Uploaden van klantbestanden naar Cisco Technical Assistance Center

Inhoud

Overzicht

Klanten zijn zeer belangrijk voor Cisco. Daarom willen wij hun problemen tijdig aanpakken en oplossen. Een manier waarop een klant kan assisteren in het proces is door de relevante bestanden naar het Cisco Technical Assistance Center (TAC) te sturen voor review. TAC Customer Support Engineers gebruiken deze bestanden om klantproblemen op te helpen lossen en Cisco biedt meerdere opties om informatie naar Cisco TAC te uploaden. De klant kan de optie kiest die past bij zijn vereisten. Een aantal van deze opties is minder veilig en leidt tot zekere inherente risico's, en elke optie kent beperkingen die de klant in overweging moet nemen voordat deze een gepaste uploadoptie kiest. Tabel 1 bevat de beschikbare uploadopties met details over de encryptiemogelijkheden voor bestanden, aanbevolen maximale bestandsgrootte en andere relevante informatie.

Tabel 1. Beschikbare uploadopties

Beschikbare opties (in voorkeursvolgorde)	Bestanden worden versleuteld	Bestanden worden versleuteld	Aanbevolen maximale bestandsgrootte

		tijdens verzending	tijdens opslag	
Support Case Manager (SCM)	Hoe	Ja	Ja	250 GB
Case File Uploader	Hoe	Ja	Ja	250 GB
Customer eXperience Drive	Hoe	Ja*	Ja	Zonder limiet
E-mail naar attach@cisco.com	Hoe	Nee**	Ja	20 MB of minder, afhankelijk van de limieten van de mailserver van de klant

*Van toepassing op alle protocollen behalve FTP. Cisco raadt bij gebruik van FTP sterk aan dat de gegevens worden versleuteld voordat ze worden geüpload.
**De klant moet versleutelen voor verzending. Verzending vanaf het netwerk of door de e-mailprovider van de klant wordt wel of niet versleuteld tijdens verzending. Beveiligde verzending is alleen gegarandeerd vanaf het punt waar de e-mail/bijlage het Cisco-netwerk bereikt.

Bestanden uploaden via Support Case Manager

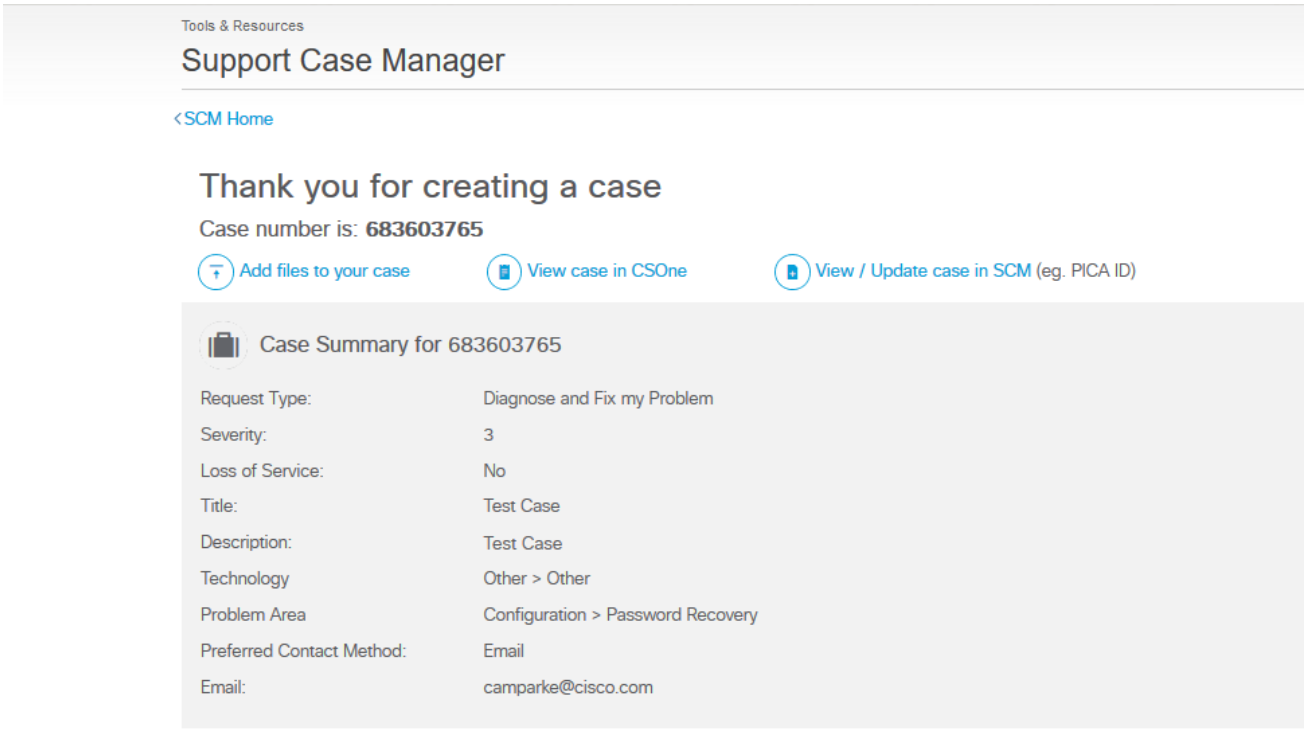
De Support Case Manager (SCM) methode voor het uploaden van bestanden heeft de voorkeur en is de best beveiligde optie voor het uploaden van bestanden naar cases. Bestanden die via deze optie worden verstuurd zijn versleuteld tijdens verzending en beperkt tot een grootte van 250 GB. Het communicatiekanaal tussen het apparaat van de klant en Cisco is versleuteld. Bestanden die met SCM worden geüpload worden direct aan de bijbehorende case gekoppeld en in een versleuteld format opgeslagen.

Bestand uploaden bij indienen van case

Volg deze stappen op het case-bevestigingsscherm. Voor gedetailleerdere instructies hoe u een case kunt maken of beheren op SCM, zie SCM help.

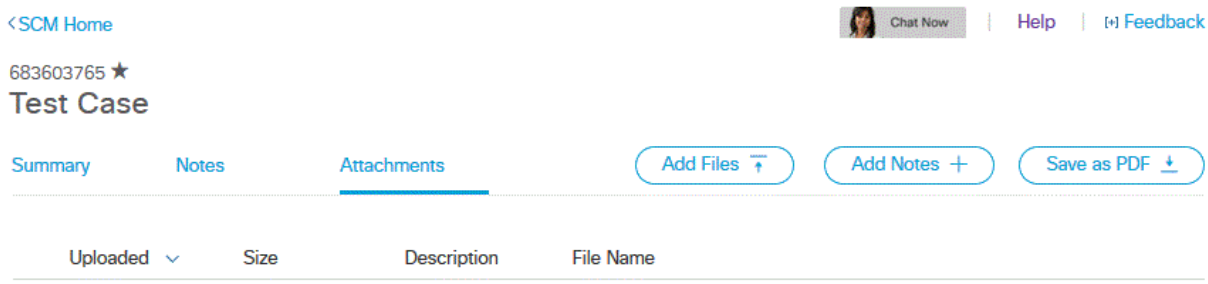
Stap 1 Kies de knop Add files to your case (afbeelding 1).

Afbeelding 1. SCM: Voeg bestanden toe aan uw case



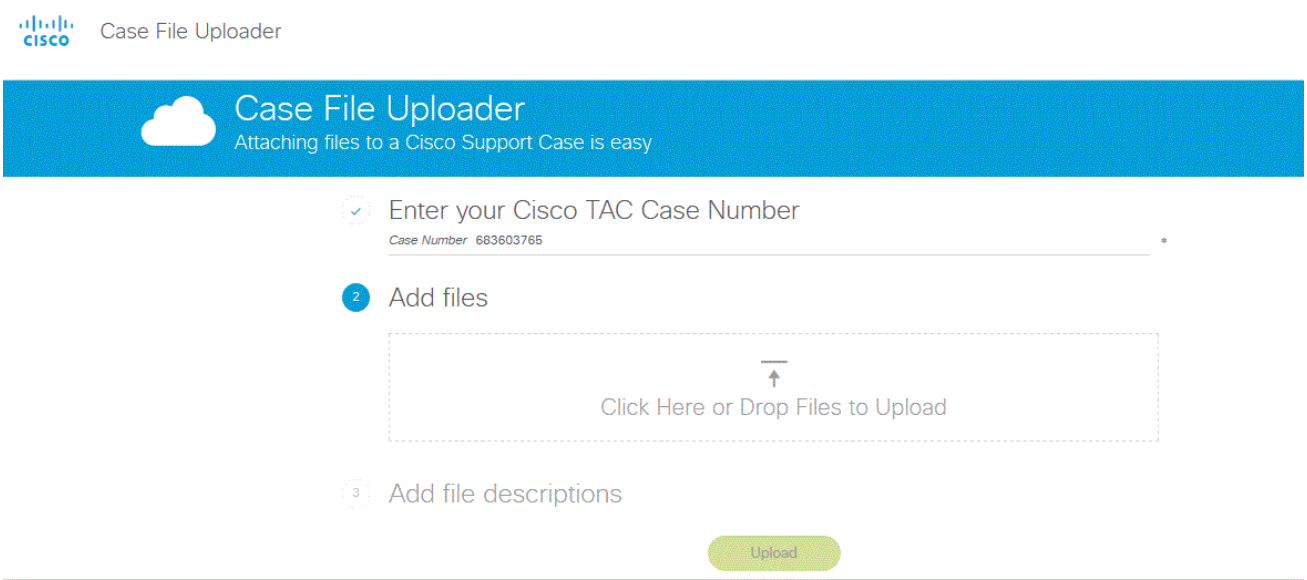
Stap 2 Kies op het tabblad Attachments de knop Add Files (afbeelding 2).

Afbeelding 2. SCM: tabblad Attachments



U wordt naar de tool Case File Uploader geleid. De case die u aanmaakt zal vooraf worden ingevuld in de tool (afbeelding 3). Ga verder naar paragraaf Case File Uploader stap 3.

Afbeelding 3. Case File Uploader: scherm voor slepen en neerzetten van bestanden



Bestand uploaden voor een bestaande case

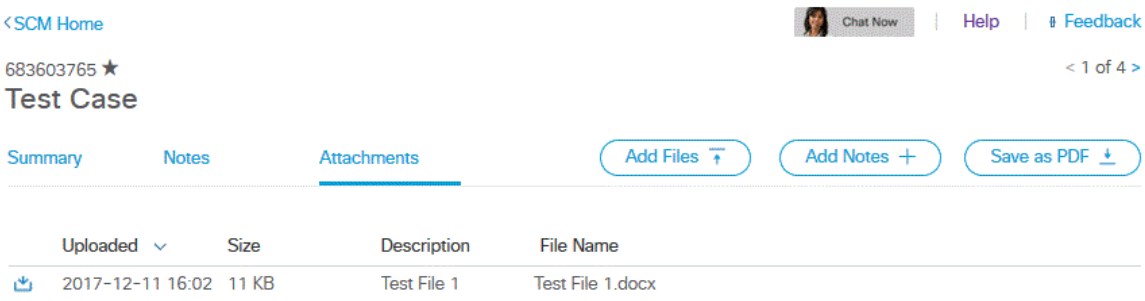
Nadat een case is ingediend kunt u de optionele informatie updaten of wijzigen.

Stap 1 Meld u aan bij SCM.

Stap 2 Klik om een case te openen en te editen op het casenummer of de casetitel in de lijst. De pagina met casedetails wordt geopend.

Stap 3 Bovenaan de pagina met casedetails staan drie tabbladen: **Samenvatting**, **opmerkingen** en **bijlagen**. Naast de tabbladen staat een aantal werkbalkknoppen: **Bestanden toevoegen**, **Opmerkingen toevoegen** en **als PDF-bestand opslaan**. Klik op **Add Files om een bestand te selecteren en het als een bijlage naar de case te uploaden (afbeelding 4).**

Afbeelding 4. Tabblad Attachments van SCM



U wordt naar de tool Case File Uploader geleid. De case die u aanmaakt zal vooraf worden ingevuld in de tool (afbeelding 3). Ga verder naar paragraaf Case File Uploader stap 3.

Naar boven

Case File Uploader

Een andere beveiligde methode om bestanden te uploaden naar een case is de Case File Uploader. Deze tool is vergelijkbaar met SCM in die zin dat bestanden die via deze optie worden

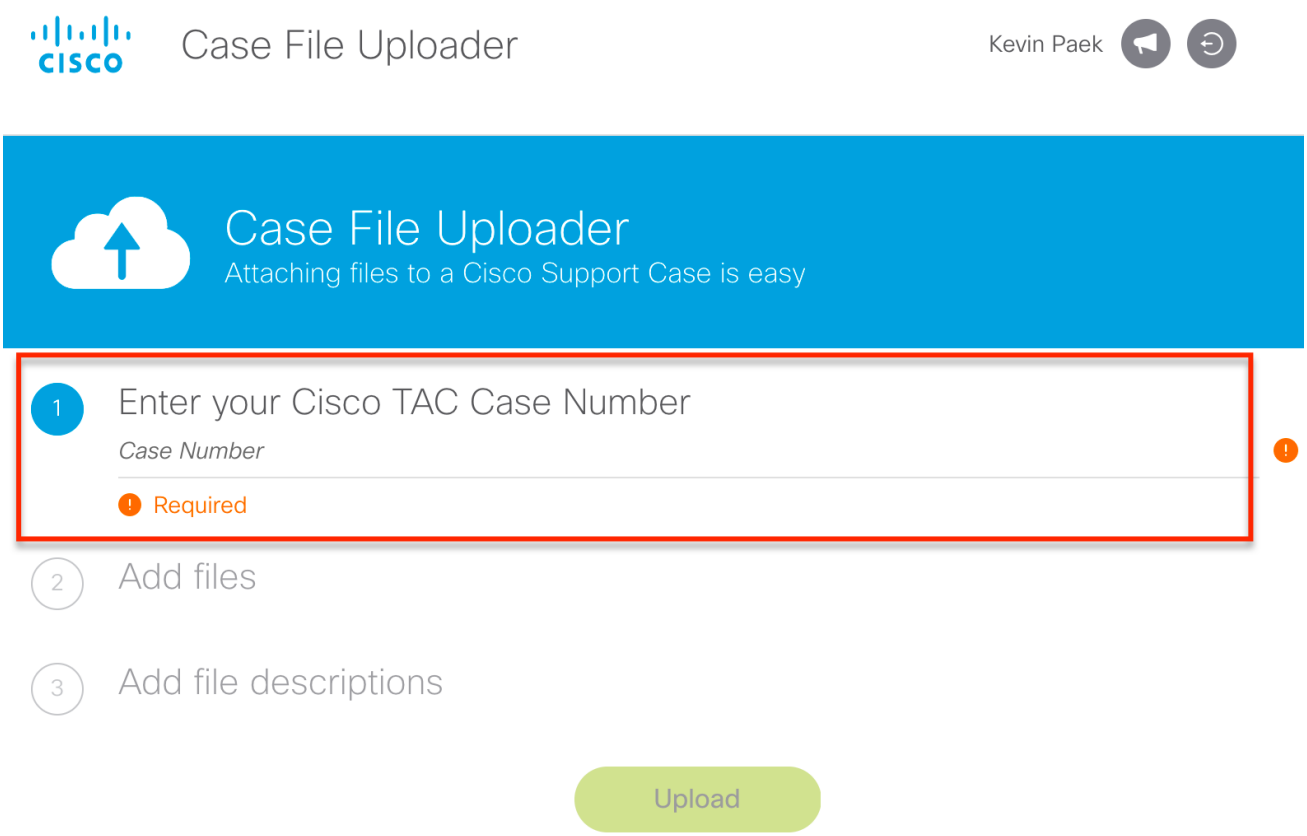
verstuurd zijn versleuteld tijdens verzending en beperkt tot een grootte van 250 GB. Het communicatiekanaal tussen het apparaat van de klant en Cisco is versleuteld. Bestanden die met Case File Uploader worden geüpload worden direct aan de bijbehorende case gekoppeld en in een versleuteld format opgeslagen. Doorloop de volgende stappen om een bestand toe te voegen met behulp van deze tool.

Opmerking: als u ontdekt dat u met de tool geen bestand naar uw case kunt uploaden, is het casenummer dat u hebt ingevoerd ongeldig of hebt u niet de vereiste rechten om bestanden toe te voegen. Om bestanden naar een case te uploaden moet uw profiel bij cisco.com verbonden zijn aan het contract waar de case voor is geopend. U kunt een servicecontract aan uw profiel toevoegen met de Cisco Profile Manager of u kunt dit voor u laten doen door uw Service Access Management-beheerder. Als u verdere assistentie nodig hebt, neem dan contact op met het Cisco Technical Assistance Center.

Stap 1 Meld u aan bij Case File Uploader.

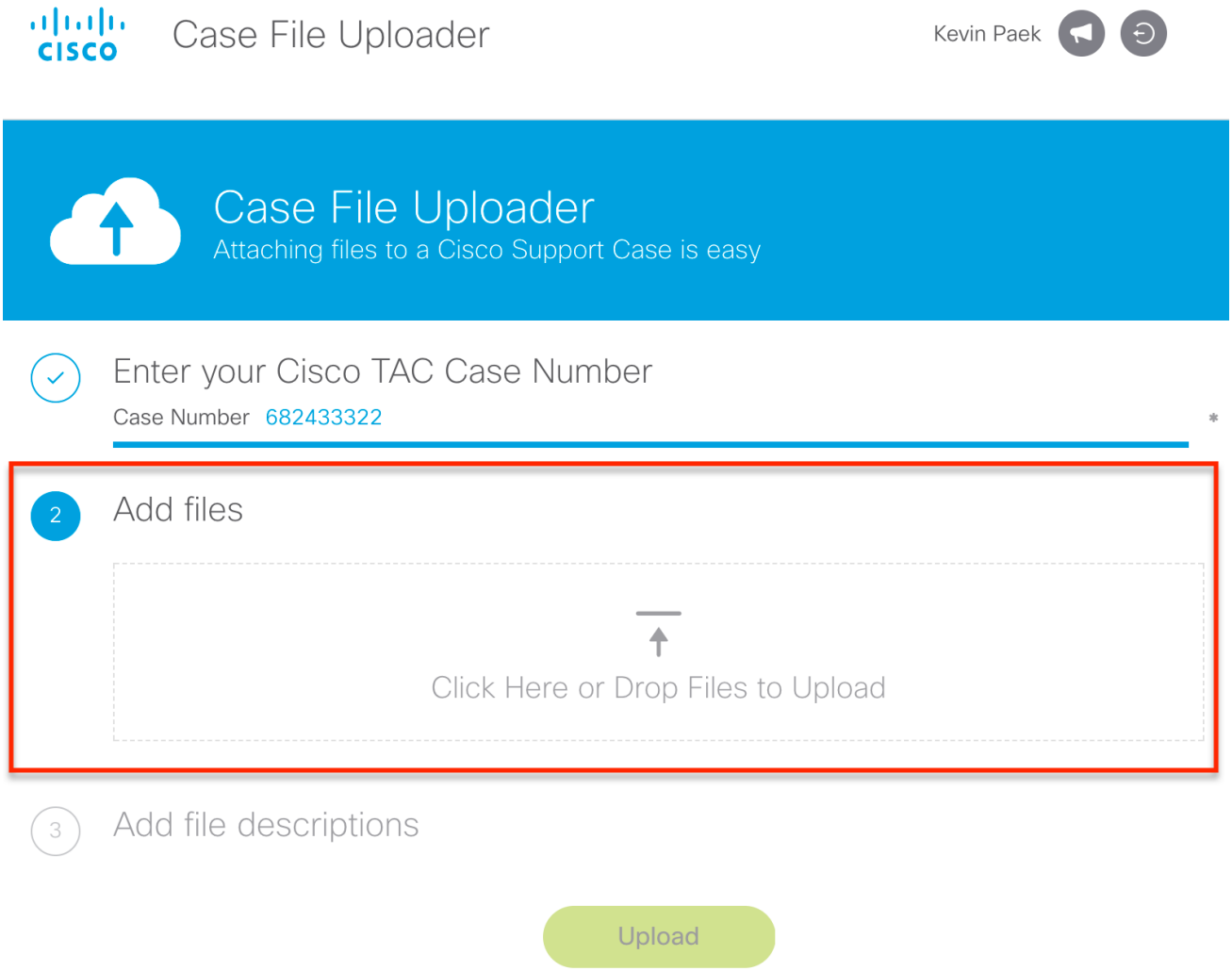
Stap 2 Voer in het daarvoor bestemde veld uw casenummer in (afbeelding 5).

Afbeelding 5. Scherm voor uploaden van casenummer



Stap 3 Voor het toevoegen van een bestand kunt u gebruikmaken van slepen en neerzetten of in het veld met stippelrand klikken om het te uploaden bestand te selecteren (afbeelding 6).

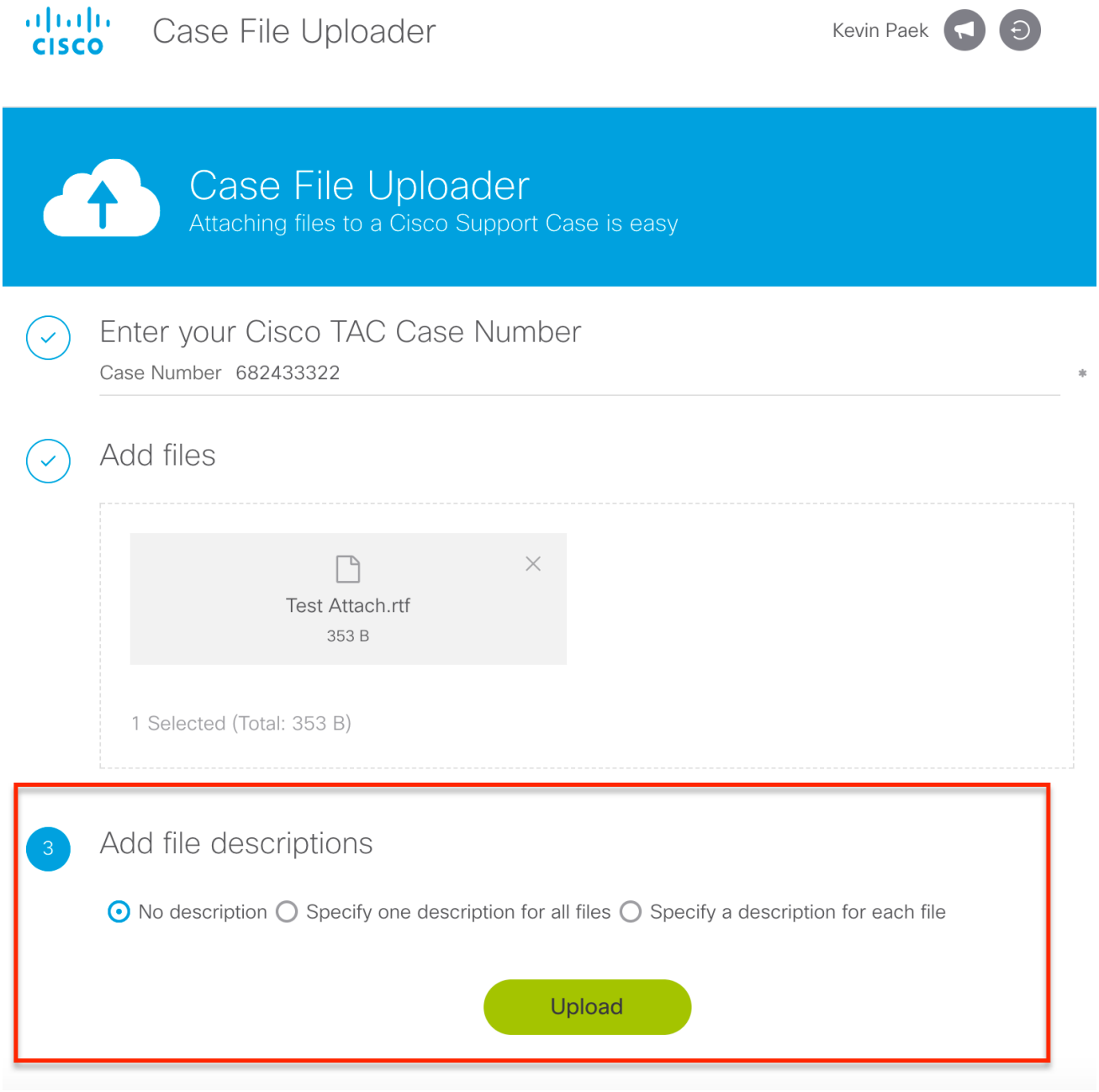
Afbeelding 6. Case File Uploader: scherm voor slepen en neerzetten van bestanden



Stap 4 **Na het kiezen van een bestand en als u geen omschrijving op hoeft te geven, klikt u op Upload**. Anders kunt u ervoor kiezen meer details toe te voegen met de andere opties. (Afbeelding 7). In de velden **Category** en **Description** kunt u meer informatie toevoegen over het bestand:

- Gebruik het veld **Category om een bijlagetype te selecteren.**
- Gebruik het veld **Description om een korte omschrijving van het bestand te geven.**

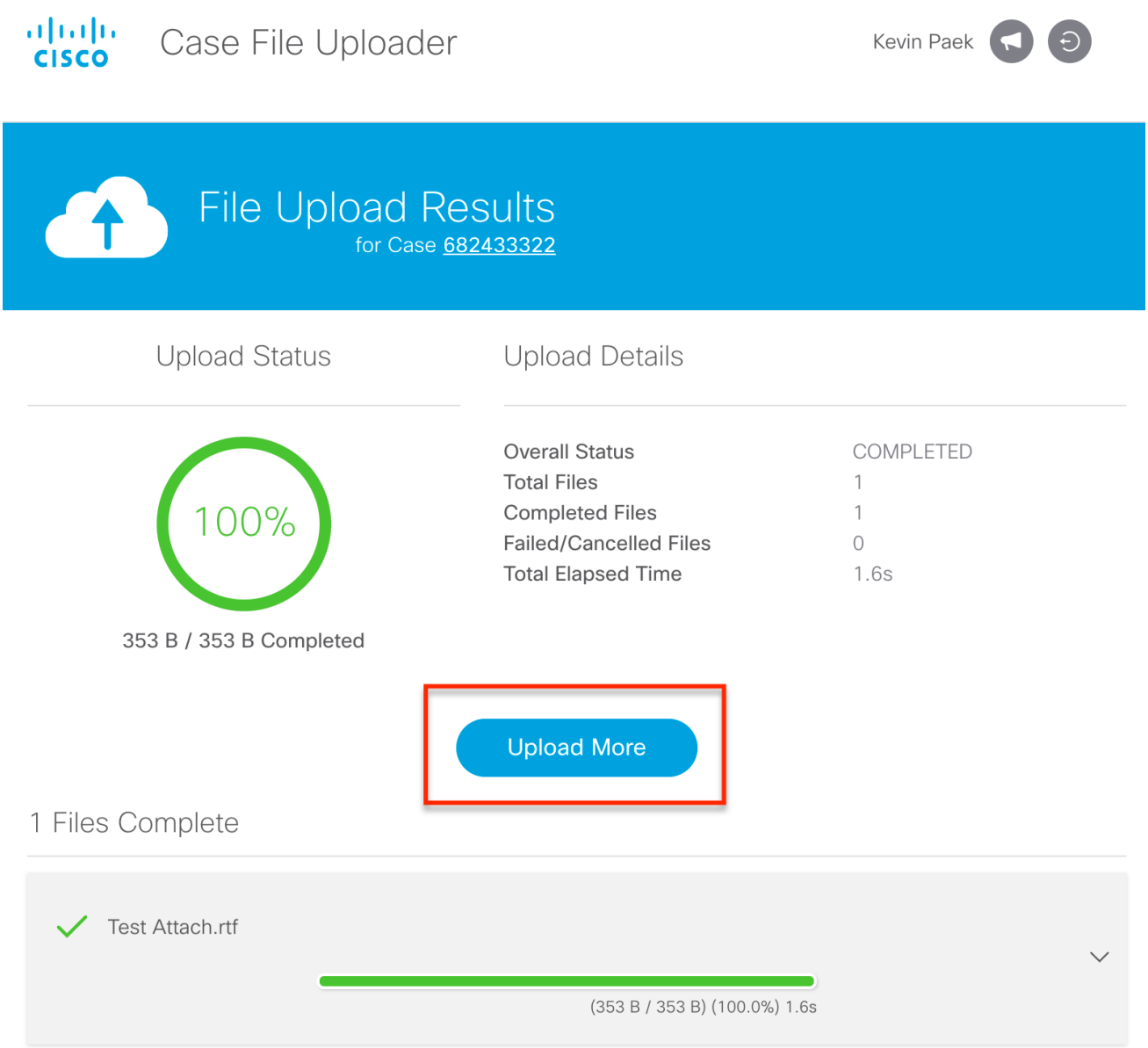
Afbeelding 7. Case File Uploader: Beschrijving van bestand invoeren



Stap 5 **Klik op Upload** om het bestand te uploaden.

Stap 6 **Het volgende scherm toont de status van het bestand.** Klik na het uploaden van het bestand op **Upload More (afbeelding 8) om extra bijlagen te uploaden.**

Afbeelding 8. Case File Uploader: scherm met uploadstatus



Naar boven

Customer eXperience Drive

Serviceoverzicht

De Customer eXperience Drive (CXD) is een multi-protocol service voor het uploaden van bestanden zonder limieten aan de geüploade bestandsgrootte. Hiermee kunnen Cisco-klanten met actieve serviceaanvragen (SR's) direct gegevens naar een case uploaden door unieke aanmeldingsgegevens te gebruiken die per SR gemaakt worden. De door CXD ondersteunde protocollen worden native ondersteund door Cisco-producten, wat het mogelijk maakt om direct van Cisco-apparaten naar SR's te uploaden.

Ondersteunde protocollen

Tabel 2 bevat een overzicht van door CXD ondersteunde protocollen. Ongeacht het gebruikte protocol is er geen limiet voor de grootte van het geüploade bestand.

Tabel 2. CXD-ondersteunde protocollen

Name	Protocol/poort	Versleuteld	Poorten voor gegevenskanalen	Opmerkingen
Secure File Transfer Protocol (SFTP)	TCP/22	Ja	N.v.t.	
Secure Copy Protocol (SCP)	TCP/22	Ja	N.v.t.	
Hyper-Text Transfer Protocol over SSL (HTTPS)	TCP/443	Ja	N.v.t.	Gebruikers- en toepassingsinterfaces beschikbaar*
File Transfer Protocol of SSL (FTPS) Impliciet	TCP/990	Ja	30000-40000	Firewalls kunnen FTPS niet inspecteren aangezien het controlekanaal is versleuteld. Daarom dient de firewall uitgaande connectiviteit toe te staan voor het gehele poortbereik voor gegevenskanalen.
File Transfer Protocol of SSL (FTPS) Expliciet	TCP/21	Ja**	30000-40000	
File Transfer Protocol (FTP)	TCP/21	Nee	30000-40000	• Cisco raadt het gebruik van FTP niet aan, aangezien het protocol geen encryptie ondersteunt. Als het moet worden gebruikt, moeten gegevens worden versleuteld voor verzending. • Firewalls moeten FTP-verkeer inspecteren zodat gegevenskanalen correct kunnen worden opgebouwd. Als FTP niet op het

				netwerk wordt geïnspecteerd, moeten de firewalls uitgaande connectiviteit toestaan voor het gehele poortbereik voor gegevenskanalen.

* Details over het gebruik van de PUT API en Python-voorbeeldcode komen later in dit document aan de orde.
** FTPS expliciete modus vereist dat de client expliciet vraagt om TLS-onderhandelingen met de code 'AUTH TLS' voordat de client probeert in te loggen.

CXD-uploadtoken

CXD maakt per SR unieke uploadtokens. Het SR-nummer en het token worden gebruikt als gebruikersnaam en wachtwoord ter verificatie voor de service en vervolgens om bestanden naar de SR te uploaden.

N.B.: De token is alleen voor het uploaden van bestanden en geeft de gebruiker geen toegang tot casebestanden of zelfs bestanden die op dit moment worden geüpload. Als de gebruiker casebestanden wil inzien, kan dat alleen in SCM.

Uploadtoken ophalen voor een SR

SCM gebruiken

Wanneer een SR is geopend, zal de CXD automatisch een uploadtoken genereren en een notitie maken in de SR waarin het token staat met enkele details over het gebruik van de service.

Voltooi de volgende stappen om een uploadtoken op te halen:

Stap 1 Meld u aan bij SCM.

Stap 2 Open de case waarvoor u het uploadtoken wilt hebben.

Stap 3 Klik op het tabblad Attachments.

Stap 4 Klik op Generate Token. Nadat het token is aangemaakt zal het worden getoond naast de knop Generate Token.

Opmerkingen:

- De gebruikersnaam is altijd het SR-nummer. De termen 'wachtwoord' en 'token' verwijzen naar het uploadtoken dat als wachtwoord wordt gebruikt wanneer daarom wordt gevraagd door CXD.
- De notitie wordt binnen een paar minuten nadat de SR is aangemaakt automatisch

toegevoegd. Als de gebruiker de notitie niet kan vinden, kan deze contact opnemen met de SR-eigenaar en kan het token handmatig aangemaakt worden.
- Deze methode zal in de nabije toekomst wijzigen. Zorg ervoor dat u deze documentatie opnieuw bezoekt voor updates.

ServiceGrid API gebruiken

Klanten die de ServiceGrid API gebruiken, kunnen het token ophalen met de GetUploadCredentials API.

N.B.: Een autorisatieteken is vereist voor het bellen van elke Cisco ServiceGrid API. Raadpleeg de Cisco ServiceGrid-documentatie voor details over het verkrijgen van een Auth-token.

HTTP-methode: POST

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

Kop:

Tabel 3: Kop voor ServiceGrid GetUploadCredentials API

Sleutel	Type	Waarde	Verplicht
Content-Type	String	application/json	Ja
Authorization	String	Bearer <Auth Token>	Ja

Tekst:

Tabel 4: Tekst voor ServiceGrid GetUploadCredentials API

Sleutel	Type	Waarde	Verplicht
username	String	Gebruikersnaam voor Cisco.com die is geautoriseerd om bestanden te uploaden naar de SR	Ja
email	String (e-mail indeling)	E-mailadres van de gebruikersnaam voor Cisco.com	Ja

Bestanden uploaden naar CXD

Desktopclients gebruiken

Over het algemeen hoeven gebruikers alleen maar een client te gebruiken, afhankelijk van het gewenste protocol, om verbinding te maken met cxd.cisco.com. Vervolgens kunnen ze verifiëren met het SR-nummer als gebruikersnaam en het uploadtoken als wachtwoord en daarna een of meer bestanden uploaden.

Afhankelijk van het protocol en de client kunnen stappen anders zijn voor gebruikers. Het is altijd

aan te bevelen om de documentatie van de client te raadplegen voor meer informatie.

Direct vanaf een Cisco-apparaat

Alle Cisco-apparaten hebben ingebouwde clients voor bestandsoverdracht, meestal gebruikt met een ‘copy’- of ‘redirect’-opdracht. Cisco-apparatuur die draait op Linux-systemen ondersteunt doorgaans een of meerdere ‘scp’, ‘sftp’ en ‘curl’ voor SCP-, SFTP- en HTTPS-integraties.

API voor uploaden van bestanden

De API voor het uploaden van bestanden gebruikt de HTTP-code PUT om bestanden naar CXD te uploaden. Voor de maximale compatibiliteit en een eenvoudige integratie is de API eenvoudig gehouden.

HTTP-methode: PUT

URL: https://cxd.cisco.com/home/<Bestandsnaam doel>

Koppen:

Tabel 5: Koppen voor CXD API voor uploaden van bestanden

Sleutel	Type	Waarde	Verplicht
Authorization	String	Basis HTTP-autorisatietekenreeks	Ja

De tekst bestaat uit de bestandsgegevens. Er zijn hier geen velden of formulieren, wat het verzoek erg eenvoudig maakt.

Python-voorbeeldcode voor gebruik van PUT API

Let op: de volgende code neemt aan dat het bestand op hetzelfde pad is opgeslagen als waarvandaan u het draait.

```
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 van bijlagen bij e-mail

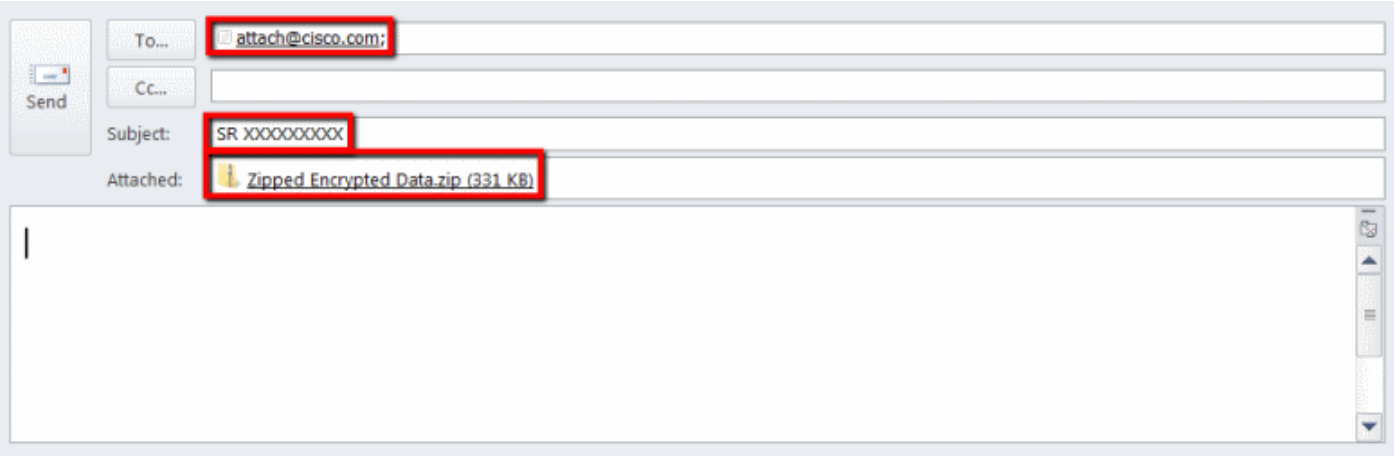
Als SCM, Case File Uploader en Customer eXperience Drive bij u niet werken, kunt u als alternatief een e-mailbijlage uploaden. Let op dat deze methode *fundamenteel onveilig* is en het bestand of de communicatiesessie voor het transport van het bestand tussen de klant en Cisco niet is versleuteld. Het is de taak van de klant om de bestanden expliciet te versleutelen voordat de bestanden als bijlage naar de e-mail worden geüpload. Als aanvullende best practice voor de beveiliging moet alle gevoelige informatie, zoals wachtwoorden, worden versluierd of verwijderd van elk configuratiebestand of logboek dat over een niet-beveiligd kanaal wordt verzonden. Ga voor meer informatie naar Bestanden versleutelen.

Nadat de bestanden zijn versleuteld kunt u aanvullende informatie en bestanden uploaden naar de case door de informatie via een e-mailbericht te verzenden naar attach@cisco.com met het casenummer in de onderwerpregel of in het bericht zelf, bijvoorbeeld, onderwerp: = Case xxxxxxxxx.

Bijlagen zijn beperkt tot 20 MB per e-mailupdate. Bijlagen die met e-mailberichten worden ingediend worden niet versleuteld tijdens verzending, maar worden direct aan de bijbehorende case gekoppeld en in een versleuteld format opgeslagen.

Hang het bestand aan een e-mailbericht en verstuur het bericht naar attach@cisco.com zoals in afbeelding 9.

Afbeelding 9. Het bestand verzenden



Het vorige screenshot laat een Microsoft Outlook e-mail zien met een versleuteld Zip-bestand als bijlage, het correcte Aan-adres en een onderwerp met de correcte notatie. Andere e-mailclients moeten dezelfde functionaliteit bieden en net zo goed presteren als Microsoft Outlook.

Naar boven

Bestanden versleutelen

De volgende voorbeelden tonen het versleutelen van bestanden met drie van de vele beschikbare opties: WinZip, de Linux-opdrachten tar en openssl, en Linux Gzip en GnuPG. Een sterk encryptie-algoritme zoals AES-128 moet worden gebruikt om de gegevens goed te beschermen. Als u Zip gebruikt, moet een toepassing worden gebruikt die AES-encryptie ondersteunt. Oudere versies van Zip-toepassingen ondersteunen een symmetrisch encryptiesysteem dat niet beveiligd is en niet moet worden gebruikt.

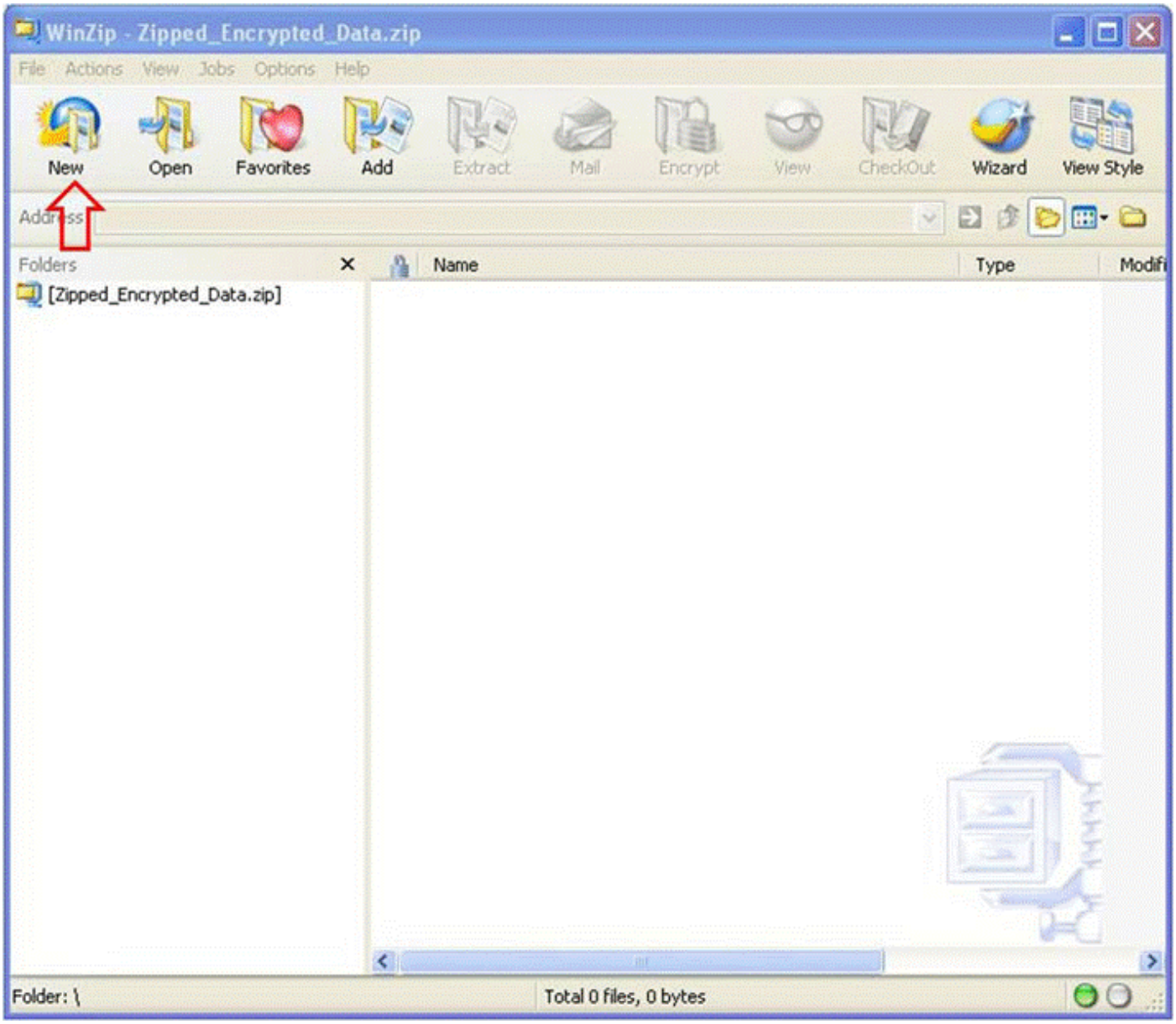
Bestanden versleutelen met WinZip

Deze paragraaf laat zien hoe u bestanden versleutelt met de toepassing WinZip. Andere

toepassingen moeten dezelfde functionaliteit bieden en net zo goed presteren als WinZip.

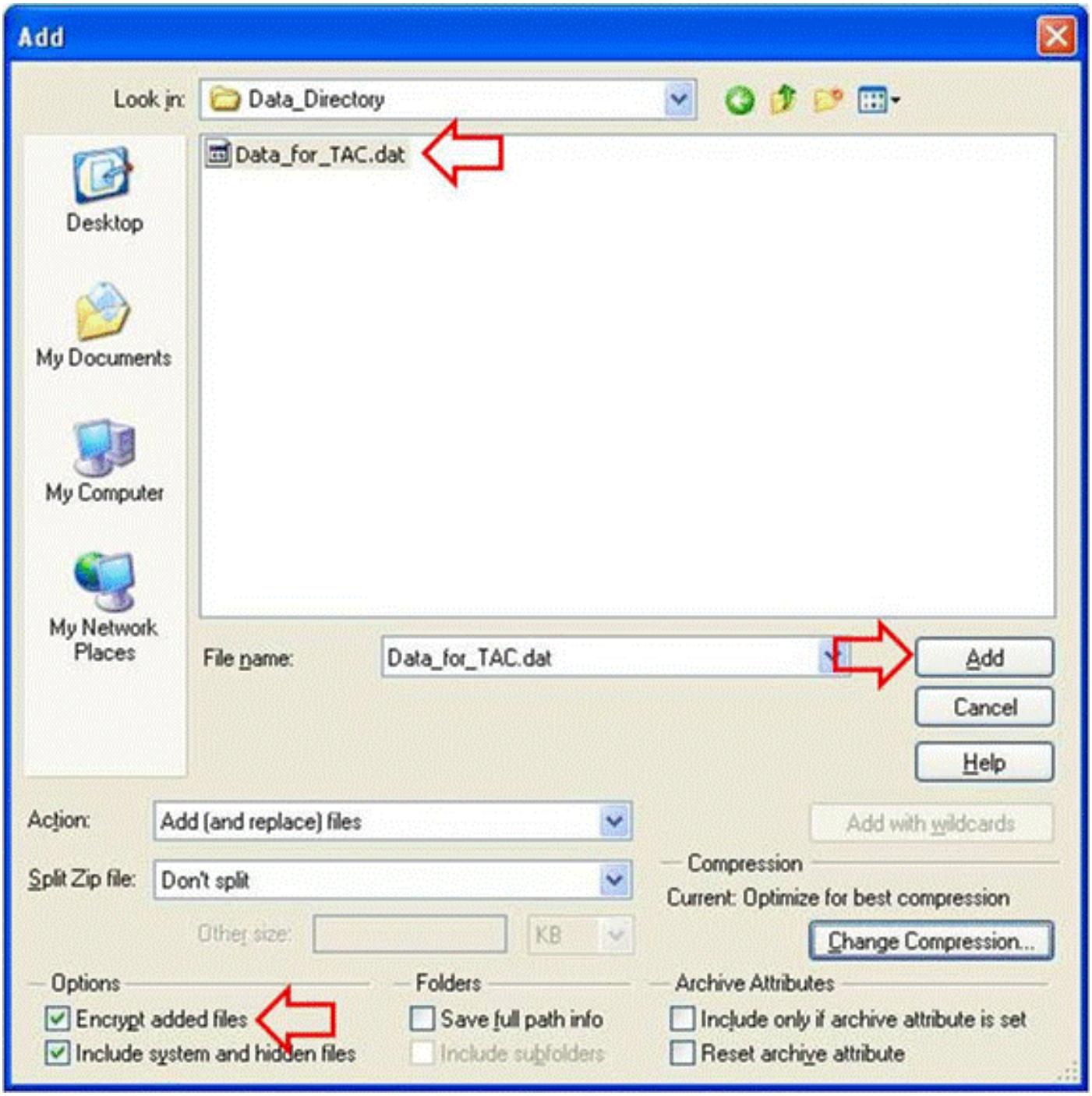
Stap 1 Maak een ZIP-archiefbestand zoals in afbeelding 11. In de WinZip GUI, klik op **New en volg de aanwijzingen in het menu om een nieuw ZIP-archiefbestand met de juiste naam te maken.** Het nieuw aangemaakte ZIP-archiefbestand wordt weergegeven.

Afbeelding 10. Een ZIP-archiefbestand maken



Stap 2 Voeg de te uploaden bestanden toe aan het ZIP-archiefbestand en selecteer de optie Encrypt added files zoals getoond in afbeelding 12. Klik vanuit het hoofdscherm van WinZip op **Add en selecteer vervolgens de bestanden die moeten worden geüpload.** De optie **Encrypt added files moet worden geselecteerd.**

Afbeelding 11. Optie Encrypt added files



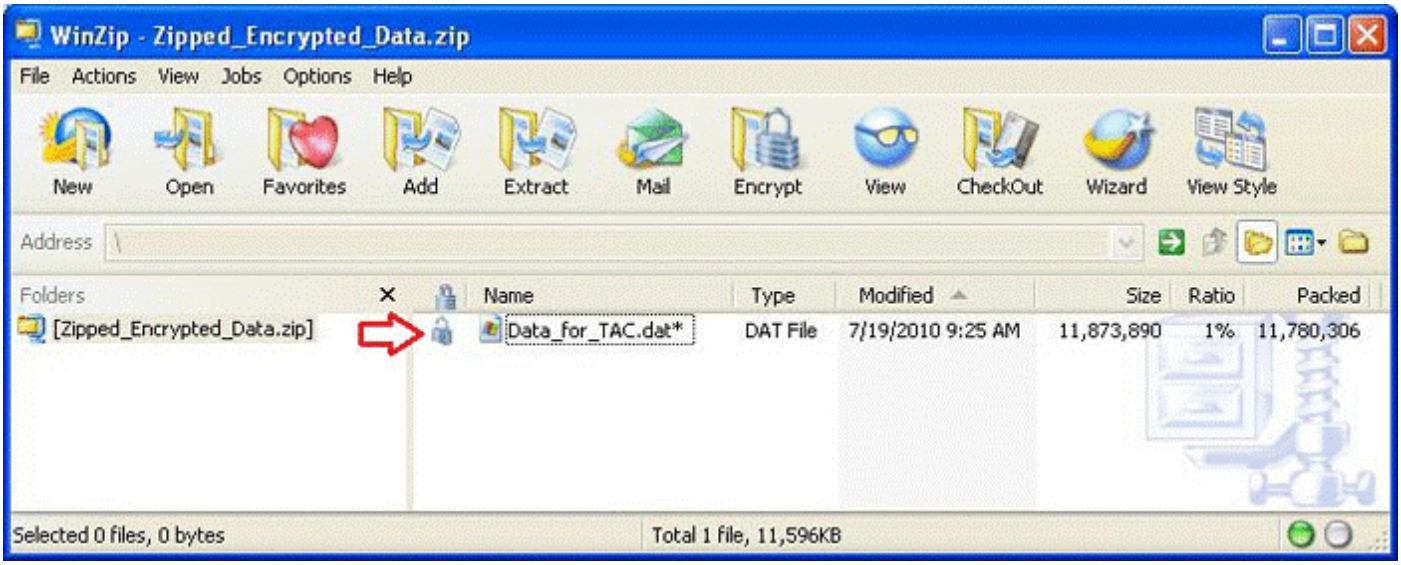
Stap 3 Versleutel het bestand met behulp van het AES-encryptie-algoritme en een sterk wachtwoord zoals in afbeelding 13:

1. Klik op **Add in het venster voor bestandselectie om het venster Encrypt te openen.**
2. Voer in het venster **Encrypt een voldoende sterk wachtwoord in.** Het wachtwoord wordt gedeeld met de Customer Support Engineer-eigenaar van de case zoals besproken in Wachtwoord doorgeven aan de TAC Customer Support Engineer.
3. Selecteer een van de AES-encryptiemethoden.
4. Klik op **OK om de bestand(en) te versleutelen en het hoofdvenster van WinZip weer te geven.**

Afbeelding 12. Het bestand versleutelen

Stap 4 Controleer dat het bestand versleuteld zoals in afbeelding 14. Versleutelde bestanden worden gemarkeerd met een ster achter de bestandsnaam of een slotpictogram in de encryptiekolom.

Afbeelding 13. Controleer de versleuteling



Bestanden versleutelen met Tar en OpenSSL

Deze paragraaf laat zien hoe u bestanden versleutelt met de opdrachten **tar en openssl van de Linux-opdrachtregel.** Andere archief- en encryptie-opdrachten moeten dezelfde functionaliteit bieden en net zo goed presteren onder Linux of Unix.

Stap 1 Maak een tar-archief van het bestand en versleutel het via OpenSSL met behulp van het AES-algoritme en een sterk wachtwoord zoals in het volgende voorbeeld. De opdrachtoutput laat de gecombineerde syntaxis zien van tar en openssl om het bestand of de bestanden te versleutelen met het AES-algoritme.

```
[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
```

Bestanden versleutelen met Gzip en GnuPG

Deze paragraaf laat zien hoe u bestanden versleutelt met de opdrachten Gzip en GnuPG van de Linux-opdrachtregel. Andere archief- en encryptie-opdrachten moeten dezelfde functionaliteit bieden en net zo goed presteren onder Linux of Unix. De opdrachtoutput toont hoe de opdrachtsyntaxis van gzip en gpg moet worden gebruikt om het bestand of de bestanden te versleutelen met het AES-algoritme.

Stap 1 Comprimeer het bestand met Gzip:

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

Stap 2 Versleutel het bestand met GnuPG met behulp van het AES-algoritme en een sterk wachtwoord:

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

Stap 3 Voer het sterke wachtwoord in en bevestig als om het wachtwoord wordt gevraagd:

```
Wachtwoord invoeren:
Wachtwoord herhalen:
```

Naar boven

Wachtwoord doorgeven aan de TAC Customer Support Engineer

Deel het versleutel-wachtwoord met de Customer Support Engineer-eigenaar van de case bij het versleutelen van bijlagen. Als best practice: gebruik een andere methode dan de methode die is gebruikt om het bestand te uploaden. Communiceer het wachtwoord out-of-band, bijvoorbeeld telefonisch of per SCM case-update als u een e-mailbericht of FTPS hebt gebruikt om het bestand te uploaden.

Bewaren van klantbestanden

Alle bestanden zijn direct toegankelijk in het casevolgsysteem voor geautoriseerd Cisco-personeel voor de periode dat de case open is en voor een periode van 18 maanden volgend op de definitieve sluiting van een case. 18 maanden na de definitieve sluiting kunnen de bestanden naar een archief worden verplaatst om ruimte te besparen, maar ze worden niet gewist (verwijderd) uit de historie van de case.

Op elk moment kan een geautoriseerd klantcontact verzoeken dat een specifiek bestand uit een

case wordt gewist. Cisco kan dat bestand dan verwijderen en een notitie aan de case toevoegen om vast te leggen welke partij het bestand verwijderde, de tijd en datum en de naam van het verwijderde bestand. Nadat een bestand op deze manier is gewist, kan het niet worden teruggehaald.

Bestanden die naar de TAC-FTP-map worden geüpload, worden vier dagen bewaard. De Customer Support Engineer-eigenaar van de case moet worden geïnformeerd wanneer er een bestand naar deze map wordt geüpload. De Customer Support Engineer moet binnen vier dagen een back-up maken van de bestanden door ze aan de case toe te voegen.

Naar boven

Samenvatting

Er zijn meerder opties voor het uploaden van informatie naar Cisco TAC zodat zij cases kunnen oplossen. SCM en Cisco's HTML5 Upload-tool bieden beide beveiligde uploads via een browser. De CXD biedt uploads via een browser, Web API en meerdere protocollen die door verschillende typen client- en Cisco-apparaten worden ondersteund.

Als u geen SCM, Cisco HTML5 bestanduploadtool of een protocol dat niet FTP is en wordt ondersteund door CXD kunt gebruiken als uw uploadmethode, zijn de minst wenselijke opties voor het uploaden van bestanden FTP, het gebruik van CXD of een e-mailbericht verzenden naar attach@cisco.com. Als u voor een van deze mogelijkheden kiest, raden we u sterk aan uw bestanden te versleutelen voor verzending. Ga voor meer informatie naar Bestanden versleutelen . U moet een sterk wachtwoord gebruiken en het wachtwoord out-of-band communiceren naar de Customer Support Engineer van de case, bijvoorbeeld telefonisch of via SCM case-update.

Alle bestanden zijn direct toegankelijk in het casevolgsysteem voor geautoriseerd Cisco-personeel voor de periode dat de case open is en voor een periode van 18 maanden volgend op de definitieve sluiting van een case.

- Na 18 maanden kunnen de bestanden naar het archief worden verplaatst.
- Op elk moment kan een geautoriseerd klantcontact verzoeken dat een specifiek bestand uit een case wordt gewist.
- Bestanden in de FTP-map worden slechts vier dagen bewaard.

Aanvullende informatie

- Technische services van Cisco gebruiken
- Cisco's wereldwijde contactgegevens voor ondersteuning
- Resourcegids voor technische services van Cisco
- Cisco Security Blog - NCSAM Tip #3: Hoe ziet een beveiligd wachtwoord eruit?
- Cisco Conferencing-producten
- De GNU Privacy Guard
- Het OpenSSL-project
- WinZip

Dit document maakt deel uit van Cisco Security Research & Operations.

eigen risico. Cisco behoudt zich het recht voor om dit document te allen tijde te wijzigen of te annuleren.

Naar boven

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.