Cisco Technical Assistance Center에 고객 파일 업로드

목차

개요

Cisco의 최우선 가치는 고객이므로 고객의 문제를 적시에 해결하는 것이 가장 중요합니다. 고객이 프로세스를 지원할 수 있는 한 가지 방법은 Cisco Technical Assistance Center(TAC)에 검토를 위한 관련 파일을 제공하는 것입니다. TAC 고객 지원 엔지니어는 이러한 파일을 사용하여 고객 문제를 해결하며, Cisco는 Cisco TAC에 정보를 업로드하는 여러 옵션을 제공하여 고객의 요구 사항을 충족시킵니다. 이러한 옵션 중 일부는 낮은 보안성으로 인해 특정한 위험을 초래할 수 있으며, 각 옵션에는 고객이 적절한 업로드 옵션을 결정하기 전에 고려해야 하는 제한 사항이 있습니다. 표 1에는 파일 암호화 기능, 권장되는 파일 크기 제한 및 기타 관련 정보를 포함하는 사용 가능한 업로드 옵션이 요약되어 있습니다.

표 1. 사용 가능한 업로드 옵션

사용 가능한 옵션(환경 설정 순서로)		파일은 전송 중에 암호화됩니다.	파일은 유휴 상태에서 암호화됩니다.	권장되는 파일 크기 제한
SCM(Support Case Manager)	방법	예	예	250GB

케이스 파일 업로더	방법	예	예	250GB
Customer eXperience Drive	방법	예*	예	제한 없음
attach@cisco.com으로 이메일 보내기	방법	아니요**	예	20MB 이하의 고객 메일 서버 제한 기준
*FTP를 제외한 모든 프로토콜에 적용됩니다. FTP를 사용하는 경우, Cisco는 업로드 전에 데이터를 암호화할 것을 적극적으로 권장합니다. **고객은 전송 전에 암호화해야 합니다. 고객의 네트워크/이메일 공급자로부터의 전송은 전송 중에 암호화되지 않을 수도 있습니다. 보안 전송은 이메일/첨부 파일이 Cisco 네트워크에 도달하는 지점에서만 보장됩니다.				

Support Case Manager 파일 업로드

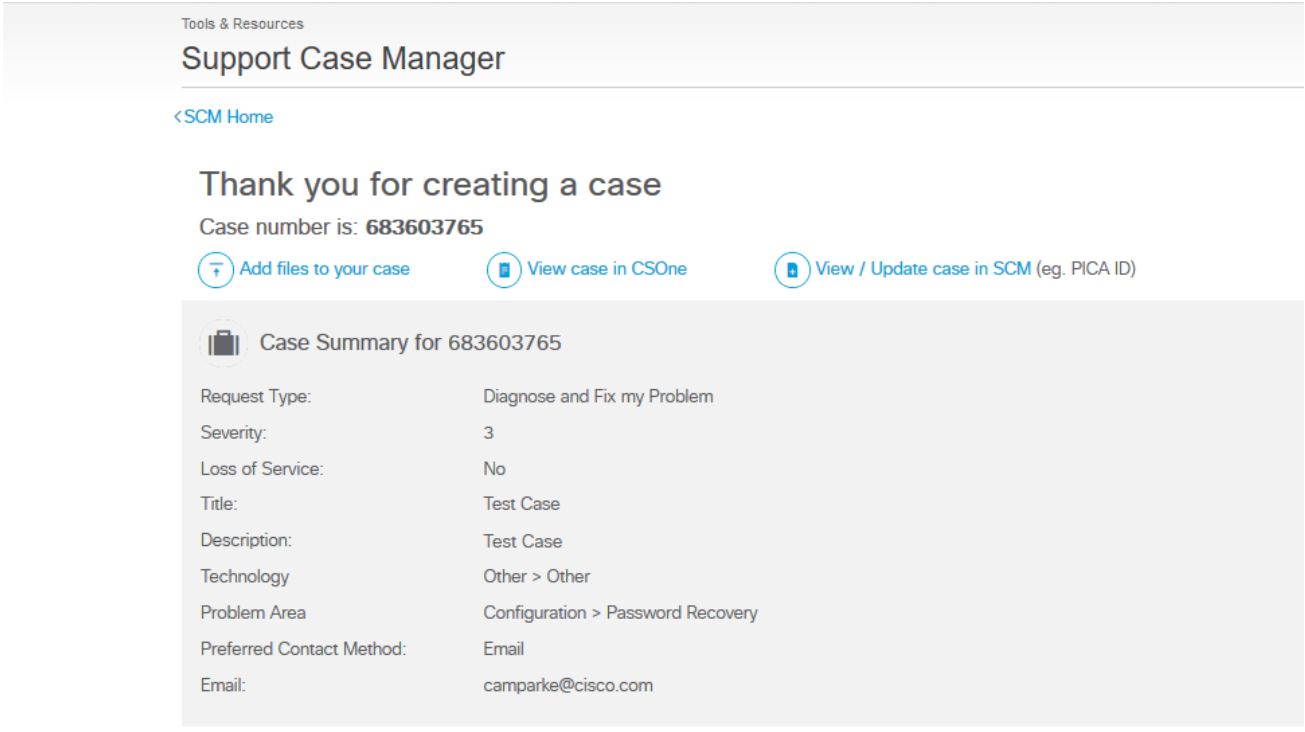
SCM(Support Case Manager) 파일 업로드 방법은 케이스에 파일을 업로딩하는 데 우선적이며 가장 안전한 옵션입니다. 이 옵션을 사용하여 전송되는 파일은 전송 중에 암호화되며 크기는 250GB로 제한됩니다. 고객의 컴퓨팅 디바이스와 Cisco 간의 통신 채널은 암호화됩니다. SCM을 통해 업로드되는 파일은 연관된 케이스에 즉시 연결되며 암호화된 형식으로 저장됩니다.

케이스 제출 시 파일 업로딩

케이스 확인 화면에서 다음 단계를 수행합니다. SCM에서 케이스를 생성하거나 관리하는 방법에 대한 자세한 지침은 SCM 도움말을 참조하십시오.

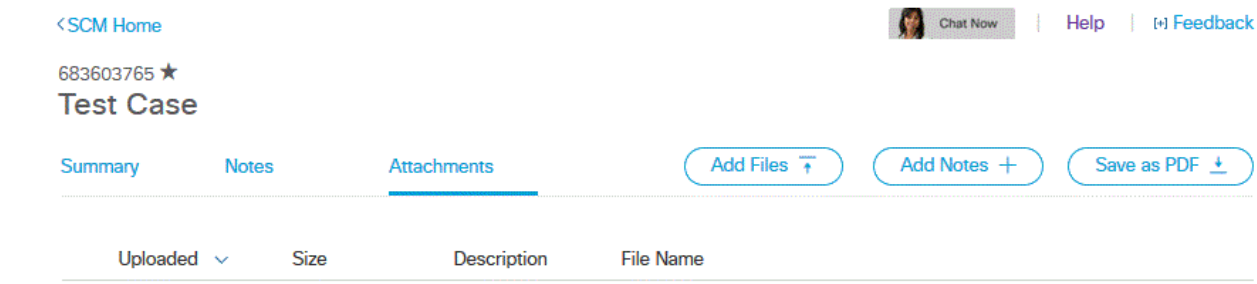
1단계 Add files to your case(케이스에 파일 추가) 버튼을 선택합니다(그림 1).

그림 1. SCM: 케이스에 파일 추가



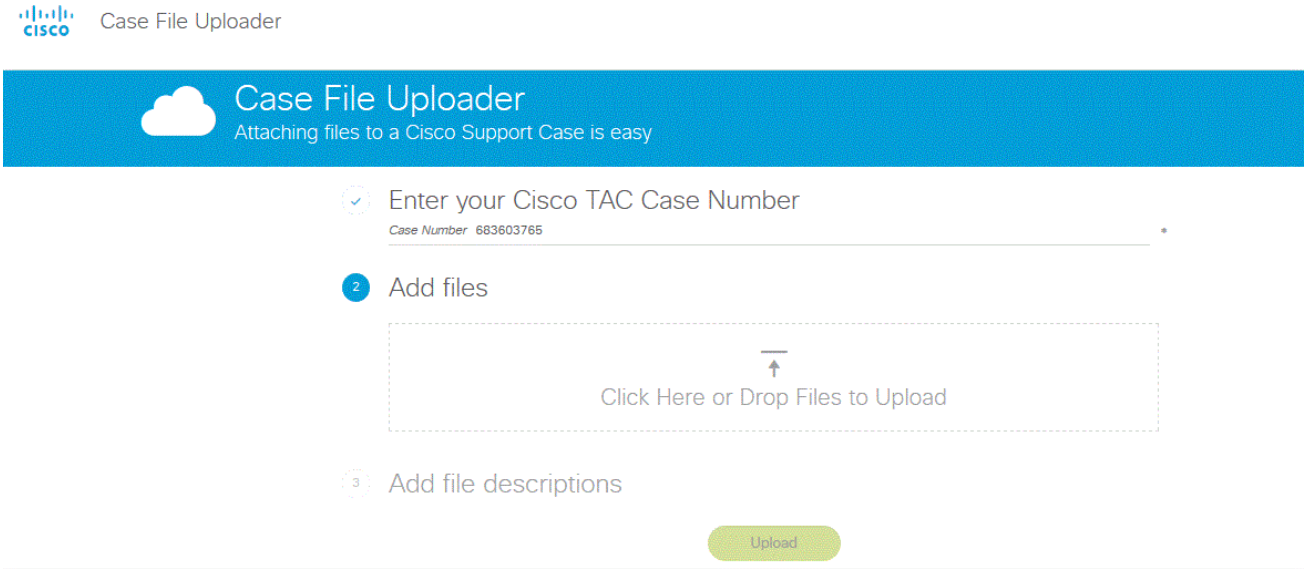
2단계 Attachments(첨부 파일) 탭에서 Add Files(파일 추가) 버튼을 선택합니다(그림 2).

그림 2. SCM: 첨부 탭



케이스 파일 업로더 툴로 이동합니다. 생성한 케이스가 툴에 미리 채워집니다(그림 3). **케이스 파일 업로더 섹션 3단계로 진행합니다.**

그림 3. 케이스 파일 업로더: 파일 끌어서 놓기 화면



기존 케이스에 파일 업로딩

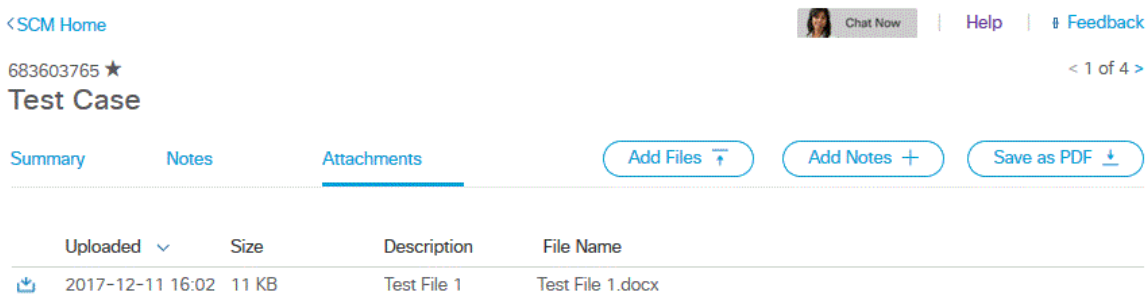
케이스를 제출한 후에는 선택적 정보를 업데이트하거나 변경할 수 있습니다.

1단계 SCM에 로그인합니다.

2단계 케이스를 열거나 편집하려면 목록에서 케이스 번호 또는 케이스 제목을 클릭합니다. 케이스 세부사항 페이지가 열립니다.

3단계 케이스 세부사항 페이지 상단에는 **요약**, **메모**, 첨부의 세 가지 탭이 **있습니다**. 탭 옆에는 **파일 첨부**, **메모 추가** 및 **PDF**로 **저장** 등의 도구 모음 단추 **세트가 있습니다**. **Add Files(파일 추가)를 클릭하여 파일을 선택하고 케이스에 첨부 파일로 업로드합니다(그림 4).**

그림 4. SCM 첨부 파일 화면



케이스 파일 업로더 툴로 이동합니다. 생성한 케이스가 툴에 미리 채워집니다(그림 3). **케이스 파일 업로더 섹션 3단계로 진행합니다.**

맨 위로 돌아가기

케이스 파일 업로더

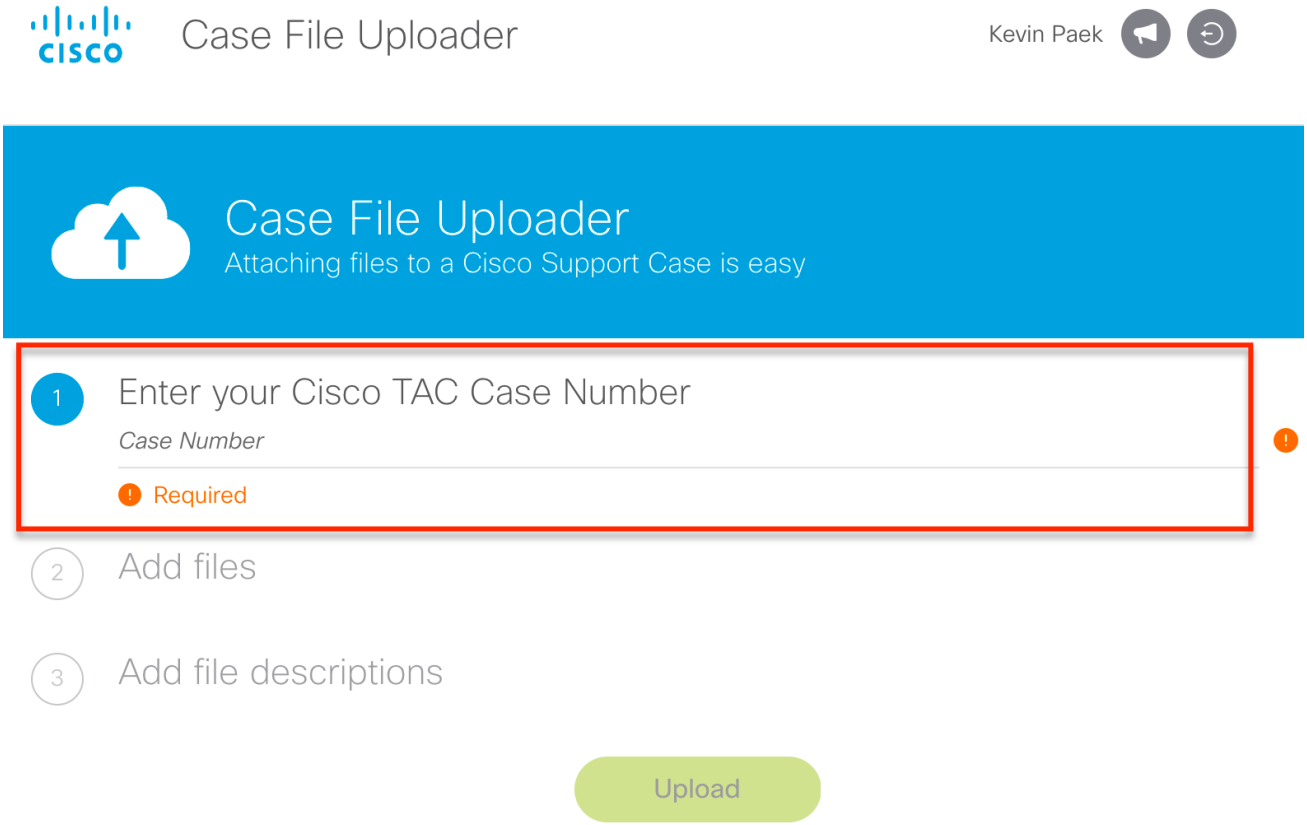
케이스에 파일을 업로드하는 다른 안전한 방법은 케이스 파일 업로더입니다. 이 툴은 이 옵션을 사용하여 전송하는 파일이 전송 중에 암호화되고 크기가 250GB로 제한된다는 점에서 SCM과 유사합니다. 고객의 컴퓨팅 디바이스와 Cisco 간의 통신 채널이 암호화됩니다. 케이스 파일 업로더를 통해 업로드되는 파일은 연관된 케이스에 즉시 연결되며 암호화된 형식으로 저장됩니다. 이 툴을 사용하여 파일을 첨부하려면 다음 단계를 완료합니다.

참고: 도구에서 케이스에 파일을 업로드할 수 없는 경우, 입력한 케이스 번호가 잘못되었거나 파일을 추가하는 데 필요한 권한이 없습니다. 케이스에 파일을 업로드하려면 케이스가 열린 계약과 cisco.com 프로파일이 관련되어 있어야 합니다. Cisco Profile Manager를 사용하여 프로파일에 서비스 계약을 추가하거나 서비스 액세스 관리자가 대신 처리하게 할 수 있습니다. 추가 지원이 필요한 경우, Cisco 기술 지원 센터에 문의하십시오.

1단계 케이스 파일 업로더에 로그인합니다.

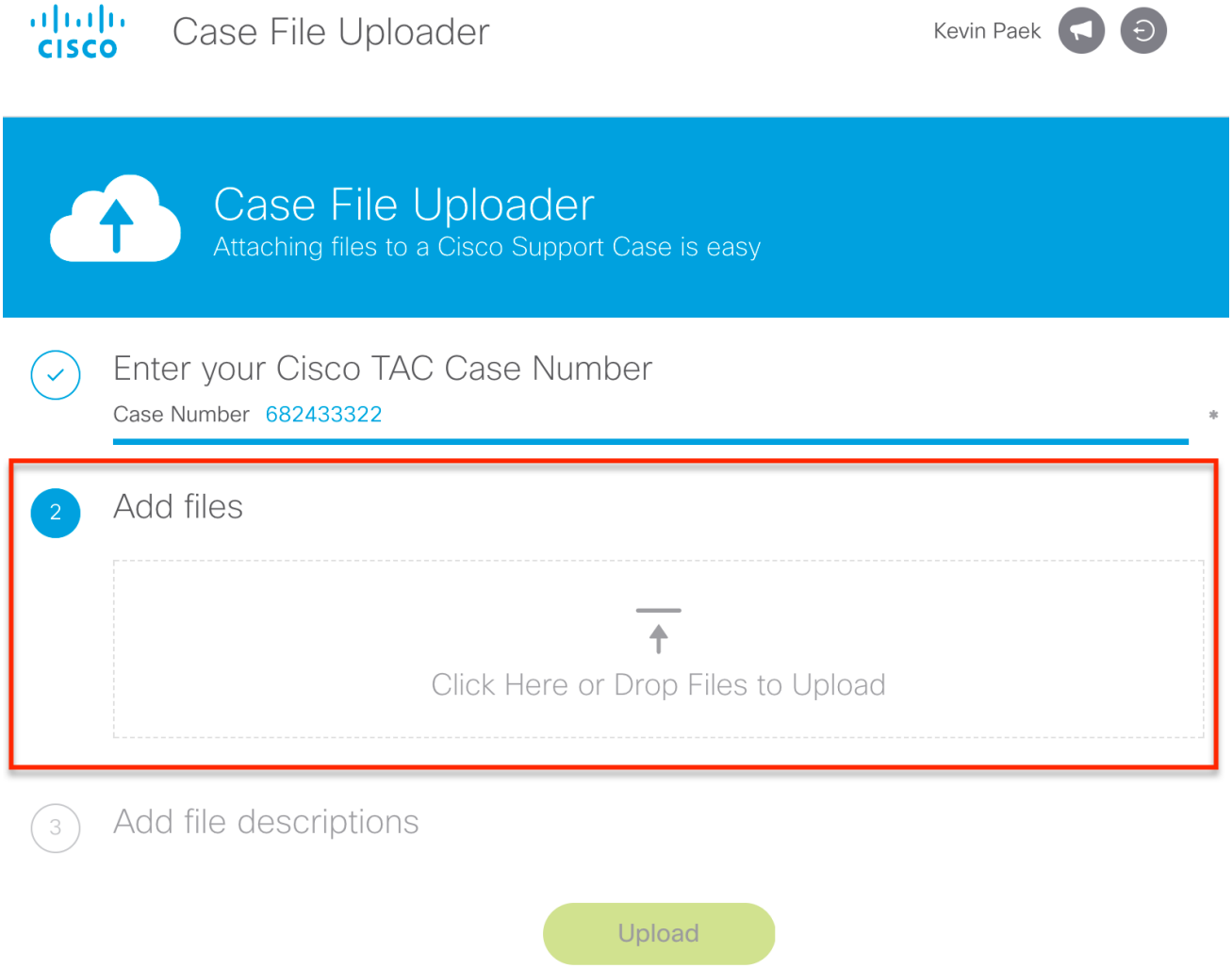
2단계 **제공된 필드에 케이스 번호를 입력합니다(그림 5).**

그림 5. 케이스 파일 업로더: 케이스 번호 입력 화면



3단계 첨부할 파일을 선택할 때, 끌어다 놓거나 점선 상자 내부를 클릭하여 업로드할 파일을 선택합니다(그림 6).

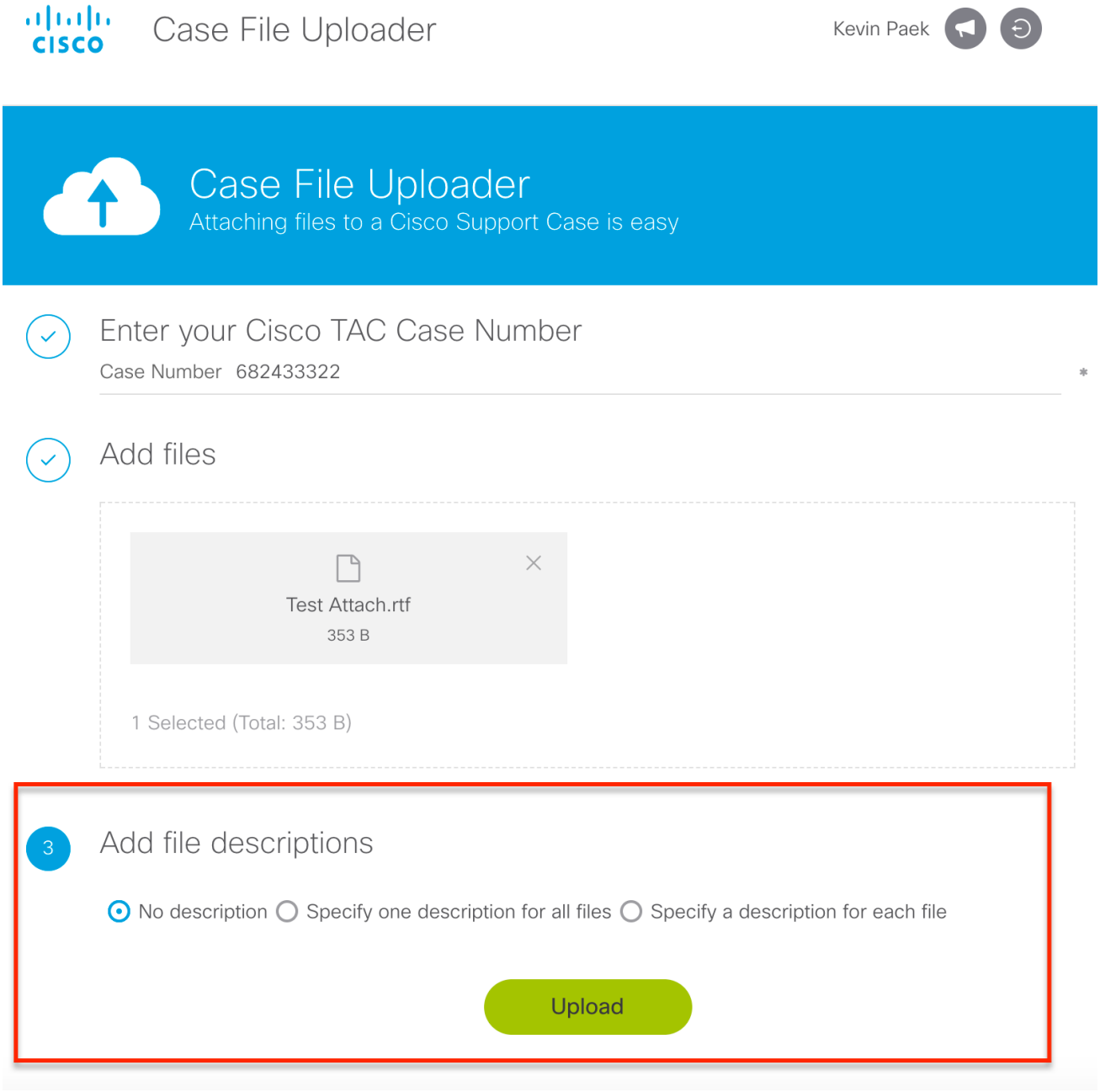
그림 6. 케이스 파일 업로더: 파일 끌어서 놓기 화면



4단계 파일을 선택한 후, 설명을 지정할 필요가 없으면 Upload(업로드)를 클릭합니다. 아니면, 다른 옵션을 사용하여 상세정보를 추가하도록 선택할 수 있습니다. (그림 7). **Category(범주)** 및 **Description(설명)** 필드를 사용하면 파일에 대한 보다 많은 정보를 추가할 수 있습니다.

- **Category(범주) 필드를 사용하여 첨부 파일 유형을 선택합니다.**
- **Description(설명) 필드를 사용하여 파일에 대한 간략한 설명을 제공합니다.**

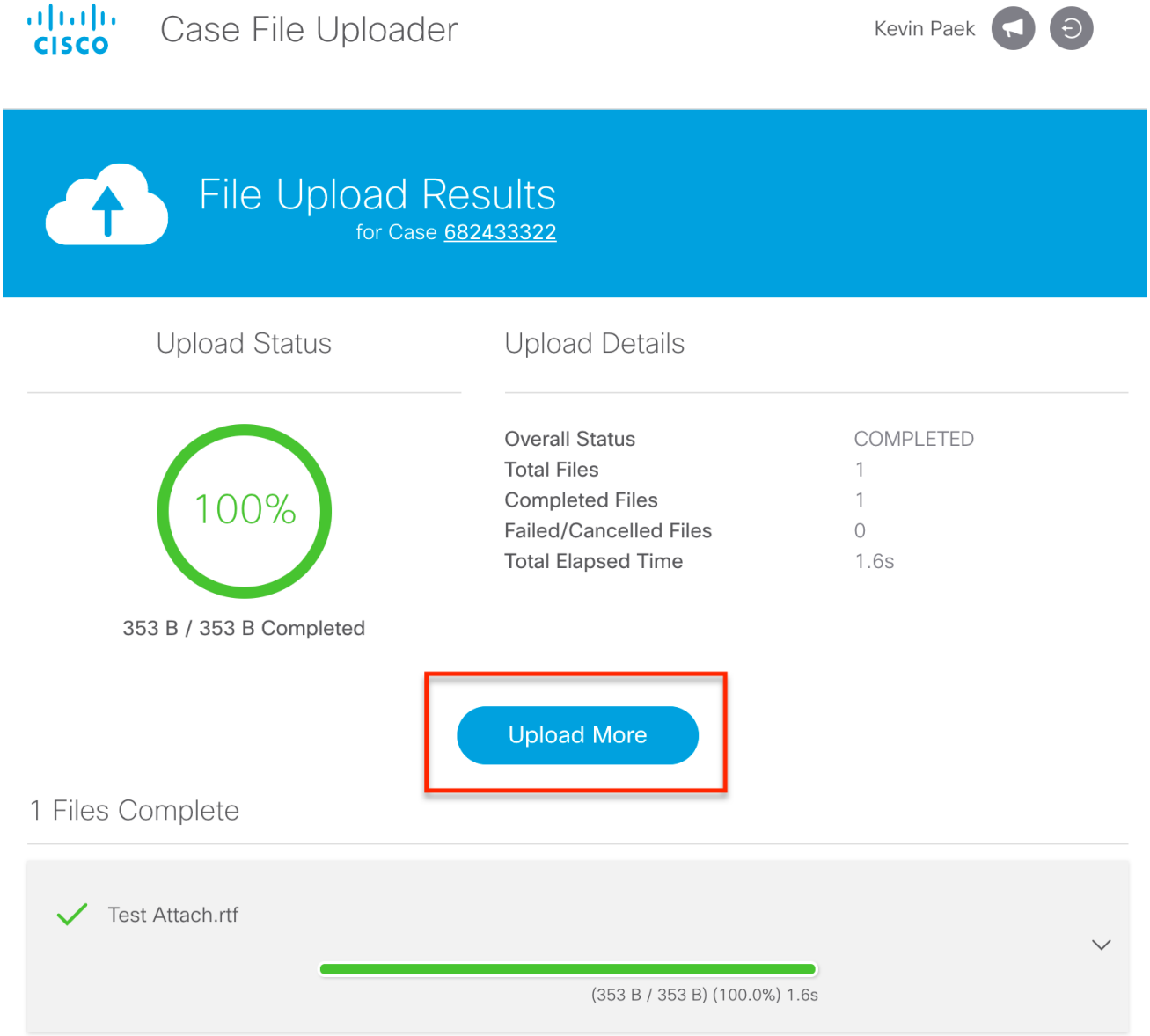
그림 7. 케이스 파일 업로더: 파일 설명 입력



5단계 **Upload(업로드)**를 클릭하여 파일을 업로드합니다.

6단계 **다음 화면은 파일의 상태를 보여줍니다.** 파일을 업로드한 후 **Upload More(추가 업로드)**를 클릭하여 추가 첨부 파일을 업로드합니다(그림 8).

그림 8. 케이스 파일 업로더: 업로드 상태 화면



맨 위로 돌아가기

Customer eXperience Drive

서비스 요약

Customer eXperience Drive(CXD)는 업로드되는 파일 크기에 제한이 없는 멀티 프로토콜 파일 업로드 서비스입니다. 이를 통해 활성 서비스 요청(SR)을 가진 Cisco 고객은 서비스 요청(SR)마다 생성되는 고유 인증서를 사용하여 케이스에 직접 데이터를 업로드할 수 있습니다. CXD에서 지원하는 프로토콜은 Cisco 제품에 기본적으로 지원되므로 Cisco 디바이스에서 SR로 직접 업로드할 수 있습니다.

지원되는 프로토콜

표 2에는 CXD에서 지원하는 프로토콜이 요약되어 있습니다. 사용 프로토콜에 관계없이, 업로드된 파일 크기에 제한이 설정되지 않는 것이 좋습니다.

표 2. CXD 지원 프로토콜

이름	프로토콜/포트	암호화	데이터 채널 포트	참고
SFTP(Secure File Transfer Protocol)	TCP/22	예	해당 없음	
SCP(Secure Copy Protocol)	TCP/22	예	해당 없음	
SSL(HTTPS)을 통한 하이퍼 텍스트 전송 프로토콜	TCP/443	예	해당 없음	사용 가능한 사용자 및 애플리케이션 인터페이스*
SSL(FTPS) Implicit의 파일 전송 프로토콜	TCP/990	예	30000-40000	제어 채널이 암호화되어 있으므로 방화벽이 FTPS를 검사할 수 없습니다. 따라서 방화벽이 전체 데이터 채널 포트 범위에 대한 아웃바운드 연결을 허용해야 합니다.
SSL(FTPS) Explicit의 파일 전송 프로토콜	TCP/21	예**	30000-40000	
FTP(File Transfer Protocol)	TCP/21	아니요	30000-40000	• 프로토콜이 암호화를 지원하지 않으므로, Cisco에서는 FTP 사용을 전혀 권장하지 않습니다. 이를 사용해야 하는 경우에는 전송 전에 데이터를 암호화해야 합니다. • 방화벽은 FTP 트래픽을 검사하여 데이터 채널이 올바르게 설정될 수 있도록 해

				야 합니다. 네트워크 전체에서 FTP가 검사되지 않는 경우, 방화벽은 전체 데이터 채널 포트 범위에 대한 아웃바운드 연결을 허용해야 합니다.
* PUT API 사용에 대한 상세정보와 샘플 python 코드는 이 문서의 뒷부분에 공유되어 있습니다. ** FTPS Explicit 모드에서는 로그인을 시도하기 전에 클라이언트가 "AUTH TLS" 명령을 사용하여 TLS 협상을 명시적으로 요청해야 합니다.				

CXD 업로드 토큰

CXD는 SR마다 고유 업로드 토큰을 생성합니다. SR 번호와 토큰은 서비스를 인증하고 이후에 SR에 파일을 업로드하기 위한 사용자 이름 및 비밀번호로 사용됩니다.

참고: 토큰은 업로드 전용이며 사용자가 케이스 파일 또는 현재 업로드되는 파일에 액세스하는 것을 허용하지 않습니다. 사용자는 SCM에서만 케이스 파일을 볼 수 있습니다.

SR에 대한 업로드 토큰 검색

SCM 사용

SR이 열리면 CXD는 자동으로 업로드 토큰을 생성하고, 토큰과 서비스 사용 방법에 대한 몇 가지 세부 정보를 포함하는 SR에 메모를 삽입합니다.

업로드 토큰을 검색하려면 다음 단계를 완료합니다.

1단계 SCM에 로그인합니다.

2단계 업로드 토큰을 받을 케이스를 엽니다.

3단계 Attachment(첨부 파일) 탭을 클릭합니다.

4단계 Generate Token(토큰 생성)을 클릭합니다. 생성된 토큰은 Generate Token(토큰 생성) 버튼 옆에 표시됩니다.

참고:

- 사용자 이름은 항상 SR 번호입니다. "비밀번호" 및 "토큰"은 업로드 토큰을 의미하는 용어이며,

이는 CXD에서 프롬프트가 표시될 때 비밀번호로 사용됩니다.
- SR을 생성하는 몇 분 내에 메모가 자동으로 첨부됩니다. 사용자가 메모를 찾을 수 없는 경우, SR 소유자에게 문의할 수 있으며 토큰은 수동으로 생성될 수 있습니다.
- 이 방식은 가까운 시일 내에 변경될 예정입니다. 나중에 이 문서에서 업데이트를 다시 확인하십시오.

ServiceGrid API 사용

ServiceGrid API를 활용하는 고객은 GetUploadCredentials API를 사용하여 프로그래밍 방식으로 토큰을 검색할 수 있습니다.

참고: Cisco ServiceGrid API를 호출하려면 인증 토큰이 필요합니다. 인증 토큰을 얻기 위한 상세정보는 Cisco ServiceGrid 설명서를 참조하십시오.

HTTP 메서드: POST

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

헤더:

표 3: ServiceGrid GetUploadCredentials API 헤더

키	유형	가치	필수
Content-Type	문자열	application/json	예
Ahthorization(권한 부여)	문자열	베어러 <Auth Token>	예

본문:

표 4: ServiceGrid GetUploadCredentials API 본문

키	유형	가치	필수
사용자 이름	문자열	SR에 대한 파일 업로드 수행 권한이 있는 Cisco.com 사용자 이름	예
email	문자열(이메일 형식)	Cisco.com 사용자 이름의 이메일 주소	예

CXD에 파일 업로딩

데스크톱 클라이언트 사용

일반적으로 사용자는 원하는 프로토콜에 따라 클라이언트를 사용하여 cxd.cisco.com에 연결하고, SR 번호를 사용자 이름으로 그리고 업로드 토큰을 비밀번호로 사용하여 인증하고, 최종적으로는 파일 또는 파일들을 업로드하기만 하면 됩니다.

프로토콜 및 클라이언트에 따라 사용자 단계는 다를 수 있습니다. 자세한 내용은 클라이언트의 설

명서를 참조하는 것이 좋습니다.

Cisco 디바이스에서 직접

모든 Cisco 디바이스에는 일반적으로 "copy(복사)" 또는 "redirect(재전송)" 명령을 사용하는 내장형 파일 전송 클라이언트가 있습니다. Linux 배포판에서 실행되는 Cisco 장비는 일반적으로 SCP, SFTP, HTTPS 통합에 대해 하나 이상의 "scp", "sftp", "curl"을 지원합니다.

파일 업로드 API

파일 업로드 API는 HTTP PUT 동사를 활용하여 CXD에 파일을 업로드합니다. 통합의 호환성과 간소화를 극대화하기 위해, API는 단순하게 유지됩니다.

HTTP 메서드: PUT

URL: https://cxd.cisco.com/home/<대상 파일 이름>

헤더:

표 5: CXD 파일 업로드 API 헤더

키	유형	가치	필수
Ahthorization(권한 부여)	문자열	기본 HTTP 인증 문자열	예

본문은 파일 데이터 자체입니다. 여기에는 필드 또는 폼이 없으므로 요청을 매우 간단하게 수행할 수 있습니다.

PUT API를 사용하기 위한 샘플 Python 코드

다음 코드는 파일이 실행 중인 것과 동일한 경로에 저장되는 것으로 가정한다는 점에 유의하십시오.

```
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")
```

이메일 첨부 파일 업로드

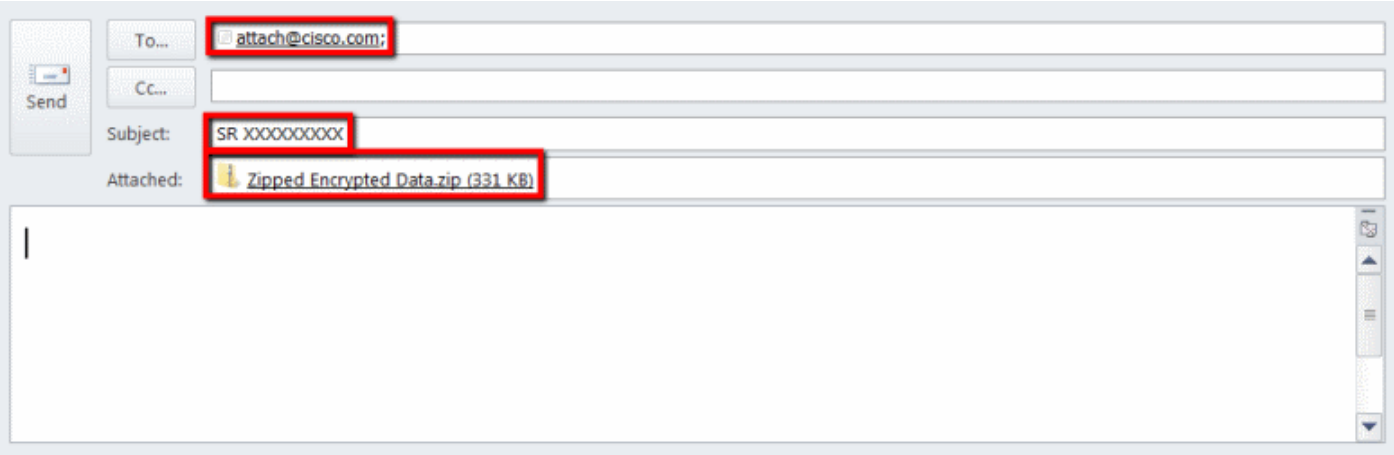
SCM, 케이스 파일 업로더 및 Customer eXperience Drive가 작동하지 않는 경우, 대체 가능한 다른 파일 업로드 방식은 이메일 첨부 파일 업로드 방식입니다. 이 방법은 *기본적으로 안전하지* 않으며 고객과 Cisco 간에 파일을 전송하는 데 사용되는 파일 또는 통신 세션을 암호화하지 않습니다. 이메일 첨부 파일을 통해 파일을 업로드하기 전에 고객이 명시적으로 파일을 암호화하는 것이 필수적입니다. 보안되지 않는 채널을 통해 전송되는 모든 컨피그레이션 파일 또는 로그에서 비밀번호와 같은 민감한 정보는 난독 처리하거나 제거하는 것이 보안에 추가로 좋은 방법입니다. 자세한 내용은 파일 암호화를 참조하십시오.

파일이 암호화된 후에는 메시지의 제목 줄에 케이스 번호가 있는(예: subject = Case xxxxxxxxx) 이메일 메시지를 통해 attach@cisco.com으로 정보를 전송하여 케이스에 추가 정보 및 파일을 업로드합니다.

첨부 파일은 이메일 업데이트당 20MB로 제한됩니다. 이메일 메시지를 사용하여 제출한 첨부 파일은 전송 중에 암호화되지는 않지만, 지정된 케이스에 즉시 연결되고 암호화된 형식으로 저장됩니다.

파일을 이메일 메시지에 첨부하고 그림 10에 나와 있는 바와 같이 attach@cisco.com으로 메시지를 전송합니다.

그림 9. 파일 보내기



이전 스크린 샷에서는 암호화된 ZIP 첨부 파일, 정확한 수신인 주소 및 올바른 형식의 제목이 있는 Microsoft Outlook 이메일을 보여줍니다. 다른 이메일 클라이언트도 Microsoft Outlook과 동일한 기능을 제공하고 수행해야 합니다.

맨 위로 돌아가기

암호화 파일

다음 예에서는 WinZip, Linux tar 및 openssl 명령, Linux Gzip 및 GnuPG와 같은 사용 가능한 여러 옵션 중 3개를 사용하여 파일을 암호화하는 방법을 보여줍니다. AES-128과 같은 강력한 암호화 방식을 사용하여 데이터를 적절히 보호해야 합니다. ZIP을 사용하는 경우, AES 암호화를 지원하는 애플리케이션을 사용해야 합니다. 이전 버전의 ZIP 애플리케이션은 안전하지 않은 대칭 암호화 시스템을 지원하므로 사용하면 안 됩니다.

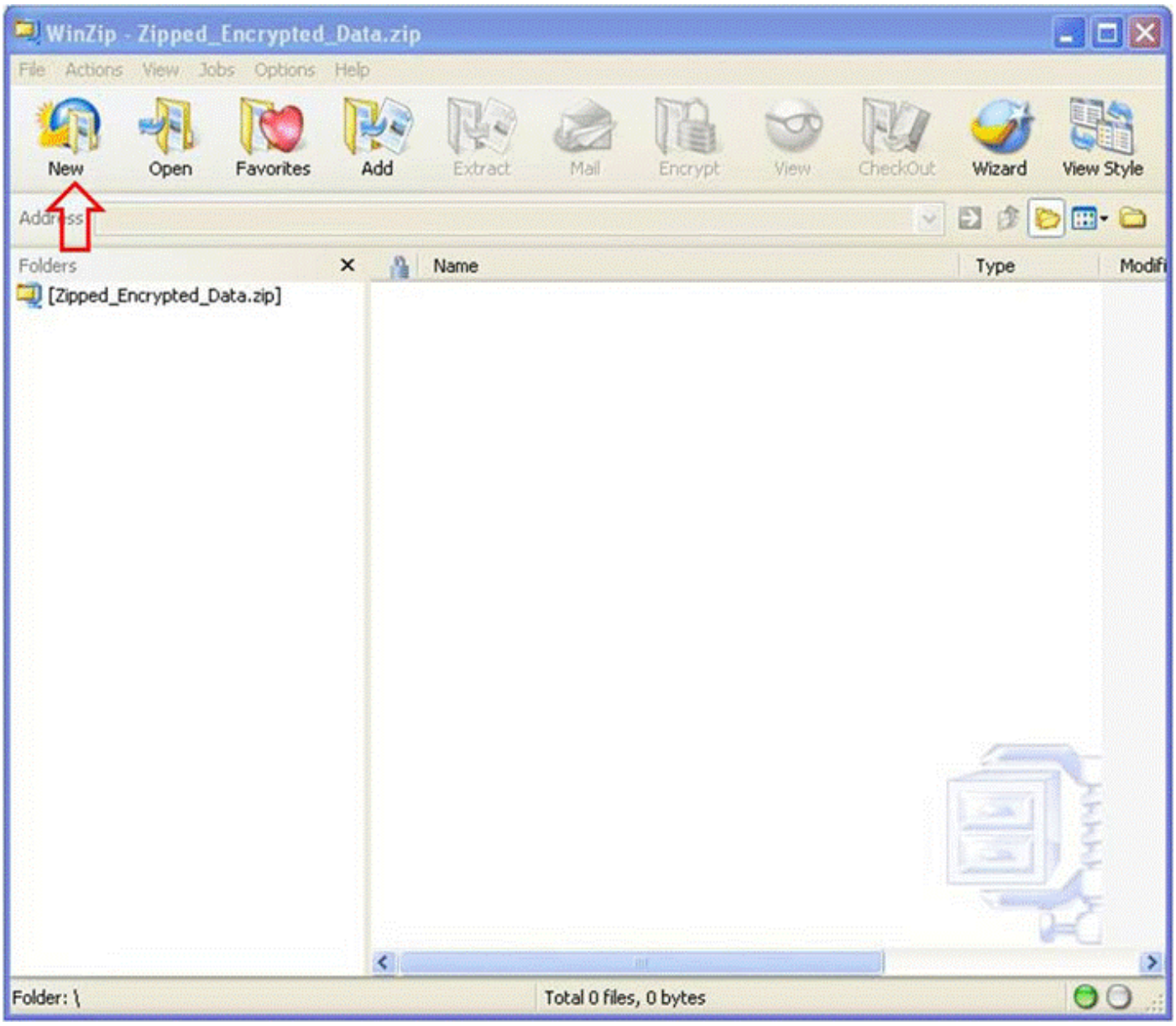
WinZip을 사용하는 암호화 파일

이 섹션에서는 WinZip 애플리케이션을 사용하여 파일을 암호화하는 방법을 보여줍니다. 다른 애플리케이션도 WinZip과 동일한 기능을 제공하고 수행해야 합니다.

1단계 그림 11과 같이 ZIP 아카이브 파일을 생성합니다. WinZip GUI에서 **New(새로 만들기)를 클**

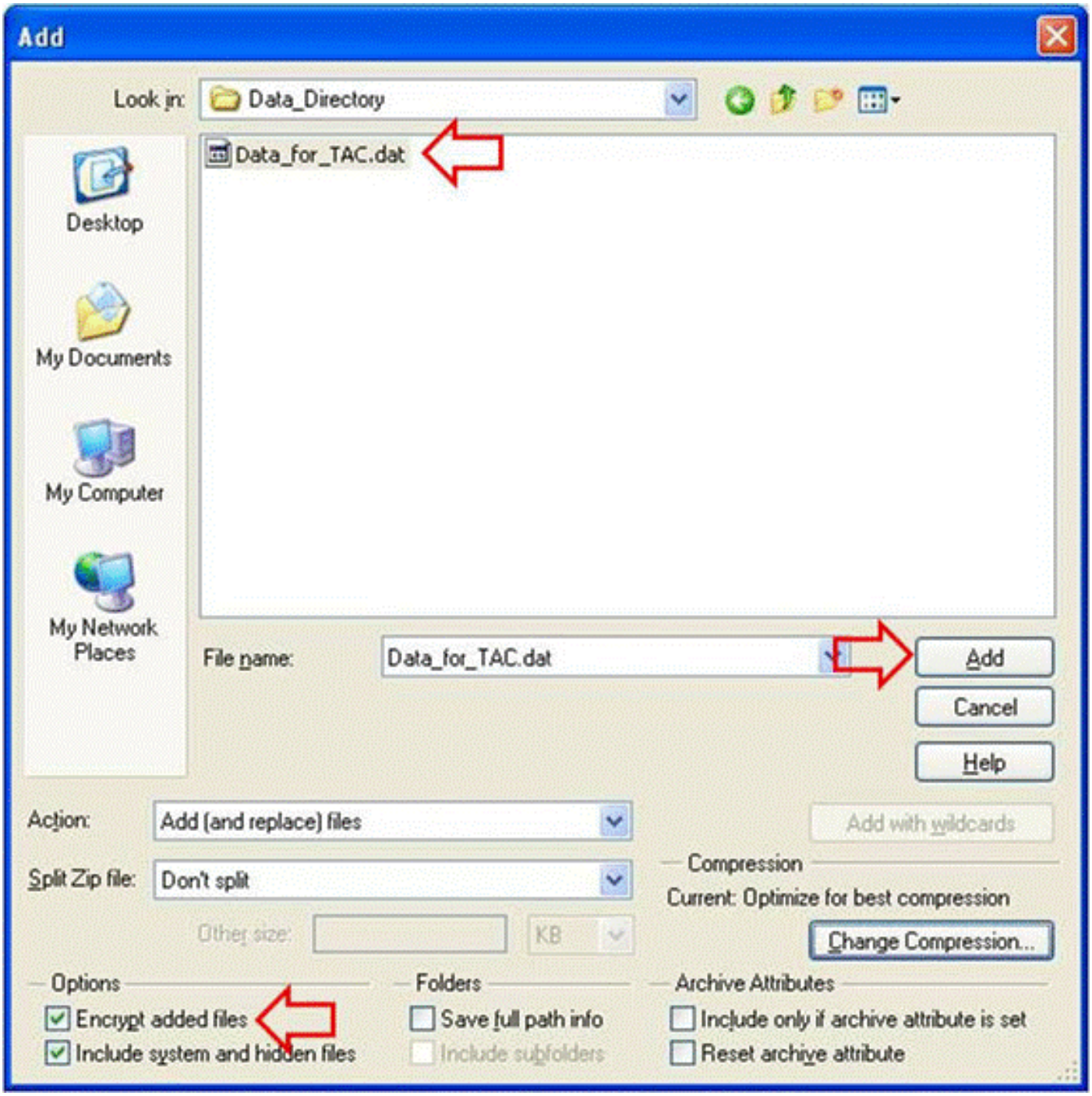
릭하고 메뉴 프롬프트에 따라 적절하게 명명한 새 ZIP 아카이브 파일을 생성합니다. 새로 생성된 ZIP 아카이브 파일이 나타납니다.

그림 10. ZIP 아카이브 만들기



2단계 ZIP 아카이브 파일에 업로드할 파일을 추가하고 그림 12에 나와 있는 바와 같이 Encrypt Add files(추가 파일 암호화) 옵션을 선택합니다. 기본 WinZip 창에서 **Add(추가)를 클릭한 다음 업로드할 파일을 선택합니다. Encrypt added files(추가된 파일 암호화) 옵션을 선택해야 합니다.**

그림 11. 추가된 파일 암호화



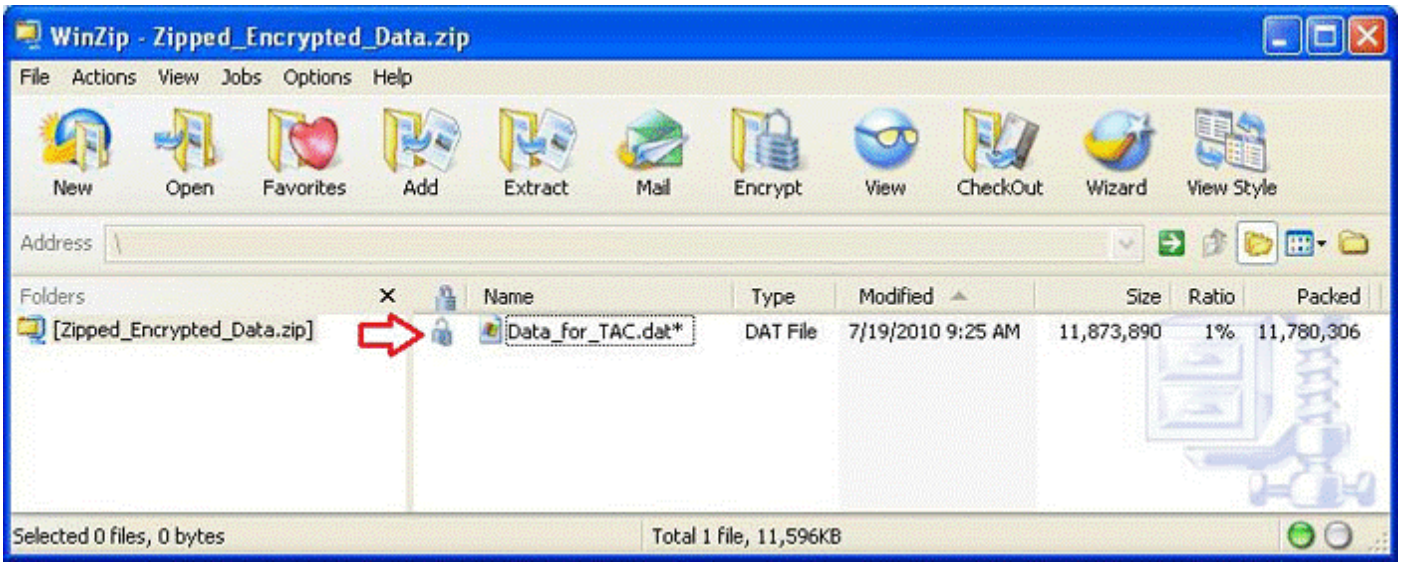
3단계 13에 표시된 대로 AES 암호화 방식과 강력한 비밀번호를 사용하여 파일을 암호화합니다.

1. 파일 선택 창에서 **Add(추가)를 클릭하여 Encrypt(암호화) 창을 엽니다.**
2. **Encrypt(암호화) 창에서 적절한 수준으로 강력한 비밀번호를 생성합니다.** TAC 고객 지원 엔지니어에게 비밀번호 전달에서 논의된 바와 같이 비밀번호는 케이스 고객 지원 엔지니어 소유자와 공유됩니다.
3. AES 암호화 방법 중 하나를 선택합니다.
4. **OK(확인)를 클릭하여 파일을 암호화하고 기본 WinZip 창을 표시합니다.**

그림 12. 파일 암호화

4단계 그림 14에 표시된 대로 파일이 암호화되었는지 확인합니다. 암호화된 파일은 파일 이름 뒤에 별표 또는 암호화 열의 자물쇠 아이콘으로 표시됩니다.

그림 13. 암호화 확인



Tar 및 OpenSSL을 사용하는 암호화 파일

이 섹션에서는 Linux 명령줄 **tar 및 openssl 명령을 사용하여 파일을 암호화하는 방법을 보여줍니다**. 다른 아카이브 및 암호화 명령도 Linux 또는 Unix와 동일한 기능을 제공하고 수행해야 합니다.

1단계 다음 예에 표시된 대로 파일의 tar 아카이브를 생성하고 AES 암호와 강력한 비밀번호를 사

용하여 OpenSSL을 통해 암호화합니다. 명령 출력은 AES 암호를 사용하여 파일을 암호화하는 결합된 tar 및 openssl 명령 구문을 보여줍니다.

```
[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 레코드 입력
60 + 1 레코드 출력
```

Gzip 및 GnuPG를 사용하는 암호화 파일

이 섹션에서는 Linux 명령줄 Gzip 및 GnuPG 명령을 사용하여 파일을 암호화하는 방법을 보여줍니다. 다른 아카이브 및 암호화 명령도 Linux 또는 Unix와 동일한 기능을 제공하고 수행해야 합니다. 명령 출력은 AES 암호를 사용하는 파일을 암호화하기 위해 gzip 및 gpg 명령 구문을 사용하는 방법을 보여줍니다.

1단계 Gzip을 사용하여 파일을 압축합니다.

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

2단계 AES 암호와 강력한 비밀번호를 사용하는 GnuPG를 통해 파일을 암호화합니다.

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

3단계 암호 프롬프트에 강력한 암호를 입력하고 확인합니다.

```
패스프레이즈 입력:
패스프레이즈 반복:
```

맨 위로 돌아가기

TAC 고객 지원 엔지니어에게 비밀번호 전달

첨부 파일을 암호화할 때, 암호화된 비밀번호를 케이스 고객 지원 엔지니어 소유자와 공유합니다. 가장 좋은 방법은 파일을 업로드하는 데 사용되는 것과 다른 방법을 사용하는 것입니다. 이메일 메시지 또는 FTPS를 사용하여 파일을 업로드한 경우에는, 전화 또는 SCM 케이스 업데이트 등과 같은 대역 외 방식으로 비밀번호를 전달합니다.

고객 파일 보관

케이스를 마지막으로 종료한 후 최대 18개월 동안과 케이스가 열려있는 기간에 대해, 케이스 추적 시스템 내에서부터 공인 Cisco 담당자에게 이르기까지 모든 파일에 즉시 액세스할 수 있습니다. 마지막 종료로부터 18개월 동안의 기간이 지난 후, 파일을 보관 스토리지 인스턴스로 이동하여 공간을 절약할 수 있지만 케이스 기록에서 제거(삭제)되지는 않습니다.

인증된 고객 컨택은 언제든지 특정 파일을 케이스에서 제거하는 것을 명시적으로 요청할 수 있습니다. 그러면 Cisco는 해당 파일을 삭제하고 케이스 메모를 추가하여 파일을 삭제한 당사자, 시간 및 날짜 스탬프, 삭제된 파일의 이름을 문서화할 수 있습니다. 이 방식으로 파일을 제거한 후에는 복구할 수 없습니다.

TAC FTP 폴더에 업로드된 파일은 4일 동안 유지됩니다. 파일을 이 폴더에 업로드할 때 케이스 고객 지원 엔지니어 소유자에게 이를 알려야 합니다. 고객 지원 엔지니어는 4일 내에 케이스에 첨부하

여 파일을 백업해야 합니다.

맨 위로 돌아가기

요약

케이스 해결에 도움이 되도록 Cisco TAC에 정보를 업로드하기 위한 여러 옵션이 있습니다. SCM 및 Cisco의 HTML5 업로드 툴은 모두 브라우저를 통해 보안 업로드를 제공하는 반면 CXD는 브라우저, 웹 API 및 다양한 유형의 클라이언트와 Cisco 디바이스에서 지원하는 여러 프로토콜을 통해 업로드를 제공합니다.

SCM, Cisco HTML 5 파일 업로드 툴 또는 파일 업로드 방법으로 FTP가 아닌 CXD에서 지원되는 프로토콜을 사용할 수 없는 경우, 가장 선호하지 않는 파일 업로드 옵션은 FTP, CXD 사용 또는 attach@cisco.com으로 전송되는 이메일 메시지입니다. 이러한 옵션 중 하나를 사용하는 경우에는 전송 전에 파일을 암호화할 것을 강력히 권고합니다. 자세한 내용은 파일 암호화를 참조하십시오. 강력한 비밀번호를 선택하여 전화 또는 SCM 케이스 업데이트 등과 같은 대역 외 방식으로 케이스 고객 지원 엔지니어에게 전달해야 합니다.

케이스를 마지막으로 종료한 후 최대 18개월 동안과 케이스가 열려있는 기간에 대해, 케이스 추적 시스템 내에서부터 공인 Cisco 담당자에게 이르기까지 모든 파일에 즉시 액세스할 수 있습니다.

- 18개월 후에 파일을 보관 스토리지로 이동할 수 있습니다.
- 인증된 고객 컨택은 언제든지 특정 파일을 케이스에서 제거하는 것을 명시적으로 요청할 수 있습니다.
- FTP 폴더의 파일은 4일 동안만 유지됩니다.

추가 정보

- Cisco 기술 서비스에 액세스
- Cisco 전 세계 지원 문의처
- Cisco 기술 서비스 리소스 가이드
- Cisco Security 블로그 - NCSAM 팁 #3: 안전한 비밀번호로 고려해야 할 사항
- Cisco 컨퍼런싱 제품
- GNU 프라이버시 가드
- OpenSSL 프로젝트
- WinZip

이 문서는 Cisco Security Research & Operations의 일부입니다.

맨 위로 돌아가기

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.