

해결 방법 및 cBR-8에서 만료된 제조업체 인증서 복구

목차

[소개](#)

[문제](#)

[Manu 인증서 정보](#)

[Manu 인증서 정보 필드 및 특성](#)

[cBR-8 CLI 명령](#)

[DOCSIS-BPI-PLUS-MIB OID](#)

[솔루션](#)

[CM 펌웨어 업데이트](#)

[알려진 Manu Cert를 Trusted로 설정](#)

[cBR-8 CLI에서 Manu Cert Information 보기](#)

[cBR-8 CLI에서 SNMP로 Manu Cert Information 보기](#)

[원격 디바이스에서 SNMP를 사용하여 Manu 인증서 정보 보기](#)

[CLI에서 Manu Cert Validity End Date를 확인합니다.](#)

[Manu Cert Trust State\(MANU 인증서 신뢰 상태\)를 Trusted\(신뢰할 수 있음\)로 설정](#)

[cBR-8 CLI 또는 SNMP를 사용하여 Manu Cert Changes 확인](#)

[알려진 Manu 인증서가 만료된 후 CM 서비스 복구](#)

[cBR-8 로그 메시지에서 Expired Manu Cert 일련 번호 식별](#)

[Expired Manu Cert의 인덱스를 식별하고 Manu Cert Trust State\(MANU 인증서 신뢰 상태\)를 Trusted\(신뢰할 수 있음\)로 설정합니다.](#)

[cBR-8에 Unknown Expired Manu Cert 설치 및 Mark Trusted](#)

[SNMP를 사용하여 cBR-8에 만료된 Manu 인증서 추가](#)

[cBR-8 CLI 명령을 사용하여 AuthInfo에서 만료된 Manu 인증서를 추가하도록 허용](#)

[cBR-8 CLI 명령을 사용하여 AuthInfo에서 만료된 CM 인증서 및 Manu 인증서를 추가하도록 허용 추가 정보](#)

[MAC 도메인/케이블 인터페이스 컨피그레이션 고려 사항](#)

[SNMP 패킷 크기 고려 사항](#)

[Manu 인증서 디버그](#)

[관련 지원 문서](#)

소개

이 문서에서는 제조업체 인증서(Manu Cert) 만료로 인해 발생하는 cBR-8 CMTS(Cable Modem Termination System) 서비스에 영향을 미치는 CM(케이블 모뎀 거부) 오류 방지, 해결 방법 및 복구 옵션에 대해 설명합니다.

문제

cBR-8에서 CM이 reject(pk) 상태로 고정되는 데에는 다른 원인이 있습니다. 한 가지 원인은 Manu

Cert가 만료되기 때문입니다. Manu Cert는 CM과 CMTS 간의 인증에 사용됩니다. 이 문서에서 Manu Cert는 DOCSIS 3.0 Security Specification CM-SP-SECv3.00이 CableLabs Mfg CA 인증서 또는 제조업체 CA 인증서라고 하는 것입니다. 만료는 cBR-8 시스템 날짜/시간이 Manu Cert 유효 종료 날짜/시간을 초과함을 의미합니다.

Manu Cert가 만료된 후 cBR-8에 등록하려고 시도하는 CM은 CMTS에 의해 reject(pk)로 표시되고 서비스가 제공되지 않습니다. cBR-8에 이미 등록된 CM과 Manu Cert가 만료될 때 서비스 중인 CM은 다음 번에 CM이 등록을 시도할 때까지 서비스 상태로 유지될 수 있습니다. 단, 단일 CM 오프라인 이벤트, cBR-8 Cable Linecard 재시작, cBR-8 다시 로드 또는 기타 이벤트가 CM 등록을 트리거한 후 발생할 수 있습니다. 그 때 CM이 인증에 실패하고 cBR-8에서 reject(pk)로 표시되고 서비스가 제공되지 않습니다.

이 문서의 정보는 [cBR-8 Product Bulletin](#)에서 Cable Modem [및 Expiring Manufacturer Certificates](#)에 게시된 내용을 확장하고 다시 포맷합니다.

참고: Cisco 버그 ID [CSCwv21785](#); 일부 버전의 Cisco IOS XE에서 이 버그로 인해 cBR-8 다시 로드 후 신뢰할 수 있는 Manu Cert의 검증에 실패합니다. 경우에 따라 Manu Cert가 있지만 더 이상 신뢰할 수 있는 상태가 아닙니다. 이 경우 이 문서에 설명된 단계를 통해 Manu Cert 신뢰 상태를 신뢰할 수 있는 상태로 변경할 수 있습니다. Manu Cert가 show cable privacy manufacturer-cert-list 명령의 출력에 없으면 수동으로 또는 이 문서에 설명된 단계를 사용하여 AuthInfo를 통해 Manu Cert를 다시 추가할 수 있습니다.

Manu 인증서 정보

관리 인증서 정보는 원격 디바이스의 cBR-8 CLI 명령 또는 SNMP(Simple Network Management Protocol) 명령을 통해 볼 수 있습니다. cBR-8 CLI는 SNMP set, get 및 get-bulk 명령도 지원합니다. 이러한 명령과 정보는 이 문서에 설명된 솔루션에 의해 사용됩니다.

Manu 인증서 정보 필드 및 특성

- 인덱스: cBR-8 database/MIB의 각 Manu Cert에 할당된 고유 정수
- 제목: X509 인증서에 인코딩된 것과 정확히 동일한 주체 이름
cn: 공용 이름 ou: 조직 단위 o: 조직: 구/군/시: 주/도 이름 c: 국가 이름
- 발급자: 인증 기관
- 일련 번호: 16진수 8진수 문자열로 표시되는 인증서 일련 번호
- 상태: 인증서의 신뢰 상태
신뢰신뢰회사슬로루트
- 출처: 인증서가 CMTS에 도달하는 방법
snmp구성 파일외부 데이터베이스기타인증 정보컴파일된 정보 코드
- 상태/행 상태: 인증서 상태
활성서비스 안 함준비 안 됨만들기 및 이동생성 및 대기파괴
- 인증서: X509 DER 인코딩 인증 기관 인증서
- 유효 날짜: CMTS 시스템 날짜 및 시간을 기준으로 Manu Cert 유효 기간을 정의하는 시작 및 종료 날짜
시작 날짜: Manu Cert 가 유효한 날짜 및 시간종료 날짜: Manu 인증서가 더 이상 유효하지 않은 날짜 및 시간
- 인증서: X509 DER 인코딩 인증 기관 인증서
- 지문: CA 인증서의 SHA-1 해시

cBR-8 CLI 명령

Manu Cert 정보는 다음 cBR-8 CLI 명령으로 볼 수 있습니다.

- cBR-8 CLI exec 모드 또는 Linecard CLI exec 모드에서 다음을 수행합니다. CBR8-1#**show cable privacy manufacturer-cert-list**
- cBR-8 Linecard CLI exec 모드에서 다음을 수행합니다. Slot-6-0#**show crypto pki certificates**

이러한 Cisco IOS® XE SNMP 명령은 cBR-8 CLI에서 SNMP OID를 가져오고 설정하는 데 사용됩니다.

- [snmp 가져오기](#)
- [snmp get-bulk](#)
- [snmp 설정](#)

이 cBR-8 케이블 인터페이스 컨피그레이션 명령은 이 문서의 솔루션 섹션에 설명된 해결 방법 및 복구에 사용됩니다.

- [케이블 프라이버시 유지 실패한 인증서](#)
- [케이블 프라이버시 생략 유효 기간](#)

DOCSIS-BPI-PLUS-MIB OID

Manu Cert 정보는 docsBpi2CmtsCACertEntry OID 분기 1.3.6.1.1.10.127.6.1.2.5.2.1에서 정의되며 [SNMP Object Navigator](#)에 [설명되어 있습니다](#).

관련 SNMP OID

```
docsBpi2CmtsCACertSubject 1.3.6.1.2.1.10.127.6.1.2.5.2.1.2
docsBpi2CmtsCACertIssuer 1.3.6.1.2.1.10.127.6.1.2.5.2.1.3
docsBpi2CmtsCACertSerialNumber 1.3.6.1.2.1.10.127.6.1.2.5.2.1.4
docsBpi2CmtsCACertTrust 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5
docsBpi2CmtsCACertSource 1.3.6.1.2.1.10.127.6.1.2.5.2.1.6
docsBpi2CmtsCACertStatus 1.3.6.1.2.1.10.127.6.1.2.5.2.1.7
docsBpi2CmtsCACert 1.3.6.1.2.1.10.127.6.1.2.5.2.1.8
```

명령 예제에서 생략 부호(...)는 가독성을 위해 일부 정보가 생략되었음을 나타냅니다.

솔루션

CM 펌웨어 업데이트는 가장 장기적인 솔루션입니다. 이 문서에 설명된 해결 방법은 만료된 Manu Certs가 있는 CM이 cBR-8에 등록하고 온라인 상태로 유지되도록 허용하지만 이러한 해결 방법은 단기간 사용에만 권장됩니다. CM 펌웨어 업데이트가 옵션이 아닌 경우 CM 교체 전략은 보안 및 운영 측면에서 좋은 장기적 솔루션입니다. 여기에서 설명하는 솔루션은 다양한 조건이나 시나리오를 다루며 개별적으로 또는 서로 조합하여 사용할 수 있습니다.

- [CM 펌웨어 업데이트](#)
- [알려진 Manu Cert를 Trusted로 설정](#)
- [알려진 Manu 인증서가 만료된 후 CM 서비스 복구](#)
- [cBR-8에 Unknown Expired Manu Cert 설치 및 Mark Trusted](#)
- [cBR-8 CLI 명령을 사용하여 AuthInfo에서 만료된 CM 인증서 및 Manu 인증서를 추가하도록 허](#)

참고: BPI가 제거되면 암호화 및 인증이 비활성화되어 해결 방법으로 그 실행 가능성을 최소화합니다.

CM 펌웨어 업데이트

대부분의 경우 CM 제조업체는 Manu Cert의 유효 종료 날짜를 연장하는 CM 펌웨어 업데이트를 제공합니다. 이 솔루션은 최상의 선택이며, Manu Cert가 만료되기 전에 수행할 경우 관련 서비스에 영향을 주지 않습니다. CM은 새 펌웨어를 로드하고 새 Manu Certs 및 CM Certs에 다시 등록합니다. 새 인증서는 제대로 인증되고 CM은 cBR-8에 성공적으로 등록할 수 있습니다. 새 Manu Cert 및 CM Cert는 cBR-8에 이미 설치된 알려진 루트 인증서로 새 인증서 체인을 다시 생성할 수 있습니다.

알려진 Manu Cert를 Trusted로 설정

CM 제조업체가 폐업하거나 CM 모델에 대한 추가 지원이 없는 등의 이유로 CM 펌웨어 업데이트를 사용할 수 없는 경우, 곧 유효 종료 날짜가 가까운 cBR-8에 이미 알려진 Manu Certs는 유효성 종료 날짜 이전에 cBR-8에서 미리 신뢰할 수 있는 것으로 표시될 수 있습니다. cBR-8 CLI 명령 및 SNMP는 일련 번호 및 신뢰 상태와 같은 Manu Cert 정보를 식별하는 데 사용되며, SNMP는 cBR-8에서 Manu Cert 신뢰 상태를 trusted로 설정하는 데 사용되는데, 이 경우 관련 CM이 등록하고 서비스 상태를 유지할 수 있습니다.

현재 사용 중인 CM 및 온라인 CM에 대해 알려진 Manu Certs는 일반적으로 cBR-8에서 DOCSIS BPI(Baseline Privacy Interface) 프로토콜을 통해 학습됩니다. CM에서 cBR-8로 전송된 AuthInfo 메시지에는 Manu Cert가 포함되어 있습니다. 각 고유한 Manu Cert는 cBR-8 메모리에 저장되며 cBR-8 CLI 명령 및 SNMP에서 해당 정보를 볼 수 있습니다.

Manu Cert가 신뢰할 수 있는 것으로 표시되면 두 가지 중요한 작업을 수행합니다. 먼저 cBR-8 BPI 소프트웨어가 만료된 유효 날짜를 무시할 수 있습니다. 둘째, Manu Cert를 cBR-8 NVRAM에 신뢰할 수 있는 상태로 저장합니다. 이렇게 하면 cBR-8 다시 로드에서 Manu Cert 상태가 유지되며 cBR-8 다시 로드될 경우 이 절차를 반복할 필요가 없습니다.

CLI 및 SNMP 명령 예는 Manu Cert 인덱스, 일련 번호 및 신뢰 상태를 식별하는 방법을 보여줍니다. 그런 다음 해당 정보를 사용하여 신뢰 상태를 신뢰할 수 있는 상태로 변경합니다. 이 예에서는 Index 4 및 Serial Number 437498F09A7DCBC1FA7AA101FE976E40의 Manu Cert를 중점적으로 살펴봅니다.

cBR-8 CLI에서 Manu Cert Information 보기

이 예에서 cBR-8 CLI 명령 **show cable privacy manufacturer-cert-list**가 사용됩니다.

```
CBR8-1#show cable privacy manufacturer-cert-list
```

```
Cable Manufacturer Certificates:
```

```
Index: 4
```

```
Issuer: cn=DOCSIS Cable Modem Root Certificate Authority,ou=Cable Modems,o=Data Over Cable Service Interface Specifications,c=US
```

```
Subject: cn=Motorola Corporation Cable Modem Root Certificate Authority,ou=ASG,ou=DOCSIS,l=San Diego,st=California,o=Motorola Corporation,c=US
```

```
State: Chained
```

```
Source: Auth Info
```

RowStatus: Active
Serial: 437498F09A7DCBC1FA7AA101FE976E40
Thumbprint: FA07609998FDCAFA8F80D87F1ACFC70E6C52C80F
Fingerprint: 0EABDBD19D8898CA9C720545913AB93B

Index: 5
Issuer: cn=CableLabs Root Certification Authority,ou=Root CA01,o=CableLabs,c=US
Subject: cn=CableLabs Device Certification Authority,ou=Device CA01,o=CableLabs,c=US
State: Chained
Source: Auth Info
RowStatus: Active
Serial: 701F760559283586AC9B0E2666562F0E
Thumbprint: E85319D1E66A8B5B2BF7E5A7C1EF654E58C78D23
Fingerprint: 15C18A9D6584D40E88D50D2FF4936982

cBR-8 CLI에서 SNMP로 Manu Cert Information 보기

이 예에서는 cBR-8 CLI 명령 [snmp get-bulk](#)가 사용됩니다. Cert Indices 4 & 5는 CMTS 메모리에 저장된 Manu Certs입니다. 인덱스 1, 2 및 3은 루트 인증서입니다. 루트 인증서는 만료 날짜가 훨씬 더 길기 때문에 문제가 되지 않습니다.

docsBpi2CmtsCACertSubject

```
CBR8-1#snmp get-bulk v2c 192.168.1.1 vrf Mgmt-intf private non-repeaters 0 max-repetitions 5 oid 1.3.6.1.2.1.10.127.6.1.2.5.2.1.2
```

SNMP Response: reqid 1752673, errstat 0, erridx 0

docsBpi2CmtsCACertSubject.1 = Data Over Cable Service Interface Specifications

docsBpi2CmtsCACertSubject.2 = tComLabs - Euro-DOCSIS

docsBpi2CmtsCACertSubject.3 = CableLabs

docsBpi2CmtsCACertSubject.4 = Motorola

docsBpi2CmtsCACertSubject.5 = CableLabs

docsBpi2CmtsCACertIssuer

```
CBR8-1#snmp get-bulk v2c 192.168.1.1 vrf Mgmt-intf private non-repeaters 0 max-repetitions 5 oid 1.3.6.1.2.1.10.127.6.1.2.5.2.1.3
```

SNMP Response: reqid 1752746, errstat 0, erridx 0

docsBpi2CmtsCACertIssuer.1 = DOCSIS Cable Modem Root Certificate Authority

docsBpi2CmtsCACertIssuer.2 = Euro-DOCSIS Cable Modem Root CA

docsBpi2CmtsCACertIssuer.3 = CableLabs Root Certification Authority

docsBpi2CmtsCACertIssuer.4 = DOCSIS Cable Modem Root Certificate Authority

docsBpi2CmtsCACertIssuer.5 = CableLabs Root Certification Authority

```
CBR8-1#snmp get-bulk v2c 192.168.1.1 vrf Mgmt-intf private non-repeaters 0 max-repetitions 5 oid 1.3.6.1.2.1.10.127.6.1.2.5.2.1.4
```

SNMP Response: reqid 2300780, errstat 0, erridx 0

docsBpi2CmtsCACertSerialNumber.1 =

58 53 64 87 28 A4 4D C0 33 5F 0C DB 33 84 9C 19

docsBpi2CmtsCACertSerialNumber.2 =

63 4B 59 63 79 0E 81 0F 3B 54 45 B3 71 4C F1 2C

docsBpi2CmtsCACertSerialNumber.3 =

62 97 48 CA C0 A6 0D CB D0 FF A8 91 40 D8 D7 61

docsBpi2CmtsCACertSerialNumber.4 =

43 74 98 F0 9A 7D CB C1 FA 7A A1 01 FE 97 6E 40

docsBpi2CmtsCACertSerialNumber.5 =

70 1F 76 05 59 28 35 86 AC 9B 0E 26 66 56 2F 0E

docsBpi2CmtsCACertTrust

```
CBR8-1#snmp get-bulk v2c 192.168.1.1 vrf Mgmt-intf private non-repeaters 0 max-repetitions 5 oid 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5
```

SNMP Response: reqid 1752778, errstat 0, erridx 0

docsBpi2CmtsCACertTrust.1 = 4

docsBpi2CmtsCACertTrust.2 = 4

```
docsBpi2CmtsCACertTrust.3 = 4
docsBpi2CmtsCACertTrust.4 = 3      (3 = chained)
docsBpi2CmtsCACertTrust.5 = 3
```

```
docsBpi2CmtsCACertSource
CBR8-1#snmp get-bulk v2c 192.168.1.1 vrf Mgmt-intf private non-repeaters 0 max-repetitions 5 oid
1.3.6.1.2.1.10.127.6.1.2.5.2.1.6
SNMP Response: reqid 1752791, errstat 0, erridx 0
docsBpi2CmtsCACertSource.1 = 4
docsBpi2CmtsCACertSource.2 = 4
docsBpi2CmtsCACertSource.3 = 4
docsBpi2CmtsCACertSource.4 = 5      (5 = authenticInfo)
docsBpi2CmtsCACertSource.5 = 5
```

```
docsBpi2CmtsCACertStatus
CBR8-1#snmp get-bulk v2c 10.122.151.12 vrf Mgmt-intf Cisco123 non-repeaters 0 max-repetitions 5
oid 1.3.6.1.2.1.10.127.6.1.2.5.2.1.7
SNMP Response: reqid 1752804, errstat 0, erridx 0
docsBpi2CmtsCACertStatus.1 = 1
docsBpi2CmtsCACertStatus.2 = 1
docsBpi2CmtsCACertStatus.3 = 1
docsBpi2CmtsCACertStatus.4 = 1      (1 = active)
docsBpi2CmtsCACertStatus.5 = 1
```

원격 디바이스에서 SNMP를 사용하여 Manu 인증서 정보 보기

이 문서의 원격 디바이스 SNMP 예에서는 원격 Ubuntu Linux 서버의 SNMP 명령을 사용합니다. 특정 SNMP 명령 및 형식은 SNMP 명령을 실행하는 데 사용되는 디바이스 및 운영 체제에 따라 달라집니다.

```
docsBpi2CmtsCACertSubject
jdoe@server1:~$ snmpwalk -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.2
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.2.1 = STRING: "Data Over Cable Service Interface
Specifications"
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.2.2 = STRING: "tComLabs - Euro-DOCSIS"
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.2.3 = STRING: "CableLabs"
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.2.4 = STRING: "Motorola Corporation"
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.2.5 = STRING: "CableLabs"
```

```
docsBpi2CmtsCACertIssuer
jdoe@server1:~$ snmpwalk -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.3
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.3.1 = STRING: "DOCSIS Cable Modem Root Certificate Authority"
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.3.2 = STRING: "Euro-DOCSIS Cable Modem Root CA"
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.3.3 = STRING: "CableLabs Root Certification Authority"
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.3.4 = STRING: "DOCSIS Cable Modem Root Certificate Authority"
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.3.5 = STRING: "CableLabs Root Certification Authority"
```

```
docsBpi2CmtsCACertSerialNumber
jdoe@server1:~$ snmpwalk -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.4
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.4.1 = Hex-STRING: 58 53 64 87 28 A4 4D C0 33 5F 0C DB 33 84 9C
19
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.4.2 = Hex-STRING: 63 4B 59 63 79 0E 81 0F 3B 54 45 B3 71 4C F1
2C
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.4.3 = Hex-STRING: 62 97 48 CA C0 A6 0D CB D0 FF A8 91 40 D8 D7
61
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.4.4 = Hex-STRING: 43 74 98 F0 9A 7D CB C1 FA 7A A1 01 FE 97 6E
40
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.4.5 = Hex-STRING: 70 1F 76 05 59 28 35 86 AC 9B 0E 26 66 56 2F
0E
```

```
docsBpi2CmtsCACertTrust
```

```
jdoo@server1:~$ snmpwalk -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.5.1 = INTEGER: 4
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.5.2 = INTEGER: 4
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.5.3 = INTEGER: 4
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.5.4 = INTEGER: 3 (3 = chained)
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.5.5 = INTEGER: 3
```

docsBpi2CmtsCACertSource

```
jdoo@server1:~$ snmpwalk -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.6
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.6.1 = INTEGER: 4
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.6.2 = INTEGER: 4
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.6.3 = INTEGER: 4
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.6.4 = INTEGER: 5 (5 = authenticInfo)
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.6.5 = INTEGER: 5
```

docsBpi2CmtsCACertStatus

```
jdoo@server1:~$ snmpwalk -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.7
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.7.1 = INTEGER: 1
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.7.2 = INTEGER: 1
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.7.3 = INTEGER: 1
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.7.4 = INTEGER: 1 (1 = active)
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.7.5 = INTEGER: 1
```

CLI에서 Manu Cert Validity End Date를 확인합니다.

cBR-8 linecard CLI 명령 **show crypto pki certificates**를 사용하여 Manu Cert 유효 종료 날짜를 식별합니다. 이 명령 출력에는 Manu Cert Index가 포함되지 않습니다. Certificate Serial Number(인증서 일련 번호)를 사용하여 이 명령에서 학습한 Manu Cert 정보를 SNMP에서 학습한 Manu Cert 정보와 상호 연결할 수 있습니다.

```
CBR8-1#request platform software console attach
```

```
request platform software console attach 6/0
#
# Connecting to the CLC console on 6/0.
# Enter Control-C to exit the console connection.
#
Slot-6-0>enable
Slot-6-0#show crypto pki certificates
```

CA Certificate

```
Status: Available
Certificate Serial Number (hex): 701F760559283586AC9B0E2666562F0E Certificate Usage:
Signature
Issuer:
  cn=CableLabs Root Certification Authority
  ou=Root CA01
  o=CableLabs
  c=US
Subject:
  cn=CableLabs Device Certification Authority
  ou=Device CA01
  o=CableLabs
  c=US
Validity Date:
  start date: 00:00:00 GMT Oct 28 2014
  end date: 23:59:59 GMT Oct 27 2049
Associated Trustpoints: e85319d1e66a8b5b2bf7e5a7c1ef654e58c78d23
```

CA Certificate

```
Status: Available
```

Certificate Serial Number (hex): 437498F09A7DCBC1FA7AA101FE976E40

Certificate Usage: Signature

Issuer:

cn=DOCSIS Cable Modem Root Certificate Authority
ou=Cable Modems
o=Data Over Cable Service Interface Specifications
c=US

Subject:

cn=Motorola Corporation Cable Modem Root Certificate Authority
ou=ASG
ou=DOCSIS
l=San Diego
st=California
o=Motorola Corporation
c=US

Validity Date:

start date: 00:00:00 GMT Jul 11 2001

end date: 23:59:59 GMT Jul 10 2021

Associated Trustpoints: fa07609998fdcafa8f80d87f1acfc70e6c52c80f

CA Certificate

Status: Available

Certificate Serial Number (hex): 629748CAC0A60DCBD0FFFA89140D8D761

Certificate Usage: Signature

Issuer:

cn=CableLabs Root Certification Authority
ou=Root CA01
o=CableLabs
c=US

Subject:

cn=CableLabs Root Certification Authority
ou=Root CA01
o=CableLabs
c=US

Validity Date:

start date: 00:00:00 GMT Oct 28 2014

end date: 23:59:59 GMT Oct 27 2064

Associated Trustpoints: DOCSIS-D31-TRUSTPOINT

CA Certificate

Status: Available

Certificate Serial Number (hex): 634B5963790E810F3B5445B3714CF12C

Certificate Usage: Signature

Issuer:

cn=Euro-DOCSIS Cable Modem Root CA
ou=Cable Modems
o=tComLabs - Euro-DOCSIS
c=BE Subject:
cn=Euro-DOCSIS Cable Modem Root CA
ou=Cable Modems
o=tComLabs - Euro-DOCSIS
c=BE

Validity Date:

start date: 00:00:00 GMT Sep 21 2001

end date: 23:59:59 GMT Sep 20 2031

Associated Trustpoints: DOCSIS-EU-TRUSTPOINT

CA Certificate

Status: Available

Certificate Serial Number (hex): 5853648728A44DC0335F0CDB33849C19

Certificate Usage: Signature

Issuer:

cn=DOCSIS Cable Modem Root Certificate Authority
ou=Cable Modems


```
o=Data Over Cable Service Interface Specifications
c=US
Subject:
  cn=DOCSIS Cable Modem Root Certificate Authority
  ou=Cable Modems
  o=Data Over Cable Service Interface Specifications
  c=US
Validity Date:
  start date: 00:00:00 GMT Feb 1 2001
  end date: 23:59:59 GMT Jan 31 2031
Associated Trustpoints: DOCSIS-US-TRUSTPOINT
```

Manu Cert Trust State(MANU 인증서 신뢰 상태)를 Trusted(신뢰할 수 있음)로 설정

다음 예에서는 Index = 4 및 Serial Number = 437498f09a7dcbc1fa7aa101fe976e40의 Manu Cert에 대해 신뢰 상태가 체인으로 변경되었음을 보여줍니다.

OID: docsBpi2CmtsCACertTrust 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5 값:

- 1: 신뢰
- 2: 신뢰
- 3: 쇠사슬로
- 4: 루트

이 예에서는 신뢰 상태를 변경하는 데 사용되는 cBR-8 CLI snmp-set 명령을 보여 줍니다

```
CBR8-1#snmp set v2c 192.168.1.1 vrf Mgmt-intf private oid 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5.4
integer 1
SNMP Response: reqid 2305483, errstat 0, erridx 0
docsBpi2CmtsCACertTrust.4 = 1 (1 = trusted)
```

이 예에서는 원격 디바이스가 신뢰 상태를 변경하기 위해 SNMP를 사용하는 것을 보여줍니다

```
jdoo@server1:~$ snmpset -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5.4 i 1
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.5.4 = INTEGER: 1 (1 = trusted)
```

cBR-8 CLI 또는 SNMP를 사용하여 Manu Cert Changes 확인

- 신뢰 값이 체인으로 변경됨
- 소스 값이 SNMP로 변경되었습니다. 이는 인증서가 BPI 프로토콜 AuthInfo 메시지가 아닌 SNMP에서 마지막으로 관리되었음을 나타냅니다.

이 예에서는 변경 사항을 확인하는 데 사용되는 cBR-8 CLI 명령을 보여 줍니다

```
CBR8-1#show cable privacy manufacturer-cert-list
Cable Manufacturer Certificates:
...
Index: 4
Issuer: cn=DOCSIS Cable Modem Root Certificate Authority,ou=Cable Modems,o=Data Over Cable
Service Interface Specifications,c=US
Subject: cn=Motorola Corporation Cable Modem Root Certificate Authority,ou=ASG,ou=DOCSIS,l=San
Diego,st=California,o=Motorola Corporation,c=US
State: Trusted
Source: SNMP
RowStatus: Active
Serial: 437498F09A7DCBC1FA7AA101FE976E40
Thumbprint: DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
```

Fingerprint: D41D8CD98F00B204E9800998ECF8427E
...

이 예에서는 원격 디바이스가 SNMP를 사용하여 변경 사항을 확인하는 방법을 보여 줍니다.

```
jdoo@server1:~$ snmpget -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5.4  
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.5.4 = INTEGER: 1 (1 = trusted)
```

```
jdoo@server1:~$ snmpget -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.6.4  
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.6.4 = INTEGER: 1 (1 = snmp)
```

알려진 Manu 인증서가 만료된 후 CM 서비스 복구

이전에 알려진 Manu Cert는 cBR-8 데이터베이스에 이미 있는 인증서로서, 일반적으로 이전 CM 등록에서 AuthInfo 메시지를 수신한 것입니다. Manu Cert가 신뢰할 수 있는 것으로 표시되지 않고 만료되면 만료된 Manu Cert를 사용하고 오프라인으로 전환하는 CM은 재등록할 수 없으며 reject(pk)로 표시됩니다. 이 섹션에서는 이 상태에서 복구하는 방법과 만료된 Manu Certs가 있는 CM이 등록되고 서비스 상태로 유지되는 방법에 대해 설명합니다.

만료된 Manu Certs로 인해 CM이 온라인 상태로 오지 못하고 reject(pk)로 표시된 경우, syslog 메시지가 생성되고 CM MAC 주소와 만료된 Manu Cert Serial Number가 포함됩니다.

cBR-8 로그 메시지에서 Expired Manu Cert 일련 번호 식별

```
CLC 6/0: Jan 11 17:36:07.094: %CBR-3-MANUFACTURE_CA_CM_CERTIFICATE_FORMAT_ERROR:  
<133>CMTS[DOCSIS]: CM MAC Addr <1234.5678.9ABC> on Interface Cable6/0/0 U1 : Manu Cert S/N  
437498F09A7DCBC1FA7AA101FE976E40 has Expired
```

Expired Manu Cert의 인덱스를 식별하고 Manu Cert Trust State(MANU 인증서 신뢰 상태)를 Trusted(신뢰할 수 있음)로 설정합니다.

이 예에서는 로그 메시지에서 Manu Cert 일련 번호의 인덱스를 식별하는 데 사용되는 cBR-8 CLI SNMP 명령을 보여 줍니다. 이 명령은 Manu Cert 신뢰 상태를 trusted로 설정하는 데 사용됩니다.

```
CBR8-1#snmp get-bulk v2c 192.168.1.1 vrf Mgmt-intf private non-repeaters 0 max-repetitions 5 oid  
1.3.6.1.2.1.10.127.6.1.2.5.2.1.4
```

```
SNMP Response: reqid 2351849, errstat 0, erridx 0  
docsBpi2CmtsCACertSerialNumber.1 =  
58 53 64 87 28 A4 4D C0 33 5F 0C DB 33 84 9C 19  
docsBpi2CmtsCACertSerialNumber.2 =  
63 4B 59 63 79 0E 81 0F 3B 54 45 B3 71 4C F1 2C  
docsBpi2CmtsCACertSerialNumber.3 =  
62 97 48 CA C0 A6 0D CB D0 FF A8 91 40 D8 D7 61  
docsBpi2CmtsCACertSerialNumber.4 =  
43 74 98 F0 9A 7D CB C1 FA 7A A1 01 FE 97 6E 40  
docsBpi2CmtsCACertSerialNumber.5 =  
70 1F 76 05 59 28 35 86 AC 9B 0E 26 66 56 2F 0E
```

```
CBR8-1#snmp set v2c 192.168.1.1 vrf Mgmt-intf private oid 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5.4  
integer 1
```

```
SNMP Response: reqid 2353143, errstat 0, erridx 0  
docsBpi2CmtsCACertTrust.4 = 1 (1 = trusted)
```

이 예에서는 원격 디바이스가 SNMP 명령을 사용하여 로그 메시지에서 Manu Cert 일련 번호의 인

덱스를 식별하는 방법을 보여 줍니다. 이 인덱스는 Manu Cert 신뢰 상태를 trusted로 설정하는 데 사용됩니다.

```
jdoo@server1:~$ snmpwalk -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.4 | grep
"43 74 98 F0 9A 7D CB C1 FA 7A A1 01 FE 97 6E 40"
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.4.4 = Hex-STRING: 43 74 98 F0 9A 7D CB C1 FA 7A A1 01 FE 97 6E 40

jdoo@server1:~$ snmpset -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5.4 i 1
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.5.4 = INTEGER: 1 (1 = trusted)
```

cBR-8에 Unknown Expired Manu Cert 설치 및 Mark Trusted

만료된 Manu Cert가 cBR-8에 알려지지 않은 경우 만료 전에 관리(신뢰된 것으로 표시)할 수 없으며 복구할 수 없습니다. 이는 이전에는 알 수 없고 cBR-8에 등록되지 않은 CM이 알 수 없고 만료된 Manu Cert로 등록하려고 시도할 때 발생합니다. 원격 디바이스에서 SNMP를 통해 cBR-8에 Manu Cert를 추가하거나 **케이블 프라이버시 retain-failed-certificates** cBR-8 케이블 인터페이스 컨피그레이션을 사용하여 AuthInfo에서 만료된 Manu Cert를 추가할 수 있습니다. 인증서 데이터의 문자 수가 CLI에서 허용하는 최대 문자 수를 초과하므로 cBR-8 CLI SNMP 명령을 사용하여 인증서를 추가할 수 없습니다. 자체 서명 인증서가 추가된 경우 cBR-8에서 인증서를 승인하려면 **cbr-8** 케이블 인터페이스에서 **cable privacy accept-self-signed-certificate** 명령을 구성해야 합니다.

SNMP를 사용하여 cBR-8에 만료된 Manu 인증서 추가

이러한 docsBpi2CmtsCACertTable OID 값을 사용하여 Manu 인증서를 새 테이블 항목으로 추가합니다. docsBpi2CmtsCACert OID에 의해 정의된 Manu Cert의 16진수 값은 지원 문서 [Modem Stuck State Diagnostics](#)를 [위해 DOCSIS 인증서를 디코딩하는 방법](#)에 설명된 CA 인증서 덤프 단계를 통해 알 수 있습니다.

```
docsBpi2CmtsCACertStatus 1.3.6.1.2.1.10.127.6.1.2.5.2.1.7 (Set to 4 to create the row entry)
docsBpi2CmtsCACert 1.3.6.1.2.1.10.127.6.1.2.5.2.1.8 (The hexadecimal data, as an X509Certificate value, for the actual X.509 certificate)
docsBpi2CmtsCACertTrust 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5 (Set to 1 to set the Manu Cert Trust state to trusted)
```

추가된 Manu Cert에 고유한 인덱스 번호를 사용합니다. cBR-8에 이미 있는 Manu Certs의 인덱스는 **show cable privacy manufacturer-cert-list** 명령을 사용하여 확인할 수 있습니다.

```
CBR8-2#show cable privacy manufacturer-cert-list | i Index
Index: 4
Index: 5
Index: 6
Index: 7
```

이 섹션의 예는 cBR-8 데이터베이스에 추가된 Manu Cert에 대해 인덱스 값 11을 사용합니다.

팁: 실제 인증서 데이터 앞에 항상 CertStatus 특성을 설정합니다. 그렇지 않으면 CMTS는 인증서가 체인으로 묶여 있다고 가정하고 제조업체 및 루트 인증서로 즉시 인증서를 확인하려고 시도합니다.

일부 운영 체제에서는 인증서를 지정하는 16진수 데이터 문자열을 입력하는 데 필요한 만큼 긴 입력 행을 허용할 수 없습니다. 따라서 그래픽 SNMP 관리자를 사용하여 이러한 특성을 설정할 수 있

습니다. 여러 인증서의 경우 더 편리한 경우 스크립트 파일을 사용할 수 있습니다.

이 예에서는 원격 디바이스가 SNMP를 사용하여 cBR-8에 Manu Cert 인증서를 추가하는 방법을 보여 줍니다. 대부분의 인증서 데이터는 가독성을 위해 전송되며, 이는 라이선스(...)로 표시됩니다.

```
jdooe@server1:~$ snmpset -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.7.11 i 4
1.3.6.1.2.1.10.127.6.1.2.5.2.1.8.11 x "0x3082...38BD" 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5.11 i 1
```

cBR-8 CLI 명령을 사용하여 AuthInfo에서 만료된 Manu 인증서를 추가하도록 허용

Manu Cert는 일반적으로 CM에서 cBR-8로 전송된 BPI Protocol AuthInfo 메시지에 의해 cBR-8 데이터베이스에 들어갑니다. AuthInfo 메시지에서 받은 고유하고 유효한 Manu Cert가 데이터베이스에 추가됩니다. CMTS에서 Manu Cert를 알 수 없고(데이터베이스에 없음) 유효 날짜가 만료된 경우 AuthInfo가 거부되고 Manu Cert가 cBR-8 데이터베이스에 추가되지 않습니다. cBR-8 케이블 인터페이스 컨피그레이션 아래에 **케이블 프라이버시 retain-failed-certificates** 해결 방법 컨피그레이션이 있을 때 AuthInfo 교환에서 만료된 Manu Cert를 CMTS에 추가할 수 있습니다. 이렇게 하면 만료된 Manu 인증서를 신뢰할 수 없는 상태로 cBR-8 데이터베이스에 추가할 수 있습니다. 만료된 Manu Cert를 사용하려면 SNMP를 사용하여 신뢰할 수 있는 것으로 표시해야 합니다. 만료된 Manu Cert가 cBR-8에 추가되고 신뢰할 수 있는 것으로 표시된 경우 **케이블 프라이버시 유지-실패 인증서** 컨피그레이션을 제거하는 것이 권장되므로 사용자 동의 없이 추가로 시스템을 시작하지 않습니다.

```
CBR8-1#config t
Enter configuration commands, one per line. End with CNTL/Z.
CBR8-1(config)#int Cable6/0/0
CBR8-1(config-if)#cable privacy retain-failed-certificates
CBR8-1(config-if)#end
```

cBR-8 CLI 명령을 사용하여 AuthInfo에서 만료된 CM 인증서 및 Manu 인증서를 추가하도록 허용

cable privacy retain-failed-certificates 및 **cable privacy skip-validity-period** 명령이 각 관련 케이블 인터페이스에서 모두 구성된 경우 AuthInfo 교환에서 만료된 CM 인증서를 CMTS에 추가할 수 있습니다. 이로 인해 cBR-8은 CM BPI AuthInfo 메시지에 전송된 모든 CM 및 Manu Certs에 대한 만료된 유효성 검사를 무시합니다. 만료된 CM 및 Manu Certs가 cBR-8에 추가되고 신뢰할 수 있는 것으로 표시되면, 설명된 구성을 제거하는 것이 추가로 권장되므로 사용자 동의 없이 시스템을 입력하지 않습니다.

```
CBR8-1#config t
Enter configuration commands, one per line. End with CNTL/Z.
CBR8-1(config)#interface Cable6/0/0
CBR8-1(config-if)#cable privacy retain-failed-certificates
CBR8-1(config-if)#cable privacy skip-validity-period
CBR8-1(config-if)#end
CBR8-1#copy run start
```

추가 정보

MAC 도메인/케이블 인터페이스 컨피그레이션 고려 사항

cable privacy retain-failed-certificates 및 **cable privacy skip-validity-period** 컨피그레이션 명령은 MAC 도메인/케이블 인터페이스 레벨에서 사용되며 제한적이지 않습니다. retain-failed-certificates 명령은 실패한 인증서를 cBR-8 데이터베이스에 추가할 수 있으며 skip-validity-period 명령은 모든 Manu 및 CM 인증서에 대한 유효성 검사를 건너뛸 수 있습니다.

SNMP 패킷 크기 고려 사항

Cert OctetString이 SNMP 패킷 크기보다 큰 경우 인증서 데이터에 대한 SNMP 가져오기는 NULL 값을 반환할 수 있습니다. 대규모 인증서를 사용할 경우 cBR-8 SNMP 컨피그레이션을 사용할 수 있습니다.

```
CBR8-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CBR8-1(config)#snmp-server packetsize 3000
CBR8-1(config)#end
CBR8-1#copy run start
```

Manu 인증서 디버그

cBR-8의 Manu Cert Debug는 `debug cable privacy ca-cert` 및 `debug cable mac-address <CM mac-address>` 명령으로 지원됩니다. 추가 디버그 정보는 지원 문서 [모뎀 장애 상태 진단을 위한 DOCSIS 인증서를 디코딩하는 방법에 설명되어 있습니다](#). 여기에는 Manu Cert의 16진수 값을 학습하는 데 사용되는 CA 인증서 덤프 단계가 포함됩니다.

관련 지원 문서

- [Cisco CMTS 라우터용 DOCSIS 1.1에서는 cBR-8 지원 및 DOCSIS BPI+\(Baseline Privacy Interface\) 구성에 대한 추가 정보를 제공합니다](#).
- [Cisco CMTS Cable Command Reference](#)는 이 문서에서 참조하는 cBR-8 CLI 명령에 대한 정보를 제공합니다.
- [uBR10K에서 Work Around and Recover Expired Manufacturer Certificates\(만료된 제조업체 인증서 작업 및 복구\)](#)는 uBR10K CMTS에 대해 이 문서와 유사한 정보를 제공합니다.
- [기술 지원 및 문서 - Cisco Systems](#)