Carregamentos de arquivo do cliente no Cisco Technical Assistance Center

Índice

Visão geral

Os clientes são de grande importância para a Cisco, e é por isso que gostamos de abordar e resolver os problemas dos clientes de maneira oportuna. Uma forma de um cliente ajudar o processo é fornecendo os arquivos relevantes para o Cisco Technical Assistance Center (TAC) para revisão. Os engenheiros de suporte ao cliente do TAC usam esses arquivos para ajudar a resolver problemas dos clientes e a Cisco fornece várias opções para o carregamento de informações para o Cisco TAC para atender aos requisitos de um cliente. Algumas dessas opções são menos seguras, levando a certos riscos inerentes, e cada opção tem limitações que os clientes devem considerar antes de decidir sobre uma opção de carregamento apropriada. A Tabela 1 resume as opções de carregamento disponíveis com detalhes sobre recursos de criptografia de arquivos, limites de tamanho de arquivos recomendados e outras informações relevantes.

Tabela 1. Opções de carregamento disponíveis

Opção disponível (em ordem de preferência)	Arquivos criptografados	Arquivos criptografados	Limite de tamanho de

		em trânsito	em repouso	arquivo recomendado
Support Case Manager (SCM)	Como fazer	Yes	Yes	250 GB
Carregador de arquivo de chamado	Como fazer	Yes	Yes	250 GB
Customer eXperience Drive	Como fazer	Sim*	Yes	Nenhum limite
Enviar por e-mail para attach@cisco.com	Como fazer	Não**	Yes	Limites de servidor de e-mail de 20 MB ou menos de acordo com o cliente
*Se aplica a todos os protocolos, exceto FTP. Ao usar o FTP, a Cisco recomenda que os dados sejam criptografados antes de serem carregados. **O cliente deve criptografar antes do trânsito. A transmissão do provedor de rede/e-mail do cliente pode ou não ser criptografada em trânsito. O trânsito seguro é garantido apenas a partir do ponto em que o e-mail/anexo atinge a rede da Cisco.				

Carregamento de arquivo no Support Case Manager

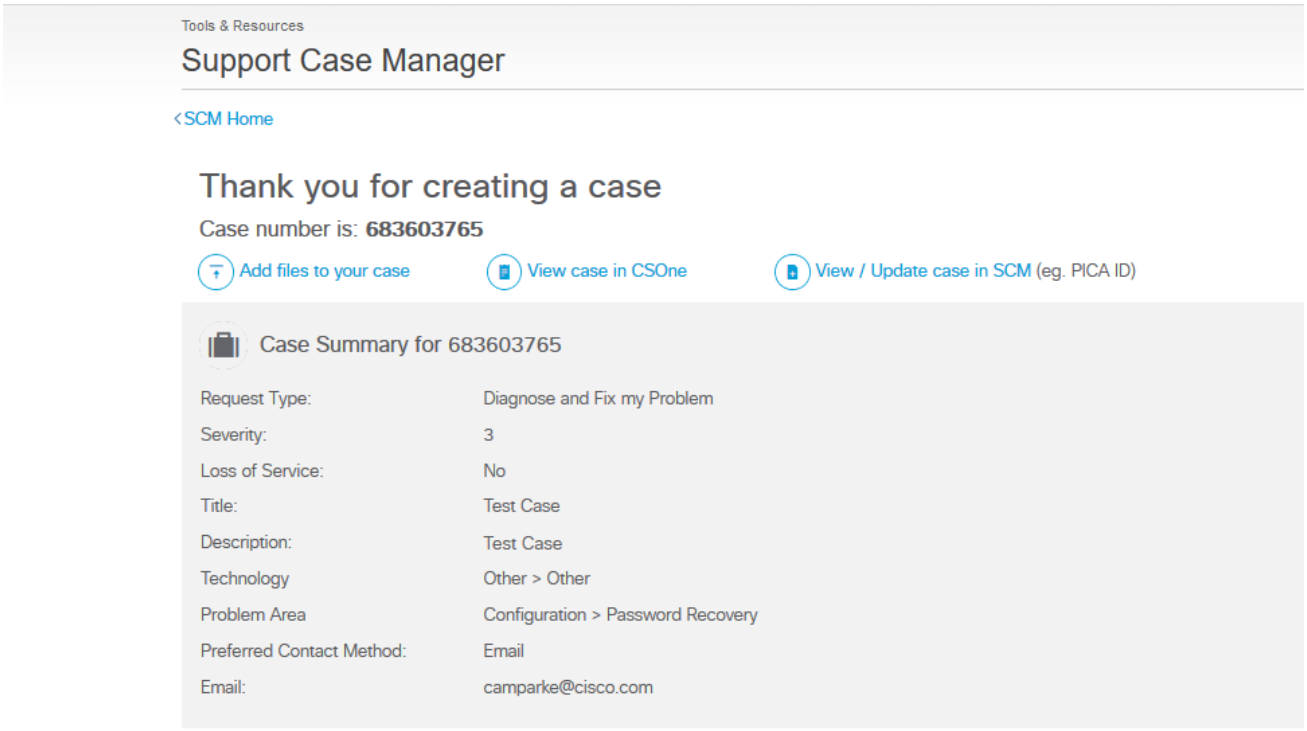
O método de carregamento de arquivo do Support Case Manager (SCM) é a opção preferida e mais segura para o carregamento de arquivos para os casos. Os arquivos transferidos usando essa opção são criptografados em trânsito e restritos a um tamanho de 250 GB. O canal de comunicação entre o cliente do dispositivo de computação e a Cisco é criptografado. Os arquivos enviados por meio do SCM são vinculados imediatamente ao chamado associado e armazenados em um formato criptografado.

Carregar um arquivo ao abrir um chamado

Siga estas etapas da tela de confirmação do chamado. Para obter instruções mais detalhadas sobre como criar ou gerenciar um chamado no SCM, consulte Ajuda do SCM.

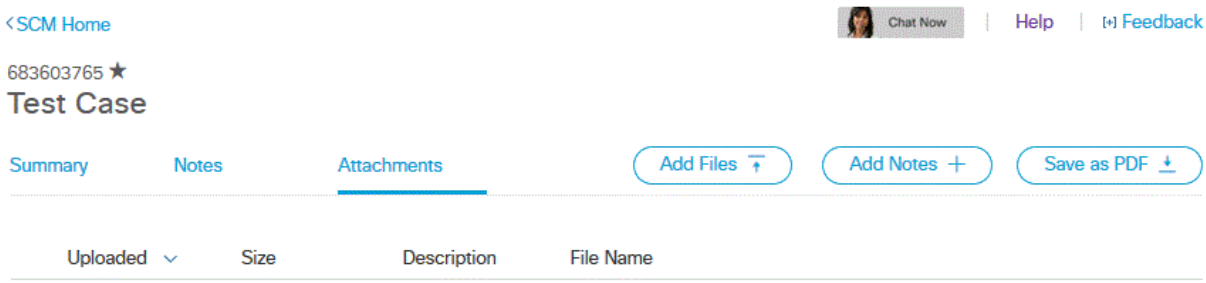
Etapa 1 Selecionar o botão **Add files to your case** (Adicionar arquivos ao chamado) (Figura 1).

Figura 1. SCM Add Files to Your Case (Adicionar arquivos ao chamado)



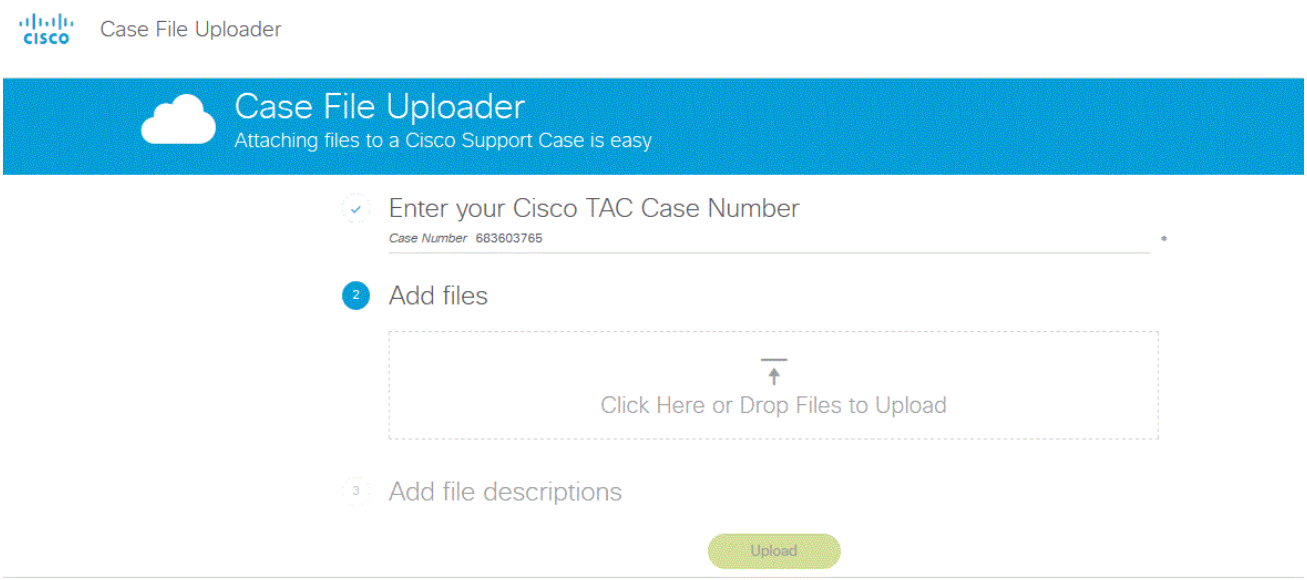
Etapa 2 Na guia Attachments (Anexos), selecione o botão **Add Files** (Adicionar arquivos) (Figura 2).

Figura 2. SCM: Guia Attachments (Anexos)



Você será direcionado para a ferramenta de carregador de arquivo de chamado. O chamado que você criou será pré-preenchido na ferramenta (Figura 3). Continue na etapa 3 da seção Carregador de arquivo de chamado.

Figura 3. Carregador de arquivo de chamado: Tela de arrastar e soltar arquivo



Carregamento de um arquivo para um chamado existente

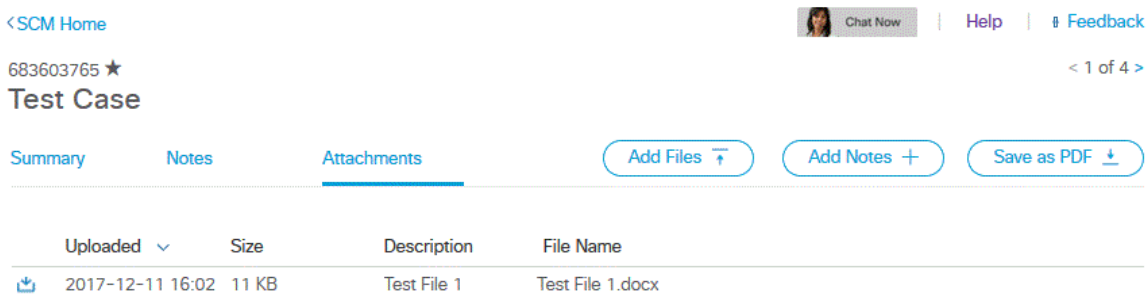
Depois do envio de um chamado, você pode atualizar ou alterar as informações opcionais.

Etapa 1 Início de uma sessão ao SCM.

Etapa 2 Para abrir e editar um caso, clique no número ou Título do chamado na lista. A página de detalhes do caso é exibida.

Etapa 3 Na parte superior da página de detalhes do chamado, há três guias: **Summary** (Resumo), **Notes** (Notas) e **Attachments** (Anexos). Ao lado das guias há um conjunto de botões de barra de ferramentas: **Attach Files** (Anexar arquivos), **Add Notes** (Adicionar notas) e **Save as PDF** (Salvar como PDF). Clique em **Add Files** (Adicionar arquivos) para selecionar um arquivo e carregá-lo como um anexo do chamado (Figura 4).

Figura 4. Tela SCM Attachments (Anexos de SCM)



Você será direcionado para a ferramenta de carregador de arquivo de chamado. O chamado que você criou será pré-preenchido na ferramenta (Figura 3). Continue na etapa 3 da seção Carregador de arquivo de chamado.

Retornar ao início

Carregador de arquivo de chamado

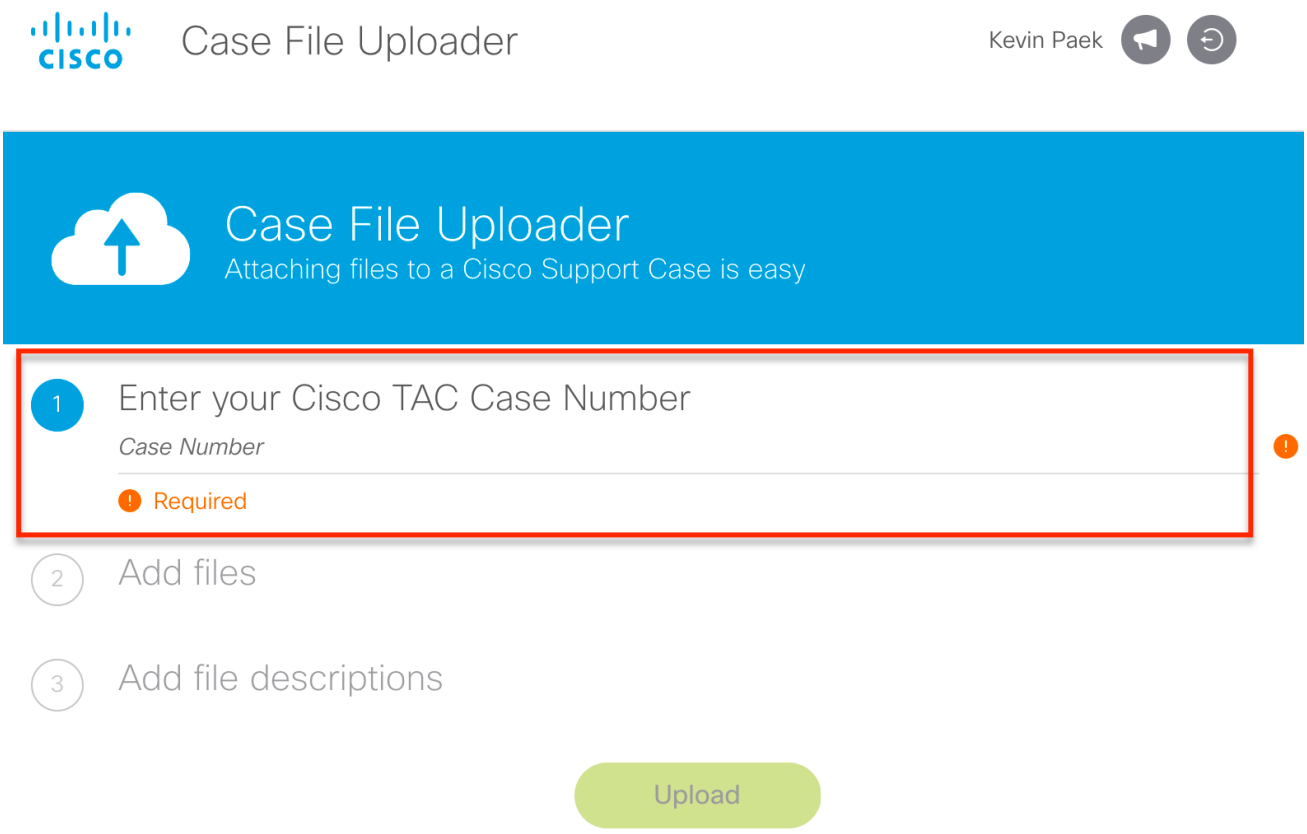
Outro método seguro de carregamento de arquivos para um chamado é o Carregador de arquivo de chamado. Essa ferramenta é similar ao SCM, pois os arquivos transferidos usando essa opção são criptografados em trânsito e restritos a um tamanho de 250 GB. O canal de comunicação entre o cliente do dispositivo de computação e a Cisco é criptografado. Arquivos carregados por meio do carregador de arquivo de chamado imediatamente são vinculados ao gabinete associado e armazenados em um formato criptografado. Siga as seguintes etapas para anexar um arquivo ao utilizar essa ferramenta.

Nota: Se você descobrir que a ferramenta não permite que você envie um arquivo para o seu chamado, o número do caso digitado é inválido ou você não tem as permissões necessárias para adicionar arquivos. Para fazer upload de arquivos para um caso, o perfil cisco.com deve estar associado ao contrato para o qual o caso foi aberto. Você pode adicionar contratos de serviço ao perfil usando o gerente de perfil da Cisco ou permitir que o administrador de gerenciamento de acesso ao serviço faça isso para você. Se você precisar de mais assistência, ligue para o Cisco Technical Assistance Center (TAC).

Etapa 1 Início de uma sessão para encaixotar o arquivo Uploader.

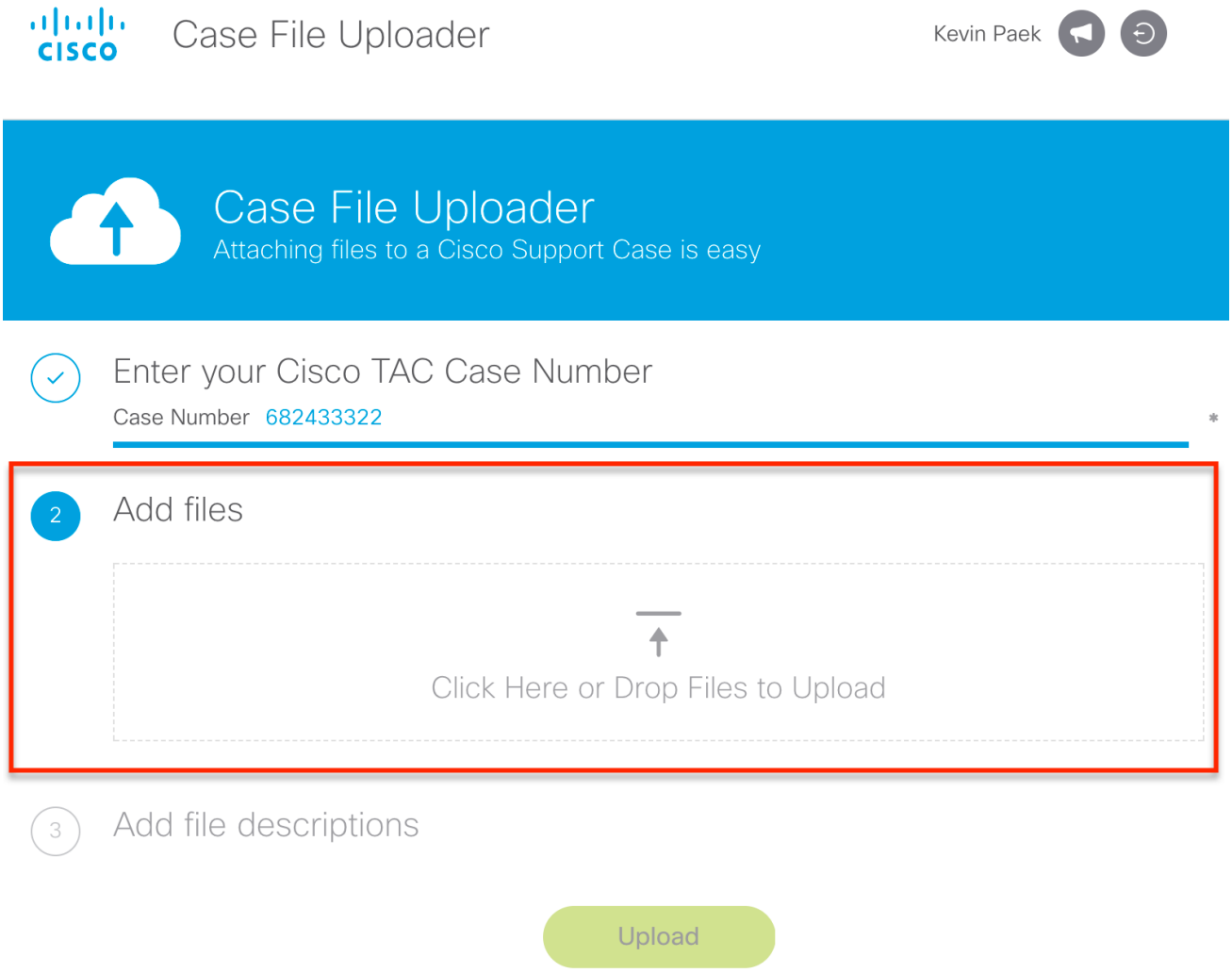
Etapa 2 Insira seu número de caso no campo fornecido (Figura 5).

Figura 5. Carregador de arquivo de chamado: Tela de entrada de número de chamado



Etapa 33 ao escolher um arquivo para anexar, arraste e solte ou clique dentro da caixa com traços para selecionar o arquivo a ser carregado (Figura 6).

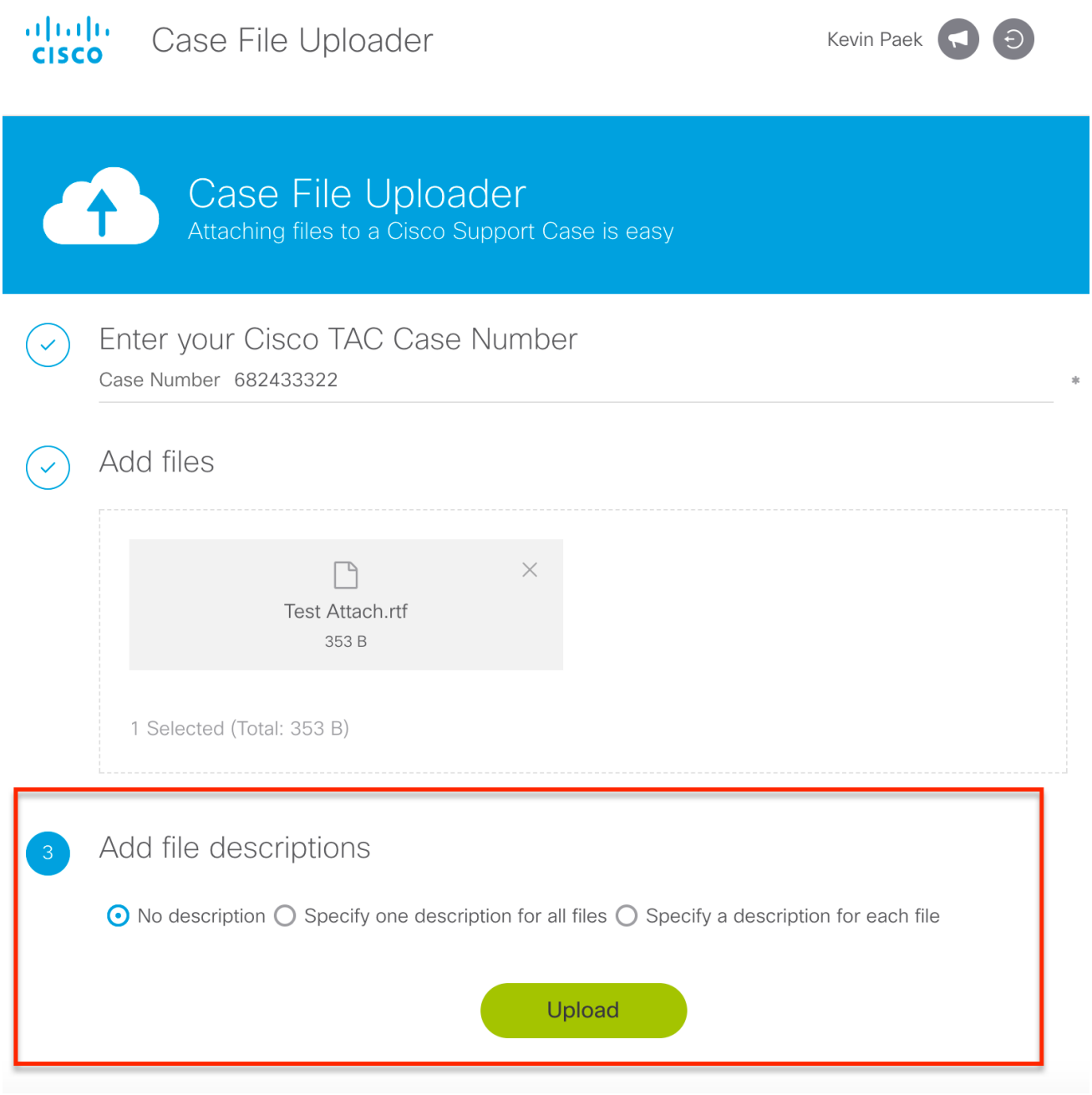
Figura 6. Carregador de arquivo de chamado: Tela de arrastar e soltar arquivo



Etapa 4 Depois de escolher um arquivo, se você precisa especificar uma descrição, clique em **Upload** (Carregar). Caso contrário, você pode optar por adicionar mais detalhes usando as outras opções. (Figura 7). Os campos **Category** (Categoria) e **Description** (Descrição) permitem que você adicione mais informações sobre o arquivo:

- Use o campo **Category** (Categoria) para selecionar um tipo de anexo.
- Use o campo **Description** (Descrição) para fornecer uma breve descrição do arquivo.

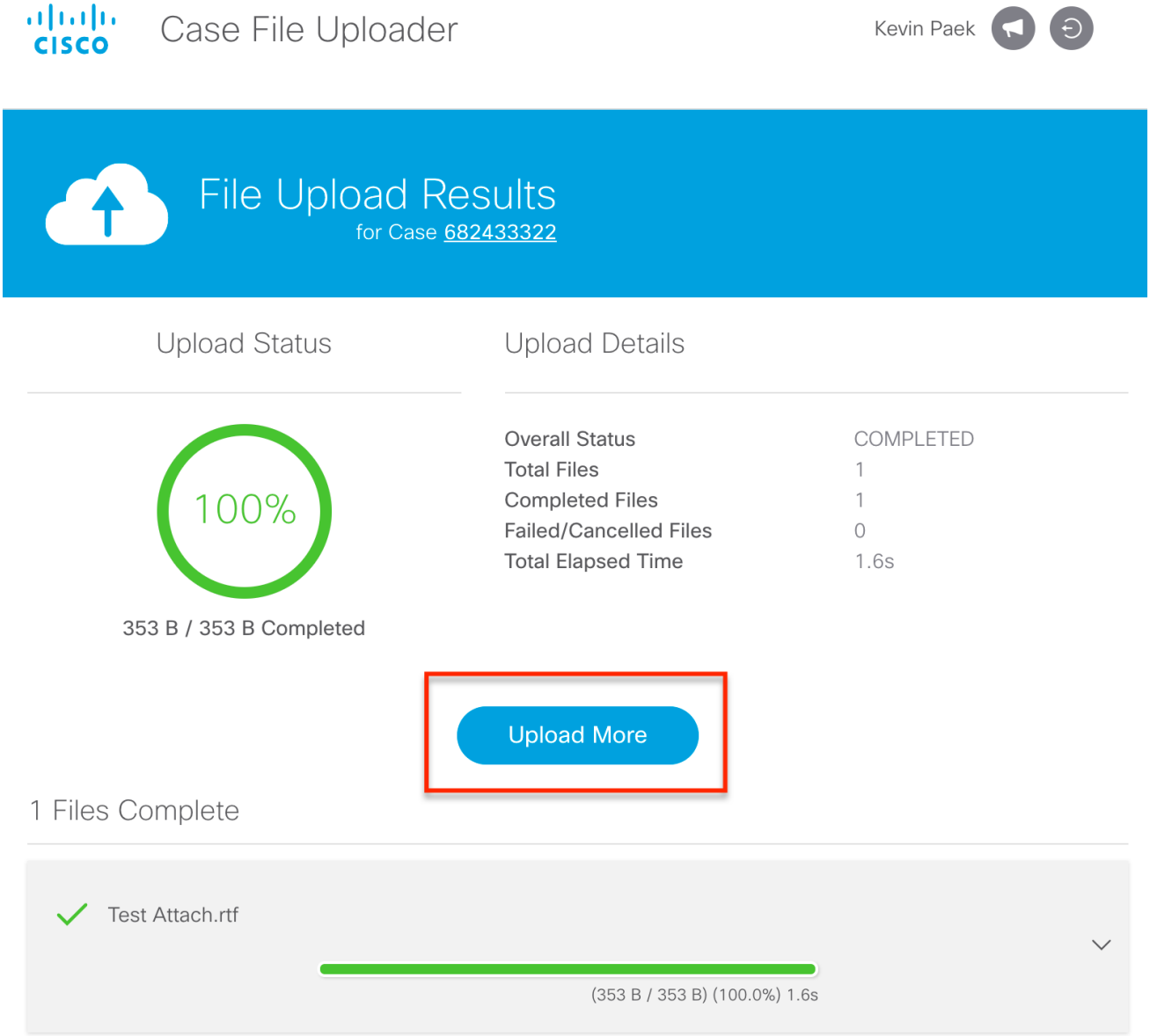
Figura 7. Carregador de arquivo de chamado: Entrada de descrição do arquivo



Etapa 5 Clique em **Upload** (Carregar) para carregar o arquivo.

Etapa 6 A próxima tela mostra o status do arquivo. Depois de carrega o arquivo, clique em **carregar mais** (Figura 8) para fazer o upload de anexos adicionais.

Figura 8. Carregador de arquivo de chamado: Tela de status de carregamento



Retornar ao início

Customer eXperience Drive

Resumo do serviço

O Customer eXperience Drive (CXD) é um serviço de carregamento de arquivos de vários protocolos, sem limitação em relação ao tamanho do arquivo enviado. Ele permite que os clientes da Cisco com solicitações de serviço (SRs) ativas carreguem dados diretamente para um chamado usando um conjunto exclusivo de credenciais criadas por SR. Os protocolos suportados pelo CXD nativamente são compatíveis com os produtos da Cisco, possibilitando o carregamento direto em dispositivos da Cisco para SRs.

Protocolos suportados

A tabela 2 resume os protocolos suportados pelo CXD. É importante observar que, independentemente do protocolo usado, não há nenhum limite definido em relação ao tamanho do arquivo carregado.

Tabela 2. Protocolos suportados pelo CXD

Nome	Protocolo/porta	Criptografado	Portas de canais de dados	Notas
Secure File Transfer Protocol (SFTP)	TCP/22	Yes	N/A	
Secure Copy Protocol (SCP)	TCP/22	Yes	N/A	
Hyper Text Transfer Protocol over SSL (HTTPS)	TCP/443	Yes	N/A	Interfaces de usuário e de aplicação disponíveis*
File Transfer Protocol of SSL (FTPS) implícito	TCP/990	Yes	30000-40000	Os firewalls não podem inspecionar FTPS, pois o canal de controle é criptografado. Portanto, o firewall precisa permitir a conectividade de saída para todo o intervalo de portas de canal de dados.
File Transfer Protocol of SSL (FTPS) explícito	TCP/21	Sim**	30000-40000	
File Transfer Protocol (FTP)	TCP/21	No	30000-40000	• A Cisco não recomenda o uso de FTP, pois o protocolo não suporta criptografia. Se ele precisar ser usado, os dados devem ser criptografados antes da transferência. • Os firewalls devem inspecionar o tráfego FTP para permitir que os canais de dados sejam

				adequadamente estabelecidos. Se o FTP não foi inspecionado em toda a rede, o firewall precisa permitir a conectividade de saída para todo o intervalo de portas de canal de dados.

* Detalhes sobre o uso da API PUT e o código python de amostra são compartilhados mais adiante neste documento.
** O modo FTPS explícito requer que o cliente solicite explicitamente as negociações TLS usando o comando “AUTH TLS”, antes de tentar efetuar login.

Token de carregamento CXD

O CXD cria tokens de carregamento exclusivos por SR. O número SR e o token são usados como nome de usuário e senha para autenticar o serviço e, subsequentemente, carregar arquivos para SR.

Nota: O token destina-se apenas para carregamento e não permitirá que o usuário acesse arquivos de casos de uso, ou até mesmo aos arquivos carregados no momento. Se o usuário quiser exibir os arquivos de chamado, isso pode ser feito apenas no SCM.

Recuperação do Token de carregamento para um SR

Uso do SCM

Quando um SÊNIOR é aberto, CXD gerará automaticamente um token da transferência de arquivo pela rede e introduzirá uma nota no SÊNIOR que contenha o token e alguns detalhes em como usar o serviço.

A fim recuperar o token da transferência de arquivo pela rede, termine estas etapas:

Etapa 1 Início de uma sessão ao SCM.

Etapa 2 Abra o caso que você gostaria de obter o token da transferência de arquivo pela rede para.

Etapa 3 Clique a aba dos **acessórios**.

Etapa 4 O clique **gerencie o token**. Uma vez que o token é gerado estará indicado ao lado do botão do token da geração.

Notas:

- O nome de usuário é sempre o número de SR. Os termos "senha" e "token" referem-se ao token de carregamento, que será usado como uma senha quando solicitado pelo CXD.

- A nota é anexada automaticamente em poucos minutos após a criação da SR. Se o usuário não puder encontrar a nota, ele poderá entrar em contato com o proprietário da SR e o token será gerado manualmente.
- Esse método está programado para mudança no futuro próximo. Certifique-se de acessar novamente essa documentação para obter as atualizações.

Uso da API ServiceGrid

Os clientes que utilizam a API ServiceGrid podem recuperar o token programaticamente usando a API GetUploadCredentials.

Nota: Um Token automático é necessário para chamar qualquer API Cisco ServiceGrid. Para obter detalhes sobre como obter um Token automático, consulte a documentação do Cisco ServiceGrid.

Método de HTTP: POST

URL: https://apx.cisco.com/custcare/tachwy/v1.0/credentials/case/<SR Number>

Cabeçalho:

Tabela 3: Cabeçalho da API ServiceGrid GetUploadCredentials

Chave	Tipo	Valor	Obrigatório
Tipo de conteúdo	Série	aplicativo/json	Yes
Autorização	Série	Portador <Auth Token>	Yes

Corpo:

Tabela 4: Corpo da API ServiceGrid GetUploadCredentials

Chave	Tipo	Valor	Obrigatório
nome do usuário	Série	Nome de usuário de Cisco.com autorizado a realizar um carregamento de arquivo para a SR	Yes
e-mail	Cadeia de caracteres (formato de e-mail)	Endereço de e-mail do nome de usuário cisco.com	Yes

Carregamento de arquivos para CXD

Utilização de clientes desktop

Em geral, tudo que o usuário precisa fazer é usar um cliente, dependendo do protocolo desejado, conectar-se ao cxd.cisco.com, autenticar usando o número de SR como nome de usuário e o token de carregamento como senha e, por fim, carregar um ou mais arquivos.

Dependendo do protocolo e do cliente, as etapas para o usuário podem ser diferentes. Sempre é recomendável consultar a documentação do cliente para obter mais detalhes.

Diretamente de um dispositivo da Cisco

Todos os dispositivos Cisco têm clientes de transferência de arquivos internos, geralmente utilizados usando um comando "redirecionar" ou "copiar". Equipamento da Cisco em execução em uma distribuição de Linux geralmente é compatível com um ou mais "scp", "sftp" e "curl" para integrações SCP, SFTP e HTTPS.

API de carregamento de arquivos

A API de carregamento de arquivo utiliza o verbo HTTP PUT para carregar arquivos CXD. Com a finalidade de compatibilidade máxima e simplicidade de integração, a API é mantida simples.

Método de HTTP: PUT

URL: do nome do arquivo de HTTPS://cxd.Cisco.com/home/<destination >

Cabeçalhos:

Tabela 5: Cabeçalhos de API de carregamento de arquivo CXD

Chave	Tipo	Valor	Obrigatório
Autorização	Série	Cadeia de caracteres de autenticação HTTP básica	Yes

O corpo consiste nos próprios dados de arquivo. Não existem campos ou formulários, tornando a solicitação muito simples.

Exemplo de código Python para usar a API PUT

Observe que o código a seguir assume que o arquivo está armazenado no mesmo caminho de execução.

```
import requests
from requests.auth import HTTPBasicAuth

url = 'https://cxd.cisco.com/home/'
username = 'SR Number'
password = 'Upload Token'
auth = HTTPBasicAuth(username, password)
filename = 'showtech.txt'
```

```
f = open(filename, 'rb')
r = requests.put(url + filename, f, auth=auth, verify=False)
r.close()
f.close()
if r.status_code == 201:
    print("File Uploaded Successfully")
```

Carregamentos de anexo de arquivo de e-mail

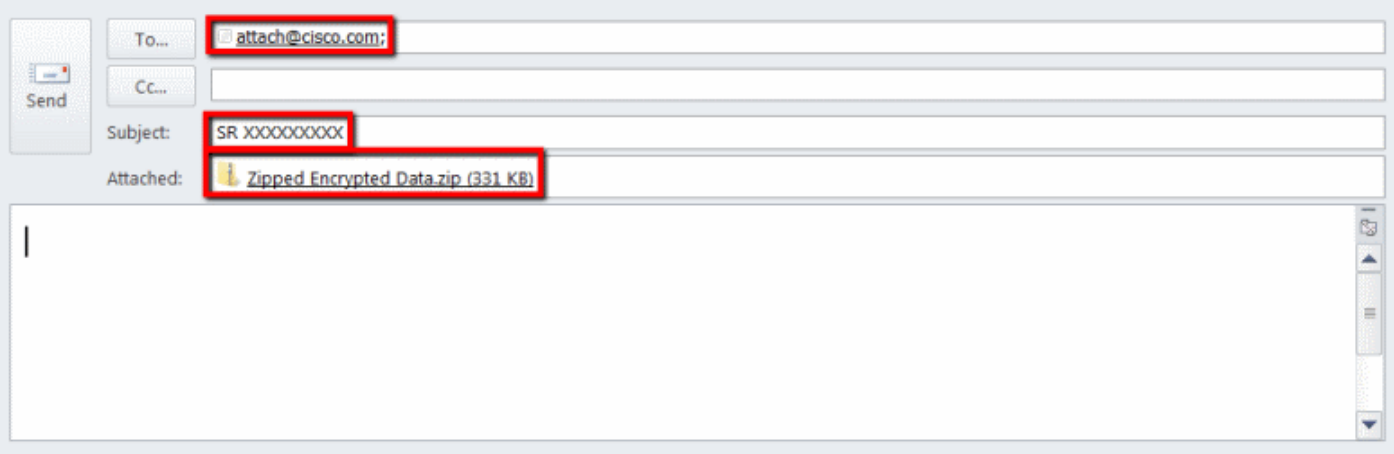
Se SCM, Carregador de arquivo de chamado e Customer eXperience Drive não funcionarem para você, outro método de carregamento de arquivo alternativo é o do anexo de arquivo de e-mail. Observe que esse método é *fundamentalmente inseguro* e não criptografa o arquivo ou a sessão de comunicação usada para transportar o arquivo entre o cliente e a Cisco. Cabe ao cliente explicitamente criptografar arquivos antes que sejam carregados em anexos de arquivo de e-mail. Como uma prática recomendada de segurança adicional, quaisquer informações confidenciais, como as senhas, devem ficar ocultas ou serem removidas de qualquer arquivo de configuração ou registro enviado por um canal não seguro. Para obter mais informações, consulte Criptografia de arquivos.

Depois que os arquivos são criptografados, carregue arquivos e informações adicionais ao chamado, enviando as informações através de uma mensagem de e-mail para attach@cisco.com com o número do caso na linha de assunto da mensagem, por exemplo, assunto = caso xxxxxxxxx.

Os anexos são limitados a 20 MB por atualização de e-mail. Anexos enviados usando mensagens de e-mail não são criptografados em trânsito, mas são imediatamente vinculados ao chamado especificado e armazenados em um formato criptografado.

Anexe o arquivo a uma mensagem de e-mail e envie-a para attach@cisco.com como mostrado na Figura 10.

Figura 9. envia o arquivo



O screenshot anterior mostra um email do Microsoft Outlook com um anexo de arquivo ZIP criptografado, o endereço Para correto e um Assunto formatado corretamente. Outros clientes de e-mail devem oferecer a mesma funcionalidade e eficiência do Microsoft Outlook.

Retornar ao início

Criptografia de arquivos

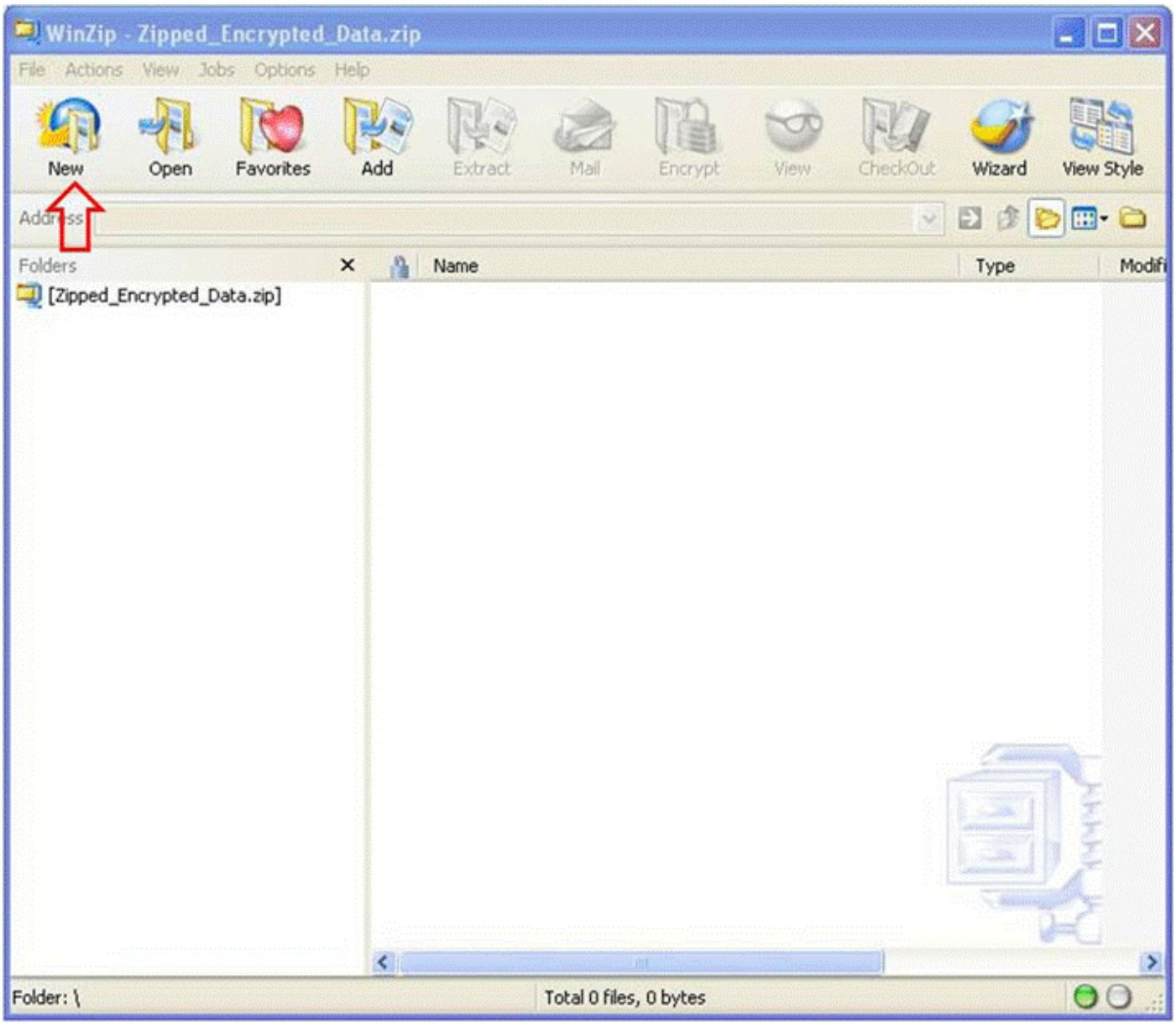
Os exemplos a seguir mostram como criptografar arquivos usando três das muitas opções disponíveis como WinZip, comandos tar e openssl do Linux e Linux Gzip e GnuPG. Uma cifra de criptografia forte como AES 128 deve ser usada para proteger os dados de maneira correta. Se você estiver usando ZIP, um aplicativo que oferece suporte à criptografia AES deve ser usado. Versões mais antigas ZIP aplicativos são compatíveis com um sistema de criptografia simétrica que não é seguro e não deve ser usado.

Criptografia de arquivos usando WinZip

Esta seção mostra como criptografar arquivos usando o aplicativo WinZip. Outros aplicativos devem oferecer a mesma funcionalidade e eficiência do WinZip.

Etapa 1 criar um arquivo ZIP, conforme mostrado na Figura 11. Na GUI do WinZip, clique em **Novo**e siga os prompts de menu para criar um novo arquivo ZIP corretamente nomeado. O novo arquivo ZIP recém-criado é exibido.

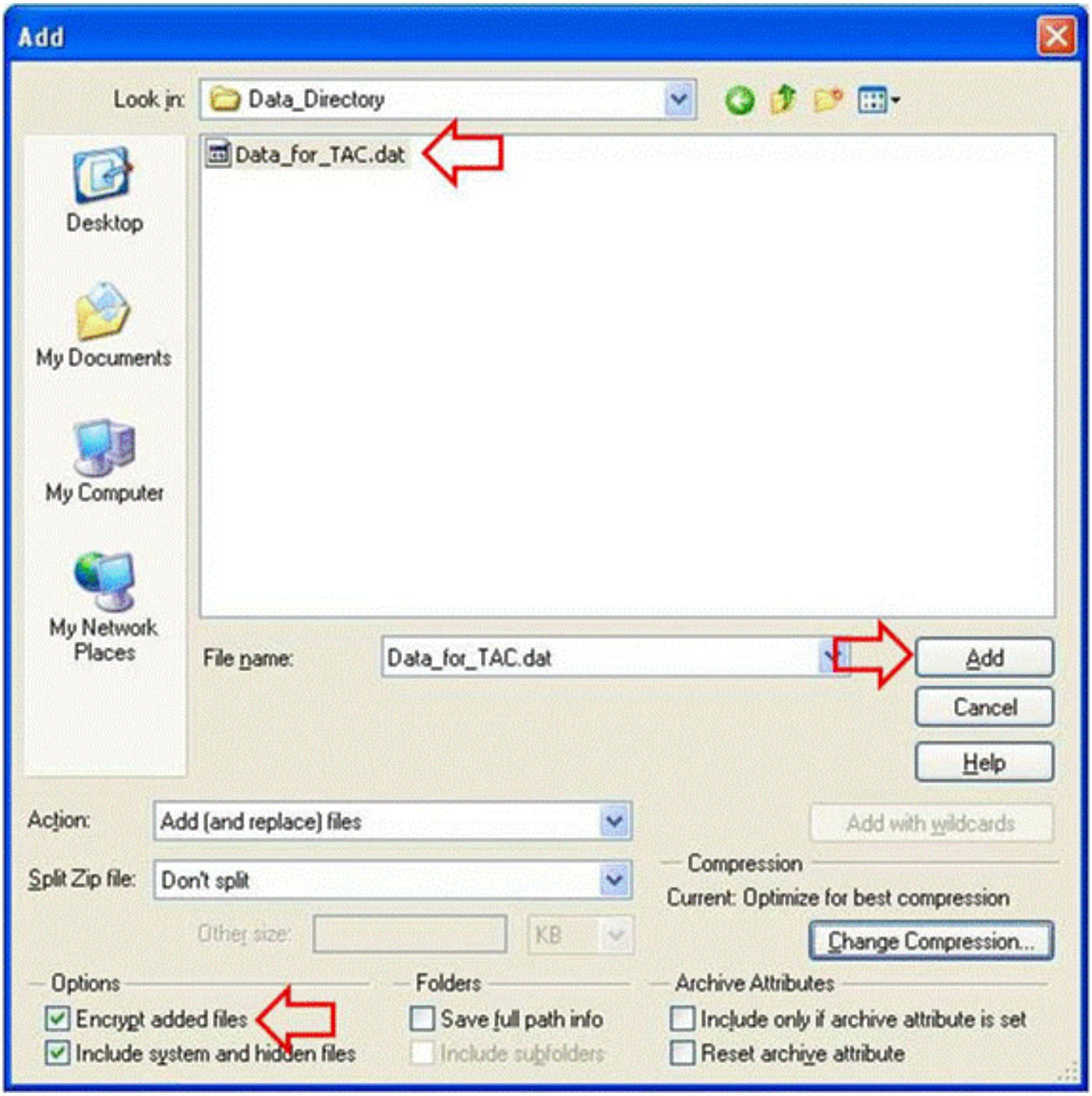
Figura 10. que cria um arquivo do FECHO DE CORRER



Etapa 2 Adicione os arquivos a serem carregados no arquivamento do ZIP e selecione a opção **Criptografar arquivos adicionados** como mostrado na Figura 12. Na janela principal do WinZip, clique em **Adicionar** e, em seguida, selecione os arquivos a serem carregados. A opção

Criptografar arquivos adicionados deve ser selecionada.

Figura 11. cifra arquivos adicionados



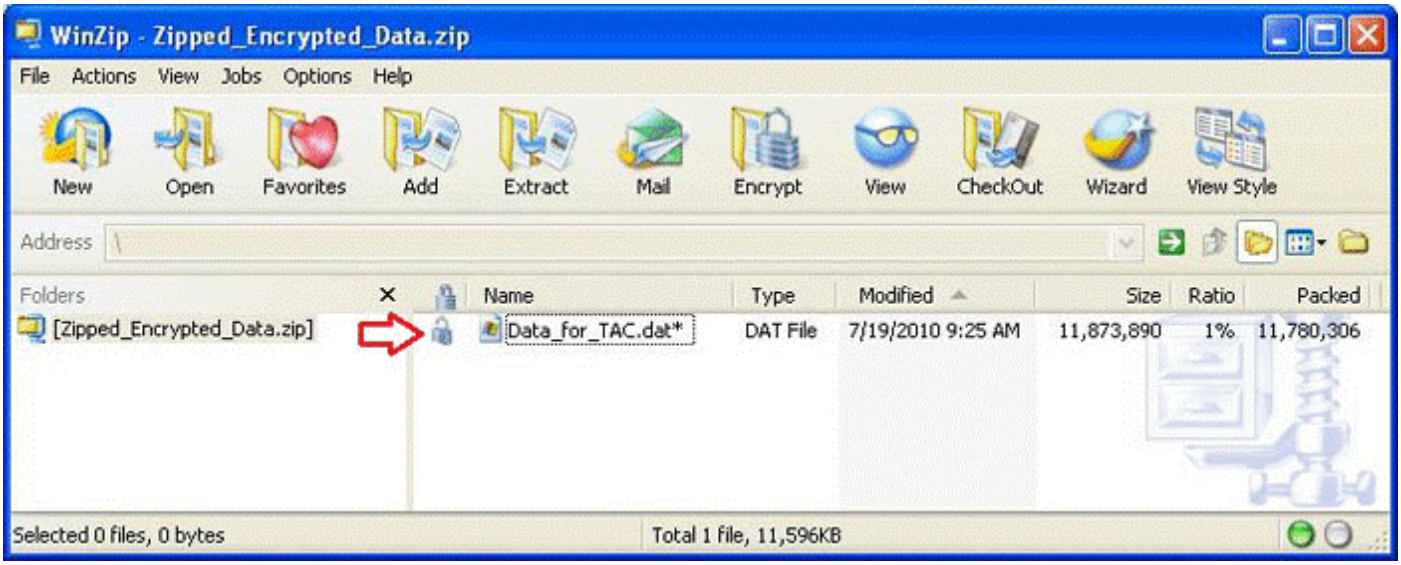
Etapa 3 Criptografe o arquivo usando a cifra de criptografia AES e uma senha forte, conforme mostrado na Figura 13:

1. Clique em **Adicionar** na janela de seleção do arquivo para abrir a janela **Criptografar**.
2. Na janela **Criptografar**, crie uma senha forte de maneira apropriada. A senha é compartilhada com o proprietário do chamado do engenheiro de suporte ao cliente, conforme discutido em Comunicação da senha para o engenheiro de suporte do cliente do TAC.
3. Escolha um dos métodos de criptografia AES.
4. Clique em **OK**para criptografar os arquivos e exibir a janela principal do WinZip.

Figura 12. Criptografar o arquivo

Etapa 4 verifique se o arquivo está criptografado como mostrado na Figura 14. Os arquivos criptografados são marcados com um asterisco após o nome ou um ícone de cadeado na coluna Criptografia.

Figura 13. Verificar a criptografia



Criptografia de arquivos usando Tar e OpenSSL

Esta seção mostra como criptografar arquivos, usando os comandos **tar** e **openssl** da linha de comando do Linux. Outros comandos de arquivo e criptografia devem oferecer a mesma funcionalidade e eficiência do Linux ou Unix.

Etapa 1 Crie um arquivamento tar do arquivo e criptografá-lo por meio do OpenSSL usando a cifra AES e uma senha forte, como mostrado no exemplo a seguir. A saída do comando mostra a sintaxe dos comandos openssl e tar combinada para criptografar o arquivo usando a cifra AES.

cvzf do alcatrão $ do [!ENTITY!] - Data_for_TAC.dat | OpenSSL aes-128-cbc - k
Str0ng_passWo5D |
    dd of=Data_for_TAC.aes128 Data_for_TAC.dat
registros de 60 + 1 em
60+1 records in

Criptografia de arquivos usando Gzip e GnuPG

Esta seção mostra como criptografar arquivos, usando os comandos de Gzip e o GnuPG de linha de comando do Linux. Outros comandos de arquivo e criptografia devem oferecer a mesma funcionalidade e eficiência do Linux ou Unix. A saída do comando mostra como usar a sintaxe do comando gzip e gpg para criptografar arquivos com a cifra AES.

Etapa 1 Compacte o arquivo usando Gzip:

gzip -9 Data_for_TAC.dat $ do [!ENTITY!]

Etapa 2 Criptografe o arquivo por GnuPG usando a cifra AES e uma senha forte:

```
user@linux ~]$ gpg –cipher-algo AES –armor –output Data_for_TAC.dat.gz.asc –symmetric
Data_for_TAC.dat.gz
```

Etapa 3 Digite e confirme a senha forte no prompt de senha:

Insira a senha:
Repita a senha:

Retornar ao início

Comunicação da senha para o engenheiro de suporte do cliente do TAC

Ao criptografar anexos, compartilhe a senha de criptografia com o proprietário do caso do engenheiro de suporte ao cliente. Como prática recomendada, use um método diferente que não seja o de carregar o arquivo. Se você usou uma mensagem de e-mail ou FTPS para carregar o arquivo, comunique a senha fora de banda, como por telefone ou atualização de caso do SCM.

Retenção do arquivo do cliente

Enquanto o processo estiver aberto e por um período de até 18 meses após o encerramento final de um chamado, todos os arquivos serão acessados instantaneamente de dentro do sistema de rastreamento de casos para o pessoal autorizado da Cisco. Após um período de 18 meses a partir do encerramento final, os arquivos podem ser movidos para uma instância de armazenamento de arquivamento com o objetivo de economizar espaço, mas eles não são eliminados (excluídos) do histórico do caso.

A qualquer momento, um contato do cliente autorizado pode solicitar expressamente que um arquivo específico seja descartado de um chamado. A Cisco pode, então, excluir esse arquivo e

adicionar uma anotação para documentar a parte que excluiu o arquivo, a data e a hora e o nome do arquivo excluído. Depois que um arquivo é descartado desta forma, ele não pode ser recuperado.

Arquivos carregados para a pasta TAC FTP são mantidos por quatro dias. O proprietário do caso do engenheiro de suporte ao cliente precisa ser informado quando um arquivo é carregado nesta pasta. O engenheiro de suporte ao cliente deve fazer backup dos arquivos em até quatro dias, anexando-os ao chamado.

Retornar ao início

Resumo

Há várias opções para o carregamento de informações para o Cisco TAC, com o objetivo de ajudar a resolver casos de uso. O SCM e a ferramenta de carregamento HTML5 da Cisco oferecem envios seguros por meio de um navegador, enquanto o CXD oferece envios por meio de um navegador, API da Web e vários protocolos compatíveis com diferentes tipos de clientes e dispositivos Cisco.

Se você não puder usar o SCM, a ferramenta de carregamento de arquivos Cisco HTML 5 ou um protocolo suportado pelo CXD que não seja FTP como método de carregamento de arquivo, as opções de carregamento menos preferidas são FTP, CXD ou uma mensagem de e-mail enviada para attach@cisco.com. Se você usar qualquer uma dessas opções, é altamente recomendável que criptografe os arquivos antes do trânsito. Para obter mais informações, consulte Criptografia de arquivos. Você deve utilizar uma senha forte e comunicar a senha ao engenheiro de suporte ao cliente fora de banda, como por telefone ou atualização de caso do SCM.

Enquanto o processo estiver aberto e por um período de até 18 meses após o encerramento final de um chamado, todos os arquivos serão acessados instantaneamente de dentro do sistema de rastreamento de casos para o pessoal autorizado da Cisco.

- Após meses 18 os arquivos podem ser movidos para o arquivamento.
- A qualquer momento, um contato do cliente autorizado pode solicitar expressamente que um arquivo específico seja descartado de um chamado.
- Os arquivos na pasta de FTP são mantidos por apenas quatro dias.

Additional Information

- Acesso aos Serviços técnicos da Cisco
- Contatos mundiais de suporte da Cisco
- Guia de recursos de Serviços técnicos da Cisco
- Blog de segurança da Cisco - Dica NCSAM 3: O que você deve considerar como senha segura
- Produtos Cisco para conferências
- O GNU Privacy Guard
- O OpenSSL Project
- WinZip

Este documento é parte de Cisco Security Research & Operations.

documento ou materiais vinculados com base no documento é de sua responsabilidade. A Cisco reserva-se o direito de alterar ou atualizar este documento a qualquer momento.

Retornar ao início