

# FMC에서 보안 클라우드 통합 연결 문제 해결

## 문제

Cisco FMC(Firewall Management Center)는 통합을 위해 Cisco Security Cloud와의 연결을 설정할 수 없습니다.

## 환경

- Cisco Secure FMC for VMware(모든 모델에 적용 가능)
- 소프트웨어 버전: 7.6.2.1(모든 버전에 적용 가능)
- 업스트림 보안 제어/방화벽 정책을 사용하는 네트워크 환경

## 해결

Cisco Security Cloud 통합 연결 문제를 해결하려면 다음 트러블슈팅 및 해결 단계를 수행하십시오.

1: FMC의 다음 명령을 루트 사용자로 사용하여 필요한 Cisco Security Cloud URL에 대한 연결을 테스트합니다.

```
curl -v -k https://www.defenseorchestrator.com
nslookup www.defenseorchestrator.com
telnet www.defenseorchestrator.com 443
curl -v -k https://admin.sse.itd.cisco.com
nslookup admin.sse.itd.cisco.com
telnet admin.sse.itd.cisco.com 443
curl -v -k https://securex.us.security.cisco.com
nslookup securex.us.security.cisco.com
telnet securex.us.security.cisco.com 443
curl -v -k https://api-services.us.sse.itd.cisco.com
nslookup api-services.us.sse.itd.cisco.com
telnet api-services.us.sse.itd.cisco.com 443
curl -v -k https://api-sse.cisco.com
nslookup api-sse.cisco.com
```

```
telnet api-sse.cisco.com 443
curl -v -k https://registration.us.sse.itd.cisco.com
nslookup registration.us.sse.itd.cisco.com
telnet registration.us.sse.itd.cisco.com 443
```

2: 연결 테스트에서 연결 거절 또는 금지된 응답이 표시되면, 업스트림 네트워크 보안 정책을 업데이트하여 us-east-1 지역에 필요한 모든 Cisco Security Cloud URL(사용 중인 지역)에 대한 FMC 아웃바운드 HTTPS 액세스를 허용합니다. 이러한 URL이 FMC에서 중간 방화벽, 프록시 또는 보안 제어를 통해 인터넷으로 연결되는 TCP 포트 443을 통해 허용되는지 확인합니다.



inline\_image\_0.png

- [www.defenseorchestrator.com](http://www.defenseorchestrator.com)
- admin.sse.itd.cisco.com
- securex.us.security.cisco.com을 참조하십시오.
- api-services.us.sse.itd.cisco.com을 참조하십시오.
- api-sse.cisco.com
- registration.us.sse.itd.cisco.com을 참조하십시오.

3: 네트워크 보안 정책을 업데이트한 후 FMC 인터페이스 및 curl/telnet 명령에서 Cisco Security Cloud 통합을 재시도합니다. 이제 모든 필수 클라우드 엔드포인트에 대한 올바른 액세스로 통합이 성공적으로 완료되었습니다.

## 원인

선택한 영역(us-east-1)에 필요한 Cisco 클라우드 URL이 네트워크 보안 제어를 통해 허용되지 않아 통합 프로세스 중에 HTTPS 연결이 실패했기 때문에 FMC가 Cisco Security Cloud 백엔드 서비스에 연결할 수 없습니다.

## 관련 콘텐츠

- [보안 클라우드 제어로 온프레미스 FMC 관리](#)
- [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.