# USUÁRIOS & PERMISSÕES

USUÁRIOS & PERMISSÕES

- AUTENTICAÇÃO 2FA - USUÁRIOS ERP 2.0

# AUTENTICAÇÃO 2FA - USUÁRIOS ERP 2.0

A **Autenticação de Dois Fatores (2FA)** é um protocolo essencial de segurança digital que adiciona uma camada extra de proteção ao processo de login no ERP 2.0 da ConnectPlug. A funcionalidade passou a ser uma **exigência obrigatória para novos usuários administradores**.

Essa medida tem grande impacto operacional e preventivo para o cliente e para a integridade dos dados:

- **Proteção Contra Invasões e Exposição de Dados:** Previne acessos indevidos e mitiga riscos de sequestro de contas ou vazamento de dados estratégicos, fiscais e financeiros da loja.
- **Obrigatoriedade e Prazo de Adequação:** Novos usuários administradores cadastrados no sistema possuem um prazo improrrogável de **72 horas (3 dias)** para realizar a ativação da 2FA. Caso a configuração não ocorra dentro dessa janela, o sistema realiza o **bloqueio do acesso através de um modal compulsório** até que a segurança seja habilitada.
- **Comunicação Direcionada por Banners:** Para orientar os usuários sem gerar atrito desnecessário, o ERP exibe alertas visuais específicos:
  - **Banner Laranja:** Exibido para **novos administradores**, alertando sobre a obrigatoriedade, a contagem regressiva do prazo de 72 horas e o risco iminente de bloqueio.
  - **Banner Verde:** Exibido para **usuários comuns** e **administradores antigos**, servindo como aviso orientativo para estimular a adoção voluntária das boas práticas de segurança.
- **Evolução da Governança:** O planejamento de produto prevê a expansão gradual da obrigatoriedade para toda a base de administradores e a liberação de travas para que empresas possam exigir a 2FA de todos os seus colaboradores.

---

## Pré-Requisitos

Antes de iniciar a configuração do duplo fator, o usuário deve garantir os seguintes pontos:

1. **Acesso ao ERP 2.0:** Possuir cadastro ativo de usuário no ERP da ConnectPlug.
2. **Canal de Validação Escolhido:**
   - **Via Aplicativo Autenticador:** Ter um app autenticador instalado no smartphone (ex.: Google Authenticator, Microsoft Authenticator ou Authy).

- **Via E-mail:** Ter acesso regular e imediato à caixa de entrada do e-mail cadastrado no usuário.

3. **Dispositivo de Confiança:** Utilizar o navegador ou terminal habitual de trabalho da empresa.

---

# ⚙ Passo a Passo

## 1. Acesso à Configuração de Segurança

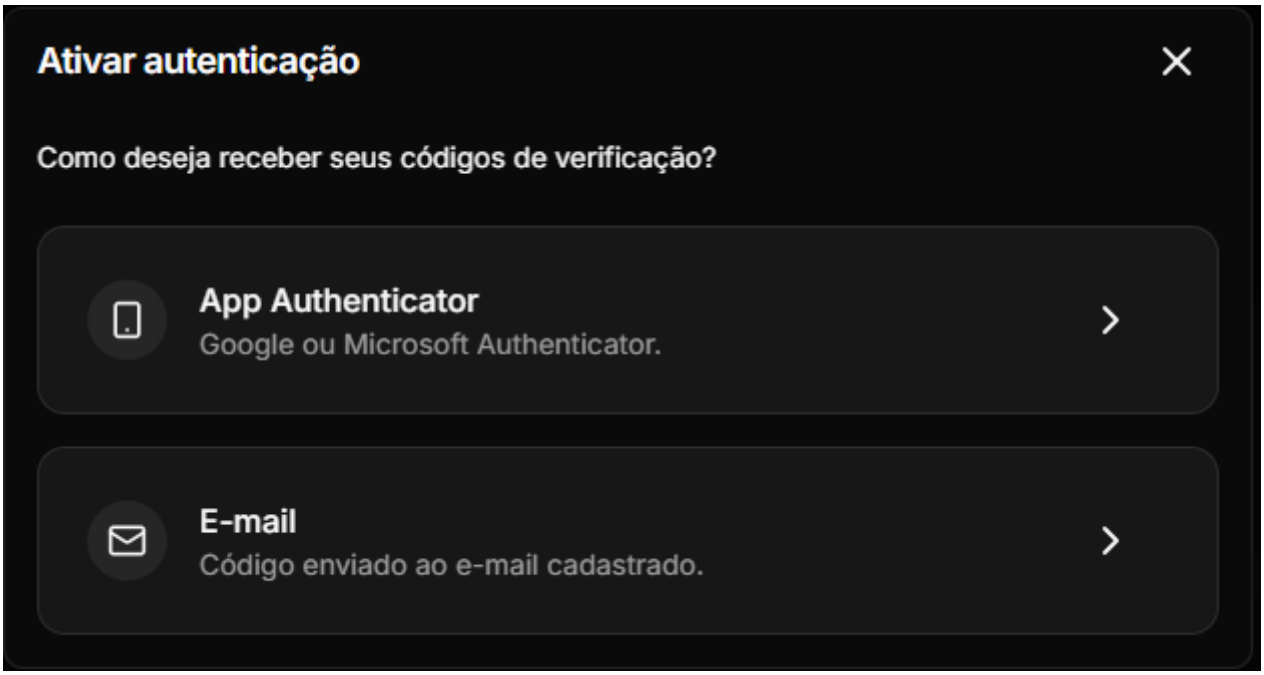
Ao acessar o ERP 2.0, localize o banner de aviso no topo da tela. Caso seja um novo administrador, clique diretamente no botão do **Banner Laranja** (ou, para outros usuários, no **Banner Verde**) para ser redirecionado à área de segurança. Se preferir, navegue diretamente até o perfil do usuário logado.




---

## 2. Escolha do Método de Autenticação

Na tela de ativação da **Autenticação em Dois Fatores**, selecione o canal de recebimento dos códigos de verificação: **Aplicativo Autenticador** ou **E-mail**.




## 3. Validação e Ativação do Código

- **Se escolheu Aplicativo Autenticador:** Abra o aplicativo no celular, escaneie o QR Code exibido na tela do ERP e digite o código de 6 dígitos gerado temporariamente pelo app.
- **Se escolheu E-mail:** Abra a sua caixa de entrada, copie o código de verificação recebido e insira-o no campo indicado do ERP. Confirme a operação para concluir o vínculo de segurança.

## Ativar autenticação

Escaneie o QR Code abaixo usando um aplicativo de segurança.

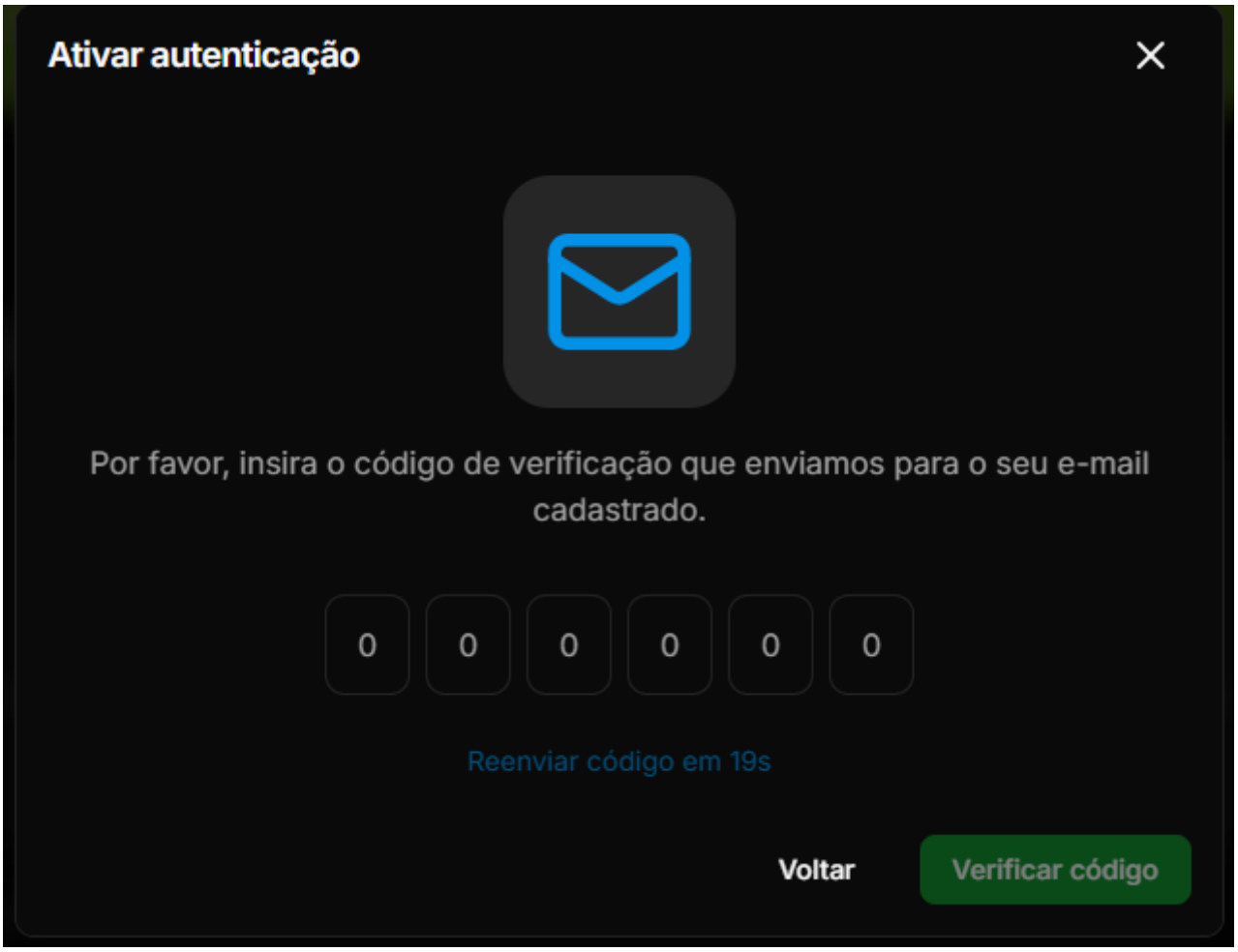


Não consegue escanear? Use a chave:

P4DI HWFW QEPV NK52 LY3V 2DXN 2FPB GZSH

0 0 0 0 0 0

Voltar Verificar código




---

## 4. Login Diário e Função "Lembrar Dispositivo"

Nos próximos acessos ao ERP, após digitar login e senha, o sistema solicitará o código de autenticação do método configurado. Para evitar atrito diário nas rotinas da loja, marque a opção **"Lembrar dispositivo"**. Com isso, o sistema **lembra o navegador por 15 dias**, exigindo uma nova validação de segurança apenas após o término desse período.

---

## Dúvidas Frequentes

- **Quem é obrigado a ativar a 2FA imediatamente?** A obrigatoriedade inicial aplica-se estritamente aos **novos usuários administradores** criados a partir da atualização. Usuários administradores antigos e usuários comuns de operação continuam, neste primeiro momento, com ativação voluntária orientada pelo banner verde.
- **O que acontece se um novo administrador não ativar o 2FA dentro de 72 horas?** Ao expirar o prazo de 72 horas (3 dias), o sistema **bloqueia a navegação** e apresenta um modal fixo obrigando a configuração do 2FA para que o usuário possa voltar a operar o ERP.
- **O usuário precisa digitar o código de dois fatores toda vez que fizer login?** Não. Ao realizar a autenticação, basta marcar a opção **"Lembrar dispositivo"**, o que mantém o computador liberado de novas solicitações de código pelo período de **15 dias**.
- **A equipe de Implantação ou Suporte da ConnectPlug pode usar o login e senha de administrador do cliente? Não! Essa prática é expressamente incorreta e**

**deve ser interrompida**. O uso de contas de clientes por colaboradores da ConnectPlug anula a eficácia da autenticação em dois fatores e expõe a operação a falhas de governança e segurança. A implantação e o suporte devem sempre atuar por meio de seus próprios acessos autorizados.

- **Quais métodos de 2FA estão disponíveis?** O usuário pode escolher receber o código de segurança através de um **aplicativo autenticador** ou diretamente pelo **e-mail** cadastrado.
- **A 2FA será obrigatória para todos os usuários no futuro?** Sim. Estão planejadas etapas futuras para estender a exigência aos administradores antigos e permitir que cada conta configure a obrigatoriedade da 2FA para todos os seus colaboradores.