Carregamentos de arquivo do cliente no Cisco Technical Assistance Center

Contents

Introdução

Este documento descreve como fazer o upload de arquivos para o Cisco Technical Assistance Center (TAC).

Overview

Os engenheiros de suporte ao cliente do TAC podem ajudá-lo a resolver um problema em tempo hábil quando tiverem arquivos relevantes anexados ao problema. Você tem várias opções para carregar os arquivos relacionados ao seu problema. Algumas dessas opções são menos seguras e podem levar a certos riscos inerentes, e cada opção tem limitações que você precisa considerar antes de decidir sobre uma opção de upload 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 upload disponíveis

Opção disponível (em ordem de preferência)		Arquivos criptografados em trânsito	Arquivos criptografados em repouso	Limite de tamanho de arquivo recomendado
Support Case Manager (SCM)	Como fazer	Yes	Yes	Nenhum limite
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, é altamente recomendável que os dados sejam criptografados antes de serem carregados.

**Você deve criptografar antes do trânsito. O trânsito seguro é garantido somente a partir do ponto onde o e-mail/anexo alcança a rede da Cisco, e não a partir da rede do cliente ou do provedor de e-mail.

Carregamento de arquivo no Support Case Manager

O método de carregamento de arquivos do Support Case Manager (SCM) é uma opção segura para carregar arquivos em casos. O canal de comunicação entre seu 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.

Carregando um arquivo em um caso

Depois de enviar o caso, você pode fazer o upload dos arquivos.

Etapa 1. Faça login no SCM.

Etapa 2. Para visualizar e editar o caso, clique no número ou no título do caso na lista. A página Case Summary (Resumo do caso) é aberta.

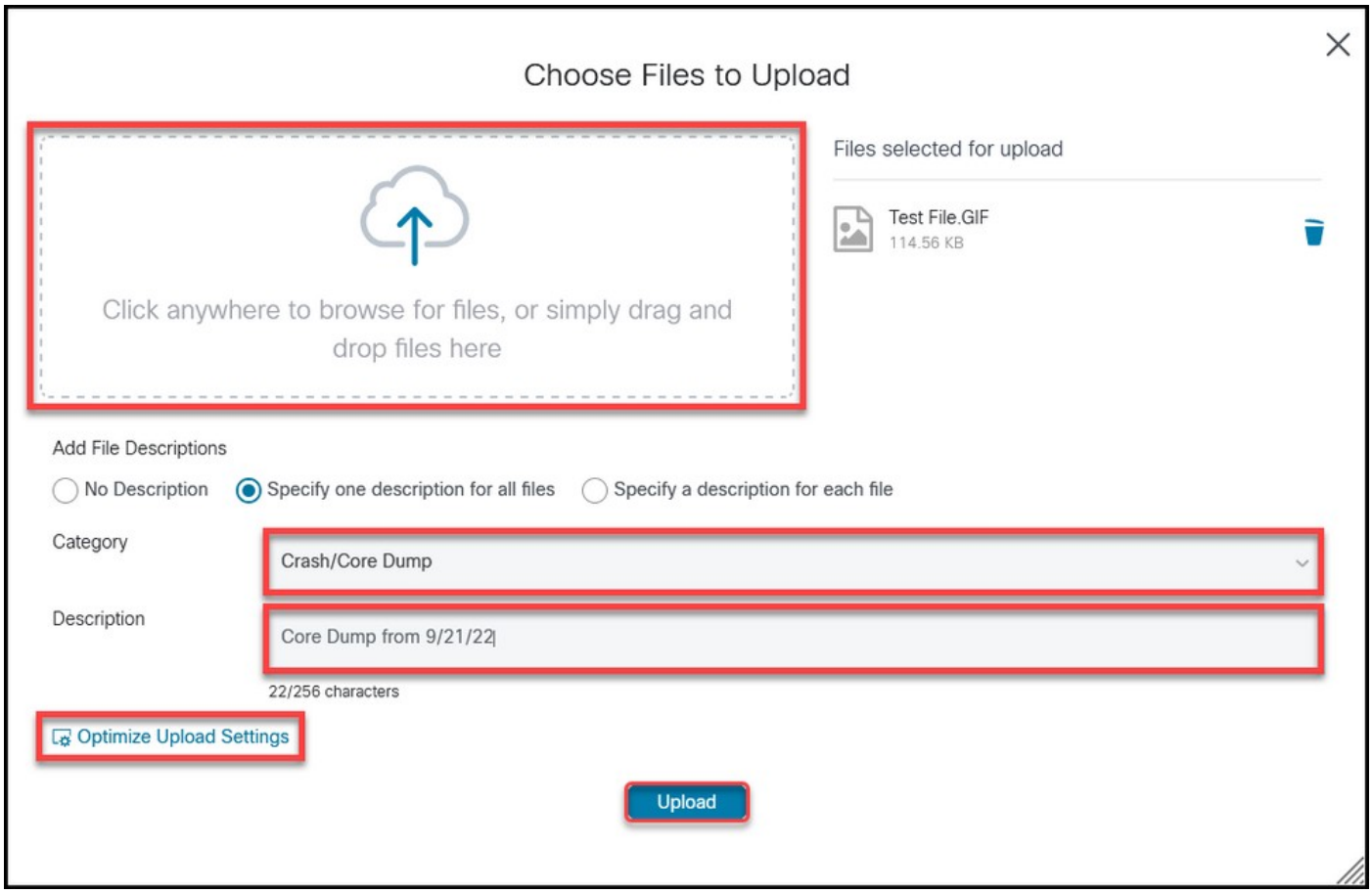
Etapa 3. Clique em **Add Files** para escolher um arquivo e carregá-lo como um anexo ao caso. O sistema exibe a ferramenta Carregador de arquivo SCM.

Etapa 4. No **Choose Files to Upload** arraste os arquivos que você deseja carregar ou clique em inside para procurar arquivos a serem carregados na máquina local.

Etapa 5. Adicione uma descrição e especifique uma categoria para todos os arquivos ou individualmente.

Nota: Para otimizar as configurações de carregamento para sua condição de rede, clique em **Optimize Upload Settings.**

Etapa 6. Clique em **Upload** para iniciar o processo de carregamento.



Passo 7. Quando todos os carregamentos estiverem concluídos, você poderá fechar a janela ou clicar em **Add More Files** para carregar mais arquivos.

Etapa 8. Os arquivos carregados podem ser gerenciados no **Attachments** guia.

Return to top

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 ajuda os clientes da Cisco com solicitações de serviço (SRs) ativas a carregar dados diretamente em um caso 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	TCP/22	Yes	N/A	

(SCP)				
Hyper Text Transfer Protocol over SSL (HTTPS)	TCP/443	Yes	N/A	Há suporte apenas para carregamentos baseados em API.
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	Yes	30000-40000	
File Transfer Protocol (FTP)	TCP/21	Yes	30000-40000	A Cisco não recomenda o uso de FTP, pois o protocolo não suporta criptografia. Se precisar ser usado, os dados precisam 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.

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 é somente para upload e não permite que o usuário acesse arquivos de caso, ou até mesmo arquivos sendo 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 uma SR é aberta, os usuários devem criar o token de carregamento para carregar o anexo.

Para recuperar/gerar o token de carregamento, siga estas etapas:

Etapa 1. Faça login no SCM.

Etapa 2. Para visualizar e editar um caso, clique no número ou no título do caso na lista. A página Case Summary (Resumo do caso) é aberta.

Etapa 3. Clique no botão **Attachments** guia.

Etapa 4. Clique em **Generate Token**. Depois que o token for gerado, ele será exibido ao lado do botão Gerar token.

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

Uso da API

Os clientes que utilizam a API podem recuperar o token programaticamente usando o comando **Get Token** API

Observação: um token de autenticação Okta é necessário para chamar a API de obtenção de token da Cisco. Para obter detalhes sobre como obter um Token automático, consulte a documentação do Cisco ServiceGrid.

Método HTTP: POST

URL: https://cxd-token.cxapps.cisco.com/cxd/token/<SR_Number>

Cabeçalho:

Tabela 3. Obter cabeçalho de API de token

Chave	Tipo	Valor
Tipo de conteúdo	Série	aplicativo/json

Autorização	Série	Portador <Auth Token>

Corpo:

Tabela 4. Corpo da API ServiceGrid GetUploadCredentials

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

Carregamento de arquivo para CXD

Uso de Clientes Desktop

Em geral, tudo o que o usuário precisa fazer é usar um cliente, dependendo do protocolo, para se conectar a cxd.cisco.com, autenticar usando o número SR como o nome de usuário e o token de carregamento como a senha e, por fim, carregar um arquivo. Dependendo do protocolo e do cliente, as etapas do usuário podem ser diferentes. É sempre recomendável consultar a documentação do cliente para obter mais detalhes.

Diretamente de um dispositivo da Cisco

Todos os dispositivos da Cisco têm clientes de transferência de arquivos integrados, normalmente utilizados com um **copy** or **redirect** comando. Os equipamentos da Cisco executados em uma distribuição Linux geralmente suportam 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. Para máxima compatibilidade e simplicidade de integração, a API é mantida simples.

Método HTTP: PUT

URL: https://cxd.cisco.com/home/<nome do arquivo de destino>

Cabeçalhos:

Tabela 5. Cabeçalhos de API de carregamento de arquivo CXD

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

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 supõe que o arquivo está armazenado no mesmo caminho a partir do qual ele está sendo executado.

```
import requests
from requests.auth import HTTPBasicAuth

username = 'SR Number'
password = 'Upload Token'
auth = HTTPBasicAuth(username, password)

filename = 'showtech.txt'  # Destination filename
url = f'https://cxd.cisco.com/home/{filename}'

headers = {"Expect": "100-continue"}

file_path = 'Local Path to the File'

with open(file_path, 'rb') as f:
    r = requests.put(url + filename, f, auth=auth, headers=headers)
    if r.status_code == 201:
        print("File Uploaded Successfully")
```

Return to top

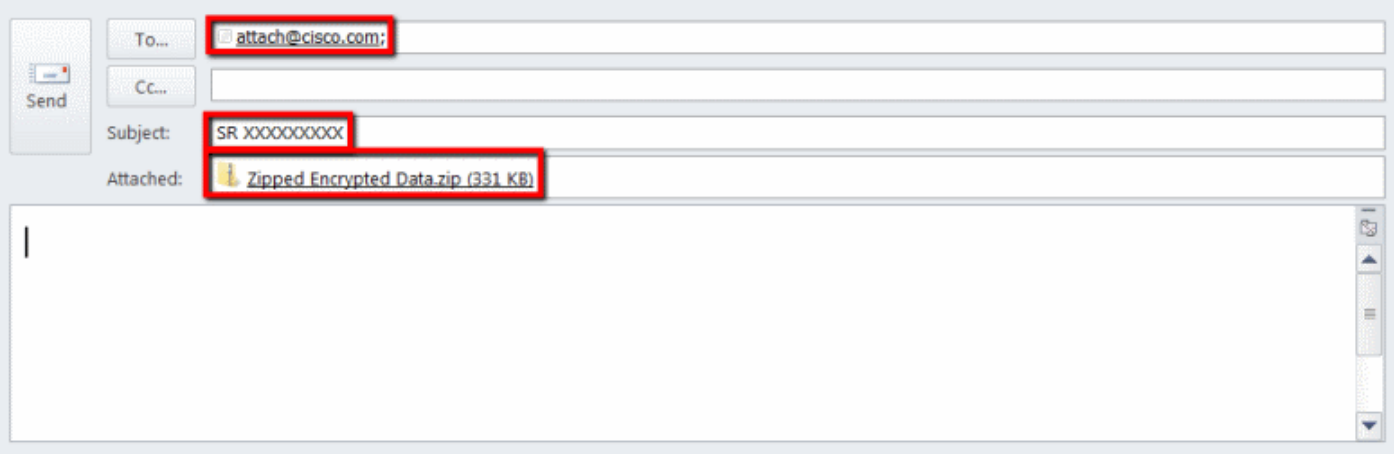
Carregamentos de anexo de arquivo de e-mail

Se o SCM e o CXD não funcionarem para você, outro método alternativo de carregamento de arquivo é o carregamento de 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, qualquer informação confidencial, como senhas, precisa ser obscurecida ou removida 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 mensagem para attach@cisco.com como mostrado nesta captura de tela.



A captura de tela anterior exibe um e-mail do Microsoft Outlook que tem um anexo de arquivo ZIP criptografado, o endereço Para correto e um Assunto formatado corretamente. Outros clientes de e-mail precisam fornecer a mesma funcionalidade e funcionar tão bem quanto o Microsoft Outlook.

Return to top

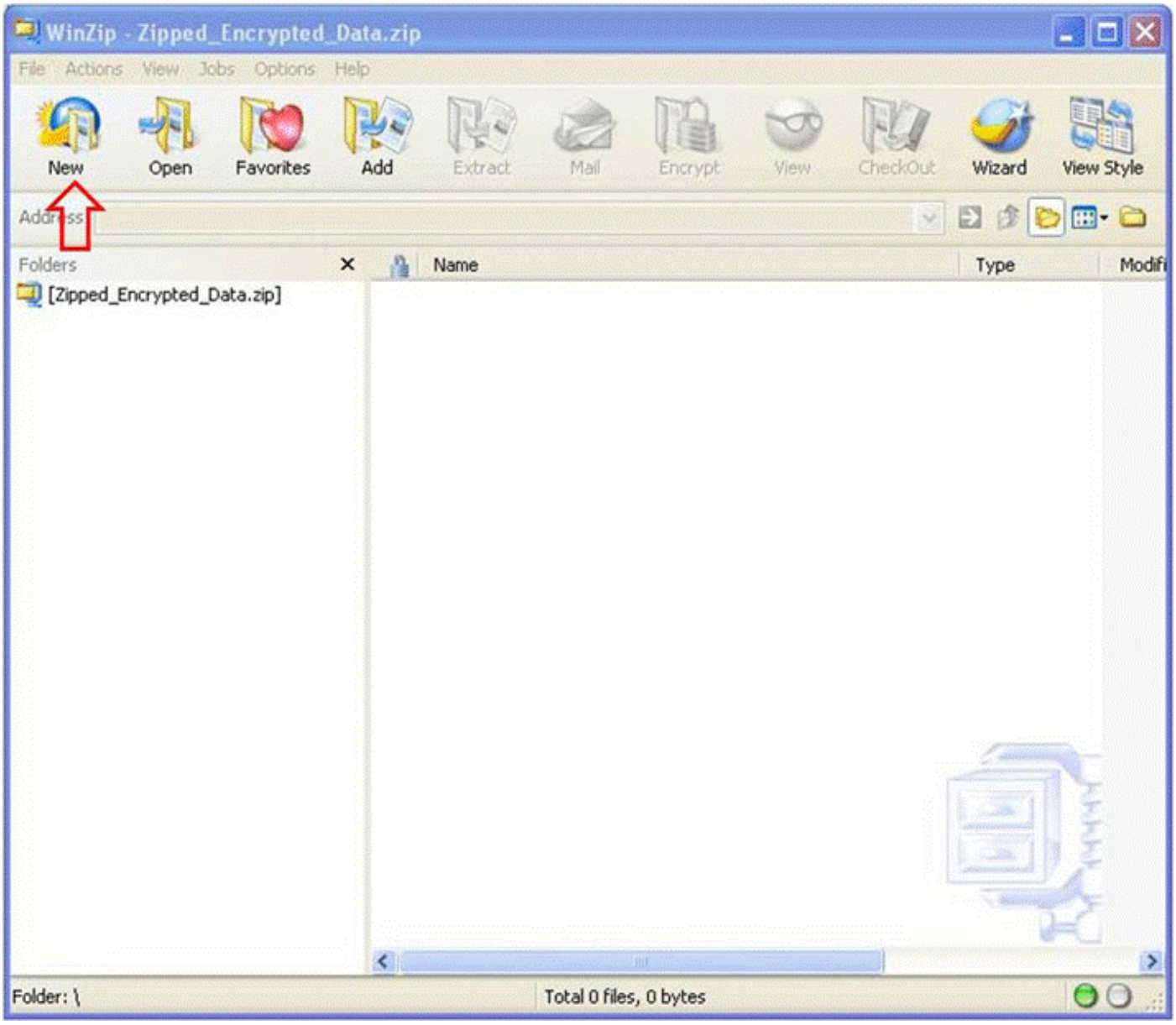
Criptografia de arquivos

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, precisa ser usada para proteger adequadamente os dados. Se você estiver usando ZIP, um aplicativo que oferece suporte à criptografia AES deve ser usado. Versões mais antigas de aplicativos ZIP suportam um sistema de criptografia simétrico que não é seguro e não deve ser usado.

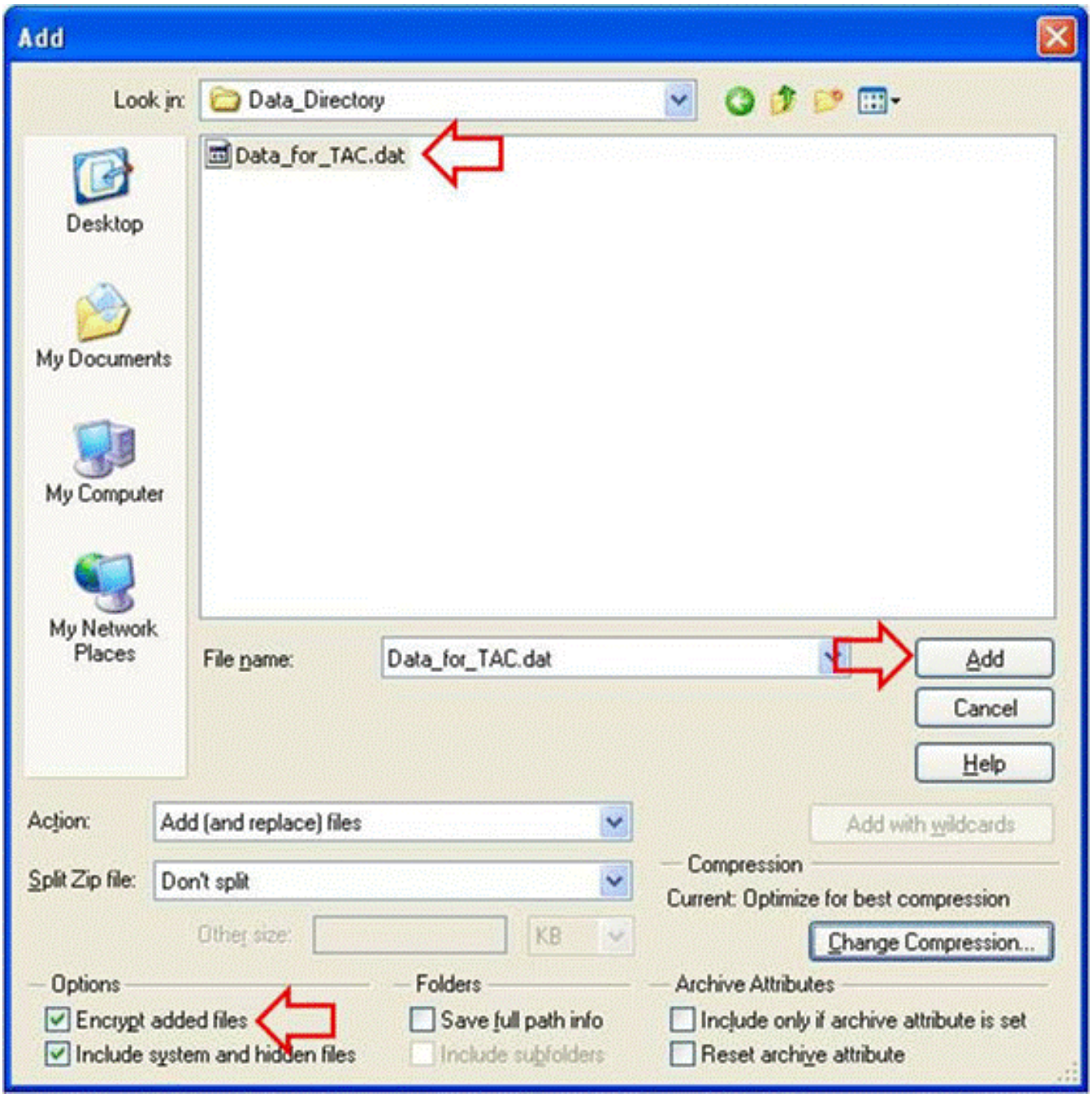
Criptografia de arquivos usando WinZip

Esta seção demonstra como criptografar arquivos usando o aplicativo WinZip. Outros aplicativos fornecem a mesma funcionalidade e desempenho, bem como WinZip.

Etapa 1. Crie um arquivo ZIP. Na GUI do WinZip, clique em **New** e siga os prompts do menu para criar um novo arquivo ZIP adequadamente nomeado. O sistema exibe o arquivo ZIP recém-criado.



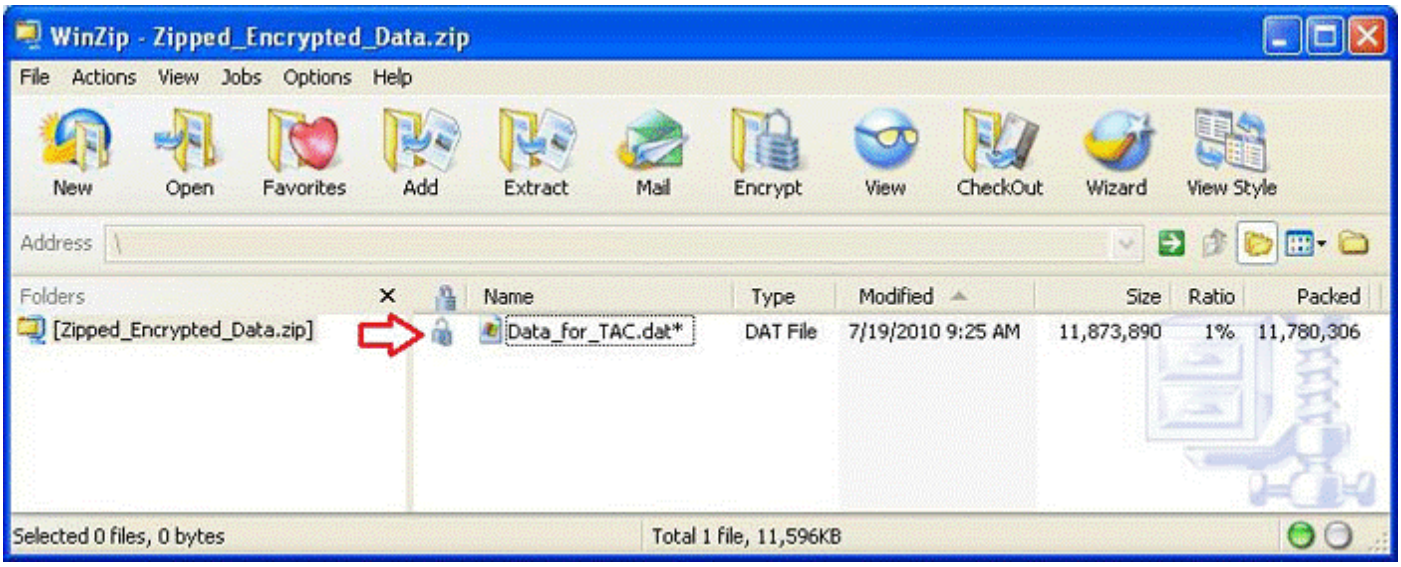
Etapa 2. Adicione o(s) arquivo(s) a ser(em) carregado(s) no arquivo ZIP e marque a caixa de seleção **Encrypt added files** caixa de seleção. Na janela principal do WinZip, clique em **Add** e escolha o(s) arquivo(s) para upload. O **Encrypt added files** deve ser marcada.



Etapa 3. Criptografe o arquivo usando a cifra de criptografia AES e uma senha forte:

1. Clique em **Add** na janela de seleção de arquivos para abrir o **Encrypt** janela.
2. No **Encrypt** crie uma senha forte adequadamente. 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.

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



Criptografia de arquivos usando Tar e OpenSSL

Esta seção mostra como criptografar arquivos usando a linha de comando do Linux **tar** e **openssl** comandos. Outros comandos de arquivamento e criptografia fornecem a mesma funcionalidade e apresentam o mesmo desempenho no Linux ou no Unix.

Etapa 1. Crie um arquivo tar do arquivo e criptografe-o através do OpenSSL usando a cifra AES e uma senha forte, como demonstrado no exemplo a seguir. A saída do comando mostra a combinação **tar** e **openssl** sintaxe de comando para criptografar os arquivos usando a cifra AES.

```
[user@linux ~] $ tar cvzf - 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 o Gnupgp

Esta seção demonstra como criptografar arquivos usando os comandos Gzip e GnuPG da linha de comando do Linux. Outros comandos de arquivamento e criptografia fornecem a mesma funcionalidade e apresentam o mesmo desempenho no Linux ou no 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 o Gzip:

```
[user@linux ~] $ tar cvzf - Data_for_TAC.dat
```

Etapa 2. Criptografe o arquivo através do 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.
```

Etapa 3. Insira e confirme a senha forte no prompt da senha:

Insira a senha:
Repita a senha:

Return to top

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.

Return to top

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 fechamento final, os arquivos podem ser movidos para uma instância de armazenamento de arquivamento para conservar espaço, mas não são removidos (excluídos) do histórico de casos.

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 precisa fazer backup dos arquivos em quatro dias, anexando-os ao caso.

Return to top

Summary

Existem várias opções para o upload de informações para o TAC para ajudá-los a resolver casos. 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 precisa empregar uma senha forte e comunicá-la ao engenheiro de suporte ao cliente do caso fora de banda, como por telefone ou por 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 18 meses, os arquivos podem ser movidos para o armazenamento de 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.

Return to top

Informações adicionais

- Acesso aos Serviços técnicos da Cisco
- Contatos mundiais de suporte da Cisco
- Guia de recursos de Serviços técnicos da Cisco
- Produtos Cisco para conferências
- O GNU Privacy Guard
- O OpenSSL Project

- WinZip

Este documento é parte de Cisco Security Research & Operations.

Return to top

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.