

# AnyConnect 인증서 기반 인증을 위한 CRL 트러블슈팅

## 목차

---

### [소개](#)

#### [사전 요구 사항](#)

##### [요구 사항](#)

##### [사용되는 구성 요소](#)

#### [배경 정보](#)

#### [토폴로지](#)

#### [중요 구성](#)

##### [CA 라우터](#)

##### [VPN 게이트웨이 컨피그레이션](#)

##### [Windows 장치](#)

#### [검증](#)

##### [시나리오 1. 인증서는 인증에 유효합니다.](#)

##### [시나리오 2. 인증서가 취소되고 인증에 실패합니다.](#)

#### [문제 해결](#)

---

## 소개

이 문서에서는 AnyConnect 인증서 기반 인증을 위해 구성된 CRL(Certificate Revocation List)의 문제를 해결하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- CA(인증 기관)
- PKI(Public Key Infrastructure)
- FTD의 RA VPN
- AnyConnect 클라이언트가 포함된 Windows 10

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- CSR1000V - Cisco IOS® XE, 버전 16.12.03 - Cisco IOS XE CA 서버
- NGFWv - 버전 7.1.0 - VPN 게이트웨이

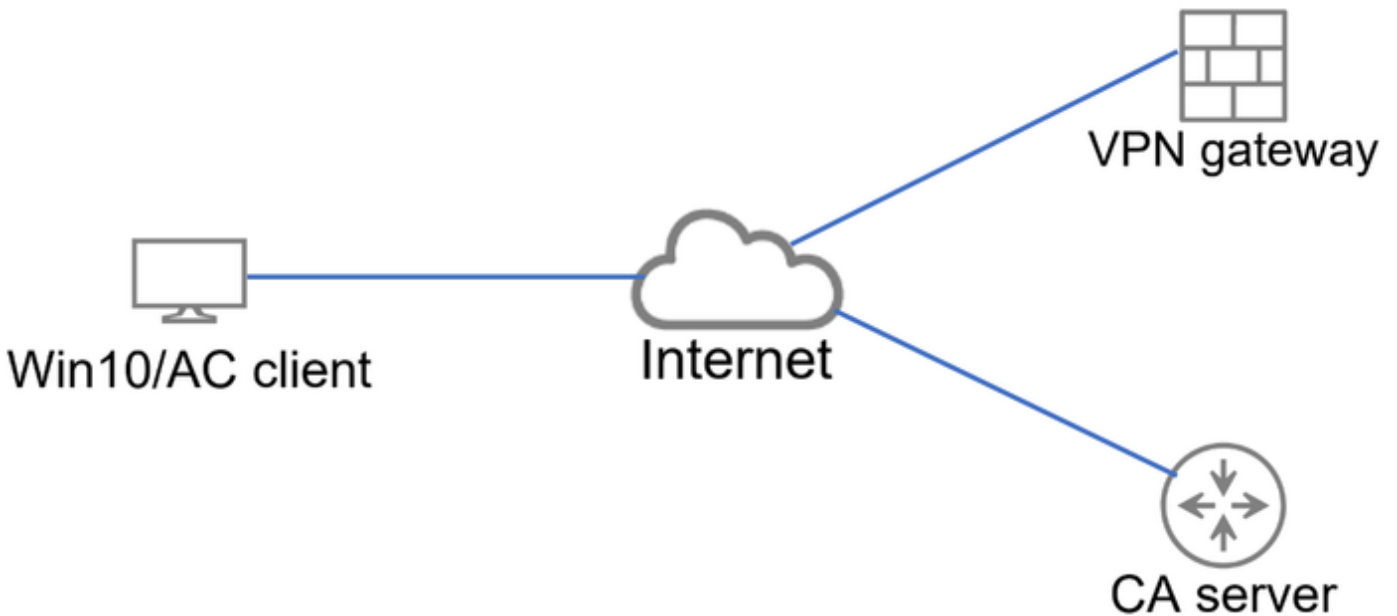
- VPN 클라이언트로 AnyConnect Secure Mobility Client 버전 4.10.07073
- 로컬 컴퓨터로서의 Windows 10

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 배경 정보

CRL을 사용하면 디바이스에서 인증서 수명이 만료되기 전에 인증서가 폐기되었는지 확인할 수 있습니다. CRL에는 인증서의 일련 번호 및 폐기 날짜가 포함됩니다. FTD(Firepower Thread Defense) 시스템 또는 기타 엔드 디바이스와 같은 보안 게이트웨이에서는 인증서 상태를 검증하여 인증서 인증을 강화하기 위해 이 기능을 사용합니다.

## 토폴로지



VPN 게이트웨이 및 CA 서버에 대한 연결을 제공하는 기본 토폴로지

## 중요 구성

CRL로 인증서 기반 인증을 수행하기 위해 제시된 컨피그레이션이 관련된 각 디바이스에서 사용되었습니다.

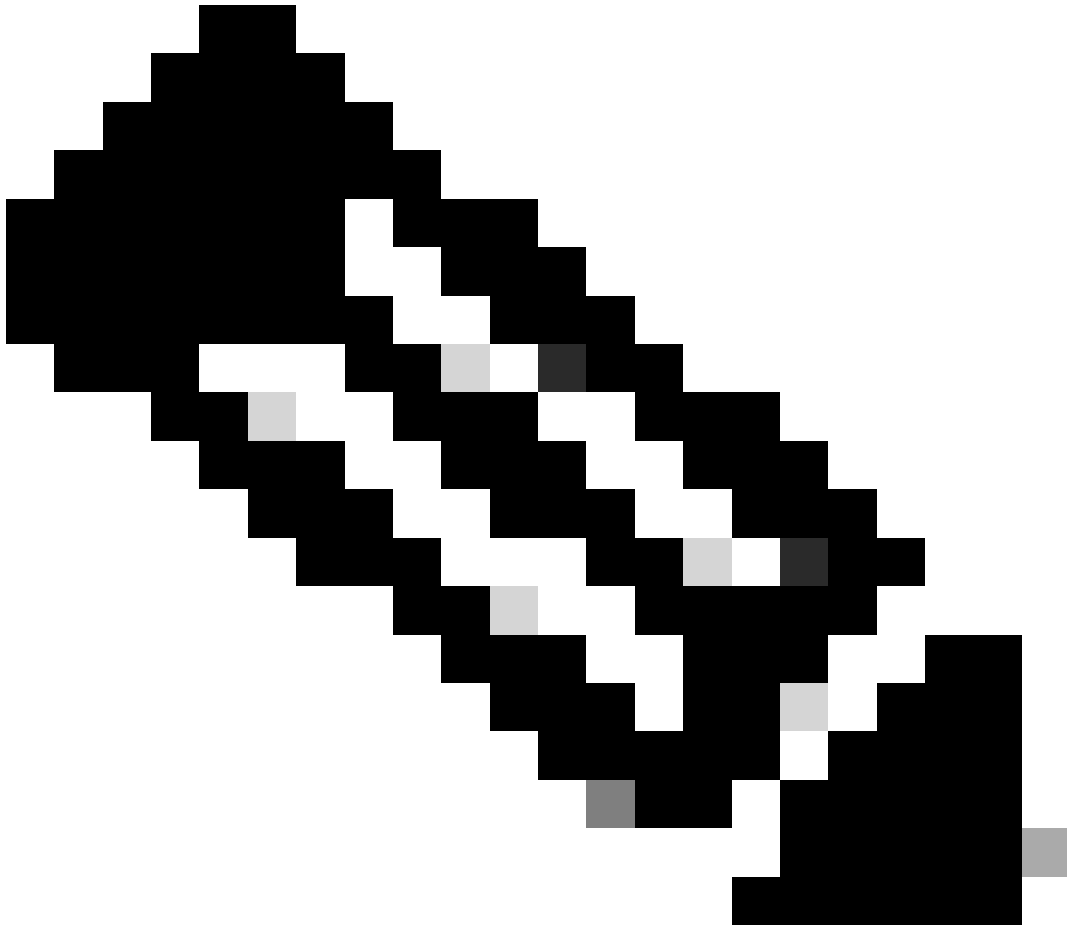
### CA 라우터

Server Certificate Authority는 VPN 게이트웨이에 대한 인증을 제공하기 위해 사용자에게 ID 인증서를 발급합니다. 또한 라우터는 CRL 데이터베이스 파일을 저장하고 CDP(CRL 배포 지점)의 역할을 합니다.

CDP는 VPN 게이트웨이 및 기타 최종 사용자가 CRL 정보를 검색하는 곳입니다. 이 정보는 로컬로

캐시되며 특정 기간 동안만 유효합니다. 이 시간이 만료되면 새 CRL이 다운로드됩니다.

---



참고: CRL 데이터베이스와 디바이스에서 CRL에 액세스할 수 있는 위치는 동일한 디바이스에 있을 수 있습니다. 그러나 보안상의 이유로 엔드 디바이스 액세스 권한이 있는 CRL은 CRL 데이터베이스와 다른 디바이스에 저장되는 것이 좋습니다. 이 예에서 CA 라우터는 CRL 데이터베이스를 저장하고 VPN 게이트웨이에 대한 CDP 역할을 합니다.

---

```
<#root>
```

```
crypto pki server CAS
database level complete
no database archive
issuer-name cn=calo_root,ou=TAC,o=cisco
grant auto
hash sha256
```

```
lifetime crl 2
```

```
lifetime certificate 300
```

```
lifetime ca-certificate 1000
```

```
cdp-url http://192.0.2.10/cgi-bin/pkiclient.exe?operation=GetCRL
```

```
eku server-auth client-auth  
database url ser nvram:
```

```
crypto pki trustpoint TP-self-signed-1507329386  
enrollment selfsigned  
subject-name cn=IOS-Self-Signed-Certificate-1507329386  
revocation-check none  
rsa-keypair TP-self-signed-1507329386
```

```
crypto pki trustpoint CAS  
revocation-check crl  
rsa-keypair CAS
```

```
interface GigabitEthernet2  
ip address 192.0.2.10 255.255.255.0  
negotiation auto
```

```
ip http server
```

```
ntp master 1
```

## VPN 게이트웨이 컨피그레이션

FTD는 인증서를 인증 방법으로 사용하는 최종 사용자에게 원격 액세스 VPN을 제공하도록 구성됩니다(인증서만 해당). 사용자로부터 ID 인증서를 수신하면 FTD는 알려진 CA(Certificate Authority)에서 발급한 인증서인지 확인하고, 인증서에 정의된 CDP에서 CRL을 가져와서 유효성을 확인합니다.

```
<#root>
```

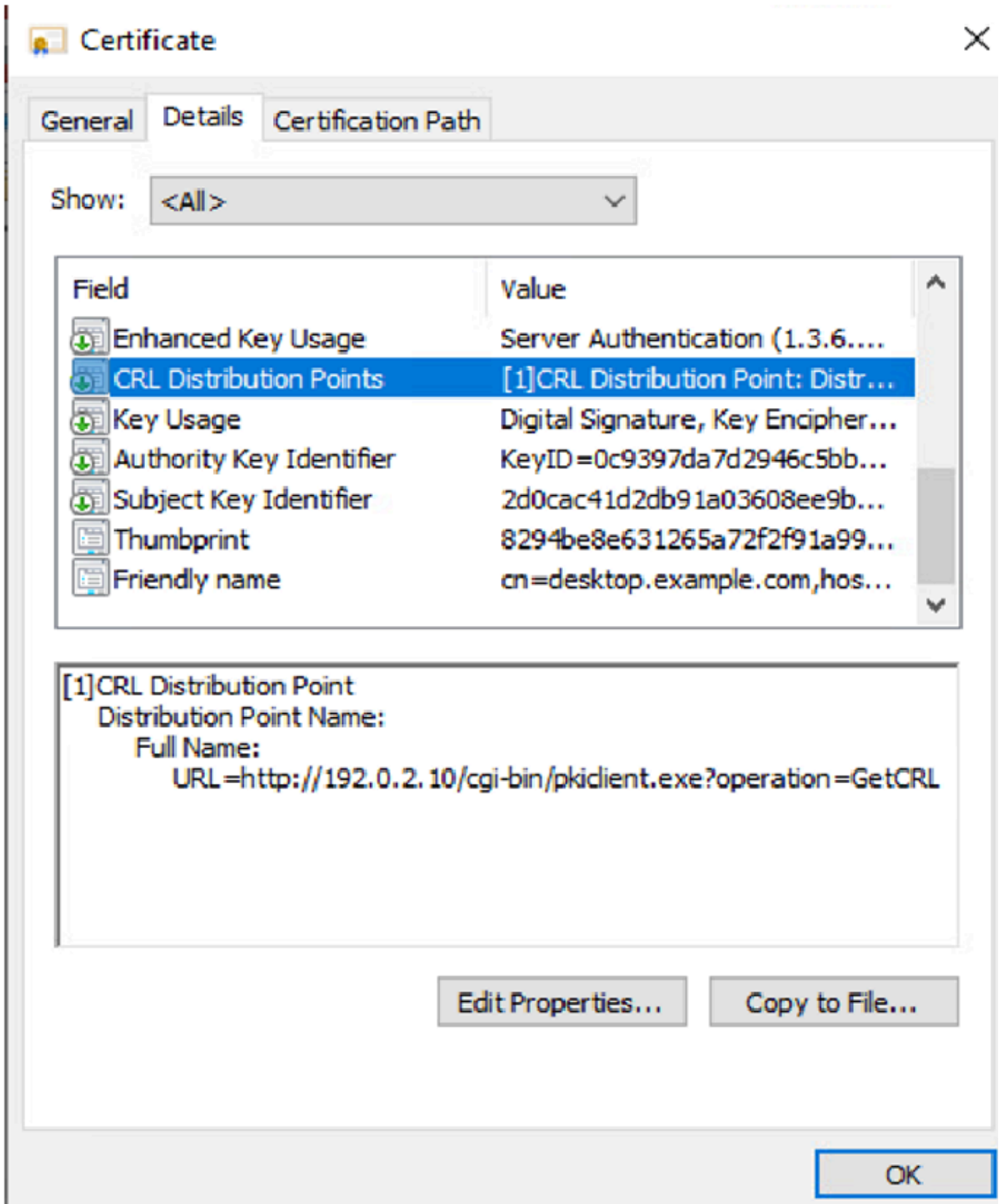
```
tunnel-group local type remote-access  
tunnel-group local general-attributes  
address-pool AC_pool  
default-group-policy local_gp  
username-from-certificate use-entire-name  
tunnel-group local_test webvpn-attributes
```

```
authentication certificate
```

```
group-alias test enable
```

## Windows 장치

ID 인증서가 CA 서버에서 발급되어 Windows 디바이스에 설치되었습니다.



## 검증

다음 디버깅 및 캡처는 유효한 인증서를 사용하는 사용자(작업 시나리오)와 취소된 인증서를 사용하는 사용자(비작업 시나리오) 간의 차이를 표시합니다.

## 시나리오 1. 인증서는 인증에 유효합니다.

사용자가 연결 시도를 시작하면 VPN 게이트웨이가 FTD에 ID 인증서를 제공합니다. 그러면 VPN 게이트웨이가 발급자가 알려진 권한을 가지고 있는지 확인하고 HTTP/GET 요청을 통해 ID 인증서에 정의된 CDP에서 CRL을 요청하기 시작합니다. CA 서버는 CRL로 응답하고 FTD는 인증서의 일련 번호가 나열되는지 확인합니다. CRL이 비어 있으므로(폐기된 인증서 없음) FTD는 인증서를 유효한 것으로 받아들이고 사용자가 인증할 수 있도록 허용합니다.

<#root>

PKI[7]: Cert to verify

PKI[7]: -----Certificate-----:

Serial Number: 2 (0x2)

Issuer: O=cisco, OU=TAC, CN=calo\_root

Subject: CN=desktop.example.com/unstructuredName=CA-router

PKI[12]: pki\_verify\_cb, pki\_oss1\_validate.c:358

PKI[8]: val status=1: cert subject: /O=cisco/OU=TAC/CN=calo\_root. ctx->error: (0)ok, cert\_idx: 1

PKI[12]: pki\_verify\_cb, pki\_oss1\_validate.c:358

PKI[8]: val status=1: cert subject: /CN=desktop.example.com/unstructuredName=CA-router. ctx->error: (0)

PKI[8]: pki\_oss1\_find\_valid\_chain took 217 microsecs

PKI[6]: Verified chain:

PKI[14]: pki\_oss1\_get\_cert\_summary, pki\_oss1.c:119

PKI[6]: -----Certificate-----:

Serial Number: 2 (0x2)

Issuer: O=cisco, OU=TAC, CN=calo\_root

Subject: CN=desktop.example.com/unstructuredName=CA-router

PKI[14]: pki\_oss1\_get\_cert\_summary, pki\_oss1.c:119

PKI[6]: -----Certificate-----:

Serial Number: 1 (0x1)

Issuer: O=cisco, OU=TAC, CN=calo\_root

Subject: O=cisco, OU=TAC, CN=calo\_root

[..output omitted]

CRYPTO\_PKI: bitValue of KEY\_USAGE = a0PKI[7]: CRYPTO\_PKI:check\_key\_usage: Checking KU for case VPN peer

PKI[7]: CRYPTO\_PKI:check\_key\_usage: KU bit digitalSignature is ON.

PKI[7]: ExtendedKeyUsage OID = serverAuth NOT acceptable for usage type SSL VPN Peer

PKI[7]: ExtendedKeyUsage OID = clientAuth acceptable for usage type: SSL VPN Peer

PKI[7]: check\_key\_usage:Extended Key/Key Usage check OK

PKI[12]: pki\_oss1\_revocation\_check, pki\_oss1\_validate.c:931

PKI[7]: Starting revocation check for session 0x06c8d45f

PKI[12]: pki\_init\_revocation, pki\_oss1\_revocation.c:162

PKI[12]: pki\_oss1\_eval\_revocation, pki\_oss1\_validate.c:699

PKI[7]: Evaluating session revocation status, 1 certs to check

PKI[8]: session 0x06c8d45f, cert 0 has rev\_status 0, using methods 1/3/0 at index 0

PKI[12]: cert\_revoc\_exempt, pki\_oss1\_revocation.c:250

PKI[13]: get\_tp\_from\_policy, pki\_oss1\_policy\_transition.c:230

PKI[11]: polinfo->name: CRL-AC

PKI[11]: tp label: Trustpool

PKI[13]: label: CRL-AC

PKI[13]: pki\_cr1\_cached, pki\_oss1\_cr1\_cache.c:1351

PKI[13]: get\_tp\_from\_policy, pki\_oss1\_policy\_transition.c:230

PKI[11]: polinfo->name: CRL-AC

PKI[11]: tp label: Trustpool

PKI[13]: label: CRL-AC

PKI[12]: pki\_ossl\_check\_cache, pki\_ossl\_crl\_cache.c:1269  
PKI[7]: Starting OSSL CRL cache check.  
PKI[12]: pki\_ossl\_crypto\_build\_crl\_dp\_list, pki\_ossl\_crl\_cache.c:326  
PKI[12]: pki\_get\_der\_cdp\_ext, crypto\_pki.c:1528  
PKI[14]: url\_type\_allowed, pki\_ossl\_crl\_cache.c:153

PKI[9]: Attempting to find cached CRL for CDP <http://192.0.2.10/cgi-bin/pkiclient.exe?operation=GetCRL>

PKI[12]: pki\_ossl\_SelectCRLByIssuerTimeDER, pki\_ossl\_crl\_cache.c:1219  
PKI[14]: pki\_ossl\_get\_name\_string, pki\_ossl.c:315  
PKI[9]: Select DER crl(O=cisco, OU=TAC, CN=calo\_root)  
PKI[12]: pki\_ossl\_get\_crl\_internal, pki\_ossl\_crl\_cache.c:506  
PKI[7]: CRL not cached. Initiating CRL download for cert idx 0.  
PKI[12]: do\_get\_crl, pki\_ossl\_revocation.c:85  
PKI[9]: starting CRL FSM #0  
PKI[11]: drive\_fsm, pki\_ossl\_revocation.c:33  
PKI[8]: [Sess: 0x06c8d45f, Cert: 0] FSM: In PKICRL\_InitTransaction  
PKI[12]: get\_cdps, pki\_crl\_fsm\_act.c:202  
PKI[13]: get\_tp\_from\_policy, pki\_ossl\_policy\_transition.c:230  
PKI[11]: polinfo->name: CRL-AC  
PKI[11]: tp label: Trustpool  
PKI[13]: label: CRL-AC  
PKI[12]: pki\_ossl\_crypto\_build\_crl\_dp\_list, pki\_ossl\_crl\_cache.c:326  
PKI[12]: pki\_get\_der\_cdp\_ext, crypto\_pki.c:1528  
PKI[14]: url\_type\_allowed, pki\_ossl\_crl\_cache.c:153

PKI[7]: cdp: (len=58, type=URI, prot=HTTP) <http://192.0.2.10/cgi-bin/pkiclient.exe?operation=GetCRL>

PKI[8]: [Sess: 0x06c8d45f, Cert: 0] FSM: PKICRL\_InitTransaction, Return status: 0  
PKI[8]: [Sess: 0x06c8d45f, Cert: 0] FSM: In PKICRL\_NextCDP  
PKI[12]: crldl\_cdp\_blacklisted, pki\_ossl\_crl.c:1374  
PKI[12]: crl\_find\_pending\_crl, pki\_ossl\_crl.c:1155  
PKI[13]: get\_pending\_crl\_list, pki\_ossl\_crl.c:1101  
PKI[13]: crypto\_pki\_get\_ossl\_env, pki\_ossl.c:42  
PKI[14]: cmp\_cdp\_info, pki\_ossl\_crl.c:1121  
PKI[14]: cmp\_cdp\_info, pki\_ossl\_crl.c:1121  
PKI[14]: cmp\_cdp\_info, pki\_ossl\_crl.c:1121  
PKI[7]: CDP is not blacklisted  
PKI[8]: [Sess: 0x06c8d45f, Cert: 0] FSM: PKICRL\_NextCDP, Return status: 0  
PKI[8]: [Sess: 0x06c8d45f, Cert: 0] FSM: In PKICRL\_Request  
PKI[13]: crldp\_download\_pending, pki\_ossl\_crl.c:1184  
PKI[12]: crl\_find\_pending\_crl, pki\_ossl\_crl.c:1155  
PKI[13]: get\_pending\_crl\_list, pki\_ossl\_crl.c:1101  
PKI[13]: crypto\_pki\_get\_ossl\_env, pki\_ossl.c:42  
PKI[14]: cmp\_cdp\_info, pki\_ossl\_crl.c:1121  
PKI[14]: cmp\_cdp\_info, pki\_ossl\_crl.c:1121  
PKI[14]: cmp\_cdp\_info, pki\_ossl\_crl.c:1121  
PKI[8]: session 0x06c8d45f adding pending CRL entry for cert 0  
PKI[12]: crldp\_add\_pending\_download, pki\_ossl\_crl.c:1203  
PKI[12]: crl\_find\_pending\_crl, pki\_ossl\_crl.c:1155  
PKI[13]: get\_pending\_crl\_list, pki\_ossl\_crl.c:1101  
PKI[13]: crypto\_pki\_get\_ossl\_env, pki\_ossl.c:42  
PKI[14]: cmp\_cdp\_info, pki\_ossl\_crl.c:1121  
PKI[14]: cmp\_cdp\_info, pki\_ossl\_crl.c:1121  
PKI[14]: cmp\_cdp\_info, pki\_ossl\_crl.c:1121  
PKI[13]: get\_pending\_crl\_list, pki\_ossl\_crl.c:1101  
PKI[13]: crypto\_pki\_get\_ossl\_env, pki\_ossl.c:42  
PKI[12]: retrieve\_crl, pki\_crl\_fsm\_act.c:233  
PKI[13]: get\_tp\_from\_policy, pki\_ossl\_policy\_transition.c:230  
PKI[11]: polinfo->name: CRL-AC  
PKI[11]: tp label: Trustpool

PKI[13]: label: CRL-AC

PKI[7]: CDP type HTTP

PKI[7]: getting http://192.0.2.10/cgi-bin/pkiclient.exe?operation=GetCRL

PKI[12]: pki\_ossl\_crl\_build\_http\_io, pki\_ossl\_crl.c:1017

PKI[13]: pki\_parse\_uri, pki\_ossl\_uri.c:75

PKI[14]: pki\_uri\_map\_protocol, pki\_ossl\_uri.c:17

PKI[14]: pki\_uri\_get\_port, pki\_ossl\_uri.c:34

PKI[13]: pki\_free\_uri, pki\_ossl\_uri.c:57

PKI[11]: pki\_crl\_request\_send\_async, pki\_ossl\_crl.c:627

PKI[8]: [15] IOCB allocated

PKI[7]: PKI CRL I/O request queue result: IO\_STATUS\_QUEUEED

PKI[8]: [Sess: 0x06c8d45f, Cert: 0] FSM: PKICRL\_Request, Return status: 0

PKI[7]: Chain revocation status: good: 0, exempt: 0, cached: 0, revoked: 0, error: 0, pending: 1, fail-

PKI[9]: Async unlocked for session 0x06c8d45f

PKI[8]: [15] Received IO request msg

PKI[8]: [15] DNS resolve issued for 192.0.2.10

PKI[9]: CERT API thread sleeps!

PKI[7]: [15] DNS resolve 192.0.2.10 (192.0.2.10)

PKI[8]: [15] Socket open success

PKI[8]: [15] IPv4 Route lookup to 192.0.2.10 use interface outside

PKI[8]: [15] Connect sent to 192.0.2.10 from 192.0.2.1

PKI[12]: pki\_io\_cbfunc\_log\_revocation\_check, pki\_ossl\_revocation.c:421

PKI[7]: 6717056: Attempting CRL revocation check from outside:192.0.2.1/62075 to 192.0.2.10/80 using HT

PKI[8]: [15] Received Socket transmit ready msg

----- Begin Data Type:HTTP Request [15]

Length: 76 -----

47 45 54 20 2f 63 67 69 2d 62 69 6e 2f 70 6b 69 | GET /cgi-bin/pki  
63 6c 69 65 6e 74 2e 65 78 65 3f 6f 70 65 72 61 | client.exe?opera  
74 69 6f 6e 3d 47 65 74 43 52 4c 20 48 54 54 50 | tion=GetCRL HTTP  
2f 31 2e 30 0d 0a 48 6f192.0.2.10 73 74 3a 20 31 39 32 2e | /1.0..Host: 192.  
31 38 31 2e 33 2e 31 30 0d 0a 0d 0a | 0.2.10....

----- End Data Type:HTTP Request [15]

Length: 76 -----

PKI[8]: [15] Sent 76 bytes

PKI[8]: [15] Received Socket read ready msg

PKI[8]: [15] read 662 bytes

PKI[8]: [15] Read EOF

PKI[12]: pki\_io\_cbfunc, pki\_crl\_fsm\_act.c:59

PKI[7]: Callback received for vcid: 0, sess\_id: 0x06c8d45f, cert\_idx: 0, status: IO\_STATUS\_OK(1), data

PKI[13]: get\_fsm\_data, pki\_ossl\_revocation.c:446

PKI[7]: [15] IOCB freed

PKI[13]: CERT\_API\_QueueFSMEvent, vpn3k\_cert\_api.c:137

PKI[13]: CERT\_API\_req\_enqueue, vpn3k\_cert\_api.c:2913

PKI[9]: CERT API thread wakes up!



PKI[12]: CERT\_API\_Q\_Process, vpn3k\_cert\_api.c:2811  
PKI[12]: CERT\_API\_process\_req\_msg, vpn3k\_cert\_api.c:2746  
PKI[8]: process msg cmd=2, session=0x06c8d45f  
PKI[9]: Async locked for session 0x06c8d45f  
PKI[11]: pki\_notify\_fsm\_evt, pki\_ossl\_revocation.c:56  
PKI[11]: drive\_fsm, pki\_ossl\_revocation.c:33  
PKI[8]: [Sess: 0x06c8d45f, Cert: 0] FSM: In PKICRL\_ProcessResp  
PKI[13]: pki\_ossl\_util\_find\_http\_payload, pki\_ossl\_utils.c:36  
  
PKI[8]: Received CRL of length 249 for session 0x06c8d45f, cert idx 0

PKI[13]: get\_tp\_from\_policy, pki\_ossl\_policy\_transition.c:230  
PKI[11]: polinfo->name: CRL-AC  
PKI[11]: tp label: Trustpool  
PKI[13]: label: CRL-AC  
PKI[12]: pki\_ossl\_crl\_add\_to\_cache, pki\_ossl\_crl\_cache.c:1177  
PKI[12]: pki\_ossl\_crypto\_verify\_and\_insert\_crl, pki\_ossl\_crl\_cache.c:1126  
PKI[12]: pki\_ossl\_insert\_der\_crl\_int, pki\_ossl\_crl\_cache.c:1017  
PKI[8]: Inserting CRL  
PKI[14]: pki\_ossl\_get\_crl\_summary, pki\_ossl.c:151  
PKI[8]: -----CRL-----:  
Certificate Revocation List (CRL):  
Version 1 (0x0)  
Signature Algorithm: sha1WithRSAEncryption  
Issuer: /O=cisco/OU=TAC/CN=calo\_root

Last Update: Sep 24 22:18:38 2023 GMT

Next Update: Sep 25 00:18:38 2023 GMT

No Revoked Certificates.

[..outout ommitted]

PKI[7]: Evaluating session revocation status, 1 certs to check

PKI[8]: session 0x06c8d45f, cert 0 has rev\_status 3, using methods 1/3/0 at index 0  
PKI[7]: Chain revocation status: good: 0, exempt: 0, cached: 1, revoked: 0, error: 0, pending: 0, fail-  
PKI[7]: session: 0x06c8d45f, all revocation processing complete  
PKI[5]: session: 0x06c8d45f, CRL for certificate 0 has been cached  
PKI[12]: pki\_ossl\_rebuild\_ca\_store, pki\_ossl\_certstore.c:194  
PKI[13]: crypto\_pki\_get\_ossl\_env, pki\_ossl.c:42  
PKI[12]: pki\_ossl\_crl\_add\_cache\_to\_store, pki\_ossl\_crl\_cache.c:1396  
PKI[9]: OSSL certstore updated with 0 certs, 1 CRLs and 0 policies, 0 certs added to stack

PKI[7]: session 0x06c8d45f, Starting chain validation with cached CRL checking

PKI[12]: pki\_ossl\_find\_valid\_chain, pki\_ossl\_validate.c:472  
PKI[9]: Begin sorted cert chain  
PKI[14]: pki\_ossl\_get\_cert\_summary, pki\_ossl.c:119  
PKI[9]: -----Certificate-----:  
Serial Number: 1 (0x1)  
Issuer: O=cisco, OU=TAC, CN=calo\_root  
Subject: O=cisco, OU=TAC, CN=calo\_root

```
PKI[14]: pki_ossl_get_cert_summary, pki_ossl.c:119
PKI[9]: -----Certificate-----:
Serial Number: 2 (0x2)
Issuer: O=cisco, OU=TAC, CN=calo_root
Subject: CN=desktop.example.com/unstructuredName=CA-router

PKI[9]: End sorted cert chain
PKI[13]: pki_ossl_get_store, pki_ossl_certstore.c:61
PKI[12]: pki_ossl_rebuild_ca_store, pki_ossl_certstore.c:194
PKI[13]: crypto_pki_get_ossl_env, pki_ossl.c:42
PKI[13]: crypto_pki_get_ossl_env, pki_ossl.c:42
PKI[14]: pki_ossl_get_cert_summary, pki_ossl.c:119
PKI[9]: Cert to verify
PKI[9]: -----Certificate-----:
Serial Number: 2 (0x2)
Issuer: O=cisco, OU=TAC, CN=calo_root
Subject: CN=desktop.example.com/unstructuredName=CA-router

PKI[12]: pki_verify_cb, pki_ossl_validate.c:358
PKI[8]: val status=1: cert subject: /O=cisco/OU=TAC/CN=calo_root. ctx->error: (0)ok, cert_idx: 1
PKI[12]: pki_verify_cb, pki_ossl_validate.c:358
PKI[8]: val status=1: cert subject: /CN=desktop.example.com/unstructuredName=CA-router. ctx->error: (0)
PKI[8]: pki_ossl_find_valid_chain took 167 microseconds

PKI[7]: session 0x06c8d45f, Validation with CRL checking completed, status 0

PKI[7]: session 0x06c8d45f, Revocation check complete, no revoked certs found

PKI[12]: pki_ossl_do_callback, pki_ossl_validate.c:164
PKI[13]: CERT_Close, vpn3k_cert_api.c:291
PKI[8]: Close session 0x06c8d45f asynchronously
PKI[13]: CERT_API_req_enqueue, vpn3k_cert_api.c:2913
PKI[9]: Async unlocked for session 0x06c8d45f
PKI[8]: No IOCB found for SOCKET_CLOSE message, handle 0x5dba666
PKI[12]: CERT_API_Q_Process, vpn3k_cert_api.c:2811
PKI[12]: CERT_API_process_req_msg, vpn3k_cert_api.c:2746
PKI[8]: process msg cmd=1, session=0x06c8d45f
PKI[9]: Async locked for session 0x06c8d45f
PKI[9]: Async unlocked for session 0x06c8d45f
PKI[13]: pki_ossl_free_valctx, pki_ossl_validate.c:251
PKI[13]: free_fsm_data, pki_ossl_revocation.c:225
PKI[13]: oosp_free_fsmdata, pki_ossl_ocsp.c:1462
PKI[13]: free_fsm_data, pki_ossl_revocation.c:225
PKI[13]: oosp_free_fsmdata, pki_ossl_ocsp.c:1462
PKI[9]: CERT API thread sleeps!
PKI[13]: CERT_GetGroupFromSSLRule, vpn3k_cert_api.c:1672
```

다음 FTD 캡처는 CRL을 검색하기 위해 FTD와 CDP(이 경우 CA 서버) 간의 HTTP 트랜잭션을 표시합니다.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.0.2.1	192.0.2.10	TCP	70	65090 → 80 [SYN] Seq=0 Win=32768 Len=0 MSS=1460 TSval=2698888496
2	0.001022	192.0.2.10	192.0.2.1	TCP	70	80 → 65090 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460
3	0.000046	192.0.2.1	192.0.2.10	TCP	66	65090 → 80 [ACK] Seq=1 Ack=1 Win=32768 Len=0 TSval=2698888496
4	0.000320	192.0.2.1	192.0.2.10	HTTP	140	GET /cgi-bin/pkiclient.exe?operation=GetCRL HTTP/1.0
5	0.000763	192.0.2.10	192.0.2.1	TCP	66	80 → 65090 [ACK] Seq=1 Ack=75 Win=28960 Len=0 TSval=3224140473
6	0.004623	192.0.2.10	192.0.2.1	TCP	728	80 → 65090 [PSH, ACK] Seq=1 Ack=75 Win=28960 Len=662 TSval=2698888502

Transmission Control Protocol, Src Port: 65090, Dst Port: 80, Seq: 1, Ack: 1, Len: 74

Hypertext Transfer Protocol

- GET /cgi-bin/pkiclient.exe?operation=GetCRL HTTP/1.0\r\n
  - [Expert Info (Chat/Sequence): GET /cgi-bin/pkiclient.exe?operation=GetCRL HTTP/1.0\r\n]
    - [GET /cgi-bin/pkiclient.exe?operation=GetCRL HTTP/1.0\r\n]
    - [Severity level: Chat]
    - [Group: Sequence]
  - Request Method: GET
  - Request URI: /cgi-bin/pkiclient.exe?operation=GetCRL
    - Request URI Path: /cgi-bin/pkiclient.exe
    - Request URI Query: operation=GetCRL
  - Request Version: HTTP/1.0
  - Host: 192.0.2.10\r\n
  - \r\n
  - [Full request URI: http://192.0.2.10/cgi-bin/pkiclient.exe?operation=GetCRL]
  - [HTTP request 1/1]
  - [Response in frame: 8]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
3	0.000046	192.0.2.1	192.0.2.10	TCP	66	65090 → 80 [ACK] Seq=1 Ack=1 Win=32768 Len=0 TSval=2698888496 TSecr=3224140467
4	0.000320	192.0.2.1	192.0.2.10	HTTP	140	GET /cgi-bin/pkiclient.exe?operation=GetCRL HTTP/1.0
5	0.000763	192.0.2.10	192.0.2.1	TCP	66	80 → 65090 [ACK] Seq=1 Ack=75 Win=28960 Len=0 TSval=3224140468 TSecr=2698888496
6	0.004623	192.0.2.10	192.0.2.1	TCP	728	80 → 65090 [PSH, ACK] Seq=1 Ack=75 Win=28960 Len=662 TSval=3224140473 TSecr=2698888496
7	0.000031	192.0.2.1	192.0.2.10	TCP	66	65090 → 80 [ACK] Seq=75 Ack=663 Win=32768 Len=0 TSval=2698888502 TSecr=3224140473
8	0.000000	192.0.2.10	192.0.2.1	PKIX-C...	66	Certificate Revocation List
9	0.000046	192.0.2.1	192.0.2.10	TCP	66	65090 → 80 [ACK] Seq=75 Ack=664 Win=32768 Len=0 TSval=2698888502 TSecr=0
10	0.000137	192.0.2.1	192.0.2.10	TCP	66	65090 → 80 [FIN, PSH, ACK] Seq=75 Ack=664 Win=32768 Len=0 TSval=2698888502 TSecr=0
11	0.000503	192.0.2.10	192.0.2.1	TCP	66	80 → 65090 [ACK] Seq=664 Ack=76 Win=28960 Len=0 TSval=3224140474 TSecr=2698888502

Frame 8: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

Ethernet II, Src: VMware\_b3:9e:77 (00:50:56:b3:9e:77), Dst: VMware\_b3:2f:ac (00:50:56:b3:2f:ac)

Internet Protocol version 4, Src: 192.0.2.10, Dst: 192.0.2.1

Transmission Control Protocol, Src Port: 80, Dst Port: 65090, Seq: 663, Ack: 75, Len: 0

[2 Reassembled TCP Segments (662 bytes): #6(662), #8(0)]

Hypertext Transfer Protocol

Certificate Revocation List

- signedCertificateList
  - signature (sha1WithRSAEncryption)
  - issuer: rdnSequence (0)
  - thisUpdate: utcTime (0)
  - nextUpdate: utcTime (0)
- algorithmIdentifier (sha1WithRSAEncryption)
  - Algorithm Id: 1.2.840.113549.1.1.5 (sha1WithRSAEncryption)
  - Padding: 0
  - encrypted: 0a9b3a3e44674360c548fb7c6f058e7ba9687c99e16311dd2bfc8a31134e59b589cbe423...

## 시나리오 2. 인증서가 취소되고 인증에 실패합니다

ID 인증서는 CA 서버에서 폐기되고 CRL 데이터베이스 파일에 등록됩니다. 그러나 업데이트된 CRL은 현재 CRL이 만료될 때까지(2시간 동안 유효하도록 구성된) FTD에서 사용할 수 없습니다.

<#root>

```
CA-router#show crypto pki server CAS crl
Certificate Revocation List:
Issuer: cn=calo_root,ou=TAC,o=cisco
This Update: 22:18:38 UTC Sep 24 2023
Next Update: 00:18:38 UTC Sep 25 2023

Number of CRL entries: 0
```

CRL size: 249 bytes

```
CA-router#show crypto pki server CAS certificates
Serial Issued date Expire date Subject Name
1 20:18:36 UTC Sep 24 2023 20:18:36 UTC Jun 20 2026 cn=calo_root ou=TAC o=cisco
2 20:19:33 UTC Sep 24 2023 20:19:33 UTC Jul 20 2024 hostname=CA-router cn=desktop.example.com

3 23:50:58 UTC Sep 24 2023 23:50:58 UTC Jul 20 2024 cn=test.cisco.com
```

CA-router#

```
crypto pki server CAS revoke 0x2
```

% Certificate 02 succesfully revoked.

```
CA-router#show crypto pki server CAS crl
Certificate Revocation List:
Issuer: cn=calo_root,ou=TAC,o=cisco
This Update: 23:59:32 UTC Sep 24 2023
Next Update: 01:59:32 UTC Sep 25 2023
Number of CRL entries: 1
CRL size: 272 bytes
```

Revoked Certificates:

Serial Number (hex): 02

Revocation Date: 23:59:32 UTC Sep 24 2023

CRL이 만료되었음을 확인한 후 새 연결을 시도할 때 인증서 검사는 대부분 이전 시나리오와 동일합니다. FTD에서 캐시에 CRL이 없음을 확인한 후 새 CRL이 요청됩니다. 새 CRL을 받으면 FTD는 ID 인증서의 일련 번호가 목록에 포함되어 있는지 여부를 확인합니다. Serial Number(일련 번호)가 Revoked(해지됨)로 표시되고 FTD가 계속해서 사용자에게 대한 액세스를 거부합니다.

<#root>

```
CRYPTO_PKI: bitValue of KEY_USAGE = a0PKI[7]: CRYPTO_PKI:check_key_usage: Checking KU for case VPN peer
PKI[7]: CRYPTO_PKI:check_key_usage: KU bit digitalSignature is ON.
PKI[7]: ExtendedKeyUsage OID = serverAuth NOT acceptable for usage type SSL VPN Peer
PKI[7]: ExtendedKeyUsage OID = clientAuth acceptable for usage type: SSL VPN Peer
PKI[7]: check_key_usage:Extended Key/Key Usage check OK
PKI[12]: pki_ossl_revocation_check, pki_ossl_validate.c:931
PKI[7]: Starting revocation check for session 0x0dc288f9
PKI[12]: pki_init_revocation, pki_ossl_revocation.c:162
```

PKI[12]: pki\_ossl\_eval\_revocation, pki\_ossl\_validate.c:699  
PKI[7]: Evaluating session revocation status, 1 certs to check  
PKI[8]: session 0x0dc288f9, cert 0 has rev\_status 0, using methods 1/3/0 at index 0  
PKI[12]: cert\_revoc\_exempt, pki\_ossl\_revocation.c:250  
PKI[13]: get\_tp\_from\_policy, pki\_ossl\_policy\_transition.c:230  
PKI[11]: polinfo->name: CRL-AC  
PKI[11]: tp label: Trustpool  
PKI[13]: label: CRL-AC  
PKI[13]: pki\_crl\_cached, pki\_ossl\_crl\_cache.c:1351  
PKI[13]: get\_tp\_from\_policy, pki\_ossl\_policy\_transition.c:230  
PKI[11]: polinfo->name: CRL-AC  
PKI[11]: tp label: Trustpool  
PKI[13]: label: CRL-AC  
PKI[12]: pki\_ossl\_check\_cache, pki\_ossl\_crl\_cache.c:1269  
PKI[7]: Starting OSSL CRL cache check.  
PKI[12]: pki\_ossl\_crypto\_build\_crdp\_list, pki\_ossl\_crl\_cache.c:326  
PKI[12]: pki\_get\_der\_cdp\_ext, crypto\_pki.c:1528  
PKI[14]: url\_type\_allowed, pki\_ossl\_crl\_cache.c:153

PKI[9]: Attempting to find cached CRL for CDP <http://192.0.2.10/cgi-bin/pkiclient.exe?operation=GetCRL>

PKI[12]: pki\_ossl\_SelectCRLByIssuerTimeDER, pki\_ossl\_crl\_cache.c:1219  
PKI[14]: pki\_ossl\_get\_name\_string, pki\_ossl.c:315  
PKI[9]: Select DER crl(O=cisco, OU=TAC, CN=calo\_root)  
PKI[12]: pki\_ossl\_get\_crl\_internal, pki\_ossl\_crl\_cache.c:506

PKI[7]: CRL not cached. Initiating CRL download for cert idx 0.

PKI[12]: do\_get\_crl, pki\_ossl\_revocation.c:85  
PKI[9]: starting CRL FSM #0  
PKI[11]: drive\_fsm, pki\_ossl\_revocation.c:33  
PKI[8]: [Sess: 0x0dc288f9, Cert: 0] FSM: In PKICRL\_InitTransaction  
PKI[12]: get\_cdps, pki\_crl\_fsm\_act.c:202  
PKI[13]: get\_tp\_from\_policy, pki\_ossl\_policy\_transition.c:230  
PKI[11]: polinfo->name: CRL-AC  
PKI[11]: tp label: Trustpool  
PKI[13]: label: CRL-AC  
PKI[12]: pki\_ossl\_crypto\_build\_crdp\_list, pki\_ossl\_crl\_cache.c:326  
PKI[12]: pki\_get\_der\_cdp\_ext, crypto\_pki.c:1528  
PKI[14]: url\_type\_allowed, pki\_ossl\_crl\_cache.c:153

PKI[7]: cdp: (len=58, type=URI, prot=HTTP) <http://192.0.2.10/cgi-bin/pkiclient.exe?operation=GetCRL>

PKI[8]: [Sess: 0x0dc288f9, Cert: 0] FSM: PKICRL\_InitTransaction, Return status: 0  
PKI[8]: [Sess: 0x0dc288f9, Cert: 0] FSM: In PKICRL\_NextCDP  
PKI[12]: crldl\_cdp\_blacklisted, pki\_ossl\_crl.c:1374  
PKI[12]: crl\_find\_pending\_crl, pki\_ossl\_crl.c:1155  
PKI[13]: get\_pending\_crl\_list, pki\_ossl\_crl.c:1101  
PKI[13]: crypto\_pki\_get\_ossl\_env, pki\_ossl.c:42  
PKI[14]: cmp\_cdp\_info, pki\_ossl\_crl.c:1121  
PKI[14]: cmp\_cdp\_info, pki\_ossl\_crl.c:1121  
PKI[14]: cmp\_cdp\_info, pki\_ossl\_crl.c:1121  
PKI[7]: CDP is not blacklisted  
PKI[8]: [Sess: 0x0dc288f9, Cert: 0] FSM: PKICRL\_NextCDP, Return status: 0  
PKI[8]: [Sess: 0x0dc288f9, Cert: 0] FSM: In PKICRL\_Request  
PKI[13]: crldp\_download\_pending, pki\_ossl\_crl.c:1184  
PKI[12]: crl\_find\_pending\_crl, pki\_ossl\_crl.c:1155  
PKI[13]: get\_pending\_crl\_list, pki\_ossl\_crl.c:1101  
PKI[13]: crypto\_pki\_get\_ossl\_env, pki\_ossl.c:42  
PKI[14]: cmp\_cdp\_info, pki\_ossl\_crl.c:1121  
PKI[14]: cmp\_cdp\_info, pki\_ossl\_crl.c:1121

PKI[14]: cmp\_cdp\_info, pki\_oss1\_crl.c:1121  
PKI[8]: session 0x0dc288f9 adding pending CRL entry for cert 0  
PKI[12]: crl\_dp\_add\_pending\_download, pki\_oss1\_crl.c:1203  
PKI[12]: crl\_find\_pending\_crl, pki\_oss1\_crl.c:1155  
PKI[13]: get\_pending\_crl\_list, pki\_oss1\_crl.c:1101  
PKI[13]: crypto\_pki\_get\_oss1\_env, pki\_oss1.c:42  
PKI[14]: cmp\_cdp\_info, pki\_oss1\_crl.c:1121  
PKI[14]: cmp\_cdp\_info, pki\_oss1\_crl.c:1121  
PKI[14]: cmp\_cdp\_info, pki\_oss1\_crl.c:1121  
PKI[13]: get\_pending\_crl\_list, pki\_oss1\_crl.c:1101  
PKI[13]: crypto\_pki\_get\_oss1\_env, pki\_oss1.c:42  
PKI[12]: retrieve\_crl, pki\_crl\_fsm\_act.c:233  
PKI[13]: get\_tp\_from\_policy, pki\_oss1\_policy\_transition.c:230  
PKI[11]: polinfo->name: CRL-AC  
PKI[11]: tp label: Trustpool  
PKI[13]: label: CRL-AC

PKI[7]: CDP type HTTP

PKI[7]: getting http://192.0.2.10/cgi-bin/pkiclient.exe?operation=GetCRL

PKI[12]: pki\_oss1\_crl\_build\_http\_io, pki\_oss1\_crl.c:1017  
PKI[13]: pki\_parse\_uri, pki\_oss1\_uri.c:75  
PKI[14]: pki\_uri\_map\_protocol, pki\_oss1\_uri.c:17  
PKI[14]: pki\_uri\_get\_port, pki\_oss1\_uri.c:34  
PKI[13]: pki\_free\_uri, pki\_oss1\_uri.c:57  
PKI[11]: pki\_crl\_request\_send\_async, pki\_oss1\_crl.c:627  
PKI[8]: [16] IOCB allocated  
PKI[7]: PKI CRL I/O request queue result: IO\_STATUS\_QUEUEUED  
PKI[8]: [Sess: 0x0dc288f9, Cert: 0] FSM: PKICRL\_Request, Return status: 0  
PKI[7]: Chain revocation status: good: 0, exempt: 0, cached: 0, revoked: 0, error: 0, pending: 1, fail-  
PKI[9]: Async unlocked for session 0x0dc288f9  
PKI[8]: [16] Received IO request msg  
PKI[8]: [16] DNS resolve issued for 192.0.2.10  
PKI[9]: CERT API thread sleeps!

PKI[7]: [16] DNS resolve 192.0.2.10 (192.0.2.10)

PKI[8]: [16] Socket open success

PKI[8]: [16] IPv4 Route lookup to 192.0.2.10 use interface outside

PKI[8]: [16] Connect sent to 192.0.2.10 from 192.0.2.1

PKI[12]: pki\_io\_cbfunc\_log\_revocation\_check, pki\_oss1\_revocation.c:421

PKI[7]: 6717056: Attempting CRL revocation check from outside:192.0.2.1/27791 to 192.0.2.10/80 using HTTP

PKI[8]: [16] Received Socket transmit ready msg

----- Begin Data Type:HTTP Request [16]

Length: 76 -----

47 45 54 20 2f 63 67 69 2d 62 69 6e 2f 70 6b 69 | GET /cgi-bin/pki  
63 6c 69 65 6e 74 2e 65 78 65 3f 6f 70 65 72 61 | client.exe?opera  
74 69 6f 6e 3d 47 65 74 43 52 4c 20 48 54 54 50 | tion=GetCRL HTTP

2f 31 2e 30 0d 0a 48 6f 73 74 3a 20 31 39 32 2e | /1.0..Host: 192.

31 38 31 2e 33 2e 31 30 0d 0a 0d 0a | 0.2.10....

----- End Data Type:HTTP Request [16]

Length: 76 -----

PKI[8]: [16] Sent 76 bytes

PKI[8]: [16] Received Socket read ready msg

PKI[8]: [16] read 685 bytes

PKI[8]: [16] Read EOF

PKI[12]: pki\_io\_cbfunc, pki\_crl\_fsm\_act.c:59

PKI[7]: Callback received for vcid: 0, sess\_id: 0x0dc288f9, cert\_idx: 0, status: IO\_STATUS\_OK(1), data1

PKI[13]: get\_fsm\_data, pki\_ossl\_revocation.c:446

PKI[7]: [16] IOCB freed

PKI[13]: CERT\_API\_QueueFSMEvent, vpn3k\_cert\_api.c:137

PKI[13]: CERT\_API\_req\_enqueue, vpn3k\_cert\_api.c:2913

PKI[9]: CERT API thread wakes up!

PKI[12]: CERT\_API\_Q\_Process, vpn3k\_cert\_api.c:2811

PKI[12]: CERT\_API\_process\_req\_msg, vpn3k\_cert\_api.c:2746

PKI[8]: process msg cmd=2, session=0x0dc288f9

PKI[9]: Async locked for session 0x0dc288f9

PKI[11]: pki\_notify\_fsm\_evt, pki\_ossl\_revocation.c:56

PKI[11]: drive\_fsm, pki\_ossl\_revocation.c:33

PKI[8]: [Sess: 0x0dc288f9, Cert: 0] FSM: In PKICRL\_ProcessResp

PKI[13]: pki\_ossl\_util\_find\_http\_payload, pki\_ossl\_utils.c:36

**PKI[8]: Received CRL of length 272 for session 0x0dc288f9, cert idx 0**

PKI[13]: get\_tp\_from\_policy, pki\_ossl\_policy\_transition.c:230

PKI[11]: polinfo->name: CRL-AC

PKI[11]: tp label: Trustpool

PKI[13]: label: CRL-AC

PKI[12]: pki\_ossl\_crl\_add\_to\_cache, pki\_ossl\_crl\_cache.c:1177

PKI[12]: pki\_ossl\_crypto\_verify\_and\_insert\_crl, pki\_ossl\_crl\_cache.c:1126

PKI[12]: pki\_ossl\_insert\_der\_crl\_int, pki\_ossl\_crl\_cache.c:1017

PKI[8]: Inserting CRL

PKI[14]: pki\_ossl\_get\_crl\_summary, pki\_ossl.c:151

PKI[8]: -----CRL-----:

Certificate Revocation List (CRL):

Version 1 (0x0)

Signature Algorithm: sha1WithRSAEncryption

Issuer: /O=cisco/OU=TAC/CN=calo\_root

Last Update: Sep 25 00:18:09 2023 GMT

Next Update: Sep 25 02:18:09 2023 GMT

**Number of Revoked Certificates: 1**

PKI[12]: asn1\_to\_unix\_time, crypto\_pki.c:1735

PKI[12]: asn1\_to\_unix\_time, crypto\_pki.c:1735

PKI[12]: pki\_ossl\_crypto\_certc\_insert\_CRL, pki\_ossl\_crl\_cache.c:735

PKI[7]: CRL: current time is 1695601164

PKI[7]: CRL: nextupdate time is 1695608289

PKI[7]: CRL: lastupdate time is 1695601089

PKI[7]: set CRL update timer with delay: 7125

PKI[12]: pki\_ossl\_get\_crl\_internal, pki\_ossl\_crl\_cache.c:506

PKI[7]: the current device time: 00:19:24 UTC Sep 25 2023

PKI[7]: the last CRL update time: 00:18:09 UTC Sep 25 2023

PKI[7]: the next CRL update time: 02:18:09 UTC Sep 25 2023

PKI[7]: CRL cache delay being set to: 3600000

PKI[14]: pki\_ossl\_set\_crl\_store\_dirty, pki\_ossl\_crl\_cache.c:1441

PKI[13]: crypto\_pki\_get\_ossl\_env, pki\_ossl.c:42

PKI[12]: crldl\_notify\_result, pki\_ossl\_crl.c:1304







PKI[12]: cert\_revoc\_exempt, pki\_ossl\_revocation.c:250  
PKI[13]: get\_tp\_from\_policy, pki\_ossl\_policy\_transition.c:230  
PKI[11]: polinfo->name: CRL-AC  
PKI[11]: tp label: Trustpool  
PKI[13]: label: CRL-AC  
PKI[13]: pki\_crl\_cached, pki\_ossl\_crl\_cache.c:1351  
PKI[13]: get\_tp\_from\_policy, pki\_ossl\_policy\_transition.c:230  
PKI[11]: polinfo->name: CRL-AC  
PKI[11]: tp label: Trustpool  
PKI[13]: label: CRL-AC  
PKI[12]: pki\_ossl\_check\_cache, pki\_ossl\_crl\_cache.c:1269  
PKI[7]: Starting OSSL CRL cache check.  
PKI[12]: pki\_ossl\_crypto\_build\_crl\_dp\_list, pki\_ossl\_crl\_cache.c:326  
PKI[12]: pki\_get\_der\_cdp\_ext, crypto\_pki.c:1528  
PKI[14]: url\_type\_allowed, pki\_ossl\_crl\_cache.c:153

PKI[9]: Attempting to find cached CRL for CDP http://192.0.2.10/cgi-bin/pkiclient.exe?operation=GetCRL

PKI[12]: pki\_ossl\_SelectCRLByIssuerTimeDER, pki\_ossl\_crl\_cache.c:1219  
PKI[14]: pki\_ossl\_get\_name\_string, pki\_ossl.c:315  
PKI[9]: Select DER crl(O=cisco, OU=TAC, CN=calo\_root)  
PKI[12]: pki\_ossl\_get\_crl\_internal, pki\_ossl\_crl\_cache.c:506  
PKI[13]: is\_crl\_dst, pki\_ossl\_crl\_cache.c:479  
PKI[7]: CRL for cert idx 0 found in cache  
PKI[7]: Chain revocation status: good: 0, exempt: 0, cached: 1, revoked: 0, error: 0, pending: 0, fail-  
PKI[7]: session: 0x1acca1bd, all revocation processing complete  
PKI[5]: session: 0x1acca1bd, CRL for certificate 0 has been cached  
PKI[12]: pki\_ossl\_rebuild\_ca\_store, pki\_ossl\_certstore.c:194  
PKI[13]: crypto\_pki\_get\_ossl\_env, pki\_ossl.c:42

PKI[7]: session 0x1acca1bd, Starting chain validation with cached CRL checking

PKI[12]: pki\_ossl\_find\_valid\_chain, pki\_ossl\_validate.c:472  
PKI[9]: Begin sorted cert chain  
PKI[14]: pki\_ossl\_get\_cert\_summary, pki\_ossl.c:119  
PKI[9]: -----Certificate-----:  
Serial Number: 1 (0x1)  
Issuer: O=cisco, OU=TAC, CN=calo\_root  
Subject: O=cisco, OU=TAC, CN=calo\_root

PKI[14]: pki\_ossl\_get\_cert\_summary, pki\_ossl.c:119  
PKI[9]: -----Certificate-----:  
Serial Number: 2 (0x2)  
Issuer: O=cisco, OU=TAC, CN=calo\_root  
Subject: CN=desktop.example.com/unstructuredName=CA-router

PKI[9]: End sorted cert chain  
PKI[13]: pki\_ossl\_get\_store, pki\_ossl\_certstore.c:61  
PKI[12]: pki\_ossl\_rebuild\_ca\_store, pki\_ossl\_certstore.c:194  
PKI[13]: crypto\_pki\_get\_ossl\_env, pki\_ossl.c:42  
PKI[13]: crypto\_pki\_get\_ossl\_env, pki\_ossl.c:42  
PKI[14]: pki\_ossl\_get\_cert\_summary, pki\_ossl.c:119  
PKI[9]: Cert to verify  
PKI[9]: -----Certificate-----:  
Serial Number: 2 (0x2)  
Issuer: O=cisco, OU=TAC, CN=calo\_root  
Subject: CN=desktop.example.com/unstructuredName=CA-router

PKI[12]: pki\_verify\_cb, pki\_ossl\_validate.c:358

PKI[6]: val status=0: cert subject: /CN=desktop.example.com/unstructuredName=CA-router. ctx->error: (23)

PKI[14]: is\_crl\_error, pki\_ossl\_validate.c:278

PKI[14]: is\_crl\_error, pki\_ossl\_validate.c:278

PKI[4]: Certificate verification error: certificate revoked

PKI[14]: map\_ossl\_error, pki\_ossl\_validate.c:62

PKI[7]: session 0x1acca1bd, Validation with CRL checking completed, status 15

PKI[5]: session 0x1acca1bd, Error in revocation check or revoked certs found

PKI[12]: pki\_ossl\_do\_callback, pki\_ossl\_validate.c:164

PKI[13]: CERT\_Close, vpn3k\_cert\_api.c:291

PKI[8]: Close session 0x1acca1bd asynchronously

PKI[13]: CERT\_API\_req\_enqueue, vpn3k\_cert\_api.c:2913

PKI[9]: Async unlocked for session 0x1acca1bd

PKI[12]: CERT\_API\_Q\_Process, vpn3k\_cert\_api.c:2811

PKI[12]: CERT\_API\_process\_req\_msg, vpn3k\_cert\_api.c:2746

PKI[8]: process msg cmd=1, session=0x1acca1bd

PKI[9]: Async locked for session 0x1acca1bd

PKI[9]: Async unlocked for session 0x1acca1bd

PKI[13]: pki\_ossl\_free\_valctx, pki\_ossl\_validate.c:251

PKI[13]: free\_fsm\_data, pki\_ossl\_revocation.c:225

PKI[13]: oosp\_free\_fsmdata, pki\_ossl\_oosp.c:1462

PKI[13]: free\_fsm\_data, pki\_ossl\_revocation.c:225

PKI[13]: oosp\_free\_fsmdata, pki\_ossl\_oosp.c:1462

PKI[9]: CERT API thread sleeps!

다음 FTD 캡처는 목록에 저장된 폐기된 인증서가 있는 경우 CRL을 검색하기 위해 FTD와 CDP 간의 HTTP 트랜잭션을 표시합니다.

No.	Time	Source	Destination	Protocol	Length	Info
4	0.000152	192.0.2.1	192.0.2.10	HTTP	140	GET /cgi-bin/pkiclient.exe?operation
5	0.000733	192.0.2.10	192.0.2.1	TCP	66	80 → 57791 [ACK] Seq=1 Ack=75 Win=2
6	0.004821	192.0.2.10	192.0.2.1	TCP	751	80 → 57791 [PSH, ACK] Seq=1 Ack=75
7	0.000107	192.0.2.1	192.0.2.10	TCP	66	57791 → 80 [ACK] Seq=75 Ack=686 Win
8	0.000015	192.0.2.10	192.0.2.1	PKIX-CRL	66	Certificate Revocation List
9	0.000092	192.0.2.1	192.0.2.10	TCP	66	57791 → 80 [ACK] Seq=75 Ack=687 Win
10	0.000046	192.0.2.1	192.0.2.10	TCP	66	57791 → 80 [FIN, PSH, ACK] Seq=75 A
11	0.000625	192.0.2.10	192.0.2.1	TCP	66	80 → 57791 [ACK] Seq=687 Ack=76 Win

```
X-XSS-Protection: 1; mode=block\r\n
X-Content-Type-Options: nosniff\r\n
X-Frame-Options: SAMEORIGIN\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.005676000 seconds]
[Request in frame: 4]
[Request URI: http://192.0.2.10/cgi-bin/pkiclient.exe?operation=GetCRL]
File Data: 272 bytes
```

```

Certificate Revocation List
  signedCertificateList
    > signature (sha1WithRSAEncryption)
    > issuer: rdnSequence (0)
    > thisUpdate: utcTime (0)
    > nextUpdate: utcTime (0)
    > revokedCertificates: 1 item
      revokedCertificates item
        userCertificate: 0x02
        > revocationDate: utcTime (0)
    > algorithmIdentifier (sha1WithRSAEncryption)
    Padding: 0
    encrypted: 7b049a1dc049f4b08c16eb35c5de48f01324a42763bf4ea72404d3c43a0cf72a20dc2fff...

```

## 문제 해결

인증서와 관련된 추가 문제를 식별하기 위해 다음 명령을 사용할 수 있습니다.

- FTD에서:

```
debug crypto ca 14
```

- CA 라우터에서:

```
debug crypto pki API
debug crypto pki callbacks
debug crypto pki messages
debug crypto pki validation
debug crypto pki error
debug crypto pki server
debug crypto pki transactions
```



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.