ASA Remote Access VPN with OCSP Verification under Microsoft Windows 2012 and OpenSSL

Document ID: 116720

Contributed by Michal Garcarz, Cisco TAC Engineer.
Nov 06, 2013

Contents

Introduction
Prerequisites
- Requirements
- Components Used

Configure
- Network Diagram
- ASA Remote Access with OCSP
- Microsoft Windows 2012 CA
  - Services Installation
  - CA Configuration for OCSP Template
  - OCSP Service Certificate
  - OCSP Service Nonces
  - CA Configuration for OCSP Extensions
- OpenSSL
- ASA with Multiple OCSP Sources
- ASA with OCSP Signed by Different CA

Verify
- ASA − Get Certificate via SCEP
- AnyConnect − Get Certificate via Web Page
- ASA VPN Remote Access with OCSP Validation
- ASA VPN Remote Access with Multiple OCSP Sources
- ASA VPN Remote Access with OCSP and Revoked Certificate

Troubleshoot
- OCSP Server Down
- Time Not Synchronized
- Signed Nonces Not Supported
- IIS7 Server Authentication

Related Information

Introduction

This document describes how to use Online Certificate Status Protocol (OCSP) validation on a Cisco Adaptive Security Appliance (ASA) for certificates presented by VPN users. Example configurations for two OCSP servers (Microsoft Windows Certificate Authority [CA] and OpenSSL) are presented. The Verify section describes detailed flows on the packet level, and the Troubleshoot section focuses on typical errors and problems.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Adaptive Security Appliance command−line interface (CLI) configuration and Secure Socket Layer (SSL) VPN configuration
- X.509 certificates
- Microsoft Windows Server
- Linux/OpenSSL

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Adaptive Security Appliance software, version 8.4 and later
- Microsoft Windows 7 with Cisco AnyConnect Secure Mobility Client, Release 3.1
- Microsoft Server 2012 R2
- Linux with OpenSSL 1.0.0j or later

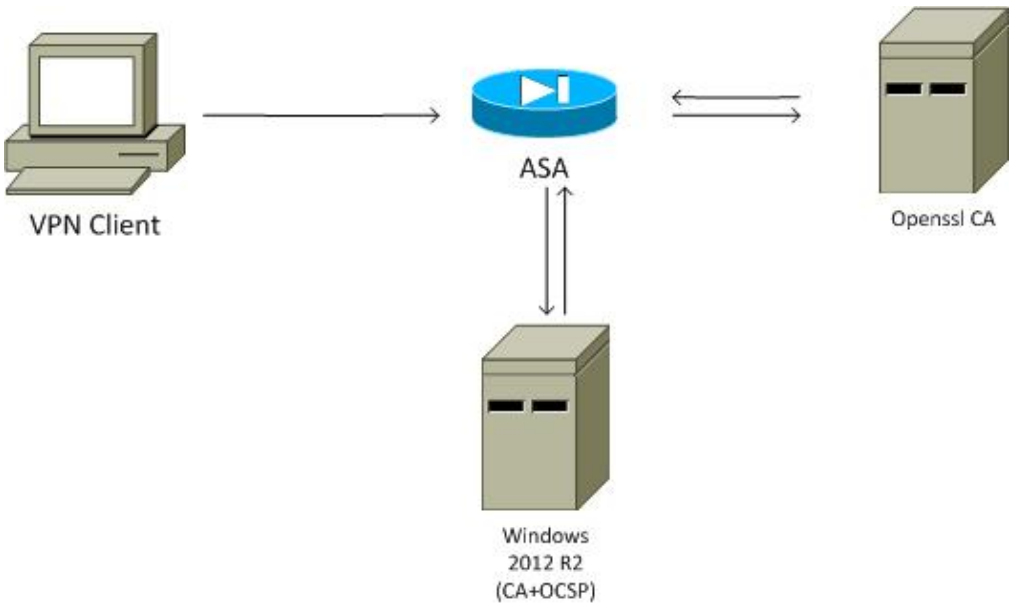
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

Note: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

Network Diagram

The client uses remote access VPN. This access can be Cisco VPN Client (IPSec), Cisco AnyConnect Secure Mobility (SSL/Internet Key Exchange Version 2 [IKEv2]), or WebVPN (portal). In order to log in, the client provides the correct certificate, as well as the username/password that were configured locally on the ASA. The client certificate is validated via the OCSP server.



ASA Remote Access with OCSP

The ASA is configured for SSL access. The client is using AnyConnect in order to login. The ASA uses Simple Certificate Enrollment Protocol (SCEP) in order to request the certificate:

```
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
```

A certificate map is created in order to identify all users whose subject−name contains the word administrator (case insensitive). Those users are bound to a tunnel−group named 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
```

The VPN configuration requires successful authorization (that is, a validated certificate). It also requires the correct credentials for the locally defined username (authentication 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
```

Microsoft Windows 2012 CA

Note: See Cisco ASA 5500 Series Configuration Guide using the CLI, 8.4 and 8.6: Configuring an External Server for Security Appliance User Authorization for details on configuration of the ASA through the CLI.

Services Installation

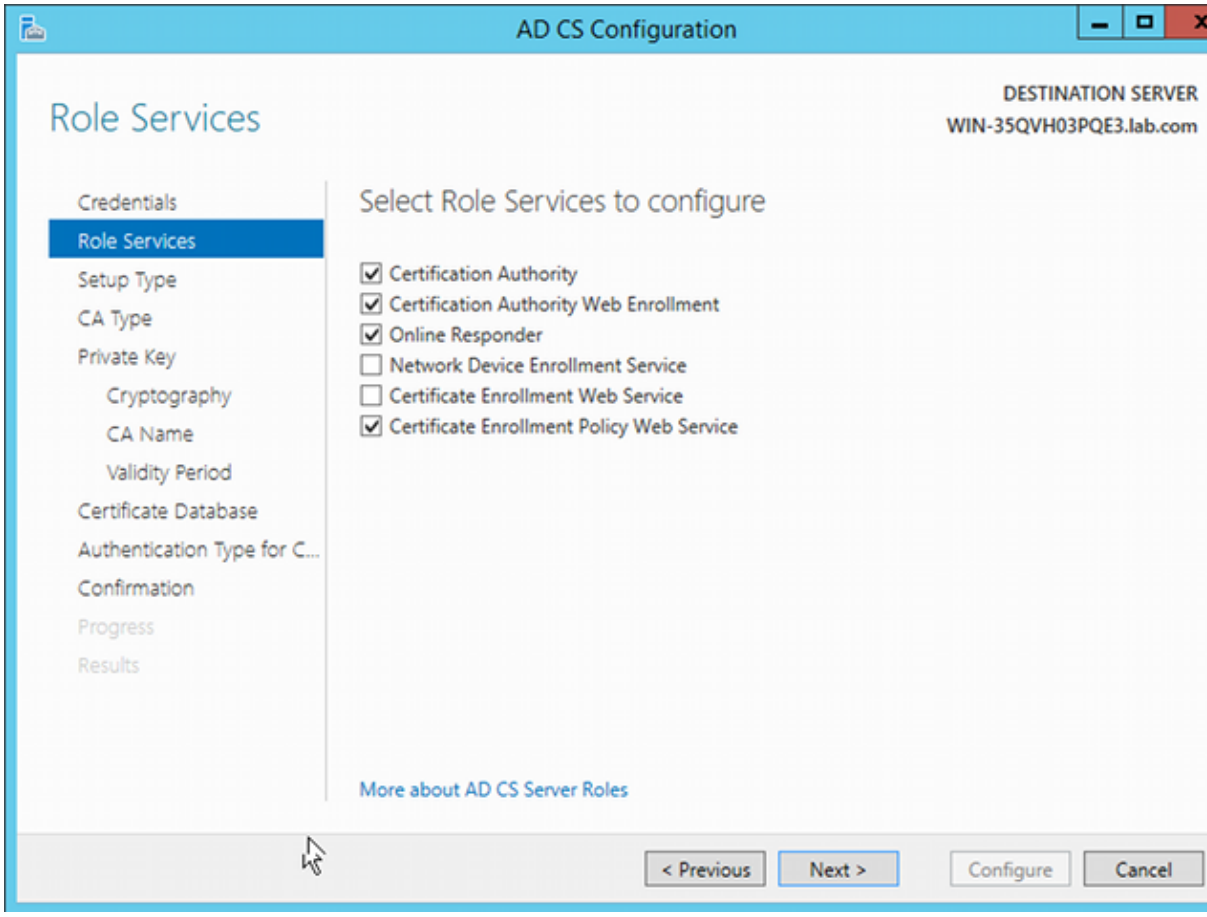
This procedure describes how to configure role services for the Microsoft server:

1. Navigate to ***Server Manager*** > ***Manage*** > ***Add Roles and Features***. The Microsoft server needs these role services:

   · Certification Authority
   · Certification Authority Web Enrollment, which is used by the client
   · Online Responder, which is needed for OCSP

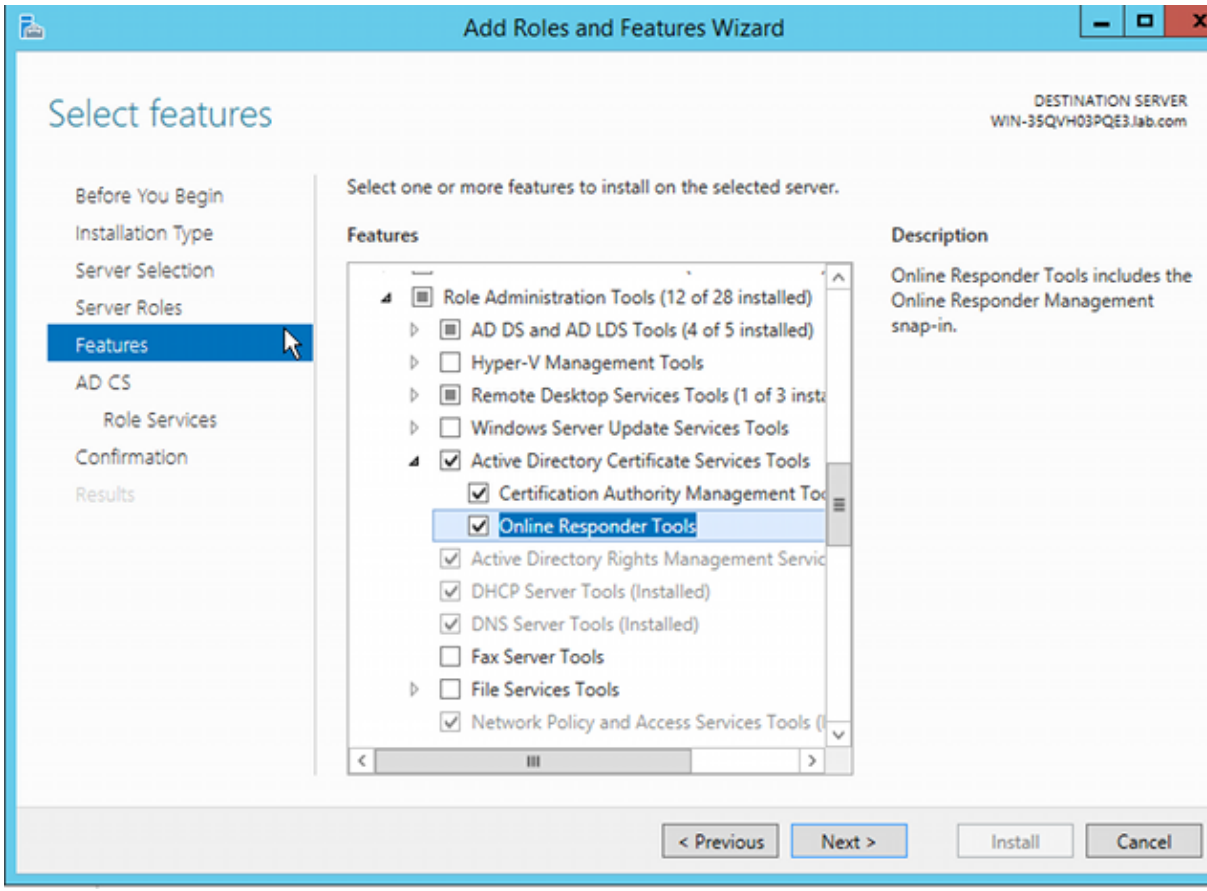
· Network Device Enrollment Service, which contains the SCEP application used by the ASA

Web service with policies can be added if needed.



It is not possible to add all the roles at the same time; for example, Network Device Enrollment Service (NDES) must be added later.

2. When you add features, be sure to include Online Responder Tools because it includes an OCSP snap−in that is used later:



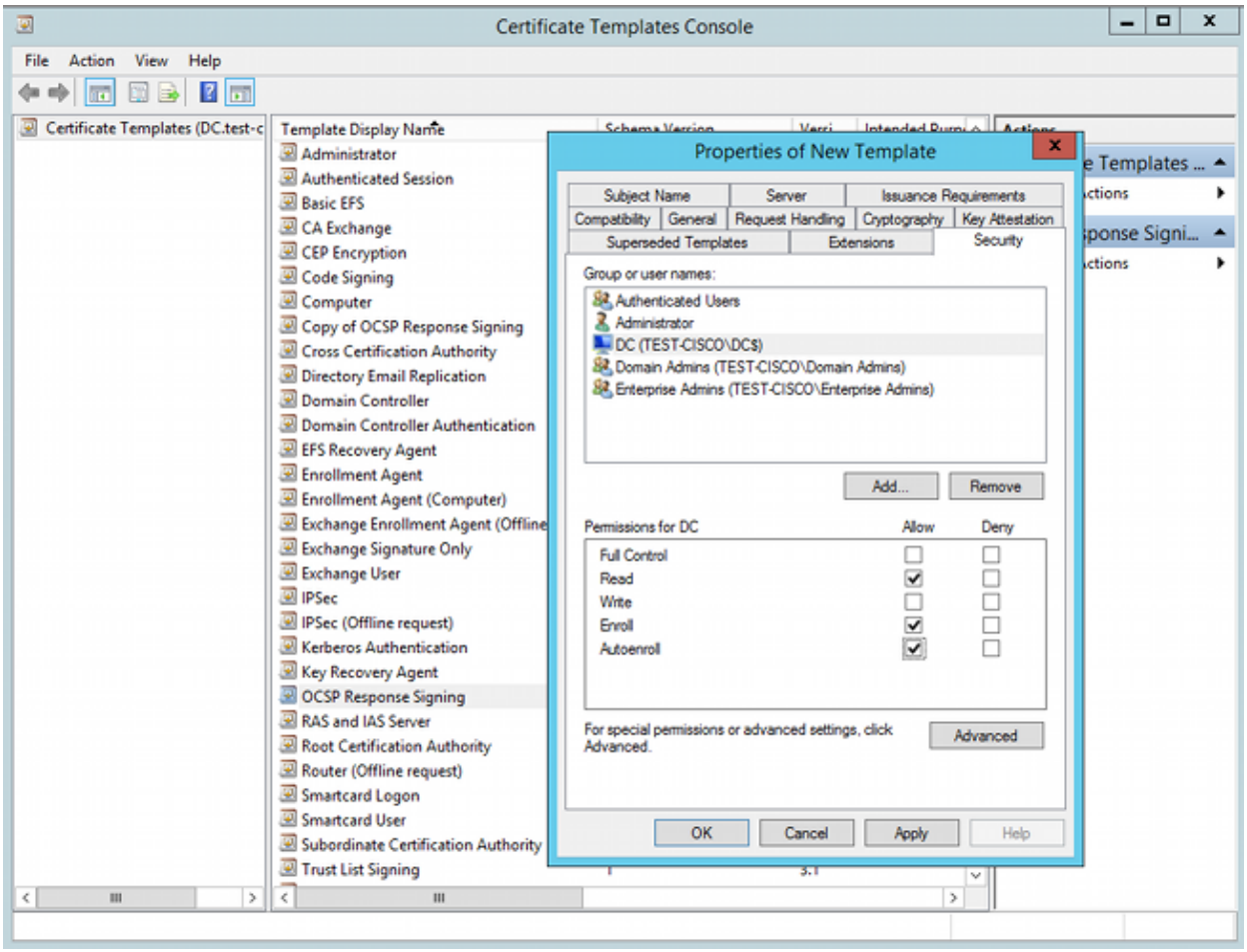
CA Configuration for OCSP Template

The OCSP service uses a certificate to sign the OCSP response. A special certificate on the Microsoft server must be generated and must include:

- Extended key usage = OCSP signing
- OCSP no revocation checking

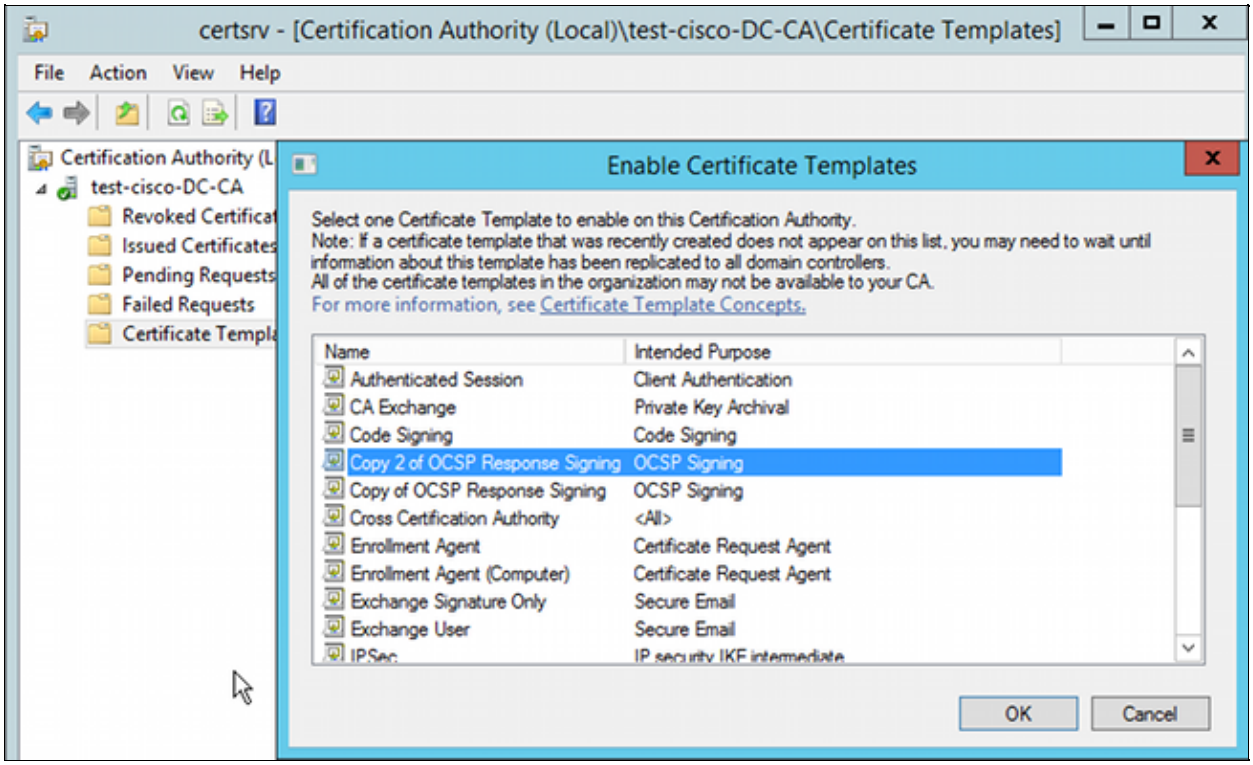
This certificate is needed in order to prevent OCSP validation loops. ASA does not use the OCSP service to try to check the certificate presented by the OCSP service.

1. Add a template for the certificate on the CA. Navigate to ***CA*** > ***Certificate Template*** > ***Manage***, select ***OCSP Response Signing***, and duplicate the template. View the properties for the newly created template, and click the ***Security*** tab. The permissions describe which entity is allowed to request a certificate that uses that template, so correct permissions are required. In this example, the entity is the OCSP service that is running on the same host (TEST−CISCO\DC), and the OCSP service needs Autoenroll privileges:



All other settings for the template can be set to default.

2. Activate the template. Navigate to ***CA*** > ***Certificate Template*** > ***New*** > ***Certificate Template to Issue***, and select the duplicate template:

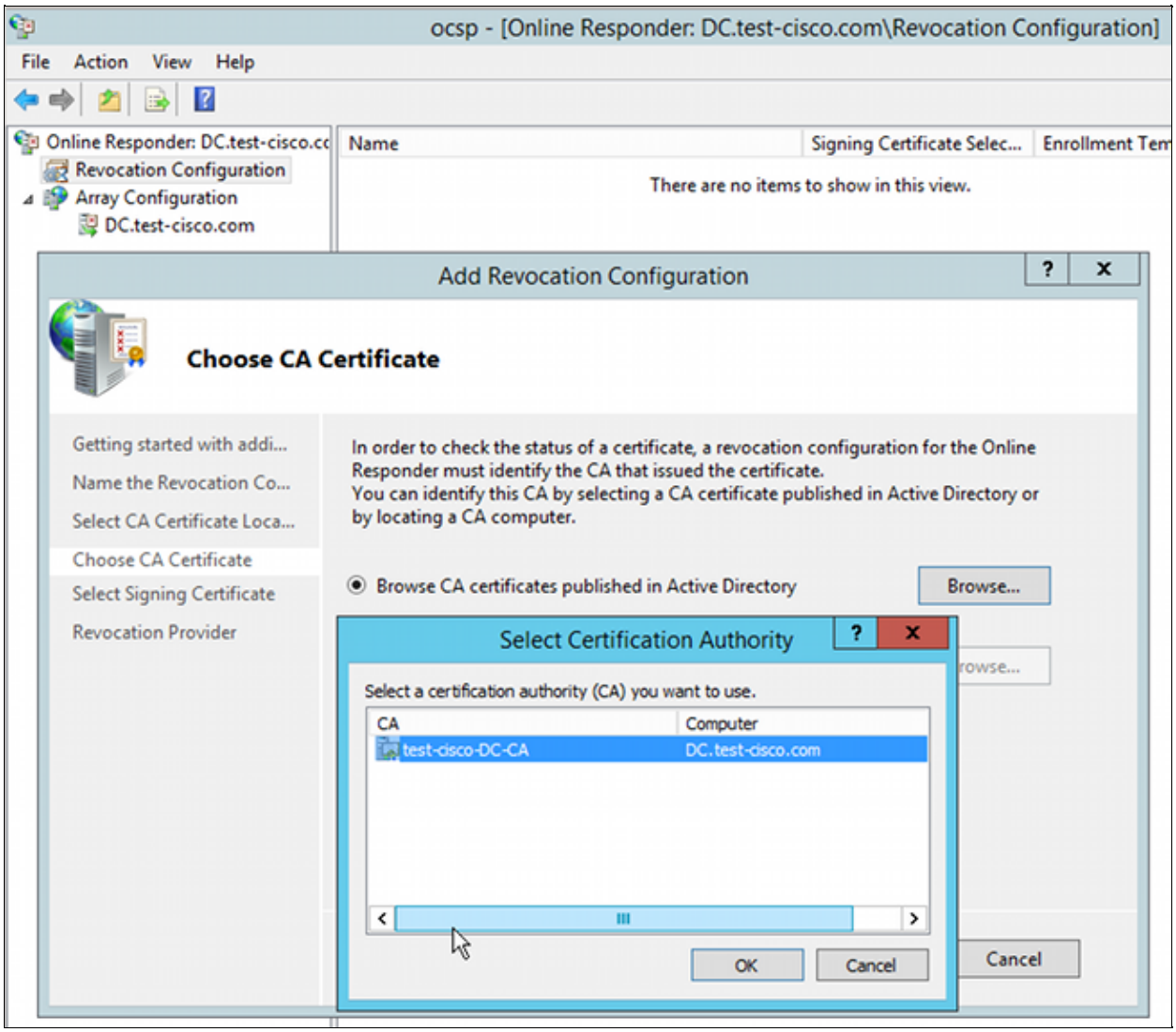


OCSP Service Certificate

This procedure describes how to use Online Configuration Management in order to configure OCSP:

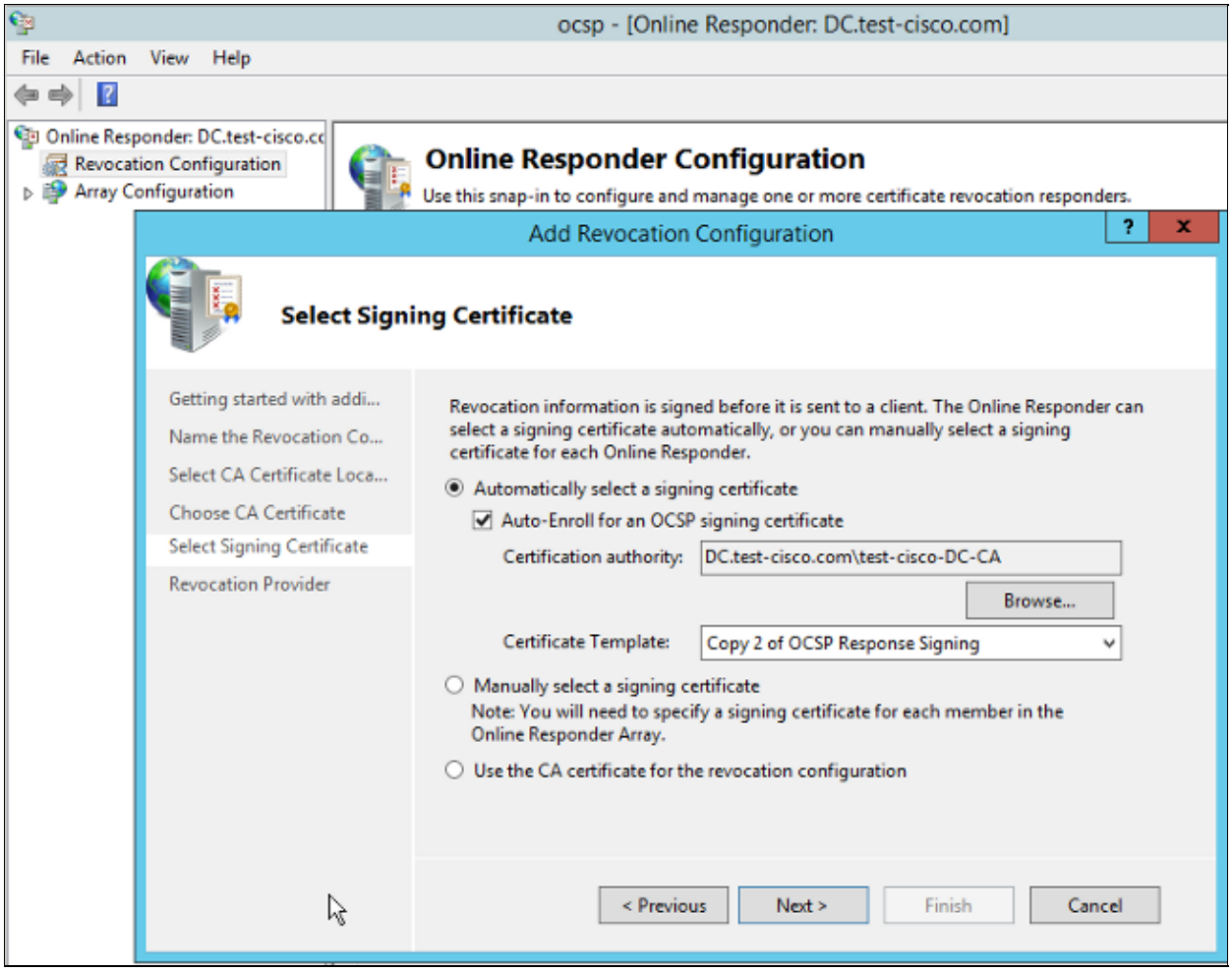
1. Navigate to ***Server Manager*** > ***Tools***.

2. Navigate to ***Revocation Configuration*** > ***Add Revocation Configuration*** in order to add a new configuration:

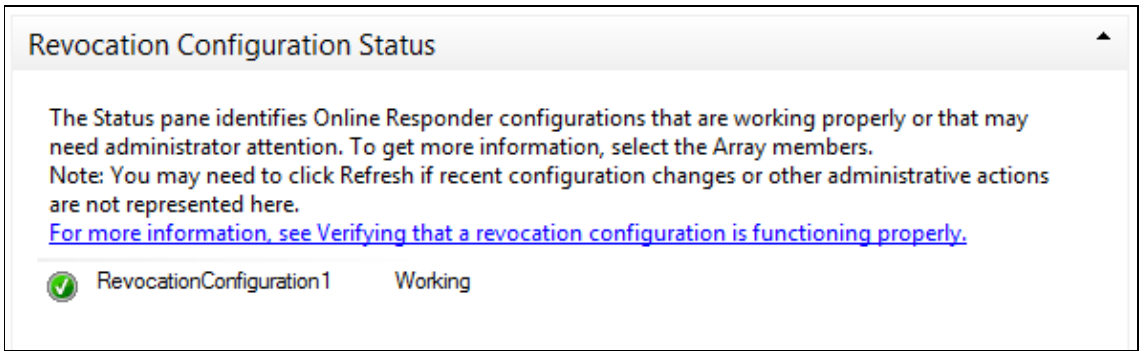


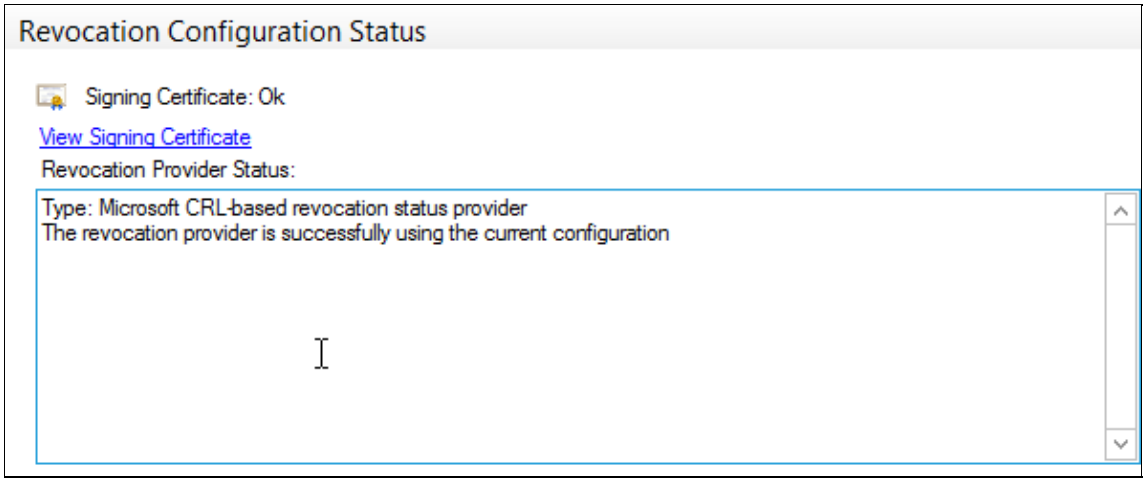
   OCSP can use the same Enterprise CA. The certificate for OCSP service is generated.

3. Use the selected Enterprise CA, and choose the template created earlier. The certificate is enrolled automatically:

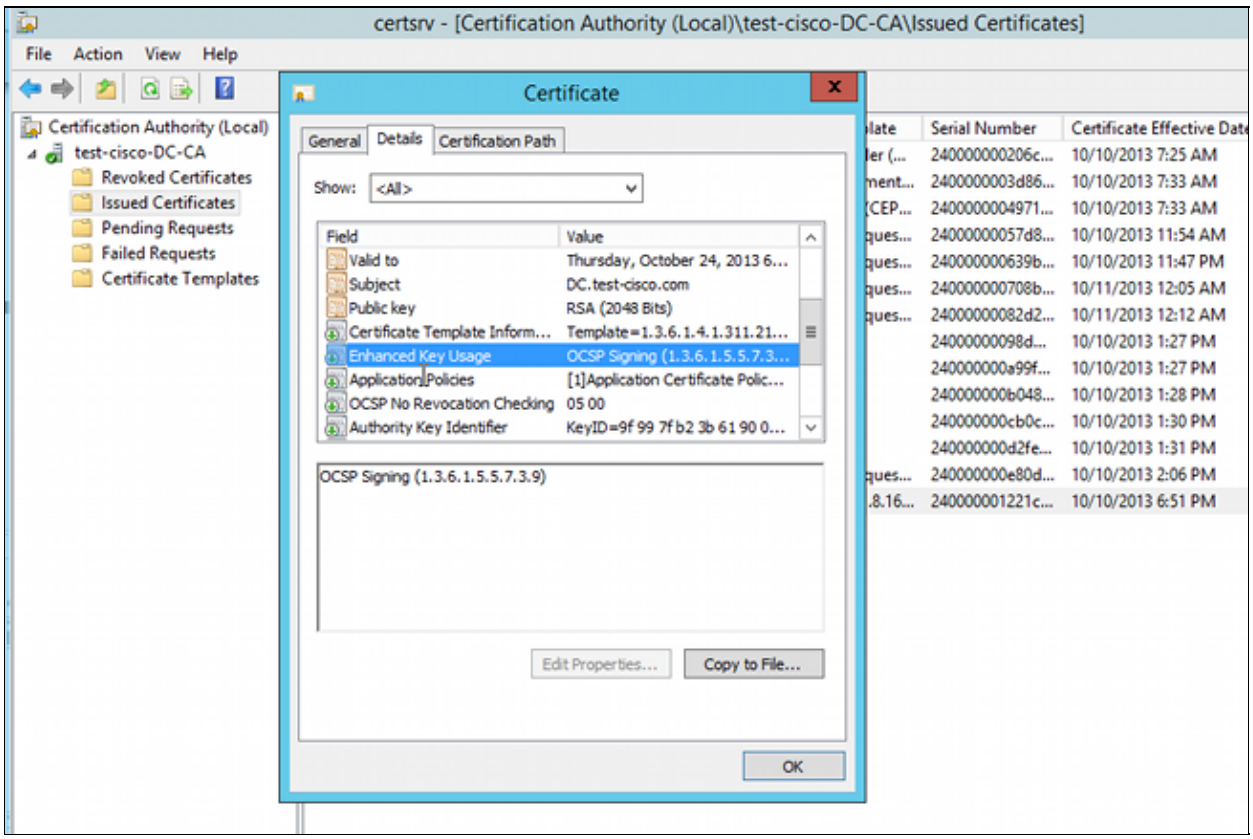


4. Confirm that the certificate is enrolled and its status is Working/OK:





5. Navigate to ***CA*** > ***Issued Certificates*** in order to verify the certificate details:

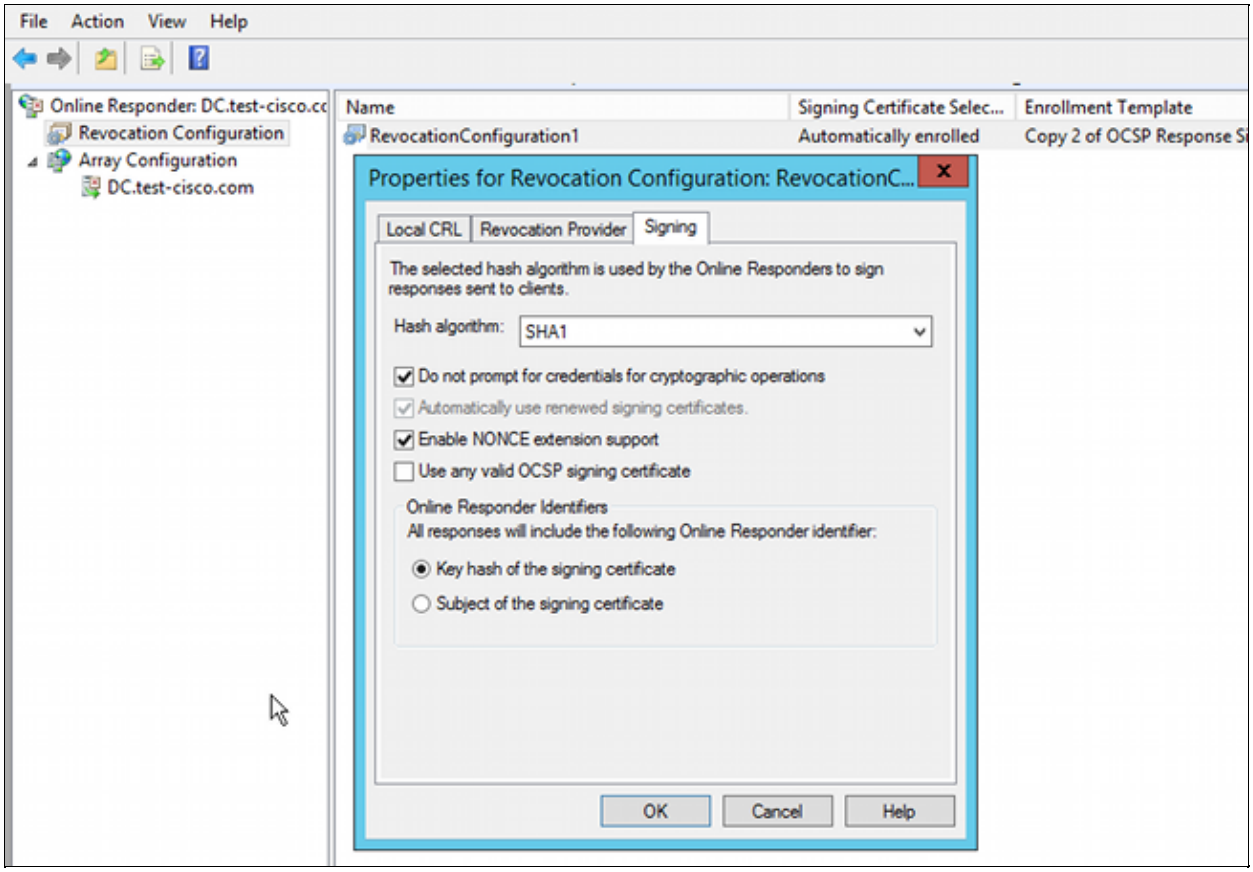


OCSP Service Nonces

Microsoft implementation of OCSP is compliant with RFC 5019 The Lightweight Online Certificate Status Protocol (OCSP) Profile for High−Volume Environments , which is a simplified version of RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol − OCSP .

The ASA uses RFC 2560 for OCSP. One of the differences in the two RFCs is that RFC 5019 does not accept signed requests sent by ASA.

It is possible to force the Microsoft OCSP service to accept those signed requests and reply with the correct signed response. Navigate to ***Revocation Configuration*** > ***RevocationConfiguration1*** > ***Edit Properties***, and select the option to ***Enable NONCE extension support***.



The OCSP service is now ready to use.

Although Cisco does not recommend this, nonces can be disabled on the ASA:

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

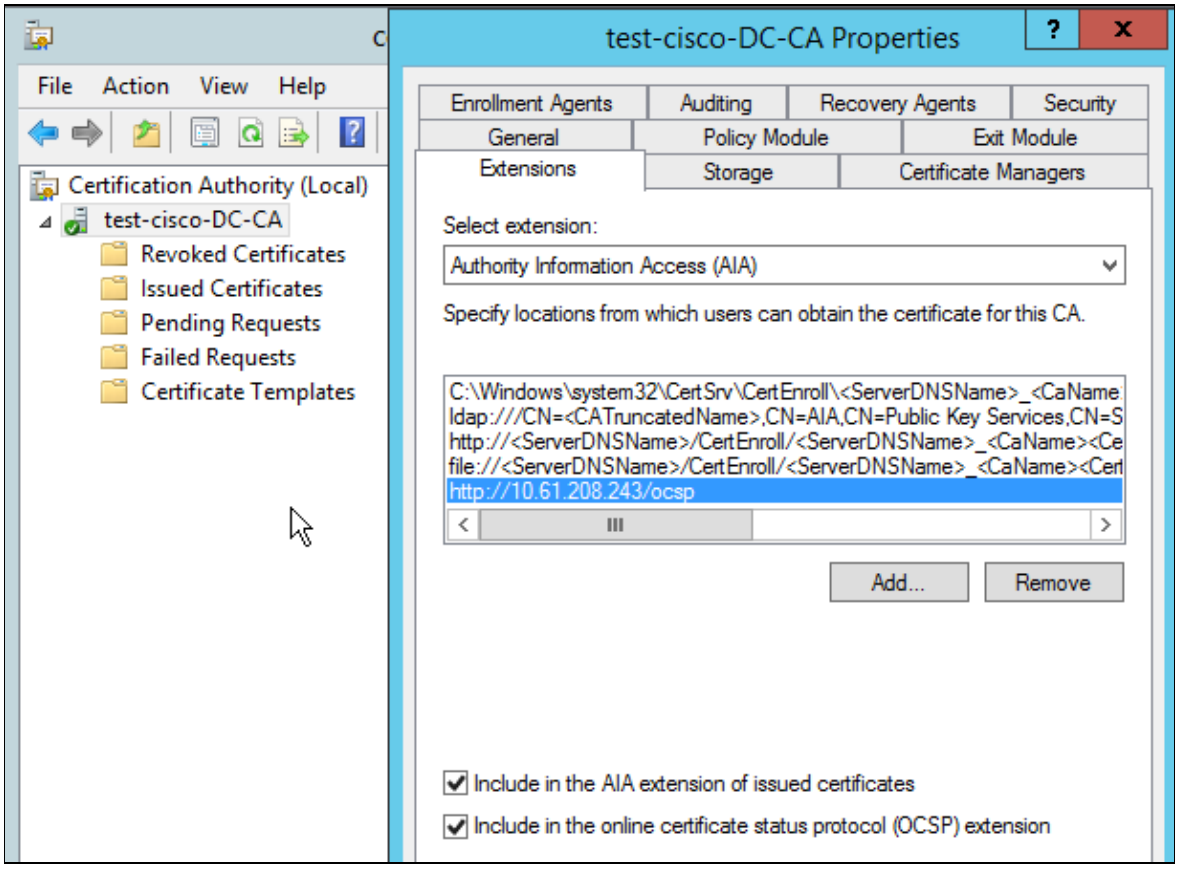
CA Configuration for OCSP Extensions

You must now reconfigure the CA to include the OCSP server extension in all issued certificates. The URL from that extension is used by ASA in order to connect to the OCSP server when a certificate is validated.

1. Open the Properties dialog box for the server on the CA.

2. Click the ***Extensions*** tab. The Authority Information Access (AIA) extension that points to the OCSP service is needed; in this example, it is http://10.61.208.243/ocsp. Enable both of these options for the AIA extension:

   - Include in the AIA extension of issued certificates
   - Include in the online certificate status protocol (OCSP) extension



This ensures that all issued certificates have a correct extension that points to the OCSP service.

OpenSSL

Note: See Cisco ASA 5500 Series Configuration Guide using the CLI, 8.4 and 8.6: Configuring an External Server for Security Appliance User Authorization for details on configuration of the ASA through the CLI.

This example assumes that the OpenSSL server is already configured. This section describes only the OCSP configuration and changes that are needed for CA configuration.

This procedure describes how to generate the OCSP certificate:

1. These parameters are needed for the OCSP responder:

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

2. These parameters are needed for user certificates:

```
[ UserCerts ]
authorityInfoAccess = OCSP;URI:http://10.61.208.243
```

3. Certificates need to be generated and signed by the CA.

4. Start the OCSP server:

```
openssl ocsp –index ourCAwebPage/index.txt –port 80 –rsigner
```

```
ocspresponder.crt −rkey ocspresponder.key −CA cacert.crt −text −out
log.txt
```

5. Test the example certificate:

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

More examples are available on the OpenSSL web site .

OpenSSL, like ASA, supports OCSP nonces; the nonces can be controlled with use of the −nonce and −no_nonce switches.

ASA with Multiple OCSP Sources

The ASA can override the OCSP URL. Even if the client certificate contains an OCSP URL, it is overwritten by the configuration on the 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
```

The OCSP server address can be defined explicitly. This command example matches all certificates with administrator in subject name, uses an OPENSSL trustpoint in order to validate OCSP signature, and uses the URL of http://11.11.11.11/ocsp in order to send the request:

```
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
```

The order used to find OCSP URL is:

1. An OCSP server you set with the ***match certificate*** command
2. An OCSP server you set with the ***ocsp url*** command
3. The OCSP server in the AIA field of the client certificate

ASA with OCSP Signed by Different CA

An OCSP response can be signed by a different CA. In such a case, it is necessary to use the ***match certificate*** command in order to use a different trustpoint on the ASA for OCSP certificate validation.

```
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
```

In this example, the ASA uses the OCSP URL rewrite for all certificates with a subject−name that contains administrator. The ASA is forced to validate the OCSP responder certificate against another trustpoint, OPENSSL. User certificates are still validated in the WIN2012 trustpoint.

Since the OCSP responder certificate has the 'OCSP no revocation checking' extension, the certificate is not verified, even when OCSP is forced to validate against the OPENSSL trustpoint.

By default, all trustpoints are searched when the ASA is trying to verify the user certificate. Validation for the OCSP responder certificate is different. The ASA searches only the trustpoint that has already been found for the user certificate (WIN2012 in this example).

Thus, it is necessary to use the ***match certificate*** command in order to force the ASA to use a different trustpoint for OCSP certificate validation (OPENSSL in this example).

User certificates are validated against the first matched trustpoint (WIN2012 in this example), which then determines the default trustpoint for OCSP responder validation.

If no specific trustpoint is provided in the ***match certificate*** command, the OCSP certificate is validated against the same trustpoint as the user certificates (WIN2012 in this example).:

```
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
```

Verify

Use this section to confirm that your configuration works properly.

Note: The Output Interpreter Tool (registered customers only) supports certain ***show*** commands. Use the Output Interpreter Tool in order to view an analysis of ***show*** command output.

ASA − Get Certificate via SCEP

This procedure describes how to obtain the certificate through use of SCEP:

1. This is the trustpoint authentication process to get the CA certificate:

```
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

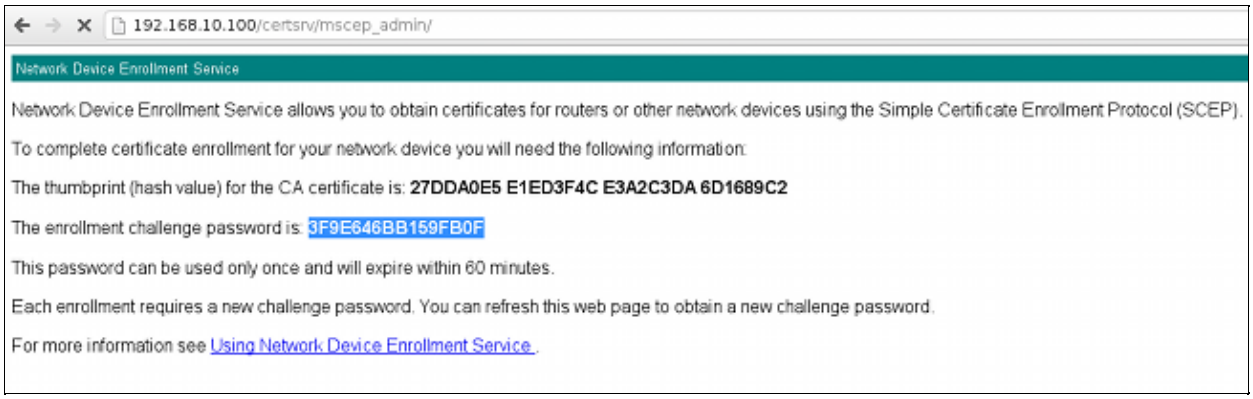
INFO: Certificate has the following attributes:
Fingerprint:     27dda0e5 e1ed3f4c e3a2c3da 6d1689c2
Do you accept this certificate? [yes/no]:

% Please answer 'yes' or 'no'.
```

```
Do you accept this certificate? [yes/no]:
yes
```

Trustpoint CA certificate accepted.

2. In order to request the certificate, the ASA needs to have a one−time SCEP password that can be obtained from the admin console at http://IP/certsrv/mscep_admin:



3. Use that password to request the certificate on the 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
```

Some output has been omitted for clarity.

4. Verify both the CA and ASA certificates:

```
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

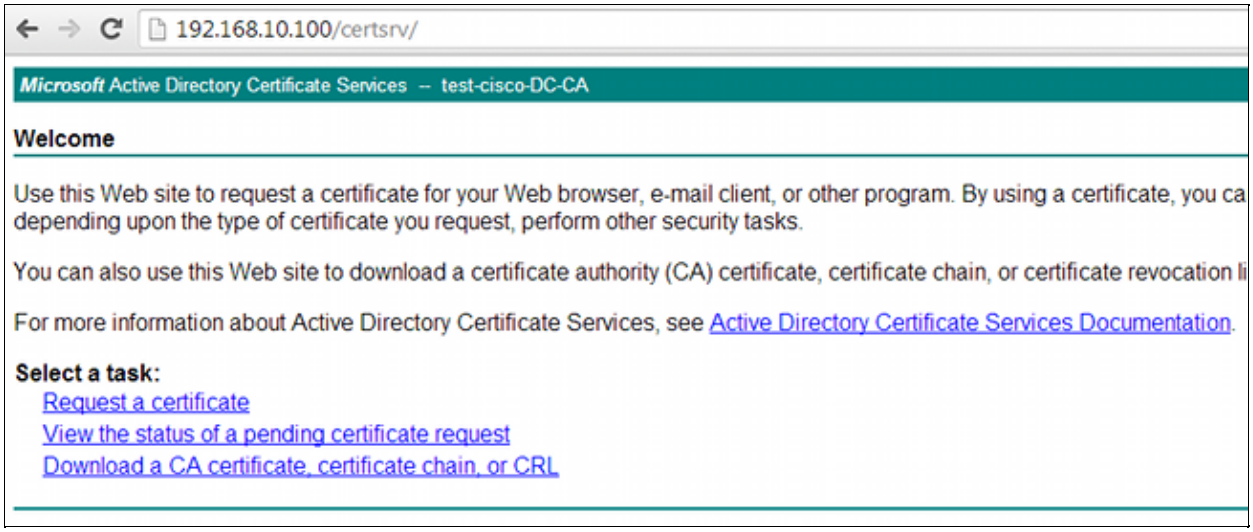
CA Certificate
  Status: Available
  Certificate Serial Number: 3d4c0881b04c799f483f4bbe91dc98ae
  Certificate Usage: Signature
  Public Key Type: RSA (2048 bits)
  Signature Algorithm: SHA1 with RSA Encryption
  Issuer Name:
    cn=test-cisco-DC-CA
    dc=test-cisco
    dc=com
  Subject Name:
    cn=test-cisco-DC-CA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

The ASA does not display most of the certificate extensions. Even though the ASA certificate contains the 'OCSP URL in AIA' extension, the ASA CLI does not present it. Cisco Bug ID CSCui44335, "ASA ENH Certificate x509 extensions displayed," requests this enhancement.

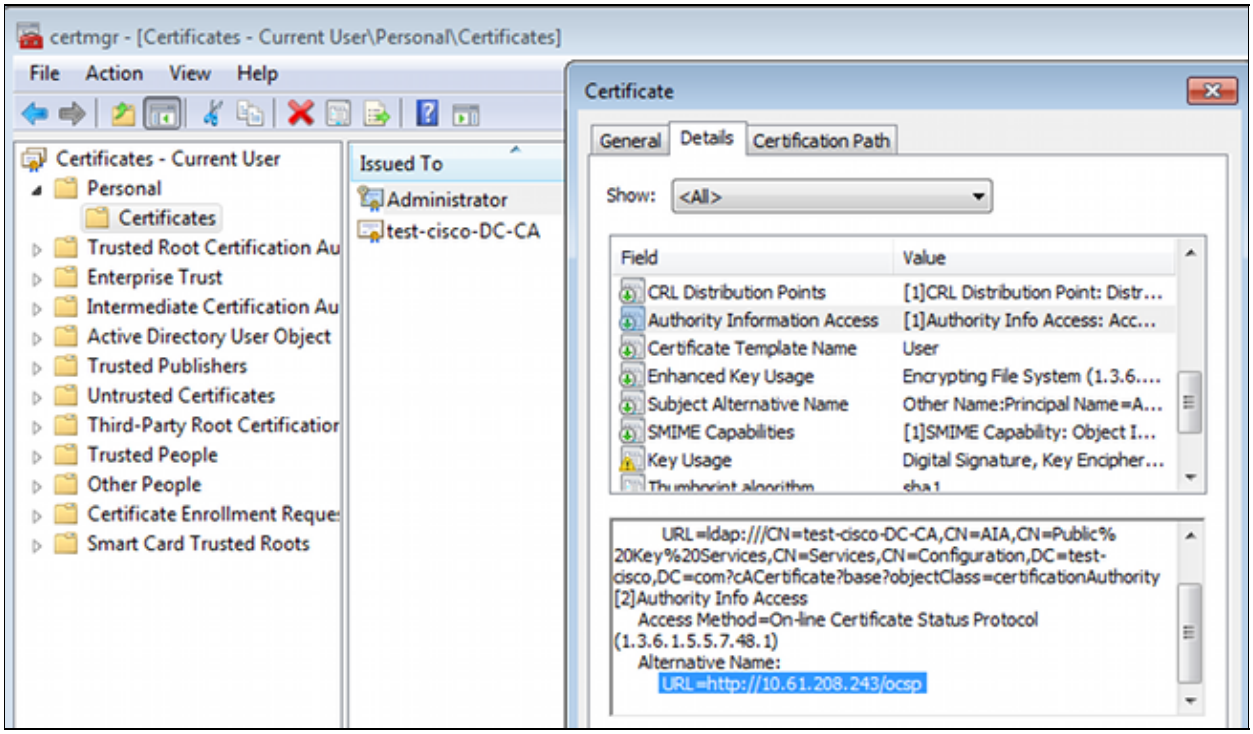
AnyConnect − Get Certificate via Web Page

This procedure describes how to obtain the certificate through use of the web browser on the client:

1. An AnyConnect user certificate can be requested through the webpage. On the client PC, use a web browser to go to the CA at http://*IP*/certsrv:



2. The user certificate can be saved in the web browser store, then exported to the Microsoft store, which is searched by AnyConnect. Use certmgr.msc in order to verify the received certificate:



AnyConnect can also request the certificate as long as there is a correct AnyConnect profile.

ASA VPN Remote Access with OCSP Validation

This procedure describes how to check OCSP validation:

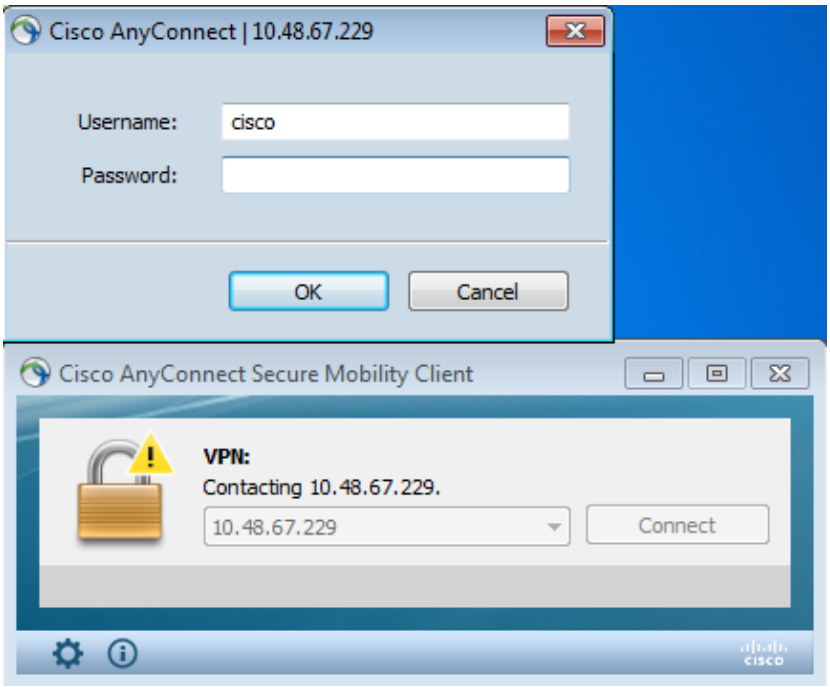
1. As it attempts to connect, the ASA reports that the certificate is being checked for OCSP. Here, the OCSP signing certificate has a no−check extension and has not been checked via OCSP:

```
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.
```

Some output has been omitted for clarity.

2. The end user provides the user credentials:



3. The VPN session is finished correctly:

```
%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. The session is created:

```
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. You can use detailed debugs for OCSP validation:

```
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

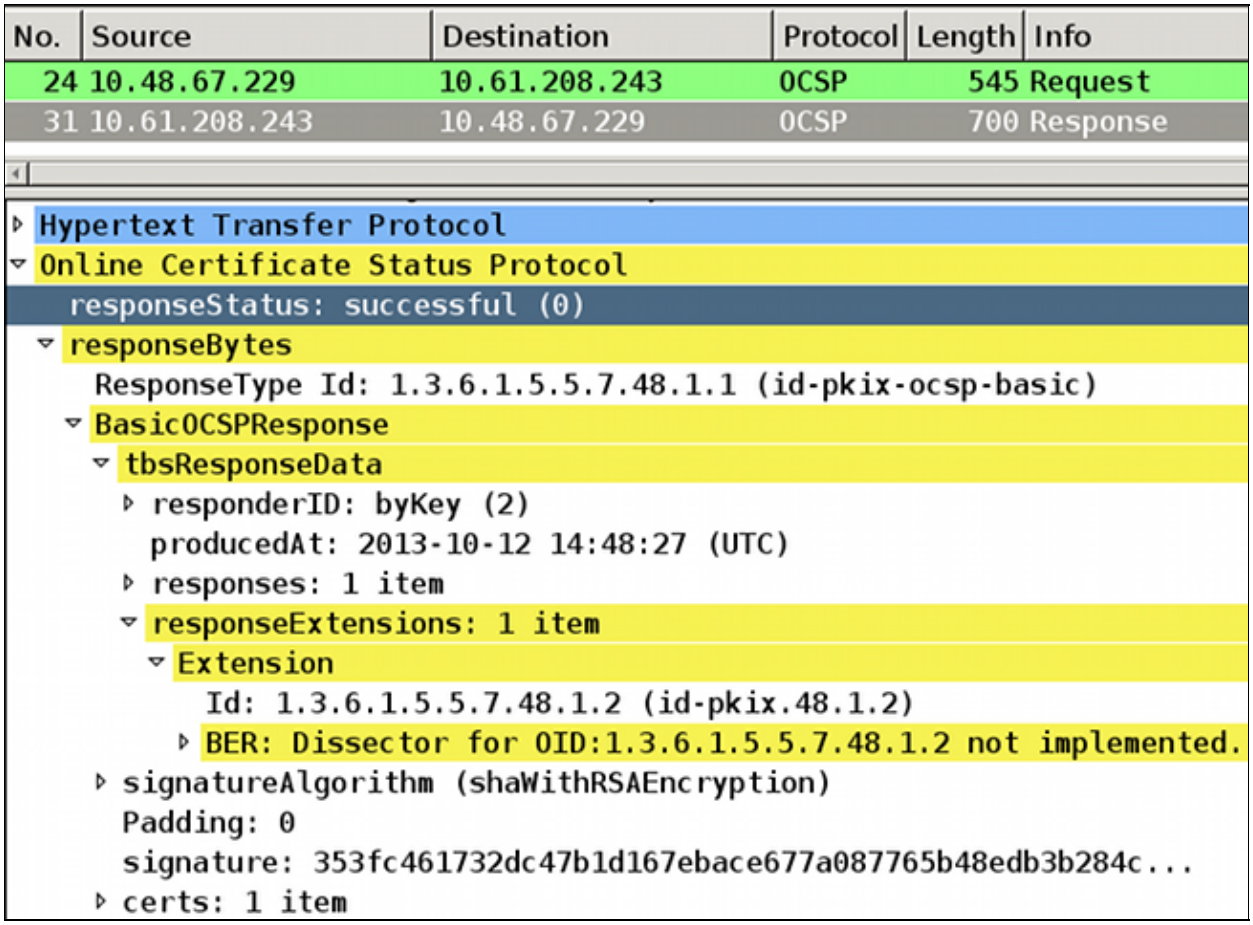
CERT-C: W ocsputil.c(538) : Error #708h
CERT-C: W ocsputil.c(538) : Error #708h

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. At the packet capture level, this is the OCSP request and correct OCSP response. The response includes the correct signature − nonce extension enabled on Microsoft OCSP:



ASA VPN Remote Access with Multiple OCSP Sources

If a match certificate is configured as explained in ASA with Multiple OCSP Sources, it takes precedence:

```
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
```

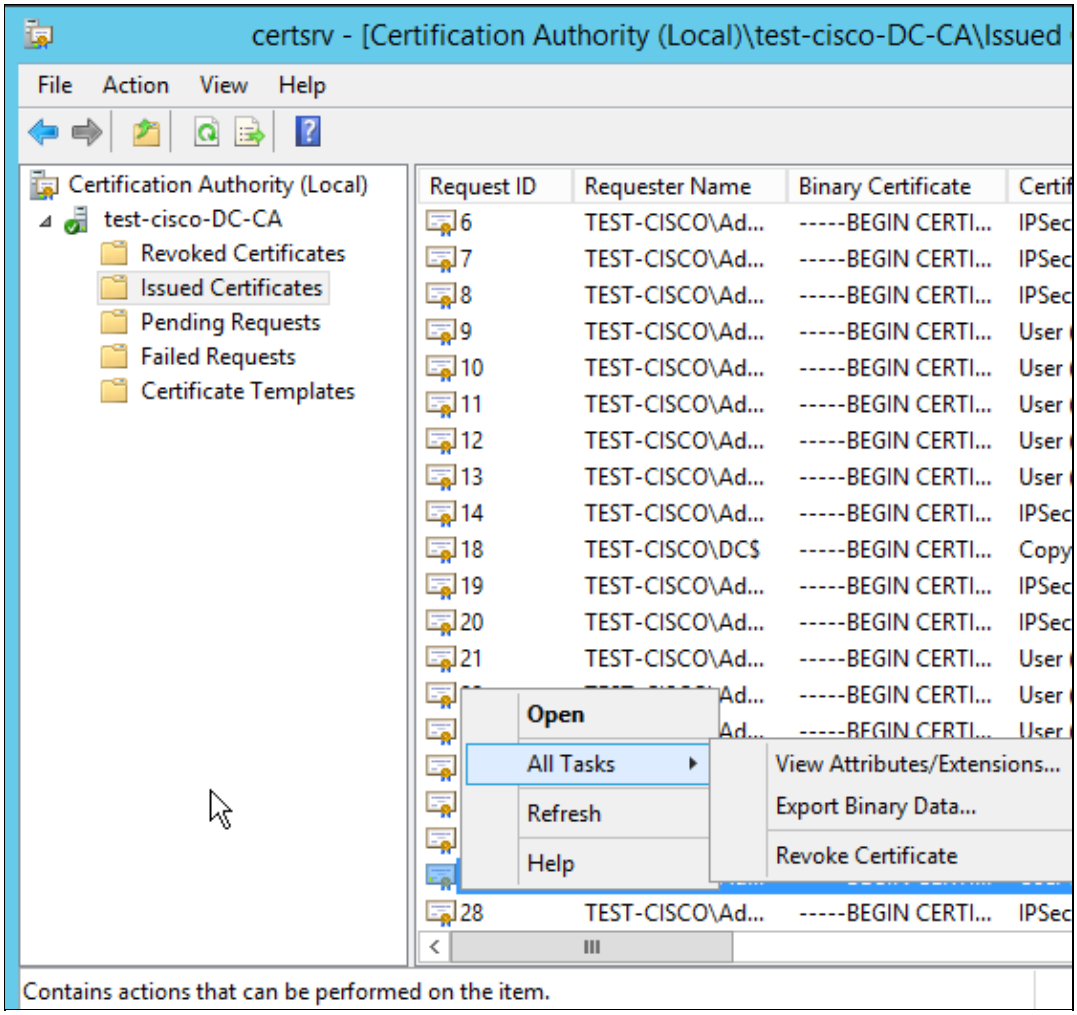
When an OCSP URL override is used, the debugs are:

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

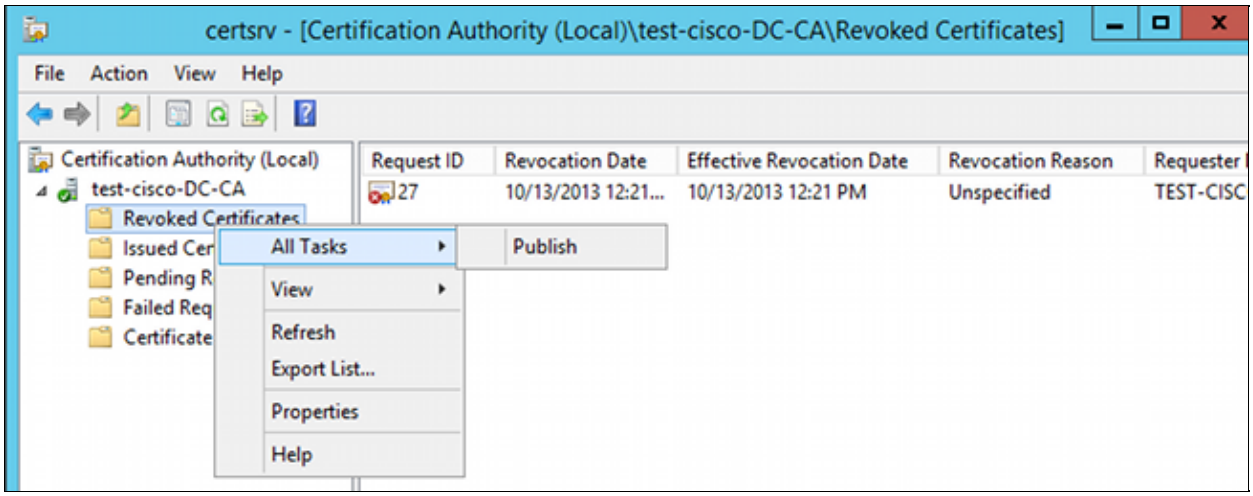
ASA VPN Remote Access with OCSP and Revoked Certificate

This procedure describes how to revoke the certificate and confirm the revoked status:

1. Revoke the client certificate:



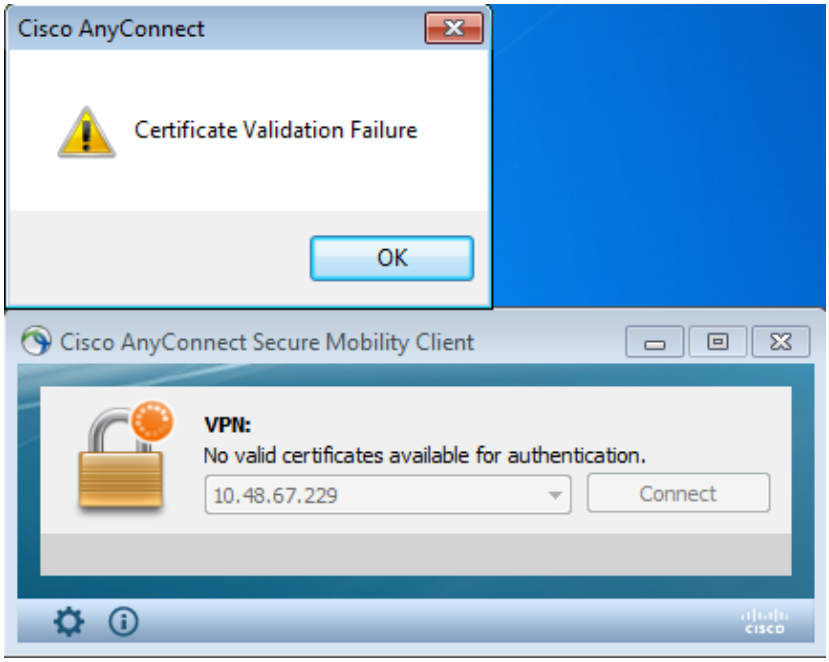
2. Publish the results:



3. [Optional] Steps 1 and 2 can also be done with the certutil CLI utility in Power Shell:

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

4. When the client tries to connect, there is a certificate validation error:



5. The AnyConnect logs also indicate the certificate validation error:

```
[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. The ASA reports the certificate status is revoked:

```
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

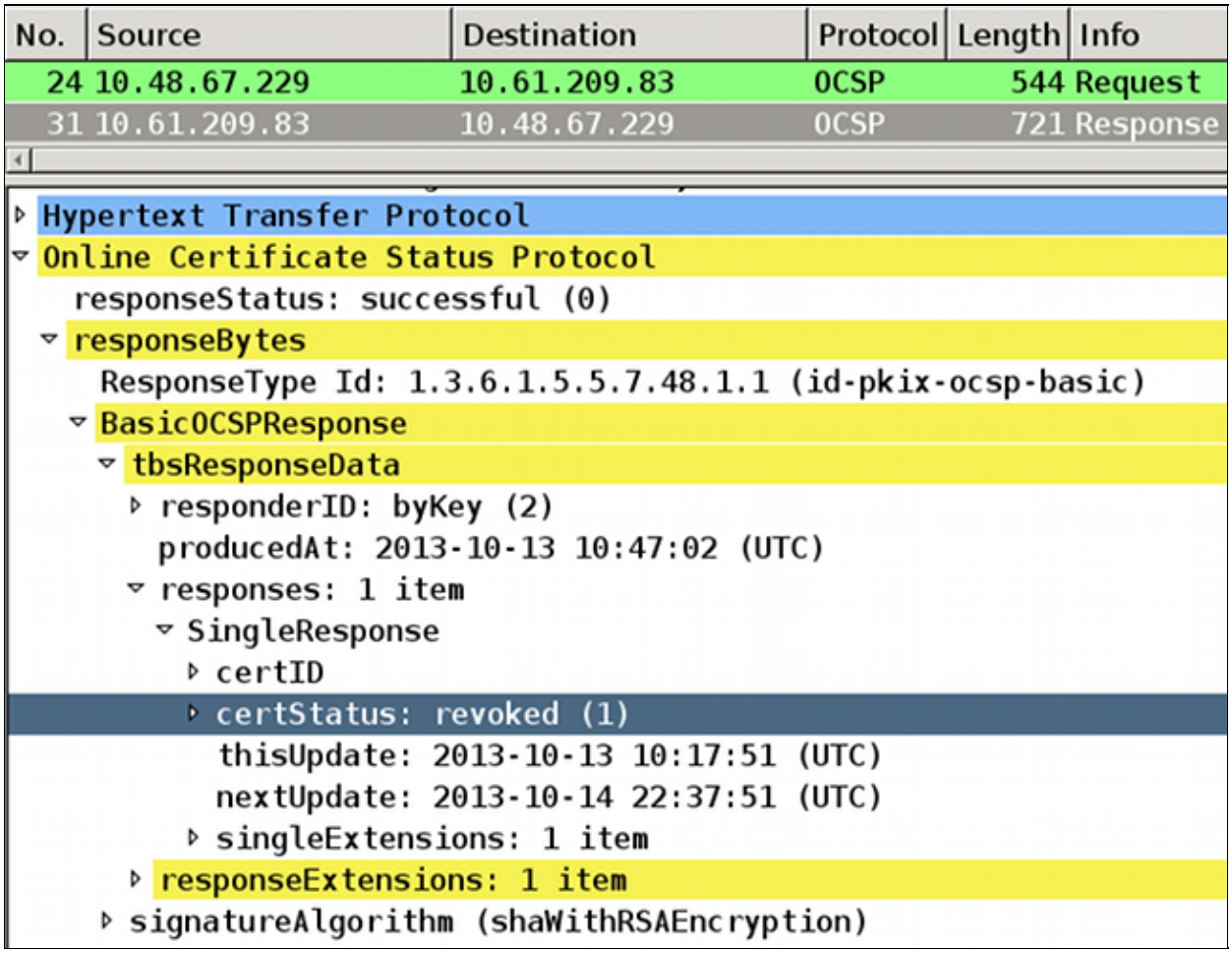
CRYPTO_PKI: transaction GetOCSP completed

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. The packet captures show a successful OCSP response with the certificate status of revoked:



Troubleshoot

This section provides information you can use to troubleshoot your configuration.

OCSP Server Down

ASA reports when the OCSP server is down:

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

Packet captures can also help with troubleshooting.

Time Not Synchronized

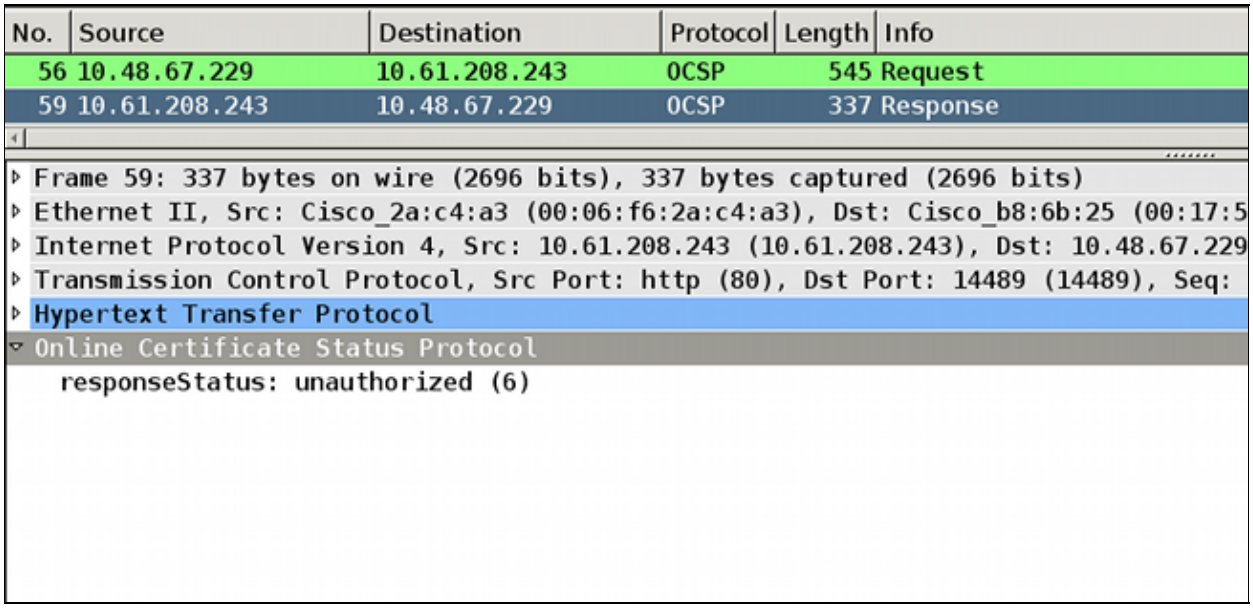
If the current time on OCSP server is older than on ASA (small differences are acceptable), the OCSP server sends an unauthorized response, and the ASA reports it:

```
CRYPTO_PKI: OCSP response status – unauthorized
```

When the ASA receives an OCSP response from future times, it also fails.

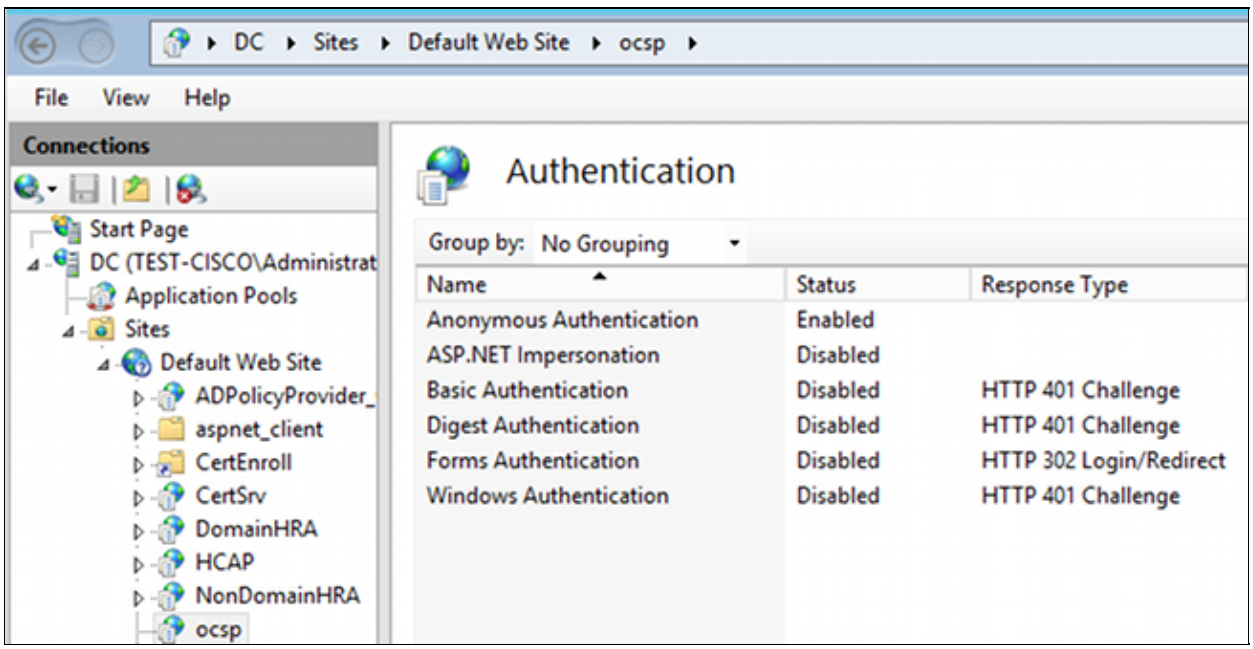
Signed Nonces Not Supported

If nonces on the server are not supported (which is the default on Microsoft Windows 2012 R2), an unauthorized response is returned:



IIS7 Server Authentication

Problems with an SCEP/OCSP request are often the result of incorrect authentication on Internet Information Services 7 (IIS7). Ensure that anonymous access is configured:



Related Information

- ***Microsoft TechNet: Online Responder Installation, Configuration, and Troubleshooting Guide***
- ***Microsoft TechNet: Configure a CA to Support OCSP Responders***

- ***Cisco ASA Series Command Reference***
- ***Technical Support & Documentation − Cisco Systems***

Updated: Nov 06, 2013 Document ID: 116720