客戶檔案上傳至 Cisco 技術援助中心

目錄

簡介

本檔案介紹如何將檔案上傳到思科技術協助中心(TAC)。

概觀

TAC客戶支援工程師將相關檔案附加到問題時，可以協助您及時解決問題。有多個選項可用於上傳與您的問題相關的檔案。其中有些選項安全性較低，可能會導致某些風險，而且每個選項都有其限制，您在決定適當的上傳選項前需要考慮這些限制。表 1 總結可用的上傳選項，並詳述檔案加密功

能、建議檔案大小限制和其他相關資訊。

表1.可用的上傳選項

可用選項（按優先順序排列）		檔案在傳送過程中已加密。	待用資料已加密。	建議的檔案大小限制
支援案件管理器 (SCM)	如何	是	是	無限制
Customer eXperience Drive	如何	是*	是	無限制
傳送電子郵件至 attach@cisco.com	如何	否**	是	20 MB 或更低（視客戶郵件伺服器限制而定）
*適用於除 FTP 以外的所有通訊協定。使用FTP時，強烈建議在上傳資料前對其進行加密。 **傳輸前必須進行加密。只能從電子郵件/附件到達思科網路的點保障安全傳輸，而不是在客戶網路或電子郵件提供商端。				

支援案件管理器檔案上傳

支援案件管理器(SCM)檔案上傳方法是將檔案上傳到案件的安全選項。您的計算裝置與思科之間的通訊通道已加密。透過 SCM 上傳的檔案會立即連結到關聯的案件並以加密格式儲存。

上傳檔案至案件

提交案件後，您可以上傳檔案。

步驟 1.登入SCM。

步驟 2.若要檢視和編輯案件，請按一下清單中的案件編號或案件標題。案件摘要頁面隨即開啟。

步驟 3.按一下 **Add Files** 以選擇檔案並上傳至案件做為附件。系統顯示SCM檔案上傳程式工具。

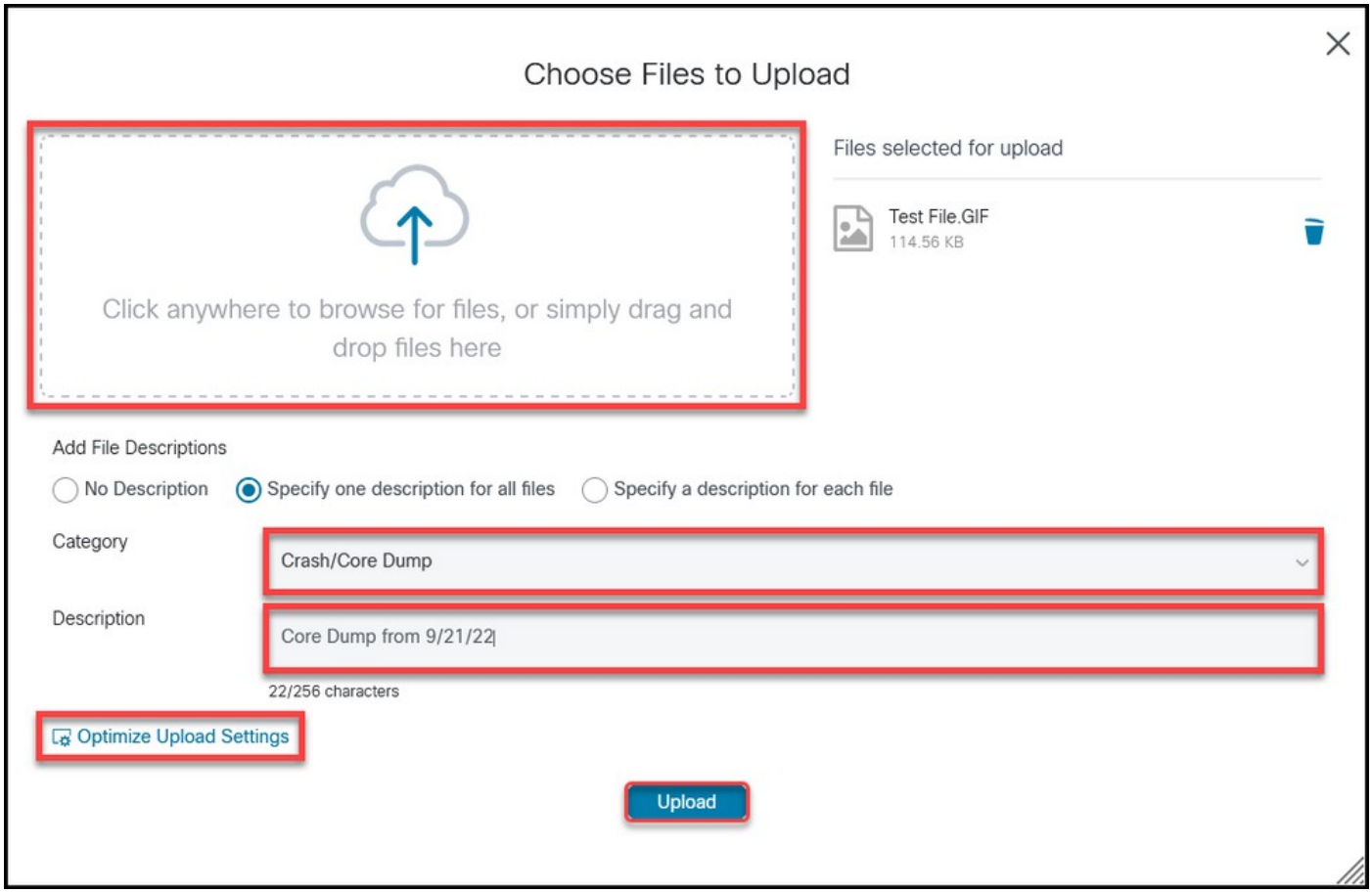
步驟 4.在 **Choose Files to Upload** 對話方塊中，拖動要上載的檔案，或按一下內部瀏覽要上載檔案的本地

電腦。

步驟 5.新增說明並為所有檔案或單獨指定一個類別。

注意：為了最佳化網路條件的上傳設定，請按一下 **Optimize Upload Settings**.

步驟 6.按一下 **Upload** 以啟動上傳程式。



步驟 7. 完成所有上傳後，您可以關閉視窗或按一下 **Add More Files** 以便上傳更多檔案。

步驟 8.上傳的檔案可以在 **Attachments** 頁籤。

返回頂端

Customer eXperience Drive

服務摘要

Customer eXperience Drive (CXD) 是一種多協定檔案上傳服務，對上傳的檔案大小沒有限制。它幫助具有主動服務請求(SR)的思科客戶使用每個SR建立的一組唯一憑證直接將資料上傳到案件。思科產品原生支援 CXD 支援的通訊協定，可直接從思科裝置上傳到 SR。

支援的通訊協定

表 2 總結 CXD 支援的通訊協定。值得注意的是，無論使用哪種通訊協定，上傳檔案都沒有大小限制。

表2.CXD支援的通訊協定

名稱	通訊協定/連接埠	已加密	資料通道埠	備註
安全檔案傳輸通訊協定 (SFTP)	TCP/22	是	不適用	
安全複製協定 (SCP)	TCP/22	是	不適用	
透過 SSL 的超文字傳輸通訊協定 (HTTPS)	TCP/443	是	不適用	僅支援基於API的上傳。
SSL (FTPS) 的檔案傳輸通訊協定（隱含）	TCP/990	是	30000-40000	由於控制通道已加密，因此防火牆無法檢查FTPS。因此，防火牆需要允許到整個資料通道埠範圍的輸出連線。

SSL 的檔案傳輸通訊協定 (FTPS) (明確)	TCP/21	是	30000-40000	
檔案傳輸通訊協定 (FTP)	TCP/21	是	30000-40000	思科完全不建議使用 FTP，因為此通訊協定不支援加密。如果必須使用，應在傳輸前對資料進行加密。 防火牆必須檢查 FTP 流量，以允許正確建立資料通道。如果在整個網路中都不檢查 FTP，則防火牆需要允許到整個資料通道埠範圍的輸出連線。

CXD 上傳權杖

CXD 會為每個 SR 建立唯一的上傳權杖。SR 編號和權杖係用來作為對服務進行身份驗證以及隨後將檔案上傳到 SR 的使用者名稱和密碼。

注意：權杖僅用於上傳，不能允許使用者存取案件檔案，甚至是目前正在上傳的檔案。如果使用者想要查看案件檔案，則只能在 SCM 中完成。

擷取 SR 的上傳權杖

使用 SCM

開啟SR時，使用者必須建立上傳權杖才能上傳附件。

若要擷取/產生上傳權杖，請完成以下步驟：

步驟 1.登入SCM。

步驟 2.若要檢視和編輯案件，請按一下清單中的案件編號或案件標題。案件摘要頁面隨即開啟。

步驟 3.按一下 **Attachments** 頁籤。

步驟 4.按一下 **Generate Token.**生成令牌後，它會顯示在「生成令牌」(Generate Token)按鈕旁邊。

注意：使用者名稱一律採用SR編號。術語「密碼」和「令牌」指的是上傳令牌，在CXD提示時該令牌被用作密碼。

使用API

使用API的客戶可以使用 **Get Token** API。

> 注意：需要Okta身份驗證權杖才能呼叫Cisco Get Token API。有關獲取身份驗證權杖的詳細資訊，請參閱 Cisco ServiceGrid 說明文件。

HTTP方法：POST

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

標題：

表3.獲取令牌API標頭

主要	類型	價值
Content-Type	字串	application/json
Authorization	字串	持有人 <Auth Token>

本文：

表4.ServiceGrid GetUploadCredentials API 本文

主要	類型	價值
使用者名稱	字串	Cisco.com 使用者名稱已獲得授權可將檔案上傳到 SR
電子郵件	字串（郵件格式）	Cisco.com 使用者名稱的電子郵件地址

上傳檔案至 CXD

使用桌面用戶端

一般情況下，使用者需要使用使用者端（視通訊協定而定），才能連線到cxd.cisco.com、使用SR編號作為使用者名稱來進行身份驗證、上傳權杖作為密碼，最後上傳檔案。視通訊協定和使用者端而定，使用者步驟可能不同。建議參閱使用者端說明檔案以瞭解更多詳細資訊。

直接從思科裝置

所有思科裝置都有內建檔案傳輸客戶端，通常使用 **copy** 或 **redirect** 指令。在Linux發行版中執行的思科裝置通常支援整合的一或多個scp、sftp和curl以整合SCP、SFTP和HTTPS。

檔案上傳 API

檔案上傳 API 利用 HTTP PUT 指令動詞將檔案上傳到 CXD。為了達到整合的最大相容性和簡便性，API應保持簡單。

HTTP方法： PUT

URL: https://cxd.cisco.com/home/<目標檔名>

標頭：

表5.CXD 檔案上傳 API 標頭

主要	類型	價值
Authorization	字串	基本 HTTP 身份驗證字串

正文是檔案資料本身。此處沒有欄位或表單，因此請求非常簡單。

使用 PUT API 的 Python 代碼範例

請注意，此代碼假定檔案儲存在您執行的同一路徑中。

```
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")
```

返回頂端

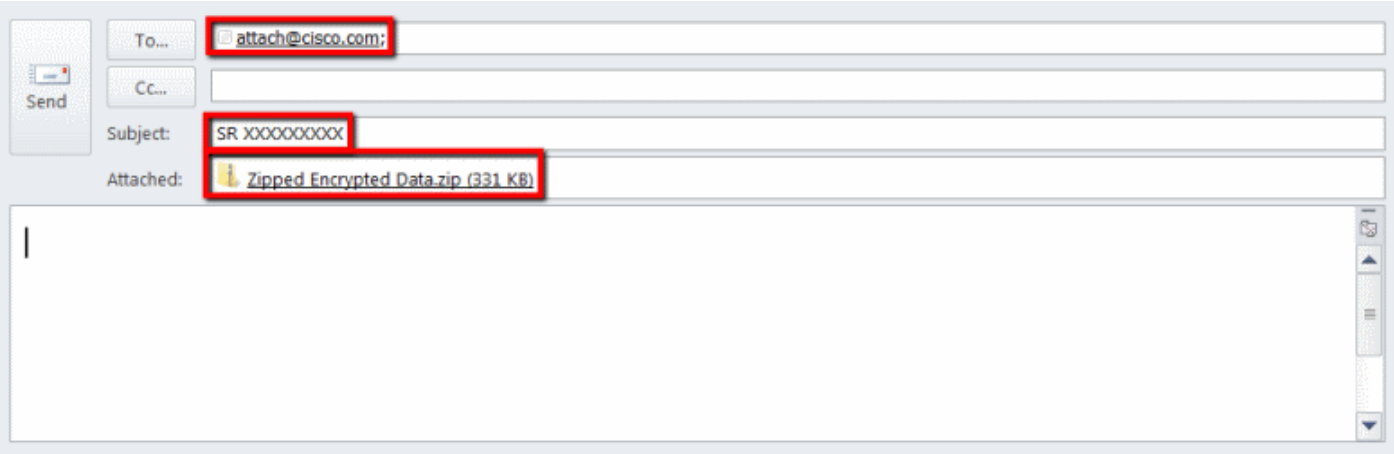
電子郵件檔案附件上傳

如果SCM和CXD無法為您效力，另一種備用檔案上傳方法是郵件檔案附件上傳。請注意，此方法基本上並不安全，不會加密在客戶和思科之間傳輸檔案的檔案或通訊工作階段。客戶必須在透過郵件檔案附件上傳檔案之前明確加密檔案。為了多一層安全防護，最佳作法是密碼等敏感資訊需進行模糊處理，或將其從透過不安全通道傳送的設定檔或記錄檔中移除。有關詳細資訊，請參閱加密檔案。

在對檔案進行加密後，若要將其他資訊和檔案上傳到案件，可以將資訊透過電子郵件訊息傳送到attach@cisco.com，並將案例編號填寫在郵件主題行，例如主題 = 案件 xxxxxxxxx。

每次郵件更新，附件大小限制為 20 MB。使用電子郵件訊息提交的附件不會在傳輸過程中加密，但會立即連結到指定的案件並以加密格式儲存。

將檔案附加到電子郵件訊息，並將郵件傳送到attach@cisco.com （如以下截圖所示）。



上一個熒幕截圖顯示一封Microsoft Outlook郵件，其中包含加密的ZIP檔附件、正確的收件人地址和格式正確的主題。其他電子郵件使用者端需要提供與Microsoft Outlook相同的功能並且可以順利執行。

返回頂端

加密檔案

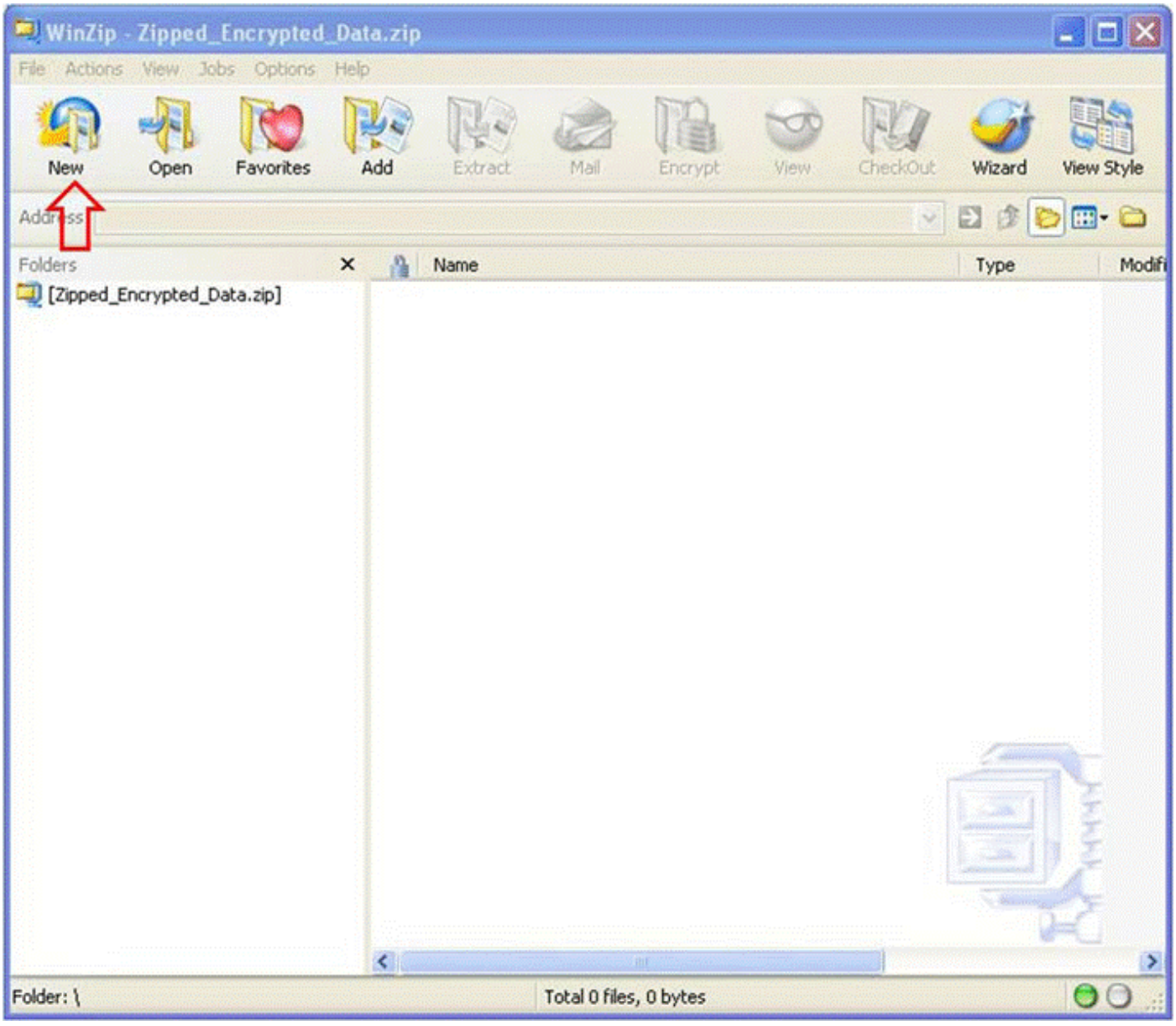
以下範例顯示如何在各種可用選項（例如 WinZip、Linux tar 和 openssl 命令以及 Linux Gzip 和

GnuPG）中使用三種選項對檔案進行加密。需要使用AES-128等強式加密密碼來妥善保護資料。如果您使用的是 ZIP，則必須使用支援 AES 加密的應用程式。較舊版本的ZIP應用程式支援對稱加密系統，這種加密方式並不安全，因此不會被使用。

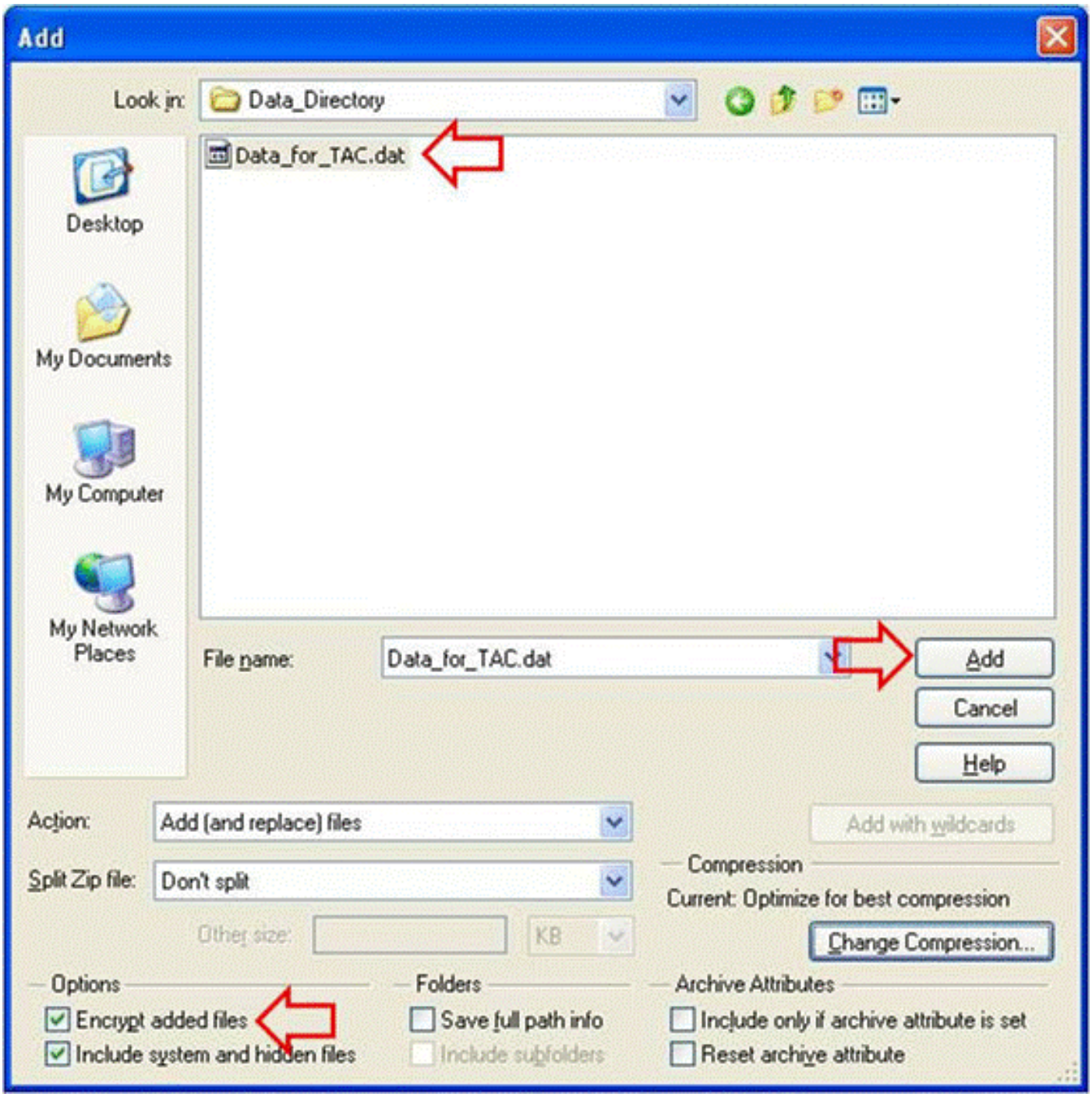
使用 WinZip 加密檔案

本節介紹如何使用WinZip應用程式加密檔案。其他應用程式會提供與WinZip相同的功能並能順利執行。

步驟 1.建立ZIP封存檔。在WinZip GUI中，按一下 **New** 並按照選單提示建立具有適當名稱的新ZIP存檔檔案。系統顯示新建立的ZIP存檔檔案。



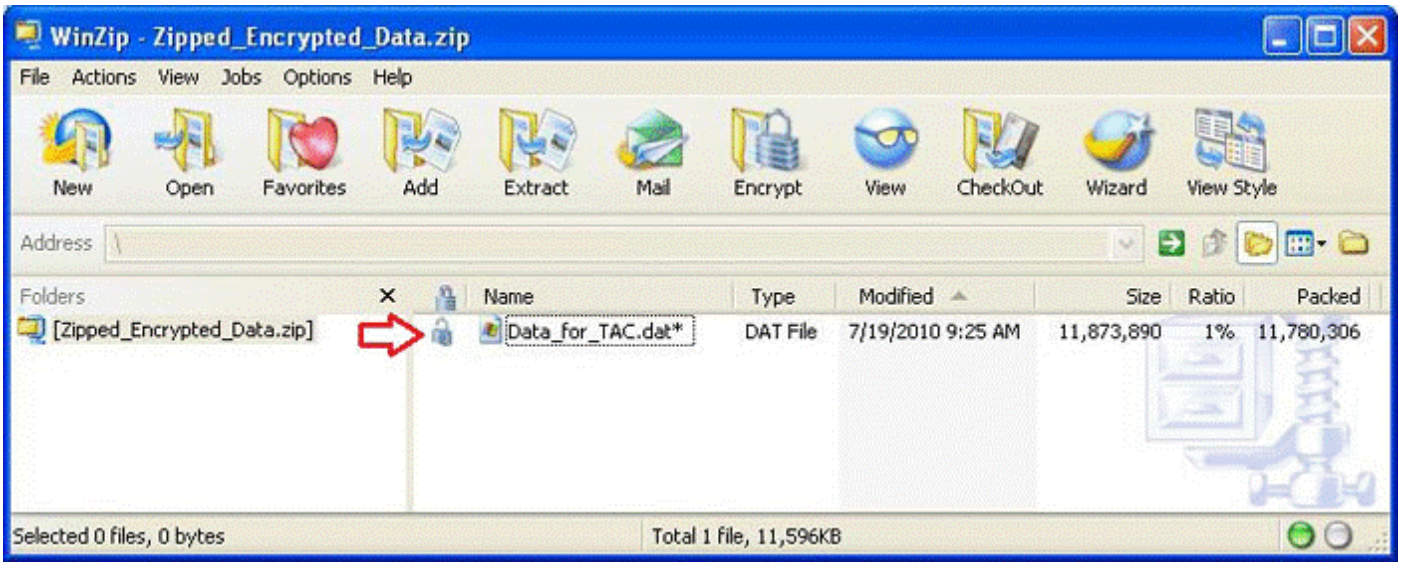
步驟 2.新增要上傳到ZIP封存檔的檔案，並檢查 **Encrypt added files** 覈取方塊。在WinZip主視窗中，按一下 **Add** 然後選擇要上傳的檔案。其 **Encrypt added files** 覈取方塊必須選中。



步驟 3.使用AES加密密碼和強式密碼加密檔案：

1. 按一下 **Add** 在「file selection」視窗中開啟 **Encrypt** 視窗。
2. 在 **Encrypt** 視窗中，建立強度適當的密碼。密碼將會與案件客戶支援工程師擁有者共用，如同在將密碼傳送給 TAC 客戶支援工程師中所述。
3. 選擇其中一個 AES 加密方法。
4. 按一下 **OK** 以便加密檔案並顯示WinZip主視窗。

步驟 4.驗證檔案是否已加密。加密的檔案在檔案名稱後標有星號，或在「Encryption」欄中標有一個鎖定圖示。



使用 Tar 和 OpenSSL 加密檔案

本節介紹如何使用Linux命令列加密檔案 **tar** 和 **openssl** 指令。其他存封存和加密命令會提供與Linux或Unix相同的功能並同樣可順利執行。

步驟 1.建立檔案的tar封存，並使用AES密碼和強式密碼透過OpenSSL對其進行加密（如以下範例所示）。命令輸出會顯示組合的 **tar** 和 **openssl** 命令語法，用於使用AES密碼加密檔案。

```
[user@linux ~] $ tar cvzf-Data_for_TAC dat | openssl aes-128-cbc-k
Str0ng_passWo5D |
    dd of = Data_for_TAC. aes128 Data_for_TAC
60+1 條記錄傳入
60+1 條記錄傳出
```

使用 Gzip 和 GnuPG 加密檔案

本節示範如何使用Linux命令列Gzip和GnuPG命令對檔案進行加密。其他存封存和加密命令會提供與Linux或Unix相同的功能並同樣可順利執行。命令輸出會顯示如何使用 gzip 和 gpg 命令語法對使用 AES 密碼的檔案進行加密。

步驟 1.使用Gzip壓縮檔案：

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

步驟 2.使用AES密碼和強式密碼透過GnuPG加密檔案：

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

步驟 3.在密碼提示字元後輸入強式密碼並加以確認：

輸入密碼短語：
再輸入一次複雜密碼：

返回頂端

將密碼傳送給 TAC 客戶支援工程師

加密附件時，請與案件客戶支援工程師擁有者一同加密密碼。最佳作法是使用除了用於上傳檔案的方法之外的方法。如果您使用電子郵件訊息或 FTPS 上傳檔案，請在頻外（例如透過電話或 SCM 案件更新）傳送密碼。

返回頂端

客戶檔案保留

如果某個案件在一段時間內處於開啟狀態且在最後結案後超過 18 個月的一段時間內，所有檔案都可從案件追蹤系統立即存取到獲得授權的思科人員。在結案後的18個月的一段時間後，檔案可能會被移至封儲存存執行個體以節省空間，但不會從案件例歷史記錄中清除（刪除）。

獲得授權的客戶聯絡人隨時都可以明確請求將特定檔案從案件中清除。然後，思科可以刪除該檔案並新增一個案件備註，以記錄刪除該檔案的人員、時間和日期戳記以及已刪除檔案的名稱。以這種方式清除檔案後，就無法復原檔案。

上傳到 TAC FTP 資料夾的檔案將會保留 4 天。如果將檔案上傳到此資料夾，則需要通知客戶支援工程師擁有者。客戶支援工程師應在四天內將檔案附加到案件中，以備份這些檔案。

返回頂端

摘要

有多個選項可用來將資訊上傳到TAC，以協助他們解決案件。SCM 和思科的 HTML5 上傳工具都提供透過瀏覽器的安全上傳，而 CXD 提供透過瀏覽器、Web API 以及不同類型的用戶端和思科裝置

支援的多種通訊協定的上傳。

如果不能使用 SCM、Cisco HTML 5 檔案上傳工具或 CXD 支援的通訊協定等不是以 FTP 作為您檔案上傳方法，則除了應該儘量避免的檔案上傳選項 FTP 外，您可以使用 CXD 或以電子郵件訊息傳送至 attach@cisco.com。如果您使用其中任一選項，強烈建議您在傳輸之前加密您的檔案。有關詳細資訊，請參閱加密檔案。您需要使用強式密碼，並在頻外（例如透過電話或SCM案件更新）將密碼傳送給案件客戶支援工程師。

如果某個案件在一段時間內處於開啟狀態且在最後結案後超過 18 個月的一段時間內，所有檔案都可從案件追蹤系統立即存取到獲得授權的思科人員。

- 18個月後，檔案即可移動到存檔儲存中。
- 獲得授權的客戶聯絡人隨時都可以明確請求將特定檔案從案件中清除。
- FTP 資料夾中的檔案僅保留四天。

返回頂端

其他資訊

- 存取思科技術服務
- 思科全球支援聯絡人
- 思科技術服務資源指南
- Cisco Conferencing 產品
- GNU Privacy Guard
- OpenSSL 專案
- WinZip

本文件是思科資安研究和營運的一部分。

返回頂端

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。