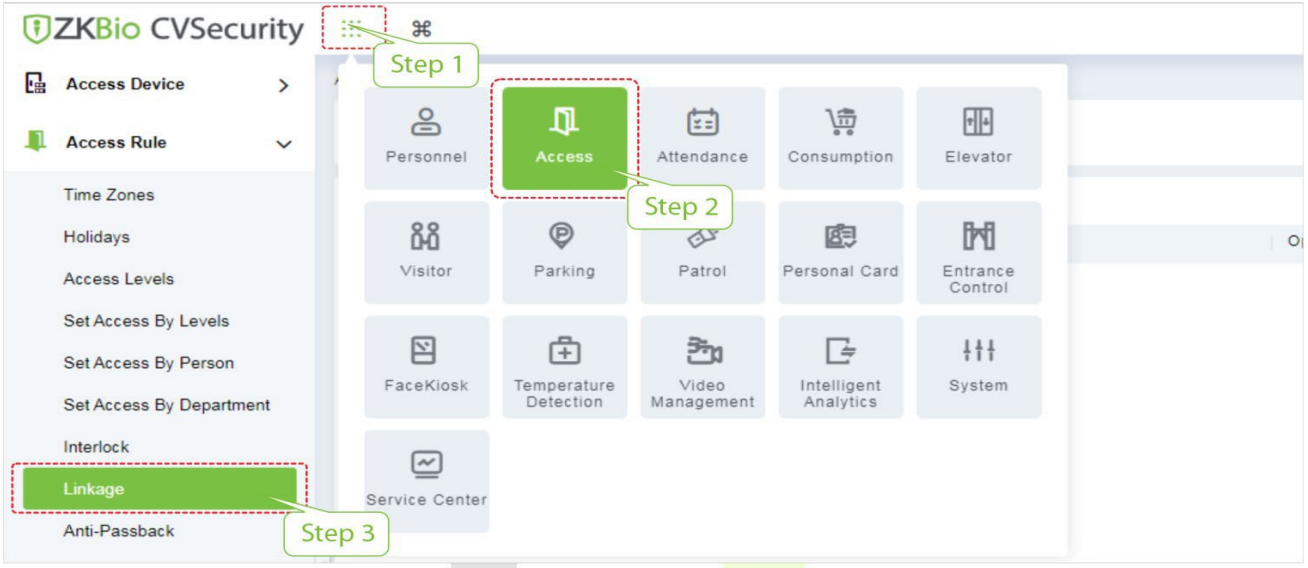


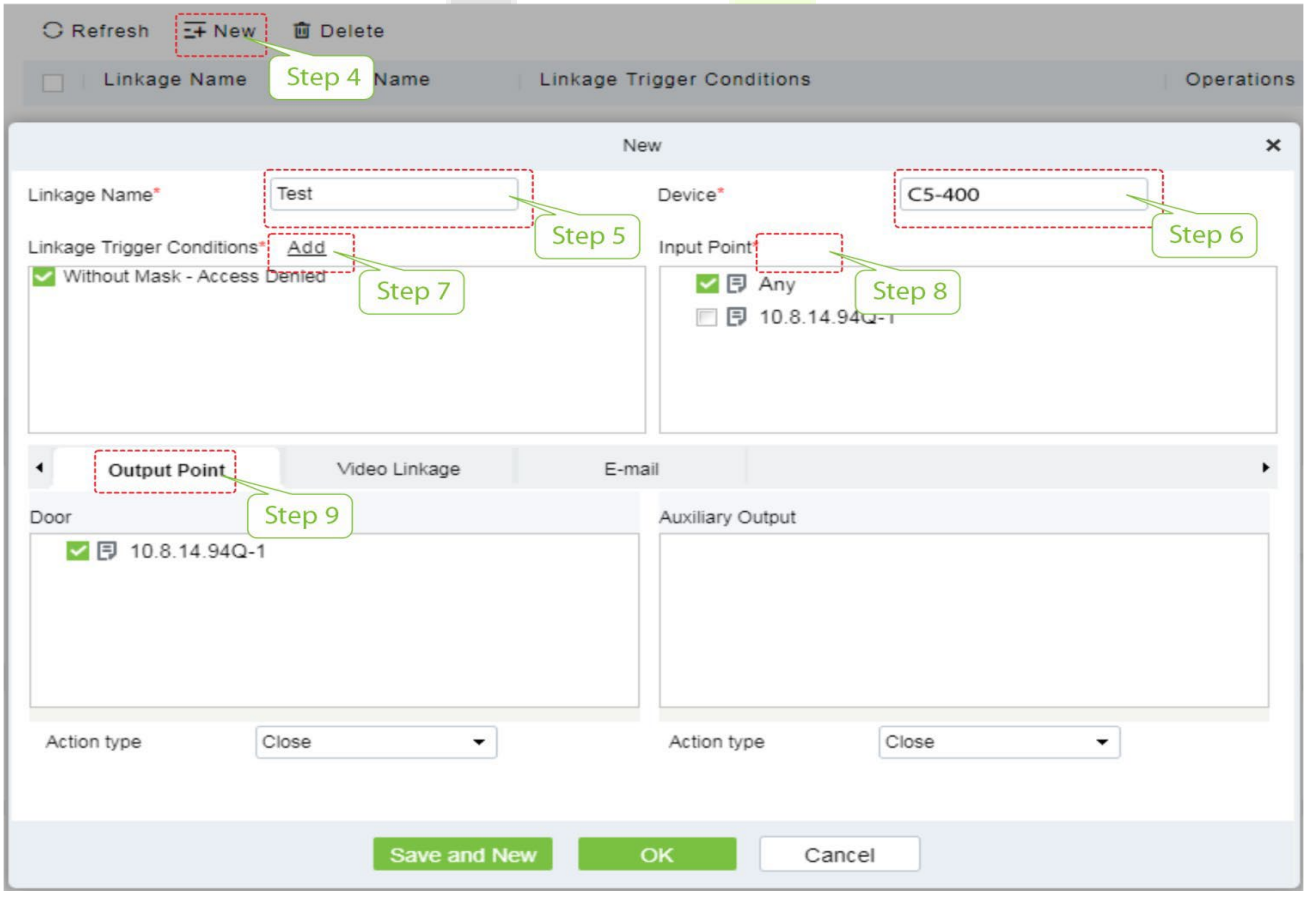


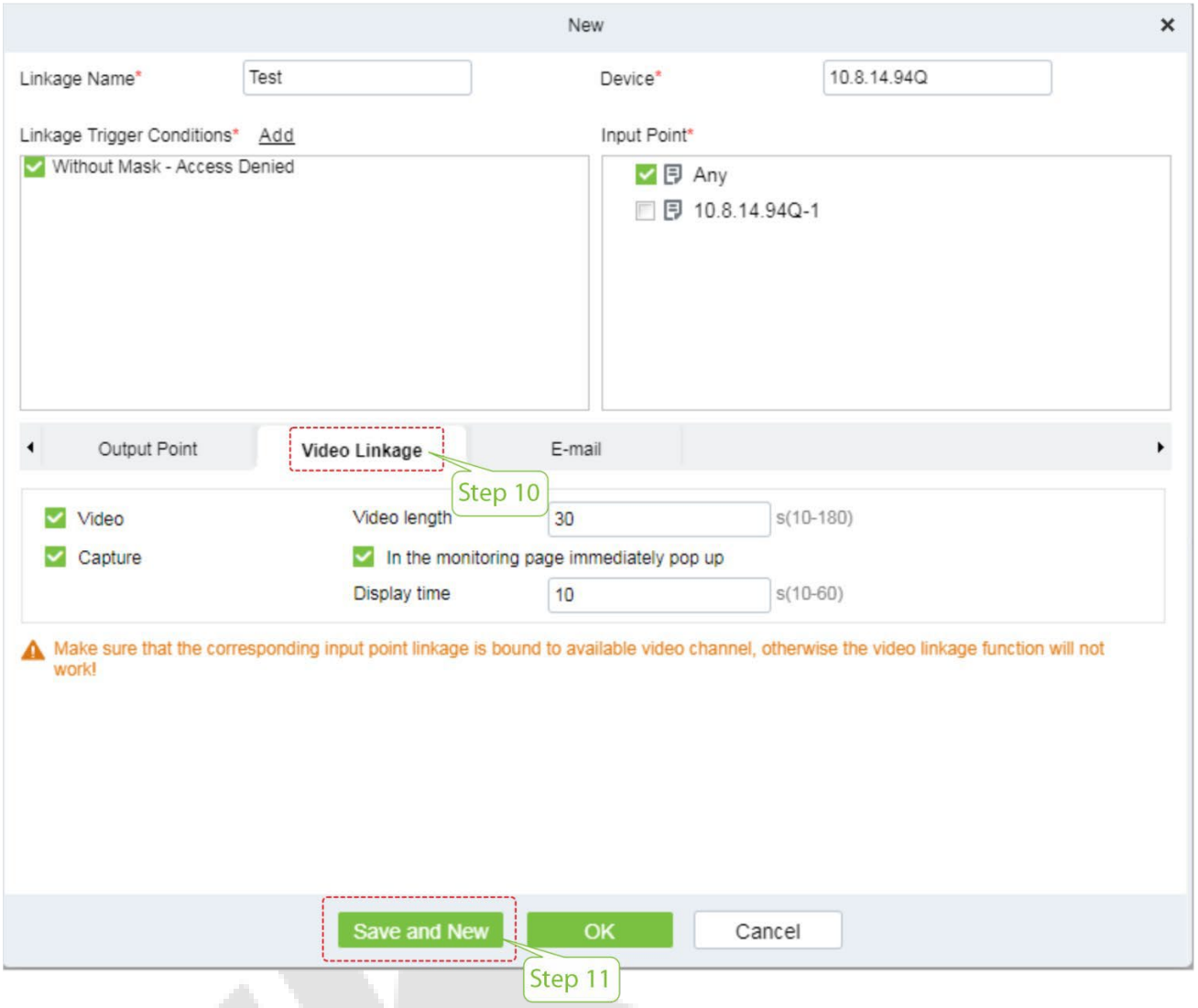
9.7.3 Vinculação

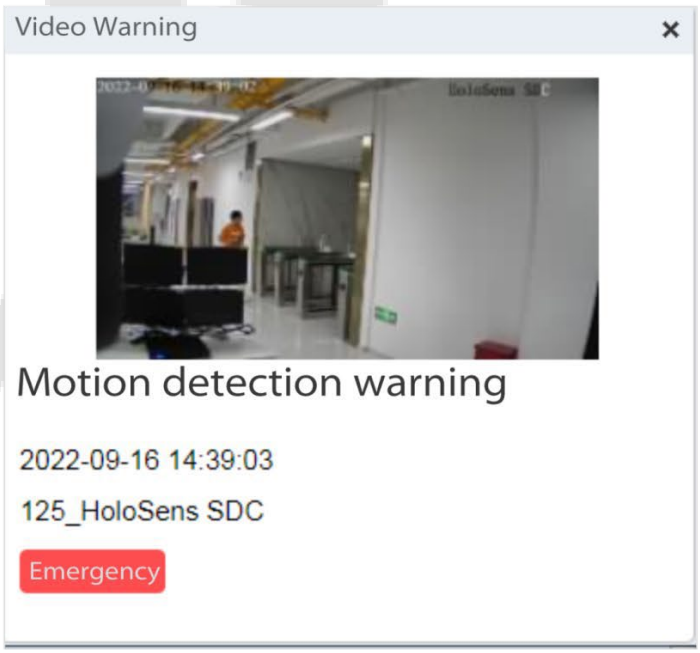
Após configurar o controlador de acesso, NVR e ProMA, você pode definir a vinculação de disparo de eventos para acesso não autorizado, verificação de abertura de portas, alarmes, anormalidades, etc., que serão exibidos na lista de eventos correspondente do monitoramento.

Clique em **Acesso** > **Vinculação** > **Adicionar** no servidor para configurar os parâmetros relacionados à vinculação. Para mais detalhes, consulte o Manual do Usuário do ZKBio CVSecurity.





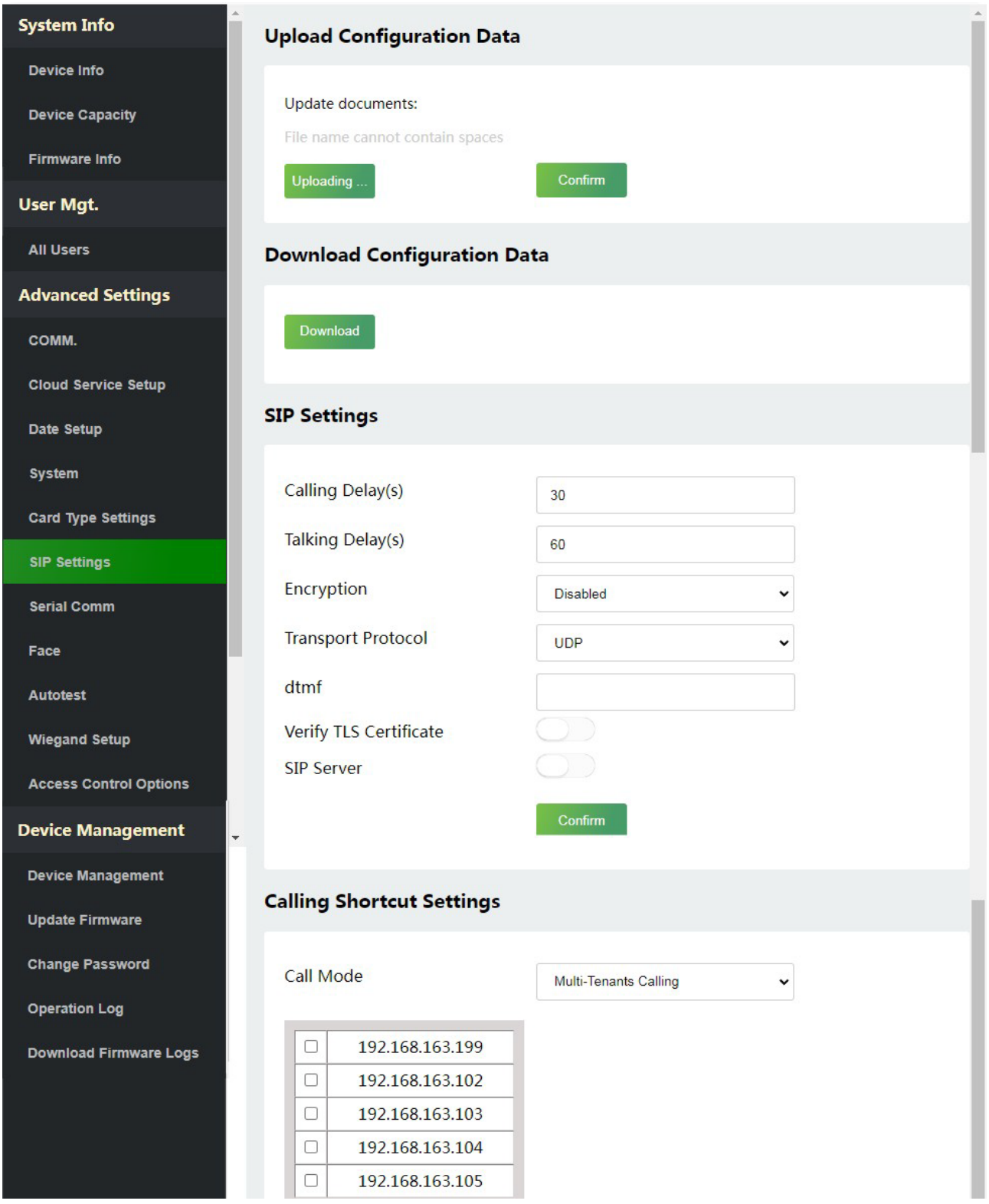




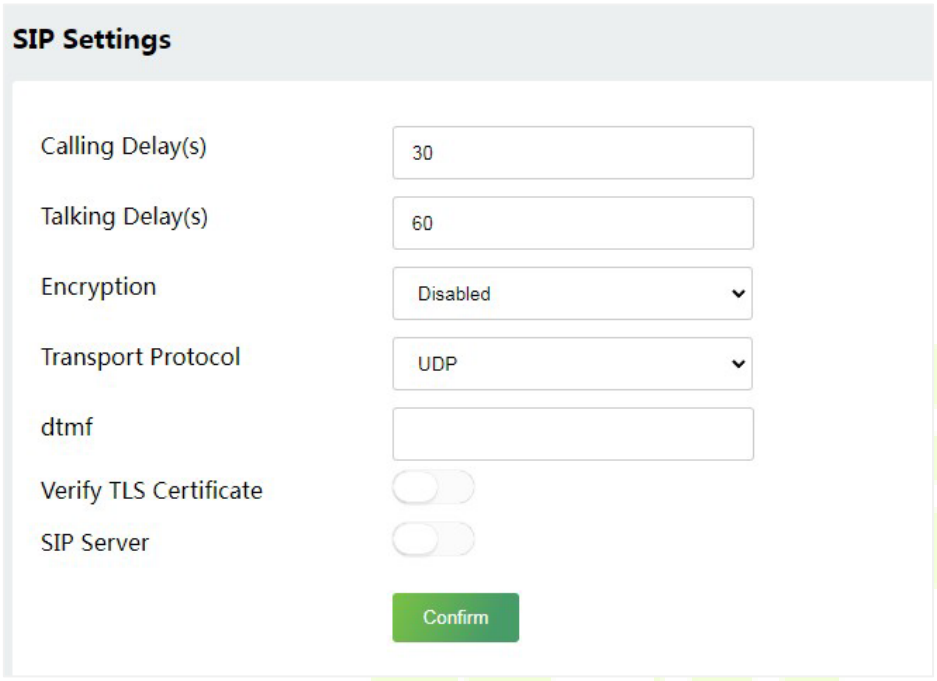
9.8 Configurações SIP★

Observação: Esta função precisa ser usada com a estação interna Vpad A2 ★.

Clique em **Configurações SIP** no Servidor Web.



9.8.1 Configurações SIP

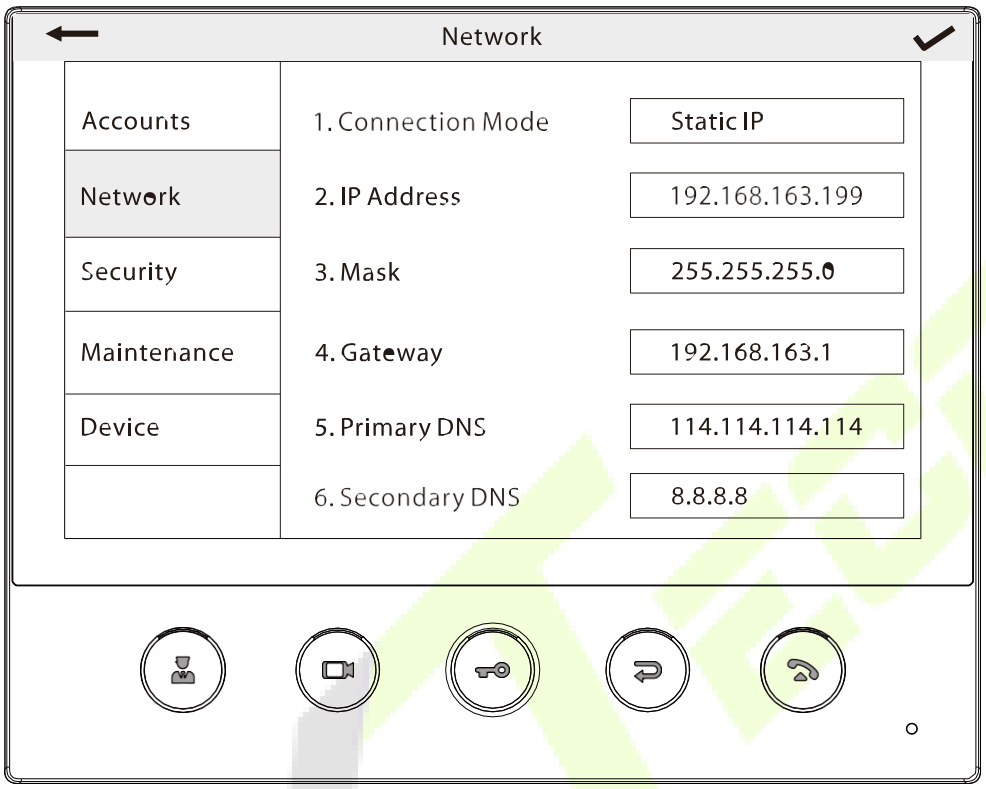


Função	Descrição
Atraso de Chamada (s)	Defina o tempo de chamada, valor válido de 30 a 60 segundos.
Atraso de Conversação (s)	Defina o tempo de intercomunicação, valor válido de 60 a 120 segundos.
Criptografia	Quando ativada, a comunicação do vídeo interfone será criptografada.
Protocolo de Transporte	Defina o protocolo de transporte entre o ProMA e a estação interna Vpad A2.
dtmf	O valor do WebServer é o mesmo valor do DMTF no dispositivo para desbloqueá-lo.
Verificar Certificado TLS	Habilitar/Desabilitar a verificação do certificado TLS.
Servidor SIP	Selecione se deseja habilitar o endereço do servidor. Depois de se conectar ao servidor, você pode chamá-lo digitando o nome de usuário da estação interna. Para mais detalhes, consulte 9.8.3 Servidor SIP.

O ProMA e a estação interna possuem dois modos para realizar o interfone de vídeo: LAN e servidor SIP. Qualquer um dos métodos pode ser selecionado para alcançar o interfone de vídeo SIP. Quando a LAN e o servidor SIP estão configurados ao mesmo tempo, ao clicar no botão da campainha do ProMA, o servidor SIP será iniciado primeiro.

9.8.2 Utilização da Rede Local (LAN)

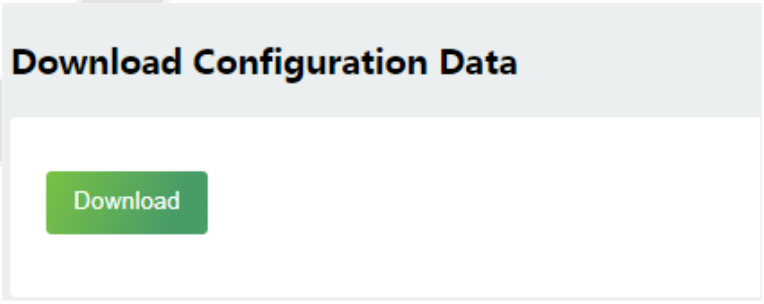
Configure o endereço IP na estação interna, toque em **Menu** > **Avançado** > **Rede** > 1. **Rede** > 1. **IPv4**.

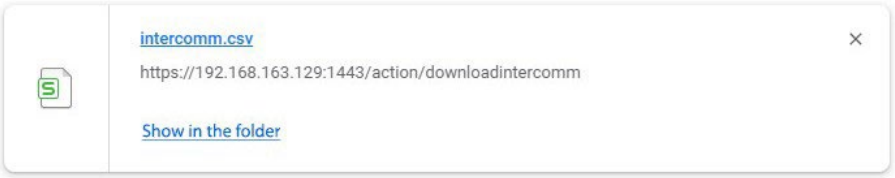


Observação: Na rede local (LAN), os endereços IP da estação interna e do ProMA devem estar no mesmo segmento de rede.

1. Baixar Dados de Configuração

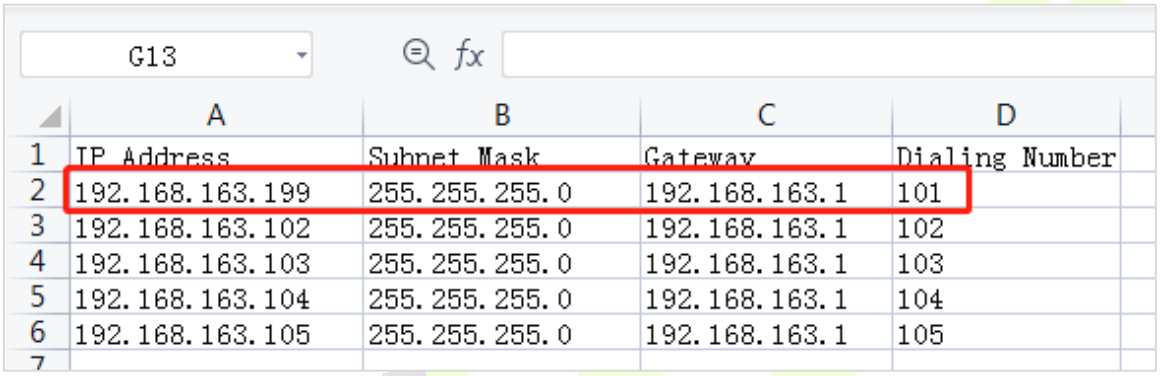
1) Clique em **Download** para baixar o arquivo e configurar os parâmetros do interfone de vídeo.





2) Abra o arquivo baixado e modifique manualmente os parâmetros do interfone de vídeo conforme necessário. Salve os parâmetros configurados para sincronizá-los com o ProMA.

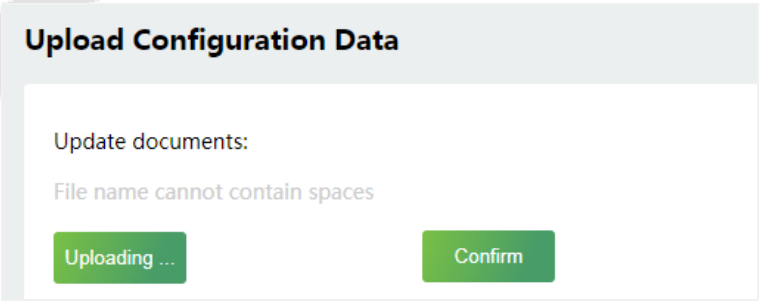
Observação: O endereço IP/Máscara de sub-rede/ Gateway devem ser os mesmos da estação interna para estabelecer a conexão.

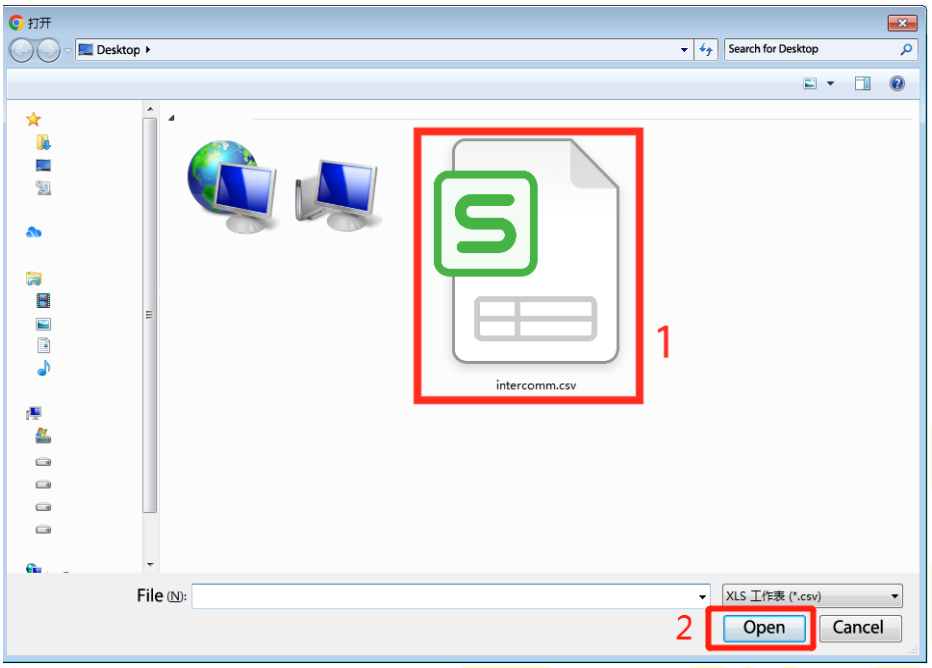


	A	B	C	D
1	IP Address	Subnet Mask	Gateway	Dialing Number
2	192.168.163.199	255.255.255.0	192.168.163.1	101
3	192.168.163.102	255.255.255.0	192.168.163.1	102
4	192.168.163.103	255.255.255.0	192.168.163.1	103
5	192.168.163.104	255.255.255.0	192.168.163.1	104
6	192.168.163.105	255.255.255.0	192.168.163.1	105

2. Enviar Dados de Configuração

1) Clique em **Carregando...** para localizar os parâmetros configurados para o interfone de vídeo.

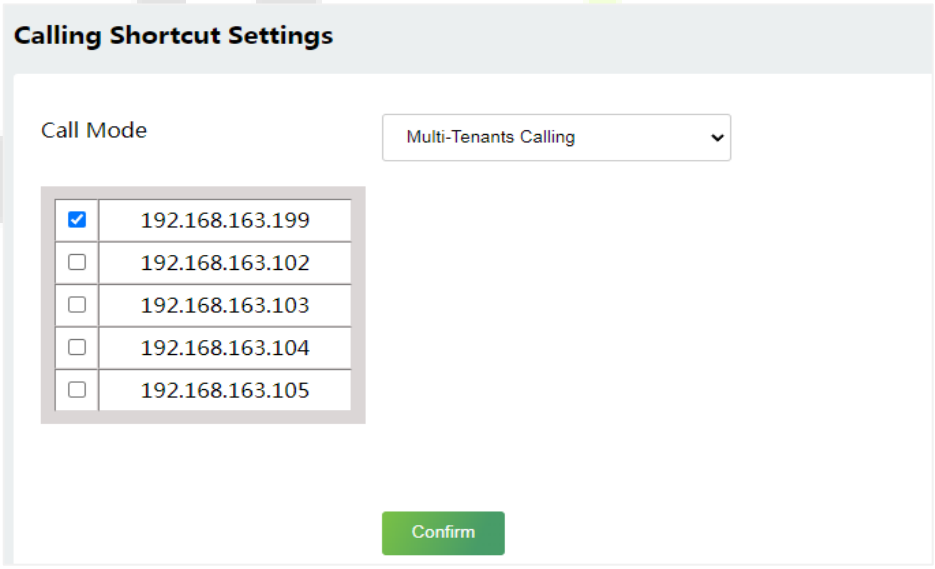




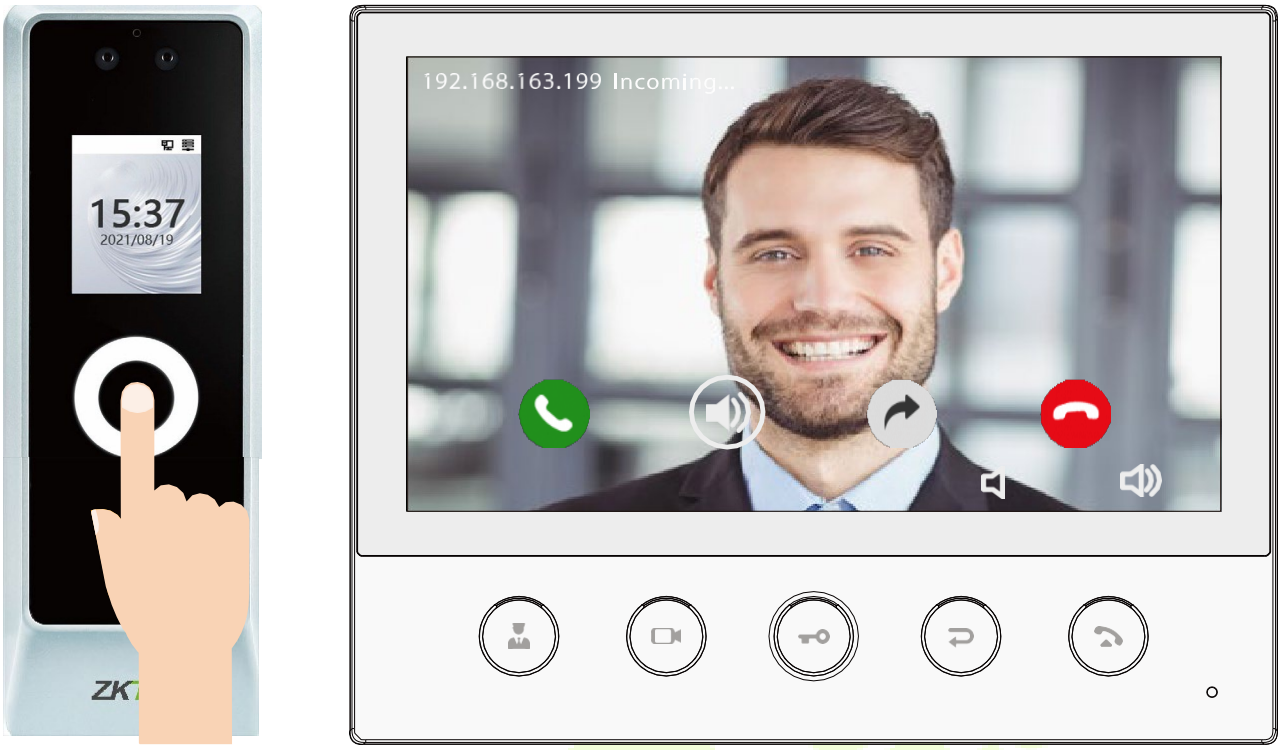
2) Clique em **Confirmar** para sincronizar os parâmetros com o ProMA

3. Configurações de Atalho de Chamada

Os parâmetros configurados serão sincronizados com o WebServer (ProMA), oferecendo suporte para chamadas individuais e multi-inquilinos.



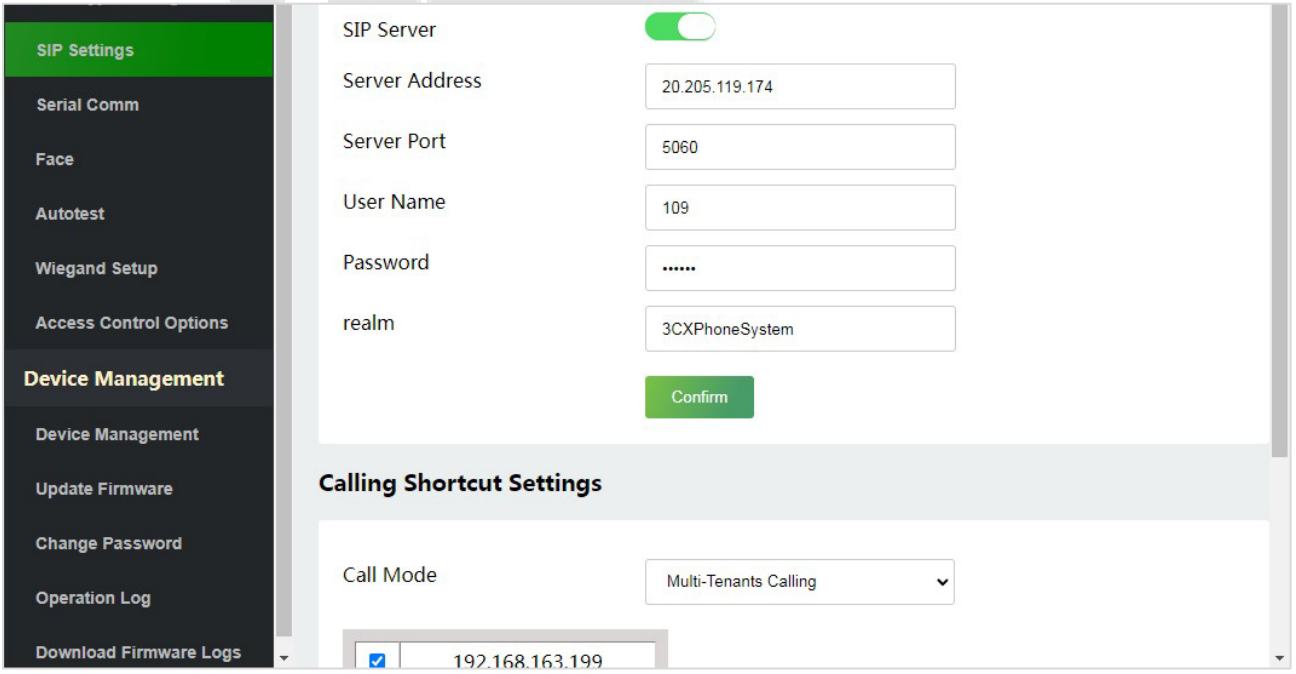
Uma vez que a estação interna esteja configurada com a rede, a função de interfone de vídeo pode ser realizada tocando no ícone no ProMA.



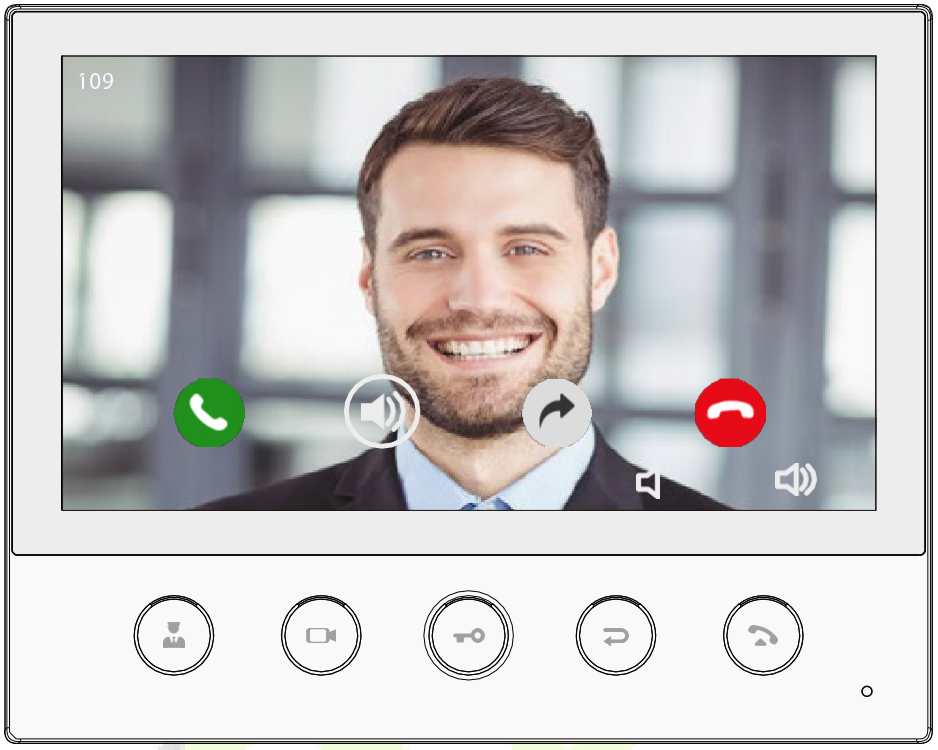
9.8.3 Servidor SIP

No Servidor Web, habilite o Servidor SIP e insira os parâmetros do servidor para a estação interna Vpad A2.

A configuração do servidor SIP não é afetada pela rede e responde mais rapidamente. É possível chamar o número do quarto com precisão de acordo com os parâmetros configurados.



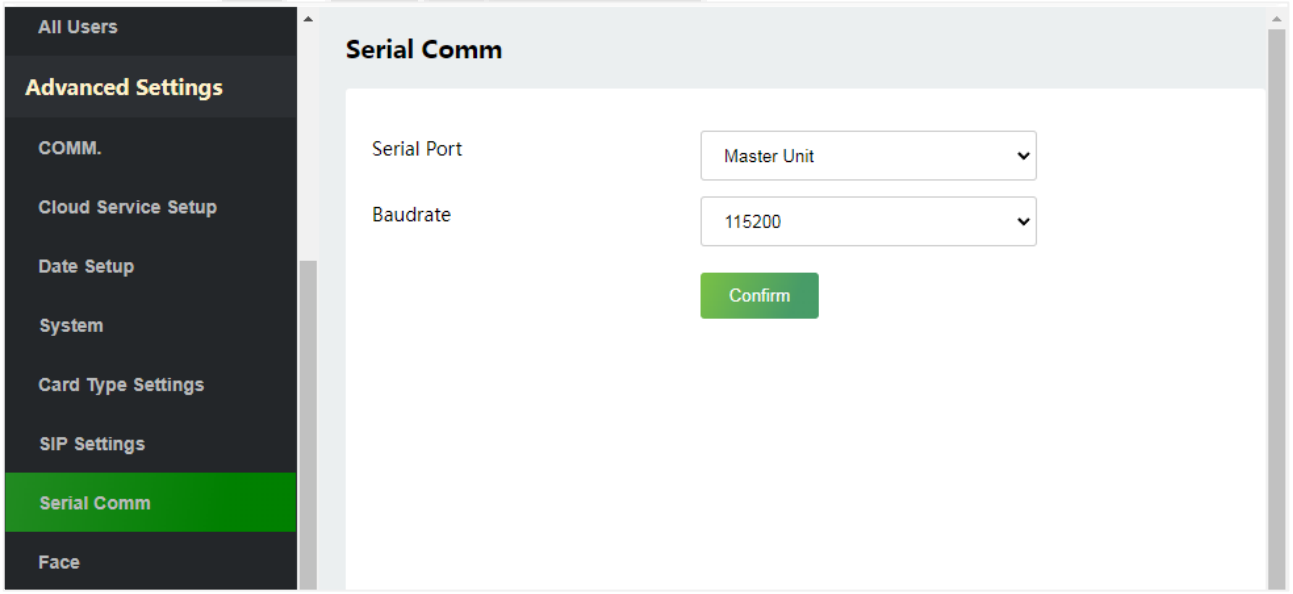
Uma vez que o Servidor SIP esteja configurado corretamente, é possível chamar o nome da conta da estação interna.



Para obter detalhes sobre a operação e uso da estação interna, consulte o manual do usuário da estação interna.

9.9 Comunicação Serial

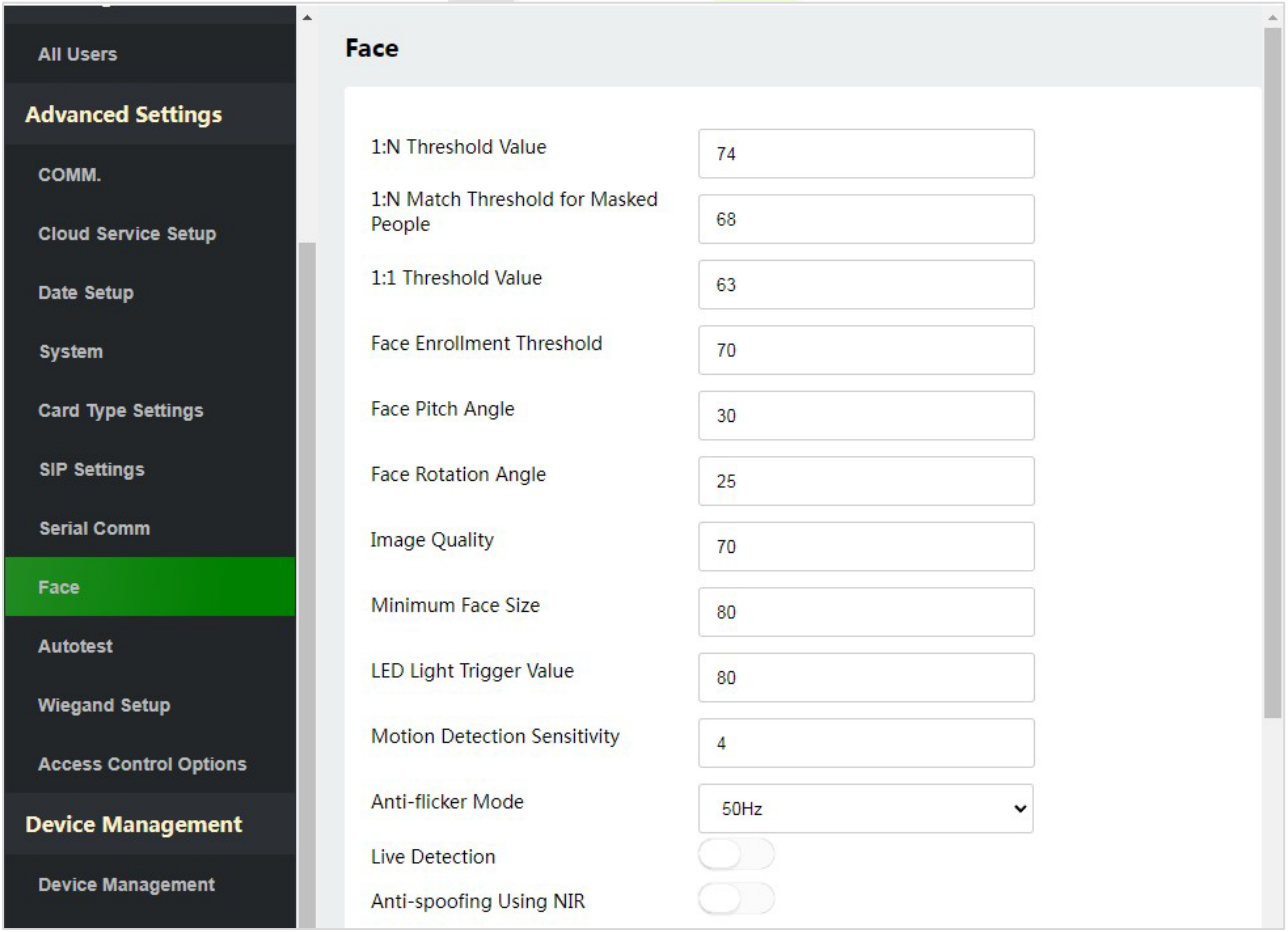
Clique em **Comunicação Serial** no Servidor Web.

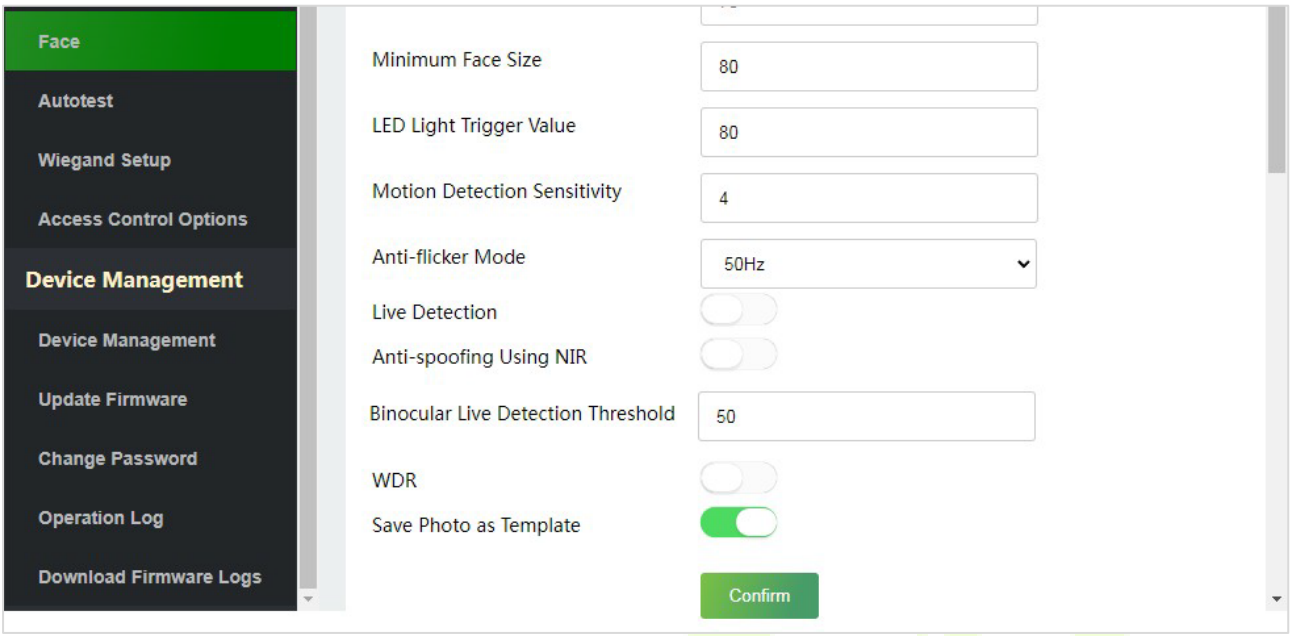


Função	Descrição
Porta Serial	**Não utilizando:** Sem comunicação com o dispositivo através da porta serial. **RS485 (PC):** Comunicação com o dispositivo através da porta serial RS485. **Unidade Mestre:** Quando o RS485 é usado como a função da "Unidade Mestre", pode ser conectado a um leitor de cartões. **DM10:** Comunicação com o dispositivo através da porta serial DM10.
Baudrate	Existem 5 opções de taxa de transmissão (baudrate) nas quais os dados se comunicam com o PC. São elas: 115200 (padrão), 57600, 38400, 19200 e 9600. Quanto maior a taxa de transmissão, mais rápida é a velocidade de comunicação, porém 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 é mais confiável.

9.10 Parâmetros de Face

Clique em **Face** no WebServer.





Função	Descrição
Limiar 1:N	No modo de autenticação facial, a autenticação só será bem-sucedida quando a similaridade entre a imagem facial adquirida e todos os modelos faciais registrados for maior que o valor estabelecido. O valor válido varia de 0 a 100. Quanto maior o valor do limiar, menor será a taxa de erro de julgamento, maior será a taxa de rejeição e vice-versa. Recomenda-se definir o valor padrão como 74.
Limiar de correspondência 1:N para pessoas com máscara	Quanto maior o valor do limiar, menor será a taxa de erro de julgamento, maior será a taxa de rejeição e vice-versa. Recomenda-se definir o valor padrão como 68.
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 cadastrados no dispositivo for maior que o valor estabelecido. O valor válido varia de 0 a 100. Quanto maior o valor do limiar, menor será a taxa de erro de julgamento e maior será a taxa de rejeição, e vice-versa. Recomenda-se definir o valor padrão como 63.
Limiar de Cadastro Facial	Durante o cadastro facial, é utilizada a comparação 1:N para determinar se o usuário já está cadastrado anteriormente. Quando a similaridade entre a imagem facial adquirida e todos os modelos faciais registrados for maior que esse limiar, indica que o rosto já foi cadastrado.

Ângulo de Inclinação do Rosto	A tolerância do ângulo de inclinação do rosto para o cadastro e comparação facial. Se o ângulo de inclinação do rosto exceder esse valor estabelecido, ele será filtrado pelo algoritmo, ou seja, será ignorado pelo terminal e nenhuma interface de cadastro ou comparação será acionada.
Ângulo de Rotação do Rosto	A tolerância do ângulo de rotação do rosto para o cadastro e comparação de modelos faciais. Se o ângulo de rotação do rosto exceder esse valor estabelecido, ele será filtrado pelo algoritmo, ou seja, será ignorado pelo terminal e nenhuma interface de cadastro ou comparação será acionada.
Qualidade da Imagem	Qualidade da imagem para o cadastro e comparação facial. Quanto maior o valor, mais nítida a imagem deve ser.
Tamanho Mínimo do Rosto	Requerido para o cadastro e comparação facial. Se o tamanho mínimo da figura capturada for menor que esse valor estabelecido, ela será filtrada e não será reconhecida como um rosto. Esse valor pode ser compreendido como a distância de comparação facial. Quanto mais distante a pessoa estiver, menor será o tamanho do rosto e menor será o número de pixels obtidos pelo algoritmo. Portanto, ajustar esse parâmetro permite ajustar a distância máxima de comparação de rostos. Quando o valor é 0, a distância de comparação facial não é limitada.
Valor de Ativação da Luz LED	Este valor controla o acionamento e desligamento da luz LED. Quanto maior o valor, mais frequentemente a luz LED será ativada.
Sensibilidade de Detecção de Movimento	É usado para definir o valor para a quantidade de mudança no campo de visão da câmera, conhecida como detecção de movimento potencial, que faz com que o terminal saia do modo de espera e acesse a interface de comparação. Quanto maior o valor, mais sensível o sistema será, ou seja, se um valor maior for definido, a interface de comparação será acionada com mais facilidade e a detecção de movimento ocorrerá com mais frequência.
Modo Anti-Flicker	Utilizado quando o WDR está desligado. Isso ajuda a reduzir a cintilação quando a tela do dispositivo pisca na mesma frequência da luz.
Detecção em Tempo Real	Detectando a tentativa de falsificação usando imagens de luz visível para determinar se a amostra de origem biométrica fornecida é realmente de uma pessoa (um ser humano vivo) ou uma representação falsa.
Limiar de Detecção em Tempo Real	Facilita a avaliação de se a imagem visível capturada é realmente de uma pessoa (um ser humano vivo). Quanto maior o valor, melhor será o desempenho anti-falsificação usando luz visível.
Anti-falsificação usando NIR (Infravermelho Próximo)	Utilizando imagens de espectro de infravermelho próximo para identificar e prevenir ataques com fotos e vídeos falsos.

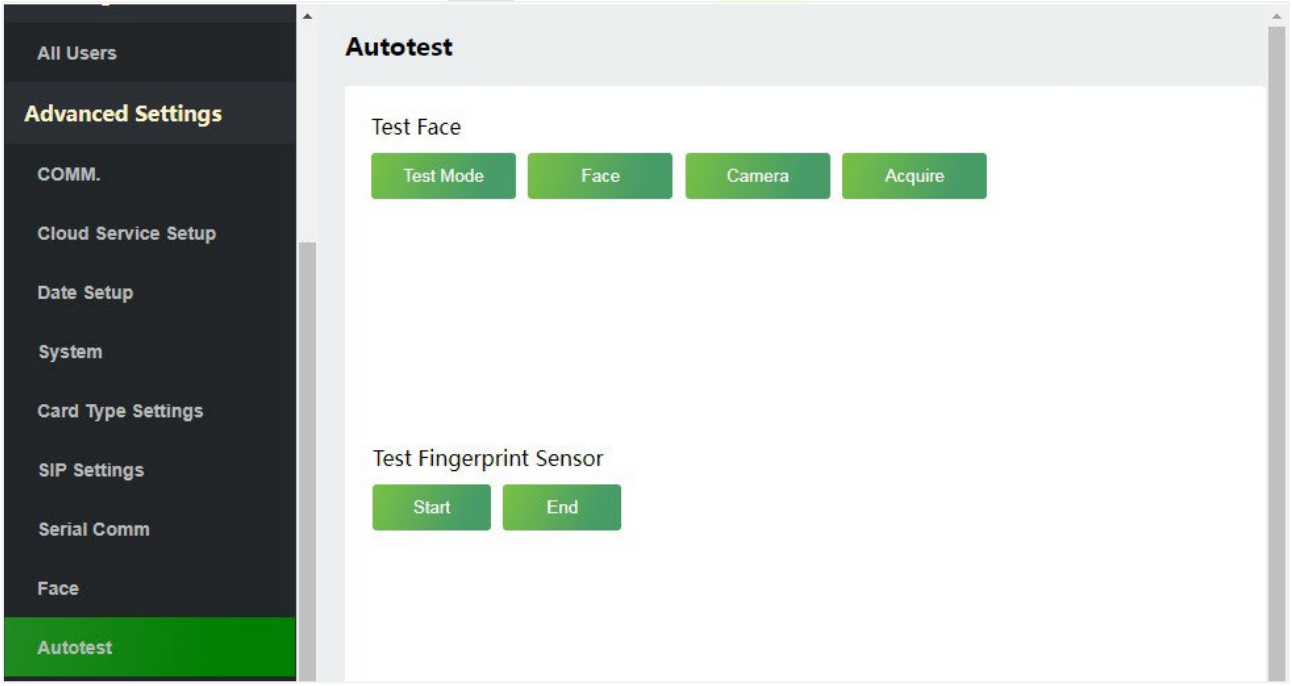
Limiar de Detecção em Tempo Real Binocular	Facilita a avaliação de se a imagem visível capturada é realmente de uma pessoa (um ser humano vivo). Quanto maior o valor, melhor será o desempenho anti-falsificação usando luz visível.
WDR	Wide Dynamic Range (WDR), que equilibra a luz e estende a visibilidade da imagem para vídeos de vigilância em cenas de iluminação de alto contraste e melhora a identificação de objetos em ambientes claros e escuros.
Salvar foto como Template	Selecionar se deve salvar a foto registrada.

Observação: O ajuste inadequado dos parâmetros de exposição e qualidade pode afetar severamente o desempenho do dispositivo. Por favor, ajuste o parâmetro de exposição apenas sob a orientação do pessoal de serviço pós-venda de nossa empresa.

9.11 Autoteste

Clique em **Autoteste** no WebServer.

Isso permite que o sistema teste automaticamente se as funções dos vários módulos estão funcionando normalmente.



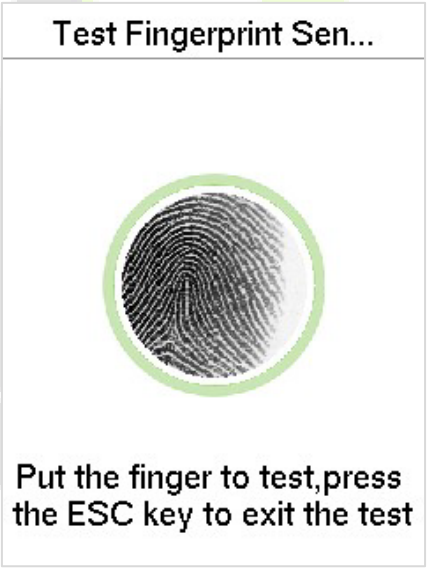
9.11.1 Testar Face

Clique em **Modo de Teste**, o dispositivo ProMA exibirá a interface de Teste de Face em tempo real. Clique em Fim do Teste para sair do teste.

Após abrir o modo de teste, o canto superior esquerdo da tela do dispositivo exibirá o valor da face em tempo real, sendo que quanto maior o valor, melhor será a qualidade da face.

9.11.2 Testar sensor de impressão digital

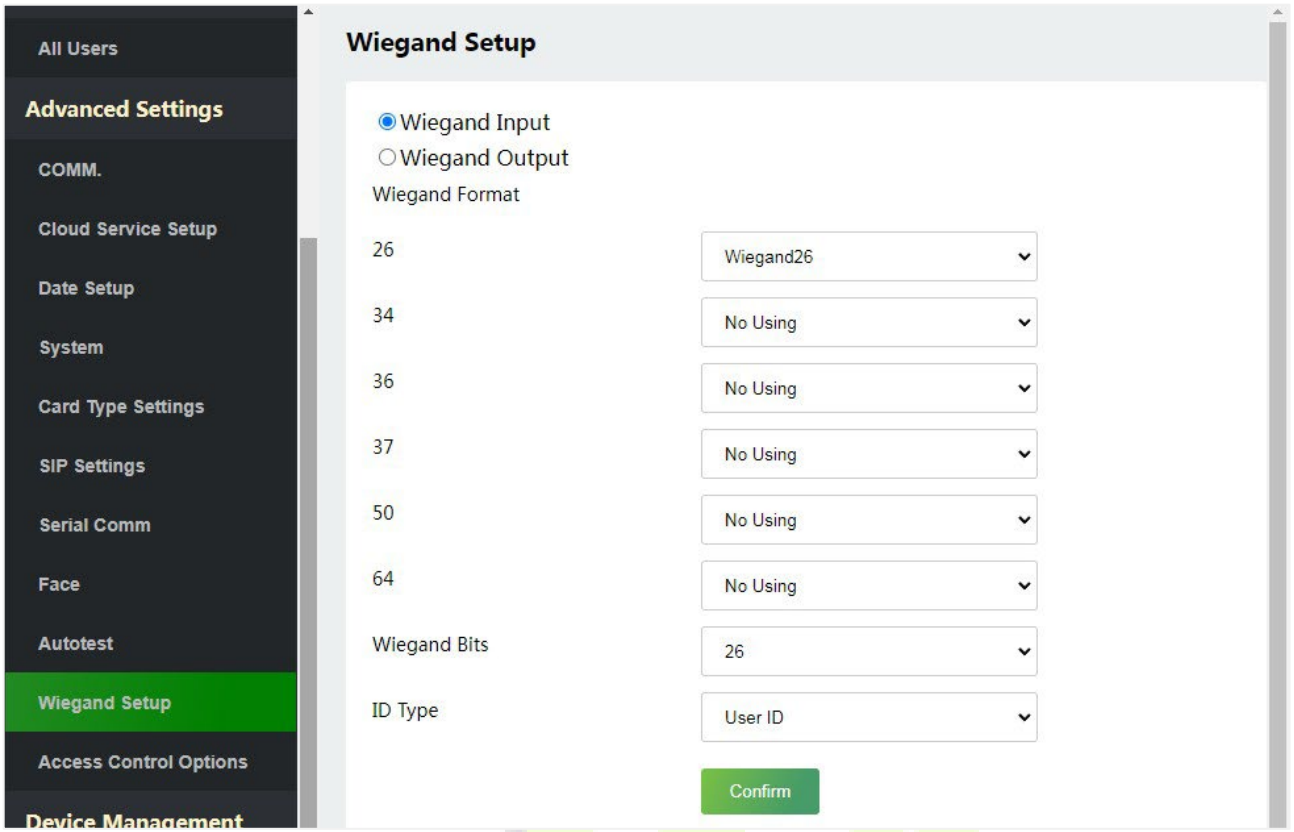
Clique em **Iniciar**, o dispositivo ProMA exibirá a interface de Teste de Impressão Digital em tempo real. Clique em **Finalizar** para sair do teste.

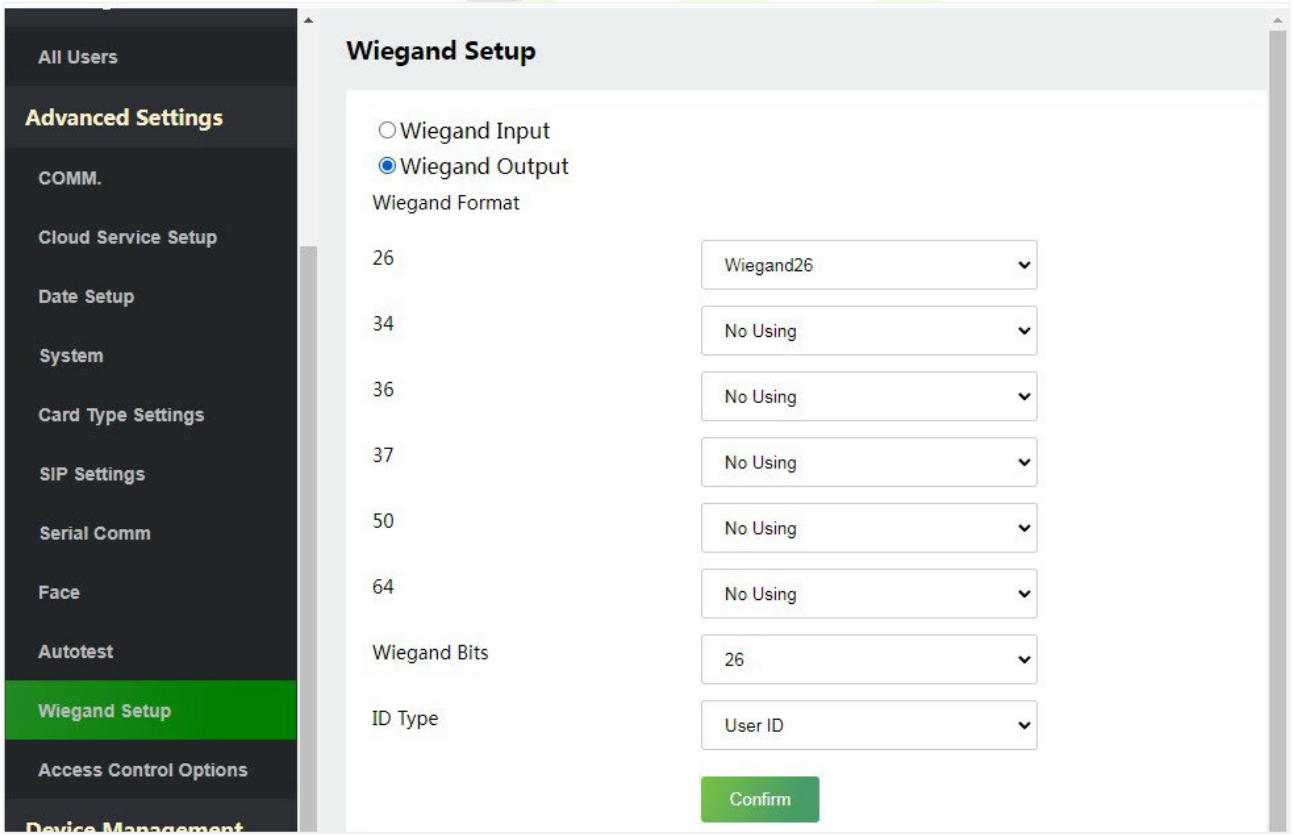


9.12 Configuração Wiegand

Clique em **Configuração Wiegand** no WebServer.

Isso é usado para configurar os parâmetros de entrada e saída Wiegand.





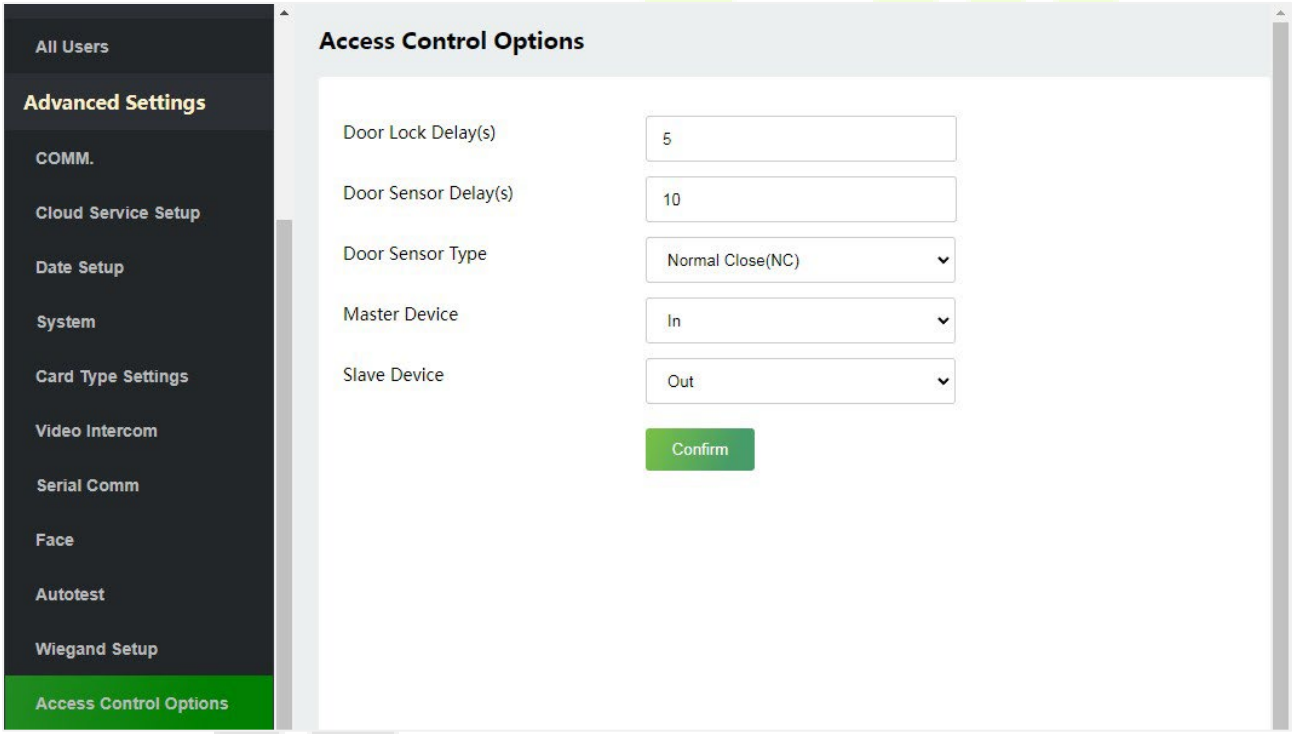
Função	Descrição
Formato Wiegand	Seu valor pode ser de 26 bits, 34 bits, 36 bits, 37 bits, 50 bits e 60 bits.
Bits Wiegand	O número de bits dos dados Wiegand
Tipo de ID	Selecione entre o ID do usuário e o número do cartão.

9.13 Opções de Controle de Acesso

Clique em **Opções de Controle de Acesso** no WebServer.

Na interface de Controle de Acesso, configure os parâmetros do controle de trava do terminal e equipamentos relacionados.

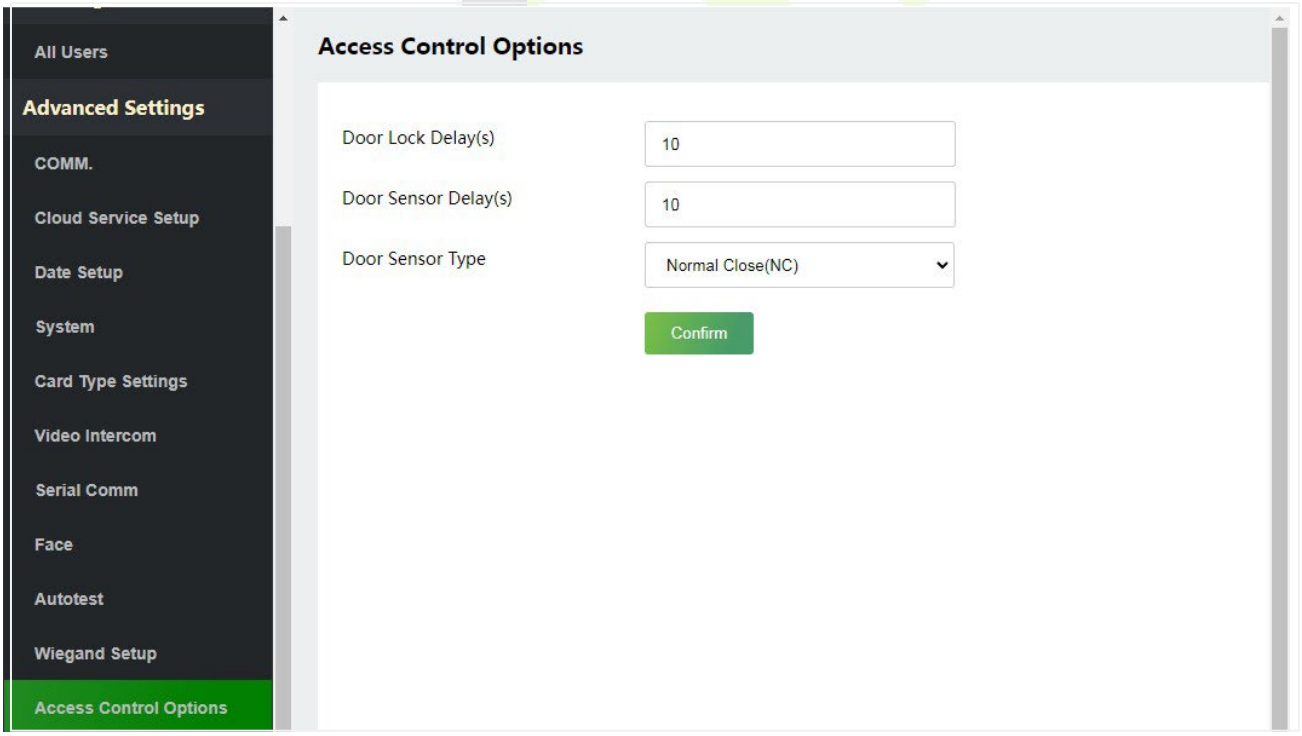
Terminal de Controle de Acesso



Função	Descrição
Atraso da Fechadura (s)	O tempo que o dispositivo controla a fechadura elétrica para permanecer no estado de desbloqueio. Valor válido: 1 a 99 segundos; 0 segundos representa a desativação da função.
Atraso do Sensor da Porta (s)	Se a porta não estiver trancada e permanecer aberta por uma determinada duração (Atraso do Sensor de Porta), um alarme será acionado. O valor válido para o Atraso do Sensor de Porta varia de 1 a 255 segundos.

Tipo de Sensor de Porta	Existem três tipos de sensores: **Nenhum, Normalmente Aberto** e **Normalmente Fechado**. **Nenhum:** Significa que o sensor de porta não está em uso. **Normalmente Aberto:** Significa que a porta está sempre aberta quando a energia elétrica está ligada. **Normalmente Fechado:** Significa que a porta está sempre fechada quando a energia elétrica está ligada.
Dispositivo Mestre	Ao configurar os dispositivos mestre e escravo, você pode definir o estado do dispositivo mestre como Saída ou Entrada. **Saída:** Um registro de verificação no dispositivo mestre é um registro de saída. **Entrada:** Um registro de verificação no dispositivo mestre é um registro de entrada.
Dispositivo Auxiliar	Ao configurar os dispositivos mestre e auxiliar, você pode definir o estado do dispositivo auxiliar como Saída ou Entrada. **Saída**: Um registro de autenticação no dispositivo auxiliar é um registro de saída. **Entrada**: Um registro de autenticação no dispositivo auxiliar é um registro de entrada.

Terminal de Registro de Presença

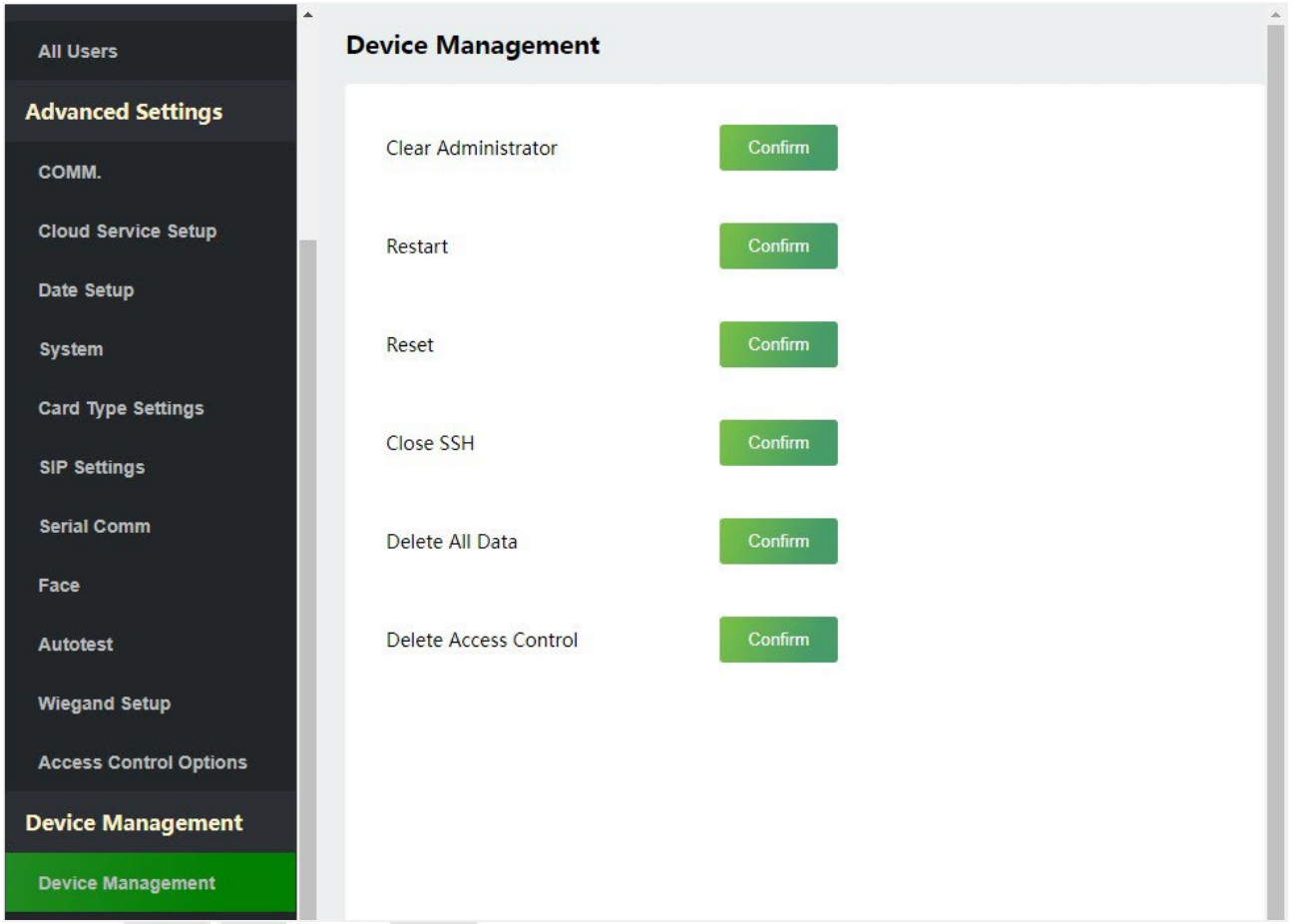


Função	Descrição
Atraso da Fechadura (s)	O tempo que o dispositivo controla a fechadura elétrica para permanecer no estado de desbloqueio. Valor válido: 1 a 99 segundos; 0 segundos representa a desativação da função.
Atraso do Sensor da Porta (s)	Se a porta não estiver trancada e permanecer aberta por uma determinada duração (Atraso do Sensor de Porta), um alarme será acionado. O valor válido para o Atraso do Sensor de Porta varia de 1 a 255 segundos.
Tipo de Sensor de Porta	Existem três tipos de sensores: **Nenhum, Normalmente Aberto** e **Normalmente Fechado**. **Nenhum:** Significa que o sensor de porta não está em uso. **Normalmente Aberto:** Significa que a porta está sempre aberta quando a energia elétrica está ligada. **Normalmente Fechado:** Significa que a porta está sempre fechada quando a energia elétrica está ligada.

10 Gerenciamento de Dispositivos

10.1 Gerenciamento de Dispositivos

Clique em **Gerenciamento de Dispositivos** no Servidor Web.



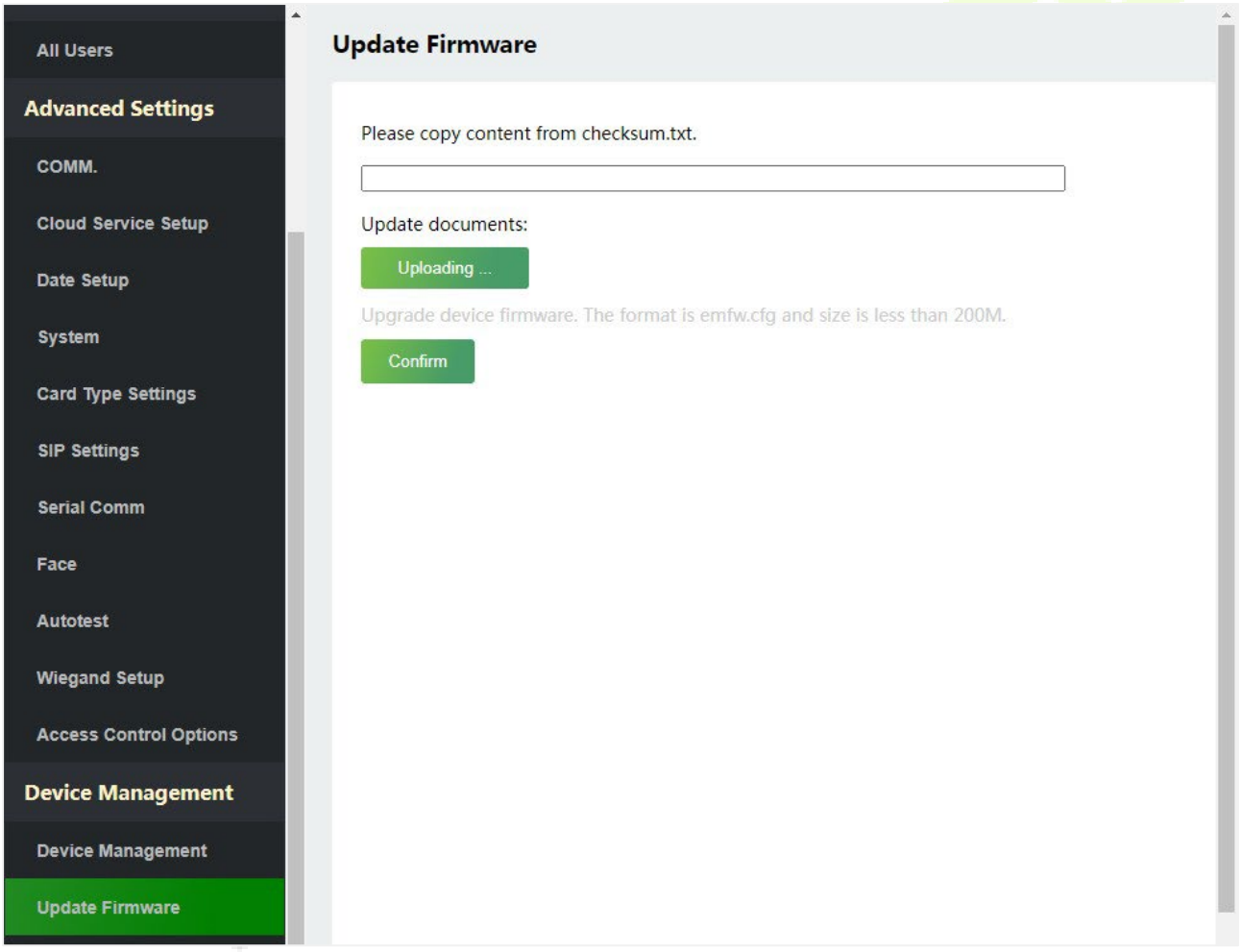
Função	Descrição
Limpar Administrador	Escolha se deseja alterar o super administrador para um usuário normal.
Reiniciar	Escolha se deseja reiniciar o dispositivo.
Reset	A função de Reset restaura as configurações do dispositivo, como as configurações de comunicação e do sistema, para as configurações padrão de fábrica (essa função não apaga os dados dos usuários registrados). ***Observação:*** Após o reset, o IP do dispositivo é restaurado para o original 192.168.1.201, por favor, consulte a seção 9.1 Configurações de Comunicação para modificar o IP.

Encerrar SSH	O SSH é usado para acessar o modo de manutenção do dispositivo. Escolha se deseja encerrar o SSH.
Excluir Todos os Dados	Para excluir as informações, registros de presença e registros de acesso de todos os usuários registrados.
Excluir Controle de Acesso	Para excluir os dados de controle de acesso do ProMA.

10.2 Atualizar Firmware

Clique em **Atualizar Firmware** no Servidor Web.

Selecione um arquivo de atualização e clique em **Confirmar** para concluir a operação de atualização do firmware.

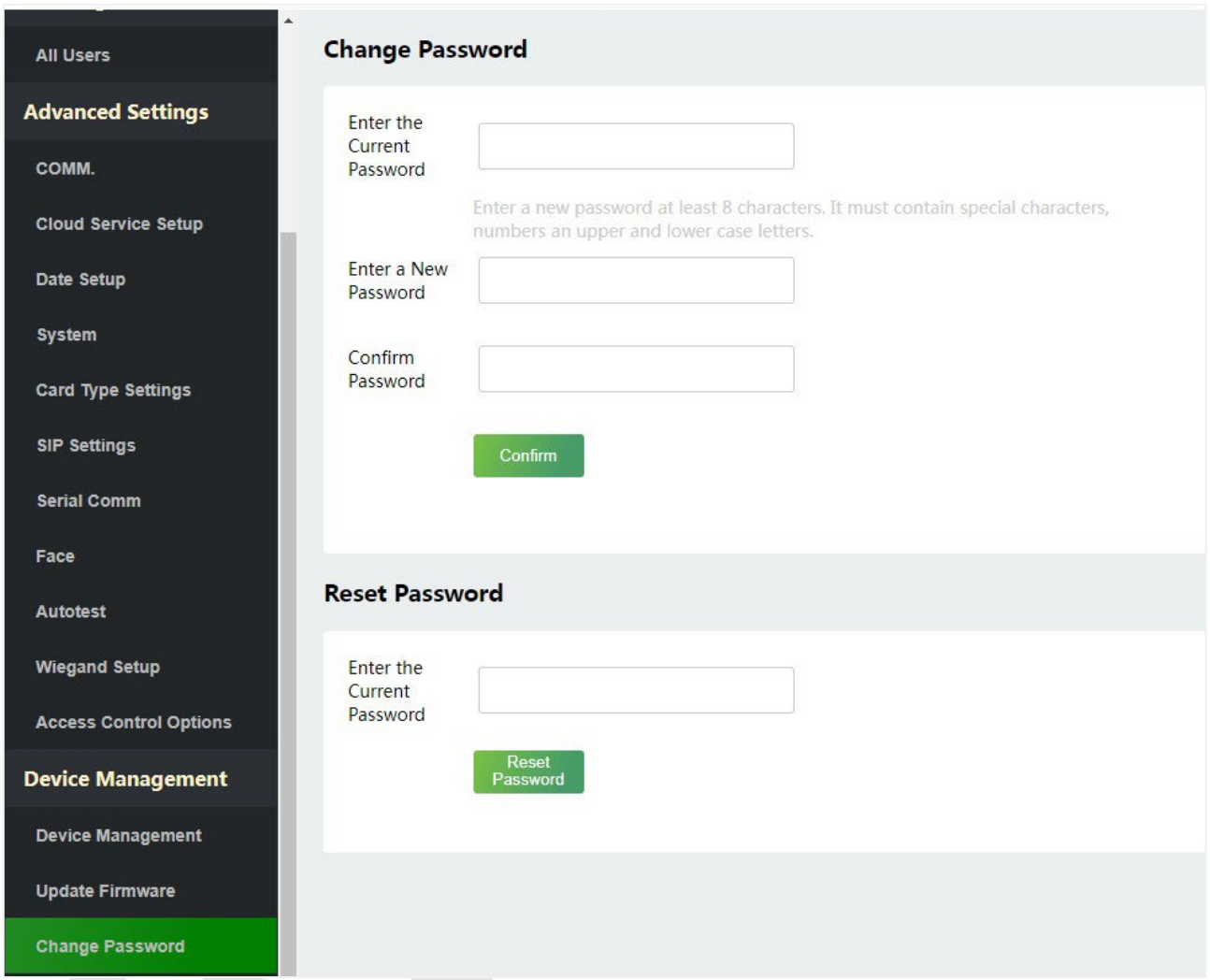


Observação: Se o arquivo de atualização for necessário, por favor, entre em contato com nosso suporte técnico. A atualização de firmware não é recomendada em circunstâncias normais.

10.3 Alterar Senha

Clique em **Alterar Senha** no Servidor Web.

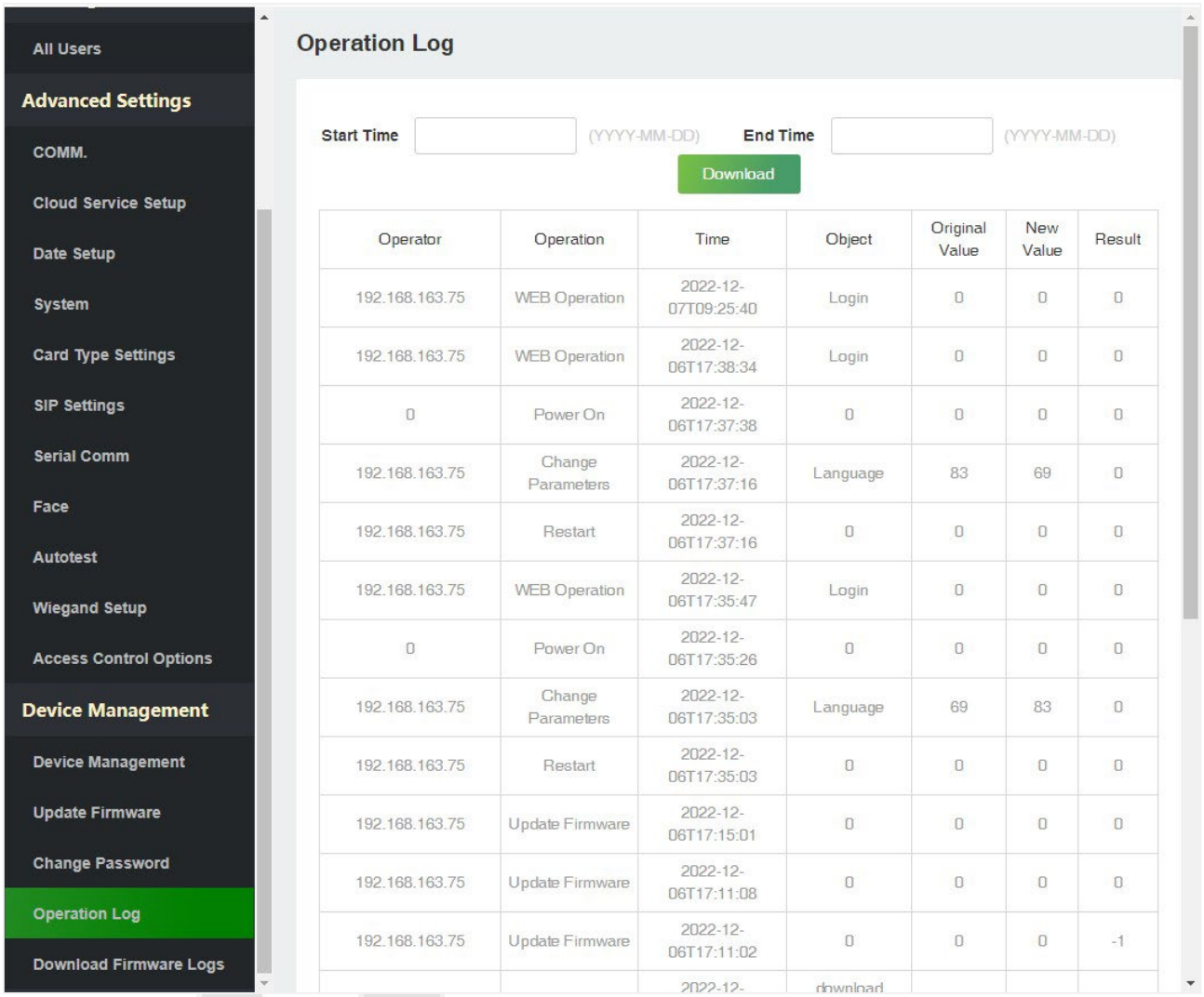
Nesta interface, você pode alterar a senha e redefinir a senha do Servidor Web.



10.4 Registro de Operações

Clique em **Registro de Operações** no Servidor Web.

Todos os registros de operações dos usuários no dispositivo ou no Servidor Web são salvos. Os usuários podem procurar e baixar esses registros por data/hora.

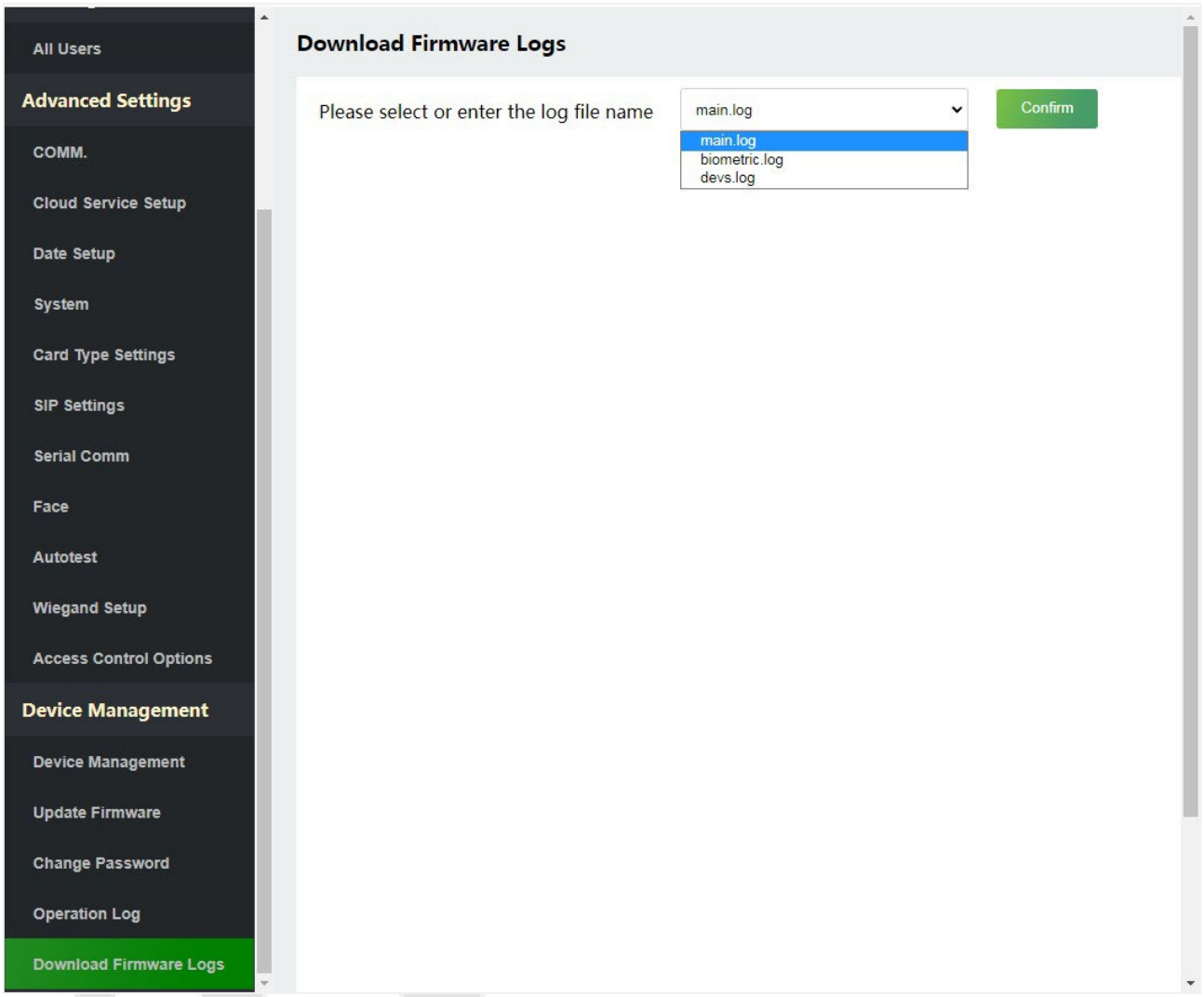


Operator	Operation	Time	Object	Original Value	New Value	Result
192.168.163.75	WEB Operation	2022-12-07T09:25:40	Login	0	0	0
192.168.163.75	WEB Operation	2022-12-06T17:38:34	Login	0	0	0
0	Power On	2022-12-06T17:37:38	0	0	0	0
192.168.163.75	Change Parameters	2022-12-06T17:37:16	Language	83	69	0
192.168.163.75	Restart	2022-12-06T17:37:16	0	0	0	0
192.168.163.75	WEB Operation	2022-12-06T17:35:47	Login	0	0	0
0	Power On	2022-12-06T17:35:26	0	0	0	0
192.168.163.75	Change Parameters	2022-12-06T17:35:03	Language	69	83	0
192.168.163.75	Restart	2022-12-06T17:35:03	0	0	0	0
192.168.163.75	Update Firmware	2022-12-06T17:15:01	0	0	0	0
192.168.163.75	Update Firmware	2022-12-06T17:11:08	0	0	0	0
192.168.163.75	Update Firmware	2022-12-06T17:11:02	0	0	0	-1
		2022-12-	download			

10.5 Baixar Registros de Firmware

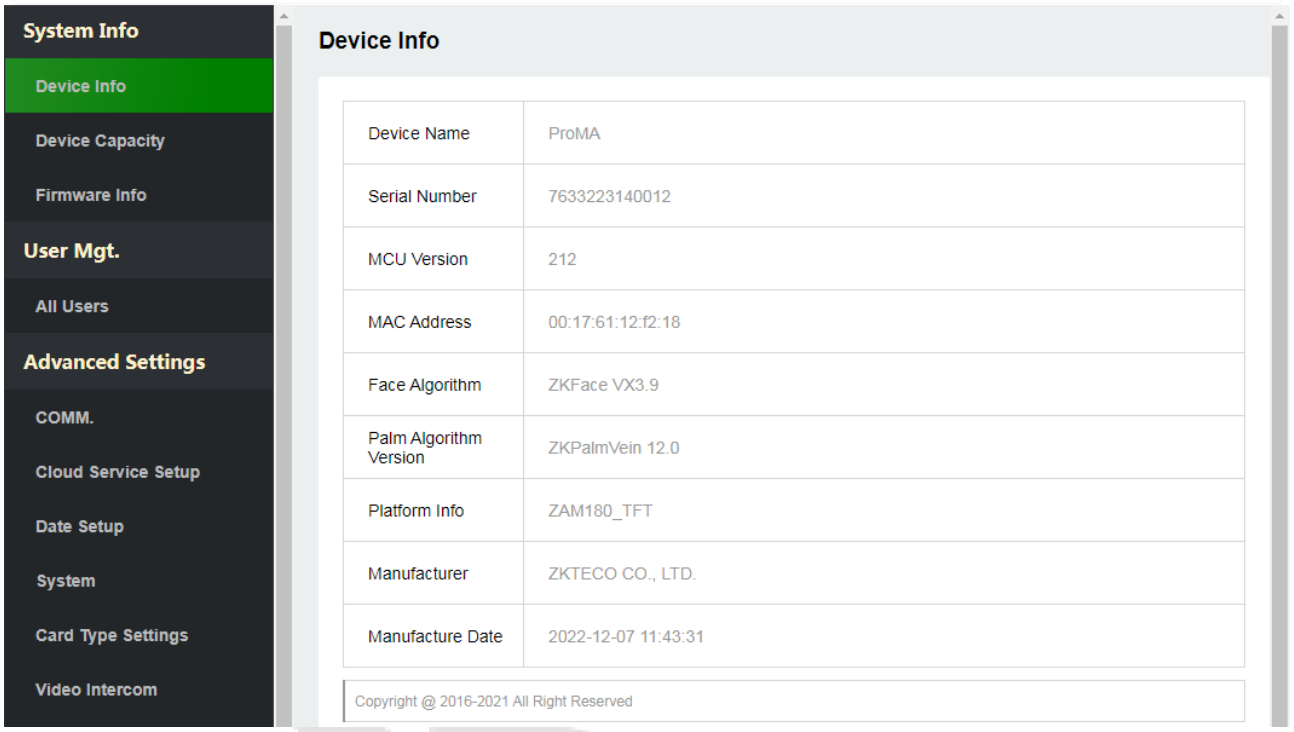
Clique em **Registro de Operações** no Servidor Web.

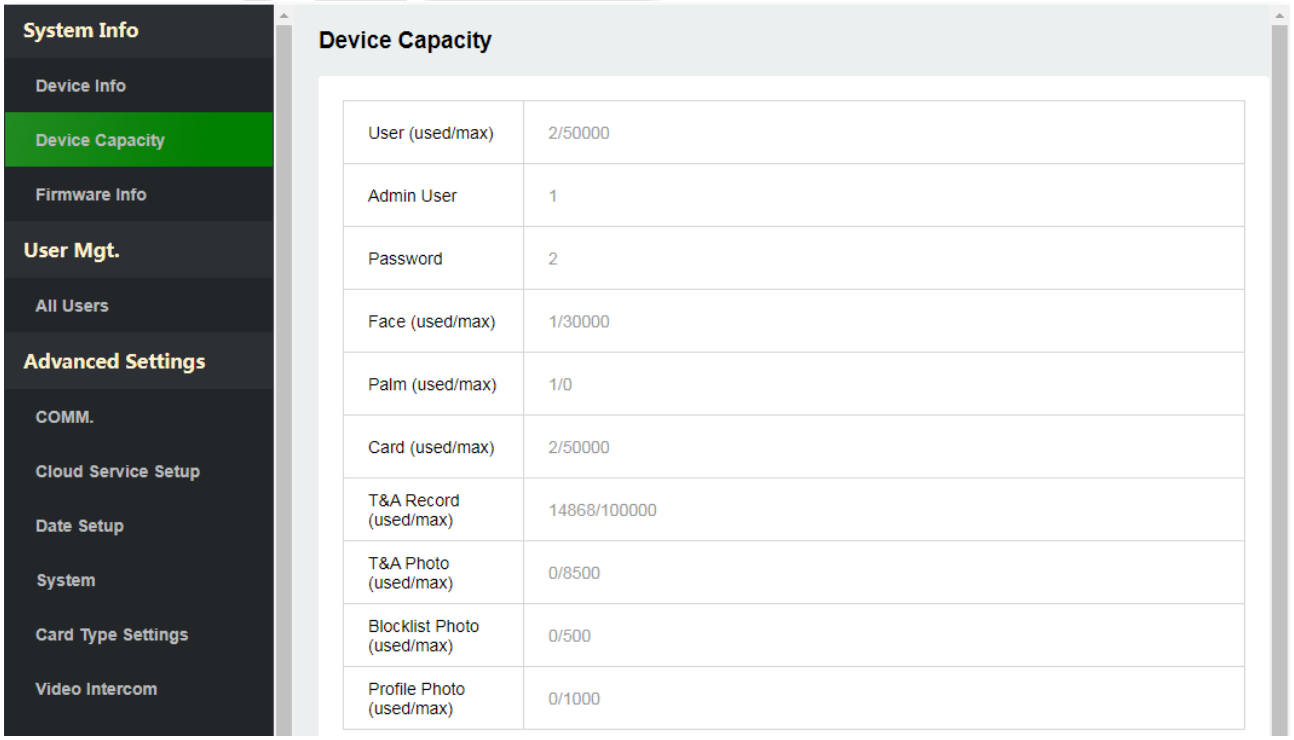
Nesta interface, você pode selecionar baixar o arquivo main.log, biometric.log ou dev.log.

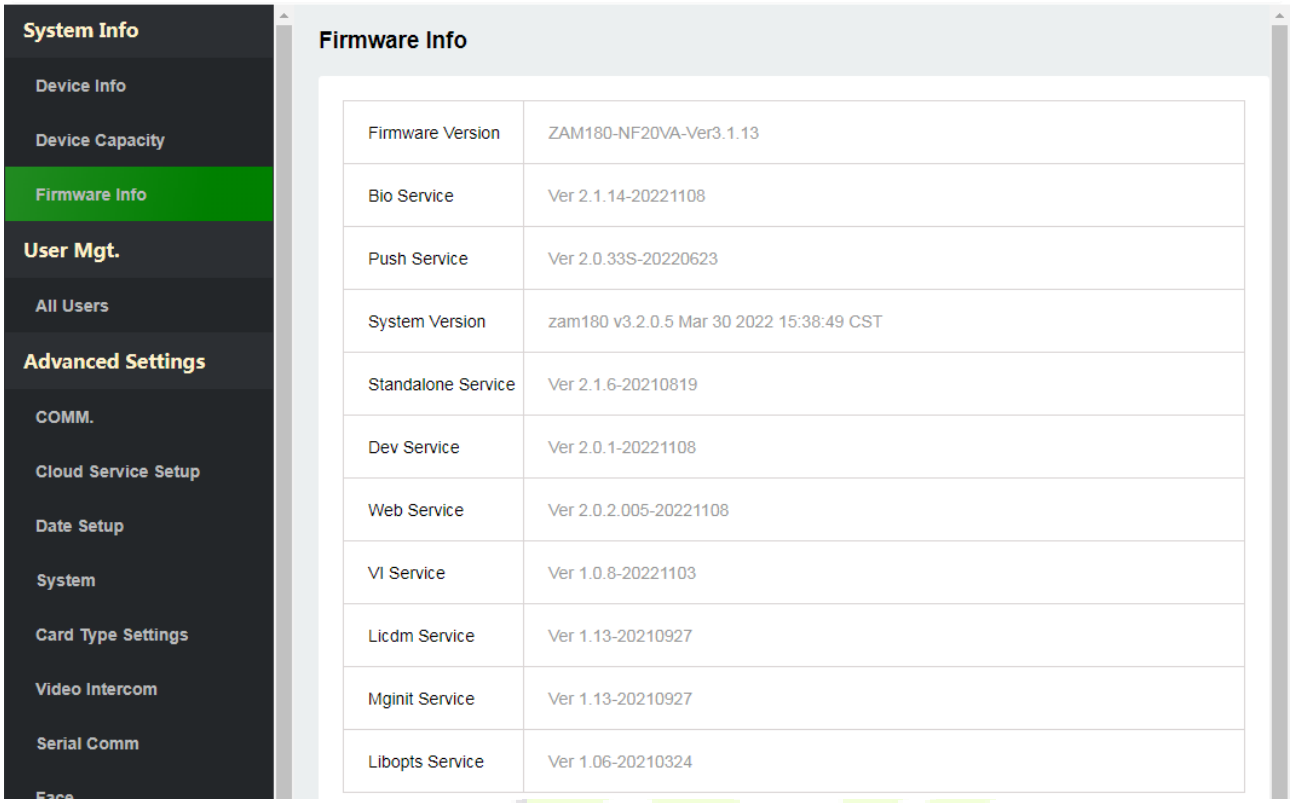


11 Informações do Sistema

Clique em **Informações do Sistema** no Servidor Web.
Nesta interface, você pode visualizar a capacidade de dados, informações do dispositivo e informações do firmware do dispositivo atual.







Função	Descrição
Informações do Dispositivo	Exibe o nome do dispositivo, número de série, versão do MCU, endereço MAC, informações da versão do algoritmo de impressão digital★ e reconhecimento facial, plataforma e informações do fabricante.
Capacidade do Dispositivo	Exibe o armazenamento de usuários do dispositivo atual, armazenamento de senhas, palmas★, impressões digitais★, cartões e faces, administradores, registros de presença e fotos de lista de presença e lista de bloqueios.
Firmware Information	Exibe a versão do firmware e outras informações de versão do dispositivo.

12 Conectar ao Software ZKBio CVSecurity

12.1 Configurar o Endereço de Comunicação

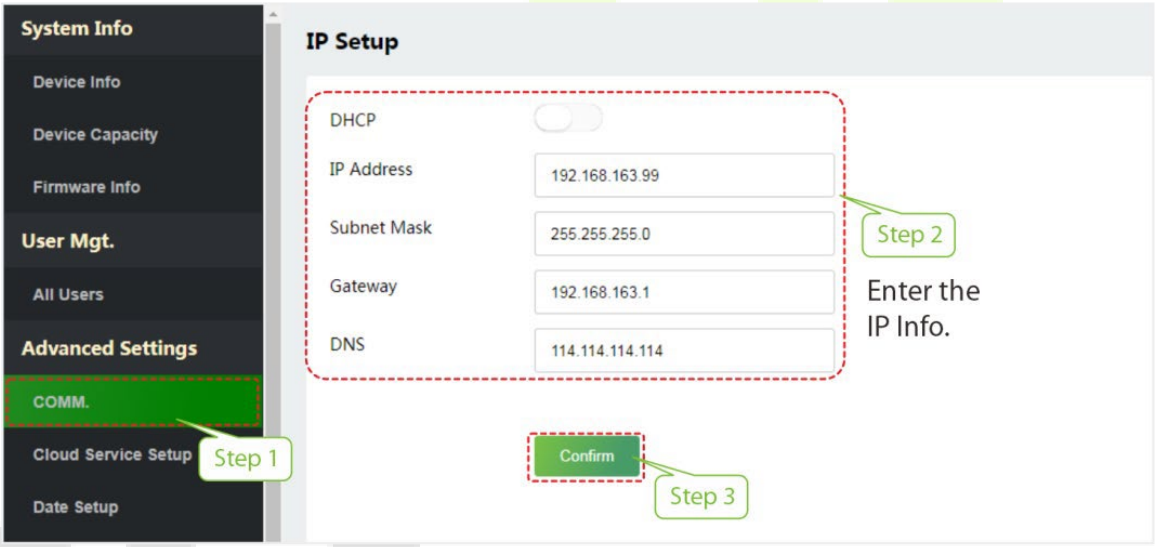
1. Clique em **Config. Com.** > **Configuração de IP** no Servidor Web para definir o endereço IP e gateway do dispositivo.

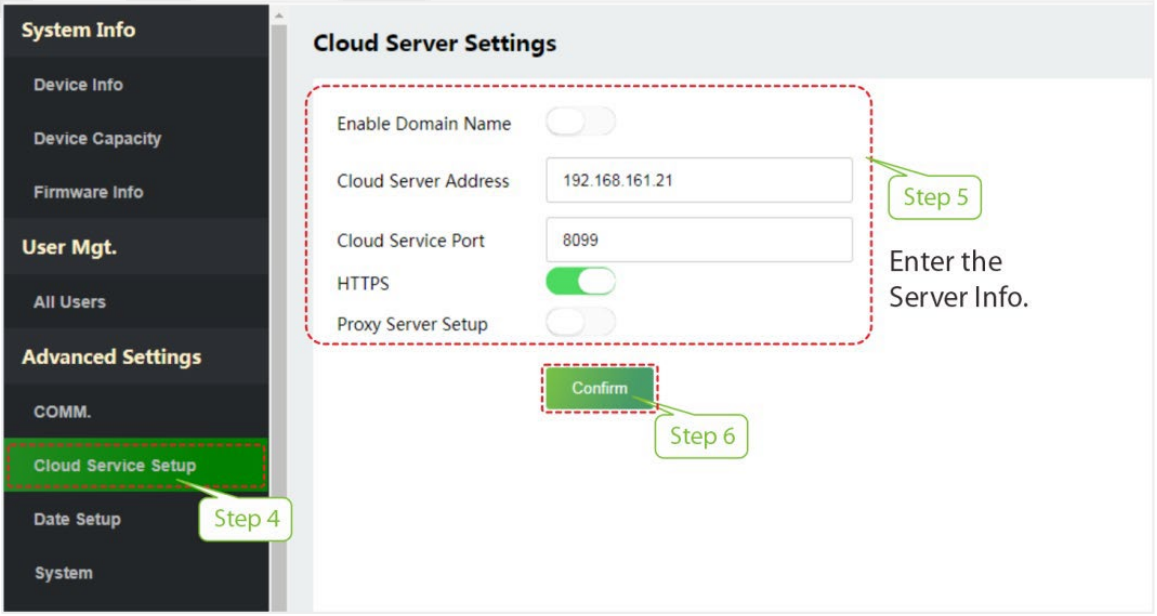
Observação: O endereço IP deve ser capaz de se comunicar com o servidor ZKBio CVSecurity, preferencialmente no mesmo segmento de rede do endereço do servidor.

2. No Servidor Web, clique em **Configuração do Servidor Cloud** para definir o endereço do servidor e a porta do servidor.

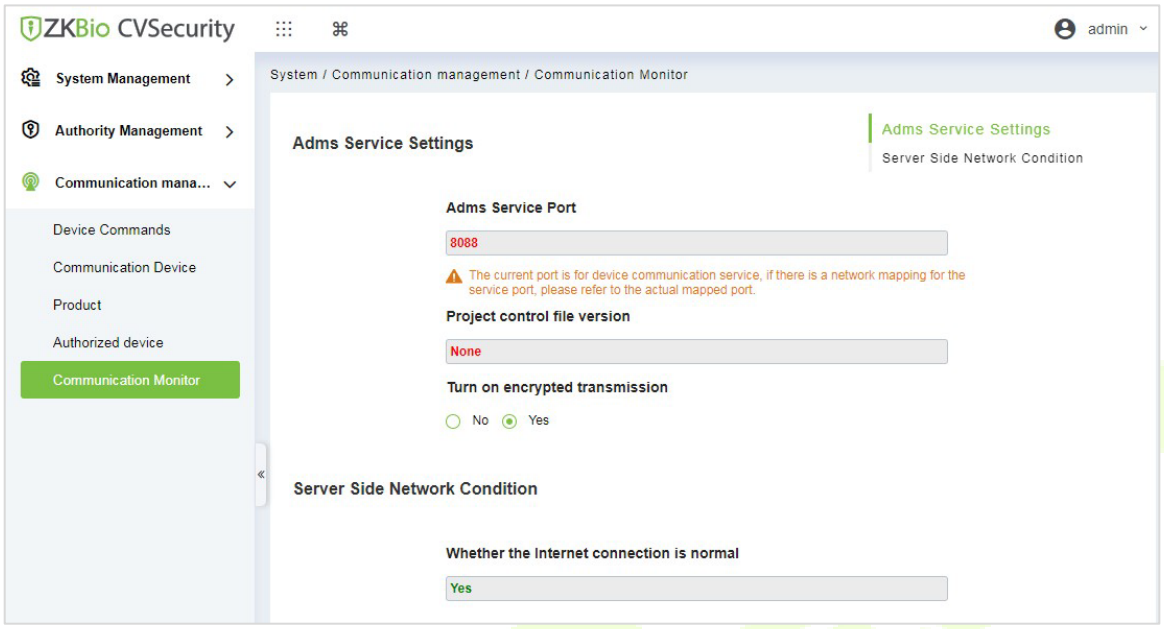
Endereço do servidor: Configure o endereço IP do servidor ZKBio CVSecurity.

Porta do servidor: Configure a porta do servidor de acordo com o ZKBio CVSecurity (O padrão é 8808).





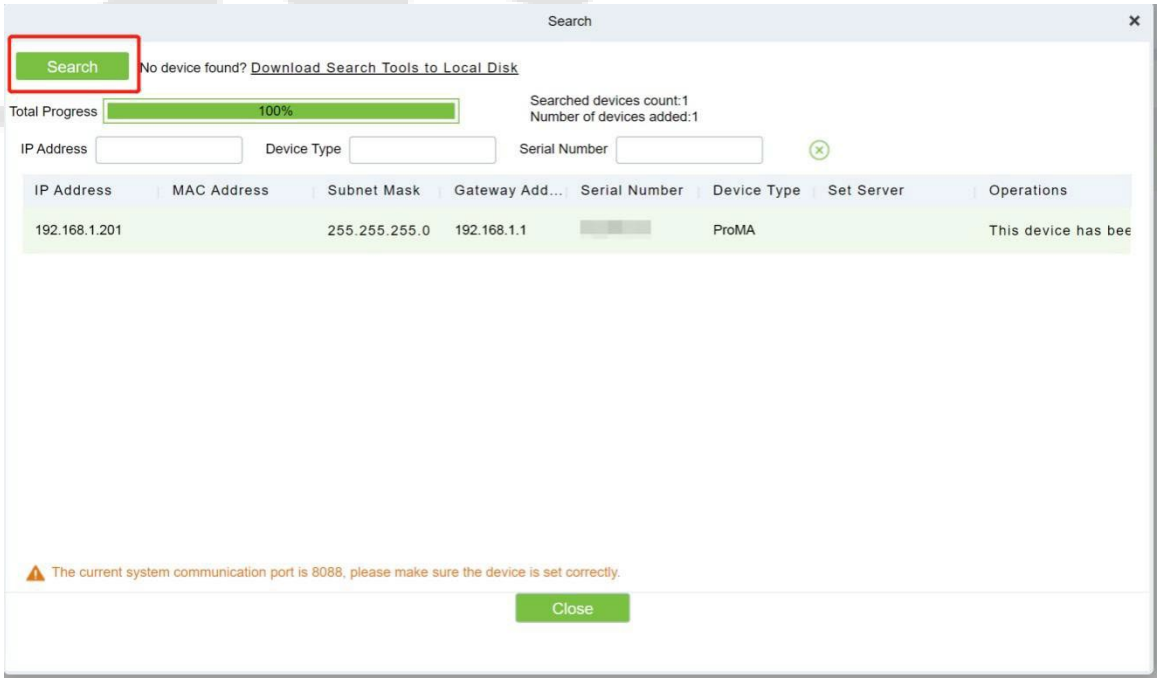
3. Faça login no software ZKBio CVSecurity, clique em **Sistema > Gerenciamento de Comunicação > Monitor de Comunicação** para configurar a Porta do Serviço ADMS, conforme mostrado na figura abaixo:



12.2 Adicionar Dispositivo no Software

Adicione o dispositivo pesquisando. O processo é o seguinte:

1) Clique em **Acesso > Dispositivo > Pesquisar** para abrir a interface de pesquisa no software.
2) Clique em **Pesquisar** e será exibida a mensagem "Pesquisando...".
3) Após a pesquisa, a lista e o número total de controladoras de acesso serão exibidos.

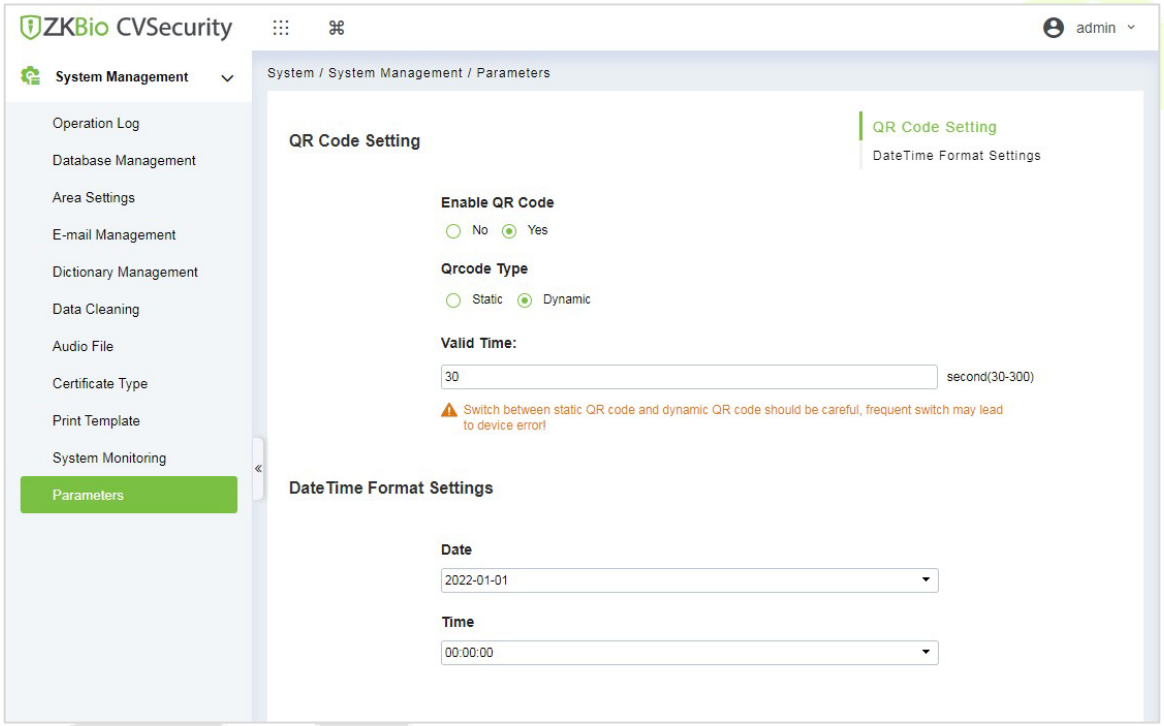


Clique em **Adicionar** na coluna de operação e uma nova janela será aberta. Selecione o tipo de ícone, área e adicione ao nível em cada menu suspenso e clique em **OK** para adicionar o dispositivo.

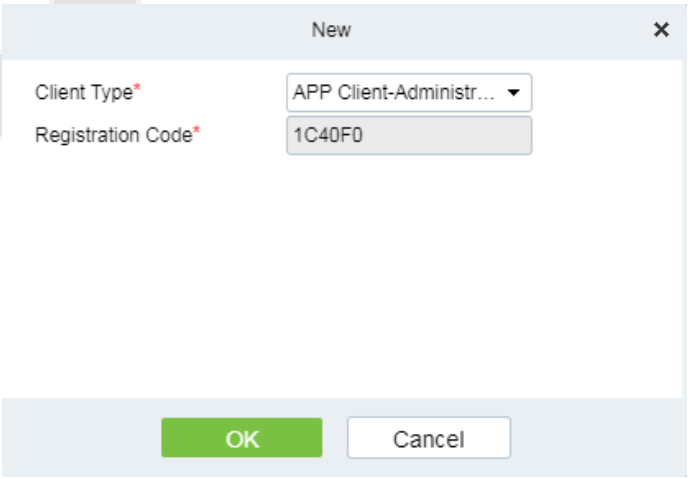
12.3 Credencial Móvel ★

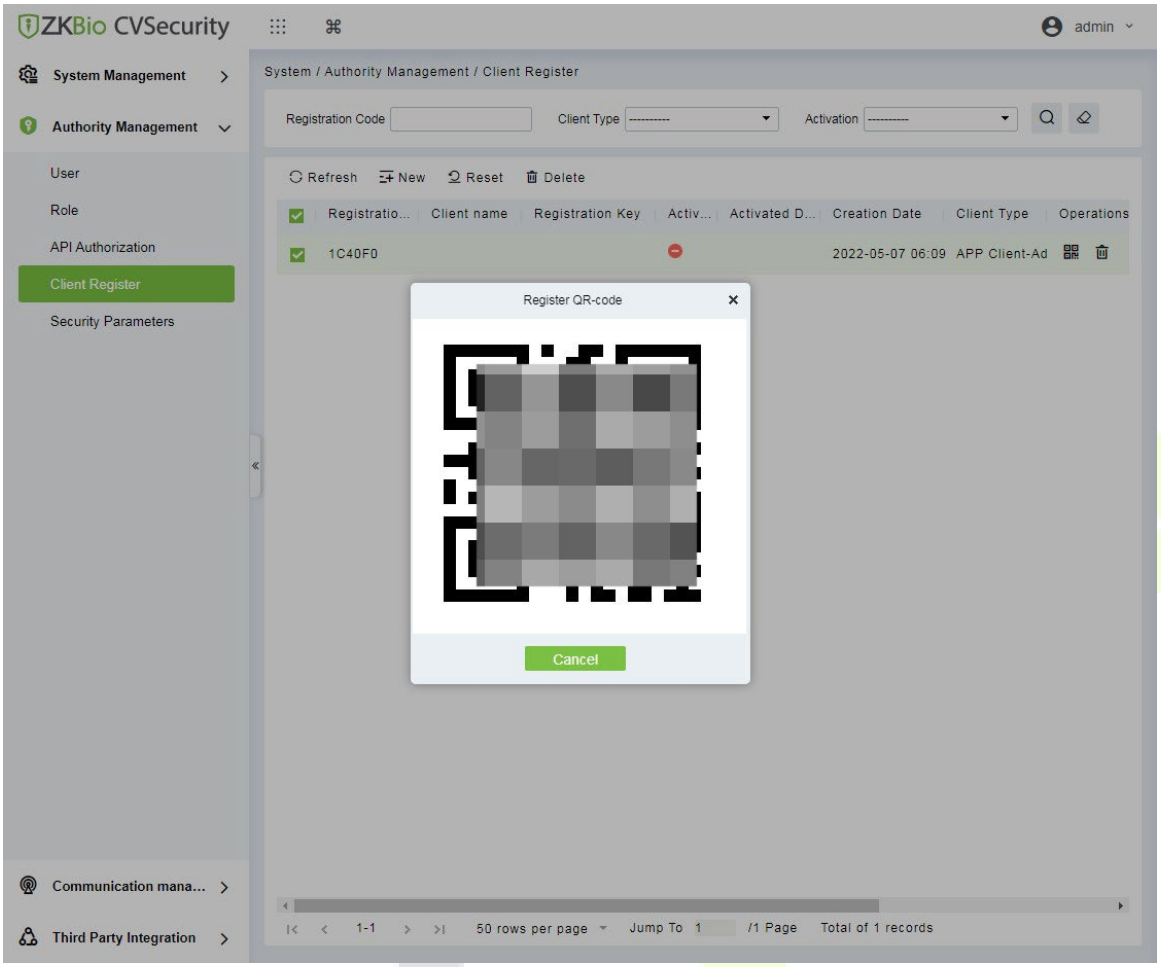
Após baixar e instalar o aplicativo, o usuário precisa configurar o Servidor antes de fazer o login. Os passos são os seguintes:

1. No ZKBio CVSecurity, acesse **Sistema > Gerenciamento de Sistema > Parâmetros** e defina **Habilitar** Código QR como **Sim**. Selecione o status do código QR de acordo com a situação real. O padrão é Dinâmico, e é possível definir o tempo de validade do código QR.

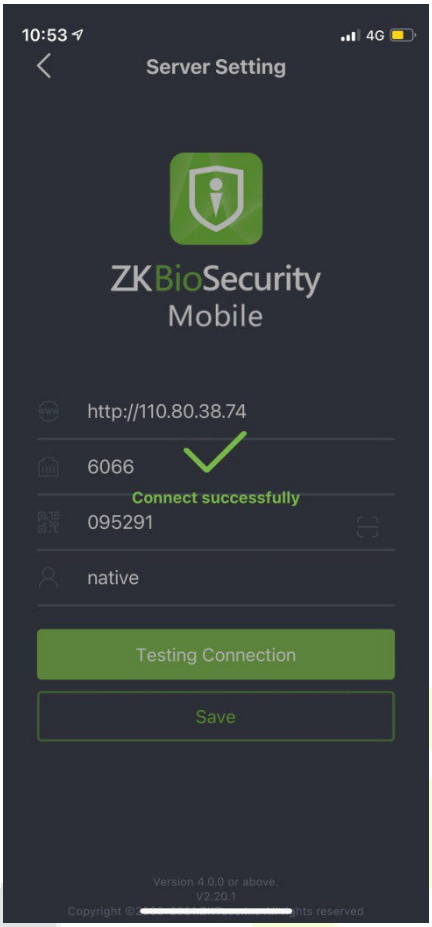


2. No Servidor, escolha **Sistema > Gerenciamento de Autoridade > Registro do Cliente** para adicionar um cliente de aplicativo registrado.





3. Abra o aplicativo no smartphone. Na tela de login, toque em **Configuração do Servidor** e digite o Endereço IP ou o Nome de Domínio do Servidor, juntamente com o Número da Porta.
4. Toque no ícone do **QR Code** para escanear o código QR do novo cliente do aplicativo. Após a identificação bem-sucedida do cliente, defina o Nome do Cliente e toque em **Teste de Conexão**.
5. Após a conexão de rede ser estabelecida com sucesso, toque em **Salvar**.

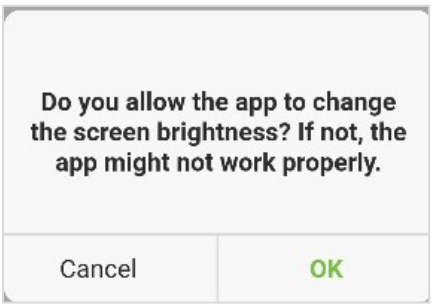


A função de Credencial Móvel só é válida ao fazer login como funcionário. Toque em Funcionário para alternar para a tela de login de funcionário. Insira o ID do funcionário e a senha (padrão: 123456) para fazer o login.

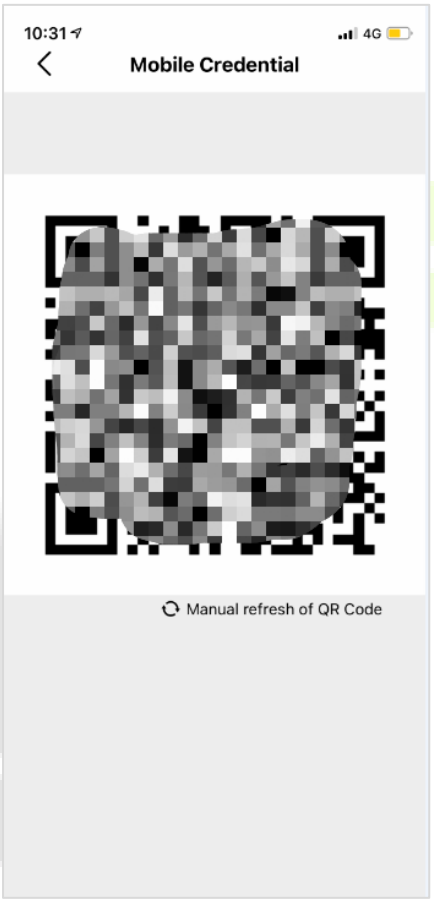
6. Toque em **Credencial Móvel** no aplicativo e um código QR será exibido, que contém informações como ID do funcionário e número do cartão (o código QR estático contém apenas o número do cartão).

   O código QR pode substituir um cartão físico em um dispositivo específico para realizar autenticação sem contato e abrir a porta.

Ao usar essa função pela primeira vez, o aplicativo solicitará autorização para modificar as configurações de brilho da tela, conforme mostrado na figura:



O código QR é atualizado automaticamente a cada 30 segundos e também suporta atualização manual.



Observação: Para outras operações específicas, por favor, consulte o Manual do Usuário do ZKBioSecurity Mobile App.

Apêndice 1

Requisitos para Cadastro no equipamento:

1) É recomendado realizar o registro em um ambiente interno com uma fonte de luz adequada, evitando subexposição ou superexposição.

2) Evite fotografar em direção a fontes de luz externas, como portas, janelas ou outras fontes de luz intensa.

3) Recomenda-se o uso de roupas de cores escuras que sejam diferentes da cor de fundo para o registro.

4) Por favor, mostre seu rosto e testa, evitando cobrir o rosto e as sobrancelhas com o cabelo.

5) A foto digital deve ter bordas retas, ser colorida e retratar apenas uma pessoa, que deve estar sem acessórios e de forma casual. Pessoas que usam óculos devem permanecer usando-os para a foto.

6) Não use acessórios como lenço ou máscara que possam cobrir a boca ou o queixo.

7) Por favor, posicione-se de frente para o dispositivo de captura e localize seu rosto na área de captura de imagem, conforme mostrado na Imagem 1.

8) Não inclua mais de um rosto na área de captura.

9) A distância recomendada para captura é de 50 cm a 80 cm, ajustável de acordo com a altura do corpo.

Requisitos para Upload de fotos no software

A foto deve ser reta, colorida, meio retratada com apenas uma pessoa e ela não deve possuir cadastro no sistema. As pessoas que usam óculos, devem permanecer de óculos para obter a captura foto via webcam ou upload da foto da pessoa usando óculos.

- **Distância dos olhos**

200 pixels ou mais são recomendados com não menos de 115 pixels de distância.

- **Expressão Facial**

Rosto neutro ou sorriso simples e olhos naturalmente abertos são recomendados.

- **Gesto e ângulo**

O ângulo de rotação horizontal não deve exceder ±10°, a elevação não deve exceder ±10° e o ângulo de depressão não deve exceder ±10°.

- **Acessórios**

Máscaras ou óculos coloridos não são permitidos durante o cadastro. A armação dos óculos não deve cobrir os olhos e não deve refletir a luz. Para pessoas com armação de óculos grossa, recomenda-se capturar duas imagens, uma com óculos e outra sem os óculos.

- **Face**

Rosto completo com contorno claro, escala real, luz uniformemente distribuída e sem sombra.

- **Formato de imagem**

Deve estar em BMP, JPG, ou JPEG.

- **Requisito de dados**

Deve seguir os requisitos:

1) Fundo branco com roupa de cor escura.
2) Modo de cor 24 bits.
3) A resolução deve estar entre 358 x 441 a 1080 x 1920.
4) A escala vertical da cabeça e do corpo deve estar na proporção de 2:1.
5) A foto deve incluir os ombros da pessoa capturada no mesmo nível horizontal.
6) Os olhos da pessoa capturada devem estar abertos e com a íris claramente visível.
7) Rosto ou sorriso simples são recomendados, sorriso excessivo mostrando os dentes não é recomendado.
8) A foto da pessoa capturada deve ser claramente visível, de cor natural, sem sombras fortes ou pontos de luz ou reflexos no rosto ou no fundo. O nível de contraste e luminosidade deve ser adequado.

Apêndice 2

Política de Privacidade

Aviso:

Para ajudar você a utilizar melhor os produtos e serviços da ZKTeco (doravante referido como "nós", "nosso" ou "nossos"), um provedor de serviços inteligentes, coletamos consistentemente suas informações pessoais. Como entendemos a importância de suas informações pessoais, levamos sua privacidade a sério e formulamos esta política de privacidade para proteger suas informações pessoais. Listamos abaixo as políticas de privacidade para compreender precisamente os dados e as medidas de proteção de privacidade relacionadas aos nossos produtos e serviços inteligentes.

Antes de utilizar nossos produtos e serviços, leia atentamente e compreenda todas as regras e disposições desta Política de Privacidade. Se você não concorda com o acordo relevante ou qualquer um de seus termos, deve parar de usar nossos produtos e serviços.

I. Informações Coletadas

Para garantir o funcionamento normal do produto e auxiliar na melhoria do serviço, coletaremos as informações fornecidas voluntariamente por você ou autorizadas por você durante o registro e uso, ou geradas como resultado do seu uso dos serviços.

1. **Informações de Registro do Usuário:** No momento do seu primeiro registro, o template biométrico **(modelo de impressão digital/modelo de face/modelo de palma)** será salvo no dispositivo de acordo com o tipo de dispositivo selecionado para verificar a semelhança única entre você e o ID do usuário registrado. Você pode inserir opcionalmente seu Nome e Código. As informações acima são necessárias para que você possa usar nossos produtos. Se você não fornecer tais informações, não poderá utilizar algumas funcionalidades do produto regularmente.

2. **Informações do Produto:** De acordo com o modelo do produto e a permissão concedida por você durante a instalação e uso de nossos serviços, as informações relacionadas ao produto no qual nossos serviços são utilizados serão coletadas quando o produto estiver conectado ao software, incluindo o Modelo do Produto, Número da Versão do Firmware, Número de Série do Produto e Informações de Capacidade do Produto. **Ao conectar seu produto ao software, leia atentamente a política de privacidade específica do software**

II. Segurança e Gerenciamento do Produto

1. Quando você utiliza nossos produtos pela primeira vez, é necessário definir o privilégio de Administrador antes de realizar operações específicas. Caso contrário, você receberá lembretes frequentes para definir o privilégio de Administrador ao acessar a interface do menu principal.

Se você ainda não definir o privilégio de Administrador após receber o aviso do sistema, você deve estar ciente do possível risco de segurança (por exemplo, os dados podem ser modificados manualmente).

2. Todas as funções de exibição das informações biométricas estão desativadas por padrão em nossos produtos. Você pode escolher Menu > Configurações do Sistema para definir se deseja exibir as informações biométricas. Se você habilitar essas funções, assumimos que você está ciente dos riscos de segurança da privacidade pessoal especificados na política de privacidade.

3. Apenas o seu ID de usuário é exibido por padrão. Você pode configurar se deseja exibir outras informações de verificação do usuário (como Nome, Departamento, Foto, etc.) sob o privilégio de Administrador. **Se você optar por exibir tais informações, assumimos que você está ciente dos potenciais riscos de segurança (por exemplo, sua foto será exibida na interface do dispositivo).**

4. A função de câmera está desativada por padrão em nossos produtos. Se você deseja habilitar essa função para tirar fotos de si mesmo para registro de presença ou tirar fotos de estranhos para controle de acesso, o produto ativará o tom de aviso da câmera. **Uma vez que você habilite essa função, assumimos que você está ciente dos potenciais riscos de segurança.**

5. Todos os dados coletados por nossos produtos são criptografados usando o algoritmo AES 256. Todos os dados enviados pelo Administrador para nossos produtos são automaticamente criptografados usando o algoritmo AES 256 e armazenados com segurança. Se o Administrador fizer o download de dados de nossos produtos, assumimos que você precisa processar os dados e está ciente do potencial risco de segurança. Nesse caso, você é responsável pelo armazenamento dos dados. Esteja ciente de que alguns dados não podem ser baixados por questões de segurança dos dados.

6. Todas as informações pessoais em nossos produtos podem ser consultadas, modificadas ou excluídas. Se você não utilizar mais nossos produtos, por favor, apague seus dados pessoais.

III. Outros

Você pode visitar o site https://www.zkteco.com/en/index/Index/privacy_protection.html para obter mais informações sobre como coletamos, usamos e armazenamos suas informações pessoais com segurança. Para acompanhar o rápido desenvolvimento da tecnologia, ajustar as operações comerciais e atender às necessidades dos clientes, iremos constantemente analisar e otimizar nossas medidas e políticas de proteção de privacidade. Fique à vontade para visitar nosso site oficial a qualquer momento para conhecer nossa política de privacidade mais recente.

Operação Ecologicamente Correta

O "período de operação ecologicamente correto" do produto refere-se ao tempo durante o qual este produto não liberará nenhuma substância tóxica ou perigosa quando usado de acordo com os pré-requisitos deste manual. O período de operação ecologicamente correto especificado para este produto não inclui baterias ou outros componentes que se desgastam facilmente e devem ser substituídos periodicamente. O período operacional ecologicamente correto da bateria é de 5 anos.

Substâncias tóxicas ou perigosas e suas quantidades

Nome do componente	Substância/Elemento Perigoso/Tóxico					
	Chumbo (Pb)	Mercúrio (Hg)	Cádmio (Cd)	Cromo hexavalente (Cr6+)	Bifenilos Polibromados (PBB)	Éteres difenílicos polibromados (PBDE)
Resistores	×	○	○	○	○	○
Capacitores	×	○	○	○	○	○
Indutores	×	○	○	○	○	○
Diodo	×	○	○	○	○	○
Componentes ESD	×	○	○	○	○	○
Buzzer	×	○	○	○	○	○
Adaptador	×	○	○	○	○	○
Parafusos	○	○	○	×	○	○

○ indica que a quantidade total de conteúdo tóxico em todos os materiais homogêneos está abaixo do limite, conforme especificado no SJ/T 11363—2006.
× indica que a quantidade total de conteúdo tóxico em todos os materiais homogêneos excede o limite, conforme especificado no SJ/T 11363—2006.

NOTA: 80% dos componentes deste produto são fabricados utilizando materiais que não são tóxicos e ecologicamente corretos. Os componentes que contêm toxinas ou elementos nocivos são incluídos devido às atuais limitações econômicas ou técnicas que impedem sua substituição por materiais não tóxicos.

Garantia

Este produto é garantido pela ZKTeco por um período de 3 meses (garantia legal), acrescidos de 9 meses de garantia adicional (garantia contratual), em um total de 1 ano, contra eventuais defeitos de material ou fabricação, desde que observadas as seguintes condições:

a) A garantia se aplica exclusivamente a produtos fornecidos pela ZKTeco do Brasil ou por Revenda Autorizada ZKTeco no Brasil.
b) O período de garantia será contado a partir da data de emissão da nota fiscal do produto.
c) Durante a garantia legal estão cobertos os custos de peças e serviços de reparo, que deverão ser realizados obrigatoriamente em Assistência Técnica ZKTeco ou na própria fábrica, conforme orientação da ZKTeco. Para o período de garantia contratual estão cobertos apenas os custos de peças que eventualmente necessitem substituição para reparo do produto, ficando excluídos os custos em relação aos serviços de manutenção (mão de obra), a remoção do produto (envio e retorno) e a visita/estadia de técnico especializado, se aplicável.
d) Detectado o defeito no produto, o usuário deverá entrar em contato com a ZKTeco nos canais de comunicação disponíveis em https://www.zkteco.com.br/suporte/, fornecendo informações sobre os produtos e problemas observados por meio do preenchimento e envio do formulário de Remessa de Material para Assistência Técnica (RMA) disponível em https://www.zkteco.com.br/manutencao/.
e) Recebidas as informações e o RMA, a ZKTeco analisará o caso e informará ao usuário sobre os próximos passos, bem como sobre a documentação que deve ser encaminhada em caso de envio do produto para a ZKTeco ou Assistência Técnica ZKTeco e/ou sobre opções para agendamento de visita técnica, quando aplicável.
f) Produtos enviados para a ZKTeco ou para Assistência Técnica ZKTeco sem notificação prévia e expressa autorização da ZKTeco não serão recebidos.
g) O produto e as peças substituídas serão garantidas pelo restante do prazo original, sendo que as peças retiradas dos produtos e/ou produtos eventualmente descartados serão de propriedade da ZKTeco.
h) Em caso de dúvidas o usuário deverá entrar em contato com a ZKTeco nos canais de comunicação disponíveis em https://www.zkteco.com.br/suporte/

Resultará nula e sem efeito esta garantia em caso de:

a) Produto que apresente lacres rompidos e/ou etiqueta de identificação violada.
b) Uso anormal do produto, inclusive em desconformidade com seu manual, especificações, desenhos, folhas de instruções ou quaisquer outros documentos relacionados, bem como em capacidade além de seus limites e taxas prescritas.
c) Uso indevido ou erro de instalação, operação, testes, armazenamento e/ou manuseio do produto.
d) Manutenção e/ou alteração no produto não aprovada previamente pela ZKTeco.
e) Defeitos e danos causados por agentes naturais (enchente, maresia e outros) ou exposição excessiva ao calor.
f) Defeitos e danos causados pelo uso de software e/ou hardware não compatíveis com especificações do produto.
g) Surtos e/ou picos de tensão na rede elétrica típicos de algumas regiões, para as quais deve-se utilizar dispositivos de proteção contra surtos elétricos.
h) Fatos ou eventos imprevisíveis ou de difícil previsão e de força maior.
i) Transporte do produto em embalagem ou de forma inadequada.
j) Furto ou roubo.
k) Desgaste natural do produto.
l) Danos exclusivamente causados pelo usuário ou por terceiros.

Em nenhum caso a ZKTeco será responsável por indenização superior ao preço da compra do produto, por qualquer perda de uso, perda de tempo, inconveniência, prejuízo comercial, perda de lucros ou economias ou outros danos diretos ou indiretos, decorrentes do uso ou impossibilidade de uso do produto.

A ZKTeco reserva-se o direito de alterar as condições e procedimentos aqui estabelecidos independente de aviso prévio, sendo de responsabilidade do usuário verificar periodicamente eventuais atualizações, que estarão disponíveis em https://www.zkteco.com.br/manutencao/. Nenhuma Revenda Credenciada ou Assistência Técnica ZKTeco tem autorização para modificar as condições aqui estabelecidas ou assumir outros compromissos em nome da ZKTeco.

Telefone: (31) 3055-3530

Endereço: Rodovia MG-010, KM 26
Loteamento 12 - Bairro Angicos
Vespasiano - MG - CEP: 33.206-240

www.zkteco.com.br