

보안 클라이언트 업로드 실패 '파일 업로드 중 오류 문제 해결 방화벽 관리 센터에 충분한 공간이 있는지 확인하십시오.'

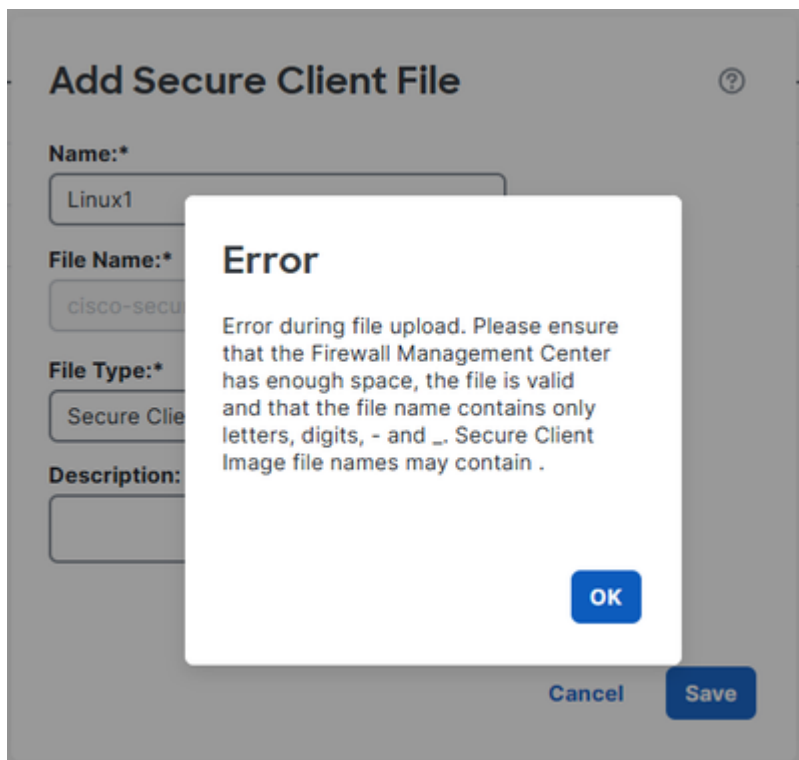
목차

문제

GUI(Graphical User Interface)를 통해 FMC(Firewall Management Center)에 cisco-secure-client-macos-5.1.18.314-webdeploy-k9.pkg와 같은 Cisco Secure Client 패키지 파일을 업로드하면 다음 오류 메시지와 함께 실패하게 됩니다.

Error during file upload. Please ensure that the Firewall Management Center has enough space, the file

파일 체크섬이 올바르고 파일 이름에 공백이나 잘못된 문자가 포함되어 있지 않더라도 업로드가 계속 실패하고 이 오류 메시지가 표시됩니다.



환경

- FMC 7.6.5. 다른 버전도 영향을 받을 수 있습니다.
- Cisco Secure Client 패키지: cisco-secure-client-macos-5.1.18.314-webdeploy-k9.pkg 다른 패키지도 영향을 받을 수 있습니다.
- Object(개체) > Object Management(개체 관리) > VPN > 100MB보다 큰 Secure Client File(보안 클라이언트 파일) 아래의 FMC에서 보안 클라이언트 패키지를 업로드합니다.

해결

해결 방법

1. SSH 세션(또는 콘솔)을 통해 FMC CLI를 엽니다.
2. 다음 명령을 실행합니다.

```
<#root>
```

```
>
```

```
expert
```

```
admin@device:~$
```

```
sudo vim +76 /usr/local/sf/htdocs/ddd/fileUpload.cgi
```

3. 키보드에서 i를 눌러 Vim을 삽입 모드로 전환합니다.
4. 더 큰 파일 패키지를 허용하도록 라인을 업데이트합니다. 특히 다음에서 변경합니다.

```
<#root>
```

```
ANY_CONNECT_IMAGE =>
```

100

1024 1024,

수신:

<#root>

ANY_CONNECT_IMAGE =>

300

1024 1024,



참고: 값은 패키지 파일 크기보다 커야 합니다. 예를 들어, 패키지가 180MB인 경우 200 1024 1024로 안전하게 설정할 수 있습니다. 300을 사용하면 더 큰 패키지를 위한 헤드룸이 제공됩니다.

5. Esc 키를 누르고 :wq를 입력한 다음 Enter 키를 눌러 파일을 저장하고 종료합니다.

6. FMC 웹 인터페이스를 통해 파일을 다시 업로드합니다.

장기적인 솔루션

FMC 버전 및 Secure Client 이미지의 크기에 따라 다음과 같은 결함에 대한 수정 사항이 있는 버전으로 업그레이드합니다.

- Cisco 버그 ID [CSCwi86503](#)는 제한을 200MB로 늘렸습니다.
- Cisco 버그 ID [CSCwq95649](#)에서 한도를 300MByte로 늘렸습니다.

원인

이 문제는 Cisco 버그 ID CSCwi86503 및 CSCwq95649으로 인해 발생하며, 각각 100MB 또는 200MB보다 큰 패키지가 FMC 장치에 업로드되는 것을 방지합니다. 이러한 결함은 FMC GUI의 파

일 업로드 메커니즘에 영향을 미치므로 파일 이름 형식 및 파일 무결성에 대한 모든 요구 사항을 충족하더라도 합법적인 패키지 파일이 거부됩니다.

관련 콘텐츠

- [Cisco 버그 ID CSCwi865033](#)
- [Cisco 버그 ID CSCwq95649](#)
- [Cisco 기술 지원 및 다운로드](#)

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.