Instruções para Utilizar Autenticação em Dois Fatores

A autenticação em 2 fatores, ou 2FA, fornece segurança adicional, pois junta algo que você sabe (a sua senha) com algo que você possui (o seu smartphone). Somente com a combinação dos dois será possível efetuar o login. Após validar a senha, será preciso informar um código de 6 dígitos, que será gerado pelo aplicativo no smartphone.

Passo 1: Sair do eproc

Antes de iniciar o cadastro, verifique se você está com uma sessão de uso do sistema aberta. Em caso positivo, encerre-a.

Passo 2: Início

Na tela inicial do eproc, insira seu usuário e senha. Mas, ao invés de entrar no sistema, clique no link "Autenticação em dois fatores". **Atenção!!! Se acessar com certificado digital, após clicar no botão correspondente, siga para o passo 3**

Descrição da Tela Inicial do eproc: Na imagem aparece o símbolo do eproc centralizado e abaixo o campo de preenchimento da sigla do usuário, abaixo o campo de prenchimento da senha do usuário e a abixo o botão ENTRAR.
Abaixo do botão ENTRAR, alinhado à direita encontra-se o link ESQUECI MINHA SENHA e abaixo o link AUTENTICAÇÃO DE DOIS FATORES.Fim.

Passo 3: Instruções

Abrirá uma janela com a seguinte mensagem: “ A autenticação em 2 fatores é um recurso para adicionar maior segurança no seu acesso ao sistema. Ao ativá-la, qualquer tentativa de login em dispositivos não liberados irá requerer também um código numérico gerado por um aplicativo. Antes de prosseguir, leia as instruções.”

Clique em "Prosseguir".

Caso você já tenha feito esse procedimento anteriormente, aparecerá a mensagem abaixo. Se você nunca usou, ignore-a. Clicar em ok.

Descrição da mensagem: “Atenção: Se a sua conta no sistema já estiver registrada no aplicativo, certifique-se de excluí-la antes da leitura do QR Code”.Fim.

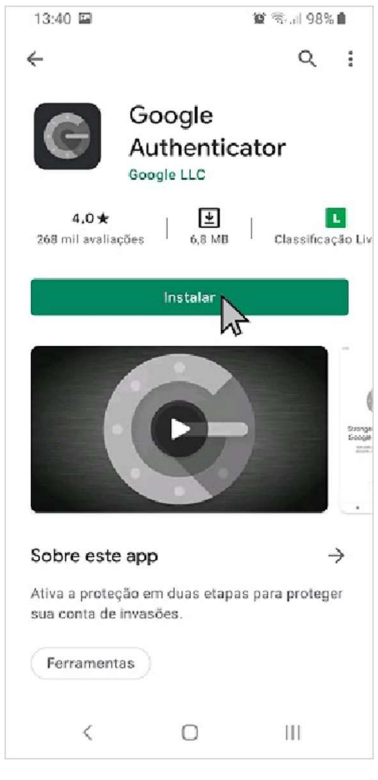
Passo 4: Instalação do Aplicativo de Autenticação

O eproc exibirá um código QR e um código alfanumérico como estes abaixo.

Descrição da tela do QR Code: Símbolo do Eproc centralizado. Abaixo o QR code. Abaixo uma seqência de 32 dígitos alfanuméricos (há possibilidade de copiá-los, clicando no ícone localizado no lado esquerdo dos 32 dígitos. Abaixo a seguinte mensagem: Antes de continuar, leia o código QR acima com o aplicativo de autenticação instaladao em seu smartphone. Caso esteja acessando esta página pelo smartphone, clique no código alfanumérico para copiá-lo. Há um link “instruções”. E embaixo, há um campo para preenchimento do email pessoal. Abaixo o Botão Enviar e o botão Cancelar.Fim.

Para lê-los, instale em seu smartphone um aplicativo próprio para autenticação em duas etapas, como o Google Authenticator, FreeOTP, Authy, etc. Nos exemplos abaixo, estamos usando o Google Authenticator.

Acesse a Apple Store ou o Google Play para instalar.



Abra o aplicativo Authenticator.

No primeiro uso, será exibida a tela abaixo. Neste caso, clique em "Primeiros passos".

Descrição da tela: O símbolo do Google Authenticator centralizado, embaixo a mensagem: “Mais segurança com o Google Authenticator” Receba códigos de verificação para todas as suas contas usando a verificação em duas etapas. Embaixo o botão Primeiros Passos. Fim.

O usuário será direcionado para tela “Configure sua primeira conta”.

Descrição da tela: Mensagem: Configure sua primeira tela. Para configurar uma conta, é necessário usar o código QR ou à chave de definição nas configurações da autenticação de dois fatores (do Google ou do serviço de terceiros). Embaixo há o link “Ler código QR” e embaixo o link “Inserir chave de configuração”. Fim.

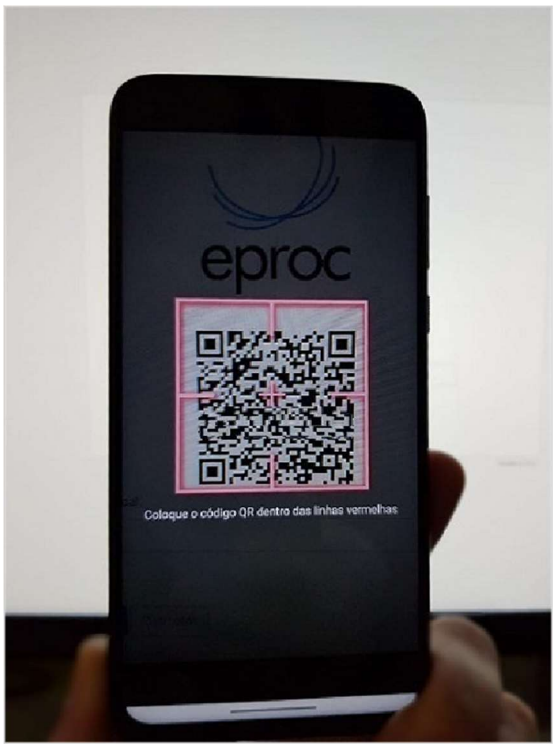
Se o eproc estiver sendo executado no computador, clique em "Ler código QR".

Caso contrário, se você está com o eproc aberto no smartphone, clique em "Inserir chave de configuração".

Se for solicitada a permissão abaixo, clique em "Permitir".

Descrição da janela permissão: Mensagem: “Permitir que Authenticator tire fotos e grave vídeos? Existe a opção de Negar ou Permitir. Fim.

Caso você tenha optado por ler o código QR, aponte a câmera para o código QR que está sendo exibido no eproc.



Ou, se você escolheu inserir a chave de configuração, clique sobre o código alfanumérico de 32 dígitos que está sendo exibido no eproc, logo abaixo do código QR, para copiá-lo.

Em seguida, cole-o no aplicativo de autenticação. Clique em "Adicionar".

Descrição da tela do aplicativo Google Authenticator: caso o usuário escolha a opção de Inserir chave de configuração, ele será direcionado para uma tela com um campo para inserção do Nome da conta, embaixo o campo para inserir a chave de 32 dígitos e embaixo um campo seletor que há as opções de Tipo de Chave Baseado no horário ou baseado na contagem. O usuário deve deixar a opção “baseado no horário”. Fim.

Clique em "Adicionar conta".

Após adicionar a conta no aplicativo, volte ao eproc na tela do QRCode .

Passo 6: Finalização do Cadastro no eproc

Informe um endereço de e-mail que não seja associado com a instituição. Por exemplo, pode ser do gmail, hotmail, yahoo, etc. É imprescindível que a senha de acesso ao e-mail seja diferente da senha de acesso ao sistema.

Clique em "Enviar" para que um link de ativação seja enviado para o endereço de e-mail fornecido. Somente após receber o e-mail e clicar no link é que o mecanismo de autenticação em 2 fatores estará ativado.

Passo 7: Login com a Autenticação em 2 Fatores

Vá à tela inicial do eproc. Informe seu usuário e senha e clique em "ENTRAR".

Se a autenticação em 2 fatores estiver ativada, então, após informar o usuário e senha, será exibida outra tela solicitando o código numérico:

Descrição da tela: Símbolo do eproc centralizado. Abaixo a mensagem: Informe o código de 6 dígitos gerado pelo aplicativo de autenticação em 2 fatores:. Abaixo o campo para inserir o código. Logo abaixo, tem um checkbox desmarcado com a mensagem “Não usar o 2FA neste dispositivo e navegador”. Abaixo o link instruções. Abaixo 3 botões: à esquerda o botão Validar, no centro o botão Desativar 2FA e à direita o botão Cancelar. Fim.

Abra o aplicativo de autenticação no seu smartphone e veja o código gerado. Insira esse código no eproc e clique em "Validar".

Obs.: o código muda a cada 30 segundos, e o sistema aceitará qualquer código gerado nos últimos 5 minutos.

De agora em diante, sempre que fizer login, será preciso consultar o seu smartphone, porque o código se modificará com frequência.

Liberação de Dispositivos

Para dispositivos usados com frequência, pode ser conveniente liberá-los da validação a cada login. Para isso, na tela onde é solicitado o código numérico, marque a opção "Não usar o 2FA neste dispositivo e navegador". Essa sinalização precisará ser realizada para cada navegador utilizado. O código poderá ser solicitado novamente se for feita a limpeza dos cookies do navegador ou se a liberação perder a validade de acordo com o período estabelecido pela instituição.

Desativando a Autenticação em 2 Fatores

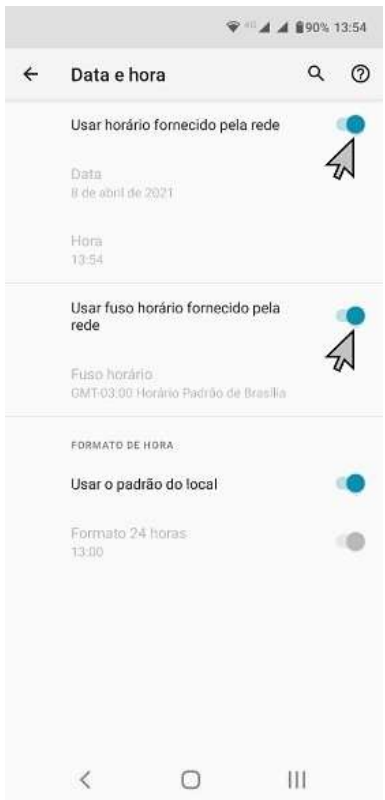
Se não conseguir validar o código por algum motivo (perda do aparelho, defeito, roubo, erro no aplicativo, etc.), é possível requisitar a desativação da autenticação em 2 fatores na mesma tela onde é solicitado o código numérico, ou então por meio do link "Autenticação em dois fatores" disponível na tela inicial de login. Clique no botão Desativar 2FA para que um e-mail com o link de desativação seja enviado para o endereço que foi fornecido no momento da leitura do código QR. Somente após receber o e-mail e clicar no link é que o mecanismo de autenticação em 2 fatores será desativado.

Solução de Problemas

Caso esteja recebendo a mensagem "Código de autenticação inválido." ou "Código de autenticação não reconhecido.", é possível que o horário no seu smartphone esteja desatualizado.

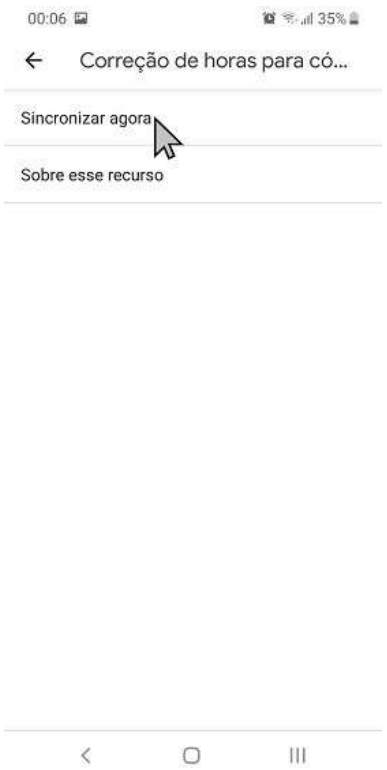
Primeiro verifique se o aparelho está configurado para obter a hora automaticamente pela rede. Abaixo estão exemplos de como fazer isso em diferentes sistemas.

Descrição: Foram apresentadas 04 telas de 04 modelos diferentes de configuração da data e hora do telefone. Recomendar ao usuário em acessar as Configurações do telefone, buscar por Data e Hora e habilitar/ativar o opção de Usar horário fornecido pela rede. Fim



Após, siga estes passos para sincronizar o horário no aplicativo do Google Autenticator:

- Na tela onde são gerados os códigos de 06 dígitos , clicar nas 03 barras sobrepostas localizadas no canto superior esquerdo em seguida Configurações e clicar em Correção de horas para códigos e depois clicar em Sincronizar agora.



Caso as alternativas acima não tenham funcionado, sugerimos que o Google Authenticator seja reinstalado ou que, ao invés dele, seja instalado o Authy: