# Caricamento di file die clienti su Cisco Technical Assistance Center

## Sommario



## Introduzione

Questo documento illustra come caricare i file in Cisco Technical Assistance Center (TAC).

## Panoramica

I tecnici di assistenza TAC possono assistere l'utente nella risoluzione tempestiva di un problema,

nel caso in cui siano stati allegati file pertinenti. Sono disponibili diverse opzioni per caricare i file relativi al problema. Alcune di queste opzioni sono meno sicure e possono causare rischi intrinseci. Ciascuna opzione presenta delle limitazioni che è necessario valutare prima scegliere la modalità di caricamento appropriata. La tabella 1 riepiloga le opzioni di caricamento disponibili e i dettagli relativi alla crittografia dei file, le dimensioni massime consigliate per i file e altre informazioni importanti.

Tabella 1. Opzioni di caricamento disponibili

| Opzione disponibile (in ordine di preferenza) | | I file vengono crittografati in transito | I file vengono crittografati inattivi | Dimensioni file consigliate |
|---|---|---|---|---|
| Supporto Case Manager (SCM) | Istruzioni | Sì | Sì | Nessun limite |
| Customer eXperience Drive | Istruzioni | Sì* | Sì | Nessun limite |
| Scrivere a attach@cisco.com | Istruzioni | No** | Sì | 20 MB o meno in base ai limiti del server di posta del cliente |

*Si applica a tutti i protocolli tranne FTP. Se si utilizza un FTP, si consiglia di crittografare i dati prima di caricarli.

**È necessario eseguire la crittografia prima della trasmissione. La trasmissione sicura è garantita solo dal punto in cui l'e-mail/l'allegato raggiunge la rete Cisco, non dal lato del cliente o del provider di e-mail.

# Caricamento di file in Support Case Manager

Il caricamento di file in Support Case Manager (SCM) è un metodo sicuro per allegare i file alle richieste. Il canale di comunicazione tra dispositivo di elaborazione e Cisco è crittografato. I file caricati tramite SCM vengono collegati immediatamente alla richiesta associata e archiviati in formato crittografato.

## Caricamento di file in richiesta

Dopo aver inviato la richiesta, è possibile caricare i file.

Passaggio 1. Accedere a SCM.

Passaggio 2. Per visualizzare e modificare la richiesta, fare clic sul numero o sul titolo nell'elenco. Si apre la pagina Riepilogo della richiesta.

Passaggio 3. Fare clic su **Add Files** per scegliere un file e caricarlo come allegato alla richiesta. Viene visualizzato lo strumento SCM File Uploader.


Passaggio 4. Nella scheda **Choose Files to Upload** trascinare i file che si desidera caricare oppure fare clic all'interno di per cercare i file da caricare nel computer locale.

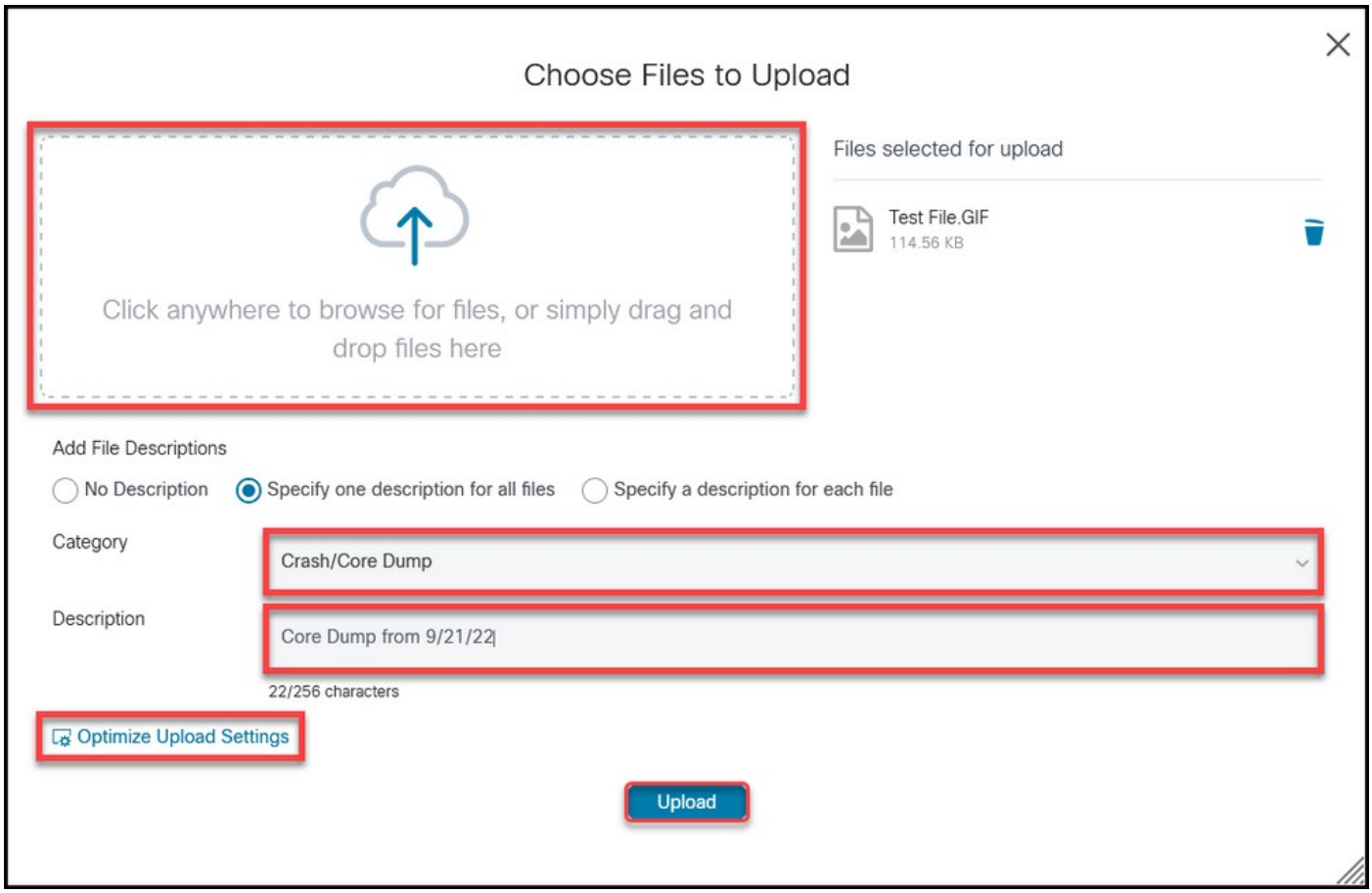
Passaggio 5. Aggiungere una descrizione e specificare una categoria per tutti i file o singolarmente.

---

Nota: per ottimizzare le impostazioni di caricamento per le condizioni della rete, fare clic su **Optimize Upload Settings.**

---

Passaggio 6. Fare clic su **Upload** per avviare il processo di caricamento.




Passaggio 7. Una volta completati tutti i caricamenti, è possibile chiudere la finestra o fare clic su **Add More Files** per caricare altri file.


Passaggio 8. I file caricati possono essere gestiti in **Attachments** scheda.


Torna su

# Customer eXperience Drive

## Riepilogo del servizio

Customer eXperience Drive (CXD) è un servizio di caricamento file multiprotocollo senza limiti di dimensioni. Aiuta i clienti Cisco con richieste di supporto (SR) attive a caricare i dati direttamente in una richiesta, utilizzando credenziali univoche per ciascuna SR. I protocolli supportati da CXD sono supportati da Cisco in modo nativo, il che consente il caricamento diretto da dispositivi Cisco alle SR.

## Protocolli supportati

La tabella 2 include i protocolli supportati da CXD. Si noti che, a prescindere dal protocollo utilizzato, non vi sono limiti alle dimensioni dei file.

Tabella 2. Protocolli supportati da CXD

| Nome | Protocollo/porta | Crittografia | Porte del canale dati | Note |
|---|---|---|---|---|
| SFTP (Secure File Transfer Protocol) | TCP/22 | Sì | N/D | |
| SCP (Secure Copy Protocol) | TCP/22 | Sì | N/D | |
| HTTPS (Hyper Text | TCP/443 | Sì | N/D | Sono supportati solo i caricamenti basati su API. |

| | | | | |
|---|---|---|---|---|
| Transfer Protocol over SSL) | | | | |
| FTPS (File Transfer Protocol of SSL) Implicit | TCP/990 | Sì | 30000-40000 | I firewall non possono ispezionare i FTPS, poiché il canale di controllo è crittografato. Pertanto, il firewall deve consentire la connettività in uscita nell'intero intervallo di porte del canale dati. |
| FTPS (File Transfer Protocol of SSL) Explicit | TCP/21 | Sì | 30000-40000 | |
| FTP (File Transfer Protocol) | TCP/21 | Sì | 30000-40000 | Cisco sconsiglia di utilizzare l'FTP, poiché il protocollo non supporta la crittografia. Qualora fosse necessario, i dati dovranno essere crittografati prima del trasferimento.<br><br>I firewall devono ispezionare il traffico FTP per consentire la corretta connessione dei canali dati. Se l'FTP non viene ispezionato in tutta la rete, i firewall devono consentire la connettività in uscita nell'intero intervallo di porte del canale dati. |

## Token di caricamento CXD

CXD crea token di caricamento univoci per SR. Il numero SR e il token vengono utilizzati come nome utente e password per autenticarsi al servizio e successivamente caricare i file nella SR.

Nota: il token è solo per il caricamento e non consente di accedere ai file della richiesta né ai file che vengono caricati. I file della richiesta, possono essere visualizzati solo in SCM.

## Recupero del token di caricamento per SR

Uso di SCM

Quando si apre una SR, gli utenti devono creare il token di caricamento per caricare l'allegato.

Per recuperare/generare il token di caricamento, procedere come segue:

Passaggio 1. Accedere a SCM.

Passaggio 2. Per visualizzare e modificare una richiesta, fare clic sul numero o sul titolo nell'elenco. Si apre la pagina Riepilogo della richiesta.

Passaggio 3. Fare clic sul pulsante **Attachments** scheda.

Passaggio 4. Fare clic su **Generate Token**. Una volta generato il token, viene visualizzato accanto al pulsante Generate Token.

---

Nota: il nome utente è sempre il numero SR. I termini password e token si riferiscono al token di caricamento, che viene utilizzato come password quando richiesto da CXD.

---

Uso dell'API

I clienti che utilizzano l'API possono recuperare il token a livello di codice utilizzando **Get Token** API.

---

Nota: è necessario un token Okta Auth per chiamare l'API Cisco Get Token. Per i dettagli su come ottenere un token Auth, consultare la documentazione di Cisco ServiceGrid.

---

Metodo HTTP: POST

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

Intestazione:

Tabella 3. Ottieni intestazione API token

| Chiave | Tipo | Valore |
|---|---|---|
| Content-Type | Stringa | application/json |
| Authorization | Stringa | Bearer <Auth Token> |

Corpo:

Tabella 4. Corpo API ServiceGrid GetUploadCredentials

| Chiave | Tipo | Valore |
|---|---|---|
| username | Stringa | Nome utente Cisco.com autorizzato a eseguire il caricamento di un file nella SR |
| email | Stringa (formato e- | Indirizzo email del nome utente cisco.com |

| | | |
|---|---|---|
| | mail) | |

## Caricamento di file in CXD

### Uso di client desktop

In generale, è sufficiente utilizzare un client, a seconda del protocollo, per collegarsi a cxd.cisco.com, eseguire l'autenticazione con il numero SR come nome utente e il token di caricamento come password, infine caricare un file. A seconda del protocollo e del client, la procedura può differire. Si consiglia sempre di consultare la documentazione del client per ulteriori dettagli.

### Direttamente da un dispositivo Cisco

Tutti i dispositivi Cisco dispongono di client di trasferimento file integrati, generalmente utilizzati con un **copy** o **redirect** Le apparecchiature Cisco in esecuzione su una distribuzione Linux supportano solitamente uno o più SCP, SFTP e CURL per le integrazioni SCP, SFTP e HTTPS.

### API di caricamento file

L'API di caricamento dei file utilizza la clausola HTTP PUT per caricare i file in CXD. Per assicurare compatibilità e semplicità di integrazione, l'API è estremamente semplice.

Metodo HTTP: PUT

URL: https://cxd.cisco.com/home/<nome file di destinazione>

Intestazioni:

Tabella 5. Intestazioni API di caricamento file CXD

| Chiave | Tipo | Valore |
|---|---|---|
| Authorization | Stringa | Stringa di autenticazione HTTP di base |

Il corpo corrisponde ai dati del file stesso. Non sono presenti campi o moduli, il che rende la richiesta molto semplice.

### Codice Python di esempio per utilizzare l'API PUT

Il codice presuppone che il file sia archiviato nel percorso di esecuzione.

```
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")
```

Torna su

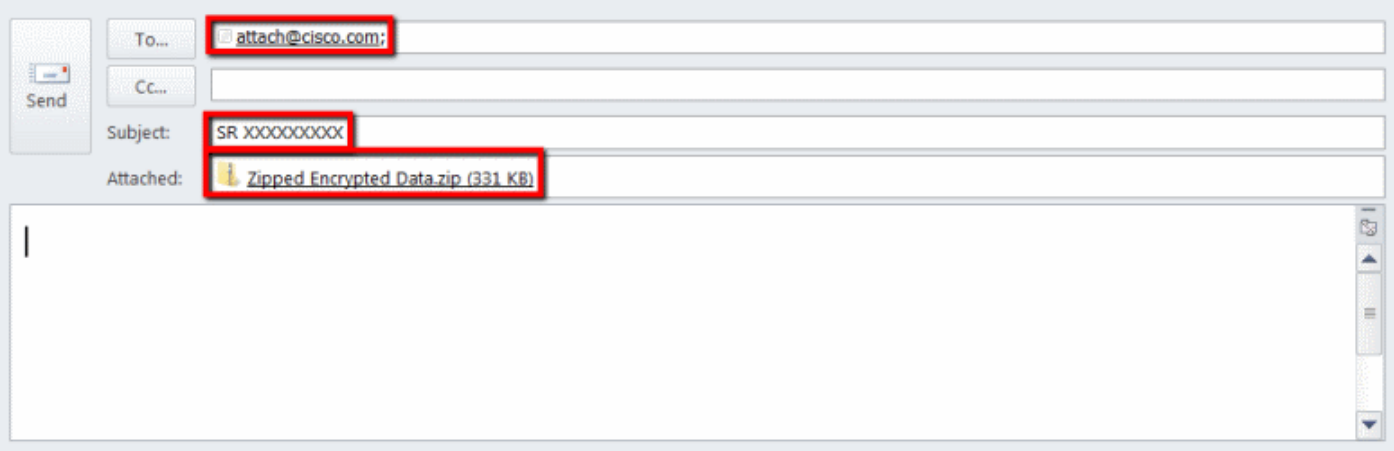
## Caricamento di allegati e-mail

Se SCM e CXD non sono idonei per l'utente, un metodo alternativo per caricare i file è tramite allegati e-mail. Tale metodo è tuttavia fondamentalmente non sicuro e non prevede la crittografia del file o della sessione di comunicazione utilizzata per il trasferimento dal cliente a Cisco. È responsabilità del cliente, eseguire la crittografia dei file prima di caricarli tramite allegati e-mail. Come ulteriore buona norma per la sicurezza, eventuali dati sensibili, come le password, devono essere celati o rimossi dai file di configurazione o di registro inviati tramite un canale non protetto. Per ulteriori informazioni, vedere Crittografia dei file.

Dopo aver crittografato i file, caricarli insieme a eventuali informazioni aggiuntive nella richiesta inviandoli tramite email a attach@cisco.com con il numero della richiesta in oggetto, ad esempio oggetto = Richiesta xxxxxxxxx.

Gli allegati sono limitati a 20 MB per e-mail di aggiornamento. Gli allegati inviati tramite e-mail non vengono crittografati in transito, ma vengono immediatamente collegati alla richiesta specificata e archiviati in formato criptato.

Allegare il file a un messaggio e-mail e inviare il messaggio a attach@cisco.com, come mostrato in questa schermata.




La schermata precedente mostra un'e-mail di Microsoft Outlook con un file ZIP allegato criptato, l'indirizzo corretto del destinatario e un oggetto formattato correttamente. Altri client di posta elettronica devono fornire le stesse funzionalità di Microsoft Outlook.

Torna su

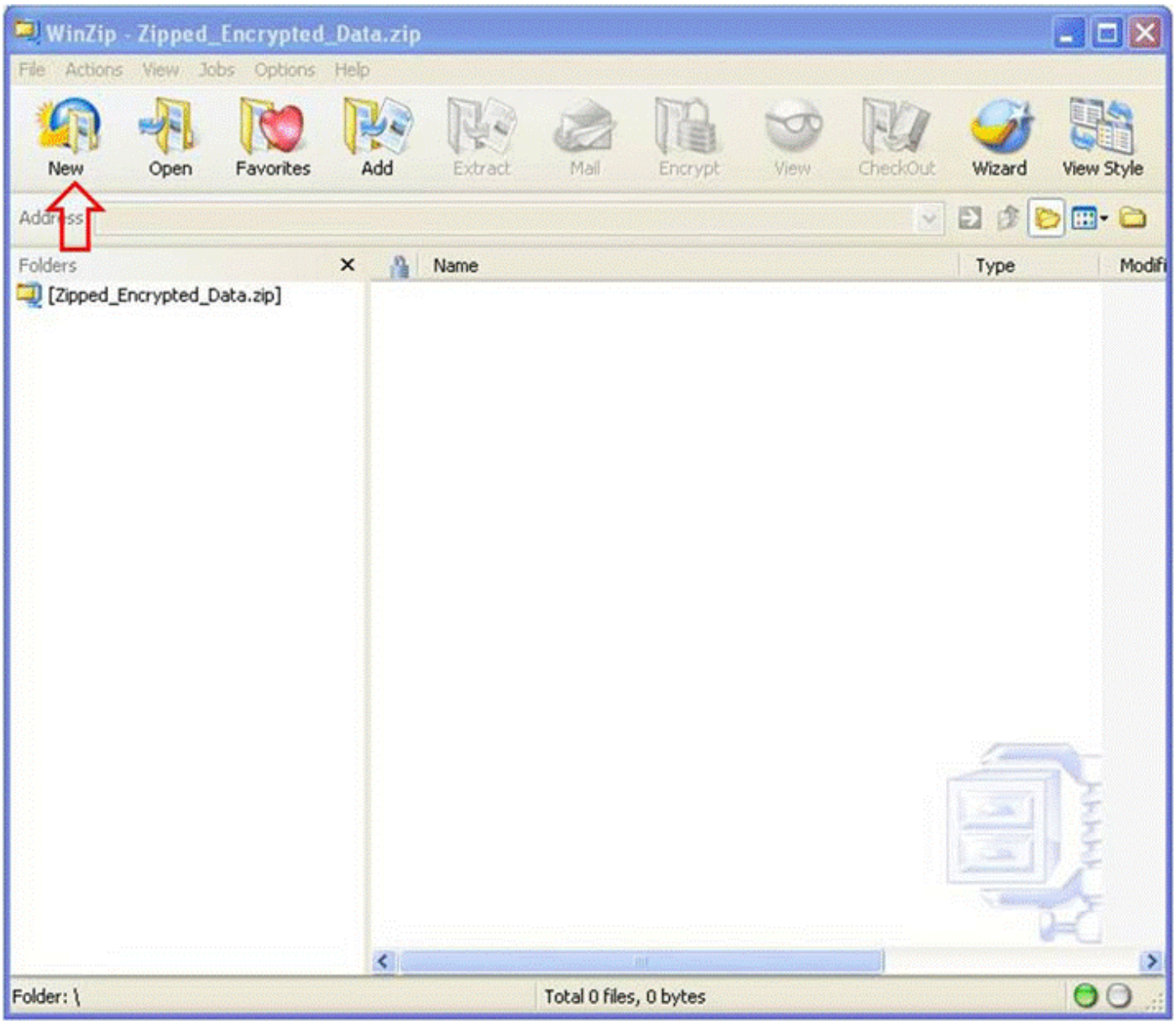
## Crittografia dei file

Gli esempi che seguono mostrano come eseguire la crittografia dei file utilizzando tre delle numerose opzioni disponibili, ad esempio WinZip, comandi Tar e OpenSSL di Linux e Linux Gzip e GnuPG. Per proteggere adeguatamente i dati, è necessario utilizzare una cifratura di crittografia efficace, come AES-128. Se si utilizza ZIP, è necessario utilizzare un'applicazione che supporta la crittografia AES. Le versioni precedenti delle applicazioni ZIP supportano un sistema di crittografia simmetrica non sicuro di cui si sconsiglia l'uso.

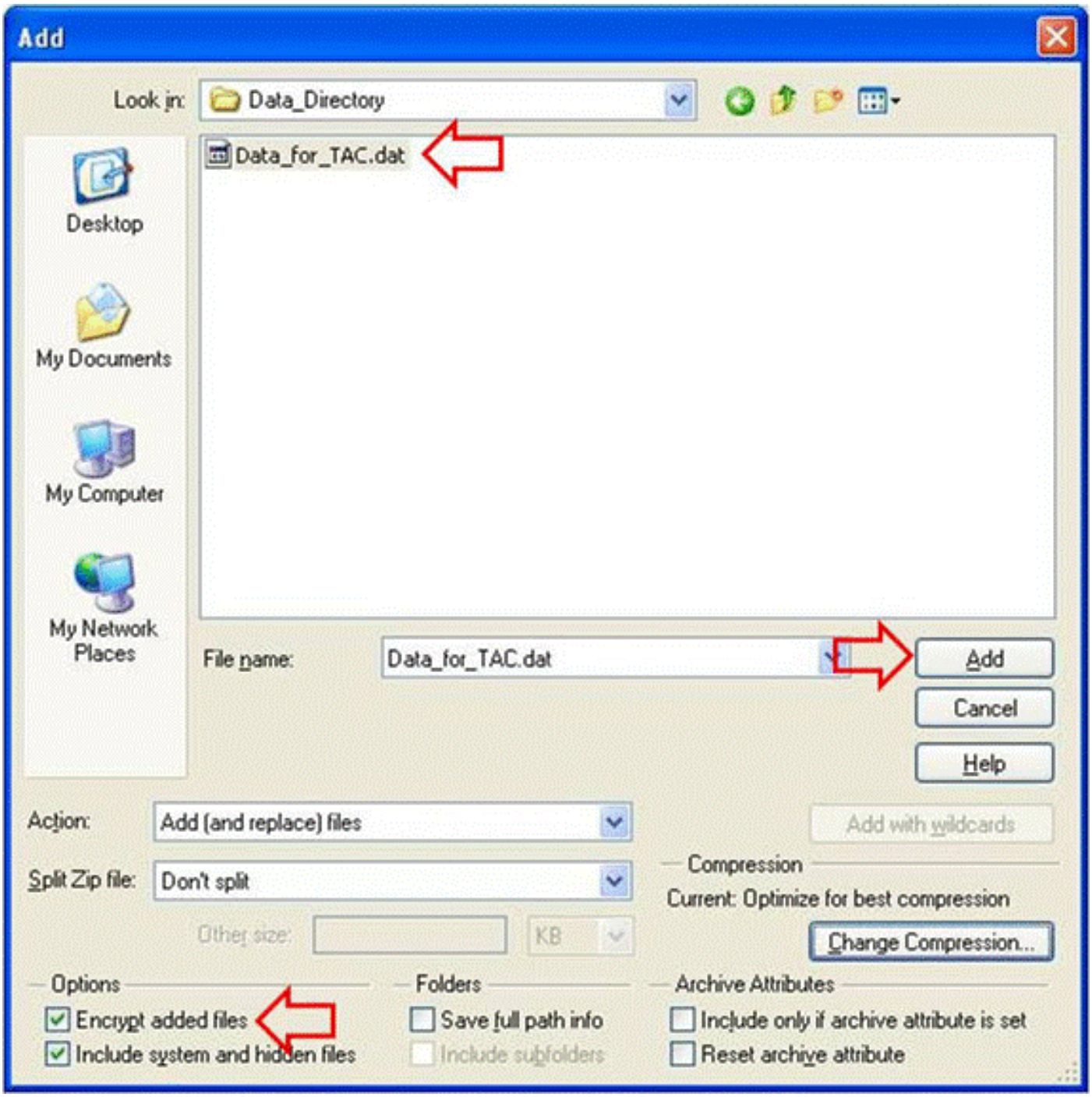
### Crittografia dei file tramite WinZip

Questa sezione illustra come eseguire la crittografia dei file con l'applicazione WinZip. Altre applicazioni forniscono la stessa funzionalità e prestazioni di WinZip.

Passaggio 1. Creare un archivio ZIP. Nell'interfaccia utente di WinZip, fare clic su New e seguire le istruzioni per creare un nuovo archivio ZIP con nome appropriato. Il sistema visualizza il nuovo archivio ZIP creato.



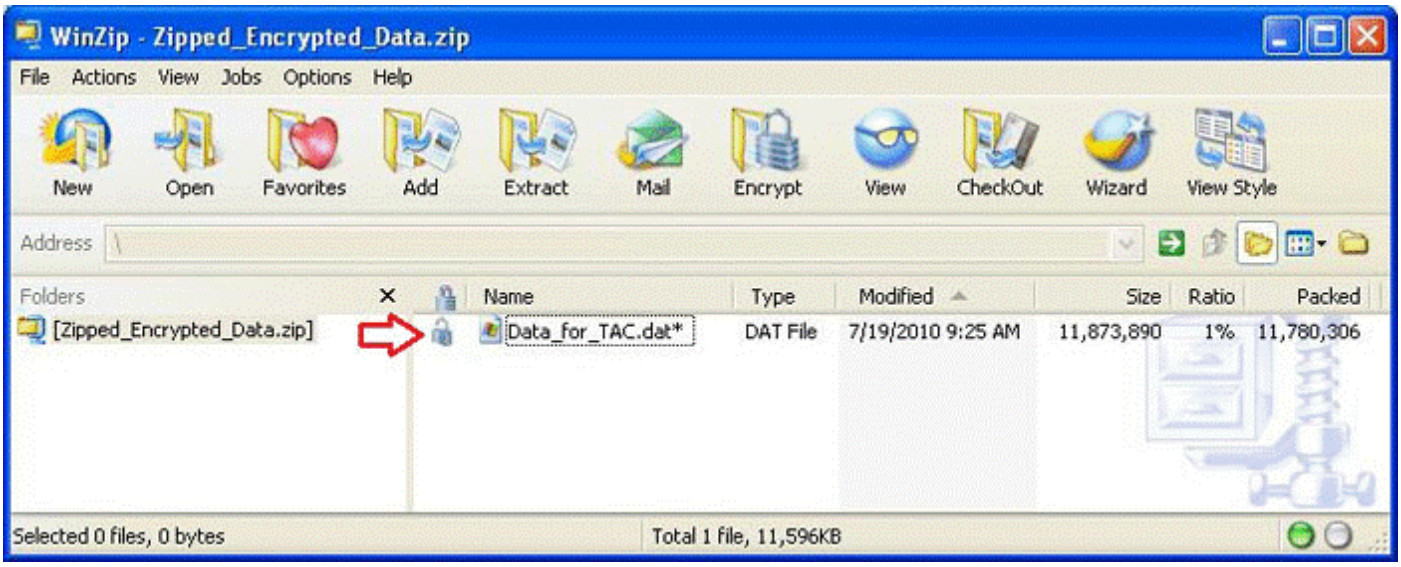

Passaggio 2. Aggiungere i file da caricare nell'archivio ZIP e controllare la **Encrypt added files** . Dalla finestra principale di WinZip, fare clic su **Add** quindi scegliere i file da caricare. OSPF (Open Shortest Path First) **Encrypt added files** deve essere selezionata.




Passaggio 3. Criptare il file con la crittografia AES e una password complessa:

1. Fare clic su **Add** nella finestra selezione file per aprire la finestra **Encrypt** finestra.
2. Nella scheda **Encrypt** creare una password efficace. La password viene condivisa con il responsabile tecnico dell'assistenza, come indicato in Comunicazione della password al tecnico di assistenza TAC.
3. Scegliere uno dei metodi di crittografia AES.
4. Fare clic su **OK** per crittografare i file e visualizzare la finestra principale di WinZip.


Passaggio 4. Verificare che il file sia crittografato. I file crittografati sono contrassegnati da un asterisco dopo il nome o da un catenaccio nella colonna Encryption.




## Crittografia dei file tramite Tar e OpenSSL

Questa sezione illustra come eseguire la crittografia dei file nella riga di comando Linux **tar** e **openssl** comandi. Altri comandi di archiviazione e crittografia offrono le stesse funzionalità e prestazioni anche in Linux o Unix.

Passaggio 1. Creare un archivio TAR con il file e crittografarlo tramite OpenSSL utilizzando la cifratura AES e una password efficace, come mostrato nell'esempio che segue. L'output del comando mostra la combinazione **tar** e **openssl** per crittografare i file con la cifratura 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
60+1 records in
60+1 records out
```

## Crittografia dei file tramite Gzip e GnuPG

Questa sezione illustra come eseguire la crittografia dei file nella riga di comando Linux con i comandi Gzip e GnuPG. Altri comandi di archiviazione e crittografia offrono le stesse funzionalità e prestazioni anche in Linux o Unix. Il risultato del comando mostra come utilizzare la sintassi dei comandi gzip e gpg per crittografare i file con la cifratura AES.

Passaggio 1. Comprimere il file utilizzando Gzip:

```
[user@linux ~]$ gzip -9 Data_for_TAC.dat
```

Passaggio 2. Criptare il file con GnuPG utilizzando la cifratura AES e una password efficace:

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

Passaggio 3. Immettere e confermare la password alla richiesta della passphrase:

Inserire la passphrase:
Ripetere la passphrase:

Torna su

## Comunicazione della password al tecnico di assistenza TAC

Quando si esegue la crittografia degli allegati, è necessario condividere la relativa password con il tecnico di assistenza responsabile della richiesta. È buona norma utilizzare un metodo diverso da quello utilizzato per caricare il file. Se il file è stato caricato tramite messaggio e-mail o FTPS, comunicare la password con un metodo esterno, ad esempio telefonicamente o tramite caricamento nella richiesta SCM.

Torna su

## Conservazione dei file dei clienti

Tutti i file restano accessibili istantaneamente dal personale Cisco autorizzato tramite il sistema di monitoraggio delle richieste per tutto il periodo in cui resta aperta una richiesta e fino ai 18 mesi che seguono la chiusura finale. Trascorso un periodo di 18 mesi dalla chiusura finale, i file possono essere spostati in un'istanza di archiviazione per preservare spazio, ma non vengono eliminati dalla cronologia della richiesta.

In qualsiasi momento, un responsabile del cliente autorizzato può richiedere esplicitamente l'eliminazione di un file da una richiesta. A tal punto, Cisco può eliminare il file e aggiungere una nota alla richiesta per informare la controparte dell'eliminazione del file, della data e dell'ora e del nome del file eliminato. Quando un file viene eliminato con questo metodo, non è possibile recuperarlo.

I file caricati nella cartella TAC FTP vengono conservati per quattro giorni. Il responsabile tecnico della richiesta di supporto deve essere informato quando un file viene caricato in questa cartella. Il

tecnico dell'assistenza deve eseguire un backup dei file entro quattro giorni allegandoli alla richiesta.

Torna su

## Riepilogo

Sono disponibili diverse opzioni per caricare informazioni in TAC per contribuire alla risoluzione delle richieste. SCM e Cisco HTML5 Upload offrono entrambi caricamenti tramite un browser, mentre CXD permette il caricamento tramite browser, Web API e vari protocolli supportati da diversi tipi di client e dispositivi Cisco.

Se non è possibile utilizzare SCM, Cisco HTML 5 File Upload Tool o un protocollo supportato da CXD non FTP come metodo di caricamento, le opzioni meno preferibili sono FTP, CXD o l'invio di un messaggio e-mail a attach@cisco.com. Se si utilizza una di queste opzioni, si consiglia vivamente di crittografare i file prima della trasmissione. Per ulteriori informazioni, vedere Crittografia dei file. È necessario utilizzare una password complessa e comunicarla al tecnico di assistenza utilizzando un altro metodo, ad esempio tramite telefono o aggiornamento della richiesta SCM.

Tutti i file restano accessibili istantaneamente dal personale Cisco autorizzato tramite il sistema di monitoraggio delle richieste per tutto il periodo in cui resta aperta una richiesta e fino ai 18 mesi che seguono la chiusura finale.

- Dopo 18 mesi, i file possono essere spostati in archiviazione.
- In qualsiasi momento, un responsabile del cliente autorizzato può richiedere esplicitamente l'eliminazione di un file da una richiesta.
- I file nella cartella FTP vengono conservati solo per quattro giorni.

Torna su

## Ulteriori informazioni

- Accesso a Cisco Technical Services
- Contatti del supporto Cisco internazionali
- Guida alle risorse Cisco Technical Services
- Prodotti Cisco Conferencing
- GNU Privacy Guard
- Progetto OpenSSL
- WinZip

Questo documento fa parte di Cisco Security Research & Operations.



Torna su

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).