VPN ad accesso remoto ASA con verifica OCSP in Microsoft Windows 2012 e OpenSSL

Sommario

Introduzione

In questo documento viene descritto come utilizzare la convalida OCSP (Online Certificate Status Protocol) su una appliance Cisco Adaptive Security (ASA) per i certificati presentati dagli utenti VPN. Vengono presentate configurazioni di esempio per due server OCSP (Microsoft Windows Certificate Authority [CA] e OpenSSL). La sezione Verifica descrive in dettaglio i flussi a livello di

pacchetto, mentre la sezione Risoluzione dei problemi si concentra sugli errori e sui problemi tipici.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione dell'interfaccia della riga di comando (CLI) di Cisco Adaptive Security Appliance e configurazione della VPN SSL (Secure Sockets Layer)
- Certificati X.509
- Server di Microsoft Windows
- Linux/OpenSSL

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Software Cisco Adaptive Security Appliance, versione 8.4 e successive
- Microsoft Windows 7 con Cisco AnyConnect Secure Mobility Client, versione 3.1
- Microsoft Server 2012 R2
- Linux con OpenSSL 1.0.0j o versioni successive

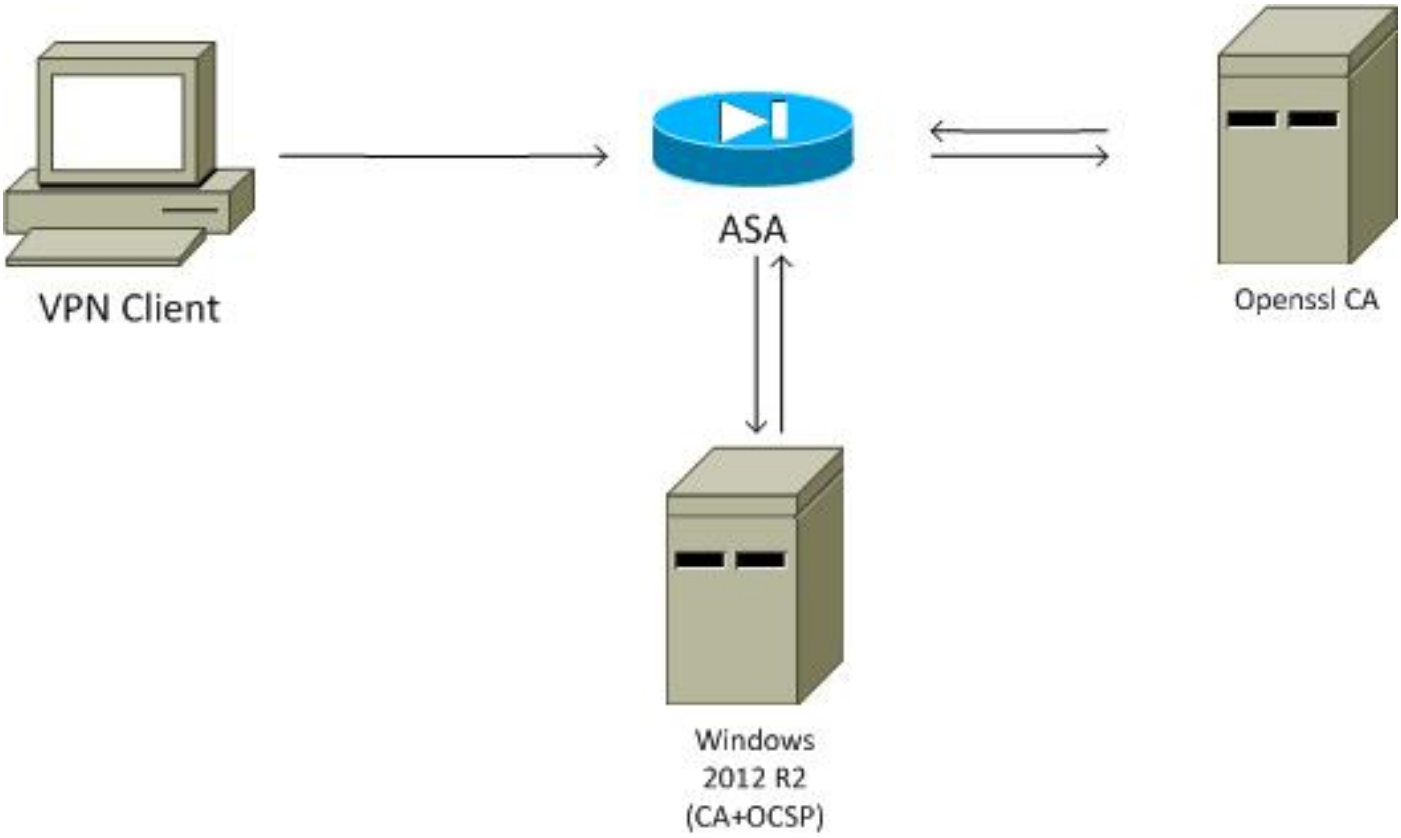
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

> **Nota**: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Il client utilizza una VPN ad accesso remoto. L'accesso può essere Cisco VPN Client (IPSec), Cisco AnyConnect Secure Mobility (SSL/Internet Key Exchange versione 2 [IKEv2]) o WebVPN (portale). Per effettuare l'accesso, il client fornisce il certificato corretto, nonché il nome utente e la password configurati localmente sull'appliance ASA. Il certificato client viene convalidato tramite il server OCSP.



Accesso remoto ASA con OCSP

L'appliance ASA è configurata per l'accesso SSL. Il client sta utilizzando AnyConnect per eseguire il login. L'appliance ASA utilizza SCEP (Simple Certificate Enrollment Protocol) per richiedere il certificato:

```
crypto ca trustpoint WIN2012
 revocation-check ocsp
 enrollment url http://10.147.25.80:80/certsrv/mscep/mscep.dll

crypto ca certificate map MAP 10
 subject-name co administrator
```

Viene creata una mappa dei certificati per identificare tutti gli utenti il cui nome soggetto contiene la parola administrator (senza distinzione tra maiuscole e minuscole). Tali utenti sono associati a un gruppo di tunnel denominato RA:

```
webvpn
 enable outside
 anyconnect image disk0:/anyconnect-win-3.1.02040-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable
 certificate-group-map MAP 10 RA
```

Per la configurazione della VPN è necessaria l'autorizzazione, ovvero un certificato convalidato. Richiede inoltre le credenziali corrette per il nome utente definito localmente (autenticazione aaa):

```
username cisco password xxxxxxx
ip local pool POOL 192.168.11.100-192.168.11.105 mask 255.255.255.0

aaa authentication LOCAL
```

```
aaa authorization LOCAL

group-policy MY internal
group-policy MY attributes
 vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless

tunnel-group RA type remote-access
tunnel-group RA general-attributes
 address-pool POOL
 default-group-policy MY
 authorization-required
tunnel-group RA webvpn-attributes
 authentication aaa certificate
 group-alias RA enable
```

CA di Microsoft Windows 2012

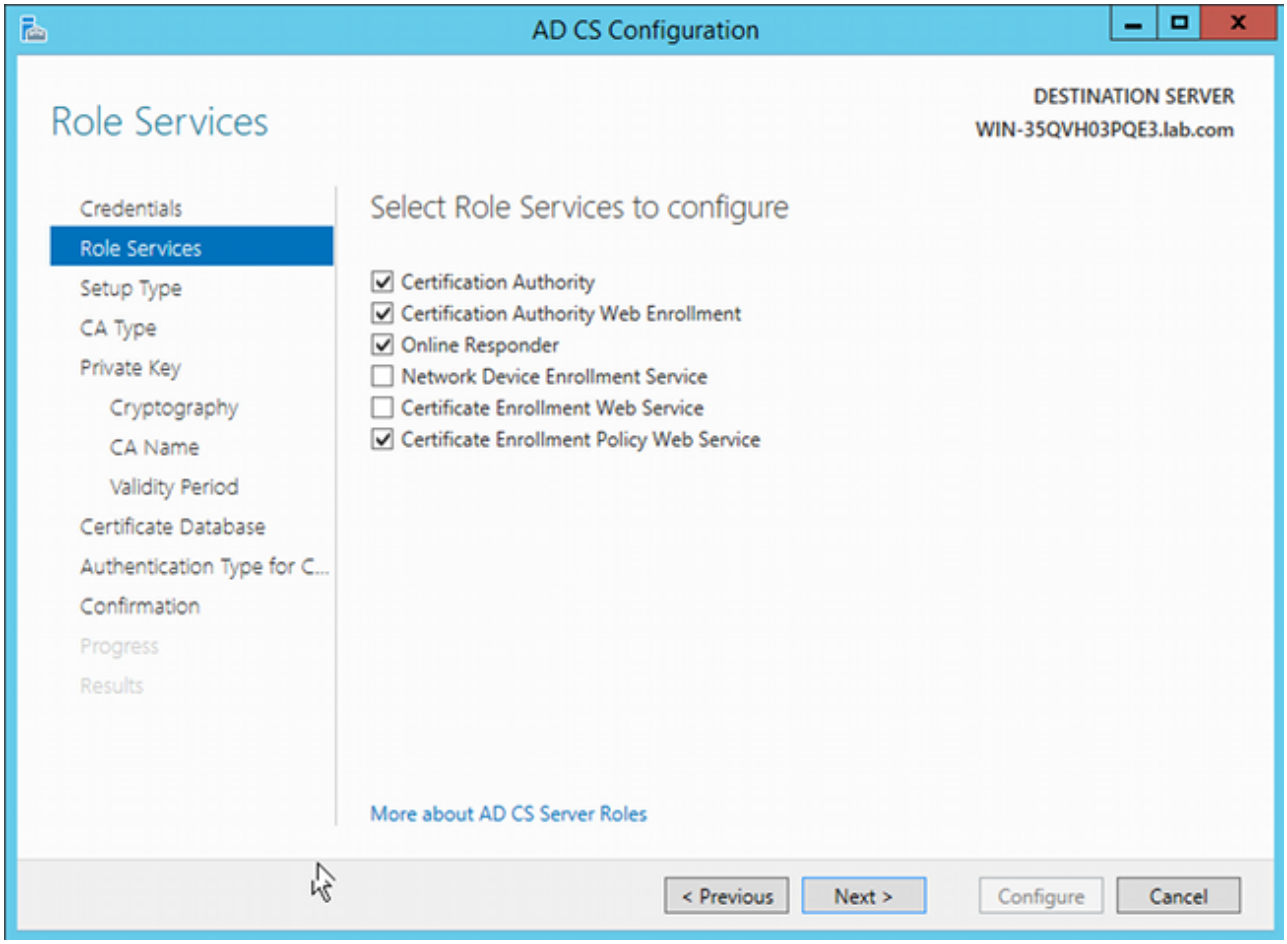
> **Nota**: vedere la guida alla configurazione di Cisco ASA serie 5500 dall'interfaccia CLI 8.4 e 8.6: configurazione di un server esterno per l'autorizzazione utente di un'appliance di sicurezza per i dettagli sulla configurazione dell'ASA dalla CLI.

Installazione servizi

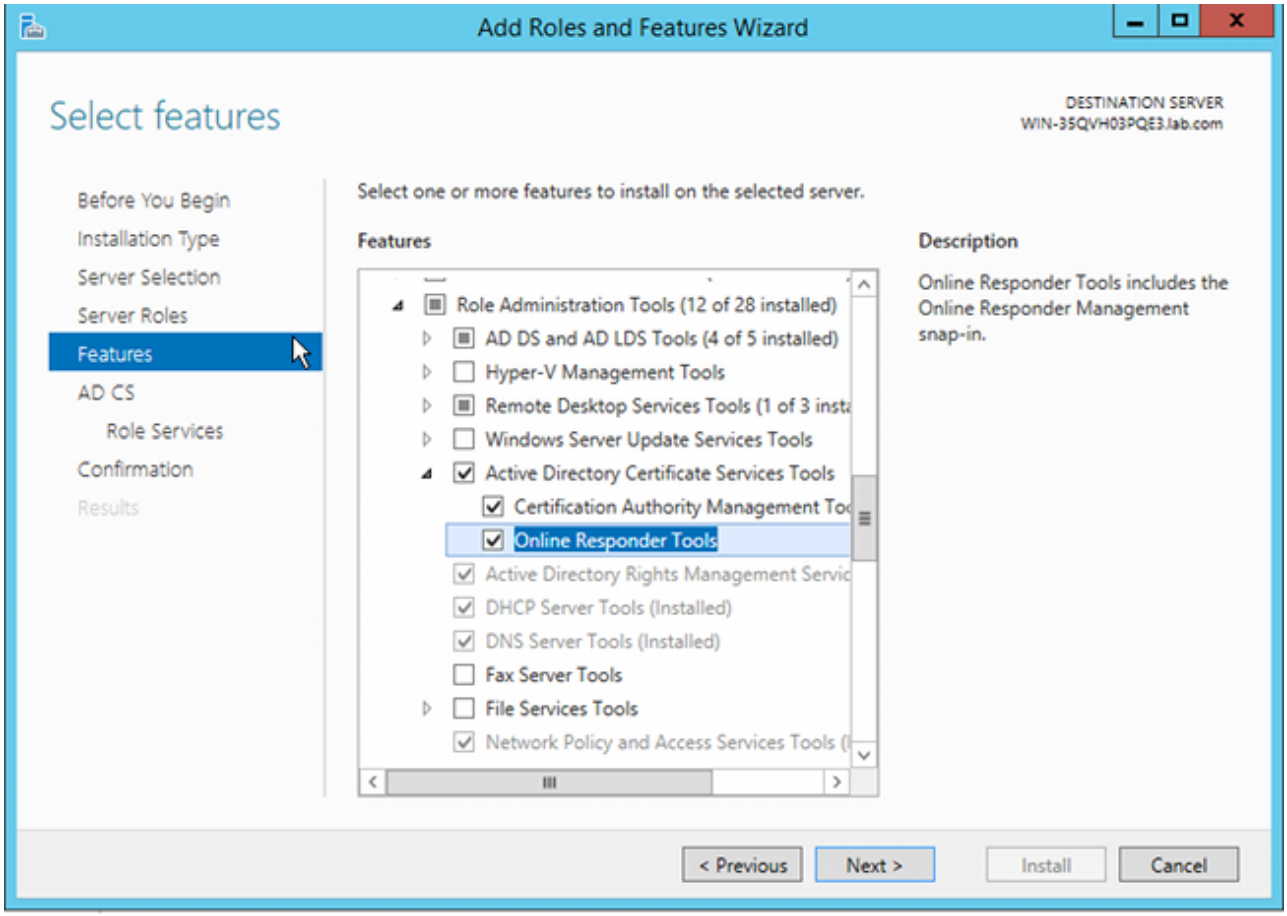
In questa procedura viene descritto come configurare i servizi ruolo per il server Microsoft:

1. Passare a **Server Manager > Gestisci > Aggiungi ruoli e funzionalità**. Per il server Microsoft sono necessari i servizi ruolo seguenti:

   Autorità di certificazioneRegistrazione Web Autorità di certificazione, utilizzata dal clientRisponditore in linea, necessario per OCSPServizio Registrazione dispositivi di rete, che contiene l'applicazione SCEP utilizzata dall'appliance ASA Se necessario, è possibile aggiungere un servizio Web con criteri.



2.
3.
4. Quando si aggiungono funzionalità, assicurarsi di includere gli strumenti Risponditore in linea, in quanto include uno snap-in OCSP utilizzato in seguito:



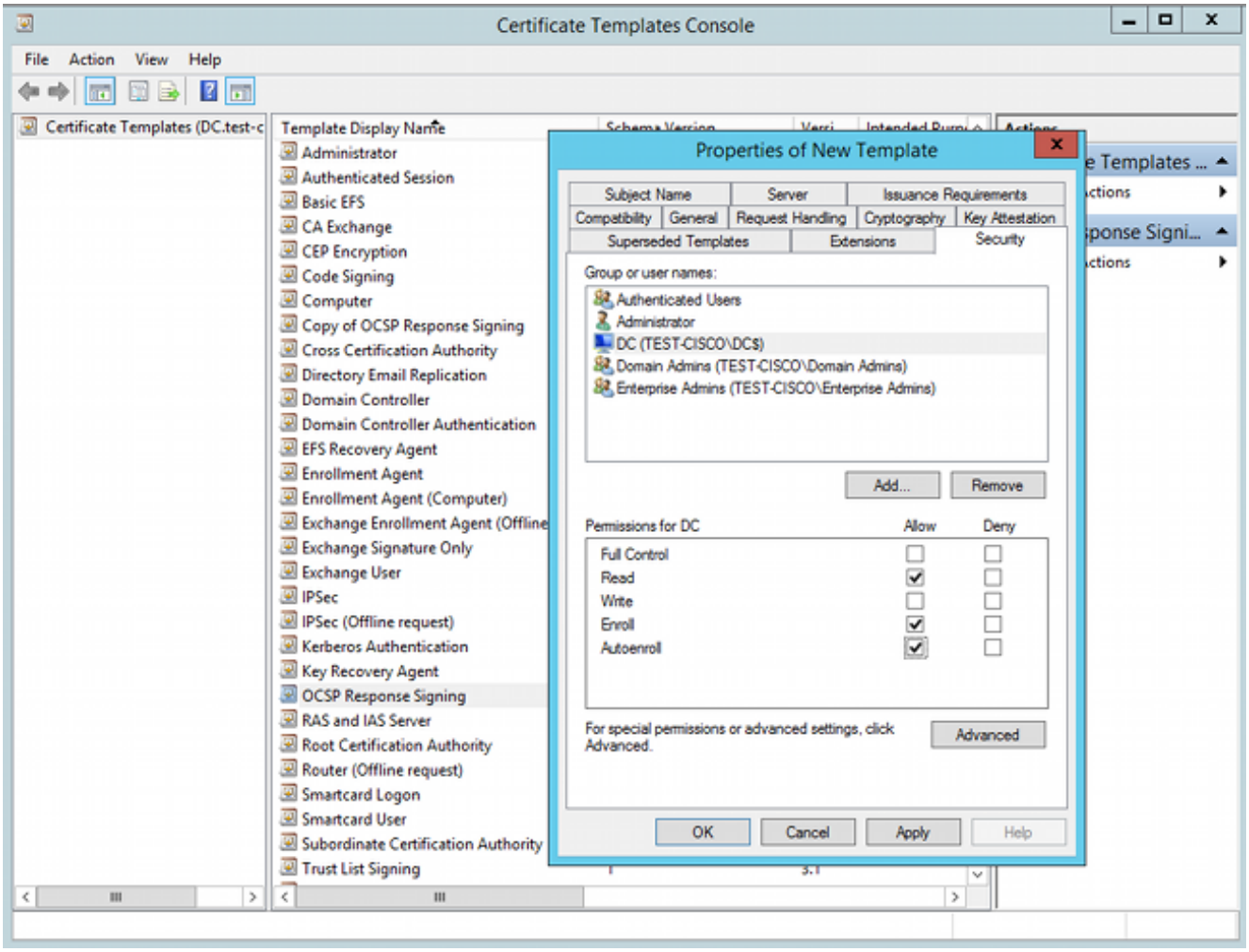
Configurazione CA per modello OCSP

Il servizio OCSP utilizza un certificato per firmare la risposta OCSP. È necessario generare un certificato speciale sul server Microsoft che includa:

- Utilizzo chiave esteso = Firma OCSP
- Nessun controllo di revoca OCSP

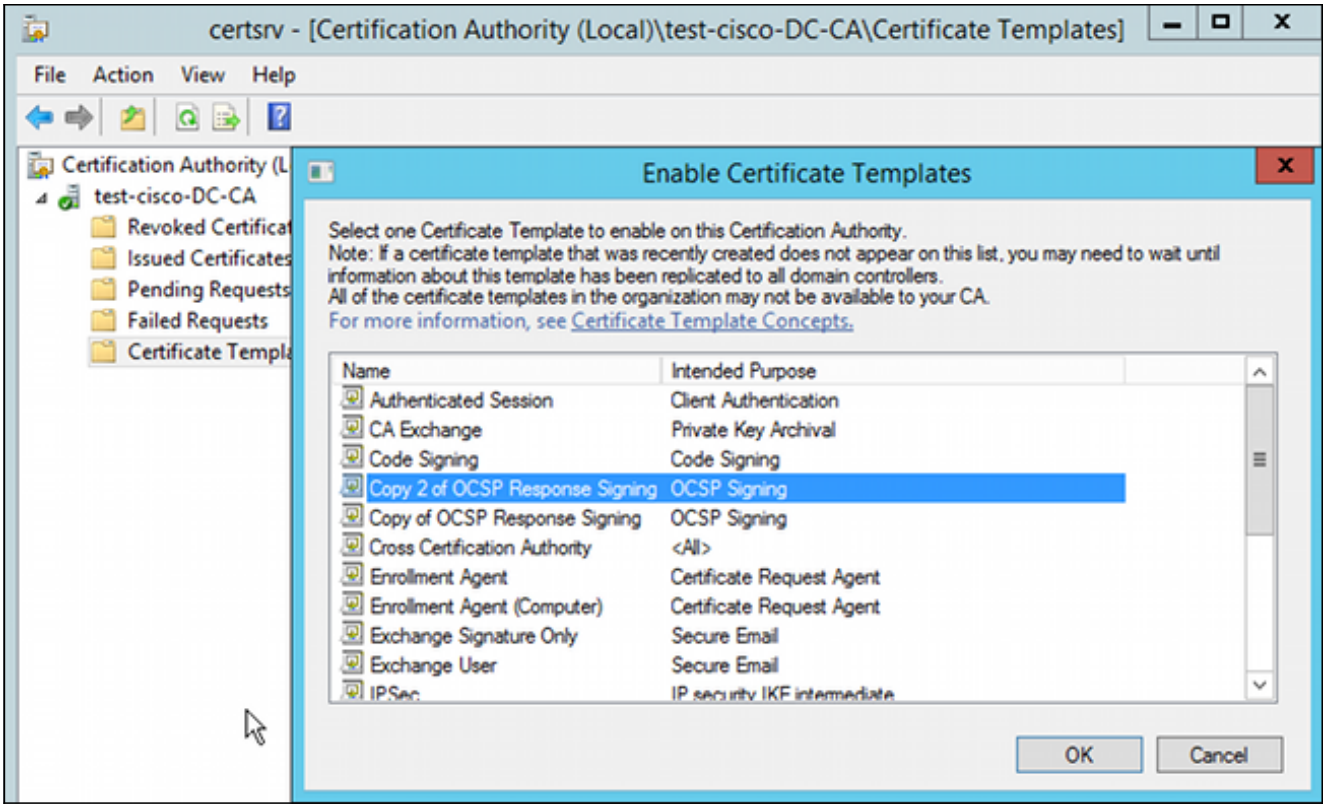
Questo certificato è necessario per evitare loop di convalida OCSP. L'appliance ASA non utilizza il servizio OCSP per provare a controllare il certificato presentato dal servizio OCSP.

1. Aggiungere un modello per il certificato nella CA. Passare a **CA > Modello di certificato > Gestisci**, selezionare **Firma risposta OCSP** e duplicare il modello. Visualizzare le proprietà del nuovo modello creato e fare clic sulla scheda **Protezione**. Le autorizzazioni descrivono quale entità è autorizzata a richiedere un certificato che utilizza tale modello, pertanto sono necessarie autorizzazioni corrette. In questo esempio, l'entità è il servizio OCSP in esecuzione sullo stesso host (TEST-CISCO\DC) e il servizio OCSP deve disporre dei privilegi di registrazione automatica:



Tutte le altre impostazioni del modello possono essere impostate sui valori predefiniti.

2. Attivate il modello. Passare a **CA > Modello di certificato > Nuovo > Modello di certificato da emettere** e selezionare il modello duplicato:

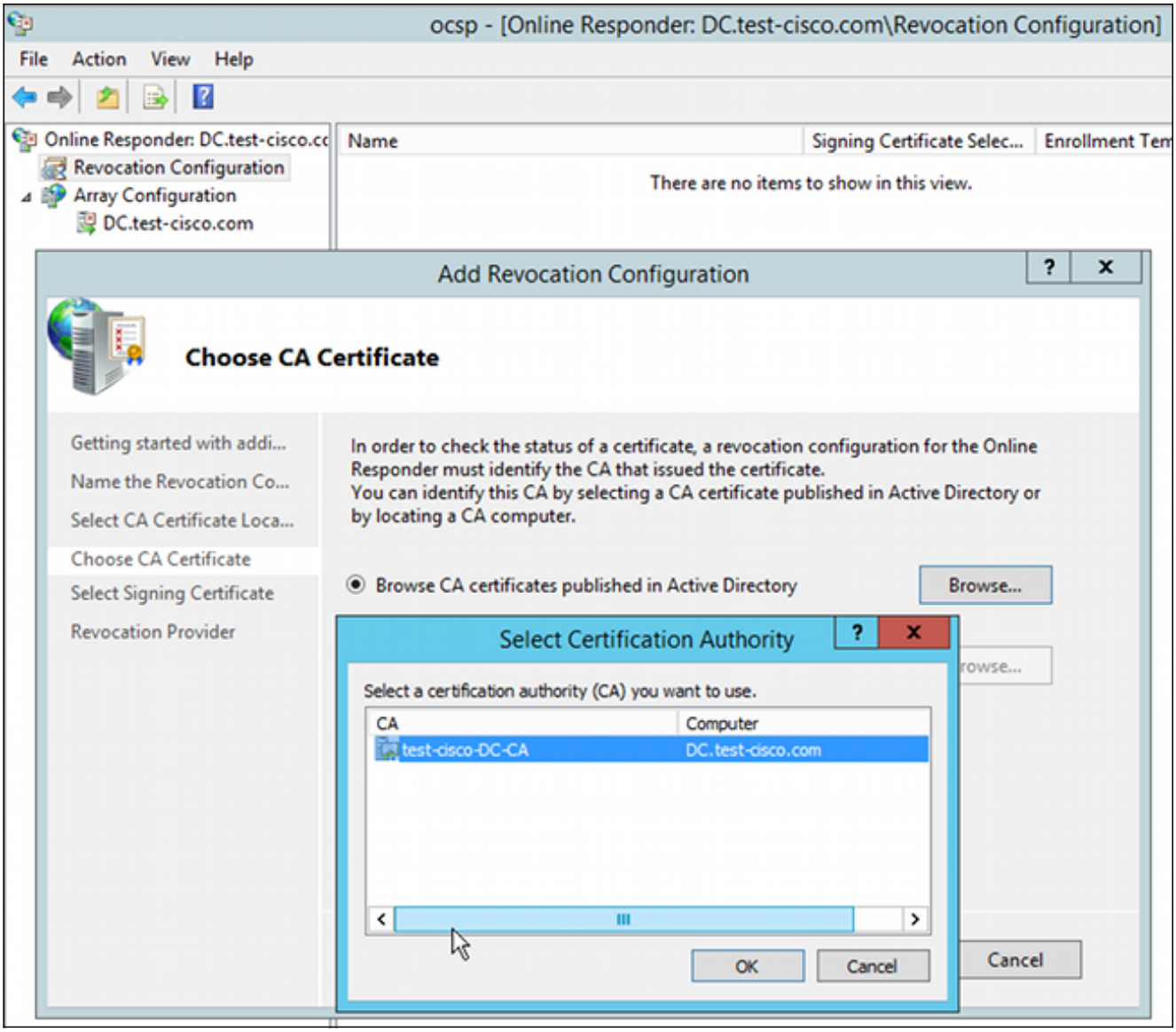


Certificato di servizio OCSP

In questa procedura viene descritto come utilizzare Gestione configurazione in linea per configurare OCSP:

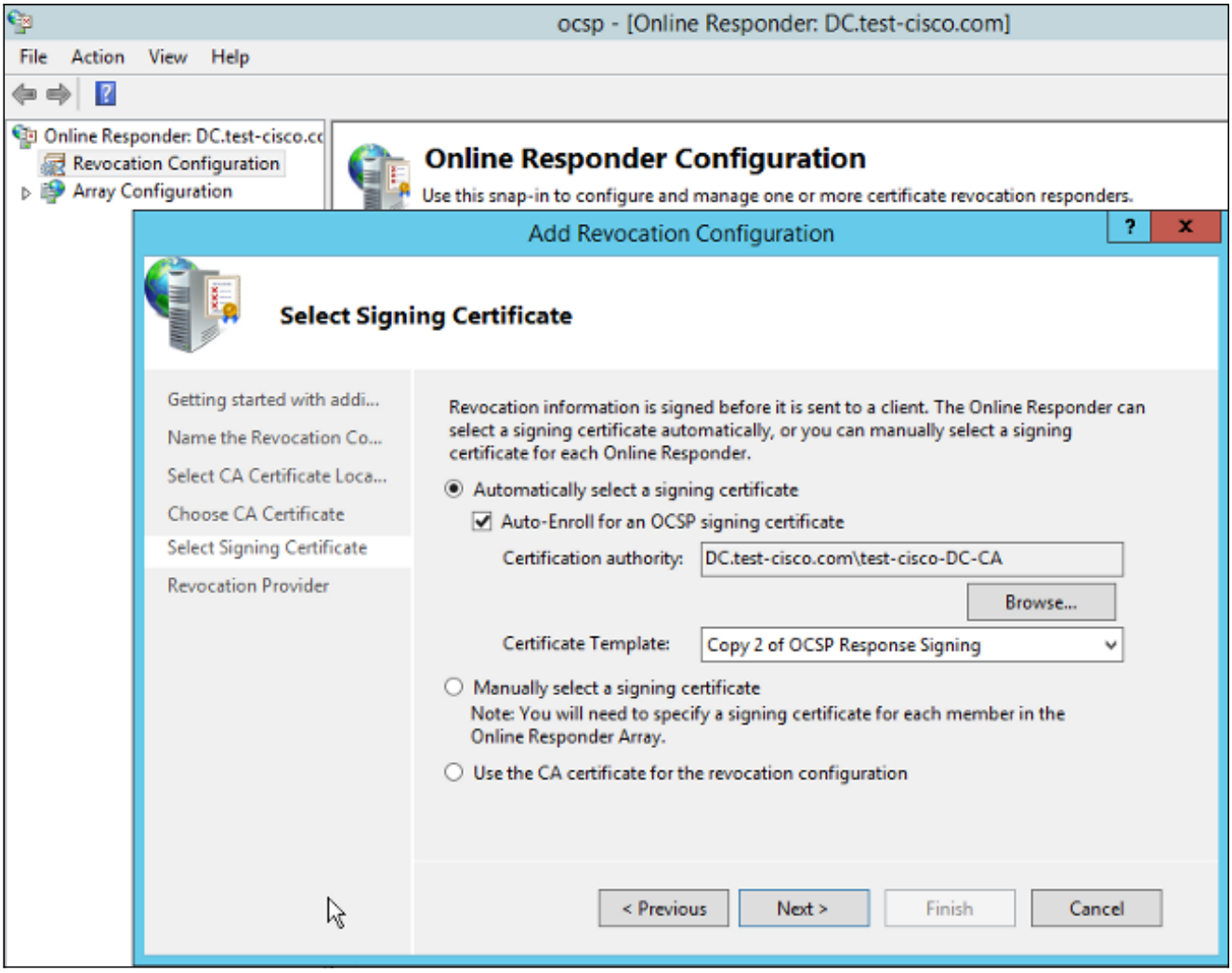
1. Passare a **Server Manager > Strumenti**.

2. Per aggiungere una nuova configurazione, selezionare **Configurazione di revoca > Aggiungi configurazione di revoca**:

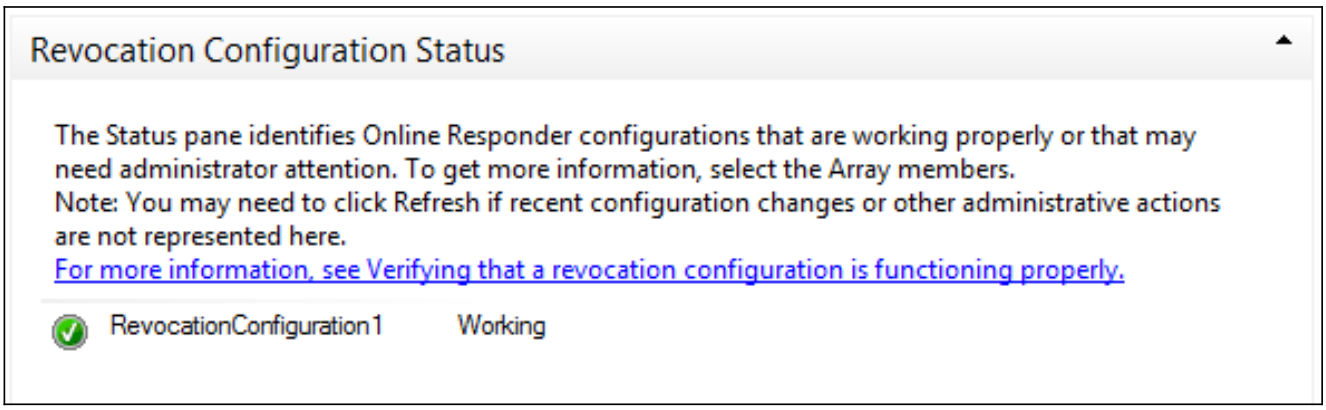


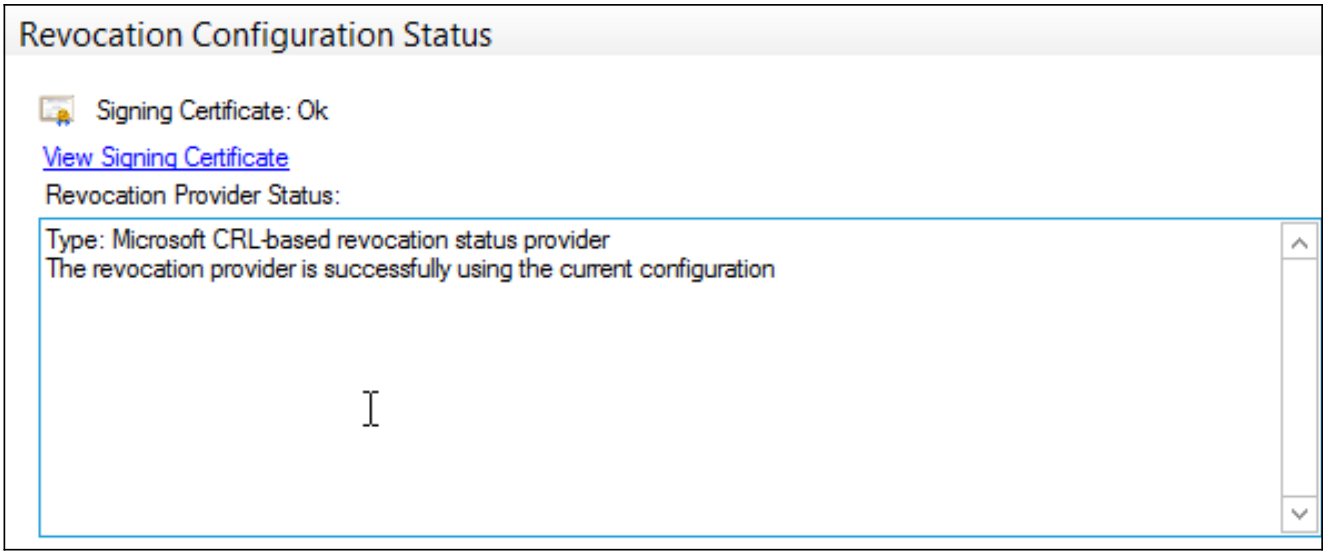
OCSP può utilizzare la stessa CA dell'organizzazione. Il certificato per il servizio OCSP è stato generato.

3. Utilizzare la CA dell'organizzazione selezionata e scegliere il modello creato in precedenza. Il certificato viene registrato automaticamente:

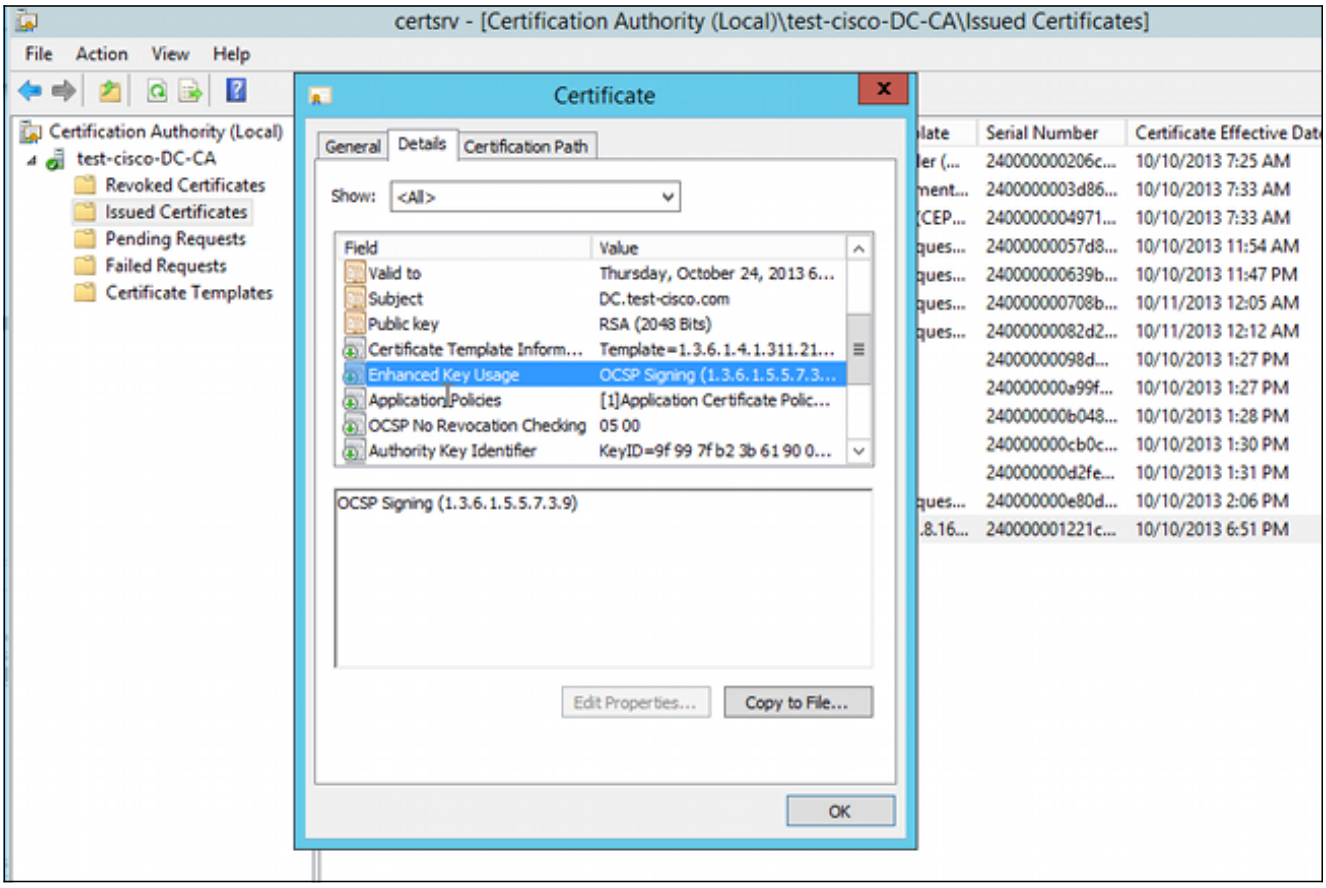


4. Confermare che il certificato è registrato e che il relativo stato è In esecuzione/OK:





5. Passare a **CA > Certificati rilasciati** per verificare i dettagli del certificato:



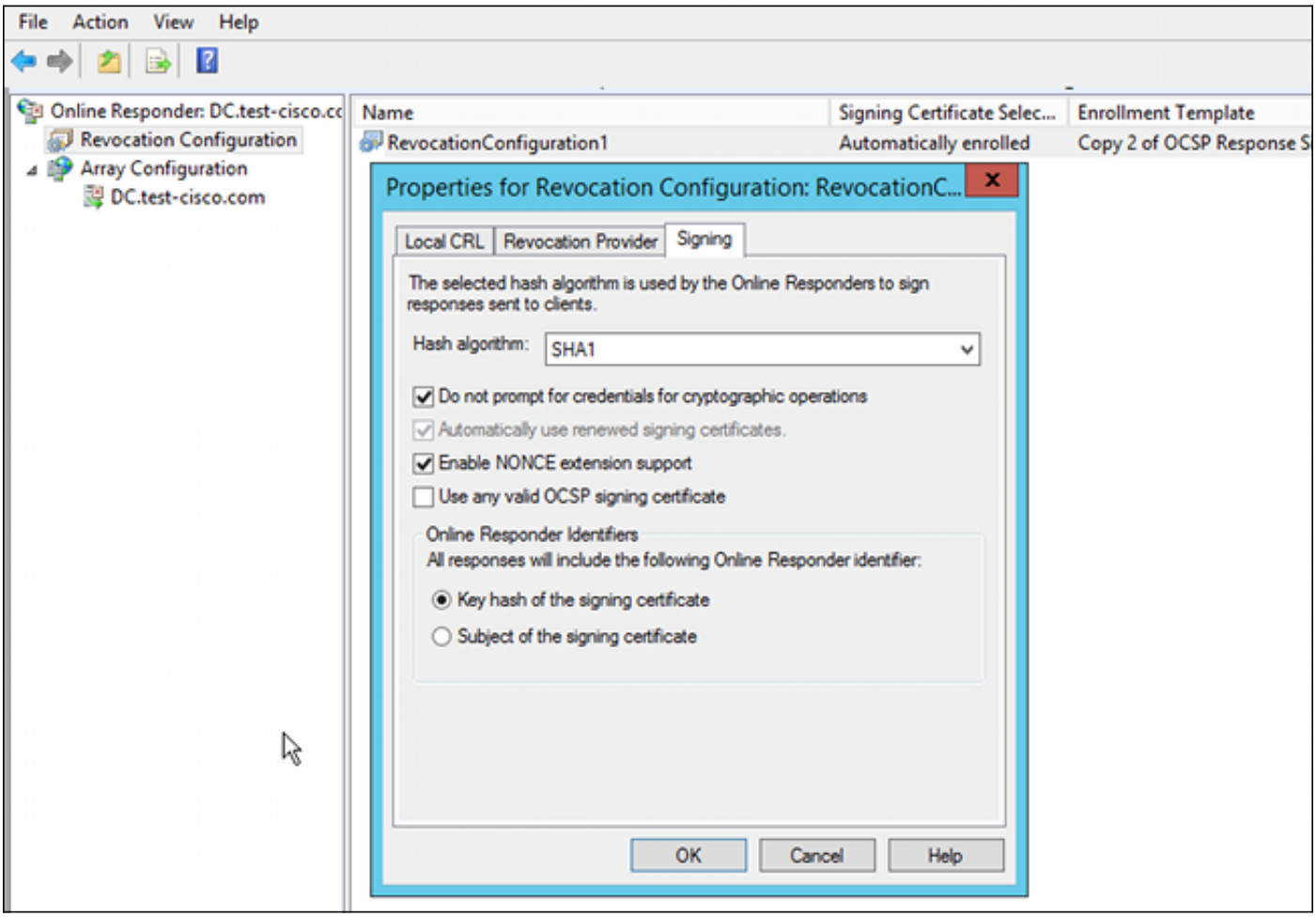
Nodi servizio OCSP

L'implementazione Microsoft di OCSP è conforme alla RFC 5019 - Il profilo OCSP (Lightweight Online Certificate Status Protocol) per ambienti con volumi elevati , che è una versione semplificata della RFC 2560 X.509 - Protocollo di stato del certificato online dell'infrastruttura a chiave pubblica Internet - OCSP .

L'ASA utilizza la RFC 2560 per OCSP. Una delle differenze nelle due RFC è che la RFC 5019 non accetta richieste firmate inviate dall'ASA.

Èpossibile forzare il servizio Microsoft OCSP ad accettare le richieste firmate e a rispondere con la

risposta firmata corretta. Passare a **Configurazione revoca > Configurazione revoca1 > Modifica proprietà** e selezionare l'opzione **Abilita supporto estensione NONCE**.



Il servizio OCSP è pronto per l'utilizzo.

Anche se Cisco sconsiglia di effettuare questa operazione, il nonce può essere disabilitato sull'appliance ASA:

```
BSNS-ASA5510-3(config-ca-trustpoint)# ocsp disable-nonce
```

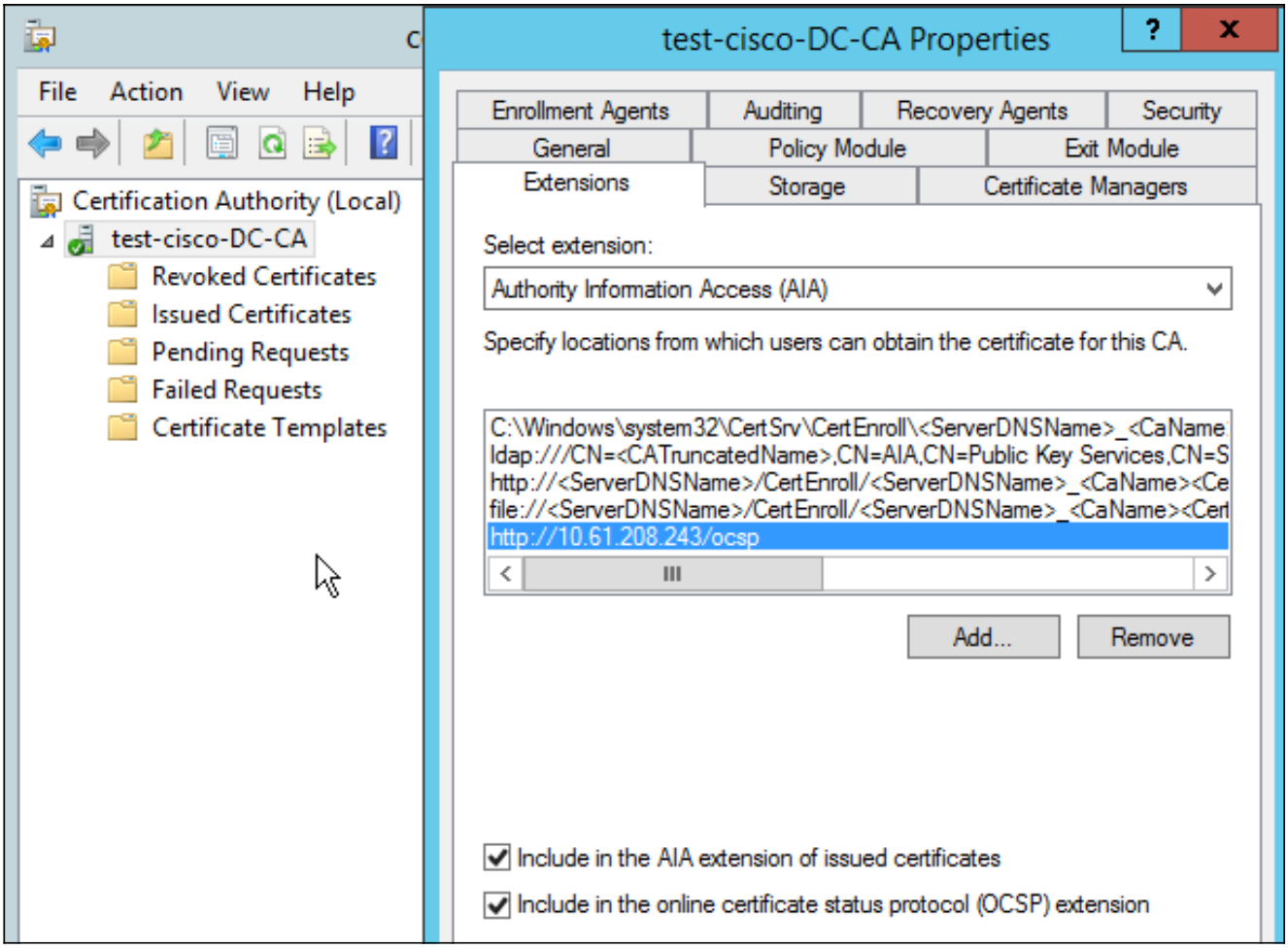
Configurazione CA per estensioni OCSP

Èquindi necessario riconfigurare la CA in modo da includere l'estensione del server OCSP in tutti i certificati rilasciati. L'URL di tale estensione viene utilizzato dall'ASA per connettersi al server OCSP quando viene convalidato un certificato.

1. Aprire la finestra di dialogo Proprietà relativa al server sulla CA.

2. Fare clic sulla scheda **Estensioni**. È necessaria l'estensione AIA (Authority Information Access) che punta al servizio OCSP. In questo esempio, è http://10.61.208.243/ocsp. Abilitare entrambe le opzioni seguenti per l'estensione AIA:

   Includi nell'estensione AIA dei certificati rilasciatiIncludi nell'estensione OCSP (Online Certificate Status Protocol)



In questo modo si garantisce che tutti i certificati rilasciati abbiano un'estensione corretta che punta al servizio OCSP.

OpenSSL

Nota: vedere la guida alla configurazione di Cisco ASA serie 5500 dall'interfaccia CLI 8.4 e 8.6: configurazione di un server esterno per l'autorizzazione utente di un'appliance di sicurezza per i dettagli sulla configurazione dell'ASA dalla CLI.

L'esempio presuppone che il server OpenSSL sia già configurato. In questa sezione vengono descritte solo la configurazione OCSP e le modifiche necessarie per la configurazione della CA.

In questa procedura viene descritto come generare il certificato OCSP:

1. Questi parametri sono necessari per il risponditore OCSP:

```
[ OCSPresponder ]
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage = OCSPSigning
```

2. I parametri seguenti sono necessari per i certificati utente:

```
[ UserCerts ]
```

```
authorityInfoAccess = OCSP;URI:http://10.61.208.243
```

3. I certificati devono essere generati e firmati dalla CA.

4. Avviare il server OCSP:

```
openssl ocsp -index ourCAwebPage/index.txt -port 80 -rsigner
ocspresponder.crt -rkey ocspresponder.key -CA cacert.crt -text -out
log.txt
```

5. Verificare il certificato di esempio:

```
openssl ocsp -CAfile cacert.crt -issuer cacert.crt -cert example-cert.crt
-url http://10.61.208.243 -resp_text
```

Ulteriori esempi sono disponibili sul sito Web OpenSSL .

OpenSSL, come ASA, supporta nonce OCSP; il nonce può essere controllato utilizzando le opzioni -nonce e -no_nonce.

ASA con più origini OCSP

L'ASA può sostituire l'URL OCSP. Anche se il certificato client contiene un URL OCSP, viene sovrascritto dalla configurazione sull'appliance ASA:

```
crypto ca trustpoint WIN2012
 revocation-check ocsp
 enrollment url http://10.61.209.83:80/certsrv/mscep/mscep.dll
 ocsp url http://10.10.10.10/ocsp
```

L'indirizzo del server OCSP può essere definito esplicitamente. In questo esempio di comando vengono associati tutti i certificati con amministratore nel nome del soggetto, viene utilizzato un trust point OPENSSL per convalidare la firma OCSP e viene utilizzato l'URL http://11.11.11.11/ocsp per inviare la richiesta:

```
crypto ca trustpoint WIN2012
 revocation-check ocsp
 enrollment url http://10.61.209.83:80/certsrv/mscep/mscep.dll
 match certificate MAP override ocsp trustpoint OPENSSL 10 url
http://11.11.11.11/ocsp

crypto ca certificate map MAP 10
 subject-name co administrator
```

L'ordine utilizzato per trovare l'URL OCSP è:

1. Server OCSP impostato con il comando **match certificate**
2. Un server OCSP impostato con il comando **ocsp url**
3. Il server OCSP nel campo AIA del certificato client

ASA con OCSP firmato da una CA diversa

Una risposta OCSP può essere firmata da un'altra CA. In questo caso, è necessario usare il comando **match certificate** per usare un trust point diverso sull'appliance ASA per la convalida del

certificato OCSP.

```
crypto ca trustpoint WIN2012
 revocation-check ocsp
 enrollment url http://10.61.209.83:80/certsrv/mscep/mscep.dll
 match certificate MAP override ocsp trustpoint OPENSSL 10 url
http://11.11.11.11/ocsp

crypto ca certificate map MAP 10
 subject-name co administrator

crypto ca trustpoint OPENSSL
enrollment terminal
revocation-check none
```

Nell'esempio, l'ASA usa la riscrittura dell'URL OCSP per tutti i certificati con un nome soggetto che contiene l'indirizzo administrator. L'appliance ASA è costretta a convalidare il certificato del risponditore OCSP rispetto a un altro trust point, OPENSSL. I certificati utente sono ancora convalidati nel trust point WIN2012.

Poiché il certificato del risponditore OCSP ha l'estensione 'Nessun controllo di revoca OCSP', il certificato non viene verificato, anche quando OCSP è costretto a eseguire la convalida rispetto al trust point OPENSSL.

Per impostazione predefinita, la ricerca viene eseguita in tutti i trust point quando l'ASA cerca di verificare il certificato utente. La convalida del certificato del risponditore OCSP è diversa. L'ASA cerca solo il trust point che è già stato trovato per il certificato utente (in questo esempio, WIN2012).

Di conseguenza, è necessario utilizzare il comando **match certificate** per forzare l'appliance ASA a utilizzare un trust point diverso per la convalida del certificato OCSP (in questo esempio, OPENSSL).

I certificati utente vengono convalidati in base al primo trust point corrispondente (WIN2012 in questo esempio), che determina quindi il trust point predefinito per la convalida del risponditore OCSP.

Se nel comando **match certificate** non viene specificato alcun trust point specifico, il certificato OCSP viene convalidato rispetto allo stesso trust point dei certificati utente (in questo esempio, WIN2012).

```
crypto ca trustpoint WIN2012
 revocation-check ocsp
 enrollment url http://10.61.209.83:80/certsrv/mscep/mscep.dll
 match certificate MAP override ocsp 10 url http://11.11.11.11/ocsp
```

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

> **Nota**: lo strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi **show**. Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show**.

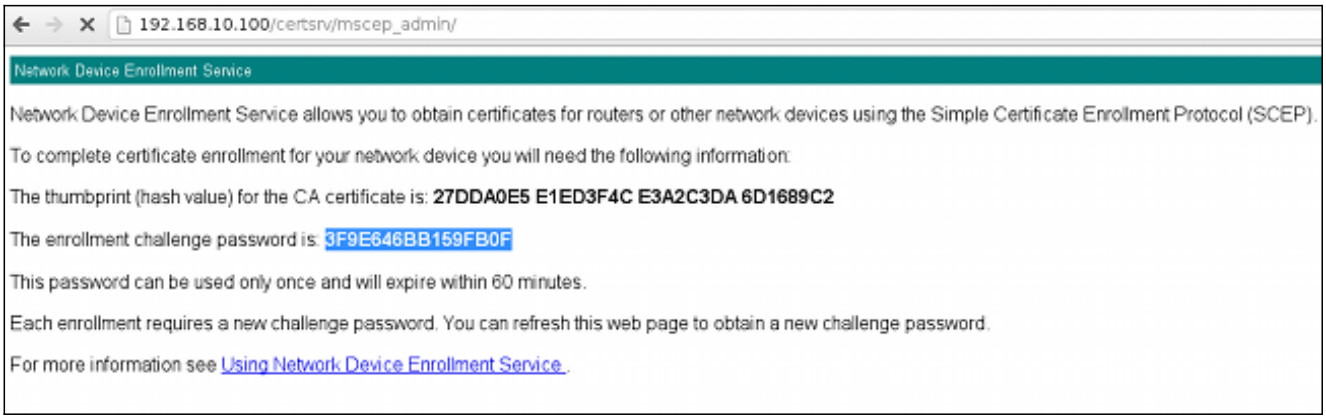
ASA - Ottieni certificato tramite SCEP

In questa procedura viene descritto come ottenere il certificato utilizzando SCEP:

1. Questo è il processo di autenticazione del trust point per ottenere il certificato CA:

```
debug crypto ca
debug crypto ca messages
debug crypto ca transaction

BSNS-ASA5510-3(config-ca-crl)# crypto ca authenticate WIN2012
Crypto CA thread wakes up!

CRYPTO_PKI: Sending CA Certificate Request:
GET /certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message=
WIN2012 HTTP/1.0
Host: 10.61.209.83

CRYPTO_PKI: http connection opened

INFO: Certificate has the following attributes:
Fingerprint:     27dda0e5 e1ed3f4c e3a2c3da 6d1689c2
Do you accept this certificate? [yes/no]:

% Please answer 'yes' or 'no'.
Do you accept this certificate? [yes/no]:
yes

Trustpoint CA certificate accepted.
```

2. Per richiedere il certificato, l'appliance ASA deve avere una password SCEP monouso ottenibile dalla console di amministrazione all'indirizzo http://IP/certsrv/mscep_admin:



3. Utilizzare questa password per richiedere il certificato sull'appliance ASA:

```
BSNS-ASA5510-3(config)# crypto ca enroll WIN2012
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
  password to the CA Administrator in order to revoke your certificate.
  For security reasons your password will not be saved in the
configuration.
  Please make a note of it.
```

```
Password: ****************
Re-enter password: ****************


% The fully-qualified domain name in the certificate will be:
BSNS-ASA5510-3.test-cisco.com
% Include the device serial number in the subject name? [yes/no]: yes
% The serial number in the certificate will be: JMX1014K16Y

Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
BSNS-ASA5510-3(config)#

CRYPTO_PKI: Sending CA Certificate Request:
GET /certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message=
WIN2012 HTTP/1.0
Host: 10.61.209.83

CRYPTO_PKI: http connection opened

CRYPTO_PKI: Found a subject match - inserting the following cert record
into certList
```

Alcuni output sono stati omessi per motivi di chiarezza.

4. Verificare i certificati CA e ASA:

```
BSNS-ASA5510-3(config)# show crypto ca certificates
Certificate
 Status: Available
 Certificate Serial Number: 240000001cbf2fc89f44fe819700000000001c
 Certificate Usage: General Purpose
 Public Key Type: RSA (1024 bits)
 Signature Algorithm: SHA1 with RSA Encryption
 Issuer Name:
   cn=test-cisco-DC-CA
   dc=test-cisco
   dc=com
 Subject Name:
    hostname=BSNS-ASA5510-3.test-cisco.com
   serialNumber=JMX1014K16Y
 CRL Distribution Points:
   [1]  ldap:///CN=test-cisco-DC-CA,CN=DC,CN=CDP,
CN=Public%20Key%20Services,CN=Services,CN=Configuration,
DC=test-cisco,DC=com?certificateRevocationList?base?objectClass=
cRLDistributionPoint
 Validity Date:
   start date: 11:02:36 CEST Oct 13 2013
   end   date: 11:02:36 CEST Oct 13 2015
 Associated Trustpoints: WIN2012

CA Certificate
 Status: Available
 Certificate Serial Number: 3d4c0881b04c799f483f4bbe91dc98ae
 Certificate Usage: Signature
 Public Key Type: RSA (2048 bits)
 Signature Algorithm: SHA1 with RSA Encryption
 Issuer Name:
    cn=test-cisco-DC-CA
   dc=test-cisco
   dc=com
 Subject Name:
```

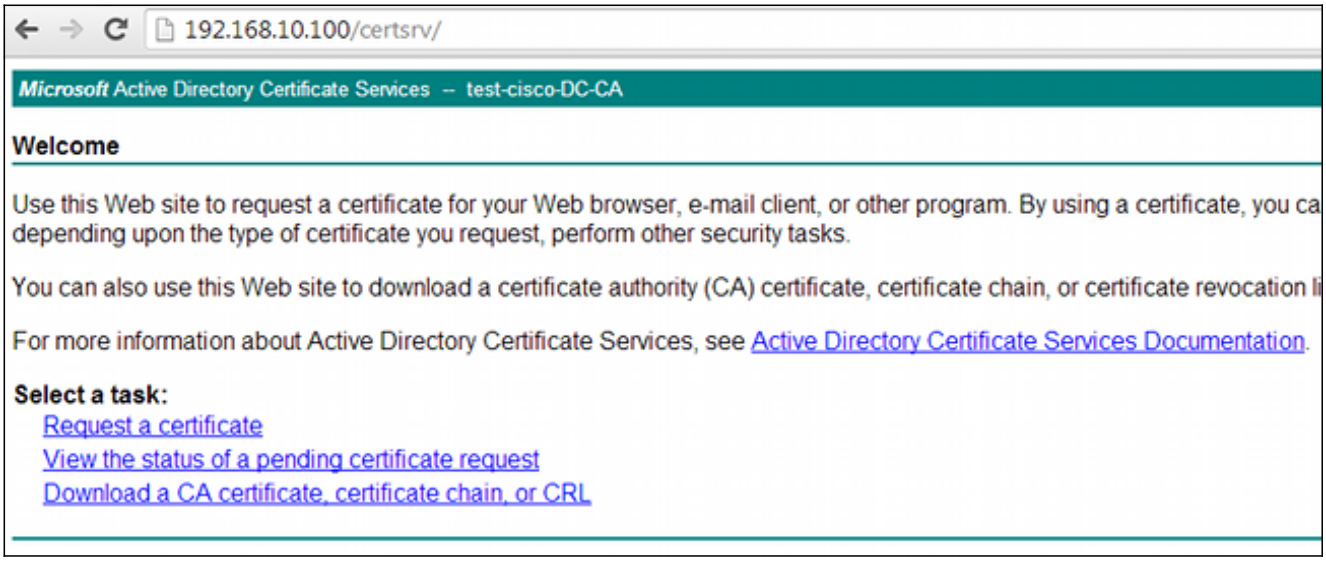
```
  cn=test-cisco-DC-CA
  dc=test-cisco
  dc=com
Validity Date:
  start date: 07:23:03 CEST Oct 10 2013
  end   date: 07:33:03 CEST Oct 10 2018
Associated Trustpoints: WIN2012
```

L'appliance ASA non visualizza la maggior parte delle estensioni dei certificati. Anche se il certificato ASA contiene l'estensione 'OCSP URL in AIA', la CLI ASA non la presenta. Questa funzione è richiesta dall'ID bug Cisco CSCui44335, "ASA ENH Certificate x509 extensions displayed" (Estensioni del certificato ENH ASA x509 visualizzate).

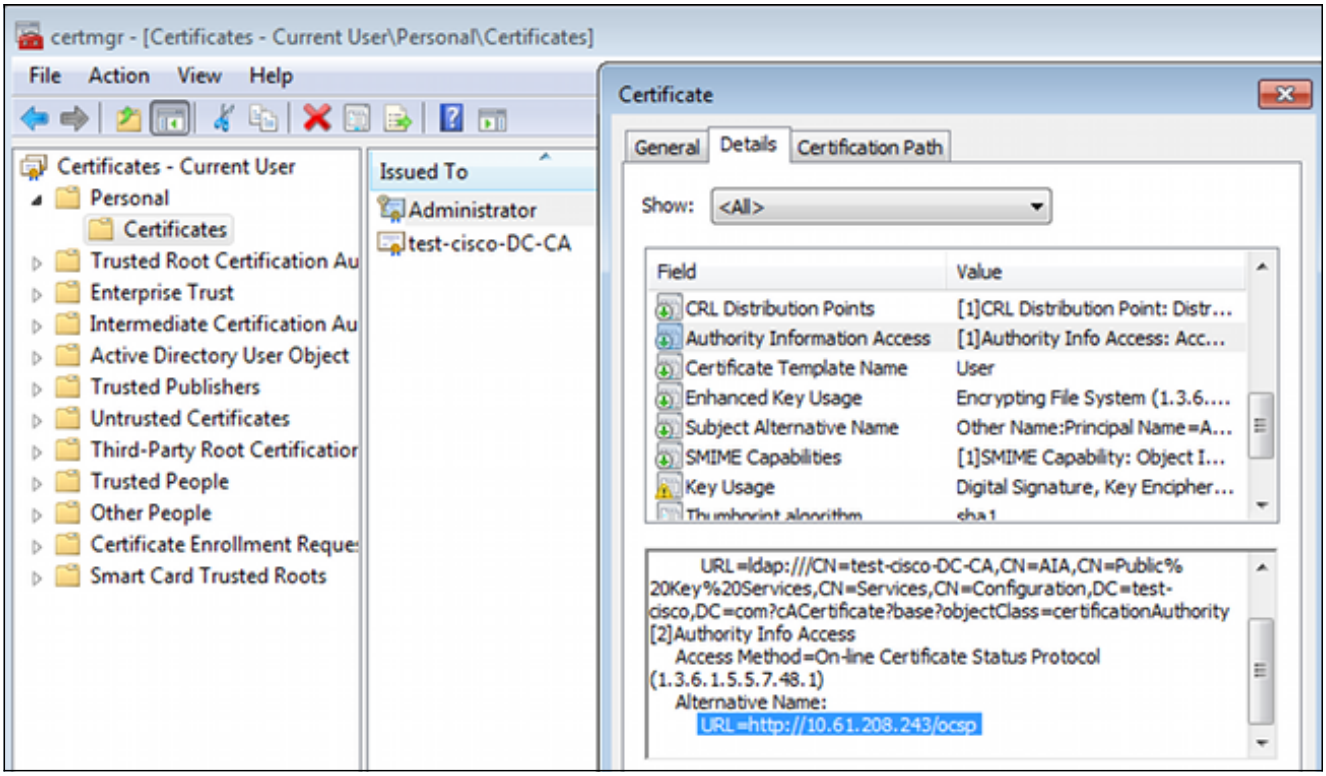
AnyConnect - Ottieni certificato tramite pagina Web

In questa procedura viene descritto come ottenere il certificato utilizzando il browser Web sul client:

1. Èpossibile richiedere un certificato utente AnyConnect tramite la pagina Web. Sul PC client, utilizzare un browser Web per accedere alla CA all'indirizzo http:///*IP*/certsrv:



2. Il certificato utente può essere salvato nell'archivio del browser Web e quindi esportato nell'archivio di Microsoft in cui è possibile eseguire la ricerca con AnyConnect. Utilizzare certmgr.msc per verificare il certificato ricevuto:



AnyConnect può anche richiedere il certificato se è presente un profilo AnyConnect corretto.

Accesso remoto VPN ASA con convalida OCSP

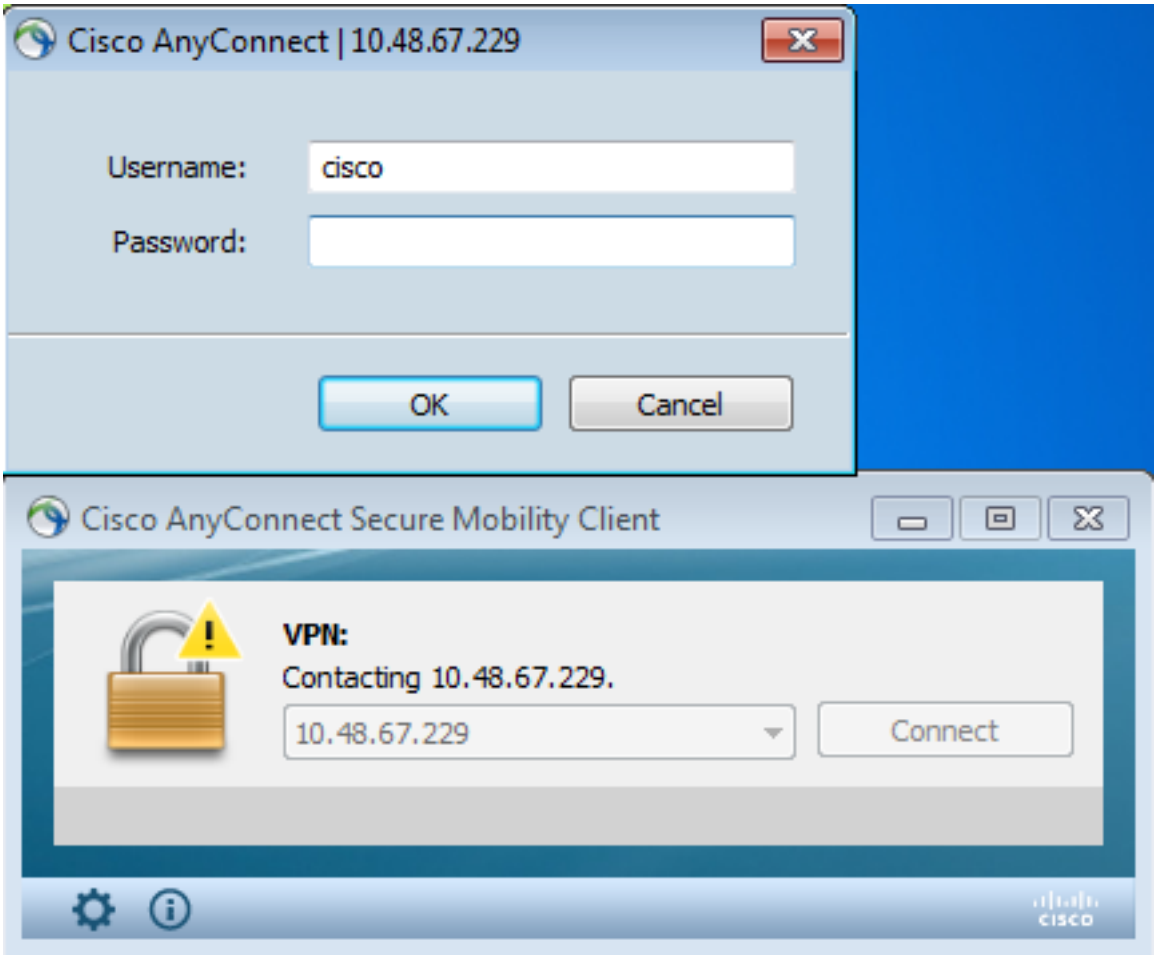
In questa procedura viene descritto come controllare la convalida OCSP:

1. Durante il tentativo di connessione, l'ASA segnala che il certificato è in fase di verifica per verificare la presenza di OCSP. Il certificato di firma OCSP ha un'estensione senza controllo e non è stato controllato tramite OCSP:

```
debug crypto ca
debug crypto ca messages
debug crypto ca transaction

%ASA-6-725001: Starting SSL handshake with client outside:
10.61.209.83/51262 for TLSv1 session.
%ASA-7-717025: Validating certificate chain containing 1 certificate(s).
%ASA-7-717029: Identified client certificate within certificate chain.
serial number: 240000001B2AD208B12811687400000000001B, subject name:
cn=Administrator,cn=Users,dc=test-cisco,dc=com.
Found a suitable trustpoint WIN2012 to validate certificate.
%ASA-7-717035: OCSP status is being checked for certificate. serial
number: 240000001B2AD208B12811687400000000001B, subject name:
cn=Administrator,cn=Users,dc=test-cisco,dc=com.
%ASA-6-302013: Built outbound TCP connection 1283 for outside:
10.61.209.83/80 (10.61.209.83/80) to identity:10.48.67.229/35751
(10.48.67.229/35751)
%ASA-6-717033: CSP response received.
%ASA-7-717034: No-check extension found in certificate. OCSP check
bypassed.
%ASA-6-717028: Certificate chain was successfully validated with
revocation status check.
```

Alcuni output sono stati omessi per motivi di chiarezza.

2. L'utente finale fornisce le credenziali dell'utente:



3. La sessione VPN è terminata correttamente:

```
%ASA-7-717036: Looking for a tunnel group match based on certificate maps
for peer certificate with serial number:
240000001B2AD208B12811687400000000001B, subject name: cn=Administrator,
cn=Users,dc=test-cisco,dc=com, issuer_name: cn=test-cisco-DC-CA,
dc=test-cisco,dc=com.
%ASA-7-717038: Tunnel group match found. Tunnel Group: RA, Peer
certificate: serial number: 240000001B2AD208B12811687400000000001B,
subject name: cn=Administrator,cn=Users,dc=test-cisco,dc=com,
issuer_name: cn=test-cisco-DC-CA,dc=test-cisco,dc=com.

%ASA-6-113012: AAA user authentication Successful : local database :
user = cisco
%ASA-6-113009: AAA retrieved default group policy (MY) for user = cisco
%ASA-6-113039: Group <MY> User <cisco> IP <10.61.209.83> AnyConnect parent
session started.
```

4. La sessione viene creata:

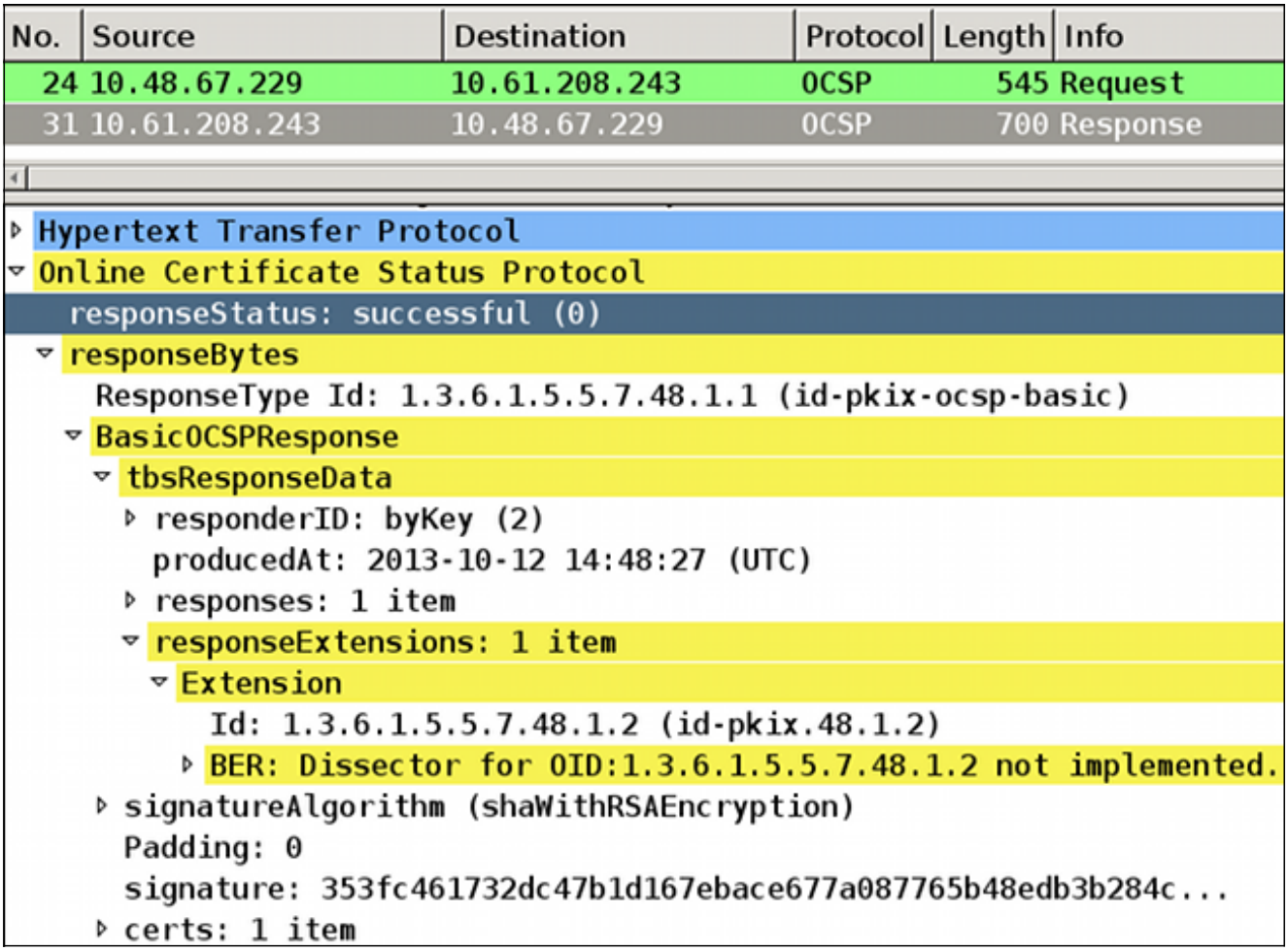
```
BSNS-ASA5510-3(config)# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username     : cisco                  Index        : 4
```

```
Assigned IP  : 192.168.11.100         Public IP    : 10.61.209.83
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4
DTLS-Tunnel: (1)AES128
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1
DTLS-Tunnel: (1)SHA1
Bytes Tx     : 10540                 Bytes Rx     : 32236
Pkts Tx      : 8                     Pkts Rx      : 209
Pkts Tx Drop : 0                     Pkts Rx Drop : 0
Group Policy : MY                    Tunnel Group : RA
Login Time   : 11:30:31 CEST Sun Oct 13 2013
Duration     : 0h:01m:05s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                   VLAN         : none

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
 Tunnel ID    : 4.1
 Public IP    : 10.61.209.83
 Encryption   : none                  Hashing      : none
 TCP Src Port : 51401                 TCP Dst Port : 443
 Auth Mode    : Certificate and userPassword
 Idle Time Out: 30 Minutes            Idle TO Left : 29 Minutes
 Client OS    : Windows
 Client Type  : AnyConnect
 Client Ver   : Cisco AnyConnect VPN Agent for Windows 3.1.02040
 Bytes Tx     : 5270                  Bytes Rx     : 788
 Pkts Tx      : 4                     Pkts Rx      : 1
 Pkts Tx Drop : 0                     Pkts Rx Drop : 0

SSL-Tunnel:
 Tunnel ID    : 4.2
 Assigned IP  : 192.168.11.100        Public IP    : 10.61.209.83
 Encryption   : RC4                   Hashing      : SHA1
 Encapsulation: TLSv1.0               TCP Src Port : 51406
 TCP Dst Port : 443                   Auth Mode    : Certificate and
userPassword
 Idle Time Out: 30 Minutes            Idle TO Left : 29 Minutes
 Client OS    : Windows
 Client Type  : SSL VPN Client
 Client Ver   : Cisco AnyConnect VPN Agent for Windows 3.1.02040
 Bytes Tx     : 5270                  Bytes Rx     : 1995
 Pkts Tx      : 4                     Pkts Rx      : 10
 Pkts Tx Drop : 0                     Pkts Rx Drop : 0

DTLS-Tunnel:
 Tunnel ID    : 4.3
 Assigned IP  : 192.168.11.100        Public IP    : 10.61.209.83
 Encryption   : AES128                Hashing      : SHA1
 Encapsulation: DTLSv1.0              UDP Src Port : 58053
 UDP Dst Port : 443                   Auth Mode    : Certificate and
userPassword
 Idle Time Out: 30 Minutes            Idle TO Left : 29 Minutes
 Client OS    : Windows
 Client Type  : DTLS VPN Client
 Client Ver   : Cisco AnyConnect VPN Agent for Windows 3.1.02040
 Bytes Tx     : 0                     Bytes Rx     : 29664
 Pkts Tx      : 0                     Pkts Rx      : 201
 Pkts Tx Drop : 0                     Pkts Rx Drop : 0
```

5. Èpossibile utilizzare i debug dettagliati per la convalida OCSP:

```
CRYPTO_PKI: Starting OCSP revocation
CRYPTO_PKI: Attempting to find OCSP override for peer cert: serial number:
2400000019F341BA75BD25E91A000000000019, subject name: cn=Administrator,
cn=Users,dc=test-cisco,dc=com, issuer_name: cn=test-cisco-DC-CA,
dc=test-cisco,dc=com.
CRYPTO_PKI: No OCSP overrides found. <-- no OCSP url in the ASA config

CRYPTO_PKI: http connection opened
CRYPTO_PKI: OCSP response received successfully.
CRYPTO_PKI: OCSP found in-band certificate: serial number:
240000001221CFA239477CE1C0000000000012, subject name:
cn=DC.test-cisco.com, issuer_name: cn=test-cisco-DC-CA,dc=test-cisco,
dc=com
CRYPTO_PKI: OCSP responderID byKeyHash
CRYPTO_PKI: OCSP response contains 1 cert singleResponses responseData
sequence.

Found response for request certificate!
CRYPTO_PKI: Verifying OCSP response with 1 certs in the responder chain
CRYPTO_PKI: Validating OCSP response using trusted CA cert: serial number:
3D4C0881B04C799F483F4BBE91DC98AE, subject name: cn=test-cisco-DC-CA,
dc=test-cisco,dc=com, issuer_name: cn=test-cisco-DC-CA,dc=test-cisco,
dc=com

CERT-C: W ocsputil.c(538) : Error #708h
CERT-C: W ocsputil.c(538) : Error #708h

CRYPTO_PKI: Validating OCSP responder certificate: serial number:
240000001221CFA239477CE1C0000000000012, subject name:
cn=DC.test-cisco.com, issuer_name: cn=test-cisco-DC-CA,dc=test-cisco,
dc=com, signature alg: SHA1/RSA

CRYPTO_PKI: verifyResponseSig:3191
CRYPTO_PKI: OCSP responder cert has a NoCheck extension
CRYPTO_PKI: Responder cert status is not revoked <-- do not verify
responder cert
CRYPTO_PKI: response signed by the CA
CRYPTO_PKI: Storage context released by thread Crypto CA

CRYPTO_PKI: transaction GetOCSP completed
CRYPTO_PKI: Process next cert, valid cert. <-- client certificate
validated correctly
```

6. A livello di acquisizione del pacchetto, si tratta della richiesta OCSP e della risposta OCSP corretta. La risposta include la firma corretta. Estensione nonce abilitata in Microsoft OCSP:



Accesso remoto VPN ASA con più origini OCSP

Se un certificato di corrispondenza è configurato come spiegato in ASA con più origini OCSP, ha la precedenza:

```
CRYPTO_PKI: Processing map MAP sequence 10...
CRYPTO_PKI: Match of subject-name field to map PASSED. Peer cert field:  =
cn=Administrator,cn=Users,dc=test-cisco,dc=com, map rule: subject-name
  co administrator.
CRYPTO_PKI: Peer cert has been authorized by map: MAP sequence: 10.
CRYPTO_PKI: Found OCSP override match. Override URL: http://11.11.11.11/ocsp,
Override trustpoint: OPENSSL
```

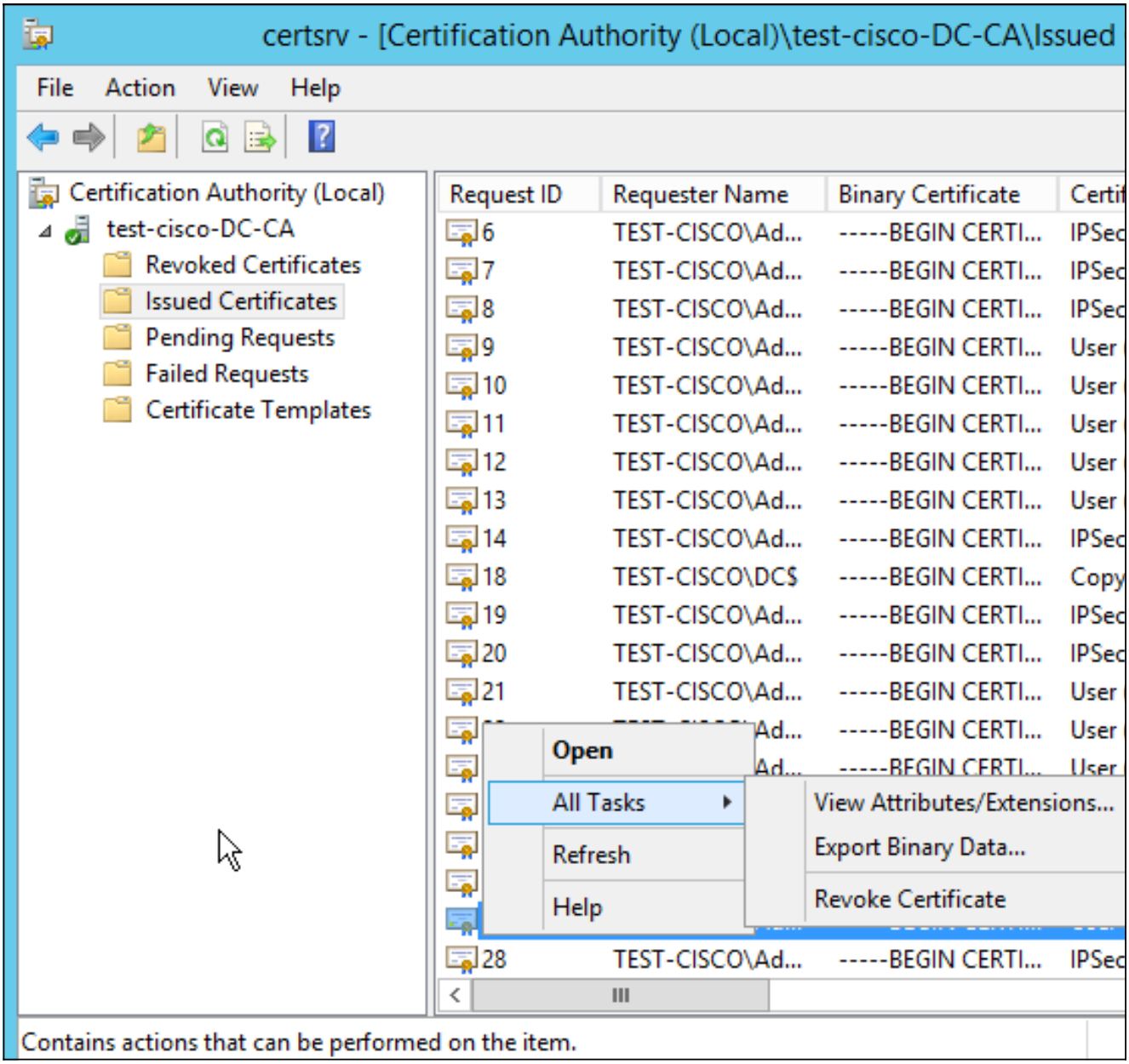
Quando si utilizza una sostituzione dell'URL OCSP, i debug sono:

```
CRYPTO_PKI: No OCSP override via cert maps found. Override was found in
trustpoint: WIN2012, URL found: http://10.10.10.10/ocsp.
```

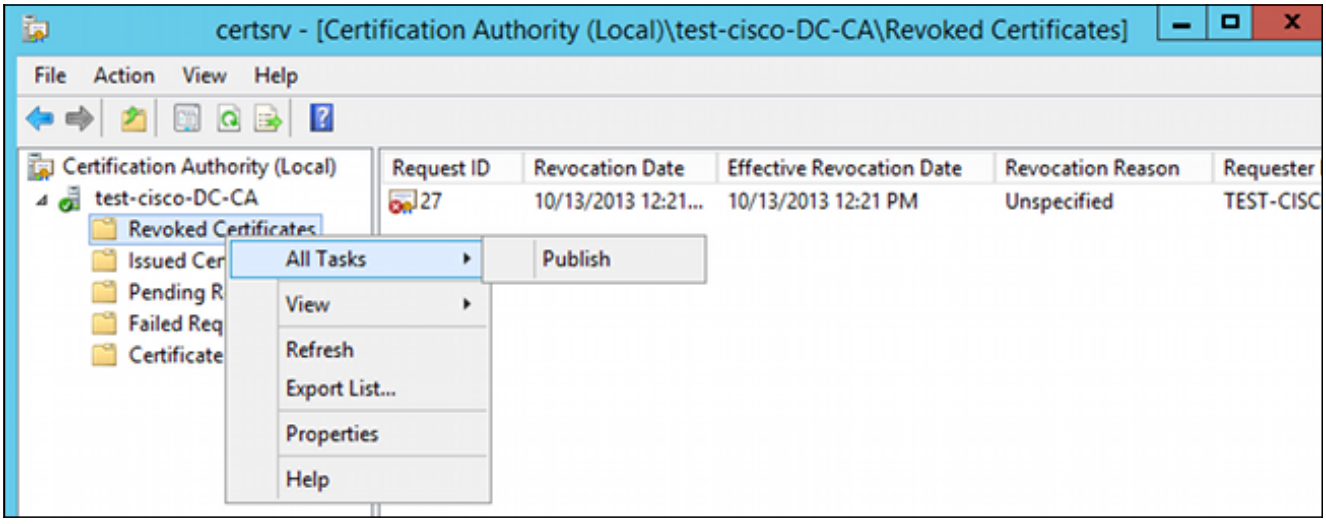
Accesso remoto VPN ASA con OCSP e certificato revocato

In questa procedura viene descritto come revocare il certificato e confermarne lo stato:

1. Revocare il certificato client:



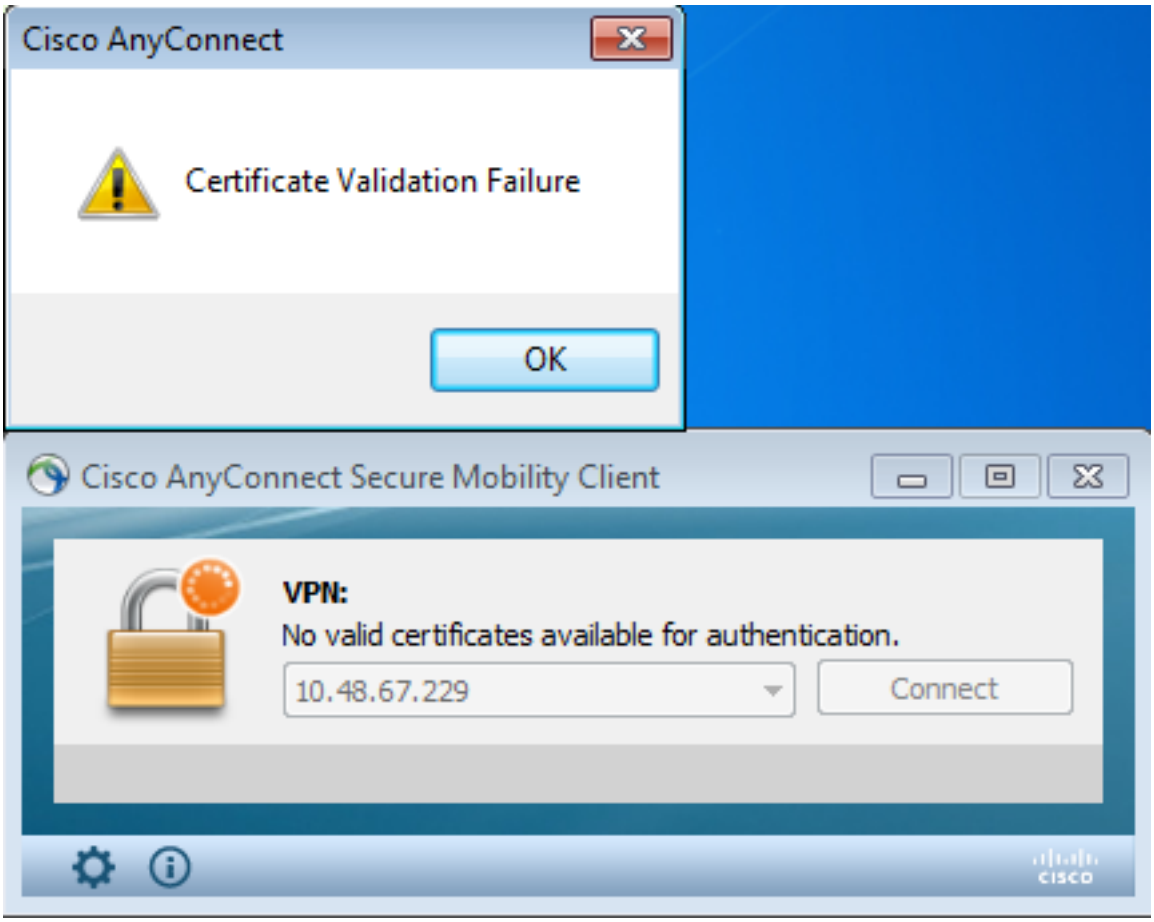
2. Pubblicare i risultati:



3. [Facoltativo] I passaggi 1 e 2 possono essere eseguiti anche con l'utility certutil CLI in Power Shell:

```
c:\certutil -crl
CertUtil: -CRL command completed succesfully.
```

4. Quando il client tenta di connettersi, si verifica un errore di convalida del certificato:



5. I log di AnyConnect indicano anche l'errore di convalida del certificato:

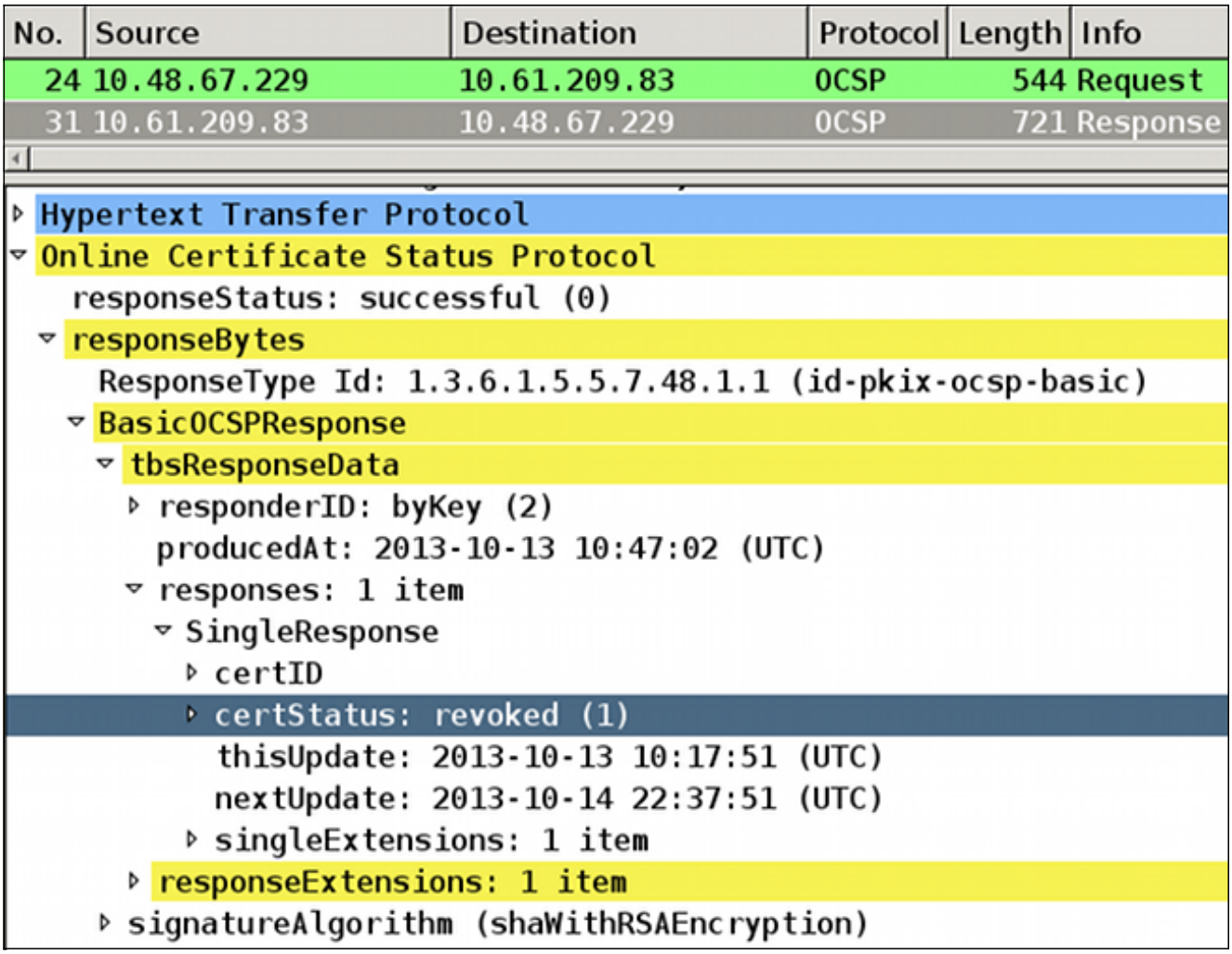
```
[2013-10-13 12:49:53] Contacting 10.48.67.229.
[2013-10-13 12:49:54] No valid certificates available for authentication.
[2013-10-13 12:49:55] Certificate Validation Failure
```

6. L'ASA segnala che lo stato del certificato è stato revocato:

```
CRYPTO_PKI: Starting OCSP revocation
CRYPTO_PKI: OCSP response received successfully.
CRYPTO_PKI: OCSP found in-band certificate: serial number:
240000001221CFA239477CE1C0000000000012, subject name:
cn=DC.test-cisco.com, issuer_name: cn=test-cisco-DC-CA,dc=test-cisco,
dc=com
CRYPTO_PKI: OCSP responderID byKeyHash
CRYPTO_PKI: OCSP response contains 1 cert singleResponses responseData
sequence.

Found response for request certificate!
CRYPTO_PKI: Verifying OCSP response with 1 certs in the responder chain
CRYPTO_PKI: Validating OCSP response using trusted CA cert: serial number:
3D4C0881B04C799F483F4BBE91DC98AE, subject name: cn=test-cisco-DC-CA,
dc=test-cisco,dc=com, issuer_name: cn=test-cisco-DC-CA,dc=test-cisco,
```

```
dc=com

CRYPTO_PKI: verifyResponseSig:3191
CRYPTO_PKI: OCSP responder cert has a NoCheck extension
CRYPTO_PKI: Responder cert status is not revoked
CRYPTO_PKI: response signed by the CA
CRYPTO_PKI: Storage context released by thread Crypto CA

CRYPTO_PKI: transaction GetOCSP completed

CRYPTO_PKI: Received OCSP response:Oct 13 2013 12:48:03: %ASA-3-717027:
Certificate chain failed validation. Generic error occurred, serial
number: 240000001B2AD208B12811687400000000001B, subject name:
cn=Administrator,cn=Users,dc=test-cisco,dc=com.

CRYPTO_PKI: Blocking chain callback called for OCSP response (trustpoint:
WIN2012, status: 1)
CRYPTO_PKI: Destroying OCSP data handle 0xae255ac0
CRYPTO_PKI: OCSP polling for trustpoint WIN2012 succeeded. Certificate
status is REVOKED.
CRYPTO_PKI: Process next cert in chain entered with status: 13.
CRYPTO_PKI: Process next cert, Cert revoked: 13
```

7. Le acquisizioni del pacchetto mostrano una risposta OCSP riuscita con lo stato del certificato revocato:



Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla

configurazione.

Server OCSP inattivo

L'appliance ASA segnala quando il server OCSP è inattivo:

```
CRYPTO_PKI: unable to find a valid OCSP server.
CRYPTO PKI: OCSP revocation check has failed.  Status: 1800.
```

L'acquisizione dei pacchetti può essere utile anche per la risoluzione dei problemi.

Ora non sincronizzata

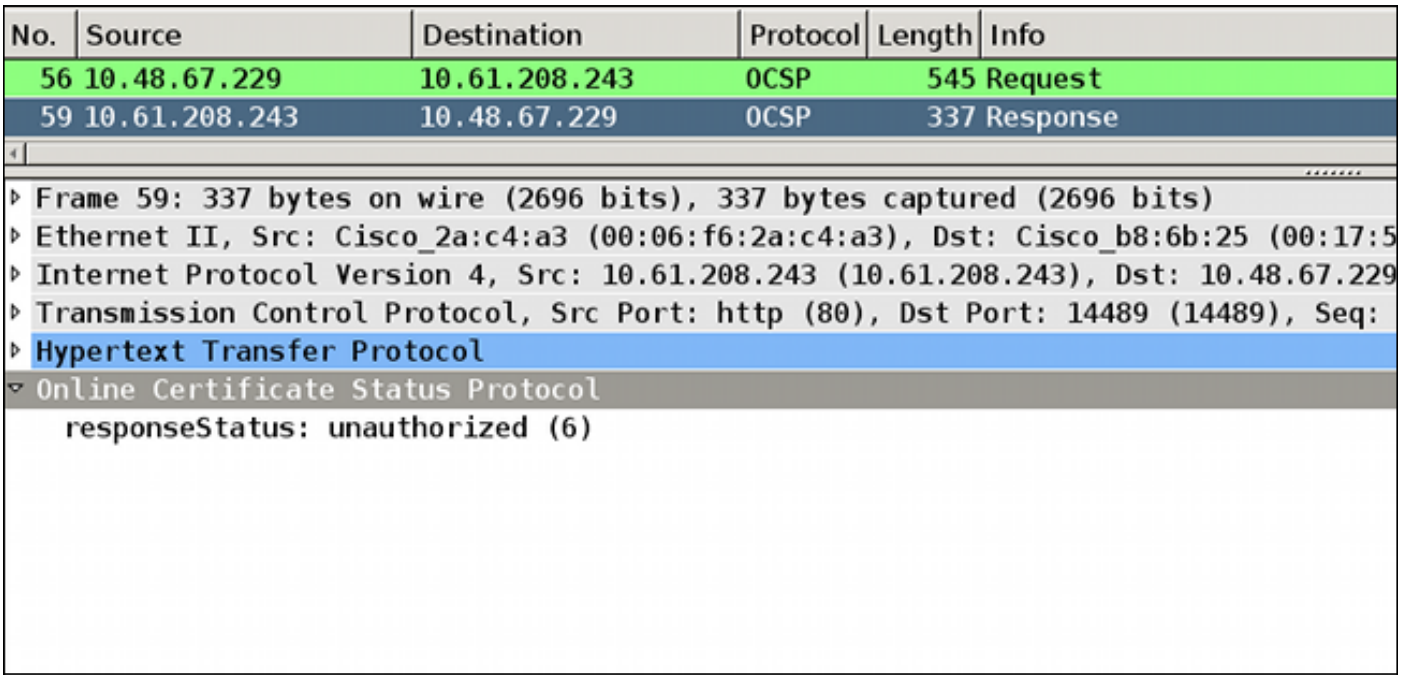
Se l'ora corrente sul server OCSP è precedente a quella sull'appliance ASA (sono accettabili piccole differenze), il server OCSP invia una risposta non autorizzata e l'ASA la segnala:

```
CRYPTO_PKI: OCSP response status - unauthorized
```

Se l'ASA riceve una risposta OCSP da tempi futuri, anche questa condizione si verifica.

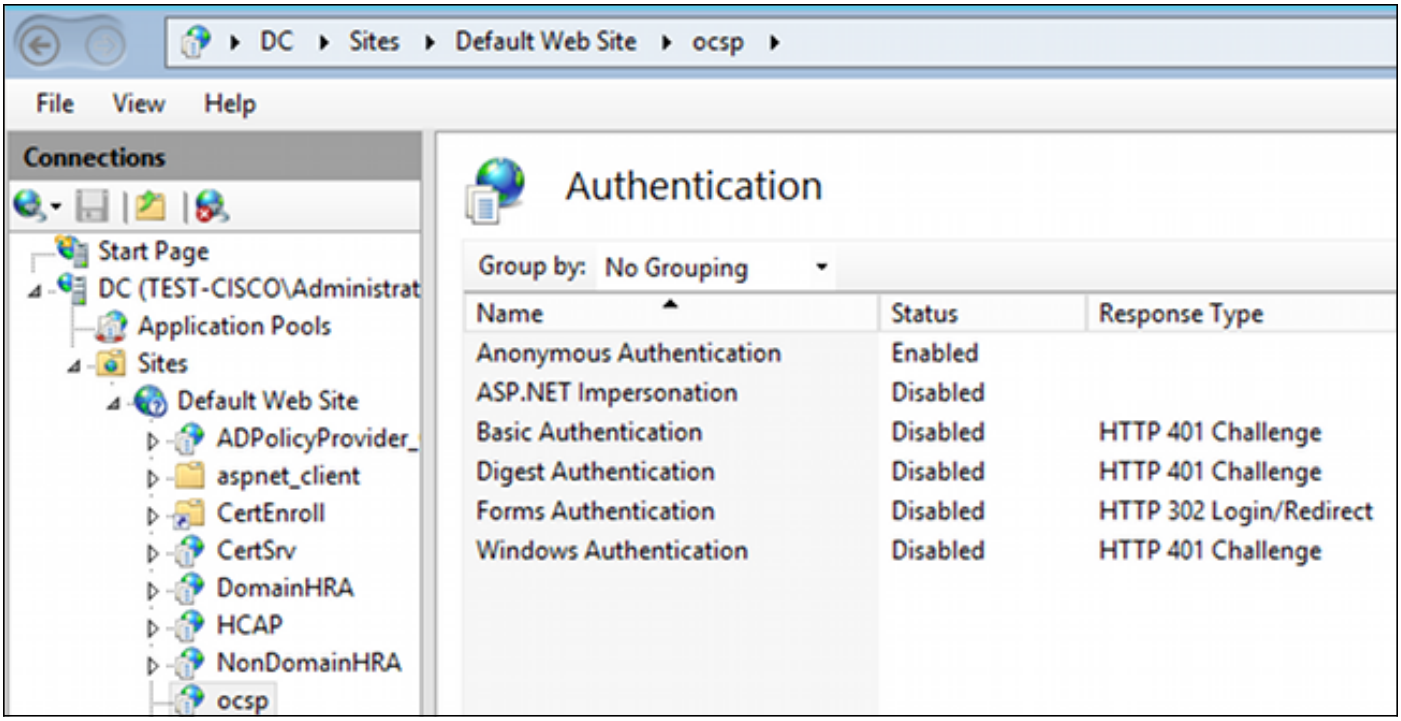
Nessun segno firmato non supportato

Se il nonces sul server non è supportato (impostazione predefinita in Microsoft Windows 2012 R2), viene restituita una risposta non autorizzata:



Autenticazione server IIS7

I problemi relativi a una richiesta SCEP/OCSP sono spesso dovuti a un'autenticazione non corretta in Internet Information Services 7 (IIS7). Verificare che l'accesso anonimo sia configurato:



Informazioni correlate

- Microsoft TechNet: Guida all'installazione, alla configurazione e alla risoluzione dei problemi del risponditore online
- Microsoft TechNet: configurazione di una CA per il supporto dei risponditori OCSP
- Guida di riferimento ai comandi di Cisco ASA serie 1000
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).