Hochladen von Kundendateien in das Cisco Technical Assistance Center

Inhalt

Überblick

Kunden sind von größter Bedeutung für Cisco, deshalb möchten wir Kundenprobleme zeitnah ansprechen und beheben. Der Kunde kann den Prozess beispielsweise unterstützen, indem er dem Cisco Technical Assistance Center (TAC) die relevanten Dateien zur Überprüfung zur Verfügung stellt. Die TAC-Kundensupporttechniker verwenden diese Dateien, um Kundenprobleme zu beheben, und Cisco bietet mehrere Optionen zum Hochladen von Informationen an das Cisco TAC, um die Anforderungen von Kunden zu erfüllen. Einige dieser Optionen sind weniger sicher und führen zu bestimmten inhärenten Risiken. Und jede Option hat Einschränkungen, die Kunden berücksichtigen sollten, bevor sie sich für eine geeignete Upload-Option entscheiden. Tabelle 1 enthält die verfügbaren Upload-Optionen mit Details zu Dateiverschlüsselungsfunktionen, empfohlene Dateigrößenbeschränkungen und andere relevante Informationen.

Tabelle 1. Verfügbare Upload-Optionen

Verfügbare Option (sortiert nach	Dateien werden bei	Dateien werden im	Empfohlene Dateigrößenbeschränkung

Präferenz)	der Übertragung verschlüsselt	ruhenden Zustand verschlüsselt	
Support Case Manager (SCM)	Ja	Ja	250 GB
Uploader für Ticket-Datei	Ja	Ja	250 GB
Customer eXperience Drive	Ja*	Ja	Keine Beschränkung
E-Mail an attach@cisco.com	Nein* *	Ja	20 MB oder weniger je nach Beschränkungen des E-Mail-Servers beim Kunden
* Gilt für alle Protokolle mit Ausnahme von FTP. Bei Verwendung von FTP empfiehlt Cisco dringend, die Daten vor dem Hochladen zu verschlüsseln. ** Der Kunde muss vor der Übertragung verschlüsseln. Übertragungen vom Netzwerk/E-Mail-Anbieter des Kunden können möglicherweise nicht verschlüsselt werden. Die sichere Übertragung ist nur ab dem Punkt garantiert, an dem die E-Mail/der Anhang das Cisco Netzwerk erreicht.			

Hochladen der Support Case Manager-Datei

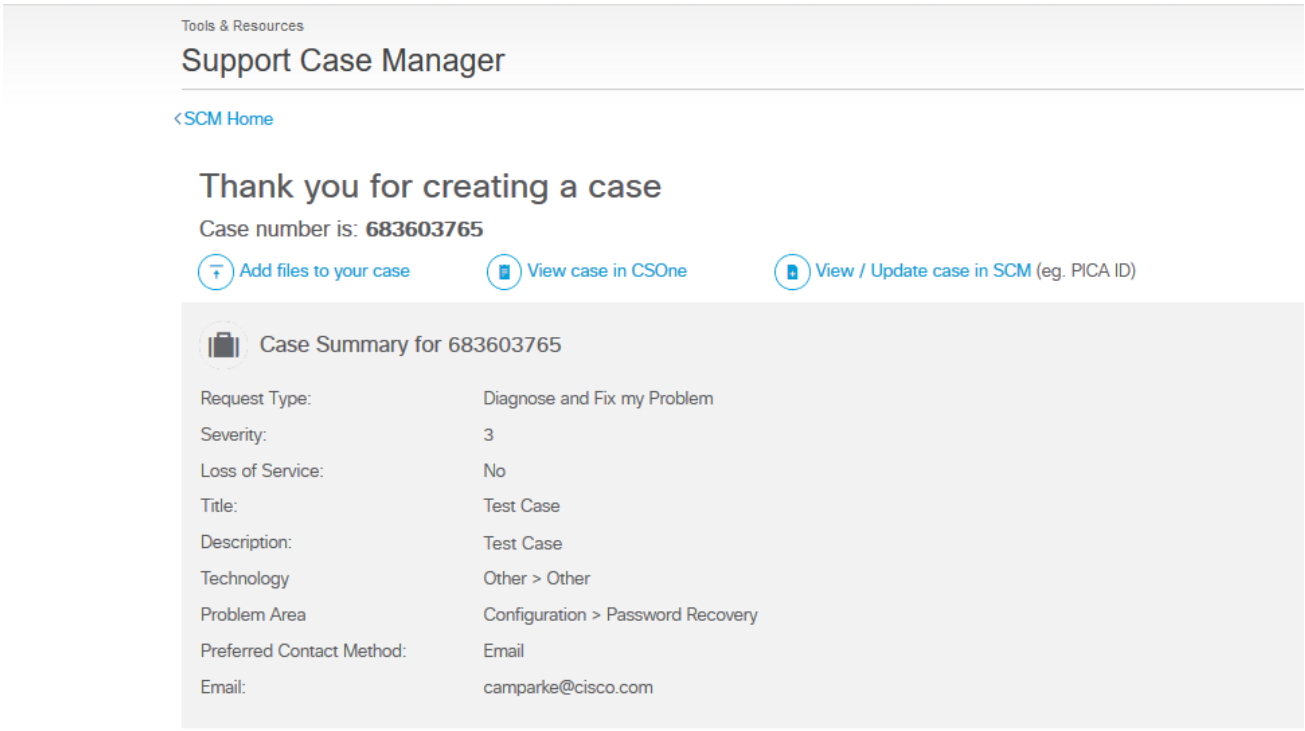
Die Datei-Upload-Methode Support Case Manager (SCM) ist die bevorzugte und sicherste Option zum Hochladen von Dateien zu Tickets. Dateien, die mit dieser Option übertragen werden, werden bei der Übertragung verschlüsselt und auf eine Größe von 250 GB beschränkt. Der Kommunikationskanal zwischen dem Computing-Gerät des Kunden und Cisco ist verschlüsselt. Über SCM hochgeladene Dateien werden sofort mit dem zugehörigen Ticket verknüpft und in verschlüsselter Form gespeichert.

Hochladen einer Datei bei der Einreichung eines Tickets

Befolgen Sie die Schritte im Bildschirm "Fallbestätigung". Detaillierte Anweisungen zum Erstellen oder Verwalten eines Tickets im SCM finden Sie in der SCM-Hilfe.

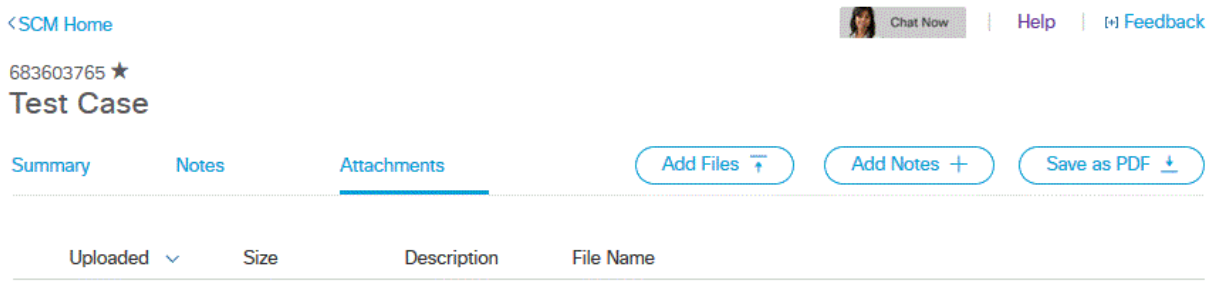
Schritt 1 Wählen Sie die Schaltfläche Dateien zu Ihrem Ticket hinzufügen (Abbildung 1).

Abbildung 1. SCM: Hinzufügen von Dateien zu Ihrem Ticket



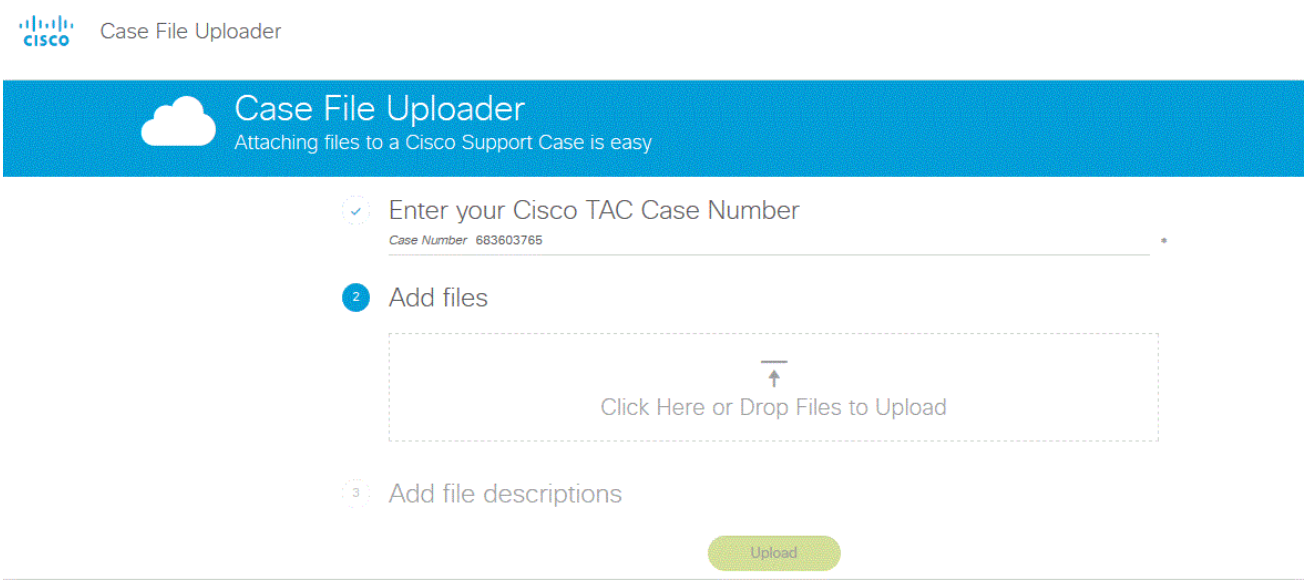
Schritt 2 Wählen Sie aus der Registerkarte "Anhänge" die Schaltfläche Dateien hinzufügen aus (Abbildung 2).

Abbildung 2. SCM: Registerkarte "Anhänge"



Sie werden zum Uploader für Ticket-Dateien geleitet. Das von Ihnen erstellte Ticket wird im Tool vorab ausgefüllt (Abbildung 3). Fahren Sie in Schritt 3 mit dem Abschnitt Uploader für Ticket-Datei fort.

Abbildung 3: Uploader für Ticket-Dateien: Drag-and-Drop-Bildschirm



Hochladen einer Datei zu einem bestehenden Ticket

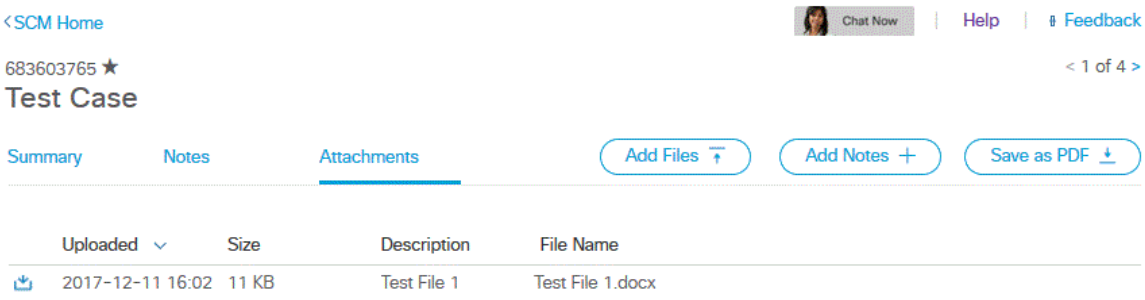
Nachdem ein Ticket eingereicht wurde, können Sie die optionalen Informationen aktualisieren oder ändern.

Schritt 1 Melden Sie sich beim SCM an.

Schritt 2 Um ein Ticket zu öffnen und zu bearbeiten, klicken Sie in der Liste auf die Ticketnummer oder den Titel. Die Seite mit Ticketdetails wird geöffnet.

Schritt 3 Oben auf der Seite mit Ticketdetails gibt es drei Registerkarten: **Übersicht**, **Notizen** und **Anhänge**. Neben den Registerkarten befinden sich eine Reihe von Symbolleistenschaltflächen: **Dateien anhängen**, **Notizen hinzufügen** und **Als PDF speichern**. Klicken Sie auf **Dateien hinzufügen , um eine Datei auszuwählen, und laden Sie sie als Anhang zum Ticket hoch (Abbildung 4).**

Abbildung 4: Bildschirm "SCM Attachments"



Sie werden zum Uploader für Ticket-Dateien geleitet. Das von Ihnen erstellte Ticket wird im Tool vorab ausgefüllt (Abbildung 3). Fahren Sie in Schritt 3 mit dem Abschnitt **Uploader für Ticket-Datei fort.**

Zum Seitenanfang

Uploader für Ticket-Datei

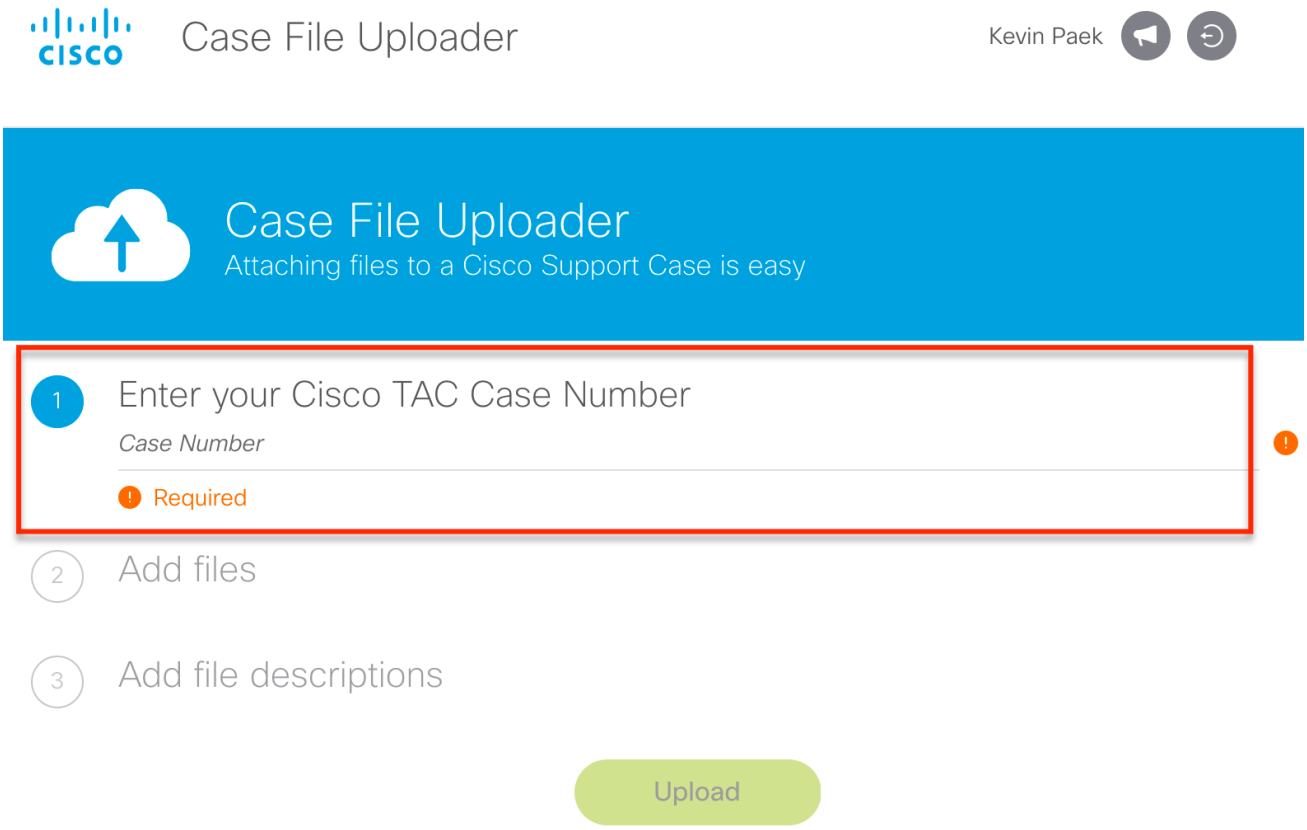
Ein weiteres sicheres Verfahren zum Hochladen von Dateien ist der Uploader für Ticket-Dateien. Dieses Tool ähnelt dem SCM, weil Dateien mit dieser Option bei der Übertragung verschlüsselt und auf eine Größe von 250 GB beschränkt werden. Der Kommunikationskanal zwischen dem Computing-Gerät des Kunden und Cisco ist verschlüsselt. Mit dem Uploader für Datei-Tickets hochgeladene Dateien werden sofort mit dem zugehörigen Ticket verknüpft und in verschlüsselter Form gespeichert. Führen Sie die folgenden Schritte aus, um eine Datei mit diesem Tool anzuhängen.

Hinweis: Wenn Sie feststellen, dass Sie mit dem Tool keine Datei zu Ihrem Ticket hochladen können, ist entweder die eingegebene Ticketnummer ungültig, oder Sie verfügen nicht über die erforderlichen Berechtigungen, um Dateien hinzuzufügen. Um Dateien zu einem Ticket hochzuladen, muss Ihr cisco.com-Profil dem Vertrag zugeordnet werden, für den das Ticket erstellt wurde. Sie können mit dem Cisco Profil Manager Ihrem Profil einen Servicevertrag hinzufügen oder Ihren Service Access Management-Administrator das für Sie erledigen lassen. Wenn Sie weitere Unterstützung benötigen, wenden Sie sich an das Cisco Technical Assistance Center.

Schritt 1 Melden Sie sich beim Uploader für Ticket-Dateien an.

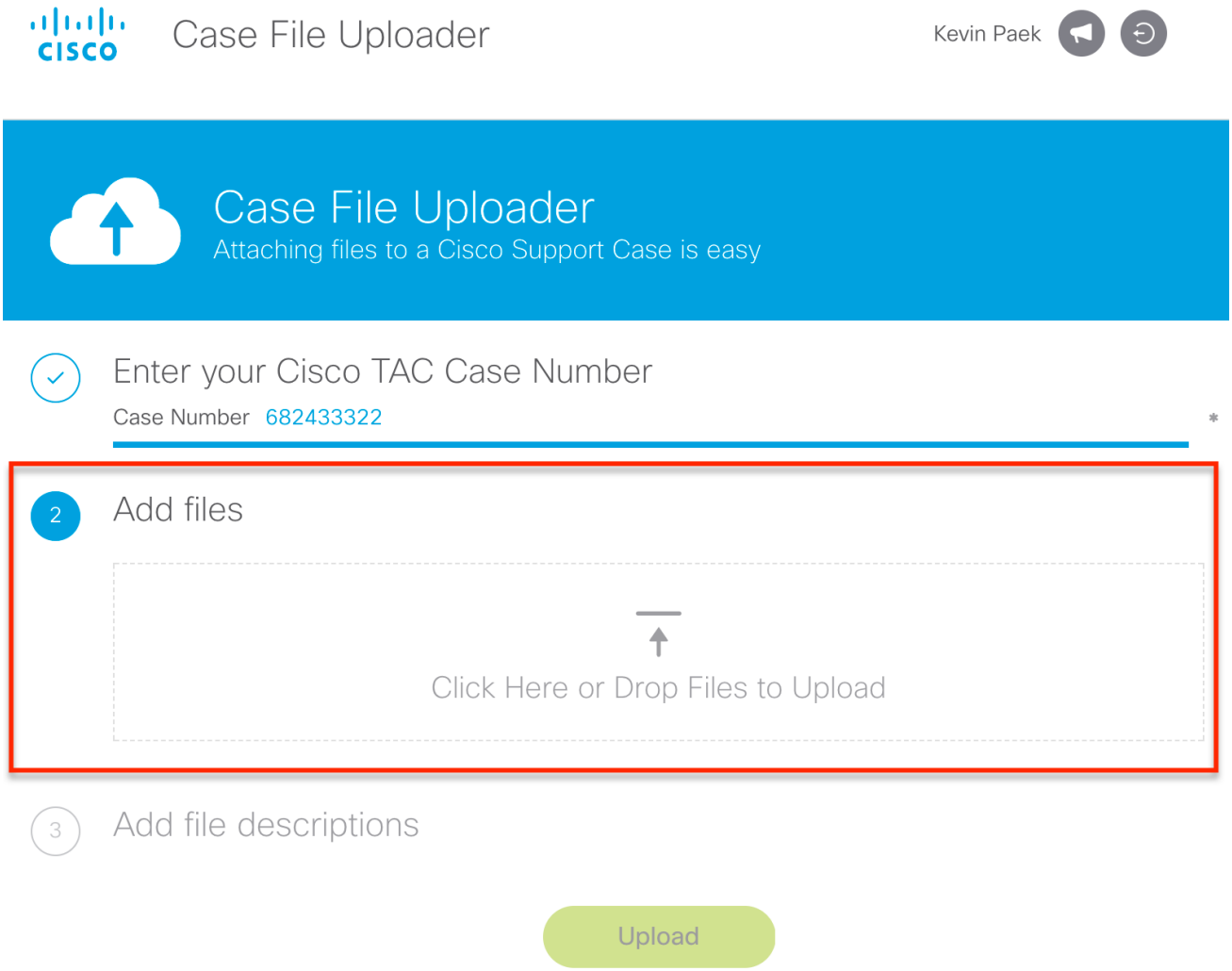
Schritt 2 Geben Sie Ihre Ticketnummer in das vorgesehene Feld ein (Abbildung 5).

Abbildung 5: Uploader für Ticket-Datei: Eingabebildschirm für Ticket-Nummer



Schritt 3 Zur Auswahl einer anzuhängenden Datei verschieben Sie diese entweder per Drag and Drop oder Sie klicken in das gestrichelte Feld, um die Datei für den Upload auszuwählen (Abbildung 6).

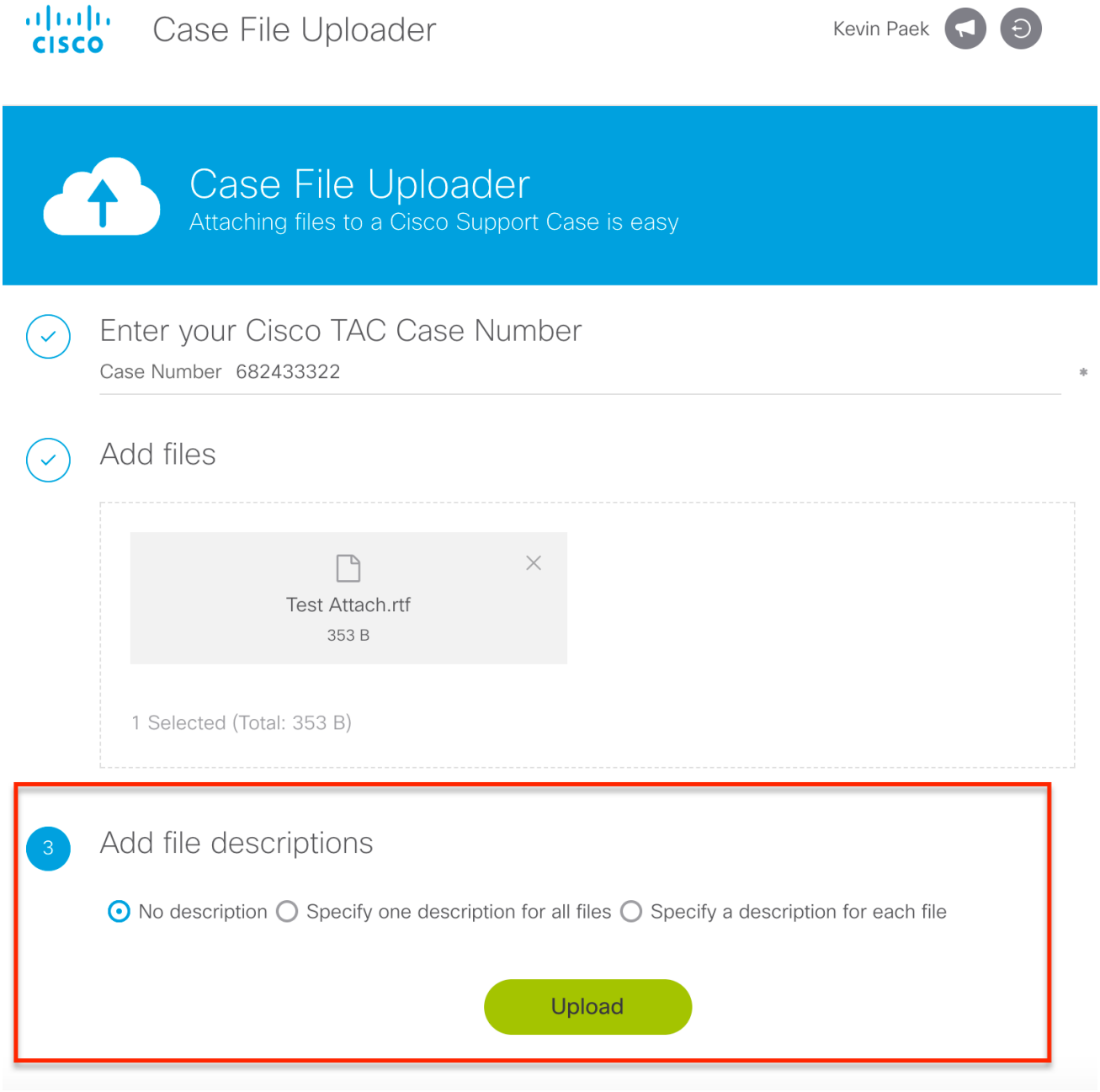
Abbildung 6: Uploader für Ticket-Dateien: Drag-and-Drop-Bildschirm



Schritt 4 Nachdem Sie eine Datei ausgewählt haben, für die keine Beschreibung erforderlich ist, klicken Sie auf Hochladen. Andernfalls können Sie mithilfe der anderen Optionen weitere Details hinzufügen. (Abbildung 7). Mithilfe der Felder **Kategorie** und **Beschreibung** können Sie weitere Informationen zur Datei hinzufügen:

- Verwenden Sie das Feld **Kategorie, um einen Anhangtyp auszuwählen.**
- Verwenden Sie das Feld **Beschreibung, um eine kurze Beschreibung der Datei anzugeben.**

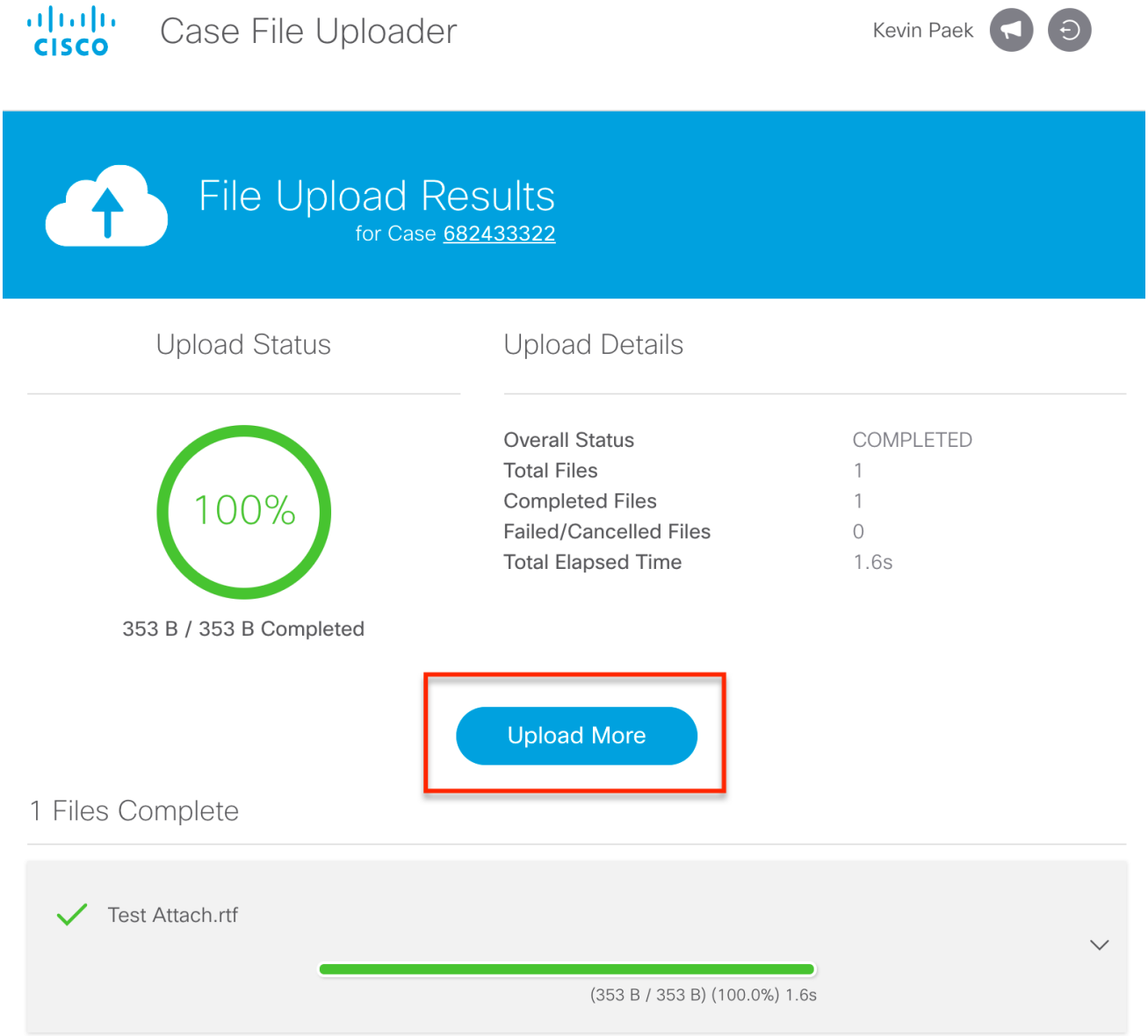
Abbildung 7: Uploader für Ticket-Dateien: Eingabe der Dateibeschreibung



Schritt 5 **Klicken Sie auf Hochladen**, um die Datei hochzuladen.

Schritt 6 **Der nächste Bildschirm zeigt den Status der Datei an.** Nachdem die Datei hochgeladen wurde, klicken Sie auf **Weitere hochladen (Abbildung 8), um zusätzliche Anhänge hochzuladen.**

Abbildung 8: Uploader für Ticket-Datei: Bildschirm "Upload Status"



Zum Seitenanfang

Customer eXperience Drive

Zusammenfassung der Services

Customer eXperience Drive (CXD) ist ein Datei-Upload-Service mit mehreren Protokollen, bei dem es keine Einschränkungen bei der Größe der hochgeladenen Datei gibt. Er ermöglicht es Cisco Kunden mit aktiven Servicetickets, Daten mithilfe von Anmeldedaten, die für jedes Serviceticket erzeugt werden, direkt zu einem Ticket hochzuladen. Die von CXD unterstützten Protokolle werden nativ von Cisco Produkten unterstützt, die das direkte Hochladen von Cisco Geräten aus zu Servicetickets ermöglichen.

Unterstützte Protokolle

Tabelle 2 fasst die von CXD unterstützten Protokolle zusammen. Es ist erwähnenswert, dass unabhängig vom verwendeten Protokoll keine Begrenzung für die Größe der hochgeladenen Datei festgelegt ist.

Tabelle 2. Von CXD unterstützte Protokolle

Name	Protokoll/Port	Verschlüsselt	Datenkanal-Ports	Hinweise
SFTP (Secure File Transfer Protocol)	TCP/22	Ja	–	
Secure Copy Protocol (SCP)	TCP/22	Ja	–	
Hypertext Transfer Protocol über SSL (HTTPS)	TCP/443	Ja	–	Benutzer- und Anwendungsschnittstellen verfügbar*
File Transfer Protocol über SSL (FTPS) implizit	TCP/990	Ja	30000-40000	Firewalls können FTPS nicht überprüfen, da der Steuerungskanal verschlüsselt ist. Daher muss die Firewall ausgehende Verbindungen zum gesamten Datenkanal-Portbereich zulassen.
File Transfer Protocol über SSL (FTPS) explizit	TCP/21	Ja**	30000-40000	
File Transfer Protocol (FTP)	TCP/21	Nein	30000-40000	• Cisco empfiehlt die Verwendung von FTP nicht, da das Protokoll keine Verschlüsselung unterstützt. Falls das Protokoll verwendet werden muss, sollten die Daten vor der Übertragung verschlüsselt werden. • Firewalls müssen den FTP-Datenverkehr überprüfen, damit Datenkanäle ordnungsgemäß eingerichtet werden können. Wenn FTP nicht im gesamten Netzwerk überprüft

				wird, müssen Firewalls ausgehende Verbindungen zum gesamten Datenkanal-Portbereich zulassen.

* Details zur Verwendung der PUT-API und des Python-Beispielcodes werden später in diesem Dokument aufgeführt.
** Der Modus "FTPS Explicit" erfordert, dass der Client mit dem Befehl "AUTH TLS" explizit TLS-Aushandlungen anfordert, bevor er sich anmeldet.

CXD-Upload-Token

CXD erstellt eindeutige Upload-Token pro Serviceticket. Für die Authentifizierung des Dienstes und das anschließende Hochladen von Dateien zum Serviceticket wird die Serviceticketnummer und das Token verwendet.

Hinweis: Das Token ist nur für den Upload bestimmt und ermöglicht dem Benutzer nicht, auf Ticket-Dateien oder sogar Dateien zuzugreifen, die gerade hochgeladen werden. Wenn der Benutzer die Ticket-Dateien anzeigen möchte, kann dies nur im SCM erfolgen.

Abrufen des Upload-Tokens für ein Serviceticket

Verwenden von SCM

Wenn ein Serviceticket geöffnet wird, generiert CXD automatisch ein Upload-Token und fügt einen Hinweis in das Serviceticket ein, welches das Token und einige Details zur Verwendung des Diensts enthält.

Um das Upload-Token abzurufen, führen Sie die folgenden Schritte aus:

Schritt 1 Melden Sie sich beim SCM an.

Schritt 2 Öffnen Sie das Ticket, für das Sie das Upload-Token abrufen möchten.

Schritt 3 Klicken Sie auf die Registerkarte Anhänge.

Schritt 4 Klicken Sie aufToken generieren. Sobald das Token generiert wurde, wird es neben der Schaltfläche "Token generieren" angezeigt.

Hinweise:

- Der Benutzername ist immer die Serviceticketnummer. Die Begriffe "Kennwort" und "Token" beziehen sich auf das Upload-Token, das als Kennwort verwendet wird, wenn Sie von CXD zu dessen Eingabe aufgefordert werden.
- Die Notiz wird innerhalb von wenigen Minuten nach der Erstellung des Servicetickets automatisch angehängt. Wenn der Benutzer die Notiz nicht finden kann, kann er sich an den Serviceticket-Verantwortlichen wenden und das Token manuell generieren lassen.
- Diese Methode soll in naher Zukunft geändert werden. Stellen Sie sicher, dass Sie diese Dokumentation für Updates erneut lesen.

Verwenden der ServiceGrid-API

Kunden, die die ServiceGrid-API nutzen, können das Token mithilfe der GetUploadCredentials-API programmatisch abrufen.

Hinweis: Zum Aufrufen einer Cisco ServiceGrid-API ist ein Auth-Token erforderlich. Weitere Informationen zum Abrufen eines Authentifizierungstokens finden Sie in der Cisco ServiceGrid-Dokumentation.

HTTP-Methode: POST

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

Header:

Tabelle 3: ServiceGrid-GetUploadCredentials-API-Header

Wichtigste	Typ	Wert	Mandatory (Obligatorisch)
Inhaltstyp	String	application/json	Ja
Autorisierung	String	Träger <Auth Token>	Ja

Nachrichtentext:

Tabelle 4: ServiceGrid-GetUploadCredentials-API - Body

Wichtigste	Typ	Wert	Mandatory (Obligatorisch)
Benutzername	String	Cisco.com-Benutzername, der autorisiert ist, einen Datei-Upload zum Serviceticket durchzuführen	Ja
E-Mail	Zeichenfolge (E-Mail-Format)	E-Mail-Adresse zum cisco.com-Benutzernamen	Ja

Hochladen von Dateien auf CXD

Verwenden von Desktop-Clients

Normalerweise muss der Benutzer je nach gewünschtem Protokoll einen Client verwenden, um eine Verbindung zu cxd.cisco.com herzustellen, sich mit der Serviceticketnummer als Benutzername und dem Upload-Token als Kennwort zu authentifizieren und schließlich eine oder mehrere Dateien hochzuladen.

Je nach Protokoll und Client können die Benutzerschritte unterschiedlich sein. Es wird immer empfohlen, die Dokumentation des Clients für weitere Details zu lesen.

Direkt von einem Cisco Gerät

Alle Cisco Geräte verfügen über integrierte Dateiübertragungs-Clients, die normalerweise mit dem Befehl "copy" oder "redirect" verwendet werden. Cisco Geräte, die auf einer Linux-Distribution ausgeführt werden, unterstützen normalerweise eine oder mehrere SCP- oder SFTP-Protokolle und Curl für SCP-, SFTP- und HTTPS-Integrationen.

API für Datei-Upload

Die Datei-Upload-API verwendet das HTTP-PUT-Verb, um Dateien auf CXD hochzuladen. Für eine maximale Kompatibilität und Einfachheit der Integration wird die API einfach gehalten.

HTTP-Methode: PUT

URL: https://cxd.cisco.com/home/<Name der Zieldatei>

Header:

Tabelle 5: API-Header für CXD-Datei-Uploads

Wichtigste	Typ	Wert	Mandatory (Obligatorisch)
Autorisierung	String	Grundlegende Zeichenfolge für HTTP-Authentifizierung	Ja

Der Text besteht aus den Dateidaten. Es gibt keine Felder oder Formulare, was die Serviceanfrage sehr einfach macht.

Python-Beispielcode für die Verwendung der PUT-API

Beachten Sie, dass der folgende Code davon ausgeht, dass die Datei in demselben Pfad gespeichert wird, von dem aus sie ausgeführt wird.

```
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")
```

Uploads von E-Mail-Dateianhängen

Wenn SCM, der Ticket-Datei-Uploader und Customer eXperience Drive nicht für Sie funktionieren, können Sie Dateien alternativ als E-Mail-Anhang hochladen. Beachten Sie, dass diese Methode *grundlegend unsicher* ist und die Datei oder die Kommunikationssitzung, die für die Übertragung der Datei zwischen dem Kunden und Cisco verwendet wird, nicht verschlüsselt ist. Es ist Sache des Kunden, Dateien explizit zu verschlüsseln, bevor sie als E-Mail-Dateianhänge hochgeladen werden. Als zusätzliche Sicherheitspraxis sollten vertrauliche Informationen wie Kennwörter verschleiert oder aus Konfigurationsdateien oder Protokollen entfernt werden, die über einen unsicheren Kanal gesendet werden. Weitere Informationen finden Sie unter Verschlüsseln von

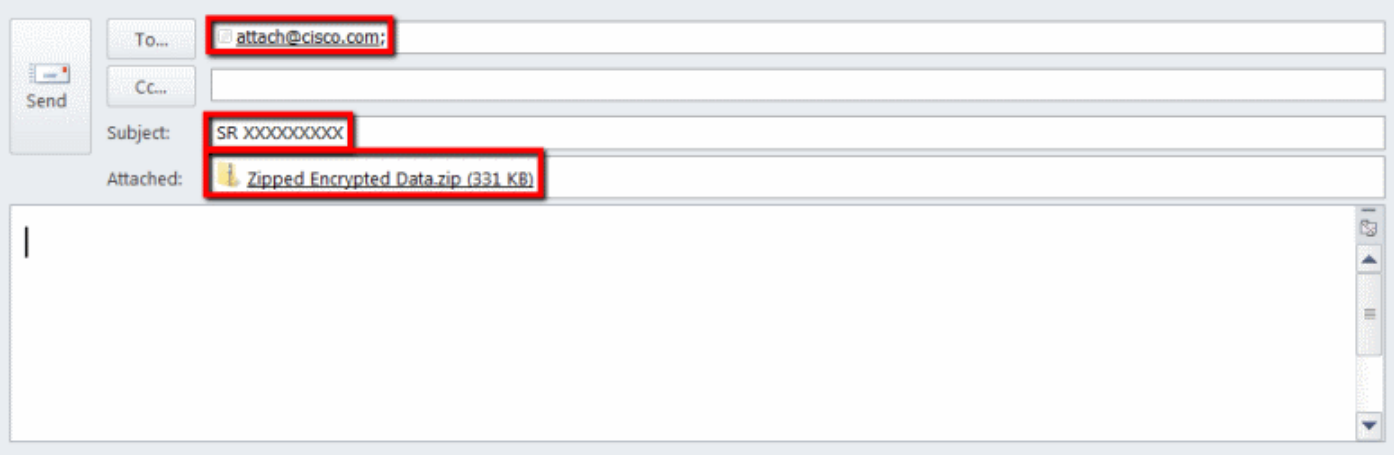
Dateien.

Nachdem die Dateien verschlüsselt wurden, laden Sie zusätzliche Informationen und Dateien hoch, indem Sie sie per E-Mail-Nachricht an attach@cisco.com senden. Geben Sie hierzu in der Betreffzeile die Ticketnummer an, z. B. Betreff = Ticket xxxxxxxxx.

Bei Versand per E-Mail ist die Größe der Anhänge auf 20 MB begrenzt. Anhänge, die mit E-Mail-Nachrichten gesendet werden, werden während der Übertragung nicht verschlüsselt, aber umgehend mit dem angegebenen Ticket verknüpft und in verschlüsselter Form gespeichert.

Hängen Sie die Datei an eine E-Mail-Nachricht an und senden Sie diese an attach@cisco.com, wie in Abbildung 10 gezeigt.

Abbildung 9: Datei senden



Der obige Screenshot zeigt eine E-Mail in Microsoft Outlook mit verschlüsseltem ZIP-Dateianhang, der korrekten Zieladresse und einem Betreff im richtigen Format. Andere E-Mail-Clients sollten dieselbe Funktionalität bereitstellen und genauso gut wie Microsoft Outlook durchführen.

Zum Seitenanfang

Verschlüsseln von Dateien

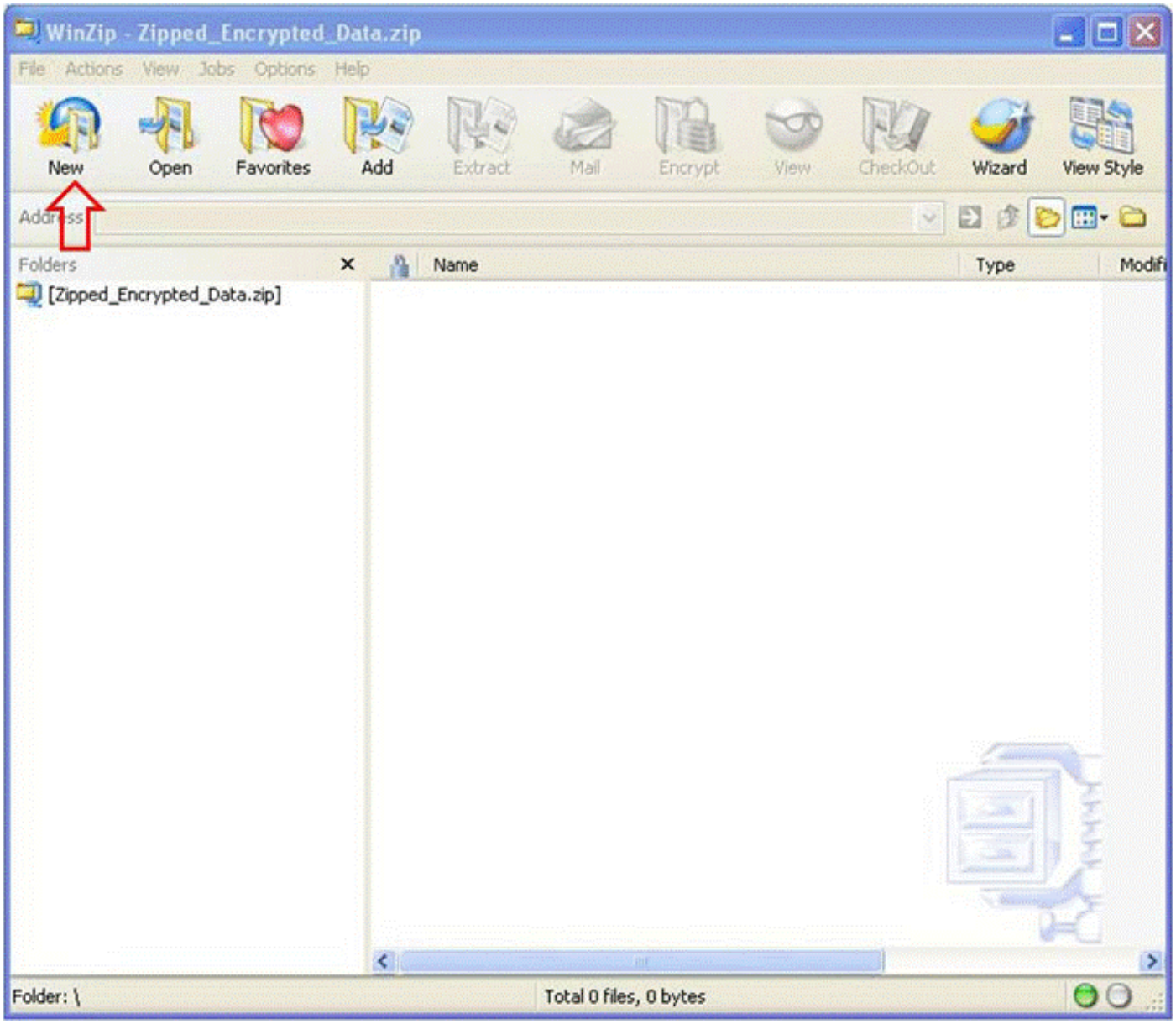
Die folgenden Beispiele zeigen, wie Sie Dateien mithilfe von drei der vielen verfügbaren Optionen wie WinZip, Linux-TAR- und OpenSSL-Befehlen sowie Linux-GZIP und GnuPG verschlüsseln. Ein starkes Verschlüsselungsverfahren wie AES-128 sollte verwendet werden, um die Daten ordnungsgemäß zu schützen. Wenn Sie ZIP verwenden, muss eine Anwendung genutzt werden, die AES-Verschlüsselung unterstützt. Ältere Versionen von ZIP-Anwendungen unterstützen ein symmetrisches Verschlüsselungssystem, das nicht sicher ist und nicht verwendet werden sollte.

Verschlüsseln von Dateien mit WinZip

In diesem Abschnitt wird gezeigt, wie Dateien mithilfe der WinZip-Anwendung verschlüsselt werden. Andere Anwendungen sollten die gleiche Funktionalität bereitstellen und ebenso gut wie WinZip funktionieren.

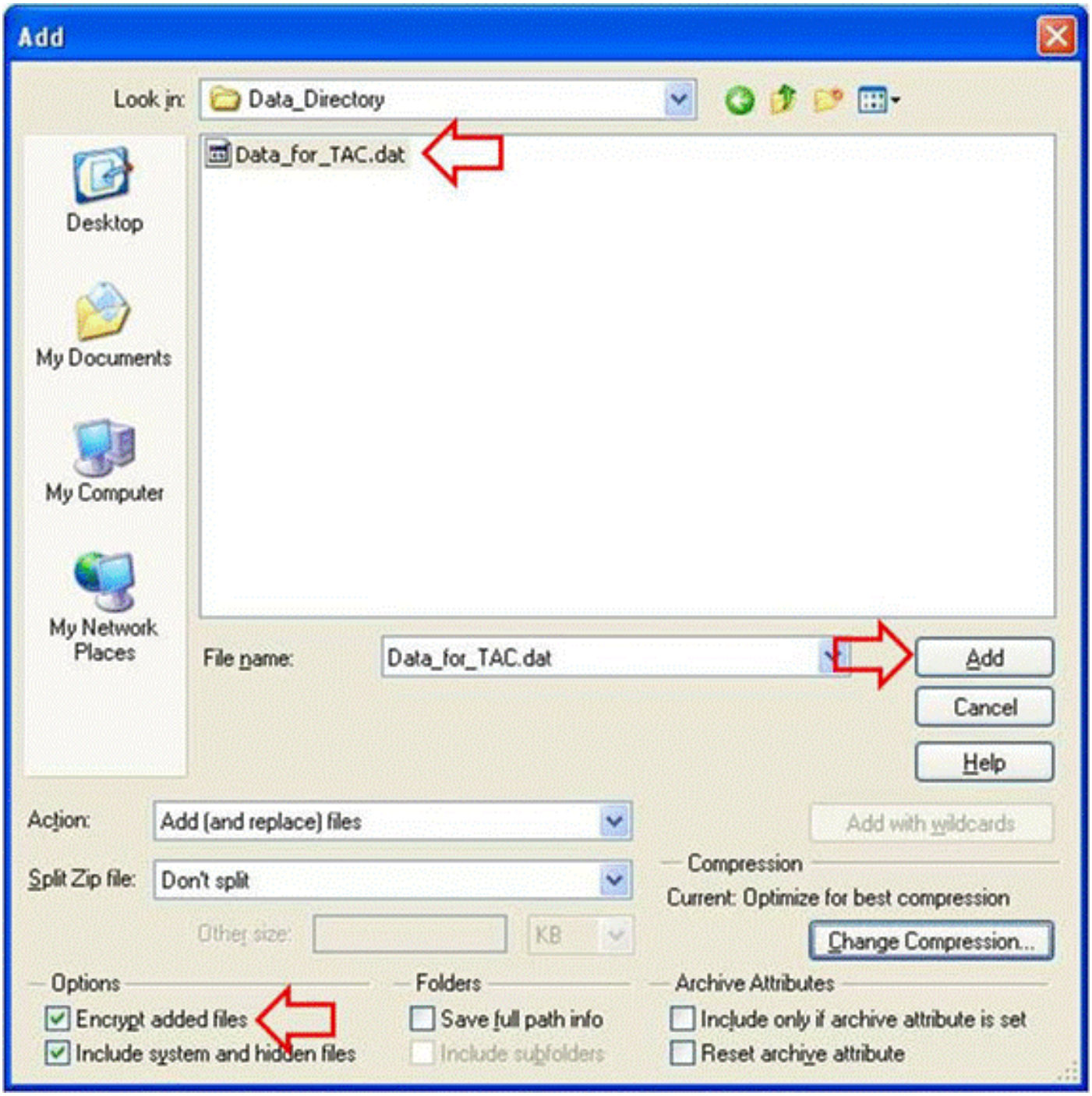
Schritt 1 Erstellen Sie eine ZIP-Archivdatei, wie in Abbildung 11 gezeigt. Klicken Sie in der WinZip-GUI auf **Neu und folgen Sie den Anweisungen im Menü, um eine korrekt benannte, neue ZIP-Archivdatei zu erstellen.** Die neu erstellte ZIP-Archivdatei wird angezeigt.

Abbildung 10: Erstellen eines ZIP-Archivs



Schritt 2 Fügen Sie die hochzuladenden Dateien der ZIP-Archivdatei hinzu und wählen Sie die Option Hinzugefügte Dateien verschlüsseln aus, wie in Abbildung 12 gezeigt. Klicken Sie im Hauptfenster von WinZip auf **Hinzufügen und wählen Sie die Dateien aus, die Sie hochladen möchten.** Wählen Sie zudem die Option **Hinzugefügte Dateien verschlüsseln aus.**

Abbildung 11: Verschlüsseln hinzugefügter Dateien



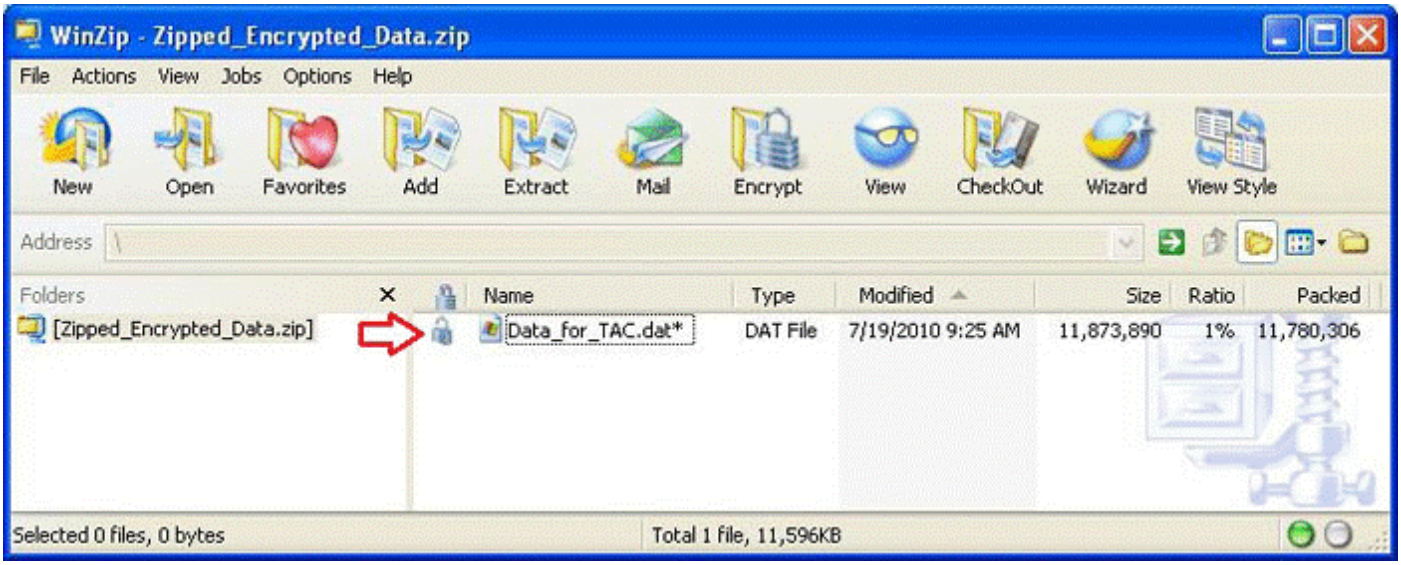
Schritt 3 Verschlüsseln Sie die Datei mit dem AES-Verschlüsselungsverfahren und einem sicheren Kennwort, wie in Abbildung 13 gezeigt:

1. Klicken Sie im Dateiauswahlfenster auf **Hinzufügen , um das Fenster Verschlüsseln zu öffnen.**
2. Erstellen Sie im Fenster **Verschlüsseln ein angemessen sicheres Kennwort.** Das Kennwort wird der für das Ticket zuständigen Person beim Kundensupport mitgeteilt, wie im Abschnitt Weitergabe des Kennworts an den TAC-Kundensupporttechniker erläutert.
3. Wählen Sie eine der AES-Verschlüsselungsmethoden aus.
4. Klicken Sie auf **OK, um die Dateien zu verschlüsseln und das Hauptfenster von WinZip anzuzeigen.**

Abbildung 12: Verschlüsseln der Datei

Schritt 4 Überprüfen Sie, ob die Datei verschlüsselt ist, wie in Abbildung 14 gezeigt.
Verschlüsselte Dateien werden mit einem Sternchen gekennzeichnet, das auf den Dateinamen folgt, oder mit einem Schlosssymbol in der Spalte "Verschlüsselung".

Abbildung 13: Überprüfen der Verschlüsselung



Verschlüsseln von Dateien mit TAR und OpenSSL

In diesem Abschnitt wird gezeigt, wie Dateien mithilfe der Linux-Befehlszeile **TAR und mit OpenSSL-Befehlen verschlüsselt werden.** Andere Archivierungs- und Verschlüsselungsbefehle sollten die gleiche Funktionalität bieten und unter Linux oder UNIX ebenso gut funktionieren.

Schritt 1 Erstellen Sie ein TAR-Archiv der Datei und verschlüsseln Sie es mit OpenSSL mithilfe des AES-Verschlüsselungsverfahrens und eines sicheren Kennworts, wie im folgenden Beispiel gezeigt. Die Befehlsausgabe zeigt die kombinierte TAR- und OpenSSL-Befehlssyntax, um die Dateien mithilfe des AES-Verschlüsselungsverfahrens zu verschlüsseln.

```
[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
```

Verschlüsseln von Dateien mit GZIP und GnuPG

In diesem Abschnitt wird gezeigt, wie Dateien mithilfe der Linux-Befehlszeile GZIP und mit GnuPG-Befehlen verschlüsselt werden. Andere Archivierungs- und Verschlüsselungsbefehle sollten die gleiche Funktionalität bieten und unter Linux oder UNIX ebenso gut funktionieren. Die Befehlsausgabe zeigt, wie die GZIP- und GPG-Befehlssyntax verwendet wird, um die Dateien mithilfe des AES-Verschlüsselungsverfahrens zu verschlüsseln.

Schritt 1 Komprimieren Sie die Datei mit GZIP:

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

Schritt 2 Verschlüsseln Sie die Datei über GnuPG mithilfe des AES-Verschlüsselungsverfahrens und eines sicheren Kennworts:

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

Schritt 3 Geben Sie ein sicheres Kennwort ein, und bestätigen Sie es an der Eingabeaufforderung der Passphrase:

```
Passphrase eingeben:
Passphrase wiederholen:
```

Zum Seitenanfang

Weitergabe des Kennworts an den TAC-Kundensupporttechniker

Geben Sie beim Verschlüsseln von Anhängen das Verschlüsselungskennwort an den Kundensupporttechniker weiter, der für das Ticket zuständig ist. Verwenden Sie als bewährtes Verfahren eine andere Methode als diejenige, die zum Hochladen der Datei verwendet wurde. Wenn Sie eine E-Mail-Nachricht oder FTP zum Hochladen der Datei verwendet haben, geben Sie das Kennwort außerhalb der Kommunikationsform z. B. per Telefon oder per SCM-Ticket-Update weiter.

Aufbewahrung von Kundendateien

Solange ein Ticket geöffnet ist und bis zu 18 Monate nach Schließen eines Tickets, sind alle Dateien für autorisierte Cisco Mitarbeiter sofort über das Ticketnachverfolgungssystem zugänglich. 18 Monate nach Schließung des Tickets werden die Dateien möglicherweise in eine Archivierungsspeicherinstanz verschoben, um Platz zu sparen. Sie werden aber nicht aus dem

Ticketverlauf gelöscht.

Ein autorisierter Kundenkontakt kann jederzeit ausdrücklich beantragen, dass eine bestimmte Datei aus einem Ticket gelöscht wird. Cisco kann diese Datei dann löschen und eine Anmerkung zum Ticket hinzufügen, um Folgendes zu dokumentieren: die Partei, welche die Datei gelöscht hat, den Zeit- und Datumsstempel und den Namen der gelöschten Datei. Nachdem eine Datei auf diese Weise gelöscht wurde, kann sie nicht mehr wiederhergestellt werden.

Dateien, die in den FTP-Ordner des TAC hochgeladen werden, werden vier Tage lang aufbewahrt. Der für das Ticket zuständige Kundensupporttechniker muss informiert werden, wenn eine Datei in diesen Ordner hochgeladen wird. Der Kundensupporttechniker sollte die Dateien innerhalb von vier Tagen sichern, indem er sie an das Ticket anhängt.

Zum Seitenanfang

Zusammenfassung

Es gibt mehrere Optionen, um Informationen für das Cisco TAC hochzuladen und es so bei der Lösung von Tickets zu unterstützen. SCM und das HTML5-Upload-Tool von Cisco bieten beide sichere Uploads über einen Browser, während CXD Uploads über einen Browser, eine Web-API und mehrere Protokolle bietet, die von verschiedenen Clients und Cisco Geräten unterstützt werden.

Wenn Sie weder SCM, noch das HTML 5-Datei-Upload-Tool von Cisco oder ein von CXD unterstütztes Protokoll nutzen können, das nicht FTP als Datei-Upload-Methode verwendet, gibt es noch weniger bevorzugte Datei-Upload-Optionen wie FTP (mit Verwendung von CXD) oder das Senden einer E-Mail-Nachricht an die Adresse attach@cisco.com. Wenn Sie eine dieser Optionen verwenden, empfehlen wir Ihnen dringend, Ihre Dateien vor der Übertragung zu verschlüsseln. Weitere Informationen finden Sie unter Verschlüsseln von Dateien. Sie sollten ein sicheres Kennwort verwenden und dieses an den Kundensupporttechniker weitergeben, z. B. außerhalb der Kommunikationsform per Telefon oder SCM-Ticket-Update.

Solange ein Ticket geöffnet ist und bis zu 18 Monate nach Schließen eines Tickets, sind alle Dateien für autorisierte Cisco Mitarbeiter sofort über das Ticketnachverfolgungssystem zugänglich.

- Nach 18 Monaten können die Dateien in den Archivierungsspeicher verschoben werden.
- Ein autorisierter Kundenkontakt kann jederzeit ausdrücklich beantragen, dass eine bestimmte Datei aus einem Ticket gelöscht wird.
- Dateien im FTP-Ordner werden nur vier Tage lang aufbewahrt.

Zusätzliche Informationen

- Zugang zu Cisco Technical Services
- Weltweiter Kontakt zum Cisco Support
- Ressourcenleitfaden zu Cisco Technical Services
- Cisco Security Blog - NCSAM-Tipp #3: Ein sicheres Passwort
- Cisco Conferencing-Produkte
- Der GNU Privacy Guard
- Das OpenSSL-Projekt
- WinZip

Dieses Dokument ist Teil von Cisco Security Research and Operations.

Zum Seitenanfang

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.