



Manual do Usuário

ACESSUS 2000 W ID

VERSÃO 1.0 OU SUPERIOR

Parabéns,
Você acaba de adquirir um produto com a qualidade JFL Alarmes, produzido no Brasil com a mais alta tecnologia de fabricação. Este manual mostra todas as funções do equipamento.

Para la versión en español, haga **CLIC AQUÍ**



ÍNDICE

1 PRODUTO.....	4
1.1 PRINCIPAIS CARACTERÍSTICAS.....	4
2 INSTALAÇÃO.....	5
2.1 PRECAUÇÕES.....	5
2.2 INSTALAÇÃO GERAL.....	5
2.3 INSTALAÇÃO COM MOVIMENTADOR.....	5
2.4 FIXAÇÃO.....	6
3 SINALIZAÇÃO AUDIOVISUAL.....	7
3.1 SINALIZAÇÃO DE ACESSO.....	7
3.2 SINALIZAÇÃO DE PROGRAMAÇÃO.....	7
3.3 SINALIZAÇÃO DA CHAVE DE RESET NA POSIÇÃO 1 OU 2.....	7
3.4 SINALIZAÇÃO DE ACESSO BLOQUEADO.....	7
4 OPERAÇÃO.....	7
5 ACESSO A FECHADURA.....	7
5.1 ACESSO UTILIZANDO TAG.....	7
5.2 ACESSO UTILIZANDO BOTOEIRA.....	7
6 ALARMES.....	8
6.1 PORTA ABERTA.....	8
6.2 ACESSO FORÇADO.....	8
6.3 VIOLAÇÃO (TAMPER).....	8
7 RECORRÊNCIA DE NEGAÇÃO.....	8
8 MODO DE PROGRAMAÇÃO.....	9
8.1 PROGRAMADOR JFL MOB.....	9
8.1.1 MEIO DE COMUNICAÇÃO BLUETOOTH.....	10
8.1.2 MEIO DE COMUNICAÇÃO NUVEM.....	10
8.2 PROGRAMADOR LINHA MONITORADA.....	11
9 PROGRAMAÇÃO DOS USUÁRIOS.....	12
10 PROGRAMAÇÃO DA COMUNICAÇÃO.....	12
10.1 REDE WI-FI.....	12
10.2 REPORTE PARA MONITORAMENTO.....	13
10.2.1 CONFIGURAÇÃO DO REPORTE.....	13
10.2.2 CANCELAR O ENVIO DOS EVENTOS PENDENTES.....	13
10.2.3 TIPOS DE EVENTOS REPORTADOS.....	13
10.3 ACESSO POR APLICATIVO VIA NUVEM.....	13
11 PROGRAMAÇÃO DA DATA E HORA.....	14
12 DIAGNÓSTICO.....	14
13 RESTAURAÇÃO DAS CONFIGURAÇÕES DE FÁBRICA (RESET).....	15
13.1 REALIZAR O RESET.....	15
13.2 BLOQUEAR O RESET.....	15
14 ATUALIZAÇÃO DO FIRMWARE (BOOTLOADER).....	16
14.1 ATUALIZAÇÃO DO FIRMWARE VIA APLICATIVO.....	16
14.2 ATUALIZAÇÃO DO FIRMWARE VIA COMPUTADOR.....	17
15 ESPECIFICAÇÕES TÉCNICAS.....	19
15.1 CARACTERÍSTICAS GERAIS.....	19
15.2 INTERFACE WI-FI.....	19
15.3 INTERFACE BLUETOOTH.....	19
15.4 INTERFACE RFID.....	19
16 TABELA DE EVENTOS CONTACT ID.....	20
17 REGULAMENTAÇÃO E INFORMAÇÕES LEGAIS.....	21
17.1 DIREITOS AUTORAIS.....	21
17.2 CERTIFICAÇÃO ANATEL.....	21
17.3 POLÍTICA DE ATUALIZAÇÃO DE SOFTWARE.....	21
17.4 LGPD – LEI GERAL DE PROTEÇÃO DE DADOS.....	22
17.5 MARCAS REGISTRADAS E CÓDIGO ABERTO.....	22

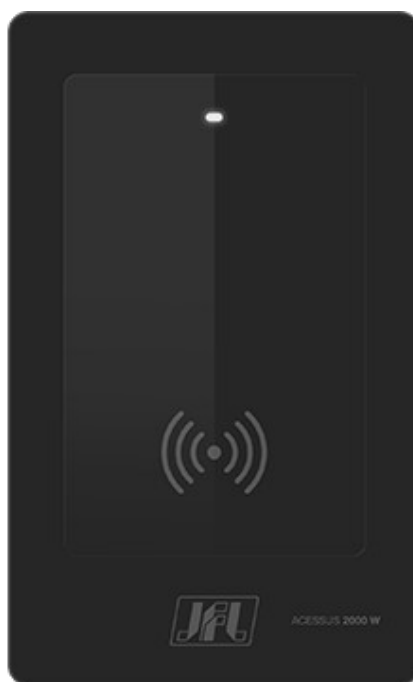
1 PRODUTO

O Controlador Acessus 2000 W ID é uma solução moderna e conectada para controle de acesso seguro e eficiente que permite autenticação por cartão (tag). Foi projetado para oferecer facilidade de instalação, gestão remota e integração com centrais de monitoramento.

Equipado com conectividade Wi-Fi, o controlador permite configuração e gerenciamento via aplicativo, além de realizar o reporte de eventos para a central de monitoramento via protocolo CONTACT ID.

1.1 PRINCIPAIS CARACTERÍSTICAS

- Controle de acesso para até 4000 usuários com cartões RFID padrão 13,56 MHz (MIFARE);
- Programação local via Bluetooth ou remota via nuvem pelo aplicativo Programador JFL Mob (Android® / iOS®);
- Programação local ou remota através do software Active Net 3.0;
- Conectividade Wi-Fi com suporte a redes WPA2;
- Envio automático de eventos para a central de monitoramento;
- Cadastro e remoção de usuários diretamente pelo aplicativo;
- Armazenamento local de usuários e até 8000 eventos (modo offline);
- Atualização remota de firmware OTA (Over-the-Air);
- Integração com fechaduras elétricas, botoeiras e sensores magnéticos;
- Alarmes de porta aberta, acesso forçado e violação;
- Função de recorrência de negação;
- Entrada para fonte externa 12 Vc.c. / 2 A (não inclusa).



A tag RFID  não está inclusa no produto e pode ser adquirida separadamente.

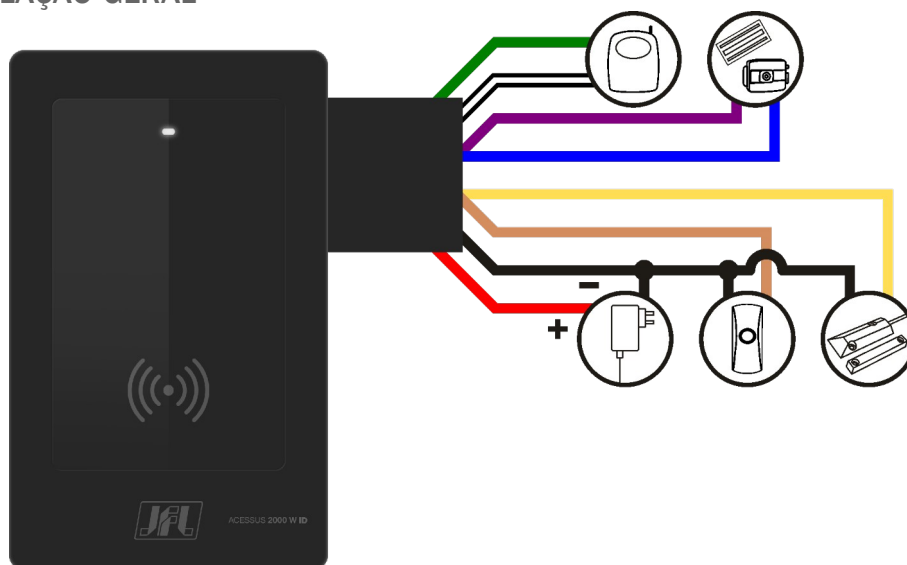
2 INSTALAÇÃO

Leia atentamente todo o manual antes de iniciar a instalação.

2.1 PRECAUÇÕES

- Evite instalar o equipamento próximo a fontes de campo magnético, como quadros de energia, motores ou outros dispositivos que possam gerar interferência.
- A instalação deve ser realizada apenas por técnicos especializados e experientes.
- Não ajuste ou modifique o equipamento por conta própria.
- A manutenção deve ser executada exclusivamente por profissionais autorizados pela JFL Alarmes.

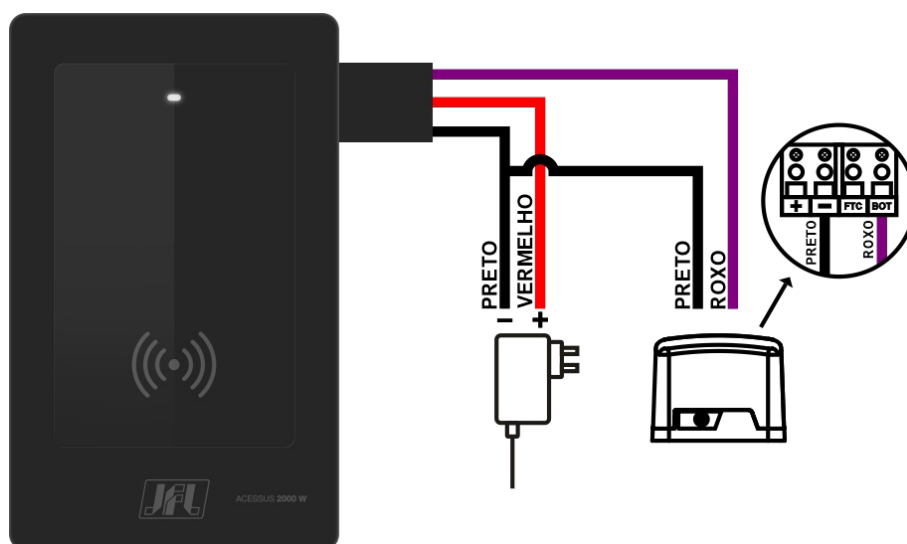
2.2 INSTALAÇÃO GERAL



Legenda:

- Branco e Verde: Saída contato seco (NF) para integração com central de alarme;
- Azul e Roxo: Saída para ligação de fechadura eletromagnética (NF), fechadura eletromecânica (pulsativa) ou movimentador (NA);
- Amarelo: Entrada para sensor de porta;
- Marrom: Entrada para botoeira "Push Button" tipo NA;
- Preto: GND (referência de terra);
- Vermelho: Entrada de alimentação 12 Vc.c.

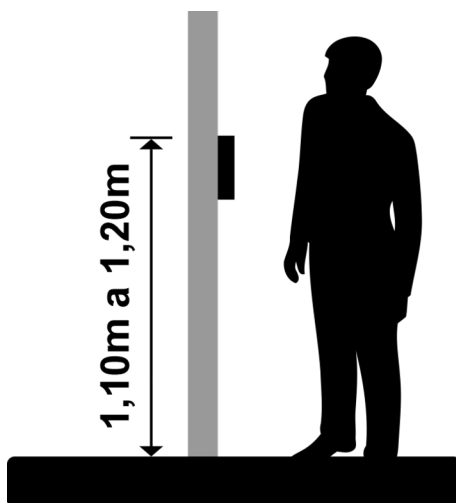
2.3 INSTALAÇÃO COM MOVIMENTADOR



2.4 FIXAÇÃO

1. Posicionamento:

- Instale o controlador em uma altura entre 1,10 m e 1,20 m em relação ao solo;
- Recomenda-se utilizar caixas padrão 4x2 do mercado para melhor acomodação dos cabos.



2. Fixação do suporte:

- Fixe o suporte do controlador na parede;
- Conecte todos os fios necessários de acordo com a legenda de cores (ver item 2.2 Instalação geral).



3. Acoplamento do controlador:

- Encaixe o controlador no suporte, começando pela parte superior;
- Pressione a parte inferior até que esteja firmemente fixado.
- Por último, recoloque o parafuso de fixação na parte inferior.



3 SINALIZAÇÃO AUDIOVISUAL

3.1 SINALIZAÇÃO DE ACESSO

- Liberado: 2 bipes curtos e pisca 2 vezes na cor verde ;
- Negado: 1 bipe longo e pisca 1 vez na cor vermelha .

3.2 SINALIZAÇÃO DE PROGRAMAÇÃO

- Aceso na cor ciano .

3.3 SINALIZAÇÃO DA CHAVE DE RESET NA POSIÇÃO 1 OU 2

- Aceso na cor rosa .



Quando o controlador entra nesta condição, nenhuma operação poderá ser realizada até que a chave CH2 seja retornada para a posição 4 (Operação).

3.4 SINALIZAÇÃO DE ACESSO BLOQUEADO

- Piscando na cor laranja .

4 OPERAÇÃO

Após concluir todas as conexões da fiação, alimente o equipamento com 12 Vc.c. e aguarde a inicialização:

1. Ao energizar, o LED acenderá na cor branca , em intensidade máxima, indicando o processo de inicialização.
2. Quando a conexão for concluída, o controlador emitirá dois bipes curtos e o LED permanecerá aceso na cor branca , em intensidade mínima, indicando que está em modo de repouso e pronto para uso.

5 ACESSO A FECHADURA

A saída de fechadura vem habilitada de fábrica.

Se necessário, o instalador pode desativá-la ou configurar o tempo e o tipo de acionamento pelo programador, na aba Entrada/Saída.

O controlador permite o acionamento da saída de fechadura sempre que o acesso não estiver bloqueado, condição em que o LED ficará piscando na cor laranja .



O bloqueio de acesso só pode ser realizado pelo software Active Net 3.0.

5.1 ACESSO UTILIZANDO TAG

Aproxime uma tag RFID válida na área indicada ((••)) no painel frontal do controlador. Se a credencial for reconhecida, o LED indicará liberação e a saída da fechadura será acionada.

5.2 ACESSO UTILIZANDO BOTOEIRA

É possível abrir a fechadura através de uma botoeira (Push Button) NA – Normalmente Aberta.

Basta conectá-la na entrada BOT do equipamento, conforme indicado no item 2.2 Instalação geral do manual.

A função de acesso por botoeira vem habilitada de fábrica. Se necessário, o instalador pode desativá-la pelo programador, na aba Entrada/Saída.

6 ALARMES

O controlador está equipado com funções de alarme que podem emitir aviso sonoro, acionar a saída de alarme e/ou enviar o evento para a central de monitoramento.

6.1 PORTA ABERTA

Emite alerta quando a porta permanecer aberta além do tempo configurado, ajudando a identificar esquecimentos ou mau fechamento.

O alarme de porta aberta vem desabilitado de fábrica. O instalador pode ativá-lo e ajustar o tempo em segundos, que o sensor com fio deve ficar aberto para que o controlador emita os avisos, utilizando o programador, na aba Entrada/Saída.

6.2 ACESSO FORÇADO

Detecta quando a porta é aberta sem autorização, como em tentativas de arrombamento, permitindo resposta imediata do sistema de segurança.

O alarme de acesso forçado vem desabilitado de fábrica e pode ser ativado pelo instalador utilizando o programador, na aba Entrada/Saída.

6.3 VIOLAÇÃO (TAMPER)

Este recurso detecta quando o controlador é aberto, removido ou sofre tentativa de violação física, ajudando a prevenir sabotagem e garantindo que o sistema seja alertado para ações corretivas.

O alarme de violação vem habilitado de fábrica e pode ser desativado pelo instalador utilizando o programador, na aba Sistema.

7 RECORRÊNCIA DE NEGAÇÃO

Este recurso de segurança permite que o sistema detecte, registre e reaja a múltiplas tentativas de acesso negado consecutivas feitas pelo mesmo usuário ou cartão RFID. Ele é projetado para prevenir abusos, fraudes, uso indevido de credenciais ou tentativas de invasão.

Funcionamento:

- O usuário apresenta um cartão RFID fora do horário permitido;
- Se o número de tentativas ultrapassar o limite configurado (ex.: 5 tentativas seguidas), o controlador é automaticamente bloqueado por 30 segundos;
- O sistema registra a tentativa de acesso negado e um evento é enviado à central de monitoramento;

A função vem habilitada de fábrica, configurada para 5 tentativas de falha. O instalador pode desativá-la ou ajustar o número de tentativas utilizando o programador, na aba Sistema.

8 MODO DE PROGRAMAÇÃO

A programação do controlador pode ser realizada através de um dos seguintes programadores:

- Aplicativo “Programador JFL Mob”;
- Software “Programador Linha Monitorada”.

8.1 PROGRAMADOR JFL MOB

1. Instalação e login:

- Acesse o aplicativo na Google Play (Play Store) para Android e na App Store para iOS;
- Baixe o aplicativo “Programador JFL Mob”;
- Crie uma conta e faça login.

2. Adicionar um local:

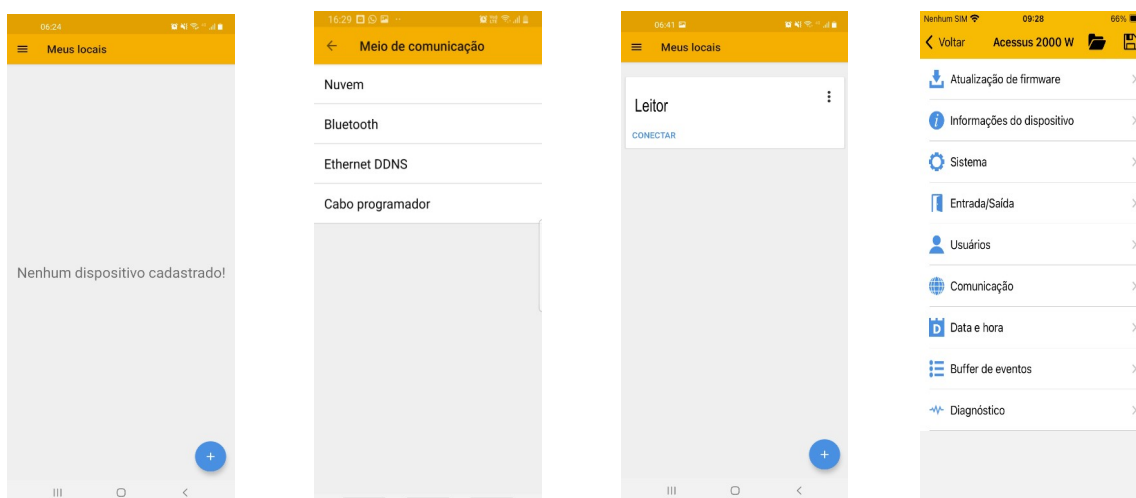
- Abra o aplicativo;
- Toque em  “Adicionar Local”;
- Selecione o meio de comunicação:
 - 8.1.1 Meio de comunicação bluetooth;
 - 8.1.2 Meio de comunicação nuvem;

3. Conectar ao controlador:

- Após cadastrar o local e criar uma senha, toque em **Conectar**;
- O aplicativo baixará toda a programação já configurada no controlador.

4. Configuração e envio:

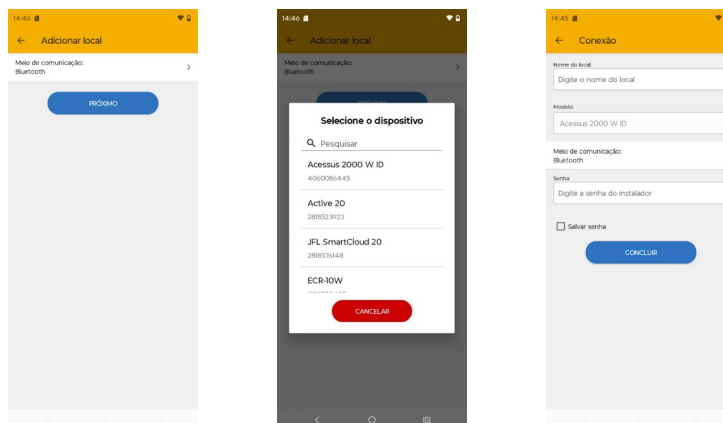
- Navegue pelas guias de programação;
- Preencha os campos desejados;
- Toque em **Enviar** para gravar as alterações no controlador.



8.1.1 MEIO DE COMUNICAÇÃO BLUETOOTH

Para programar o controlador via Bluetooth:

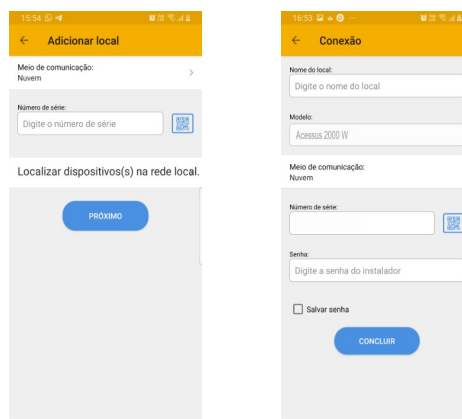
1. Toque em **Próximo**;
2. Selecione o produto que deseja programar (ex.: Acessus 2000 W ID);
3. Preencha os seguintes campos:
 - Nome do local;
 - Senha de acesso;
 - Marque a opção “Salvar senha”, se desejar;
4. Toque em **Concluir** para finalizar a configuração do Bluetooth.



8.1.2 MEIO DE COMUNICAÇÃO NUVEM

Para programar o controlador utilizando a conexão com a nuvem:

1. Preencha o número de série do controlador ou, se preferir, escaneie a etiqueta QR Code;
2. Toque em **Próximo**;
3. Preencha os seguintes campos:
 - Nome do local;
 - Senha de acesso;
 - Marque a opção “Salvar senha”, se desejar;
4. Toque em **Concluir** para finalizar a configuração via nuvem.



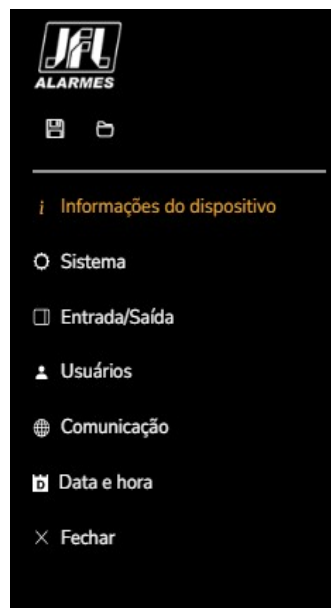
- A velocidade e estabilidade da conexão pode influenciar no tempo de programação.
- Para que seja possível a conexão via nuvem é necessário que o Acessus 2000 W ID esteja conectado a uma rede Wi-Fi.

8.2 PROGRAMADOR LINHA MONITORADA

Também é possível realizar a programação do controlador utilizando o software Programador Linha Monitorada.

Para isso, siga os passos:

1. Entre no site da JFL e baixe o software Programador Linha Monitorada;
2. Abra o software;
3. Clique em  para adicionar um equipamento;
4. Selecione o produto que deseja programar (ACESSUS 2000 W ID);
5. Clique em ;
6. Selecione a porta serial em que o cabo programador está conectado;
7. Insira a senha de instalador;
8. Marque a opção “Salvar senha”, se desejar;
9. Clique em conectar, o software fará o download automático de toda programação já configurada no controlador;
10. Navegue pelas guias de programação, preencha os campos necessários e clique em **Enviar** para gravar as alterações.



9 PROGRAMAÇÃO DOS USUÁRIOS

O controlador possibilita o cadastro e gerenciamento de até 4.000 usuários. Para cada usuário, pode ser vinculada uma TAG RFID.

Existem dois tipos de usuários no sistema:

- Instalador: responsável pela programação do funcionamento do controlador.
- Administrador: responsável pelo gerenciamento de usuários, podendo criar cadastros, cadastrar TAGs e apagar usuários.



O Administrador não pode alterar as configurações do controlador.

Os usuários podem ser cadastrados e gerenciados por dois meios:

- No equipamento: através do aplicativo Programador Mob JFL ou software Programador Linha Monitorada, utilizado pelo instalador ou por um usuário administrador.
- Via Active Net 3.0: a empresa de monitoramento é responsável pelo gerenciamento remoto dos usuários, aplicando regras de controle de acesso.



- Ao alterar o modo de gerenciamento de usuários de Equipamento para Active NET, os usuários não são migrados para o banco de dados do Active NET. Nesse modo, o equipamento passará a operar exclusivamente com os usuários cadastrados no Active NET.
- Caso o modo seja alterado para Active NET e, posteriormente, seja necessário retornar para o modo Equipamento, será obrigatório realizar um Reset Total, o qual apagará todos os usuários cadastrados no sistema.

10 PROGRAMAÇÃO DA COMUNICAÇÃO

O controlador permite a configuração dos parâmetros de conexão com a rede Wi-Fi, possibilitando:

- Programação remota;
- Envio de eventos para a estação de monitoramento;
- Atualização remota do firmware do controlador.



Durante a instalação, certifique-se de que as portas e serviços a seguir estejam liberados no firewall (solicite ao administrador de rede, se necessário):

- Porta 123 (UDP) – utilizada pelo serviço NTP, responsável por obter data e hora automaticamente;
- Porta 8883 (TCP) – utilizada pelo serviço MQTT, responsável pela comunicação com a nuvem com segurança TLS.

10.1 REDE WI-FI

O controlador permite configurar manualmente os parâmetros de rede ou habilitar o modo DHCP para receber os endereços automaticamente.

- Configurações da rede local (IP fixo): Permite definir manualmente os seguintes parâmetros:
 - Endereço IP;
 - Máscara de sub-rede;
 - Gateway;
 - Servidor DNS.

- **DHCP:** Quando habilitado, o controlador obtém automaticamente os endereços de rede do servidor DHCP.
- **Nome da rede (SSID) e senha:** Informe o nome da rede Wi-Fi e a senha de autenticação para conectar o controlador ao ponto de acesso sem fio.

10.2 REPORTE PARA MONITORAMENTO

O controlador possui a função de enviar todos os eventos ocorridos para a estação de monitoramento.

- A estação de monitoramento pode ser:
 - Uma empresa de monitoramento remota;
 - A própria portaria do condomínio, caso haja um computador com o software Active Net 3.0 instalado.

10.2.1 CONFIGURAÇÃO DO REPORTE

Para comunicar-se com a estação de monitoramento, programe os seguintes parâmetros no equipamento:

1. Habilitar reporte via Wi-Fi;
2. Programar o endereço IP de destino e a porta de destino:
 - Estes valores correspondem ao computador onde o Active NET 3.0 está instalado;
 - Pode ser um IP dinâmico ou um endereço da rede local do condomínio.



O protocolo padrão para envio dos eventos é o CONTACT ID.

10.2.2 CANCELAR O ENVIO DOS EVENTOS PENDENTES

Para cancelar o envio de eventos que ainda estão na fila:

1. Desabilite o reporte no equipamento;
2. Aguarde alguns segundos para que os eventos pendentes sejam apagados da lista de envio;
3. Habilite novamente o reporte se desejar.

10.2.3 TIPOS DE EVENTOS REPORTADOS

O controlador pode gerar notificações para diferentes situações:

- **Alteração de programação:** Reporta acesso à programação e alterações realizadas;
- **Problema de rede IP:** Reporta falhas ou problemas relacionados à rede IP;
- **Acesso negado:** Reporta quando um usuário tenta acionar o controlador fora da faixa de horários permitido;
- **Acesso bloqueado:** Reporta quando um usuário tenta acionar o controlador enquanto ele está bloqueado.

10.3 ACESSO POR APLICATIVO VIA NUVEM

Para que o controlador se comunique com o aplicativo via nuvem, é necessário programar os seguintes parâmetros no equipamento:

1. Conectar à rede local conforme descrito no item 10.1 Rede wi-fi.

2. Habilitar o acesso por aplicativo via nuvem através da conexão Wi-Fi.

Configuração do primeiro usuário:

- Ao criar um local no aplicativo, será necessário definir uma senha de acesso;
- Se você for o primeiro usuário, basta inserir a senha no aplicativo;



Ao se conectar ao controlador, a senha será salva automaticamente no equipamento.

11 PROGRAMAÇÃO DA DATA E HORA

O controlador pode ajustar automaticamente a data e hora via rede Wi-Fi. Para isso, é necessário selecionar o fuso horário correto.

Opções de configuração de fuso horário:

- Desabilitado: O controlador não ajusta a data e hora automaticamente.
- UTC-2: Tempo coordenado universal menos 2 horas.
- Horário de Brasília com horário de verão (UTC-3): Com o fim do horário de verão no Brasil, funciona igual ao Horário de Brasília, sem adiantar ou atrasar o relógio.
- Horário de Brasília (UTC-3): Horário de Brasília sem ajustes de horário de verão. Normalmente adotado nos estados da região Nordeste, Pará, Amapá e Tocantins.
- Horário do Amazonas (UTC-4): Horário de Brasília menos 1 hora, sem ajustes de horário de verão. Normalmente adotado nos estados Amazonas, Rondônia e Roraima.
- Horário do Amazonas com horário de verão (UTC-4): Com o fim do horário de verão, funciona igual ao Horário do Amazonas, sem adiantar ou atrasar o relógio.
- Horário do Acre (UTC-5): Horário de Brasília menos 2 horas, normalmente adotado no estado do Acre e parte do estado do Amazonas.
- UTC-6 a UTC-8: Segue o tempo coordenado universal subtraindo 6, 7 ou 8 horas, respectivamente.



Estes fusos são utilizados para outros países das Américas. Para uso fora do Brasil, consulte o fuso horário local do país.

12 DIAGNÓSTICO

O controlador possui uma função de diagnóstico que auxilia a identificar rapidamente possíveis falhas na comunicação via rede Wi-Fi e no funcionamento do hardware. A sinalização é exibida da seguinte forma:

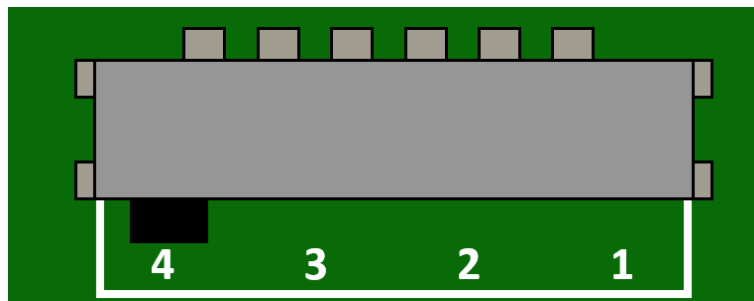
- Verde: Funcionamento normal.
- Amarelo: Verifique a configuração ou condições de instalação.
- Vermelho: Problema identificado, requer correção imediata.
- Cinza: Função ou recurso desativado.

13 RESTAURAÇÃO DAS CONFIGURAÇÕES DE FÁBRICA (RESET)

13.1 REALIZAR O RESET

Para restaurar as configurações do controlador, siga os passos abaixo:

1. Abra o controlador e localize a chave CH2 (conforme figura de referência).



2. Com o controlador desligado, ajuste a chave CH2 para:
 - Posição 1: *Reset parcial* – restaura apenas a senha do instalador.
 - Posição 2: *Reset total* – restaura todas as configurações e programações do equipamento.
3. Ligue o controlador.
4. Se a restauração for concluída com sucesso, o controlador emitirá 2 bipes curtos e o LED piscará 2 vezes em verde ●, permanecendo em seguida na cor rosa ● para indicar que a chave CH2 ainda está na posição de reset.
5. Desligue o controlador e retorne a chave CH2 para a posição 4.
6. Ligue o controlador novamente para iniciar a operação normal.



Caso o controlador emita 1 bipe longo e pisca 1 vez em vermelho ●, a restauração não pode ser realizada. Verifique o item 13.2 Bloquear o Reset.

13.2 BLOQUEAR O RESET

A função de bloquear o reset de um equipamento é um recurso de segurança que impede que o usuário, ou alguém com acesso físico ao controlador, possa restaurá-lo para as configurações de fábrica ou reinicializar toda a programação sem autorização.



Se o reset for bloqueado e a senha for perdida, não há mais como acessar o equipamento que deve ser enviado a assistência técnica da JFL.

14 ATUALIZAÇÃO DO FIRMWARE (BOOTLOADER)

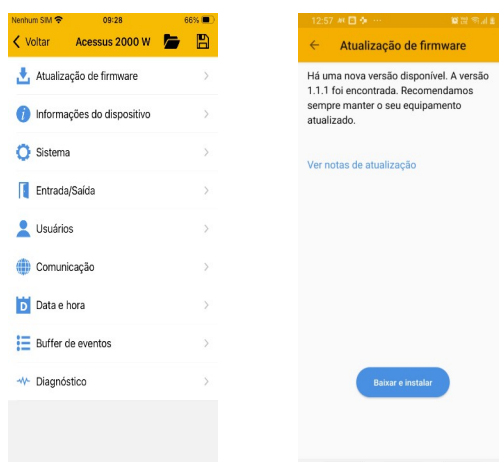
14.1 ATUALIZAÇÃO DO FIRMWARE VIA APLICATIVO

O controlador pode ter seu firmware atualizado remotamente pelo aplicativo programador, desde que esteja conectado à nuvem por meio da rede Wi-Fi.

O equipamento verifica periodicamente na nuvem JFL se existe uma nova versão de firmware disponível. Quando houver, o aplicativo exibirá automaticamente a opção de atualização.

Para realizar o procedimento:

1. Certifique-se de que o aplicativo esteja conectado ao controlador;
2. Toque em **Atualização de firmware**;
3. Toque em **Baixar e instalar**;
4. Aguarde a conclusão do processo. O controlador será reiniciado automaticamente após a atualização.

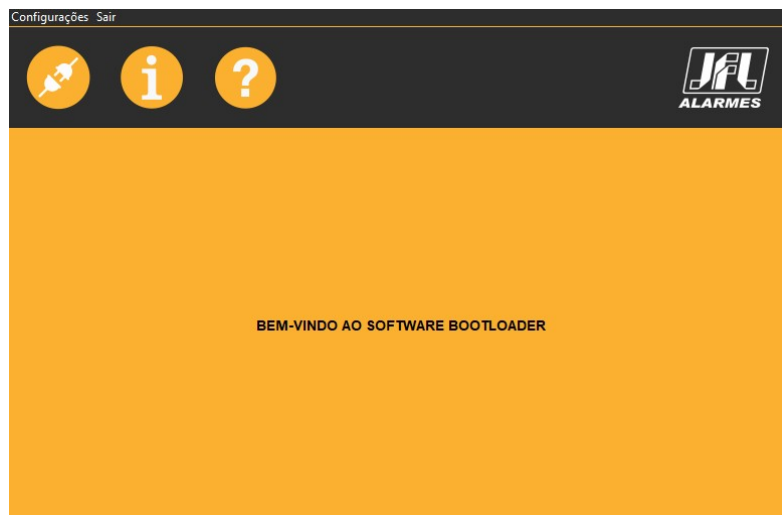


14.2 ATUALIZAÇÃO DO FIRMWARE VIA COMPUTADOR

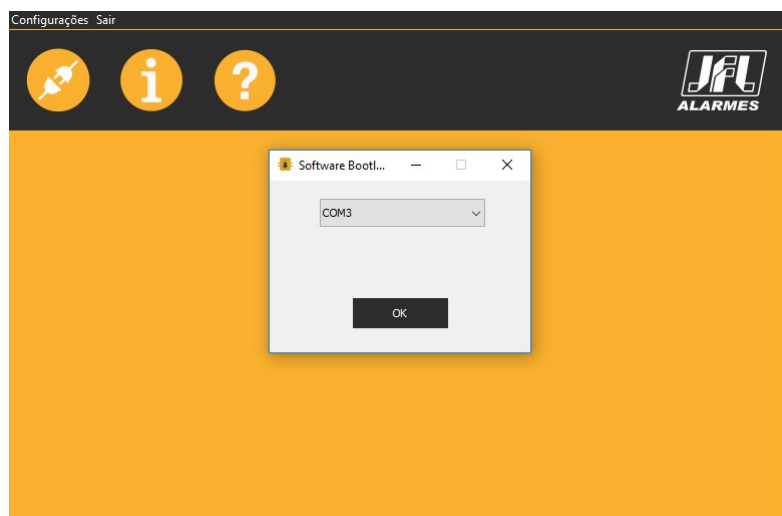
A atualização local do firmware pode ser realizada em campo utilizando um computador com o software Bootloader JFL instalado e o cabo programador JFL.

Para realizar o procedimento:

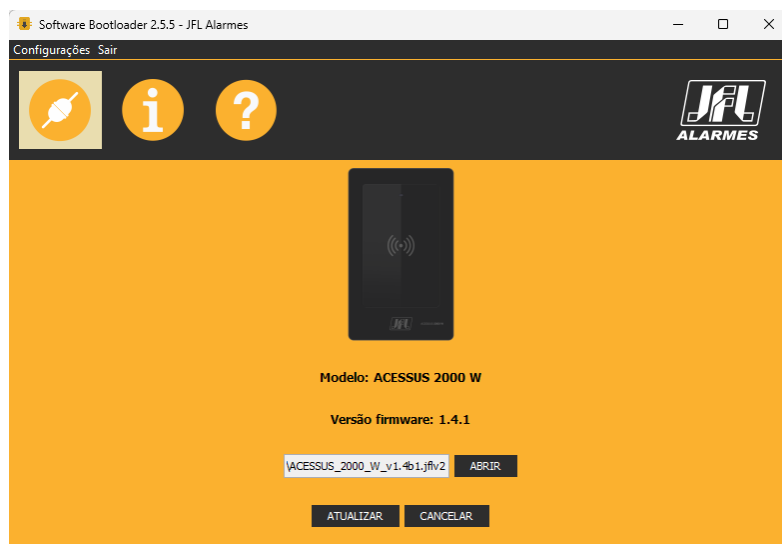
1. Com o controlador desligado, conecte o cabo programador e posicione a chave CH2 na posição 3, conforme ilustrado no item 13 Restauração das configurações de fábrica (Reset).
2. Ligue o controlador;
3. Abra o software Bootloader JFL no computador;



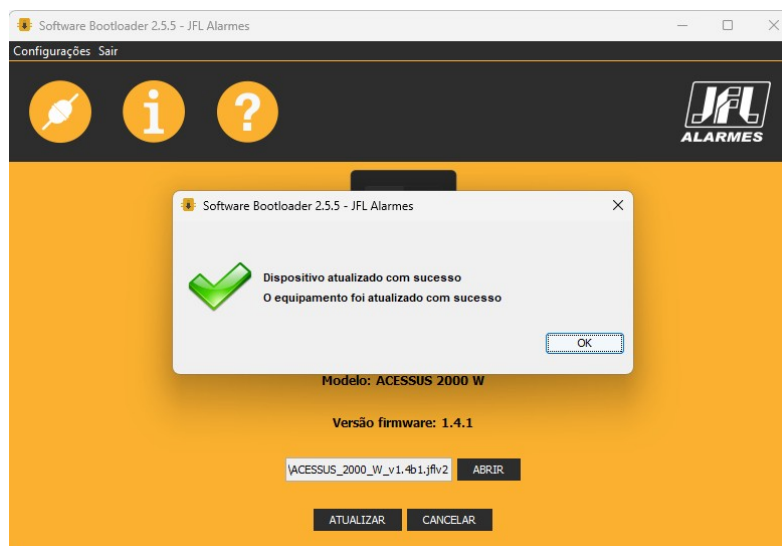
4. Selecione a porta serial correspondente;



5. Carregue o arquivo de firmware fornecido pela JFL;



6. Clique em **Atualizar** e aguarde o término do processo;



7. Ao finalizar, desligue o controlador, retorne a chave **CH2** para a posição 4 e religue o equipamento.



- Não desligue o controlador nem remova o cabo programador durante o processo de atualização.
- Certifique-se de utilizar apenas arquivos de firmware oficiais da JFL para evitar danos ao equipamento.

15 ESPECIFICAÇÕES TÉCNICAS

15.1 CARACTERÍSTICAS GERAIS

- Alimentação: Fonte externa 12 Vc.c. /2 A (não inclusa);
- Consumo em repouso: 0,5 W;
- Corrente máxima na saída da fechadura: A corrente máxima da saída para fechaduras depende da capacidade de corrente da fonte de alimentação. Sendo a corrente máxima permitida de 2 A;
- Buffer de eventos: 8000 eventos;
- Dimensões: 112,5 x 69,5 x 22 mm;
- Peso: 90 g.

15.2 INTERFACE WI-FI

- Interface de rede sem fio: 802.11 b/g/n (802.11n até 150 Mbps);
- Frequência da rede sem fio: 2,4 GHz a 2,5 GHz;
- Endereçamento IP: IPv4 fixo ou DHCP;
- Protocolos de rede: TCP/IP, DHCP, NTP e MQTT;
- Camada de segurança: TLS 1.2;
- Data e hora automática: Via protocolo NTP;
- Consumo médio de banda de internet: 4 Kbps;
- Tipo da antena: Interna.

15.3 INTERFACE BLUETOOTH

- Interface Bluetooth: Bluetooth 4.2 modo BLE;
- Frequência da rede Bluetooth: 2,4 GHz a 2,5 GHz;
- Classe de potência: Classe 1 e 2 (até 10 metros).
- Tipo da antena: Interna.

15.4 INTERFACE RFID

- Faixa de operação: 13,553 – 13,567 MHz;
- Modulação: ASK;
- Taxa de transmissão: 106 kbps (compatível até 848 kbps);
- Tipo da antena: Interna.

16 TABELA DE EVENTOS CONTACT ID

Código	Descrição do evento	Categoria notificação	Código	Descrição da restauração do evento	Categoria notificação
1134	Alarme de porta aberta	Alarme	3134	Restauração do alarme de porta aberta	Eventos gerais
1137	Alarme de violação (Tamper)	Alarme	3137	Restauração do alarme de violação (Tamper)	Eventos gerais
1305	Reset de sistema	Eventos gerais	---	---	---
1306	Alteração de programação	Eventos gerais	---	---	---
1359	Problema de Wi-Fi	Problema	3359	Restauração de Wi-Fi	Problema
1410	Acesso remoto	Eventos gerais	---	---	---
1417	Nova atualização de firmware encontrada	Eventos gerais	---	---	---
1420	Acesso bloqueado	Eventos gerais	3420	Restauração do acesso bloqueado	Eventos gerais
1421	Acesso negado	Eventos gerais	---	---	---
1423	Alarme de acesso forçado	Alarme	3423	Restauração do alarme acesso forçado	Eventos gerais
1435	Acesso por botoeira	Abertura	---	---	---
1438	Acesso de usuário por tag	Abertura	---	---	---
1448	Acesso de usuário remoto	Abertura	---	---	---

17 REGULAMENTAÇÃO E INFORMAÇÕES LEGAIS

17.1 DIREITOS AUTORAIS

Este manual está protegido pelas leis internacionais dos direitos autorais. Parte alguma deste manual pode ser reproduzida, distribuída, traduzida ou transmitida de qualquer forma e em qualquer meio, seja eletrônico ou mecânico, incluindo fotocopiadora, gravação ou armazenamento em qualquer sistema de informação ou recuperação sem autorização da JFL.

17.2 CERTIFICAÇÃO ANATEL

Para mais informações, consulte o site da Anatel – www.gov.br/anatel/pt-br/



07741-25-05074

Res. 680

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

17.3 POLÍTICA DE ATUALIZAÇÃO DE SOFTWARE

A JFL preocupada com a segurança dos equipamentos, visando minimizar ou corrigir vulnerabilidades, realiza melhorias periódicas nos softwares/firmwares dos equipamentos. Isto ajuda a manter os equipamentos protegidos contra softwares maliciosos, ataques de hackers, roubo de informações confidenciais e eventuais falhas exploradas por pessoas mal-intencionadas. A JFL utiliza nuvem com tecnologia de segurança e criptografia de ponta a ponta (TLS 1.2 com certificado digital assinado por uma autoridade de certificação) mesmos usados por bancos, para garantir que não haja interceptação de informações pela rede de computadores.

A JFL pratica as seguintes políticas nos produtos e aplicativos:

- Sempre atualizamos os aplicativos nas lojas das plataformas móveis a fim de mitigar problemas de segurança;
- Informações pessoais e informações sensíveis nos aplicativos são armazenadas de forma criptografadas como sugere a LGPD (lei geral de proteção de dados);
- A JFL disponibiliza atualizações do equipamento por no mínimo dois anos após o lançamento ou enquanto este produto estiver sendo distribuído ao mercado;
- A JFL disponibiliza um serviço de atendimento ao consumidor (SAC) para esclarecimentos de qualquer dúvida sobre os equipamentos;
- O histórico de atualizações do produto incluindo as vulnerabilidades identificadas, medidas de mitigação e correções de segurança podem ser acessados [aqui](#);
- Se você acreditar que encontrou uma vulnerabilidade de segurança ou privacidade em um produto da JFL, entre em contato com o SAC;
- Para garantir a proteção dos clientes, a JFL não divulga, não discute nem confirma problemas de segurança até que uma investigação seja conduzida e as correções estejam disponíveis;
- É dever do usuário manter sempre o equipamento, o aplicativo e os módulos de comunicação com os seus respectivos softwares/firmwares atualizados. Para isso, a JFL recomenda que contrate uma empresa ou um profissional de segurança autorizado para que possa dar manutenção preventiva no sistema e analisar eventuais melhorias no sistema a fim de aumentar a proteção do usuário.

- Em casos especiais que há uma falha de segurança grave que pode ser explorada por pessoas indevidas ou que faça o equipamento perder a comunicação com os servidores na nuvem, a JFL pode atualizar a versão do equipamento automaticamente sem o consentimento do usuário.

17.4 LGPD – LEI GERAL DE PROTEÇÃO DE DADOS

Este equipamento possui dados de usuários gravados em sua memória como nome de usuários, número de apartamento e outras configurações. Estes dados são protegidos por senha contra pessoas não autorizadas. A JFL não possui acesso, não coleta, não utiliza e não faz nenhum tratamento destes dados.

17.5 MARCAS REGISTRADAS E CÓDIGO ABERTO

- Bluetooth® é uma marca mundialmente registrada da Bluetooth SIG, Inc.
- Wi-Fi®, o logo Wi-Fi são marcas registradas da Wi-Fi Alliance.
- Apple, iPhone, iPad e App Store são marcas registradas da Apple Inc registradas nos EUA e em outros países e regiões. iOS é uma marca comercial registrada da Cisco nos EUA e em outros países e é utilizada sob licença.
- O nome “Android”, o logotipo do Android, a marca “Google Play” e outras marcas registradas do Google são propriedades da Google LLC e não fazem parte dos recursos disponíveis no Android Open Source Project.
- Todas as outras marcas registradas e direitos autorais são de propriedade de seus respectivos proprietários.
- As licenças de código aberto usadas nos aplicativos e no firmware dos equipamentos podem ser encontradas no site da JFL.

GARANTIA

A JFL Equipamentos Eletrônicos Indústria e Comércio Ltda garante este aparelho por um período de 12 meses a partir da data de aquisição, contra defeitos de fabricação que impeçam o funcionamento dentro das características técnicas especificadas do produto. Durante o período de vigência da garantia, a JFL irá reparar (ou trocar, a critério próprio), qualquer componente que apresente defeito, excluindo a bateria que sofre desgaste naturalmente.

Excetuam-se da garantia os defeitos ocorridos por:

- Instalação fora do padrão técnico especificado neste manual;
- Uso inadequado;
- Violação do equipamento;
- Fenômenos atmosféricos e acidentais.

A visita de pessoa técnica a local diverso dependerá de autorização expressa do cliente, que arcará com as despesas decorrentes da viagem, ou o aparelho deverá ser devolvido a empresa vendedora para que seja reparado.



JFL EQUIPAMENTOS ELETRÔNICOS IND. COM. LTDA

Rua João Mota, 471 - Jardim das Palmeiras
CEP 37.538-714 - Santa Rita do Sapucaí / MG

Fone: (35) 3473-3550 / Fax: (35) 3473-3571
www.jfl.com.br

Rev.:00 16/07/26