Guia de Usuário

AC-2000

https://www.acura.com.br

<Terminologia>

- **Admin, Administrador**.

- O administrador é o usuário que tem acesso ao Menu de configurações do terminal, que pode cadastrar/modificar/apagar usuários e mudar as configurações do terminal.

Caso não tenha nenhum administrador cadastrado, qualquer pessoa pode acessar o menu do terminal e mudar alguma configuração. Portanto, é extremamente recomendado que se tenha pelo menos um administrador cadastrado.

- O administrador tem permissão para mudar configurações importantes. Atenção ao fazer qualquer modificação no cadastro e operação.

- **Identificação 1:1 (Verificação 1:1)**

- Refere-se ao método no qual a digital inserida é comparada com a digital cadastrada no ID do usuário ou no Cartão.
- Esse método é chamado de Identificação 1:1 porque a digital é comparada somente com a digital cadastrada no banco de dados referenciada pelo ID ou no Cartão RFID do usuário.

- **Identificação 1:N**

- Refere-se ao método no qual a digital inserida é comparada com o banco de dados do terminal, sem que haja uma referência da digital com o ID ou cartão RFID do usuário.

- **TOC**

- TOC = Template On Card, significa que o cartão do tipo mifare carrega na memória a template da impressão digital.

- **Nível de Autenticação**

- É um nível de segurança de autenticação, tem escala de 1 a 9 de acordo com o grau de concordância. A autenticação vai ser sucedida quando o grau de concordância entre duas digitais comparadas for maior que o nível de autenticação estabelecido.
- Quanto maior o nível de autenticação, maior será o nível de segurança. Porém, requer maior taxa de concordância, então a probabilidade de ocorrer falha na autenticação pode aumentar.
- Nível 1:1 de autenticação é usado para Identificação 1:1
- Nível 1:N de autenticação é usado para Identificação 1:N

- **Método de autenticação**

- Os métodos de autenticação podem ser: autenticação por impressão digital (FP), autenticação por cartão (RF), por senha e várias formas de autenticação a partir da combinação destes métodos.
- Exemplo: Autenticação por Cartão ou Biometria se refere quando a autenticação for feita usando a biometria ou o cartão, um dos dois.

- **Detecção de Dedo Falso**

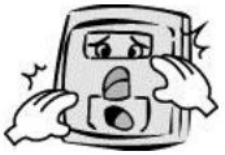
- Esta função permite somente a entrada de digitais reais e bloqueia a entrada de imitação de digitais produzidas usando borracha, papel, filme e silicone.

Tabela de Conteúdo

1. Antes de Ligar

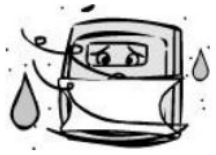
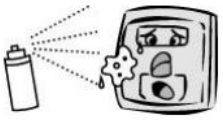
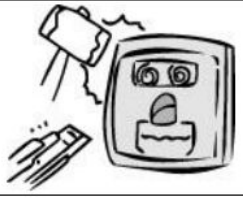
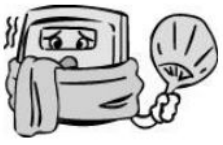
1.1. Notas de Segurança

- Avisos

Não opera o terminal com as mãos molhadas, e preste atenção para não deixar entrar nenhum líquido, como água, dentro do terminal. → Caso contrário, poderá ocorrer um mau funcionamento ou choque elétrico. 	Mantenha o terminal longe de inflamáveis → Caso contrário, poderá provocar um incêndio 
Não desmonte, repare ou remodele o terminal à sua disposição → Caso contrário, pode causar mau funcionamento, choque elétrico ou incêndio. 	Não permita que as crianças toquem o terminal descuidadamente. → Caso contrário, poderá causar acidentes de segurança das crianças ou mau funcionamento 

- O não cumprimento das instruções de segurança pode causar morte ou lesões graves aos utilizadores

- Precauções

Não instale o terminal em um local exposto à luz direta do sol → Caso contrário, pode causar mau funcionamento, deformação e descoloração. 	Não instale o terminal em locais úmidos ou poeirentos. → Caso contrário, pode causar mau funcionamento. 
Não limpe este terminal por aspersão de água, nem limpe com benzeno, diluente e álcool. → Caso contrário, pode causar choque elétrico ou incêndio. 	Mantenha o terminal longe de imãs. → Caso contrário, pode causar falha e mau funcionamento. 
Mantenha o Sensor Biométrico Limpo. → Caso contrário, a biometria pode não ser reconhecida. 	Não pulverizar inseticidas ou inflamáveis no terminal → Caso contrário, pode causar deformação e descoloração 
Mantenha o terminal afastado de choques ou objetos pontiagudos. → Caso contrário, pode danificar o terminal e resultar em mau funcionamento. 	Não instale o terminal em um local onde haja uma mudança de temperatura severa → Caso contrário, poderá causar mau funcionamento. 

- O não cumprimento das instruções de segurança pode causar lesões pessoais ou danos materiais aos utilizadores.

※ Não nos responsabilizamos por quaisquer acidentes e danos que possam resultar da não conformidade das informações contidas neste manual.

1.2. Descrição do Terminal

1.3. Sinal do LED mostrado durante operação

Azul	Alimentação	Ligado: Normal Oscilante: Comunicando via Bluetooth
Verde	Porta	Ligado: Porta aberta Desligado: Porta fechada
Vermelho	Alarme	Desligado: Normal Oscilante: Quando o terminal é violado ou se houver solicitação de autenticação com administração

※ O LED pode acender de forma simultânea em alguns casos (Ex. Vermelho e Azul piscando)

1.4. Sons de campainha usados durante operação

Beep	Quando uma digital é inserida ou um cartão é apresentado	- Quando o cartão é lido; - Quando a entrada de digital está concluída e que o usuário pode tirar o dedo
Be peep	Som de falha	- Falha na autenticação ou falha na captura
Brrrrrrp	Esperando pela entrada	- Notificando o status de espera da entrada de digital ou senha do usuário
Beeeep	Sucesso	- Sucesso na a autenticação ou a conclusão dos trabalhos

1.5. Cadastro e posicionamento adequado do dedo

- Posicionamento adequado do dedo

  Se possível, use o dedo indicador e insira o dedo como se estivesse carimbando sua digital. Somente encostar o dedo no sensor não é suficiente para efetuar o cadastro. A forma adequada é encostar o centro da digital no sensor biométrico.

- Se possível use o dedo indicador.

Usando o dedo indicador, pode-se obter uma impressão digital mais precisa e estável.

- Verifique se a digital está apagada ou se há cicatriz.

Dedo muito seco ou molhado, com digital apagada ou com cicatriz são difíceis de serem reconhecidos. Nesses casos, use um dedo diferente para cadastro.

- Condições das digitais dos usuários

  A digital pode não ser reconhecida ou ser inconveniente seu uso, dependendo das suas condições.

  ➢ Esse produto é um sistema de reconhecimento biométrico. Se a digital estiver danificada ou fraca, não deve ser usada. Nesse caso, use cartão RFID.

  ➢ Se a sua pele estiver muito seca, abafe sobre seu dedo para umedecê-lo.

  ➢ As digitais de crianças normalmente são muito pequenas ou são um pouco apagadas. É necessário recadastrar a digital a cada 6 meses.

  ➢ As digitais de idosos podem ser difíceis de ser cadastradas por possuírem as linhas das digitais muito finas.

  ➢ É recomendado o cadastro de pelo menos 2 digitais por pessoa.

2. Introdução do Produto

2.1. Recursos

- **Função auto detecção**
  - Basta posicionar a digital no sensor que a autenticação será executada sem necessitar inserir uma chave adicional.

- **Simples autenticação usando biometria**
  - O uso da tecnologia de identificação biométrica previne contra perda de senha, cartão, chave ou roubo. Com o uso de autenticação biometria o aumenta-se o nível de segurança.

- **Sistema de Controle de Acesso usando a rede (LAN)**
  - Como a comunicação entre o leitor biométrico e o servidor de autenticação é feito usando cabo UTP e protocolo TCP/IP, pode ser usada a instalação da rede local existente. A auto-detecção da rede 10/100Mbps fornece rápida velocidade e permite fácil gerenciamento e monitoração através da rede.

- **Vários e flexíveis métodos de controle de acesso**
  - Perfeita função de controle de acesso garantindo diferenciação de acesso para cada grupo de usuários.

- **Usado em aplicações para vários tipos de sistemas, como controle de acesso, controle de ponto* e controle de refeições**
  - Várias aplicações diferentes disponíveis. O método de operação pode ser configurado no menu do terminal.

    *No Brasil não é possível utilizá-lo como relógio de ponto devido à portaria MTE N.º1510, norma do Ministério do trabalho e Emprego que estabelece especificações técnicas para os aparelhos de Registro Eletrônico de Ponto (REP)

- **Alta capacidade de armazenamento do servidor**
  - Em caso de gerenciar as pessoas que entram com o servidor, ele permite tratar um número quase ilimitado de pessoas.

    Obs.: A velocidade de autenticação irá depender das configurações do computador utilizado como servidor.

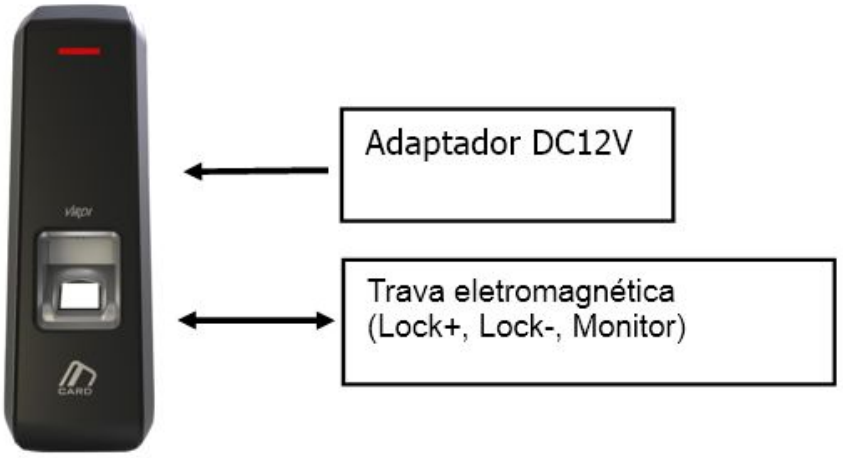
- **Vários métodos de cadastro e autenticação**

Existem 3 métodos de de autenticação disponíveis para os usuários (FP, Card, M.Key). Que devem ser escolhidos antes de fazer o cadastro do usuário ou do administrador.

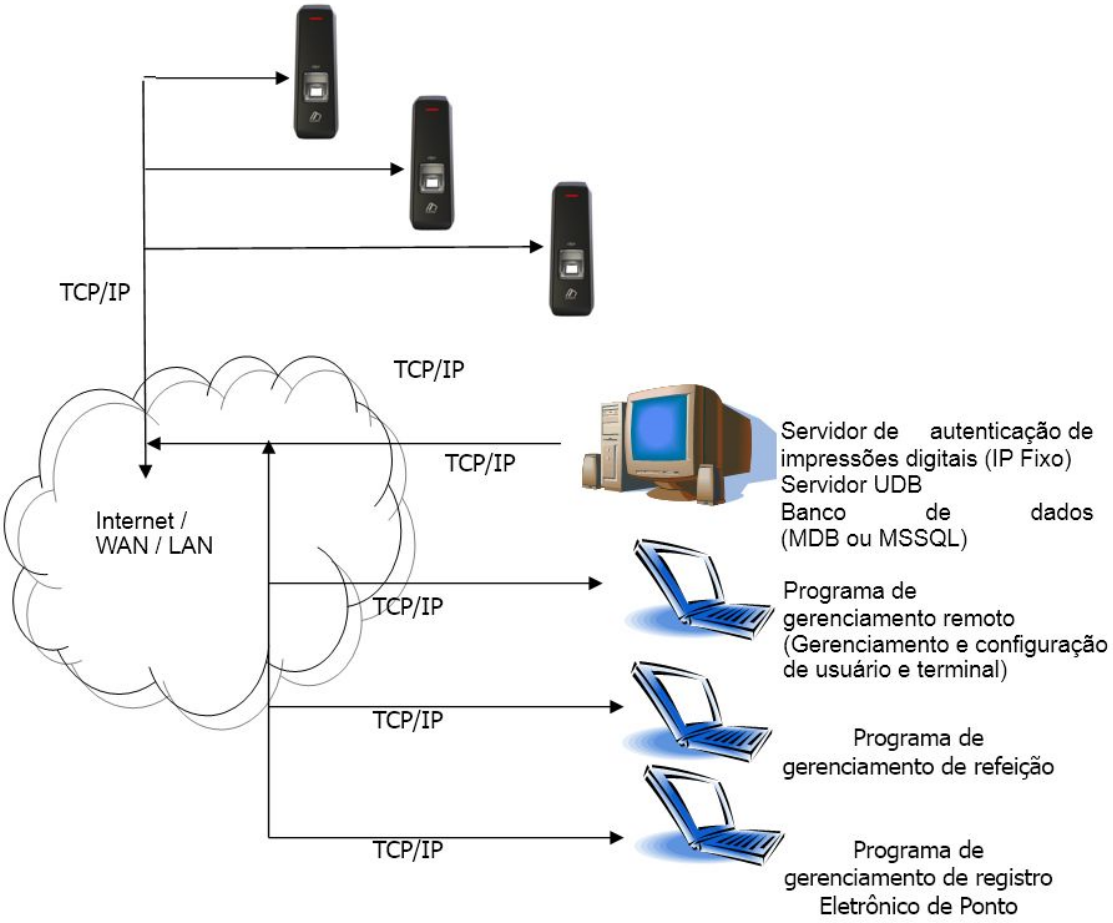
FP	Cadastro da digital Autenticação pela digital
Cartão	Cadastro do cartão Autenticação pelo cartão
M. Key	Cadastro do Mobile Key Autenticação pelo Mobile Key
Cartão ou FP	Cadastro do cartão e digital Autenticação pelo cartão ou digital
Cartão & FP	Cadastro do cartão e digital Autenticação pelo cartão seguido pela digital

2.2. Diagrama de Configuração

2.2.1. Stand Alone (Acesso)



2.2.2. Conexão com Servidor PC (Acesso, Time & Atendimento, Cafeteria)



2.3. Especificação

Divisão	ESPECIFICAÇÃO	OBSERVAÇÃO
CPU	32 Bit RISC CPU (400MHz)	
MEMÓRIA	64M DDR2 RAM	
	32M NOR FLASH	1.500 Usuários 1.500 Digitais 100.000 Logs
Sensor de Impressão Digital	Óptico	
Velocidade de Autenticação	Menos que 1 segundo	
Área de Escaneamento / Resolução	14.8 * 17.9mm / 500 DPI	
FRR / FAR	0.1% / 0.001%	
Temperatura /Umidade	-20 ~ 60 /Menor que 90% RH	
Adaptador AC / DC	ENTRADA: Universal AC 100 ~ 250V	
	SAÍDA: DC 12V	
	Certificados: UL, CSA, CE	
Controle de Fechadura	EM, Strike, Motor Lock, Porta Automática	
E/S	3 E (1 BT Saída, 2 Monitor) 1 S (Controle de Fechadura)	
Porta de Comunicação	TCP/IP (10/100Mbps)	Comunicação do servidor de autenticação
	Bluetooth	Aplicativo UNIS-B Plus
	RS-485	Comunicação do dispositivo externo
	Wiegand E/S	Leitor de cartão ou Comunicação do dispositivo externo
Leitor de Cartão	125KHz RF ou 13.56MHz Smart	14443A, 13.56MHz
Tamanho	58mm * 191mm * 62mm	

3. Configurando o Ambiente

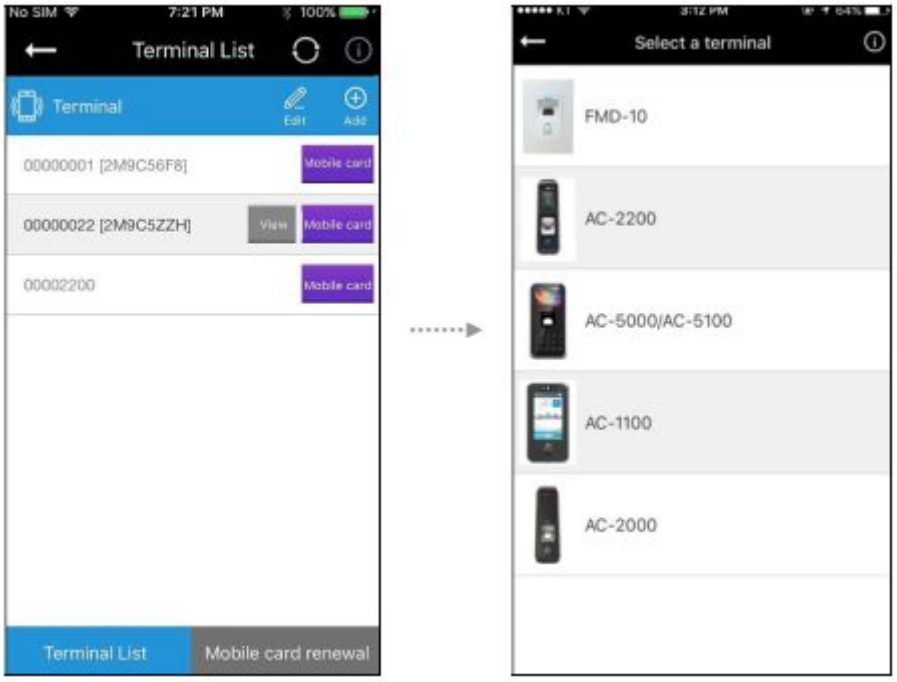
3.1. Pontos de verificação antes da configuração do ambiente

3.1.1 Executando o UNIS-B Plus (Aplicativo)

Abra o App Store no seu Smartphone e instale o Mobile App 'UNIS-B Plus'. Clique no ícone UNIS-B Plus instalado para executar o programa. Após a inicialização por mais de 2 segundos, a tela do menu de introdução será exibida automaticamente.

3.1.2 Adicionar Terminal

Ao selecionar [Adicionar] no canto superior direito de [Lista de terminais], a tela Seleção de terminal será exibida.

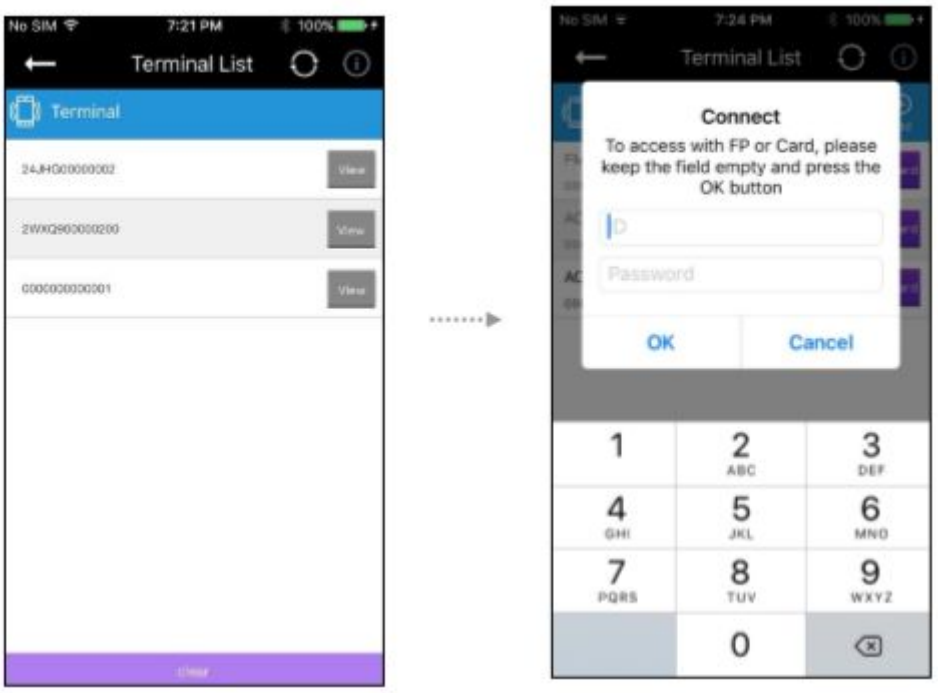


Selecione o terminal que você deseja registrar e vá para a tela Pesquisa de terminal para descobrir o Guia de registro de terminal

Quando abrir o Tamper Switch na parte traseira do dispositivo, coloque o dedo na janela de entrada de impressão digital e aguarde cerca de 5 segundos para operar e registrar o Terminal.

3.1.3 Acesso como usuário Administrador

Ao pressionar o botão [Visualizar] na tela [Lista de terminais], a tela a seguir será exibida para solicitar o ID do usuário e a senha.



Mesmo se não houver administrador registrado no terminal, o usuário poderá acessar o dispositivo sem inserir ID e senha.

Se houver um administrador registrado no terminal, o usuário poderá acessar o dispositivo, tentando métodos de autenticação predefinidos.

Se houver alguma entrada de ID do usuário, a autenticação 1: 1 será executada, mas a autenticação 1: N será executada se o ID do usuário não estiver registrado.

Após a autenticação bem-sucedida, a tela irá para o menu Gerenciamento de usuários.

3.2. Configurações de Usuário

3.2.1 Adicionar Usuário

Ao pressionar o botão [Adicionar] na tela principal [Gerenciamento de usuários], a tela a seguir será exibida.

Digite as informações do usuário para se registrar na tela [Adicionar usuário].

Quando você completar as informações do usuário, selecione o botão [Salvar] no canto superior direito.

Se as informações do usuário forem inseridas corretamente, o terminal estará pronto para a entrada de cartões ou impressões digitais.

Quando o método de autenticação definido é concluído, ele retorna à tela [Gerenciamento de usuários].

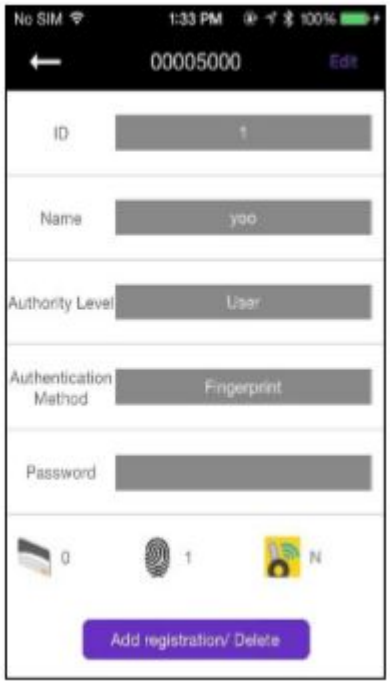
3.2.2 Deletar Usuário

Ao pressionar o botão [Editar] na tela principal [Gerenciamento de usuários], a seguinte tela será exibida.

Selecione o ID do usuário que você deseja excluir registrado no terminal e pressione o botão [Excluir] ou, se desejar excluir todas as informações registradas, pressione o botão [Excluir tudo].
[Se o modo estiver definido como "Rede", o botão [Excluir tudo] será desativado.]

3.2.3 Modificar Usuário

Selecione o usuário que você deseja modificar na tela [Gerenciamento de usuário], e a tela vai para Detalhes do usuário.



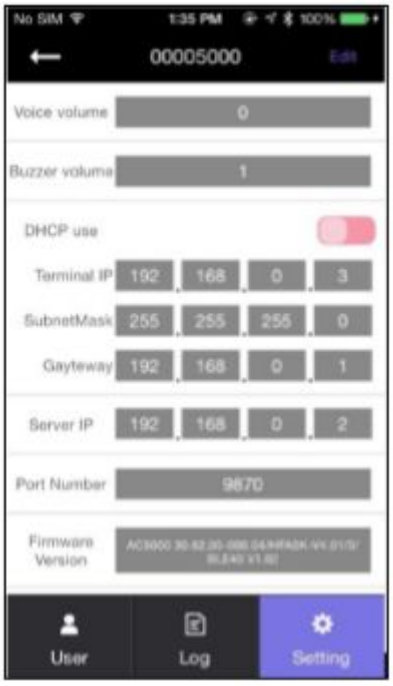
Após alterar as informações do usuário, exceto o ID, pressione o botão [Salvar] na tela para salvar as alterações, e também a tela pode mostrar o status de espera pela autenticação adicional quando necessário.

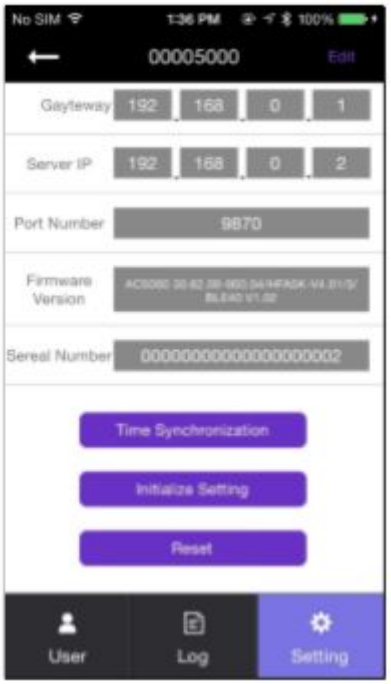
Quando a modificação estiver concluída, a tela retornará para [Gerenciamento de usuários].

3.3. Configurações de Terminal

3.3.1 Configurações via UNIS-B Plus

Ao pressionar o botão [Setting] no canto inferior direito da tela, a tela a seguir será exibida





Para modificar a configuração existente do terminal, pressione o botão [Editar] no canto superior direito da tela para entrar no modo de edição. Quando a modificação da configuração do terminal estiver concluída, pressione o botão [Salvar] para salvar os valores alterados e retornar à tela principal.

▸ Volume da campainha
Defina o volume do som da campainha do terminal.

▸ Controlador de bloqueio
485 controladores podem ser selecionados. Você pode selecionar LC-010, BLC-015 e MCP040. E eles executarão autenticação, controle de bloqueio e processamento de log

▸ Formato do cartão
Quando definido como Hexa, hexadecimal será exibido. Quando definido como decimal, é exibido em decimal. Se você selecionar [4. Formato 5] com o leitor de cartão RF (baixa frequência) instalado, a autenticidade do cartão EM é exibida em notação decimal.

▸ 1: N Nível
Defina o nível de verificação de 5 a 9 quando a autenticação 1: N estiver em andamento.

▸ 1: 1 Nível
Defina o nível de verificação de 1 a 9 quando a autenticação 1: N estiver em andamento

▸ Uso de DHCP
Defina se deseja usar IP estático.

▸ IP do Terminal
Defina o IP do terminal.

▸ IP do servidor
Defina o IP do servidor quando usado em conjunto com um servidor UNIS.

▸ Máscara de sub-rede
Defina o valor da máscara de sub-rede do terminal.

▸ Gateway
Defina o valor do gateway do terminal.

▸ Número da porta
Defina a porta do servidor UNIS. (Padrão: 9870)

▸ Versão do firmware
A versão do firmware do dispositivo e a versão do firmware BLE são exibidas.

▸ Sincronização de tempo
Defina a hora do terminal e a hora do celular para corresponder

▸ Inicializar configuração
Inicialize todos os dados, exceto logs e informações do usuário

▸ Restauração de fábrica
Redefina a configuração do terminal.

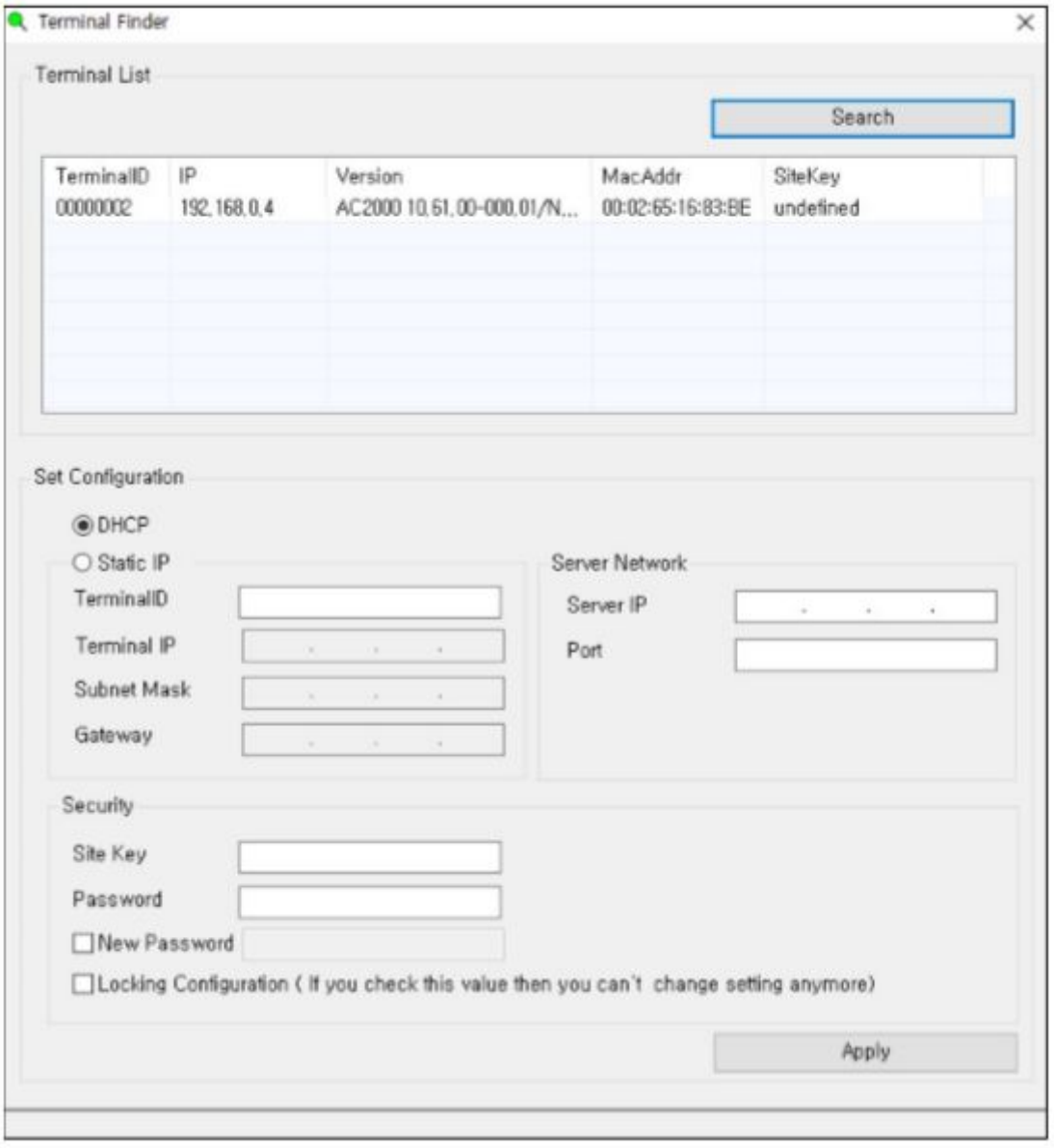
※ Depois de salvar a configuração, o terminal será reiniciado, portanto, é recomendável conectar-se com um intervalo de 30 a 60 segundos.

3.3.2 Configurar IP do Terminal via Terminal Finder

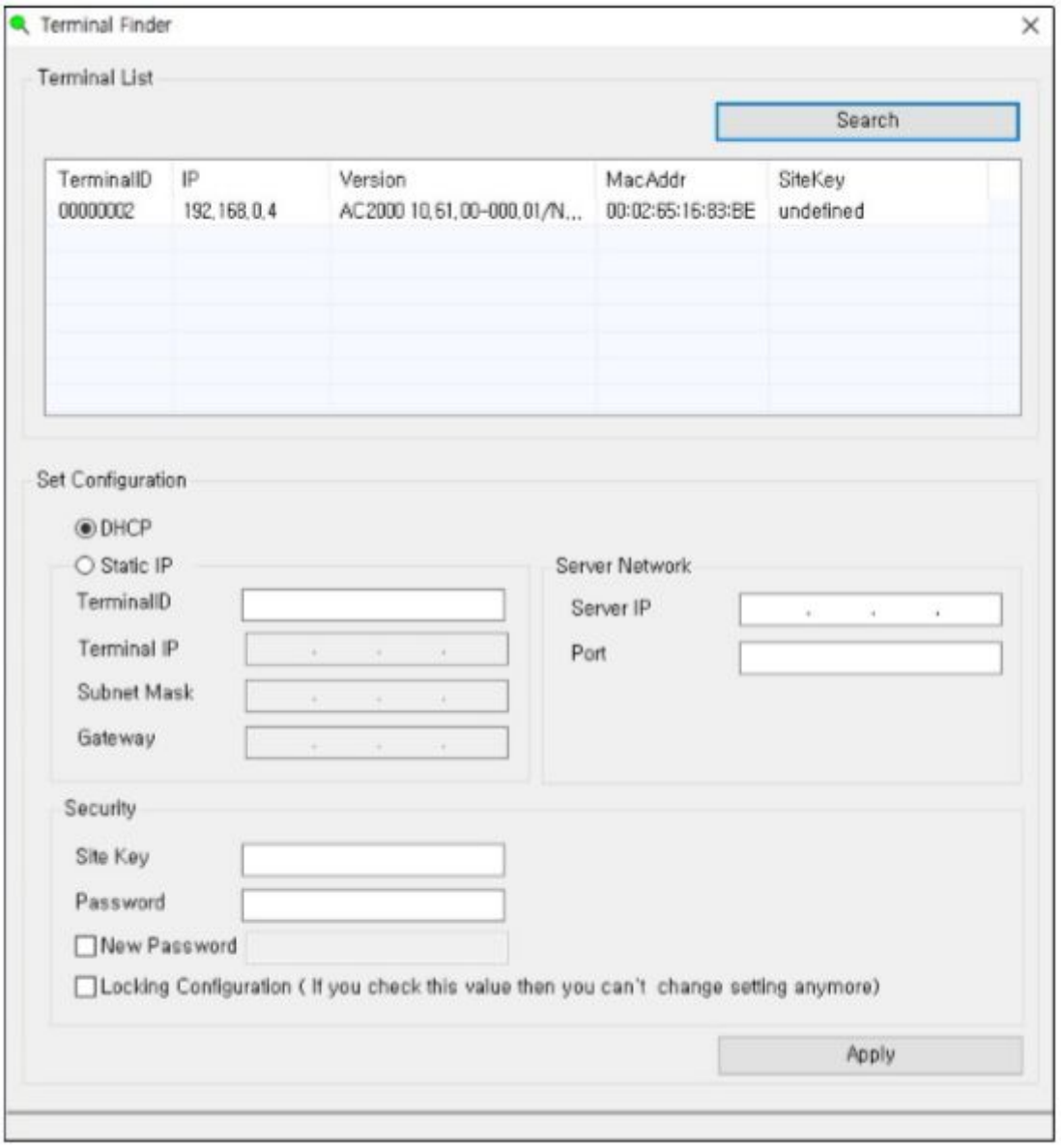
Antes de conectar o AC 2000 ao programa do servidor UNIS, convém alterá-lo para outro IP ou outro ID do terminal. Nesse caso, você precisa de um programa separado. O local é Arquivos de Programas -> UNIS -> pasta Patch e é chamado de Terminal Finder Program. Com este programa, você pode procurar todos os dispositivos na mesma rede e alterar as configurações de rede (IP do terminal, IP do servidor e ID do terminal etc.)

1) Adicione o ID do terminal do AC 2000 em [Gerenciamento de terminal] -> [Adicionar terminal] no UNIS e clique no botão [Adicionar]

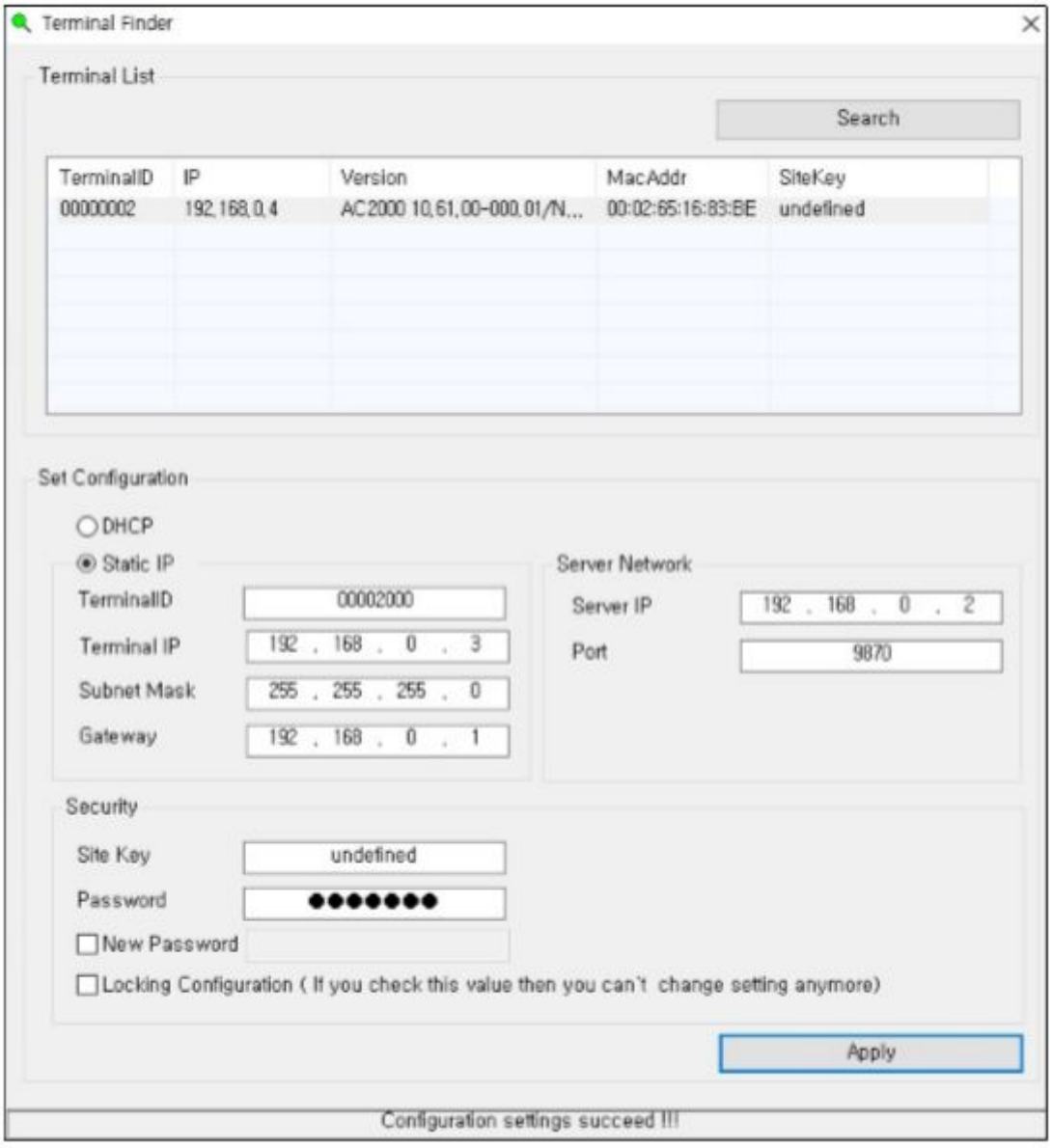
2) Conecte o AC 2000 à rede usando o cabo UTP padrão.
3) Abra o programa Terminal Finder.
4) Clique no botão [Pesquisar] - Uma lista de todos os dispositivos na rede será exibida.



5) Selecione o dispositivo para alterar a configuração. É destacado e o valor atual da configuração é exibido.



6) Modifique o valor da rede



7) Para aumentar a segurança, você pode alterar a senha antes de clicar no botão [Aplicar]. A senha padrão é 0842650. Essa senha pode ser alterada. Você também pode usar a opção de bloqueio se não desejar alterar as configurações de rede novamente pelo método de pesquisa UDP. Se as opções de Aviso e bloqueio estiverem definidas, talvez não seja possível configurar usando o programa Terminal Finder.

8) Clique no botão [Apply] (Aplicar) e o 'sucesso das definições de configuração' será exibido na parte inferior da tela.

4. Como Usar o Terminal

4.1. Autenticação

4.1.1 Autenticação por Impressão Digital

Quando você coloca uma impressão digital no sensor de digital, o sensor acende e a impressão digital é inserida. Não remova o dedo até que o sensor de impressão digital esteja completamente desligado.

4.1.2 Autenticação por Cartão

Coloque o cartão na entrada do terminal.

4.1.3 Múltiplas autenticações.

O método de autenticação para usuários que precisam autenticar dois ou mais métodos de autenticação juntos, como autenticação de cartão e impressão digital, continua com a autenticação restante se o método de autenticação inserido for bem-sucedido.

5. Problemas e Soluções

5.1. Quando a autenticação com a digital falha

▸ Se o terminal operar autenticação 1: N (servidor) no modo de rede e o servidor for usado para negócios ou uso pessoal, a taxa de reconhecimento e o tempo de autenticação podem demorar muito tempo devido à carga do servidor. Por favor, construa um servidor privado.

▸ Verifique se há arranhões ou objetos estranhos nos dedos ou no sensor e limpe-os. Se a cicatriz for grande, registre outra impressão digital através do administrador.

▸ Se o status da impressão digital não for bom, diminua o nível de segurança pessoal nas informações do usuário e tente a autenticação 1: 1.

5.2. Quando há falha na inserção da digital

Se a impressão digital estiver muito seca ou úmida, ela pode não ser inserida corretamente. Se estiver úmido, limpe-o com uma toalha seca. Se estiver seco, sopre os dedos ou coloque óleo e tente novamente.

5.3. Quando a comunicação com a rede falha

▸ Verifique se o terminal está registrado no item de gerenciamento de informações do programa UNIS.
▸ No caso de terminal não registrado, verifique as configurações do seu dispositivo no programa Terminal Finder.

- IP do servidor com o programa UNIS instalado.
- Verifique se o ID do dispositivo está corretamente.
- Se o DHCP não for usado, verifique as informações relevantes.

5.4. Autenticação com sucesso mas o acesso não é permitido.

Verifique se o fuso horário não é o limite de tempo para acesso.

6. Produtos abrangidos por este manual

Este guia de usuário pertence ao seguinte produto:

Leitor	***Código***
AC2000 RF	500.996
AC2000 SC	500.997

6.1 Nota de homologação

O leitor AC2000 RF e AC2000 SC foram testados e homologados nos termos do Regulamento para Certificação e Homologação de Produtos para Telecomunicações, aprovado pela Resolução Anatel nº 242, de 30 de novembro de 2000.
Tipos: Sistemas de Identificação por Radiofrequências – Categoria II.
Serviço/Aplicação: Radiocomunicação de Radiação Restrita.
"Este equipamento não tem direito à proteção contra interferência prejudicial e não pode causar interferência em sistemas devidamente autorizados".

6.2 Aviso Legal

Ainda que todos os esforços tenham sido realizados com o objetivo de assegurar que este documento e as informações contidas no mesmo estão corretas, a ACURA Technologies e quaisquer outras partes envolvidas na criação deste documento declaram que este é fornecido “como está”, sem nenhuma garantia explícita ou implícita, incluindo, mas não limitado a, quaisquer garantias de que o uso das informações aqui contidas não infringirão nenhum direito, de legitimidade ou adequação à propósito, e portanto renuncia a qualquer responsabilidade, direta ou indireta, por perdas ou danos relacionadas ao uso deste documento.
As informações contidas neste documento podem ser alteradas sem aviso prévio.

6.3 Sobre a Acura

A ACURA é a pioneira no mercado de Identificação por Rádio Frequência (RFID) no Brasil e América Latina, e tem desbravado com sucesso, desde o final dos anos 90, a sua adoção em larga escala nos mais diversos setores da economia, da mineração à siderurgia, da agricultura ao processamento de alimentos, da logística ao varejo, do transporte à cadeia de distribuição, do controle de acesso ao gerenciamento de ativos. Promotora de novas tecnologias, inovadora, ágil e com foco na viabilidade dos projetos de vanguarda.

Desenvolvimento Tecnológico e Escritório Comercial
Wall Street Business
Av. Antártico, 381 - Jardim do Mar, São Bernardo do Campo - SP, 09726-150
(11)3028-4600

