

對AnyConnect基於證書的身份驗證的CRL進行故障排除

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[拓撲](#)

[重要配置](#)

[CA路由器](#)

[VPN網關配置](#)

[Windows裝置](#)

[驗證](#)

[案例 1.憑證對驗證有效](#)

[案例 2.證書被吊銷，身份驗證失敗](#)

[疑難排解](#)

簡介

本文檔介紹如何對為AnyConnect基於證書的身份驗證配置的證書撤銷清單(CRL)進行故障排除。

必要條件

需求

思科建議您瞭解以下主題：

- 憑證授權單位(CA)
- 公開金鑰基礎架構 (PKI)
- FTD上的RA VPN
- 帶AnyConnect客戶端的Windows 10

採用元件

本檔案中的資訊是根據以下軟體版本：

- CSR1000V - Cisco IOS® XE，版本16.12.03 -作為Cisco IOS XE CA伺服器
- NGFWv - 7.1.0版-作為VPN網關
- AnyConnect安全移動客戶端4.10.07073版-作為VPN客戶端

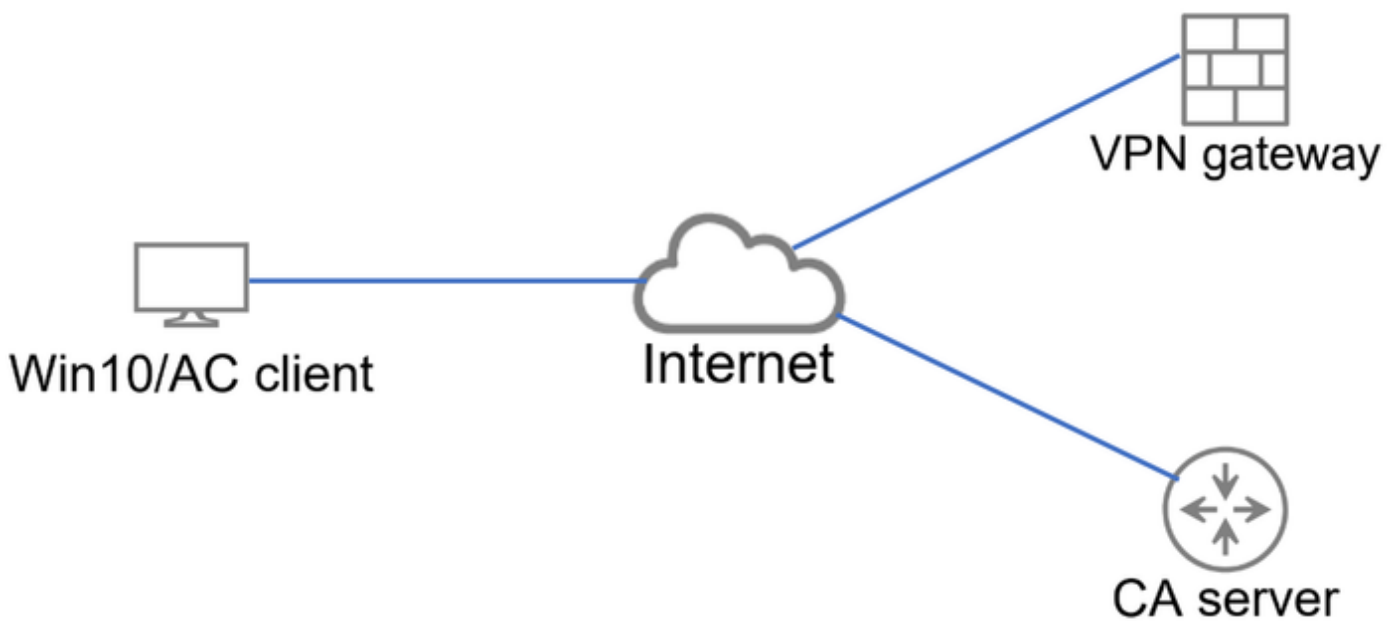
- Windows 10作為本地電腦

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

CRL使裝置能夠確定證書是否在證書有效期到期之前被吊銷。CRL包含證書的序列號和撤銷日期。安全閘道(例如Firepower執行緒防禦(FTD)系統或其他終端裝置)使用此功能，藉由驗證憑證狀態來加強憑證驗證。

拓撲



提供與VPN網關和CA伺服器連線的基本拓撲。

重要配置

為了使用CRL完成基於證書的身份驗證，在涉及的每台裝置中均使用了顯示的配置。

CA路由器

伺服器證書頒發機構負責向使用者頒發身份證書，以便根據VPN網關提供身份驗證。此外，路由器會儲存CRL資料庫檔案並充當CRL分發點(CDP)。

CDP是VPN網關和其他終端使用者檢索CRL資訊的位置。此資訊會快取至本機，且僅在一段特定時間內有效；當此時間到期時，會下載新的CRL。

註：CRL資料庫和裝置可以訪問CRL的位置可以在同一台裝置上。但是，出於安全原因，建議終端裝置訪問的CRL儲存在CRL資料庫以外的其他裝置中。在本例中，CA路由器儲存CRL資料庫並充當VPN網關的CDP。

```
<#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
rsakeypair TP-self-signed-1507329386

crypto pki trustpoint CAS
revocation-check crl
rsakeypair CAS

interface GigabitEthernet2
ip address 192.0.2.10 255.255.255.0
negotiation auto

ip http server

ntp master 1
```

VPN網關配置

設定FTD是為了使用憑證作為驗證方法（僅限憑證）向終端使用者提供遠端存取VPN。從使用者接收身分辨識憑證後，FTD會驗證憑證是否由已知憑證授權單位(CA)核發，並透過從憑證中定義的CDP取得CRL來確認其有效性。

```
<#root>

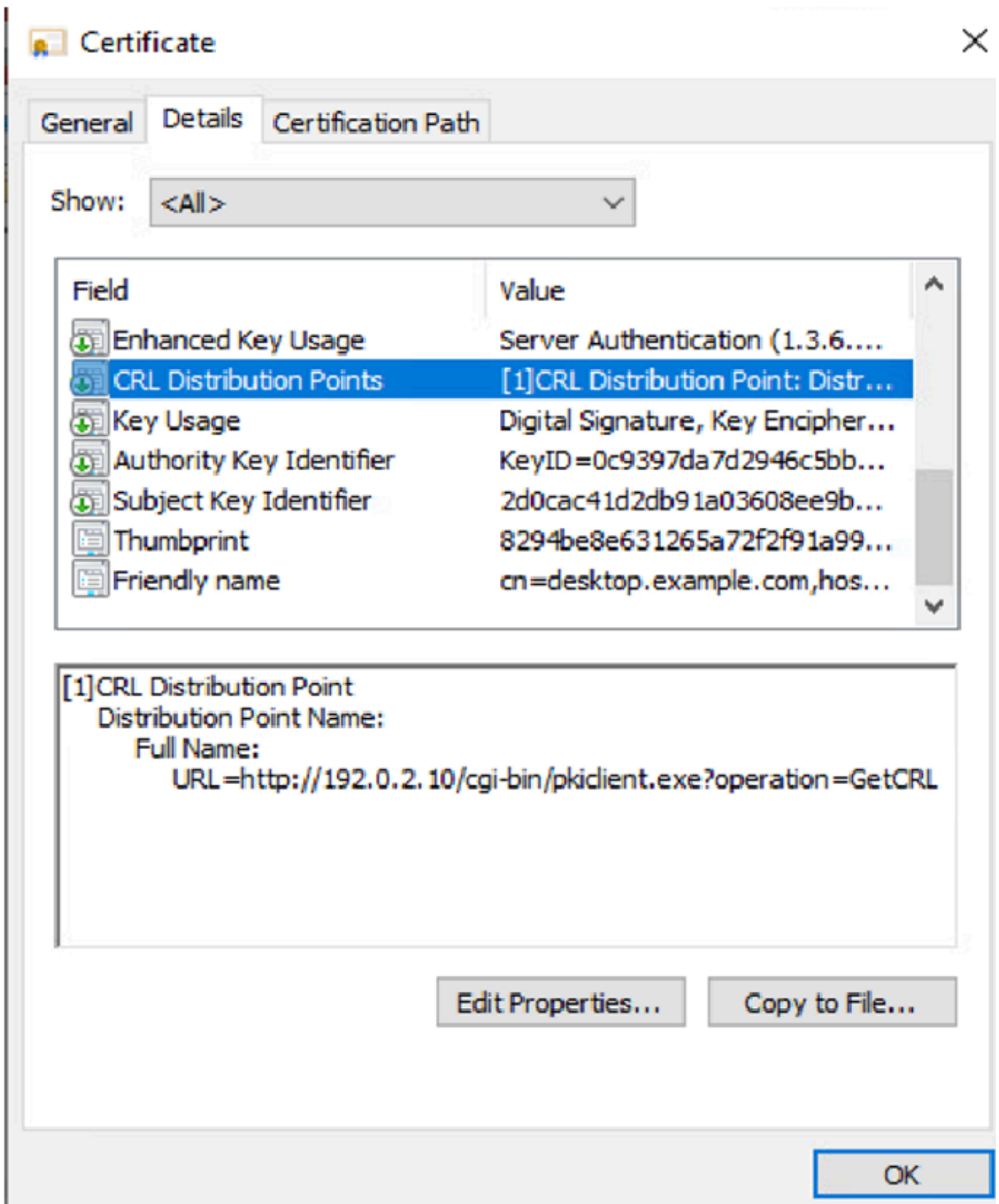
tunnel-group local type remote-access
tunnel-group local general-attributes
address-pool AC_pool
default-group-policy local_gp
username-from-certificate use-entire-name
tunnel-group local_test webvpn-attributes

authentication certificate

group-alias test enable
```

Windows裝置

身份證書由CA伺服器頒發並安裝到Windows裝置中。



驗證

接下來的調試和捕獲顯示了使用有效證書的使用者（工作場景）和使用已撤銷證書的使用者（非工作場景）之間的差異。

案例 1.憑證對驗證有效

當使用者開始連線嘗試時，會向FTD提供其辨識憑證，VPN閘道會驗證簽發者是否為已知授權單位，並開始透過HTTP/GET要求從辨識憑證中定義的CDP要求CRL。CA伺服器會使用CRL回覆，而FTD會檢查憑證的「序號」是否已列出。由於CRL是空的（沒有撤銷的憑證），因此FTD接受憑證為有效並允許使用者進行驗證。

```
<#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 ommitted]
```

```
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_oss1_check_cache, pki_oss1_cr1_cache.c:1269
```

PKI[7]: Starting OSSL CRL cache check.
PKI[12]: pki_oss1_crypto_build_crldp_list, pki_oss1_crl_cache.c:326
PKI[12]: pki_get_der_cdp_ext, crypto_pki.c:1528
PKI[14]: url_type_allowed, pki_oss1_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_oss1_SelectCRLByIssuerTimeDER, pki_oss1_crl_cache.c:1219
PKI[14]: pki_oss1_get_name_string, pki_oss1.c:315
PKI[9]: Select DER crl(O=cisco, OU=TAC, CN=calo_root)
PKI[12]: pki_oss1_get_crl_internal, pki_oss1_crl_cache.c:506
PKI[7]: CRL not cached. Initiating CRL download for cert idx 0.
PKI[12]: do_get_crl, pki_oss1_revocation.c:85
PKI[9]: starting CRL FSM #0
PKI[11]: drive_fsm, pki_oss1_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_oss1_policy_transition.c:230
PKI[11]: polinfo->name: CRL-AC
PKI[11]: tp label: Trustpool
PKI[13]: label: CRL-AC
PKI[12]: pki_oss1_crypto_build_crldp_list, pki_oss1_crl_cache.c:326
PKI[12]: pki_get_der_cdp_ext, crypto_pki.c:1528
PKI[14]: url_type_allowed, pki_oss1_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]: crldp_cdp_blacklisted, pki_oss1_crl.c:1374
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[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_oss1_crl.c:1184
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[8]: session 0x06c8d45f adding pending CRL entry for cert 0
PKI[12]: crldp_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_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_QUEUED

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 microsecs

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
```

下一個FTD擷取會顯示FTD和CDP (此案例為CA伺服器) 之間的HTTP交易, 以便擷取CRL。

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=26
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=14
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=26988
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=3224
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 TSv

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=2698
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=322414047
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
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=269888856

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

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: rdnsSequence (0)
 - thisUpdate: utcTime (0)
 - nextUpdate: utcTime (0)
- algorithmIdentifier (sha1withRSAEncryption)
 - Algorithm Id: 1.2.840.113549.1.1.5 (sha1withRSAEncryption)
 - Padding: 0
 - encrypted: 0a9b3a3e44674360c548fb7c6f058e7ba9687c99e16311dd2bfc8a31134e59b589cbe423...

案例 2. 證書被吊銷，身份驗證失敗

身份證書在CA伺服器中被吊銷，並在CRL資料庫檔案中註冊。但是，更新的CRL在目前CRL到期（設定為兩小時有效）之前無法供FTD使用。

<#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

在確認CRL過期後嘗試建立新連線時，證書檢查與前一個場景基本相同。FTD確認快取中沒有CRL後，會要求新的CRL。收到新CRL後，FTD會檢查身分憑證的序號是否屬於清單的一部分。序號會標籤為已撤銷，且FTD會繼續拒絕使用者的存取。

<#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_ssl_revocation_check, pki_ssl_validate.c:931
PKI[7]: Starting revocation check for session 0x0dc288f9
PKI[12]: pki_init_revocation, pki_ssl_revocation.c:162
PKI[12]: pki_ssl_eval_revocation, pki_ssl_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_cr_cached, pki_ossl_cr_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_cr_cache.c:1269
PKI[7]: Starting OSSL CRL cache check.
PKI[12]: pki_ossl_crypto_build_crldp_list, pki_ossl_cr_cache.c:326
PKI[12]: pki_get_der_cdp_ext, crypto_pki.c:1528
PKI[14]: url_type_allowed, pki_ossl_cr_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_cr_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_cr_internal, pki_ossl_cr_cache.c:506

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

PKI[12]: do_get_cr, 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_cr_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_crldp_list, pki_ossl_cr_cache.c:326
PKI[12]: pki_get_der_cdp_ext, crypto_pki.c:1528
PKI[14]: url_type_allowed, pki_ossl_cr_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]: crld_cdp_blacklisted, pki_ossl_cr.c:1374
PKI[12]: crl_find_pending_crl, pki_ossl_cr.c:1155
PKI[13]: get_pending_crl_list, pki_ossl_cr.c:1101
PKI[13]: crypto_pki_get_ossl_env, pki_ossl.c:42
PKI[14]: cmp_cdp_info, pki_ossl_cr.c:1121
PKI[14]: cmp_cdp_info, pki_ossl_cr.c:1121
PKI[14]: cmp_cdp_info, pki_ossl_cr.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_cr.c:1184
PKI[12]: crl_find_pending_crl, pki_ossl_cr.c:1155
PKI[13]: get_pending_crl_list, pki_ossl_cr.c:1101
PKI[13]: crypto_pki_get_ossl_env, pki_ossl.c:42
PKI[14]: cmp_cdp_info, pki_ossl_cr.c:1121
PKI[14]: cmp_cdp_info, pki_ossl_cr.c:1121
PKI[14]: cmp_cdp_info, pki_ossl_cr.c:1121
PKI[8]: session 0x0dc288f9 adding pending CRL entry for cert 0

PKI[12]: crl_dp_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]: [16] IOCB allocated
PKI[7]: PKI CRL I/O request queue result: IO_STATUS_QUEUEED
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_ossl_revocation.c:421

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

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), data[
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]: crl_find_pending_crl, pki_ossl_crl.c:1155
PKI[13]: get_pending_crl_list, pki_ossl_crl.c:1101

PKI[7]: session 0x0dc288f9, Validation with CRL checking completed, status 15
PKI[5]: session 0x0dc288f9, Error in revocation check or revoked certs found
PKI[12]: pki_ssl_do_callback, pki_ssl_validate.c:164
PKI[13]: CERT_Close, vpn3k_cert_api.c:291
PKI[8]: Close session 0x0dc288f9 asynchronously
PKI[13]: CERT_API_req_enqueue, vpn3k_cert_api.c:2913
PKI[9]: Async unlocked for session 0x0dc288f9
PKI[8]: No IOCB found for SOCKET_CLOSE message, handle 0x1a6b367e
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=0x0dc288f9
PKI[9]: Async locked for session 0x0dc288f9
PKI[9]: Async unlocked for session 0x0dc288f9
PKI[13]: pki_ssl_free_valctx, pki_ssl_validate.c:251
PKI[13]: free_fsm_data, pki_ssl_revocation.c:225
PKI[13]: oosp_free_fsmdata, pki_ssl_oosp.c:1462
PKI[13]: free_fsm_data, pki_ssl_revocation.c:225
PKI[13]: oosp_free_fsmdata, pki_ssl_oosp.c:1462
PKI[9]: CERT API thread sleeps!

[..output omitted]

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_ssl_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_ssl_validate.c:358
PKI[8]: val status=1: cert subject: /CN=desktop.example.com/unstructuredName=CA-router. ctx->error: (0)
PKI[8]: pki_ssl_find_valid_chain took 233 microsecs
PKI[6]: Verified chain:
PKI[14]: pki_ssl_get_cert_summary, pki_ssl.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_ssl_get_cert_summary, pki_ssl.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_ssl_revocation_check, pki_ssl_validate.c:931
PKI[7]: Starting revocation check for session 0x1acca1bd
PKI[12]: pki_init_revocation, pki_ssl_revocation.c:162
PKI[12]: pki_ssl_eval_revocation, pki_ssl_validate.c:699
PKI[7]: Evaluating session revocation status, 1 certs to check
PKI[8]: session 0x1acca1bd, cert 0 has rev_status 0, using methods 1/3/0 at index 0
PKI[12]: cert_revoc_exempt, pki_ssl_revocation.c:250
PKI[13]: get_tp_from_policy, pki_ssl_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_oss1_crl_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_oss1_check_cache, pki_oss1_crl_cache.c:1269
PKI[7]: Starting OSSL CRL cache check.
PKI[12]: pki_oss1_crypto_build_crl_dp_list, pki_oss1_crl_cache.c:326
PKI[12]: pki_get_der_cdp_ext, crypto_pki.c:1528
PKI[14]: url_type_allowed, pki_oss1_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_oss1_SelectCRLByIssuerTimeDER, pki_oss1_crl_cache.c:1219
PKI[14]: pki_oss1_get_name_string, pki_oss1.c:315
PKI[9]: Select DER crl(O=cisco, OU=TAC, CN=calo_root)
PKI[12]: pki_oss1_get_crl_internal, pki_oss1_crl_cache.c:506
PKI[13]: is_crl_dst, pki_oss1_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_oss1_rebuild_ca_store, pki_oss1_certstore.c:194
PKI[13]: crypto_pki_get_oss1_env, pki_oss1.c:42

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

PKI[12]: pki_oss1_find_valid_chain, pki_oss1_validate.c:472
PKI[9]: Begin sorted cert chain
PKI[14]: pki_oss1_get_cert_summary, pki_oss1.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_oss1_get_cert_summary, pki_oss1.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_oss1_get_store, pki_oss1_certstore.c:61
PKI[12]: pki_oss1_rebuild_ca_store, pki_oss1_certstore.c:194
PKI[13]: crypto_pki_get_oss1_env, pki_oss1.c:42
PKI[13]: crypto_pki_get_oss1_env, pki_oss1.c:42
PKI[14]: pki_oss1_get_cert_summary, pki_oss1.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_oss1_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_oss1_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_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!

下一個FTD擷取顯示FTD和CDP之間的HTTP交易，以便在清單中儲存已撤銷憑證的情況下擷取CRL。

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...

```

疑難排解

以下命令可用於辨識與憑證相關的進一步問題：

- 在FTD上：

```
debug crypto ca 14
```

- 在CA路由器上：

```

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

```


關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。