

**CONECTA**

**GUIA COMPLETO PARA  
CONFIGURAÇÃO DE CHAVES DE  
SEGURANÇA EM DISPOSITIVOS  
USB**

# Introdução

O uso de dispositivos USB em servidores on-premises apresenta riscos significativos de segurança e operacionais.

Esses dispositivos podem introduzir malware, vírus ou ransomware, comprometendo a segurança dos dados e a integridade do sistema. Além disso, há riscos de perda de dados sensíveis, acesso não autorizado e desestabilização do sistema devido a conflitos de hardware ou software.

A falta de controle e monitoramento pode levar a problemas de conformidade com políticas de segurança e regulamentos de proteção de dados.

Para mitigar esses riscos, é essencial implementar políticas restritivas, utilizar software de segurança, adotar a criptografia de dados, monitorar e auditar o uso de dispositivos USB, além de promover a educação e o treinamento dos funcionários.

Este guia oferece um passo a passo para a configuração de chaves de segurança em dispositivos USB, visando proteger servidores on-premises contra essas ameaças.

# Sumário

Preparação da Máquina.....	4
Criação do Arquivo.....	5
Adição de Senha.....	6
Exemplos e Evidências.....	7
Considerações Finais.....	8

# Preparação da Máquina

Antes de iniciar a criação do arquivo **key.txt**, insira o dispositivo USB em uma máquina que não tenha nossa aplicação instalada. Se a aplicação já estiver instalada, não será possível adicionar o arquivo corretamente.

# Criação do Arquivo

## 1 - Acessar o Diretório Raiz:

- Abra o explorador de arquivos do sistema operacional (por exemplo, Windows Explorer, Finder no macOS, ou um gerenciador de arquivos no Linux).
- Navegue até o dispositivo USB recém-inserido.
- Certifique-se de que está no diretório raiz do dispositivo USB, que é o primeiro nível do dispositivo, sem entrar em pastas.

## 2 - Criar o Arquivo de Texto:

- Clique com o botão direito do mouse no diretório raiz do dispositivo USB.
- Selecione a opção para criar um novo arquivo de texto (por exemplo, "Novo > Documento de Texto" no Windows).
- Nomeie o arquivo exatamente como **key.txt** (sem aspas e em minúsculas).

## 3 - Verificação do Nome:

- Verifique que o nome do arquivo está correto e que a extensão .txt é visível. Caso contrário, ajuste as configurações do explorador de arquivos para mostrar as extensões de arquivos conhecidos.

# Adição de Senha

## 1 - Abrir o Arquivo de Texto:

- Dê um duplo clique no arquivo key.txt para abri-lo em um editor de texto simples (por exemplo, Notepad no Windows, TextEdit no macOS, ou Gedit no Linux).

## 2 - Inserir a Senha:

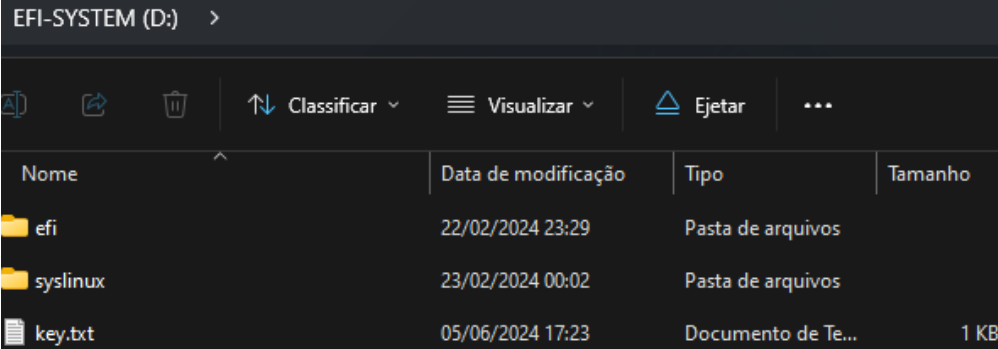
- Digite uma senha forte e segura. A senha deve ser exclusiva e conhecida apenas pelos funcionários autorizados.
- Uma senha forte geralmente inclui uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais.

## 3 - Salvar o Arquivo:

- Após digitar a senha, salve o arquivo.
- Feche o editor de texto e verifique se o conteúdo foi salvo corretamente.

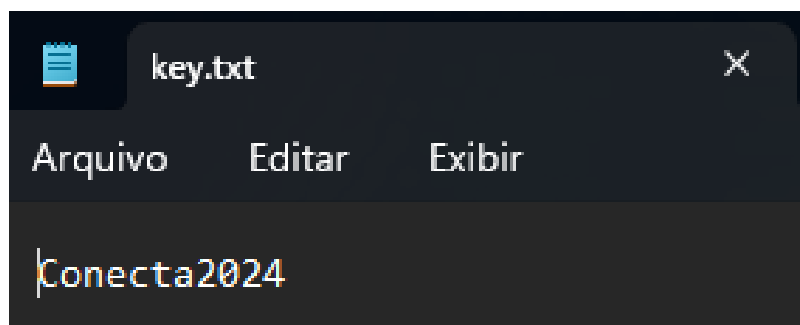
# Exemplos e Evidências

Diretório raiz do dispositivo com o arquivo:



Nome	Data de modificação	Tipo	Tamanho
efi	22/02/2024 23:29	Pasta de arquivos	
syslinux	23/02/2024 00:02	Pasta de arquivos	
key.txt	05/06/2024 17:23	Documento de Te...	1 KB

Exemplo de Senha dentro do arquivo key.txt:



# Considerações Finais

## **Confidencialidade:**

- Mantenha a senha em sigilo e compartilhe-a apenas com funcionários autorizados.
- Evite anotar a senha em locais inseguros ou acessíveis a pessoas não autorizadas.

## **Manutenção da Senha:**

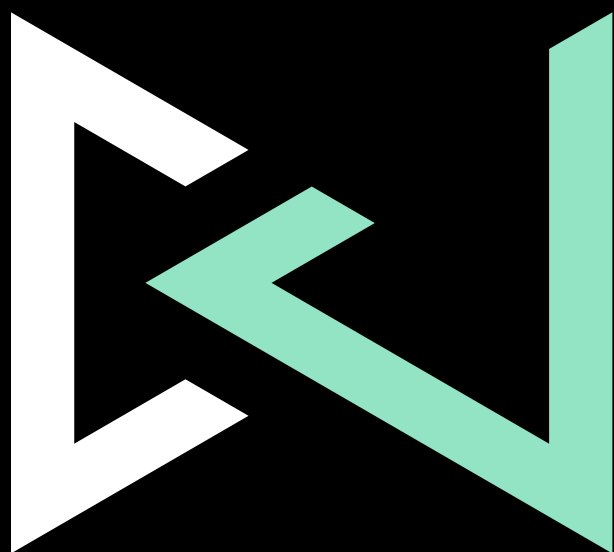
- Considere alterar a senha periodicamente para manter a segurança.
- Em caso de suspeita de comprometimento, altere a senha imediatamente e atualize o arquivo key.txt conforme os passos descritos acima.

## **Documentação e Treinamento:**

- Documente o procedimento para futuros usos e treine os funcionários responsáveis pela manutenção dos dispositivos USB sobre a importância e os detalhes deste processo.

Seguindo esses passos detalhados, você garantirá que o dispositivo USB esteja configurado corretamente e protegido contra acessos não autorizados.





# CONECTA

**TRANSFORMANDO IDEIAS EM REDES DE SUCESSO**

