Cisco IOS XE 및 GuestShell CA Trust eMudhra Intrust 가이드

목차

목적

이 문서에서는 Mudhra 루트 및 중간 인증 기관에 대한 긴급 불신을 위한 Cisco IOS® XE 지침을 제공합니다.

컨피그레이션에서 영향을 받는 계층을 허용하는 서비스에 대한 CA 트러스트를 감사하고 관리하려면 이 가이드를 사용합니다. 제품 적용 가능성 및 필요한 교정은 Cisco 정보 제공에 정의되어 있습니다. 신뢰를 변경하기 전에 Cisco IOS XE 릴리스에 대한 명령 지원 및 서비스 영향을 확인하십시오.

Cisco 정보: cisco-sa-emudhra-info-ScS22A1r

영향을 받는 도메인 CA 인증서: 원본 및 상호 서명

2026년 10월 29일에 인벤토리 확인됨 8개의 Mudhra 발급 CA 키가 영향을 받습니다. TLS는 6개, 코드 서명은 2개입니다. 각 키는 원래 emSign에서 발급한 CA 인증서 및 Sectigo 교차 서명된 CA 인증서에 나타납니다. 따라서 인벤토리에는 16개의 인증서가 포함됩니다. 12개의 TLS 및 4개의 코드 서명 인증서

각 원래/교차 서명 쌍에는 동일한 주체 및 공개 키가 있지만 발급자, 일련 번호 및 SHA-256 인증서 지문이 다릅니다. 두 양식은 대체 인증 경로를 제공하며 둘 다 감사에 포함해야 합니다.

A. 발급자 및 영향을 받는 인증서 인벤토리

발급자 A — 원래 TLS 인증서: CN=emSign 루트 TLS CA - G3, O=Mudhra Technologies Limited, C=IN.

발급자 B — 원래 코드 서명 인증서: CN=emSign 루트 CS CA - G3, O=Mudhra Technologies Limited, C=IN.

발급자 C — 모든 상호 서명 인증서: CN=AAA Certificate Services, O=Comodo CA Limited,

L=Salford, ST=Greater Manchester, C=GB(Sectigo).

G3B 제목: O=eMudhra BV, C=NL. G3C 제목: O=eMudhra Inc, C=US 각 변형 셀은 발급자 참조, 16진수 시리얼 및 SHA-256 핑거프린트(두 줄)를 나열합니다. 선행 제로 패딩은 직렬 값을 변경하지 않습니다.

영향을 받는 발급 CA(CN)	원본 인증서 발급자/일련 번호(16진수)/SHA-256	Sectigo 상호 서명 인증서 발급자/일련 번호(16진수)/SHA-256
1. EM DV TLS CA - G3B TLS	발급자 A A4AEE678F23362B4C0E460B772F214 42C4ACCD12C4F59597925E1A08A7A901 02608543809308D50EC427E118BA1493	발급자 C A024FDF4BA665C785CE4A020483858B7 45A883F349AEDFD5F3A649B5498FFB12 1712BA8B448F3F2A91DBC5A766FCDDBE
2. EM OV TLS CA - G3B TLS	발급자 A 6CADA367FB1C100088120EA202D568 98B896625C0C230ADEEC3EB2CF6AAD50 01ECF9156A68644E82374CE5833BC25B	발급자 C E94223BDE92F914E5AB9ACABFDAC3710 5F1DED4DD590AF74631290CF073B122A 2AAC6A1FA479778A0BD43579BD832699
3. EM EV TLS CA - G3B TLS	발급자 A C7C41EFE92D825F05EAE841A4A82C1 E7568FE6E12331F4FD7DE61DA4C7559D 0F8EB192A218D4741A3BA75184333838	발급자 C D8F8685E4F2BD9D82402A85A1C1EB731 579480AEA166290BD3C643589E795FC0 D0E54E86505D180F1DFF99EFD3199512
4. EM DV TLS CA - G3C TLS	발급자 A 588B2E3C2BB8CDA13E1A1209254321 0164D7CEAE5BB909C272AF151FF44B11 77AE9B47D9424B94F1D9558C30934D19	발급자 C 91F347F1A5B7D39962B95E0EE4E299D1 62B7F9868263F72F6911FC78CEAF72C1 979158B7368BF648683BB2AA39B02E72
5. EM OV	발급자 A	발급자 C

영향을 받는 발급 CA(CN)	원본 인증서 발급자/일련 번호(16진수)/SHA-256	Sectigo 상호 서명 인증서 발급자/일련 번호(16진수)/SHA-256
TLS CA - G3C TLS	296926C227A3A1526392B19482A504 CB6E15165AC802E9B3F993F16C25D41F 4E81C21EBDE71AE1B012AC00BF9C7C3F	8D5A4811939EF447D77111CDD9849AE9 7485B51C0ED192878FA1D2F948FB529A E1842CC5086C4B67F7BE5B2039DE9489
6. EM EV TLS CA - G3C TLS	발급자 A 8009928A64107601AF05FA2F19F109 432EC25F0D28DE9006D97BF752F17BBB 2CD41F669933FCB072D9A1148D0261F3	발급자 C 05F078752DECE7A1BB8595D303167171 FD9D5C2DBBD4995AB69B8D50C439D952 7B00529199C2FD01B2174EB58F07021F
7. EM OV CS CA - G3B 코드 서명	발급자 B 7818933F8F85B4619A2B35FBA83D0A 9E39DE2881273ACC225A149C72BA3E0F 51424963669AB633EE1DC7DF5DB067B4	발급자 C 41E32B73AC185D6CE0D7480BACF84E69 A496E23AC0CAB8155FC9B117B97EAE36 8EFCBB9041AEC8804D5A308D2D01C2D8
8. EM OV CS CA - G3C 코드 서명	발급자 B 544B7F922C31AE220A4A922916F6E6 4B2460A466F95FD40113BCDCCA2CEB29 B3B093921DE45474DA7DF48874C630B1	발급자 C D6A5EF613B390F32EF9CDF349F772841 84112972B8E59D14560AE7E711965447 4AAD119990CF3722BFC1E3B91615E1FD

B. 구별할 수 있는 인증 경로

원래 TLS 경로

```
emSign ECC Root CA - G3
  +-- emSign Root TLS CA - G3 (issued by emSign ECC Root CA - G3)
       +-- Original EM DV/OV/EV TLS CA - G3B or G3C
            +-- TLS identity certificate
```

원래 코드 서명 경로(루트 CS를 직접 신뢰함)

```
emSign Root CS CA - G3
  +-- Original EM OV CS CA - G3B or G3C
       +-- Code-signing identity certificate
```

섹터 교차 서명 경로(TLS 및 코드 서명)

```
AAA Certificate Services
  +-- One of the eight cross-signed CAs listed above
       +-- TLS or code-signing identity certificate
```

TLS 경로는 emSign Root TLS CA - G3에서 종료할 수 있으며, 이 CA를 직접 신뢰합니다. 다이어그램에는 관련 발급자 관계가 나와 있습니다. 수락된 경로는 사용 중인 서비스의 트러스트 앵커 및 유효성 검사 정책에 따라 달라집니다.

표시된 상위/루트 CA는 체인 컨텍스트를 제공하며 8개의 손상된 발급 키에 포함되지 않습니다. 상위/루트를 제거하거나 불신하는 결정은 손상된 중간 키를 식별하는 것과는 별개입니다.

식별을 위해 인증서 발급자 및 일련 번호를 SHA-256 핑거프린트와 함께 사용합니다. 주체 이름만으로는 충분하지 않습니다. 인증서 핑거프린트는 하나의 인증서 변형을 식별합니다. spki SHA-256 해시는 원본 및 교차 서명된 양식에서 공유하는 공개 키를 식별합니다. 캐시된 중간만 제거해도 피어가 나머지 신뢰할 수 있는 경로를 통해 중간을 제공할 수 있습니다.

소스 및 확인 날짜

인증서 식별자는 2026년 10월 29일 공개 인시던트 첨부에 대해 검증되었습니다. 각 원본/교차 서명 쌍에는 동일한 공개 키가 포함되어 있습니다. 제품 적용 가능성 및 교정 상태에 대해서는 라이브 Cisco 정보를 사용합니다.

Cisco 정보: cisco-sa-emudhra-info-ScS22A1r

Mozilla 인시던트 레코드: eMudhra 중간 키 보안 침해(2083449)

원래 CA 인증서 첨부 파일(9664066)

AAA 상호 서명 CA 인증서 첨부 파일(9664067)

Apple: 원본 및 교차 서명된 TLS 인증서 경로 및 핑거프린트

2026년 10월 31일을 기준으로 이 가이드에 나와 있는 손상된 CA 중에서 emSign 루트 CA - G1이 식별되지 않습니다. 신뢰가 지속되면 조직 정책 및 후속 자문 업데이트의 적용을 받습니다.

Cisco IOS XE에서 인증서 신뢰를 관리하는 방법

구성된 PKI 신뢰 지점에는 CA/ID 인증서 및 검증 정책이 있습니다. PKI 신뢰 풀에는 이 신뢰 풀을 사용하는 서비스에 대한 기본 제공 및 다운로드된 CA 인증서가 포함되어 있습니다. 각 관련 서비스에서 사용하는 트러스트 소스 및 정책을 식별합니다. 신뢰 풀을 변경해도 별도로 구성된 신뢰 지점은 교체되지 않습니다.

1. 감사 및 준비

소프트웨어 릴리스, 장치 시간 및 설치된 인증서를 확인합니다.

<#root>

```
show version show clock show crypto pki trustpoints show running-config | section crypto pki trustpoint
```

Subject(주체)를 지원 컨텍스트로 사용하여 전체 인증서 발급자 및 16진수 일련 번호를 인벤토리와 비교합니다. Cisco IOS XE에 MD5 및 SHA1 지문만 표시되는 경우, 인벤토리 SHA-256 지문은 해당 출력에서 직접 비교할 수 없습니다. 디바이스 외부의 인증서 파일 확인을 위해 제공됩니다. 일련 번호의 00 안쪽 여백은 다를 수 있습니다. 공급업체 이름 검색에서는 후보자만 식별합니다. 각 신뢰 지점에 의존하는 서비스를 기록하고 직접 신뢰하는 중간을 포함하여 원래 경로와 교차 서명된 경로를 모두 확인합니다.

예: 루트 CA 및 영향을 받는 하위 CA

자세한 인증서의 축약된 예가 표시됩니다. 다른 필드는 생략됩니다. Subject(주체), Issuer(발급자) 및 Serial Number(일련 번호)를 비교합니다.

루트 CA 예: emSign ECC 루트 CA - G3

```
CA Certificate
```

```
  Certificate Serial Number (hex): 3CF607A968700EDA8B84
  Issuer:
    cn=emSign ECC Root CA - G3
  Subject:
    cn=emSign ECC Root CA - G3
  Associated Trustpoints:
```

영향을 받는 하위 CA 예: 원본 emSign 발급 인증서

```
CA Certificate
  Certificate Serial Number (hex): 00A4AEE678F23362B4C0E460B772F214
  Issuer:
    cn=emSign Root TLS CA - G3
  Subject:
    cn=EM DV TLS CA - G3B
  Associated Trustpoints:
```

영향을 받는 하위 CA 예: Sectigo 상호 서명 인증서

```
CA Certificate
  Certificate Serial Number (hex): 00A024FDF4BA665C785CE4A020483858B7
  Issuer:
    cn=AAA Certificate Services
  Subject:
    cn=EM DV TLS CA - G3B
  Associated Trustpoints:
```

두 SubCA 양식 모두 Subject는 동일하지만 Issuer와 serials가 다릅니다. 전체 발급자 및 일련번호를 인벤토리에 대응시킵니다. 앞에 00 패딩은 다를 수 있습니다. 연결된 신뢰 지점을 기록하여 소유 신뢰 지점 또는 풀을 찾습니다. 표시된 루트는 체인 컨텍스트입니다. 8개의 보안 침해 발생 키 중 하나가 아닙니다.

복구 액세스 방법 및 승인된 교체 번들을 사용할 수 있도록 유지합니다. 필요한 경우 승인된 인증서/키 백업 절차를 사용합니다. 컨피그레이션 백업 이 복사본만 개인 키 백업이 아닙니다.

<#root>

copy running-config

꺾쇠 괄호 자리 표시자를 승인된 장치별 값으로 바꿉니다. flash와 같은 show 파일 시스템에 표시된 파일 시스템을 사용합니다. 또는 bootflash:.

2. 신뢰 경로 검토

직접 신뢰받는 영향을 받는 하위 CA 제거

신뢰 지점 및 다운로드한 신뢰 풀 번들에서 직접 신뢰받는 영향을 받는 하위 CA를 제거합니다. 손상된 CA에서 직접 신뢰를 재정의하려면 해지 설정에 의존하지 마십시오.

선택적 루트 CA 제거

루트 CA 제거는 추가 보호를 위한 선택적 권장 사항입니다. 실제 서비스 CRL/OCSP에서 현재 상태를 확인하고, 신뢰할 수 있는 상위 항목에서 영향을 받는 SubCA를 평가하고, 영향을 받는 원본, 교차 서명 및 적용 가능한 더 긴 체인을 거부하고, 구성된 방법 중 어느 것도 사용 가능한 상태를 제공하지 않는 경우 유효성 검사에 실패할 경우, 필수 루트를 신뢰할 수 있습니다. 이러한 확인된 조건에서 폐기 검사는 루트를 삭제하지 않고 식별된 감염된 발급자를 보호합니다.

해지 서비스에 대한 의존도를 줄이기 위해 불필요한 루트/트러스트 앵커를 제거하는 것을 고려하십시오. 먼저 서비스 종속성 평가: aaa 인증서 서비스를 제거하면 관련이 없는 합법적인 체인을 중단할 수 있습니다. eMudhra 및 AAA 경로를 모두 포함합니다. 캐시된 SubCA만 삭제해도 나머지 신뢰할 수 있는 상위 항목을 통해 피어 제공 복사본이 차단되지 않습니다.

선택한 신뢰 지점 제거

제거할 관리자가 구성한 신뢰 지점의 경우:

<#root>

configure terminal no crypto pki trustpoint

end

수락하기 전에 확인을 검토하십시오. 신뢰 지점을 제거하면 연결된 인증서가 제거됩니다. 디바이스 ID를 교체해야 하는 경우 디바이스 키와 일치하는 교체 인증서를 얻고 서비스 등록 절차를 사용하여 서비스 바인딩을 업데이트합니다. 새 CA 인증서를 설치한다고 해서 디바이스 ID가 대체되는 것은 아닙니다.

다운로드한 신뢰 풀 항목의 경우 번들 교체 절차를 사용합니다. 내장형 또는 기능 관리 앵커는 지원되는 제품 업데이트 또는 Cisco TAC 지침이 필요합니다.

3. 필요한 경우 다운로드한 신뢰 풀을 업데이트합니다

다운로드한 번들에 교체가 필요한 경우 다음 단계를 수행합니다. 필수 상위/루트는 2단계의 검증된 폐기 조건에서 계속 신뢰할 수 있습니다.

3.1 다운로드한 번들이 설치되어 사용되고 있는지 확인

<#root>

show running-config | section crypto pki certificate pool show crypto pki trustpool verbose show crypto

crypto pki certificate pool(암호화 pki 인증서 풀) 및 Trustpool(신뢰 풀)로 표시된 CA 레코드에서 케이블 항목을 찾습니다. 다운로드했습니다. 번들 파일 이름은 ios.p7b 또는 ios_core.p7b와 다를 수 있습니다. 저장된 파일 또는 구성된 새로 고침 URL만으로는 해당 인증서가 서비스에 의해 설치되었거나 사용되고 있음을 증명하지 않습니다. 서비스가 신뢰 풀을 사용하는지 확인하고 해당 CA 레코드를 영향받는 인벤토리와 비교합니다. 다운로드한 CA가 설치되지 않은 경우 정리 및 교체를 건너뜁니다. 다른 트러스트 소스를 평가합니다.

3.2 다운로드한 신뢰 풀을 정리합니다

정리 전에 복구 액세스 및 승인된 복구 번들을 사용할 수 있도록 유지합니다. 전송이 트러스트를 제거하는 데 의존할 경우 이후에 다운로드하지 못할 수 있습니다. 종속 서비스 중단에 대한 계획

<#root>

configure terminal crypto pki trustpool clean end

show crypto pki trustpool verbose

다운로드한 CA 레코드가 없어졌는지 확인합니다. 정리에서는 다운로드한 모든 신뢰 풀 인증서 및 관리되는 번들 파일을 제거합니다. 내장형 CA와 별도의 신뢰 지점은 그대로 유지됩니다. 교체 및 서비스 확인이 성공할 때까지 저장하지 마십시오.

3.3 승인된 교체 번들 받기 및 설치

승인된 Cisco 서명 번들을 얻습니다. 필수 서비스에 대해 ios.p7b 또는 ios_core.p7b를 선택하고 영향받는 인증서 및 위에서 식별한 원치 않는 트러스트 앵커를 제외하는지 확인합니다. 2026년 10월 31일에 확인된 레거시 번들에는 ios.p7b의 emSign Root CA - G1이 포함되어 있지만 ios_core.p7b의 eMudhra 또는 AAA Certificate Services CA는 포함되어 있지 않습니다. 코어에 더 작은 신뢰 집합이 있습니다. 전환하기 전에 서비스 종속성을 확인하고 설치한 번들의 내용을 확인합니다. 승인된 HTTPS 또는 SCP 전송을 사용하여 관리되는 신뢰 풀 스토리지 외부로 스테이징합니다.

Cisco 전체 CA 번들: ios.p7b

Cisco 코어 CA 번들: ios_core.p7b

<#root>

show file systems copy

configure terminal crypto pki trustpool import url

end show crypto pki trustpool verbose

예를 들어 준비된 URL은 flash:approved-ios.p7b일 수 있습니다. 가져오기가 실패할 경우 저장하기

전에 승인된 번들을 복원합니다. 원하는 CA 및 필요한 연결을 확인합니다. 정리가 인증서 거부 목록이 아닙니다. 나머지 신뢰 지점, 내장 CA 및 대체 경로가 강제 폐기 또는 신뢰 경로 제거를 통해 영향을 받는 체인을 거부하는지 확인합니다.

4. 검증 및 새로 고침 정책 구성

변경하기 전에 기존 신뢰 풀 정책, 영향을 받는 신뢰 지점 정책, 인증서 맵 바인딩을 기록하고 필요한 경우 복원할 수 있도록 URL을 새로 고칩니다.

관련 구성된 신뢰 지점의 경우:

<#root>

configure terminal crypto pki trustpoint

revocation-check crl ocsp exit end

신뢰 풀 정책을 사용하는 서비스의 경우:

<#root>

configure terminal crypto pki trustpool policy chain-validation revocation-check crl ocsp exit end show

표시된 신뢰 풀 정책이 루트에 대한 검증을 계속하고 crl ocsp를 나열하는지 확인합니다. 디바이스는 CRL을 먼저 시도하고 CRL 검색을 사용할 수 없을 때 OCSP를 시도합니다. 영향을 받는 인증서를 평가할 때 취소된 결과는 검증에 실패합니다. 성공적인 폐기 검사가 필요한 경우 아무 것도 추가하지 마십시오.

올바른 시간, 연결 가능한 CA 게시 상태 엔드포인트, 수락된 응답 형식 및 적용 가능한 폐기-생략 예외 없음을 확인합니다. 영향을 받는 SubCA 상태는 신뢰할 수 있는 부모 아래에서 평가되어야 합니다. 해당 SubCA의 직접 신뢰는 상위 항목을 확인하기 전에 검증을 중지할 수 있습니다. 실제 서비스가 사용 가능한 현재 상태를 가져오고 영향을 받는 체인을 거부하는지 확인합니다. 상태 서버 액세스 및 거부 동작을 확인할 수 없는 경우 컨피그레이션만 확인된 보호로 간주하지 마십시오. 완화

계획에 필요한 경우 관련 신뢰 경로를 제거하십시오. 사용 불가 상태를 우회하려면 없음을 추가하지 마십시오.

보호를 확인하기 전에 캐시된 CRL 새로 고침

CA가 새로운 CRL을 게시한 후에도 이미 로컬 캐시/데이터베이스에 있는 사용 가능한 CRL을 재사용할 수 있습니다. 상태-서버 연결성을 확인한 다음 보호를 검증하기 전에 이전 CRL을 지웁니다.

<#root>

show crypto pki crls clear crypto pki crl show crypto pki crls

clear 명령은 모든 신뢰 지점에 대한 로컬 CRL을 제거합니다. 교체 제품을 다운로드하는 것은 아닙니다. 이전 항목이 제거되었는지 확인한 다음 해당 서비스에서 새 연결 또는 인증서 검증을 시작합니다. show crypto pki crl을 다시 실행하고 각 관련 발급자, LastUpdate, NextUpdate 및 배포 지점을 CA의 현재 게시에 대해 확인합니다. ID 인증서 발급자 CRL뿐만 아니라 영향받는 SubCA를 포괄하는 상위 발급자 CRL을 포함합니다. 영향을 받는 체인이 거부되었는지 확인합니다. 지우기는 상태 데이터를 가져오는 동안 새 연결에 일시적으로 영향을 줄 수 있습니다. fail-closed 검증을 유지합니다.

번들 새로 고침 소스 검토

연결된 디바이스의 경우, 승인된 만료 기반 번들 새로 고침 소스를 선택적으로 구성합니다.

<#root>

configure terminal crypto pki trustpool policy cabundle url

exit end show crypto pki trustpool policy

구성된 모든 번들 소스를 검토합니다. 만료 기반 새로 고침은 즉각적인 보안 업데이트를 대체하지 않으며 원하지 않는 신뢰 경로를 복원해서는 안 됩니다.

선택적 certificate-map 필터: 적용 범위 및 제한 사항

Cisco IOS XE 인증서 맵(cert-map)은 발급자 이름과 같은 인증서 특성과 일치합니다. 추가 조치로서, 필터는 나열된 8개의 CA에서 직접 발급한 ID(리프) 인증서를 거부하는 데 도움이 될 수 있습니다. 기존 일치 인증서 정책을 적용하기 전에 신뢰 지점을 검토합니다.

실험용 랩 장치에서 EM DV TLS CA - G3B에 따라 실험실 ID를 사용하여 2026년 10월 29일에 동작을 테스트했습니다. PKI 피어 인증서 검증에서 필터는 직접 발급된 ID를 거부했지만 추가 하위 SubCA를 통해 발급된 ID는 차단하지 않았습니다. 목록에 없는 올바른 발급자가 통과했습니다. 동작 검사 기능은 영향을 받는 발급자 하나를 사용했으며, 필터를 격리하기 위해 임시 랩 신뢰 지점에서만 해지 기능이 비활성화되었습니다. 이 필터로 응용 프로그램 핸드셰이크 및 기타 릴리스를 검증하지 않았습니다. 실제 서비스에 의존하기 전에 테스트합니다.

<#root>

configure terminal crypto pki certificate map EMSIGN-ISSUER-FILTER 10 issuer-name nc cn=EM DV TLS CA - G

match certificate EMSIGN-ISSUER-FILTER exit end

여기서 nc는 '포함하지 않음'을 의미한다. 8개의 모든 부정적인 발급자 이름 조건을 동일한 항목(시퀀스 10)에 유지하십시오. 이 필터를 통과하려면 인증서가 모두 일치해야 합니다. 나열된 이름과 일치하는 직접 발급자가 필터를 통과하지 못합니다.

Cisco IOS XE는 표준화된 항목을 표시할 수 있습니다(예: issuer-name nc cn = em dv tls ca - g3b). 이 소문자와 간격 형식은 행동 검사에 존재하였다. 서비스에서 실제로 사용하는 검증 신뢰 지점에 대한 맵 및 해당 바인딩을 확인합니다.

<#root>

show running-config | section crypto pki certificate map show running-config | section crypto pki trustp

이 필터는 체인 차원의 CA 거부 목록을 제공하지 않습니다. 예를 들면 다음과 같습니다.

Trusted root CA

```
  +-- Affected SubCA
       +-- New child SubCA
            +-- ID (leaf) certificate
```

ID 인증서 발급자는 새 하위 SubCA이므로 발급자 이름 필터는 체인에서 더 위에 있는 영향을 받는 CA를 식별하지 않습니다. CA 제약 조건 및 폐기 등 다른 검사도 계속 적용됩니다. 이 가이드에서 폐기 검증 및 선택적 루트 제거 절차와 함께 이 필터를 추가 보호로만 사용합니다. 실제 서비스로 직접 발급된 하위 SubCA 및 합법적인 인증서를 테스트합니다.

4단계 롤백

기록된 폐기 방법, 체인 유효성 검사 설정 및 인증서 맵 바인딩을 복원합니다. 이 절차에서 추가한 새로 고침 URL을 제거하고 변경된 이전 URL을 복원합니다. 이 예에서는 추가된 새로 고침 URL 및 필터 바인딩만 제거합니다. 다른 정책 설정은 복원되지 않습니다.

<#root>

configure terminal crypto pki trustpool policy no cabundle url

exit

crypto pki trustpoint

no match certificate EMSIGN-ISSUER-FILTER exit end

이 절차에 의해 URL 및 바인딩이 추가된 경우에만 이러한 제거를 실행합니다. 이전 인증서 맵 바인딩이 대체된 경우 복원합니다. 다른 컨피그레이션에서 참조하는 맵이 없음을 확인한 후에만 새로 생성된 맵을 제거합니다.

기본값으로 재설정하는 경우에만 crypto pki trustpool 정책을 사용하지 마십시오. 이 광범위한 재설

정은 구성된 새로 고침 URL을 지우고 폐기 검사를 none으로 재설정합니다. 이전 사용자 지정 정책을 복원하지 않습니다. 정책 롤백은 삭제된 인증서를 복원하지 않으며, 설치된 번들을 되돌리거나 지워진 CRL을 복원합니다. 저장하기 전에 필요한 서비스 및 영향을 받는 체인 거부를 다시 확인하십시오.

5. 보호 확인 및 저장

- 피어 공급 중간을 포함하여 영향을 받는 원래 체인과 교차 서명 체인이 거부되었는지 확인합니다. 더 긴 체인이 관련된 경우, 영향을 받는 CA가 더 높은 체인에 있을 때 거부를 확인합니다.
- 필수 정상 연결이 여전히 작동하며 대체 ID가 원하는 서비스에 바인딩되어 있는지 확인합니다.
- 해지 데이터를 사용할 수 없을 때 동작 확인 기존 TLS/IPsec 세션은 정책 변경을 통해 자동으로 재검증되지 않습니다. 필요한 경우 서비스 지원 재연결 절차를 사용합니다.

검사가 성공한 후:

<#root>

```
show crypto pki certificates verbose show crypto pki trustpool policy write memory
```

다음 계획된 다시 로드 후 및 해당되는 경우 대기 디바이스에서 지속성을 확인합니다. 결과가 예상 신뢰 정책과 다를 경우, 로그를 보존하고 Cisco TAC에 문의한 후 확인된 신뢰 변경 사항을 고려하십시오.

추가 읽기

Cisco IOS XE PKI 신뢰 풀 관리

Cisco: Cisco IOS XE PKI를 사용하여 CA 서명 인증서 구성

Cisco: CRL 캐싱 및 해지 확인

Cisco IOS XE GuestShell CA 트러스트 가이드

1단계: 장치 GuestShell 배포 상태 감사

GuestShell이 설치되어 있고 RUNNING 또는 DEPLOYED 상태인 Cisco IOS XE 시스템에서만 교정이 필요합니다. GuestShell이 DEPLOYED 상태인 경우 교정 명령을 실행하기 전에 먼저 'guestshell enable' 명령으로 활성화해야 합니다. show app-hosting list에 '앱을 찾을 수 없음'이 표시되면(GuestShell이 배포되거나 활성화되지 않음) GuestShell에 대한 작업이 필요하지 않습니다.

A. DEPLOYED 상태의 GuestShell(작업 필요: 먼저 활성화해야 함)

show app-hosting list가 DEPLOYED 상태의 GuestShell을 보고할 경우 GuestShell 컨테이너 저장소가 있지만 컨테이너가 중지됩니다. bash를 입력하기 전에 'guestshell enable'을 실행해야 하며, 선택적으로 교정을 완료한 후 중지된 상태로 돌아가면 'guestshell disable'을 실행해야 합니다.

<#root>

```
Router#

show app-hosting list

App id                                   State
------------------------------------------------------------
guestshell                               DEPLOYED
```

B. GuestShell이 RUNNING 상태임(작업 필요: 직접 진행)

show app-hosting list reports GuestShell in the RUNNING state(앱 호스팅 목록 표시)에서 GuestShell이 실행 중이므로 GuestShell이 실행 중이므로 다음 단계로 직접 진행할 수 있습니다.

<#root>

```
Router#

show app-hosting list

App id                                   State
------------------------------------------------------------
guestshell                               RUNNING
```

B. GuestShell 사용 안 함/배포되지 않음(작업 필요 없음)

show app-hosting list에 No App found가 표시되면 GuestShell이 시스템에 설치되어 있지 않거나 활

성화되어 있지 않으며 추가 작업이 필요하지 않습니다.

<#root>

```
Router#

show app-hosting list

No App found
```

2단계: GuestShell 액세스 및 CA 불신 적용

Cisco IOS XE 특권 EXEC('enable') 프롬프트에서 이 명령을 실행합니다. GuestShell이 DEPLOYED 상태인 경우 먼저 활성화하십시오. 그런 다음 기본 셸을 입력하고 루트로 에스컬레이션한 다음 모든 Cisco IOS XE 릴리스에서 호환성을 보장하도록 동적 폴더 선택을 사용하여 CA 차단 목록을 구성합니다.

<#root>

```
! 1. If GuestShell is in DEPLOYED state, enable it first:
Router#

guestshell enable


! 2. Enter GuestShell bash shell:
Router#

guestshell run bash


! 3. Escalate to root user inside GuestShell:
[guestshell@guestshell ~]$

sudo -s


! 4. Prepare the ca-trust blocklist directory (compatible with 17.15.x and 17.18.x):
d=/etc/pki/ca-trust/source/blocklist
[ -d "$d" ] || d=/etc/pki/ca-trust/source/blacklist
mkdir -p "$d"
```

손상된 Mudhra 인증서 불멸

trust extract 명령을 실행하여 손상된 각 eMudhra 인증서를 ca-trust blocklist 디렉토리로 직접 추출한 다음 시스템 신뢰 저장소를 재구축합니다.

```
trust extract --overwrite --format=pem-bundle \
  --filter='pkcs11:object=emSign%20ECC%20Root%20CA%20-%20G3;type=cert' \
  "$d/emSign_ECC_Root_CA_-_G3.pem"

trust extract --overwrite --format=pem-bundle \
  --filter='pkcs11:object=Comodo%20AAA%20Services%20root;type=cert' \
  "$d/Comodo_AAA_Services_root.pem"

trust extract --overwrite --format=pem-bundle \
  --filter='pkcs11:object=emSign%20ECC%20Root%20CA%20-%20C3;type=cert' \
  "$d/emSign_ECC_Root_CA_-_C3.pem"

trust extract --overwrite --format=pem-bundle \
  --filter='pkcs11:object=emSign%20Root%20CA%20-%20C1;type=cert' \
  "$d/emSign_Root_CA_-_C1.pem"

update-ca-trust extract
```

3단계: GuestShell에서 신뢰할 수 없는 인증서 확인

추출된 인증서 4개가 시스템 불신/차단 목록 정책에 표시되고 아래 verification 명령을 사용하여 활성 트러스트 앵커에서 제외되는지 확인합니다. 이 명령은 인증서가 차단 목록 정책에 등록되었음을 확인합니다.

```
###Verify with below command
[guestshell@guestshell ~]$ trust list --filter=trust-policy --purpose=server-auth | grep -E -A3 'emSign
    label: AAA Certificate Services
    trust: distrusted
    category: authority

--
    label: emSign ECC Root CA - C3
    trust: distrusted
    category: authority

--
    label: emSign ECC Root CA - G3
    trust: distrusted
    category: authority

--
    label: emSign Root CA - C1
    trust: distrusted
    category: authority

--
    label: emSign Root CA - G1
    trust: anchor
    category: authority

Output will vary based on CentOS Stream version
###Verify CentOS Stream Version
[guestshell@guestshell ~]$ cat /etc/redhat-release
CentOS Stream release 8
```

```
OS                          CentOS Stream 8       CentOS Stream 9
Directory                   blacklist only        blocklist
Result shown                 trust: blacklisted    trust: distrusted
```

4단계: 상태 지속성 및 컨테이너 수명 주기

컨테이너 지속성 참고: 이러한 인증서 불신 수정은 'guestshell enable' 및 'guestshell disable' 작업 전반에 지속되며, /etc/pki/ca-trust가 영구 컨테이너 스토리지에 상주하기 때문에 디바이스가 재부팅됩니다.

DEPLOYED 상태로 돌아가기(해당되는 경우): GuestShell이 원래 DEPLOYED 상태였고 이 불확실 절차를 실행하기 위해서만 활성화된 경우, bash를 종료하고 IOS 특권 EXEC 프롬프트에서 'guestshell disable'을 실행하여 GuestShell을 이전의 중지된 상태로 되돌립니다.

<#root>

```
[root@guestshell ~]#
```

exit

```
[guestshell@guestshell ~]$
```

exit

```
Router#
```

guestshell disable

라이프사이클의 주요 고려 사항: GuestShell이 'guestshell destroy'로 완전히 제거되면 컨테이너 파일 시스템이 제거됩니다. 이후에 GuestShell을 다시 활성화하면 컨테이너가 기본 시스템 이미지에서 다시 생성되며 이러한 불신 교정 단계를 다시 적용해야 합니다.

5단계: 롤백 절차(CA 신뢰 복원)

불신 컨피그레이션을 취소하고 Cisco IOS XE 릴리스에서 기본 CA 신뢰를 복원하려면, 동적으로 액티브 차단 목록 디렉토리($d)를 선택하고, 이 절차에서 추가된 4개의 인증서 파일(Comodo AAA Services root 포함)을 제거한 다음, 신뢰 저장소를 재구축합니다.

<#root>

```
! Escalate to root user inside GuestShell:
[guestshell@guestshell ~]$
```

```
sudo -s


d=/etc/pki/ca-trust/source/blocklist
[ -d "$d" ] || d=/etc/pki/ca-trust/source/blacklist

! Remove only the four certificate files added during remediation:
rm -f "$d/emSign_ECC_Root_CA_-_G3.pem" "$d/Comodo_AAA_Services_root.pem" \
      "$d/emSign_ECC_Root_CA_-_C3.pem" "$d/emSign_Root_CA_-_C1.pem"

! Rebuild the system CA trust store:
update-ca-trust extract
```

차단 목록 디렉토리에 제거된 파일이 더 이상 없는지 확인합니다.

<#root>

```
[root@guestshell ~]#

ls -l "$d"/

total 0
```

CA 신뢰 복원 확인: 3단계 확인 명령을 다시 실행하여 5개 인증서 모두 활성 트러스트 앵커로 돌아왔는지 확인합니다(모든 항목은 trust를 보고합니다. 앵커):

<#root>

```
[root@guestshell ~]#

trust list --filter=trust-policy --purpose=server-auth | grep -E -A3 'emSign|AAA'

    trust: anchor
    trust: anchor
    trust: anchor
    trust: anchor
    trust: anchor
```

엔드 투 엔드 실행 기록 예

이 기록은 Cisco IOS XE 디바이스에서 성공적으로 완료된 GuestShell 감사, 교정 및 확인 세션을 보여줍니다.

<#root>

```
Router#
```

```
guestshell run bash

[guestshell@guestshell ~]$ sudo -s
bash-4.4#

d=/etc/pki/ca-trust/source/blocklist

bash-4.4#

[ -d "$d" ] || d=/etc/pki/ca-trust/source/blacklist

bash-4.4#

mkdir -p "$d"

bash-4.4#

trust extract --overwrite --format=pem-bundle \ >   --filter='pkcs11:object=emSign%20ECC%20Root%20CA%20-

bash-4.4#

trust extract --overwrite --format=pem-bundle \ >   --filter='pkcs11:object=Comodo%20AAA%20Services%20ro

bash-4.4#

trust extract --overwrite --format=pem-bundle \ >   --filter='pkcs11:object=emSign%20ECC%20Root%20CA%20-

bash-4.4#

trust extract --overwrite --format=pem-bundle \ >   --filter='pkcs11:object=emSign%20Root%20CA%20-%20C1;

bash-4.4#

update-ca-trust extract

bash-4.4#

trust list --filter=trust-policy --purpose=server-auth | grep -E -A3 'emSign|AAA'

    label: emSign ECC Root CA - G3
    trust: blacklisted
    category: authority

--
    label: AAA Certificate Services
    trust: blacklisted
    category: authority

--
    label: emSign ECC Root CA - C3
    trust: blacklisted
    category: authority
```

```
--
    label: emSign Root CA - C1
    trust: blacklisted
    category: authority

--
    label: emSign Root CA - G1
    trust: anchor
    category: authority

bash-4.4#

cat /etc/redhat-release

CentOS Stream release 8
bash-4.4#

d=/etc/pki/ca-trust/source/blocklist

bash-4.4#

[ -d "$d" ] || d=/etc/pki/ca-trust/source/blacklist

bash-4.4#

rm -f "$d/emSign_ECC_Root_CA_-_G3.pem" "$d/Comodo_AAA_Services_root.pem" \ >       "$d/emSign_ECC_Root_C

bash-4.4#
bash-4.4#

update-ca-trust extract

bash-4.4#

ls -l "$d"/

total 0
```

명령 요약 매트릭스

운영 작업	CL
GuestShell 상태 감사	`show app-hosting list`
GuestShell 활성화(구축	`guestshell enable`

된 경우)	
GuestShell Bash 입력	`guestshell run bash`
루트 사용자로 전환	`sudo -s`
차단 목록 디렉터리 준비	`d=/etc/pki/ca-trust/source/blocklist; [ -d "$d" ] || d=/etc/pki/ca-trust/source/blacklist;`
차단 목록에 CA 추출	`trust extract --overwrite --format=pem-bundle ... (x4 CAs)`
CA 트러스트 저장소 다시 빌드	`update-ca-trust extract`
불신 정책 검증	`trust list --filter=trust-policy --purpose=server-auth`
Restore DEPLOYED State(구축된 상태 복원)(선택 사항)	`guestshell disable`
신뢰 롤백/복원	`rm -f "$d/emSign_ECC_Root_CA_-_G3.pem" "$d/Comodo_AAA_Services_root.pem" "$d/emSign_ECC_Roo`

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.