

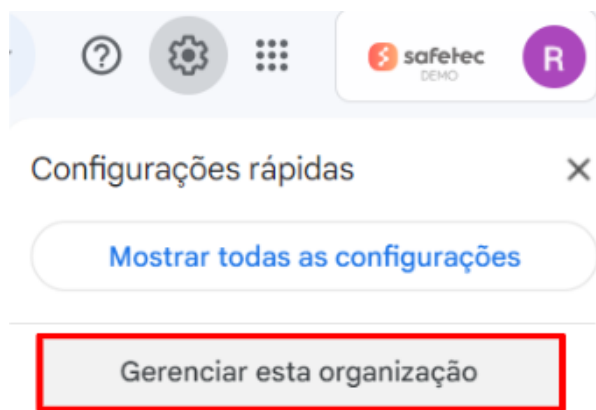
A autenticação em duas etapas fornece uma camada extra de segurança aos usuários, fazendo com que além de usuário e senha, também seja exigido um código enviado para um aparelho móvel previamente cadastrado.

Para que os usuários possam usar este recurso é necessário habilitar através do painel de controle, desta forma eles estarão aptos a ativar e configurar a autenticação em duas etapas.

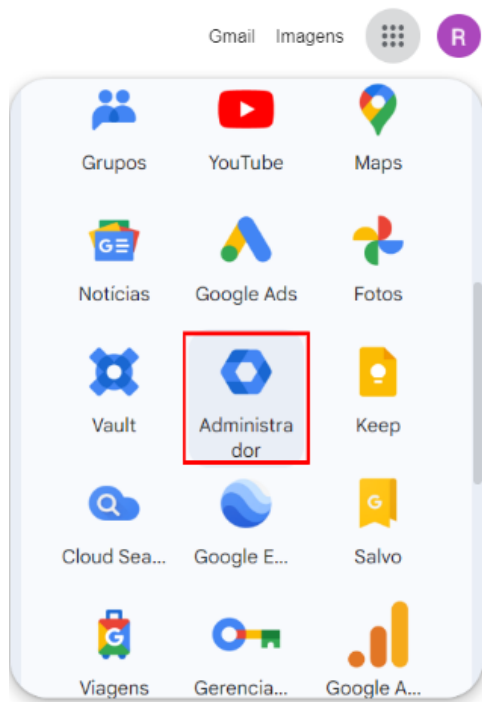
1. Acesse o Admin Console, de uma destas três maneiras:

- Acesse painel de controle através da URL admin.google.com, em seguida se autenticar com login e senha;

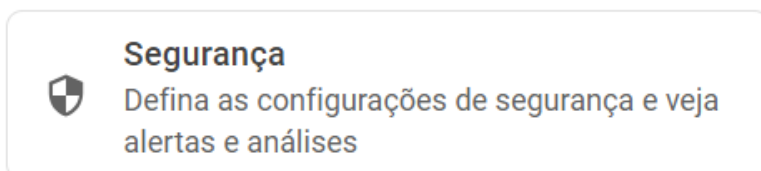
- No Gmail, clique na engrenagem  no canto superior direito e depois em "**Gerenciar esta organização**";



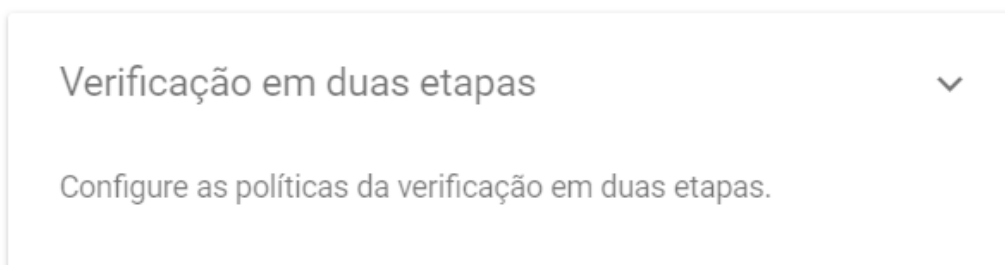
- No menu de aplicativos do Google , role o scroll para baixo e selecione a opção **"Administrador"**;



2. Clique na opção **"Segurança"**;



3. Desça a página e clique em **"Verificação em duas etapas"**;



4. Em **"Verificação em duas etapas"**, na parte de **"Autenticação"**, marque a opção **"Permitir que os usuários ativem a verificação em duas etapas"**;

Autenticação

Aplicada no local

Adicione uma camada extra de segurança às contas de usuário pedindo que eles confirmem a própria identidade ao digitar um nome de usuário e uma senha. [Saiba mais](#)



Permitir que os usuários ativem a verificação em duas etapas

Aplicação



Desativar



Ativar



Ativada a partir de

Date



Obs.: a confirmação em duas etapas não pode ser usada para contas que usam um serviço SAML de logon único (SSO). Consulte o Serviço SAML de SSO para o Google Workspace.

5. No final da página clique em "**Salvar**".

SALVAR

Obs.: Quando seus usuários se inscreverem na confirmação em duas etapas, talvez eles precisem usar senhas específicas de aplicativos além de seus códigos de confirmação. Para aplicativos instalados que não têm um campo de confirmação em duas etapas, seus usuários precisarão [gerar uma senha específica de aplicativo](#) em cada dispositivo ou aplicativo em vez da senha comum para acessar a Conta do Google.

Os dispositivos comuns que exigem senhas específicas de aplicativo são: Gmail e Google Agenda nos telefones Android, Active Sync para Windows Mobile e iPhone, e clientes IMAP como Thunderbird.

Caso deseje aplicar as alterações imediatamente para usuários ou iniciar um processo de adoção, siga os passo abaixo:

1. Do lado esquerdo da tela você pode selecionar a organização;

Unidades organizacionais

Pesquisar unidades organizacionais

- ▼ Safetec Demo
 - ▶ Colaboradores ST
 - ▶ DEMO Chrome

3. Caso deseje aplicar imediatamente a verificação em duas etapas marque a opção "**Ativado**";

Verificação em duas etapas

Autenticação
Herdado

Adicione uma camada extra de segurança às contas de usuário pedindo que eles confirmem a própria identidade ao digitar um nome de usuário e uma senha. [Saiba mais](#)

☒ Permitir que os usuários ativem a verificação em duas etapas

Aplicação

☐ Desativado

☒ Ativado

☐ Ativada a partir de 

Obs.: Marcar essa opção pressupõe que o usuário já tenha configurado a verificação em duas etapas na sua conta. Caso o usuário não tenha configurado a verificação em duas etapas na sua conta, o mesmo não conseguirá acessar a conta.

4. Caso deseje dar um tempo para que os usuários configurem a verificação em duas etapas na sua conta, marque a opção "**Ativada a partir de**";

Autenticação

Aplicada no local

Adicione uma camada extra de segurança às contas de usuário pedindo que eles confirmem a própria identidade ao digitar um nome de usuário e uma senha. [Saiba mais](#)

☒ Permitir que os usuários ativem a verificação em duas etapas

Aplicação

☐ Desativar

☐ Ativar

☒ Ativada a partir de Date



< agosto de 2024 ▾ >

Após selecionar o prazo limite para a configuração da autenticação em duas etapas na contas. Os usuários toda a vez de logar em suas contas, serão lembrados da ativação da autenticação em duas etapas.

OBS: Caso selecione algum desses 2, você irá se deparar com mais algumas opções, você poderá configurar se o usuário pode se inscrever antes da imposição da verificação de duas etapas, selecionar o [método de verificação permitido](#), e a [frequência de verificação](#).

Métodos

Selecione o método a ser aplicado. [Saiba mais](#)

☒ Indiferente

☐ Tudo, exceto códigos de verificação por SMS ou chamada telefônica

☐ Apenas a chave de segurança

OBS: a opção "**Frequência**" permite que a verificação seja automática nos dispositivos confiáveis do usuário.

Frequência

Para não repetir a verificação em duas etapas, os usuários podem fazer login nos dispositivos de confiança. [Saiba mais](#)

☒ Permitir que o usuário confie no dispositivo

5. Clique em "**Salvar**".

SALVAR

