



마이그레이션 문제 해결

- [Secure Firewall 마이그레이션 툴 문제 해결, 1 페이지](#)
- [문제 해결에 사용되는 로그 및 기타 파일, 2 페이지](#)
- [Check Point 파일 업로드 실패 문제 해결, 2 페이지](#)

Secure Firewall 마이그레이션 툴 문제 해결

마이그레이션은 일반적으로 Check Point 컨피그레이션 파일을 업로드하는 동안이나 마이그레이션된 컨피그레이션을 Firewall Management Center에 푸시하는 동안 실패합니다.

Check Point 컨피그레이션에서 마이그레이션 프로세스가 실패하는 몇 가지 일반적인 시나리오는 다음과 같습니다.

- Check Point Config.zip에서 파일이 누락되었습니다.
- Secure Firewall 마이그레이션 툴이 Check Point Config.zip에서 잘못된 파일을 감지했습니다.
- Check Point 컨피그레이션 파일이 .zip 이외의 압축 파일 형식인 경우.

Secure Firewall 마이그레이션 툴 지원 번들

Secure Firewall 마이그레이션 툴은 로그 파일, DB, 구성 파일과 같은 중요한 문제 해결 정보를 추출하도록 지원 번들을 다운로드하는 옵션을 제공합니다. 다음을 수행하십시오.

1. **Complete Migration**(마이그레이션 완료) 화면에서 **Support**(지원) 버튼을 클릭합니다.
도움말 지원 페이지가 나타납니다.
2. **Support Bundle**(지원 번들) 체크 박스를 선택한 다음 다운로드할 컨피그레이션 파일을 선택합니다.



참고 로그 및 dB 파일은 기본적으로 다운로드하도록 선택됩니다.

3. **Download**(다운로드)를 클릭합니다.

지원 번들 파일은 로컬 경로에 .zip으로 다운로드됩니다. 압축 폴더의 압축을 풀고 로그 파일, DB 및 컨피그레이션 파일을 봅니다.

4. **Email us**(이메일 문의)를 클릭하여 기술 팀에 실패 세부 정보를 이메일로 보냅니다.

다운로드한 지원 파일을 이메일에 첨부할 수도 있습니다.

5. **Visit TAC page**(TAC 페이지 방문)를 클릭하여 Cisco 지원 페이지에서 TAC 케이스를 생성합니다.



참고 마이그레이션하는 동안 언제든지 지원 페이지에서 TAC 케이스를 열 수 있습니다.

문제 해결에 사용되는 로그 및 기타 파일

다음 파일에서 문제를 식별하고 해결하는 데 유용한 정보를 찾을 수 있습니다.

파일	위치
로그 파일	<migration_tool_folder>\logs
마이그레이션 전 보고서	<migration_tool_folder>\resources
마이그레이션 후 보고서	<migration_tool_folder>\resources
구문 분석되지 않은 파일	<migration_tool_folder>\resources

Check Point 파일 업로드 실패 문제 해결

Check Point 컨피그레이션 파일이 업로드되지 않는 경우 일반적인 이유는 Secure Firewall 마이그레이션 툴이 파일에서 하나 이상의 라인을 구문 분석할 수 없기 때문입니다.

다음 위치에서 업로드 및 구문 분석 실패를 일으킨 오류에 대한 정보를 찾을 수 있습니다.

- **Unparsed file**(구문 분석되지 않은 파일) - 파일의 끝을 확인하여 성공적으로 구문 분석된 Check Point 컨피그레이션 파일의 마지막으로 무시된 라인을 식별합니다.
- **예기치 않은 파일** - Check Point에 대해 잘못된 파일이 감지되었습니다. 예를 들어 Mac OS를 사용하여 압축하면 Mac 시스템 파일이 생성됩니다. Mac 파일을 제거합니다.
- **(r75-r77.30만 해당) Incorrectly named files**(잘못 명명된 파일) - 보안 정책 및 NAT 정책 파일의 이름이 Check Point에 대해 올바르게 지정되지 않은 경우입니다. ACL 및 NAT 파일의 이름을 올바르게 변경합니다.
- **누락된 파일** - Check Point config.zip 파일에서 일부 파일이 누락되었습니다. 필요한 파일을 추가합니다.



참고 r77의 경우 누락된 컨피그레이션 파일을 수동으로 추출합니다. 자세한 내용은 [Check Point r77 컨피그레이션 파일 내보내기](#)를 참조하십시오.

r80-r82의 경우 Live Connect를 사용하여 Secure Firewall 마이그레이션 툴에 대한 올바른 구성 파일을 추출합니다. 자세한 내용은 [Check Point r80-r82 구성 파일 내보내기](#)를 참조하십시오.

Check Point 문제 해결 예: 개체 그룹의 멤버를 찾을 수 없음(r75-r77.30만 해당)

이 예에서는 요소의 컨피그레이션 오류로 인해 Checkpoint 컨피그레이션 파일 업로드 및 구문 분석이 실패했습니다.

프로시저

단계 1 오류 메시지를 검토하여 문제를 식별합니다.

이 실패로 인해 다음 오류 메시지가 생성됩니다.

Location	오류 메시지
Secure Firewall 마이그레이션 툴 메시지	Check Point 컨피그레이션 파일이 구문 분석되어 오류가 발생했습니다. 구문 분석 오류에 대해서는 마이그레이션 전 보고서 오류 섹션을 참조하고, 푸시 단계 중에 발생하는 푸시 오류에 대해서는 마이그레이션 후 보고서 를 참조하십시오.
로그 파일	[ERROR objectGroupRules] > "ERROR, SERVICE_GROUP_RULE not applied for port-group object [services_epacity_nt_abc] as CheckPoint object [ica] does not exist in <service> table;" [INFO objectGroupRules] > "Parsing object-group service:[services_gvxs06]" [INFO objectGroupRules] > "Parsing object-group service:[services_iphigenia]" [INFO objectGroupRules] > "Parsing object-group service:[Services_KPN_ISP]"

단계 2 Check Point services.xml 파일을 엽니다.

단계 3 이름이 services_gvxs06인 개체 그룹을 검색합니다.

단계 4 스마트 대시보드를 사용 중인 개체 그룹에 대해 누락된 멤버를 생성합니다.

단계 5 컨피그레이션 파일을 다시 내보냅니다. 자세한 내용은 [Check Point 컨피그레이션 파일 내보내기](#)를 참조하십시오.

단계 6 오류가 더 이상 없으면 새 Check Point 컨피그레이션 zip 파일을 Secure Firewall 마이그레이션 툴에 업로드하고 마이그레이션을 계속합니다.

Live Connect의 Check Point(r80-r82) 문제 해결 예

예 1: Check Point Security Manager에 대한 세부 정보를 요청합니다.

이 예에서 Secure Firewall 마이그레이션 툴은 Check Point Security Manager에 대한 세부 정보를 요청합니다.

오류 메시지를 검토하여 문제를 식별합니다. 이 실패로 인해 다음 오류 메시지가 생성됩니다.

Location	오류 메시지
Secure Firewall 마이그레이션 툴 메시지	Check Point Security Manager에 대한 세부 정보를 제공하기 위한 요청 화면.
로그 파일	[오류 connect_cp] > "권한 부족, 시간 초과 문제 등으로 인해 Extracted-objects.json 파일을 추출할 수 없습니다. 자세한 정보는 Secure Firewall 마이그레이션 툴 UG를 참조하십시오." 127.0.0.1 - - [20/Jul/2020 17:20:43] "POST /api/CP/connect HTTP/1.1" 500 -

잘못된 자격증명입니다. 자격 증명을 사전 스테이징하려면 다음 단계를 수행합니다. 사용되는 자격 증명에는 Check Point Security Manager용 Check Point Gaia에 /bin/bash 셸 프로파일이 있어야 합니다. 일반 구축을 위해 슈퍼 사용자 권한이 있는 Check Point Security Manager용 Check Point 스마트 콘솔 애플리케이션에서 동일한 자격 증명에 스테이징되어야 합니다. 멀티 도메인 구축을 사용하는 경우 권한은 슈퍼 사용자여야 합니다. 자세한 내용은 [Live Connect를 사용한 컨피그레이션 추출을 위한 Check Point\(r80-r82\) 디바이스 사전 스테이징](#)을 참고하십시오.

예 2: 잘못된 파일 형식

이 예에서는 잘못된 파일 형식으로 인해 Secure Firewall 마이그레이션 툴 마이그레이션이 차단되었습니다.

오류 메시지를 검토하여 문제를 식별합니다. 이 실패로 인해 다음 오류 메시지가 생성됩니다.

Location	오류 메시지
Secure Firewall 마이그레이션 툴 메시지	차단됨
로그 파일	[오류 cp_device_connection] > "잘못된 파일 형식" 2020-07-20 17:10:57,347 [오류 connect_cp] > ".tar 파일을 다운로드할 수 없습니다." 127.0.0.1 - - [20/Jul/2020 17:10:57] "GET /api/CP/generate_tar_file?package=Standard HTTP/1.1" 500 -

잘못된 자격증명입니다. 자격 증명을 사전 스테이징하려면 다음 단계를 수행합니다. 사용되는 자격 증명에는 Check Point Security Manager용 Check Point Gaia에 `/bin/bash` 셸 프로파일이 있어야 합니다. 슈퍼 사용자 권한이 있는 Check Point Security Manager용 Check Point 스마트 콘솔 애플리케이션에서 동일한 자격 증명이 스테이징되어야 합니다. 멀티 도메인 구축을 사용하는 경우 슈퍼 사용자 권한을 부여해야 합니다. 자세한 내용은 [Live Connect를 사용한 컨피그레이션 추출을 위한 Check Point\(r80-r82\) 디바이스 사전 스테이징](#)을 참고하십시오.

예 3: Threat Defense에서 차단된 VSX 기능이 지원되지 않음

이 예에서는 Threat Defense에서 차단된 VSX 기능으로 인해 Secure Firewall 마이그레이션 툴 마이그레이션이 실패합니다.

오류 메시지를 검토하여 문제를 식별합니다. 이 실패로 인해 다음 오류 메시지가 생성됩니다.

Location	오류 메시지
Secure Firewall 마이그레이션 툴 메시지	FTD에서 차단된 VSX 기능이 지원되지 않습니다.
로그 파일	[오류 config_upload] > "VSX 기능이 FTD에서 지원되지 않음" 역추적(가장 최근 호출)

문제 설명 - 이 오류는 Check Point r80.40부터 `fw vsx stat` 명령이 더 이상 사용되지 않을 때 발생합니다.

이 문제를 해결하려면 다음 단계를 수행합니다.

1. `config.zip` 파일의 압축을 풉니다.
2. `networking.txt` 파일을 엽니다.

다음은 샘플 출력의 예입니다.

```
firewall> fw vsx stat
Deprecated command, Please see sk144112 for alternative
Deprecated commands: cphaprob cpinfo cplic fw ips raidconfig fwaccel
```

다음과 같이 수동으로 교체합니다.

```
firewall> fw vsx stat
VSX is not supported on this platform
```

3. 모든 파일을 선택하고 `.zip` 확장자로 압축합니다.

번역에 관하여

Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.

번역에 관하여

Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.