

보안 엔드포인트 - 프라이빗 클라우드 루트 CA 인증서 만료

목차

- [소개](#)
 - [기술 세부사항](#)
 - [영향](#)
 - [라이선스 재생성](#)
 - [라이선스 교체](#)
 - [확인](#)
-

소개

이 문서에서는 라이선스 재생성과 버전 3.9.0 이상의 발표 관련 필수 정보에 대해 설명합니다. 프라이빗 클라우드 릴리스 정보 참조:

<https://docs.amp.cisco.com/Private%20Cloud%20Release%20Notes.pdf>

중요! Secure Endpoint Private Cloud 루트 인증서가 2023년 9월 3일에 만료됩니다. 결과적으로 라이선스가 동시에 만료됩니다. 새 라이선스 파일을 가져오고 정상 운영을 유지하려면 고객 지원에 문의하십시오.

기술 세부사항

영향을 받는 버전: 2023년 4월 11일 이전에 생성된 지원되는 모든 Cisco Secure Endpoint Private Cloud 라이선스.

인증서 체인의 내부 루트 CA 인증서로 사용되는 현재 루트 CA 인증서는 2023년 9월 3일부로 만료됩니다. 이 경로에 있는 인증서의 코드 조각: /opt/fire/etc/ssl/certs(어플라이언스에서 SSH 액세스가 활성화된 경우에만 어플라이언스에서 이 경로를 탐색할 수 있음)

```
[root@fireamp certs]# /usr/bin/openssl x509 -text -noout -in /opt/fire/etc/ssl/certs/root.fireamp.crt Certificate: Issuer: C=US, O=Sourcefire, O=Immunet, OU=PrivateCloud Appliance, CN=FireAMP Private Cloud ROOT CA Validity Not Before: Sep 4 17:32:46 2013 GMT Not After : Sep 2 17:32:46 2023 GMT Subject: C=US, O=Sourcefire, O=Immunet, OU=PrivateCloud Appliance, CN=FireAMP Private Cloud ROOT CA
```

이 인증서 및 관련 인증서 체인을 갱신하려면 라이선스를 다시 생성해야 합니다. 디바이스가 정상적으로 작동하도록 하려면 프라이빗 클라우드 어플라이언스에서 생성 및 적용된 새 라이선스를 가져오는 것이 필수입니다.

라이선스를 재생성하면 다음 인증서가 갱신됩니다.

- ca_intermediate.crt: 인증서 체인 서명에 내부적으로 사용되는 중간 인증서입니다
- ca_signing.crt: 커넥터 정책에 서명하는 데 사용되는 인증서입니다

- chained.fireamp.crt: 내부 서비스에 대한 인증서 검증에 사용됩니다.

중요: root.fireamp.crt는 라이선스 갱신의 일부로 또는 3.9.0 릴리스로 업그레이드하여 갱신되지 않습니다. 이 인증서는 어플라이언스 버전 릴리스 4.0.1의 일부로 갱신됩니다.

영향

새 라이선스가 어플라이언스에 설치되지 않고 CA 인증서가 만료되면 포털에서 정책을 수정할 때 커넥터에서 정책 동기화 실패가 발생합니다. 따라서 라이선스가 2023년 9월 3일에 만료되기 전에 업데이트되어야 합니다

라이선스 재생성

Secure Endpoint Licensing Team에 문의하여 업데이트된 인증서로 라이선스를 다시 생성하도록 요청해야 합니다.

새 라이선스 파일을 받으려면 Support Case Manager에서 온라인으로 지원 사례를 여십시오.

<https://mycase.cloudapps.cisco.com/case>

1단계: Cisco ID로 Cisco Support Portal(Cisco 지원 포털)에 로그인한 후 "Open New Case(새 케이스 열기)"를 클릭합니다.

2단계: Software Licensing -> Security Related Licensing -> FireAMP/ThreatGrid를 선택합니다.

3단계: "Problem Description"(문제 설명)에 이 정보를 기입하십시오.

Cisco.com ID:

제품 이름: Cisco Secure Endpoint Private Cloud

문제/요청 세부사항: 새 루트 CA가 포함된 프라이빗 클라우드 라이선스

Cisco SO# 및/또는 웹 주문 ID 번호:

회사 이름:

전체 이름:

Email:

장치 ID:

중요 !!

4단계: 관리 포털(Configuration(컨피그레이션) -> License(라이선스)의 라이선스 페이지 스크린샷을 추가할 것을 요청합니다.

5단계: 요청을 받으면 새 라이선스를 다시 생성합니다. Secure Endpoint Provisioning 팀이 이메일을 통해 새 라이선스를 보냅니다.

라이선스 교체

Cisco 라이선싱 팀으로부터 받은 새 라이선스를 사용하는 방법에 대한 지침은 Secure Endpoint Private Cloud Administration Portal Guide(Secure Endpoint Private Cloud 관리 포털 설명서)(<https://docs.amp.cisco.com/SecureEndpointPCAdminGuide.pdf>)를 참조하십시오.

28페이지의 "라이선스" 섹션을 참조하십시오.

라이선스를 교체한 후에는 어플라이언스를 재구성하여 새 라이선스를 적용하십시오.

확인

중요: 3.9.0 이상 버전의 어플라이언스에서는 새 라이선스가 적용된 후에도 프라이빗 클라우드 어플라이언스 관리 포털의 알림이 계속 표시되며 안전하게 무시될 수 있습니다. 이 문제는 어플라이언스 릴리스 4.1.0에서 수정되며, 문제가 이전 릴리스에서 수정되었는지 확인하기 위해 이 프로세스를 따를 수 있습니다.

인증서가 올바르게 갱신되었는지 확인하려면 다음 단계를 수행하십시오.

```
[root@fireamp certs]# /usr/bin/openssl x509 -text -noout -in /opt/fire/etc/ssl/certs/ca_intermediate.crt Certificate: Data: Version: 3 (0x2) Serial Number: 2 (0x2) Signature Algorithm: sha256WithRSAEncryption Issuer: C=US, O=Sourcefire, O=Immunet, OU=PrivateCloud Appliance, CN=FireAMP Private Cloud ROOT CA Validity Not Before: Mar 2 04:10:43 2023 GMT Not After : Feb 29 04:10:43 2028 GMT
[root@fireamp certs]# /usr/bin/openssl x509 -text -noout -in /opt/fire/etc/ssl/certs/ca_signing.crt Certificate: Data: Version: 3 (0x2) Serial Number: 7330 (0x1ca2) Signature Algorithm: sha256WithRSAEncryption Issuer: C=US, O=Sourcefire, O=Immunet, OU=PrivateCloud Appliance, CN=FireAMP Private Cloud Intermediate CA/emailAddress=private-cloud-licensing@sourcefire.com Validity Not Before: Apr 11 12:42:45 2023 GMT Not After : Apr 9 12:42:45 2028 GMT [root@fireamp certs]# /usr/bin/openssl x509 -text -noout -in /opt/fire/etc/ssl/certs/chained.fireamp.crt Certificate: Data: Version: 3 (0x2) Serial Number: 2 (0x2) Signature Algorithm: sha256WithRSAEncryption Issuer: C=US, O=Sourcefire, O=Immunet, OU=PrivateCloud Appliance, CN=FireAMP Private Cloud ROOT CA Validity Not Before: Mar 2 04:10:43 2023 GMT Not After : Feb 29 04:10:43 2028 GMT
```

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.