Microsoft Windows 2012 및 OpenSSL에서 OCSP 확인을 사용하는 ASA Remote Access VPN

목차

소개

이 문서에서는 VPN 사용자가 제공한 인증서에 대해 Cisco ASA(Adaptive Security Appliance)에서 OCSP(Online Certificate Status Protocol) 검증을 사용하는 방법에 대해 설명합니다. 2개의 OCSP

서버(Microsoft Windows CA[Certificate Authority] 및 OpenSSL)에 대한 컨피그레이션의 예가 나와 있습니다. Verify(확인) 섹션에서는 패킷 레벨의 세부 플로우에 대해 설명하고 Troubleshoot(문제 해결) 섹션에서는 일반적인 오류 및 문제에 초점을 맞춥니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Adaptive Security Appliance CLI(command-line interface) 컨피그레이션 및 SSL(Secure Socket Layer) VPN 컨피그레이션
- X.509 인증서
- Microsoft Windows 서버
- Linux/OpenSSL

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Adaptive Security Appliance 소프트웨어, 버전 8.4 이상
- Microsoft Windows 7 및 Cisco AnyConnect Secure Mobility Client, 릴리스 3.1
- Microsoft Server 2012 R2
- Linux(OpenSSL 1.0.0j 이상)

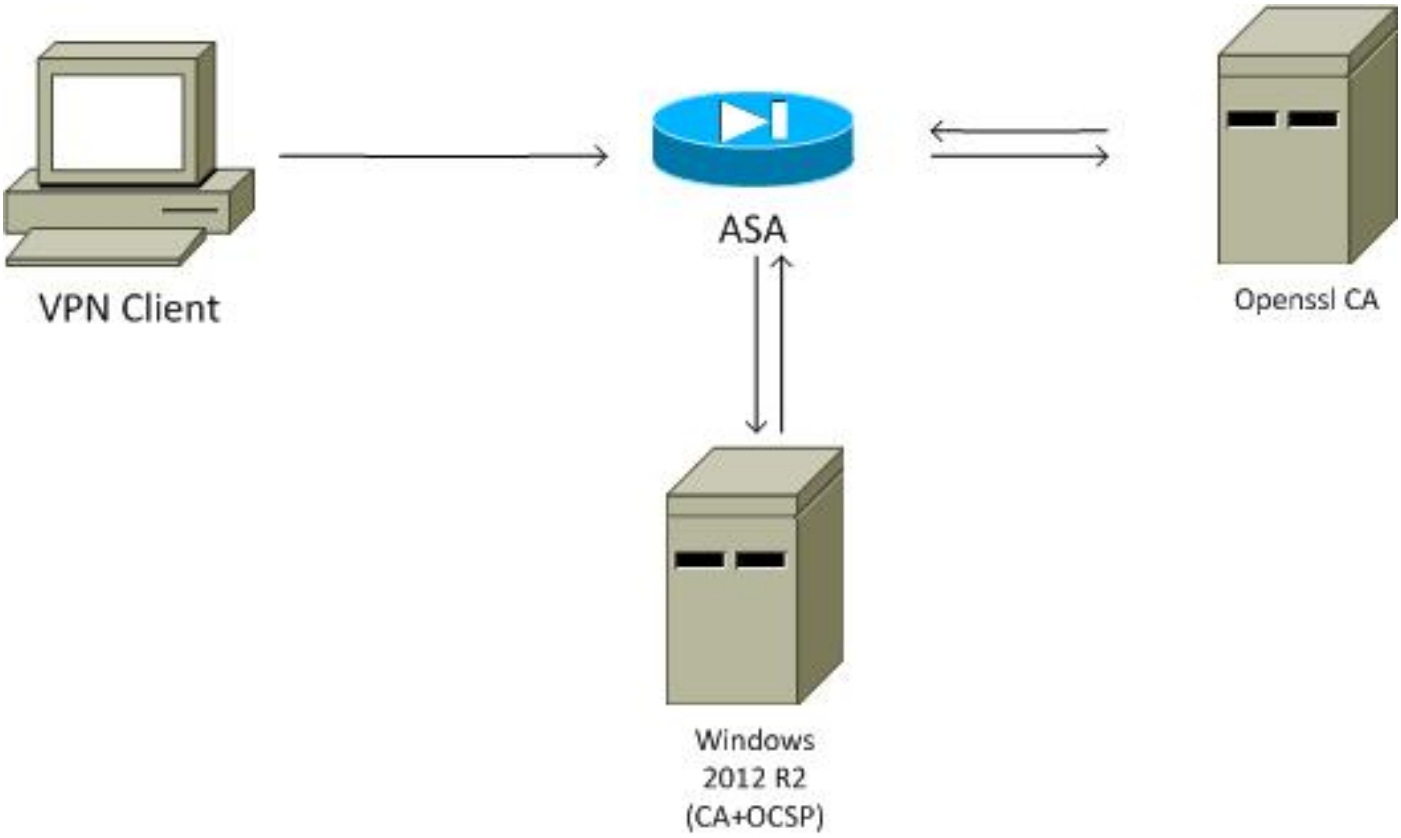
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

> **참고**: 이 섹션에서 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용하십시오.

네트워크 다이어그램

클라이언트는 원격 액세스 VPN을 사용합니다. 이 액세스는 Cisco VPN 클라이언트(IPSec), Cisco AnyConnect Secure Mobility(SSL/IKEv2(Internet Key Exchange Version 2)) 또는 WebVPN(포털)이 될 수 있습니다. 로그인하기 위해 클라이언트는 올바른 인증서와 ASA에서 로컬로 구성된 사용자 이름/비밀번호를 제공합니다. 클라이언트 인증서는 OCSP 서버를 통해 확인 됩니다.



OCSP를 사용하는 ASA 원격 액세스

ASA는 SSL 액세스를 위해 구성됩니다. 클라이언트가 로그인하기 위해 AnyConnect를 사용하고 있습니다. ASA는 인증서를 요청하기 위해 SCEP(Simple Certificate Enrollment Protocol)를 사용합니다.

```
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
```

주체 이름에 administrator라는 단어가 포함된 모든 사용자를 식별하기 위해 인증서 맵이 생성됩니다(대/소문자 구분 안 함). 이러한 사용자는 RA라는 터널 그룹에 바인딩됩니다.

```
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
```

VPN 컨피그레이션에는 성공적인 권한 부여(즉, 검증된 인증서)가 필요합니다. 또한 로컬로 정의된 사용자 이름(인증 aaa)에 대한 올바른 자격 증명이 필요합니다.

```
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

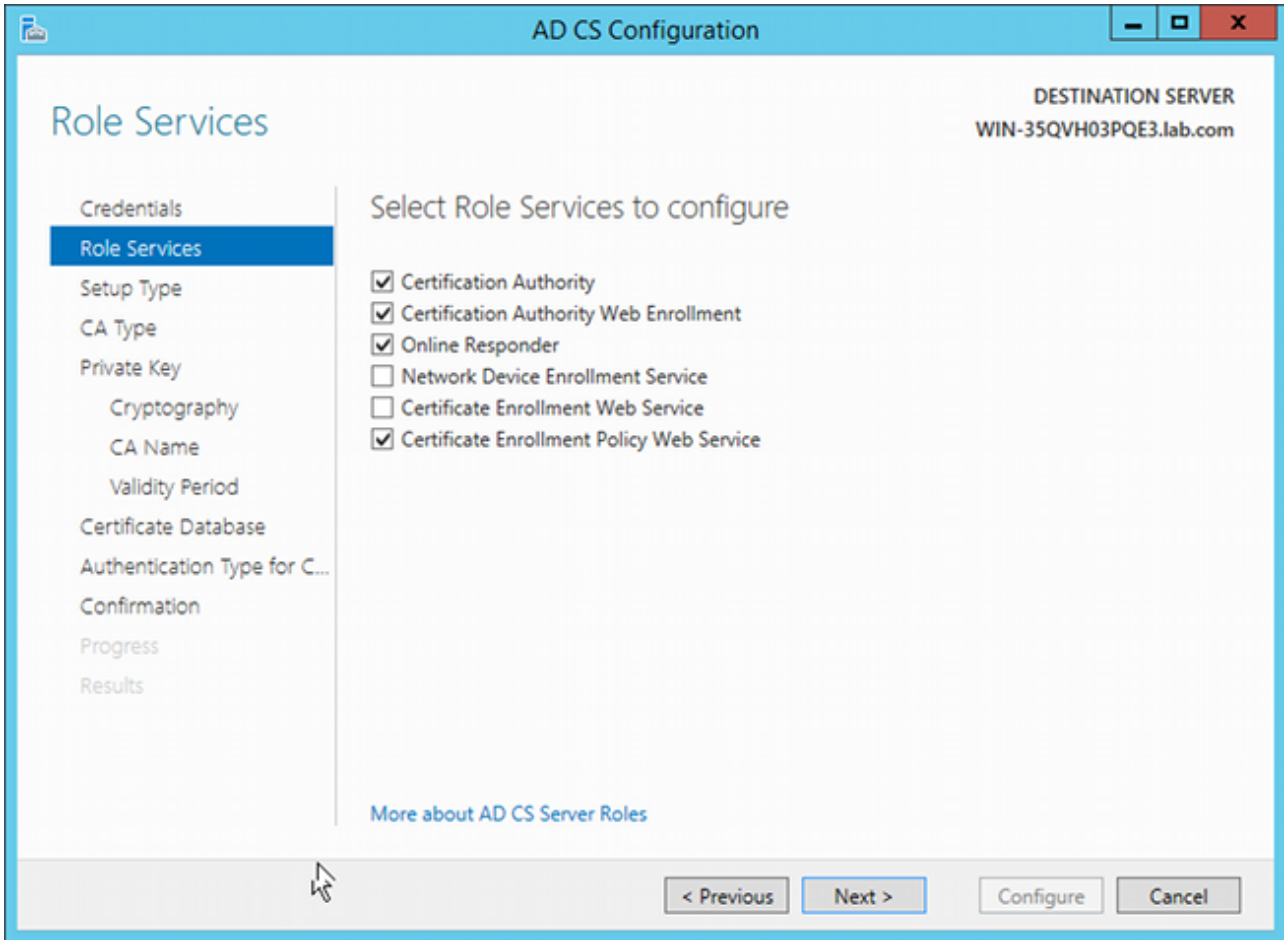
> **참고**: CLI를 통한 ASA 컨피그레이션에 대한 자세한 내용은 CLI, 8.4 및 8.6: Configuring an External Server for Security Appliance User Authorization을 사용하는 Cisco ASA 5500 Series 컨피그레이션 가이드를 참조하십시오.

서비스 설치

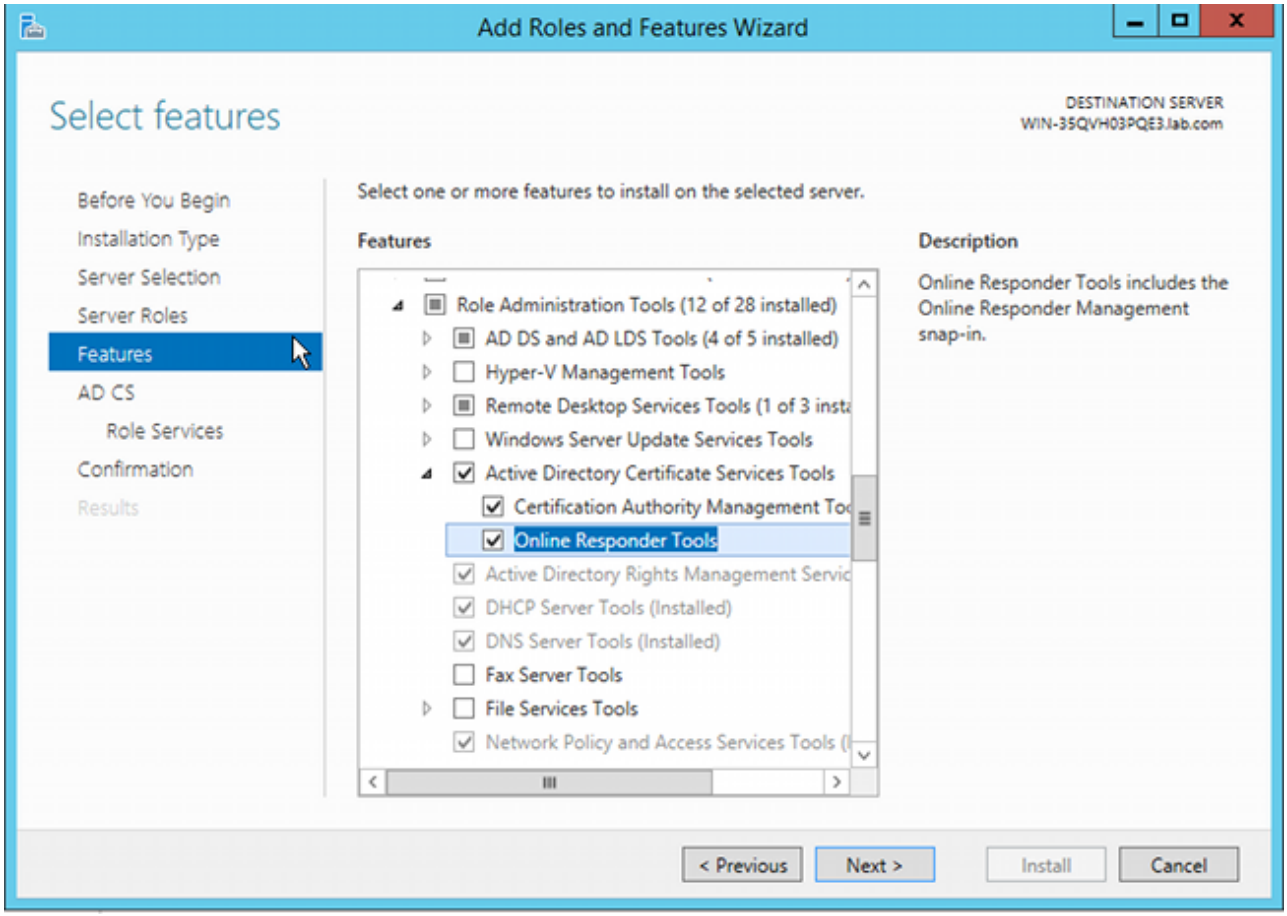
이 절차에서는 Microsoft 서버에 대해 역할 서비스를 구성하는 방법에 대해 설명합니다.

1. **Server Manager > Manage > Add Roles and Features로 이동합니다**. Microsoft 서버에는 다음과 같은 역할 서비스가 필요합니다.

   인증 기관클라이언트에서 사용하는 인증 기관 웹 등록OCSP에 필요한 온라인 응답기 ASA에서 사용하는 SCEP 애플리케이션이 포함된 네트워크 디바이스 등록 서비스 필요한 경우 정책이 포함된 웹 서비스를 추가할 수 있습니다.



2.
3.
4. 기능을 추가할 때 나중에 사용하는 OCSP 스냅인이 포함되어 있으므로 온라인 응답자 도구를 포함해야 합니다.



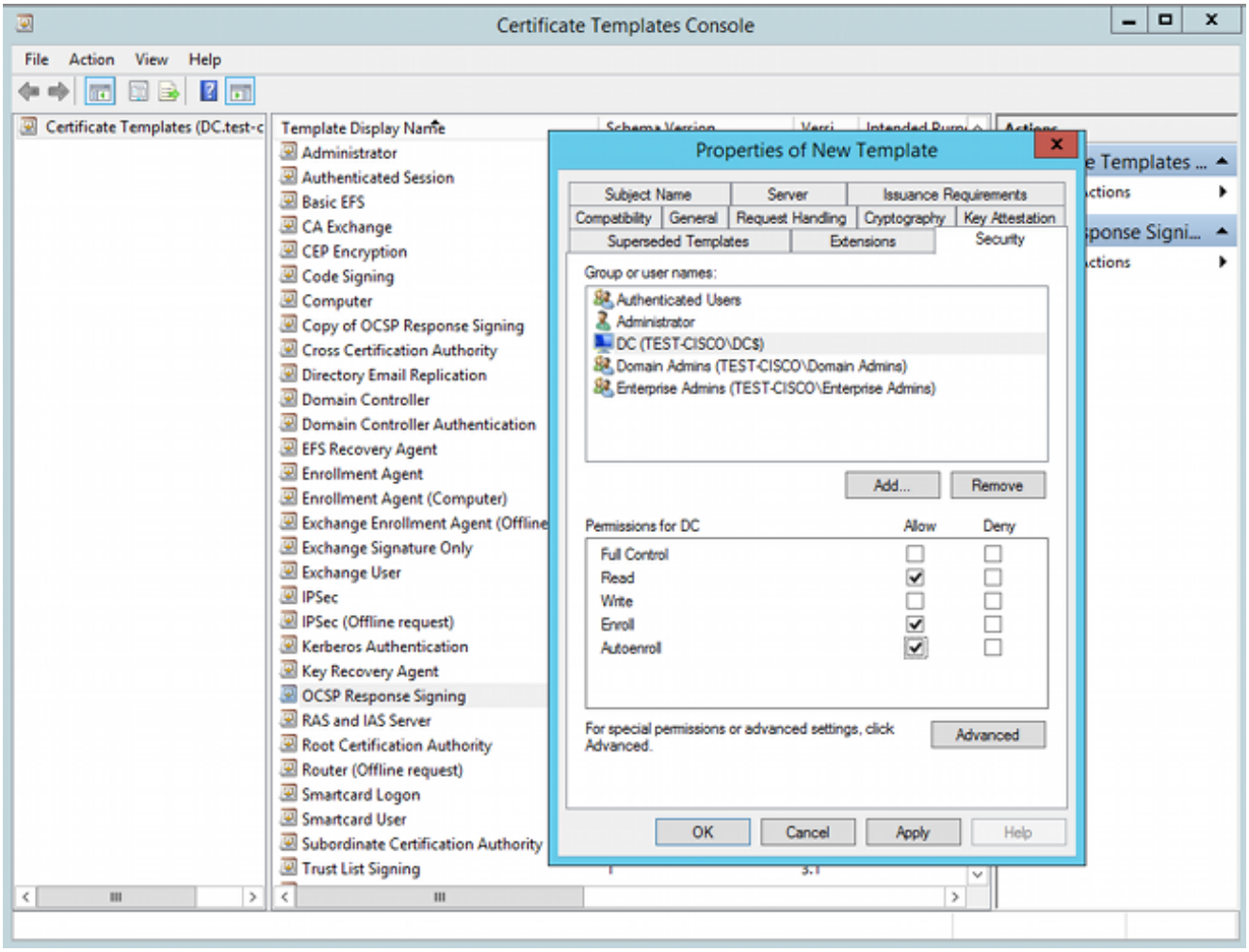
OCSP 템플릿에 대한 CA 컨피그레이션

OCSP 서비스는 인증서를 사용하여 OCSP 응답에 서명합니다. Microsoft 서버에 특수 인증서를 생성하고 다음을 포함해야 합니다.

- 확장 키 사용 = OCSP 서명
- OCSP 폐기 검사 없음

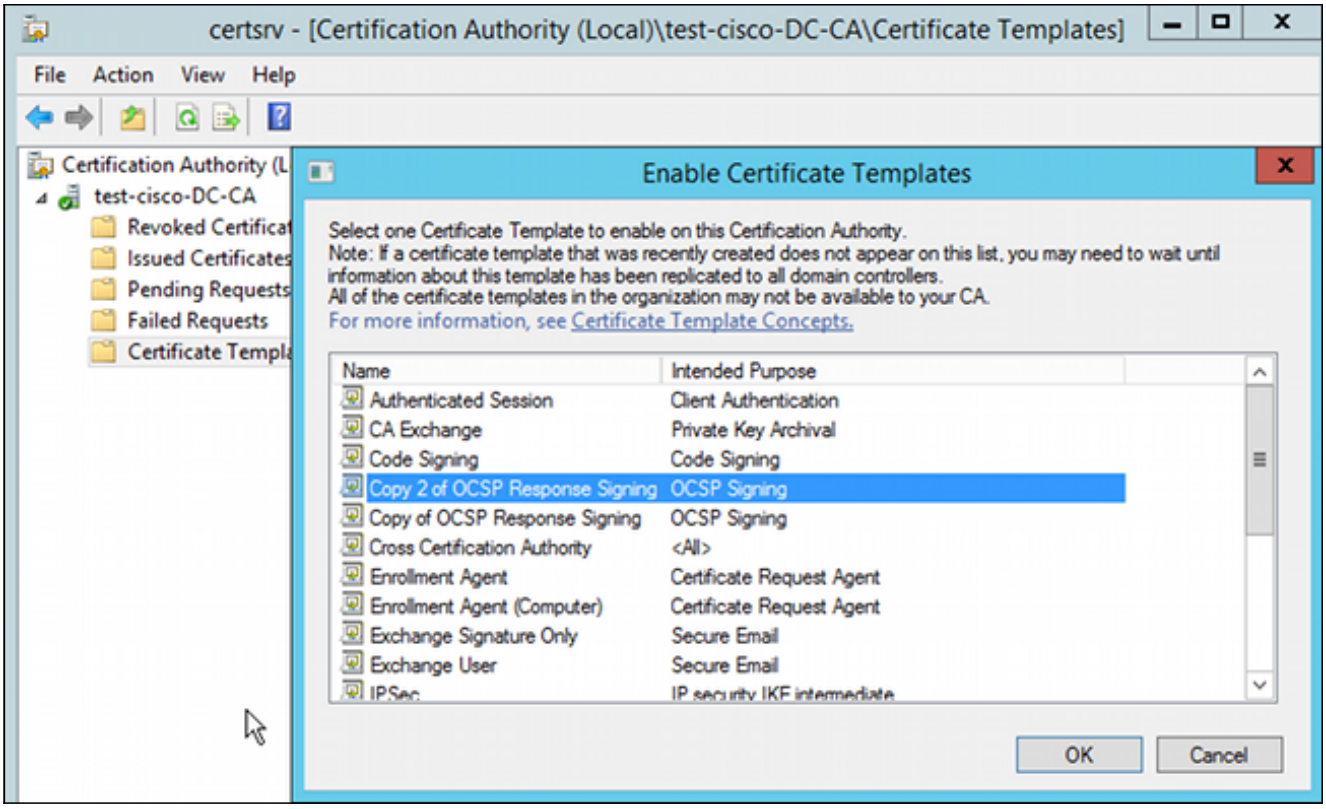
이 인증서는 OCSP 유효성 검사 루프를 방지하기 위해 필요합니다. ASA는 OCSP 서비스를 사용하여 OCSP 서비스가 제공하는 인증서를 확인하지 않습니다.

1. CA의 인증서에 대한 템플릿을 추가합니다. **CA > Certificate Template(인증서 템플릿) > Manage(관리)**로 이동하여 **OCSP Response Signing(OCSP 응답 서명)을 선택하고** 템플릿을 복제합니다. 새로 만든 템플릿의 등록 정보를 보고 **보안** 탭을 클릭합니다. 권한은 어떤 엔티티가 해당 템플릿을 사용하는 인증서를 요청할 수 있는지 설명하므로 올바른 권한이 필요합니다. 이 예에서 엔티티는 동일한 호스트(TEST-CISCO\DC)에서 실행 중인 OCSP 서비스이며 OCSP 서비스에는 자동 등록 권한이 필요합니다.



템플릿에 대한 다른 모든 설정을 기본값으로 설정할 수 있습니다.

2. 템플릿을 활성화합니다. **CA > Certificate Template(인증서 템플릿) > New(새로 만들기) > Certificate Template to Issue(발급할 인증서 템플릿)로 이동한 다음** 중복 템플릿을 선택합니다.

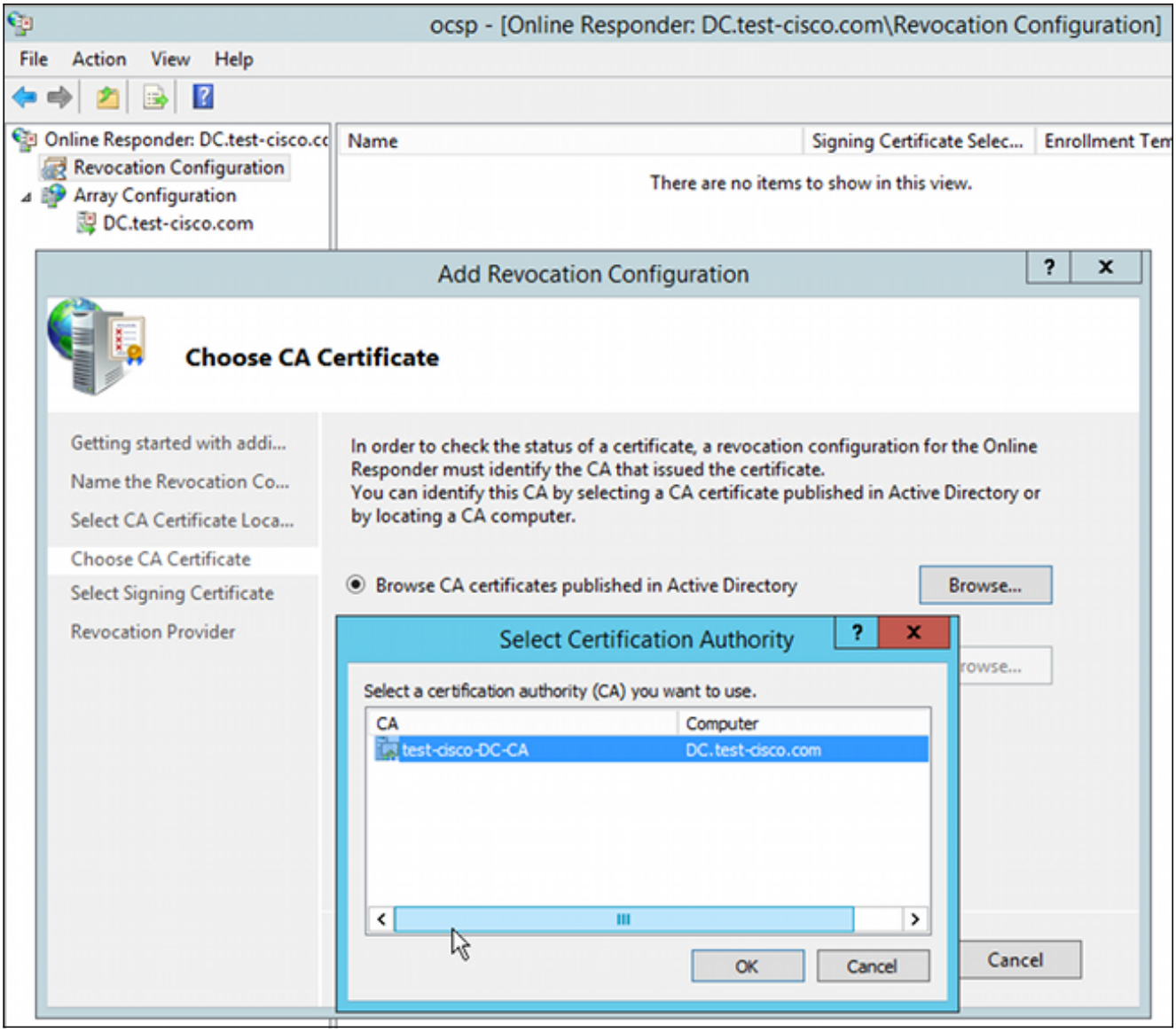


OCSP 서비스 인증서

이 절차에서는 OCSP를 구성하기 위해 온라인 구성 관리를 사용하는 방법에 대해 설명합니다.

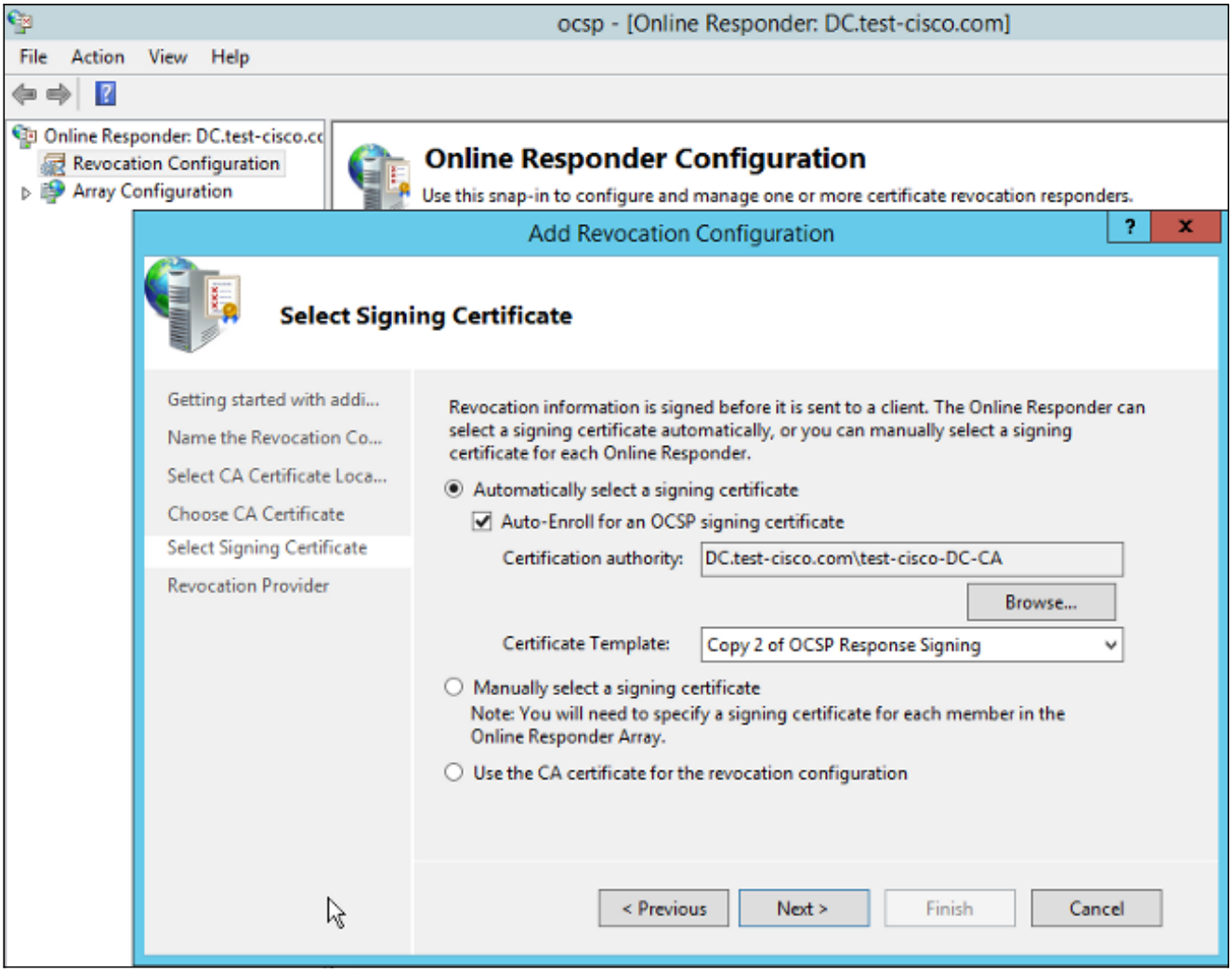
1. **Server Manager > Tools로** 이동합니다.

2. 새 컨피그레이션을 추가하려면 **Revocation Configuration(해지 컨피그레이션) >** Add Revocation Configuration(해지 컨피그레이션 추가)으로 이동합니다.

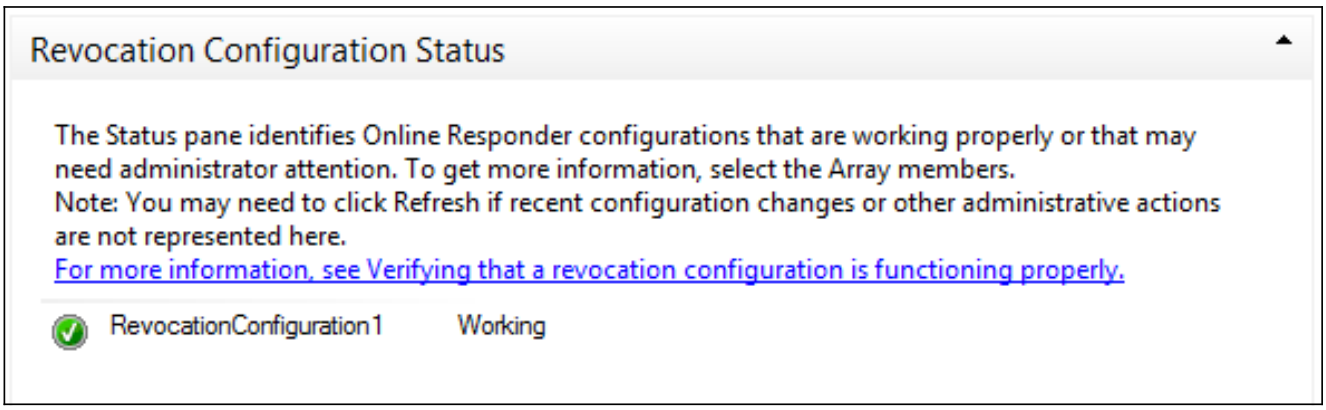


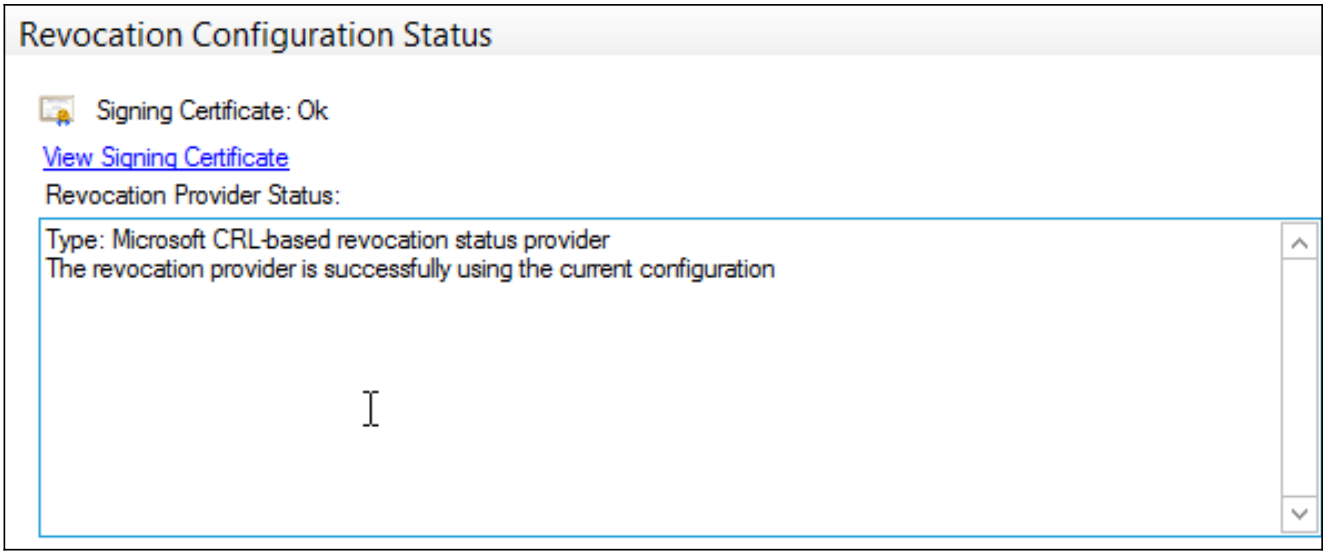
OCSP는 동일한 엔터프라이즈 CA를 사용할 수 있습니다. OCSP 서비스에 대한 인증서가 생성됩니다.

3. 선택한 Enterprise CA를 사용하고 이전에 생성한 템플릿을 선택합니다. 인증서가 자동으로 등록됩니다.

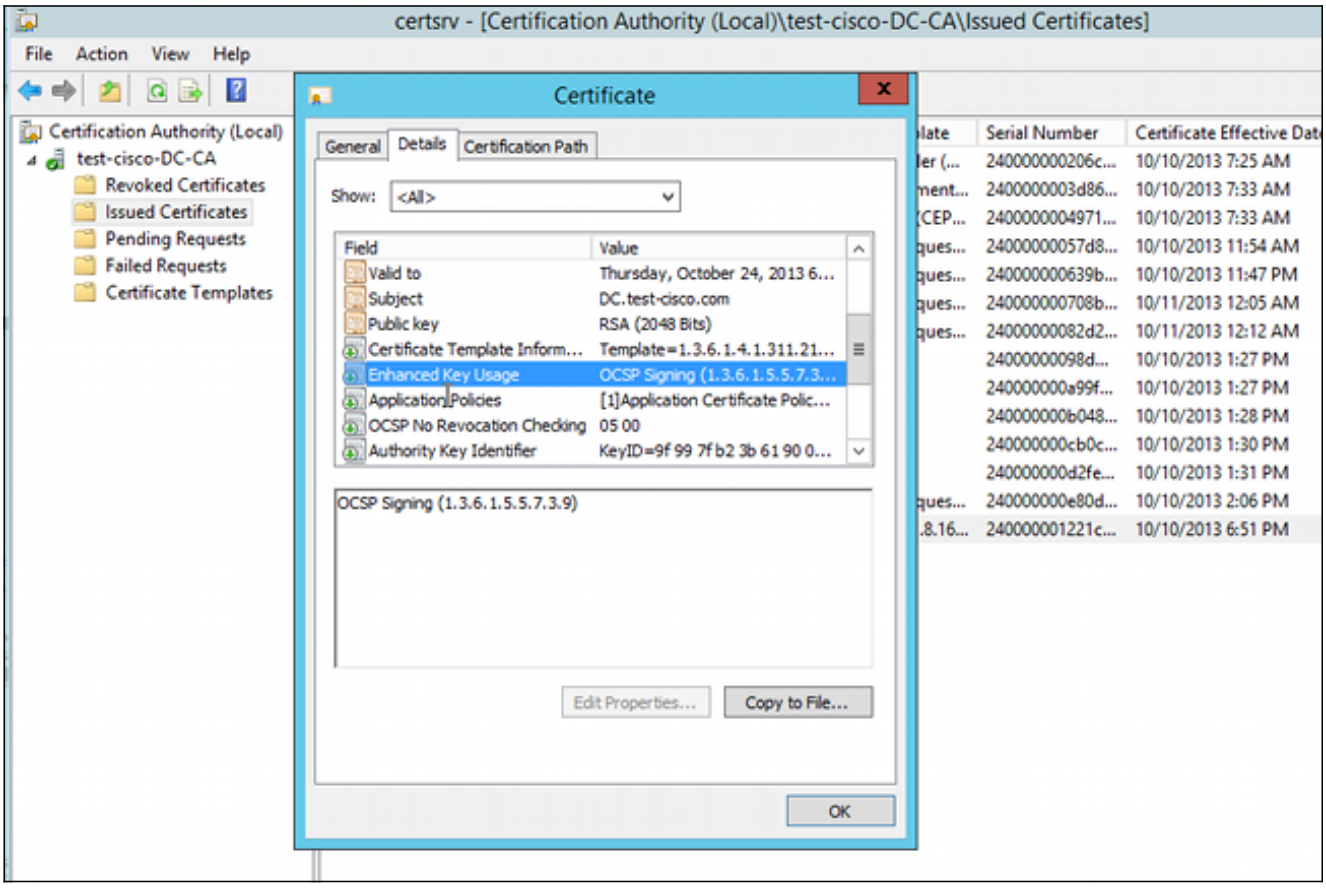


4. 인증서가 등록되었으며 상태가 Working/OK인지 확인합니다.





5. 인증서 세부사항을 확인하기 위해 **CA > Issued Certificates**(발급된 인증서)로 이동합니다.



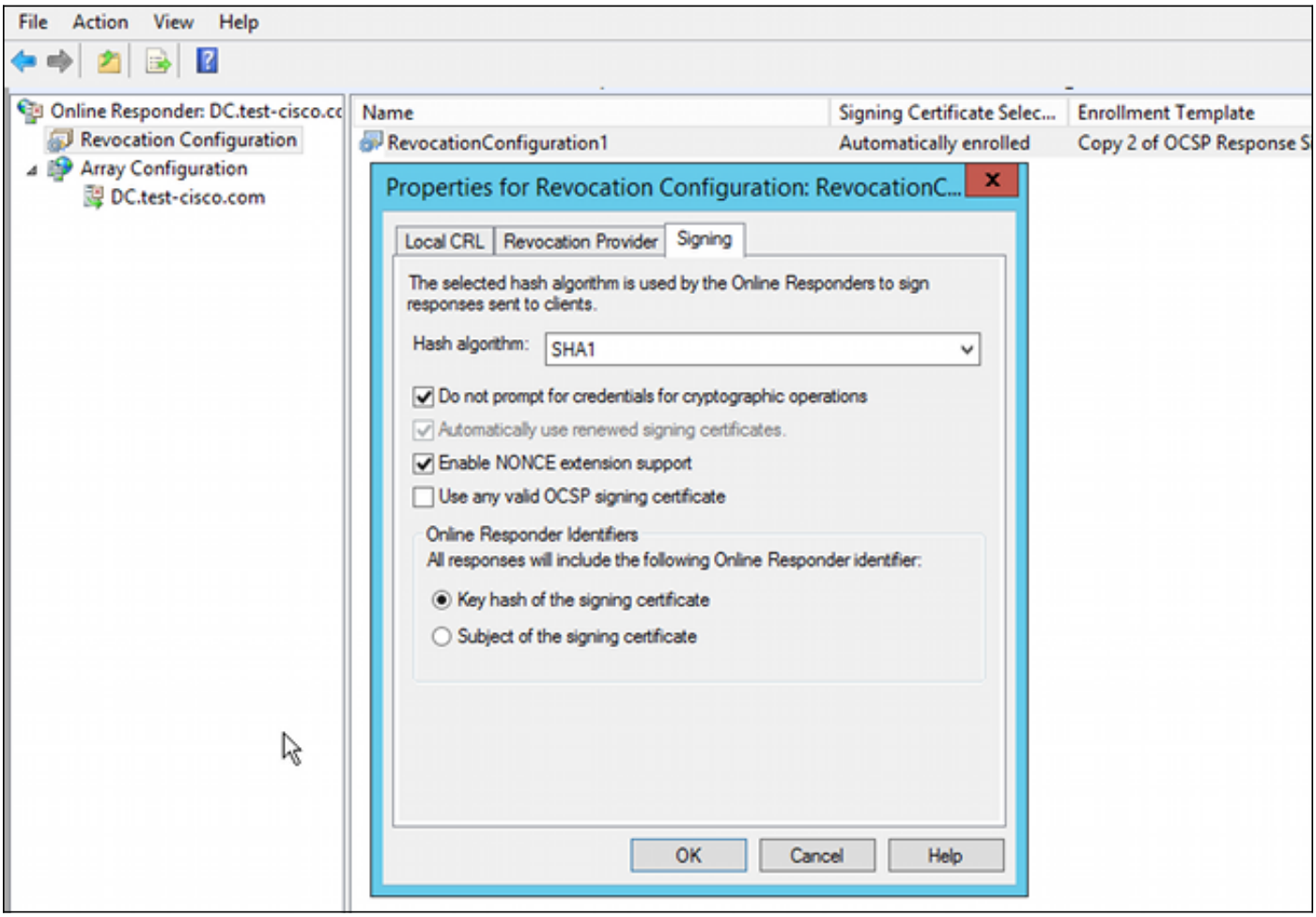
OCSP 서비스 거부

OCSP의 Microsoft 구현은 RFC 5019 The Lightweight Online Certificate Status Protocol(OCSP) Profile for High-Volume Environments, is simplified version of RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP를 준수합니다.

ASA는 OCSP에 RFC 2560을 사용합니다. 두 RFC의 차이점 중 하나는 RFC 5019가 ASA에서 전송한 서명된 요청을 수락하지 않는다는 것입니다.

Microsoft OCSP 서비스가 서명된 요청을 수락하고 올바른 서명된 응답으로 회신하도록 강제할 수 있습니다. Revocation Configuration(**해지 컨피그레이션**) > **RevocationConfiguration1(해지 컨피그**

레이션1) > Edit Properties(속성 편집)로 이동하고 Enable NONCE extension support(NONCE 확장 지원 활성화) **옵션을 선택합니다**.



이제 OCSP 서비스를 사용할 준비가 되었습니다.

Cisco에서는 이를 권장하지 않지만 ASA에서는 nonce를 비활성화할 수 있습니다.

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

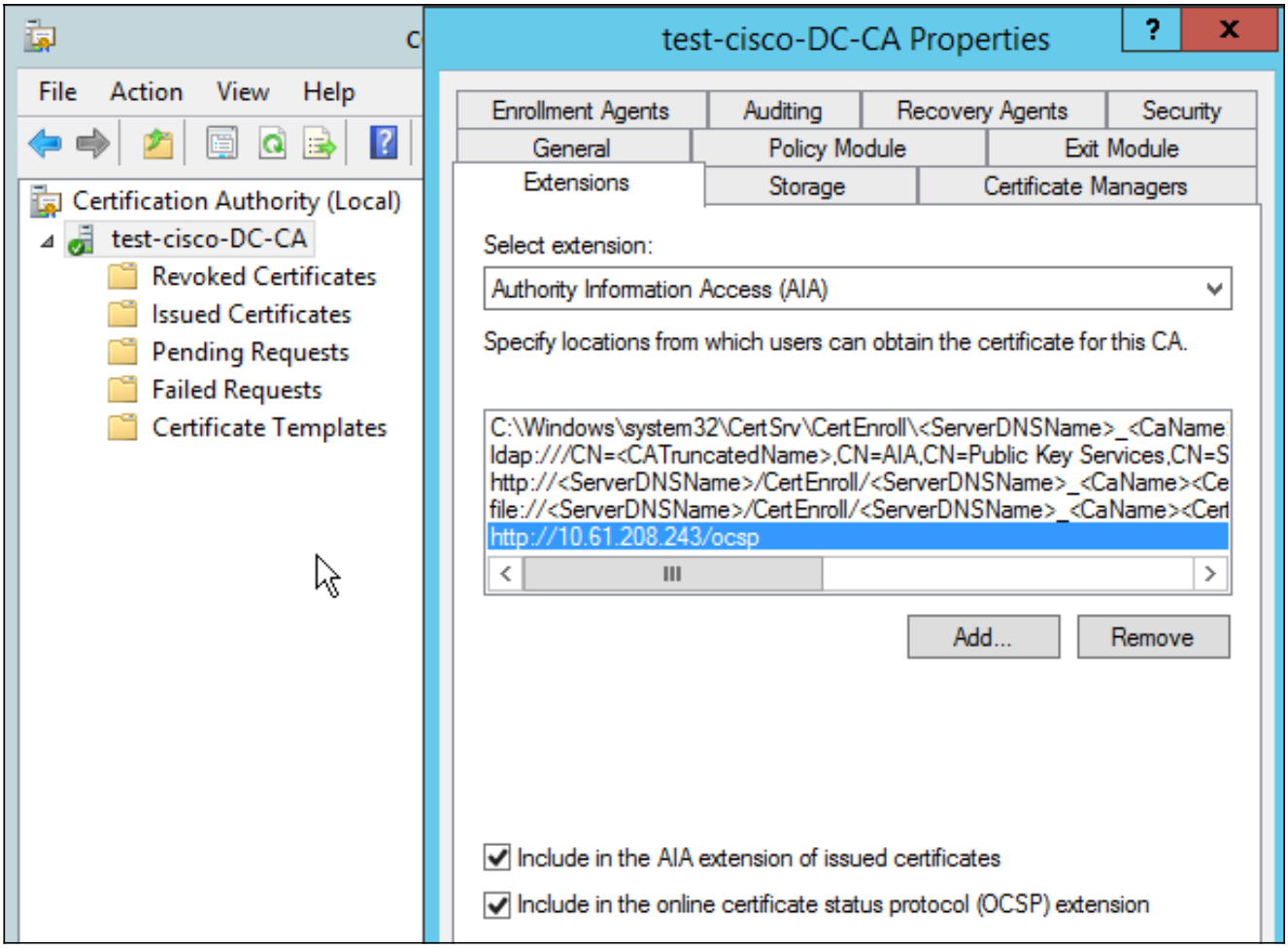
OCSP 확장을 위한 CA 컨피그레이션

이제 모든 발급된 인증서에 OCSP 서버 확장을 포함하도록 CA를 재구성해야 합니다. 해당 확장의 URL은 인증서가 검증될 때 OCSP 서버에 연결하기 위해 ASA에서 사용됩니다.

1. CA에서 서버의 Properties(속성) 대화 상자를 엽니다.

2. Extensions(확장) **탭을** 클릭합니다. OCSP 서비스를 가리키는 AIA(Authority Information Access) 확장이 필요합니다. 이 예에서는 http://10.61.208.243/ocsp입니다. AIA 내선 번호에 대해 다음 두 옵션을 모두 활성화합니다.

   발급된 인증서의 AIA 내선에 포함OCSP(Online Certificate Status Protocol) 확장에 포함



이렇게 하면 발급된 모든 인증서에 OCSP 서비스를 가리키는 올바른 확장명이 지정됩니다.

OpenSSL

참고: CLI를 통한 ASA 컨피그레이션에 대한 자세한 내용은 CLI, 8.4 및 8.6: Configuring an External Server for Security Appliance User Authorization을 사용하는 Cisco ASA 5500 Series 컨피그레이션 가이드를 참조하십시오.

이 예에서는 OpenSSL 서버가 이미 구성되어 있다고 가정합니다. 이 섹션에서는 OCSP 컨피그레이션 및 CA 컨피그레이션에 필요한 변경 사항만 설명합니다.

이 절차에서는 OCSP 인증서를 생성하는 방법에 대해 설명합니다.

1. OCSP 응답기에 다음 매개변수가 필요합니다.

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

2. 사용자 인증서에는 다음 매개변수가 필요합니다.

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

3. 인증서는 CA에서 생성하고 서명해야 합니다.

4. OCSP 서버를 시작합니다.

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

5. 예제 인증서를 테스트합니다.

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

OpenSSL 웹 사이트에서 더 많은 예를 볼 수 있습니다.

OpenSSL은 ASA와 마찬가지로 OCSP 논스를 지원합니다. 논스는 -nonce 및 -no_nonce 스위치를 사용하여 제어할 수 있습니다.

ASA with Multiple OCSP Sources(여러 OCSP 소스가 있는 ASA)

ASA는 OCSP URL을 재정의할 수 있습니다. 클라이언트 인증서에 OCSP URL이 포함된 경우에도 ASA의 컨피그레이션에서 이를 덮어씁니다.

```
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
```

OCSP 서버 주소는 명시적으로 정의할 수 있습니다. 이 명령 예에서는 주체 이름에 관리자가 있는 모든 인증서를 일치시키고, OCSP 서명을 검증하기 위해 OPENSSL 신뢰 지점을 사용하며, 요청을 보내기 위해 http://11.11.11.11/ocsp의 URL을 사용합니다.

```
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
```

OCSP URL을 찾는 데 사용되는 순서는 다음과 같습니다.

1. match certificate 명령으로 설정한 OCSP 서버
2. ocsp url 명령으로 설정한 OCSP 서버
3. 클라이언트 인증서의 AIA 필드에 있는 OCSP 서버

다른 CA에서 서명한 ASA with OCSP

OCSP 응답은 다른 CA에서 서명할 수 있습니다. 이러한 경우 OCSP 인증서 검증을 위해 ASA에서 다른 신뢰 지점을 사용하려면 match certificate 명령을 사용해야 합니다.

```
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
```

이 예에서 ASA는 관리자가 포함된 주체 이름의 모든 인증서에 대해 OCSP URL 재작성을 사용합니다. ASA는 다른 신뢰 지점인 OPENSSL에 대해 OCSP responder 인증서의 유효성을 검사해야 합니다. 사용자 인증서는 WIN2012 신뢰 지점에서 계속 검증됩니다.

OCSP responder 인증서에는 'OCSP no revocation checking' 확장이 있으므로 OCSP가 OPENSSL 신뢰 지점에 대해 강제로 검증되는 경우에도 인증서가 검증되지 않습니다.

기본적으로 모든 신뢰 지점은 ASA에서 사용자 인증서를 확인하려고 할 때 검색됩니다. OCSP responder 인증서에 대한 검증이 다릅니다. ASA는 사용자 인증서에 대해 이미 발견된 신뢰 지점만 검색합니다(이 예에서는 WIN2012).

따라서 ASA가 OCSP 인증서 검증(이 예에서는 OPENSSL)에 다른 신뢰 지점을 사용하도록 강제하려면 match certificate 명령을 사용해야 합니다.

사용자 인증서는 처음 일치하는 신뢰 지점(이 예에서는 WIN2012)에 대해 검증되며, 이 신뢰 지점은 OCSP responder 검증에 대한 기본 신뢰 지점을 결정합니다.

match certificate 명령에 특정 신뢰 지점이 제공되지 않은 경우, OCSP 인증서는 사용자 인증서와 동일한 신뢰 지점에 대해 검증됩니다(이 예에서는 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
```

다음을 확인합니다.

설정이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

> **참고**: Output Interpreter Tool(등록된 고객만 해당)은 특정 **show** 명령을 지원합니다. **show** 명령 출력의 분석을 보려면 아웃풋 인터프리터 툴을 사용합니다.

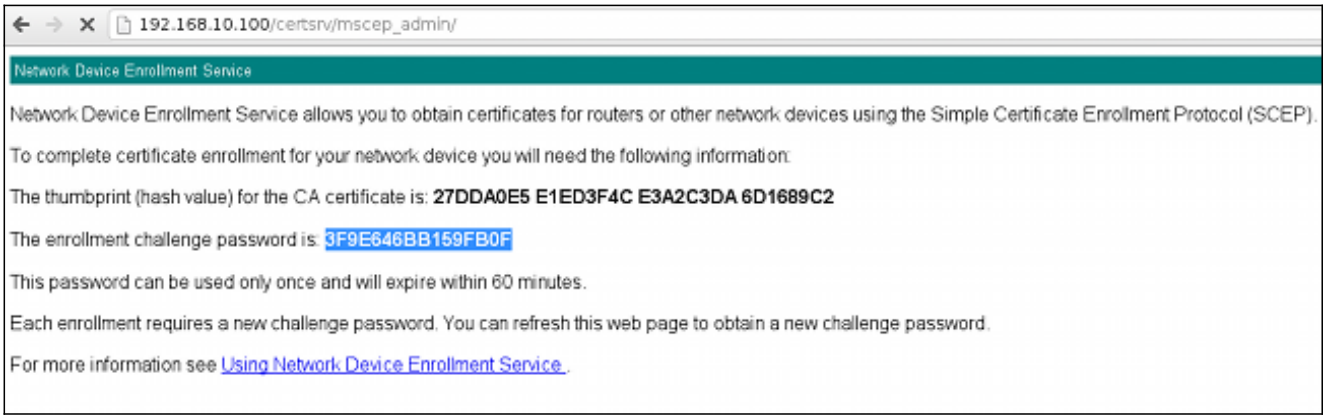
ASA - SCEP를 통해 인증서 가져오기

이 절차에서는 SCEP를 사용하여 인증서를 가져오는 방법에 대해 설명합니다.

1. 다음은 CA 인증서를 가져오기 위한 신뢰 지점 인증 프로세스입니다.

```
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. 인증서를 요청하려면 ASA에 관리 콘솔(http://IP/certsrv/mscep_admin)에서 얻을 수 있는 일회용 SCEP 비밀번호가 있어야 합니다.



3. 이 비밀번호를 사용하여 ASA에 인증서를 요청합니다.

```
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
```

일부 출력은 명확성을 위해 생략되었습니다.

4. CA 및 ASA 인증서를 모두 확인합니다.

```
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
```

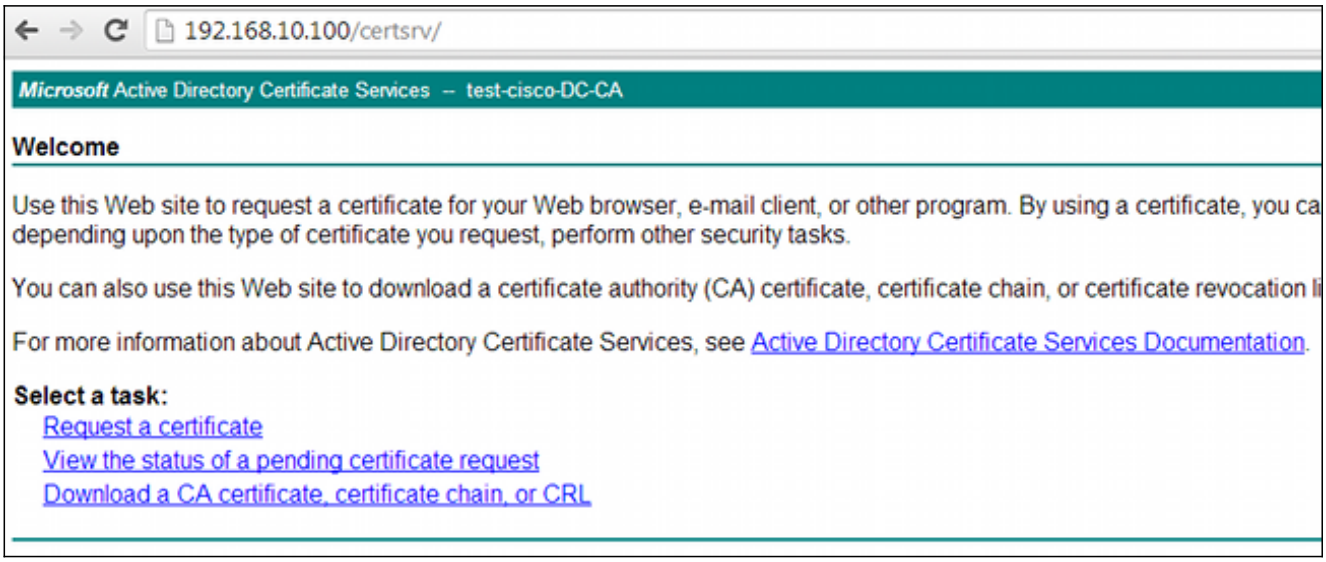
ASA는 대부분의 인증서 확장을 표시하지 않습니다. ASA 인증서에 'AIA의 OCSP URL' 확장이

포함되어 있더라도 ASA CLI는 이를 제공하지 않습니다. Cisco Bug ID CSCui44335, "ASA ENH Certificate x509 extensions displayed"에서 이 개선을 요청합니다.

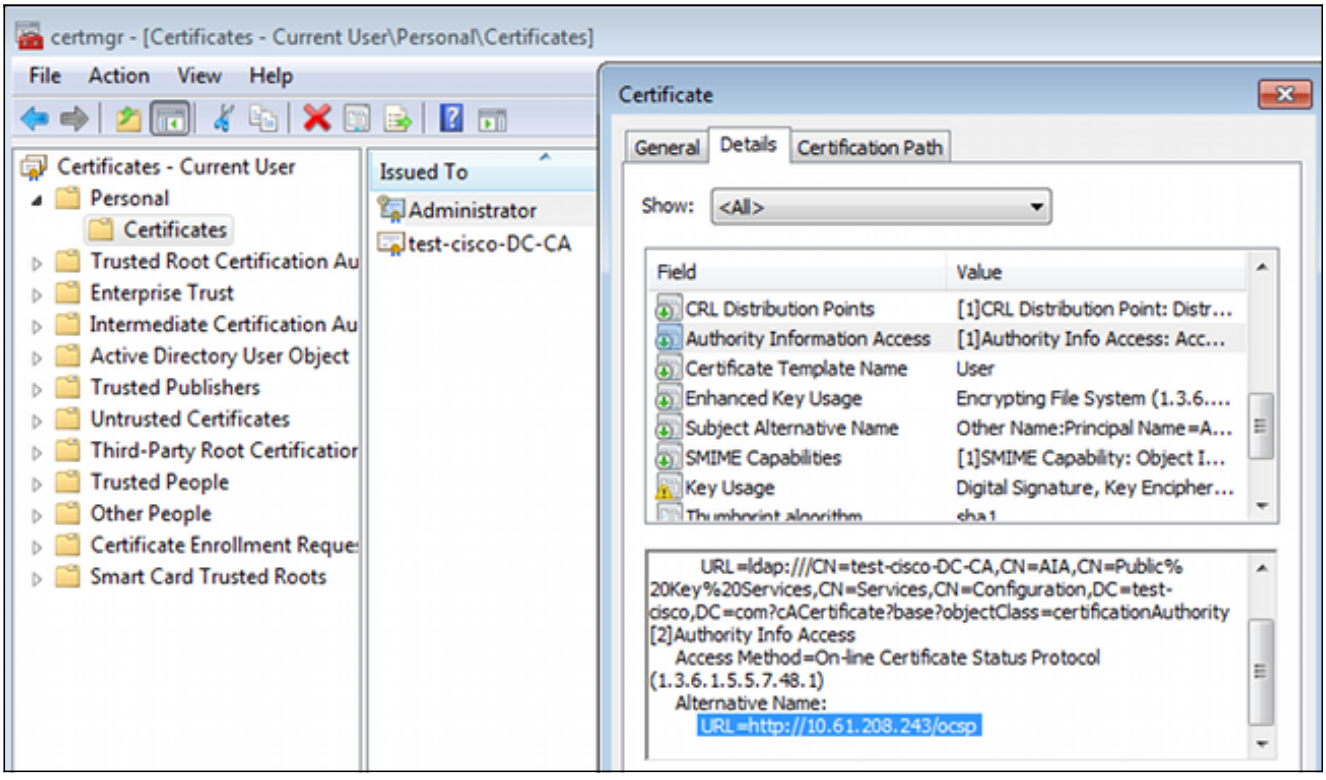
AnyConnect - 웹 페이지를 통해 인증서 가져오기

이 절차에서는 클라이언트에서 웹 브라우저를 사용하여 인증서를 가져오는 방법에 대해 설명합니다.

1. 웹 페이지를 통해 AnyConnect 사용자 인증서를 요청할 수 있습니다. 클라이언트 PC에서 웹 브라우저를 사용하여 CA(http://*IP*/certsrv)로 이동합니다.



2. 사용자 인증서를 웹 브라우저 저장소에 저장한 다음 AnyConnect에서 검색하는 Microsoft 저장소로 내보낼 수 있습니다. 수신된 인증서를 확인하려면 certmgr.msc를 사용합니다.



올바른 AnyConnect 프로파일이 있는 경우 AnyConnect에서 인증서를 요청할 수도 있습니다.

OCSP 검증을 통한 ASA VPN 원격 액세스

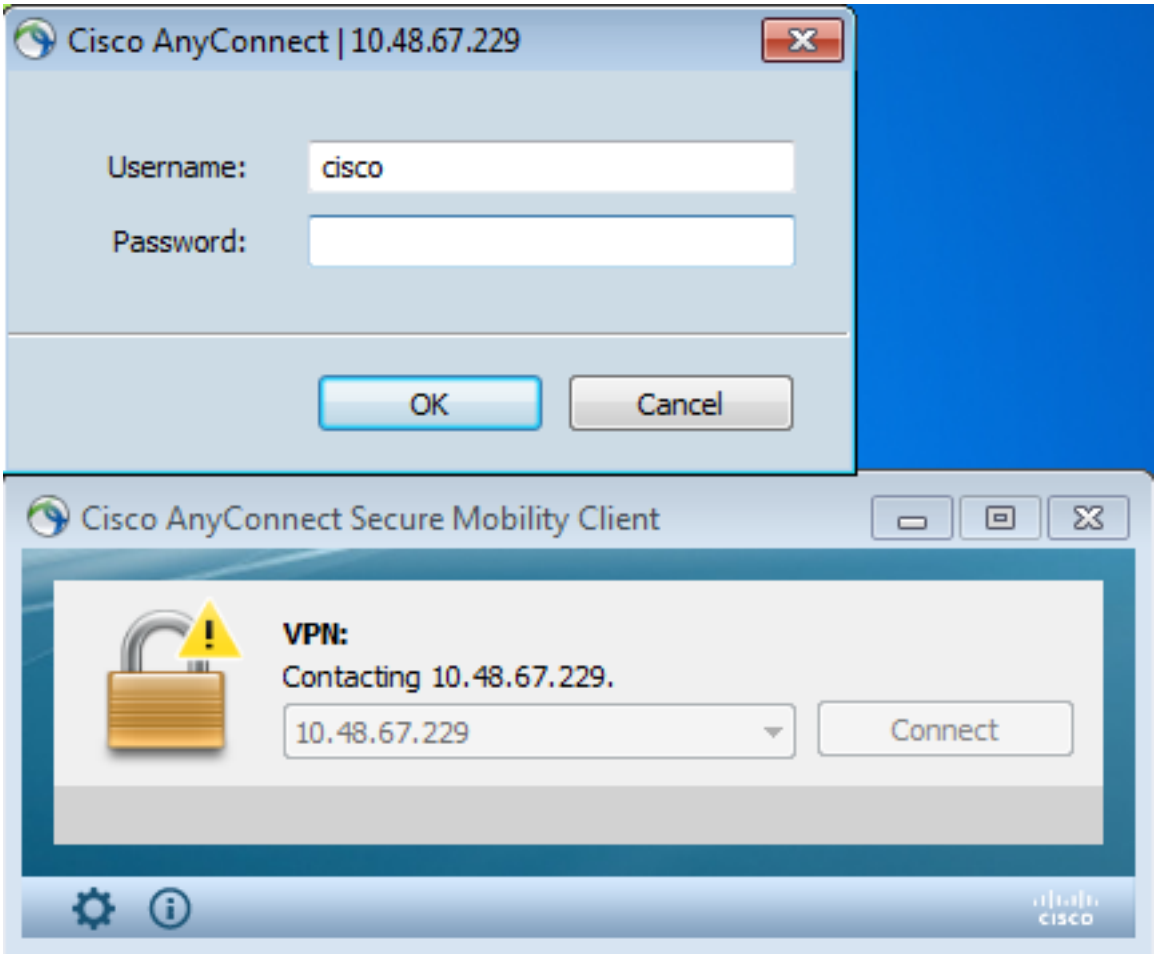
이 절차에서는 OCSP 검증을 확인하는 방법에 대해 설명합니다.

1. 연결을 시도할 때 ASA는 인증서가 OCSP에 대해 검사 중임을 보고합니다. 여기서 OCSP 서명 인증서는 no-check 확장명을 가지며 OCSP를 통해 검사되지 않았습니다.

```
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.
```

일부 출력은 명확성을 위해 생략되었습니다.

2. 최종 사용자는 사용자 자격 증명을 제공합니다.



3. VPN 세션이 올바르게 완료되었습니다.

```
%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. 세션이 생성됩니다.

```
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
```

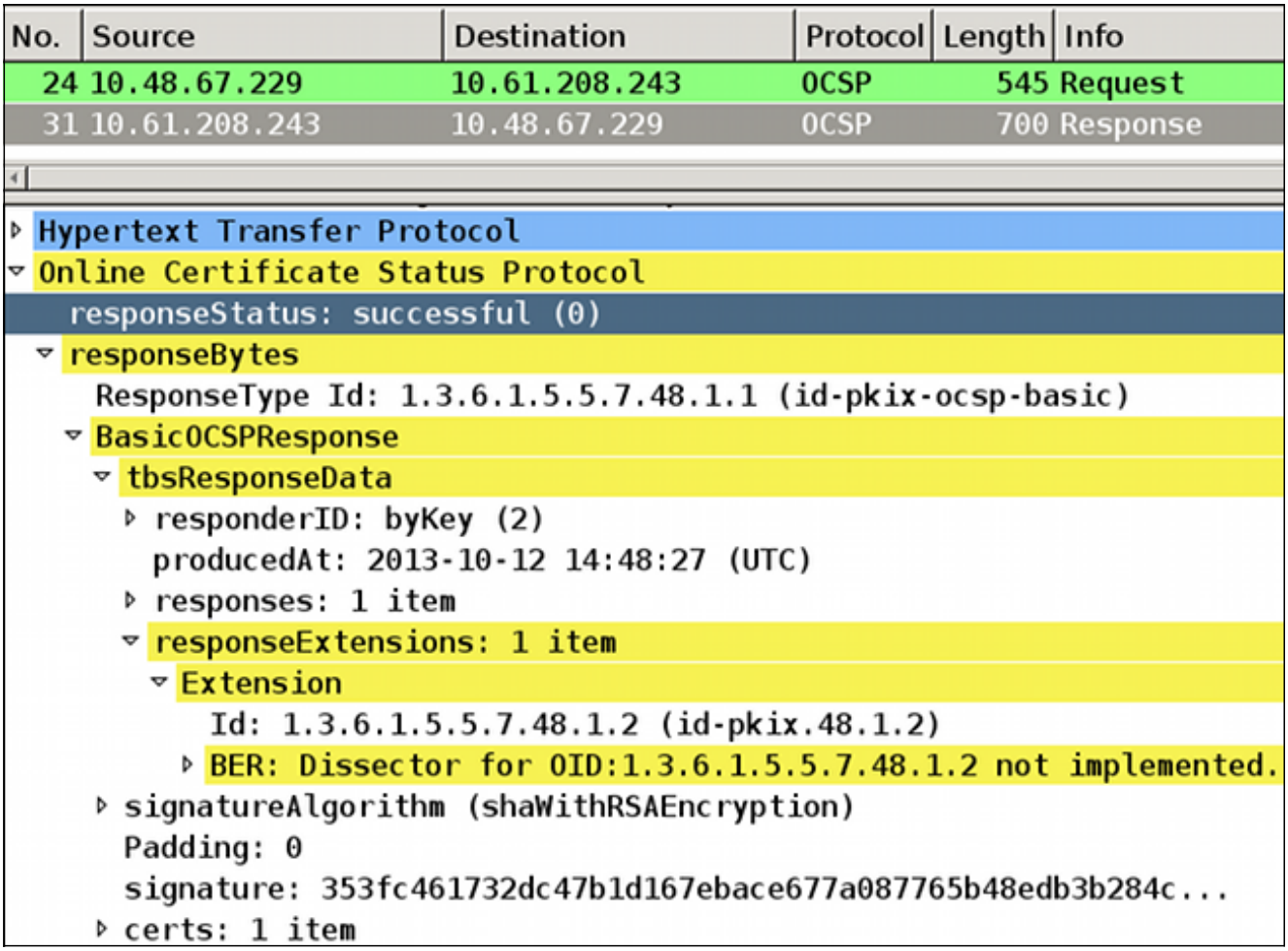
```
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1
DTLS-Tunnel: (1)SHA1
Bytes Tx     : 10540                  Bytes Rx     : 32236
Pkts Tx      : 8                      Pkts Rx      : 209
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : MY                     Tunnel 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. OCSP 검증에 자세한 디버그를 사용할 수 있습니다.

```
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. 패킷 캡처 레벨에서 이는 OCSP 요청 및 올바른 OCSP 응답입니다. 응답에는 올바른 서명(Microsoft OCSP에서 활성화된 nonce 확장)이 포함됩니다.



여러 OCSP 소스를 사용하는 ASA VPN 원격 액세스

ASA with Multiple OCSP Sources에서 설명한 대로 일치 인증서가 구성된 경우, 일치 인증서가 우선적으로 적용됩니다.

```
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
```

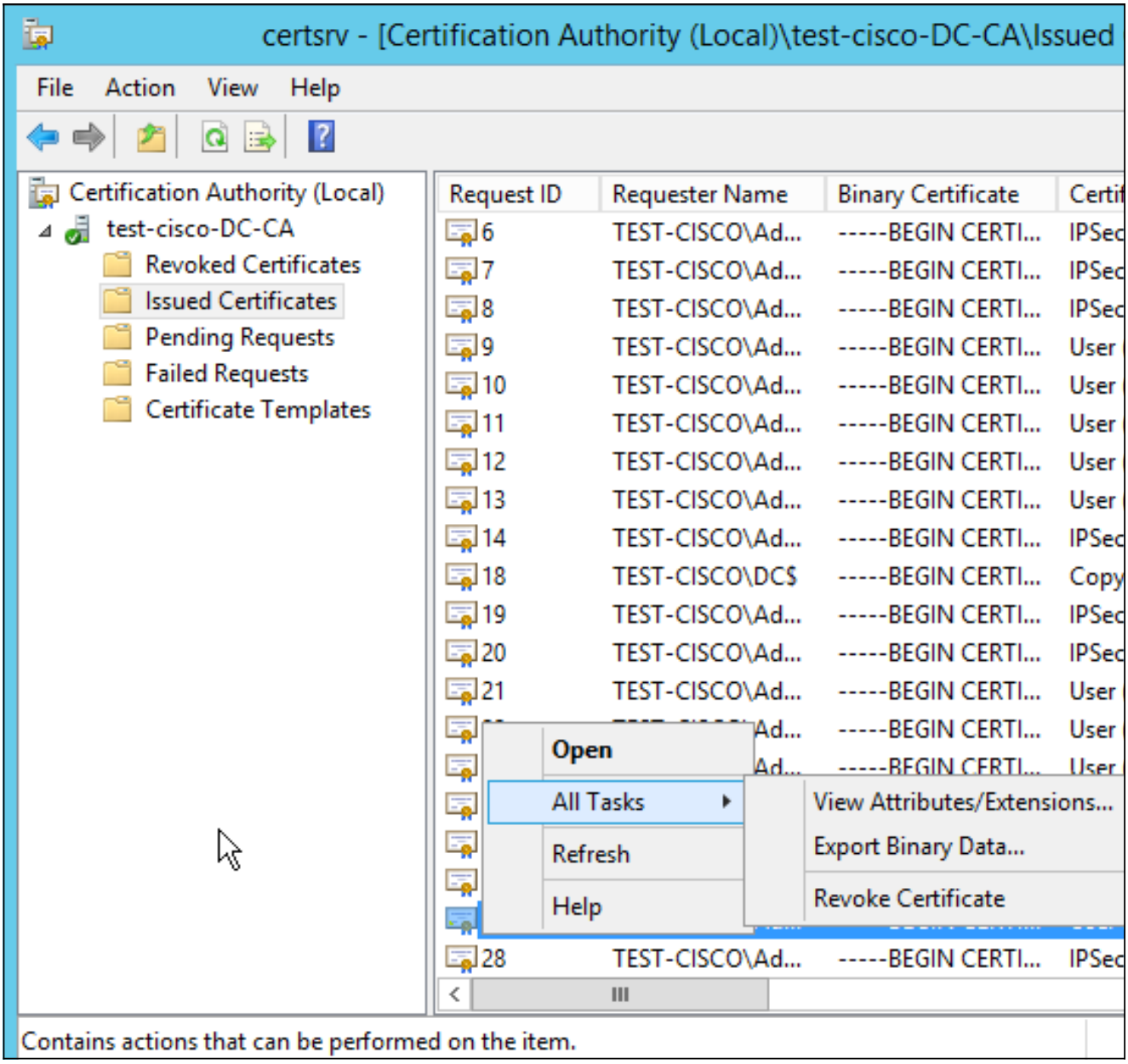
OCSP URL 재정의가 사용되는 경우 디버깅은 다음과 같습니다.

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

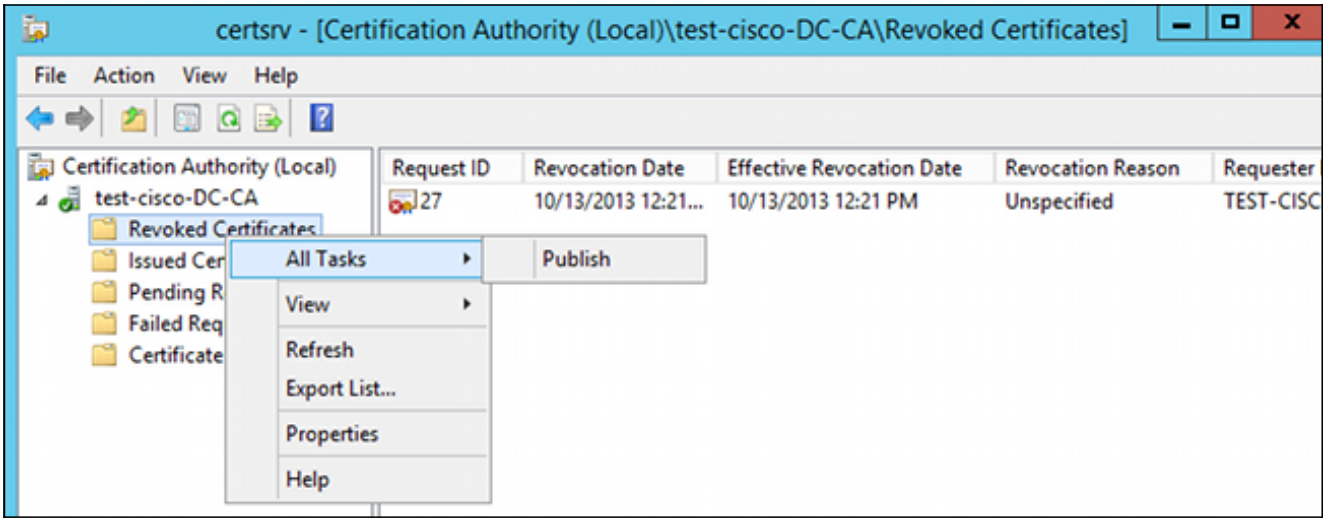
OCSP 및 폐기된 인증서를 사용하는 ASA VPN 원격 액세스

이 절차에서는 인증서를 폐기하고 폐기된 상태를 확인하는 방법에 대해 설명합니다.

1. 클라이언트 인증서 해지:



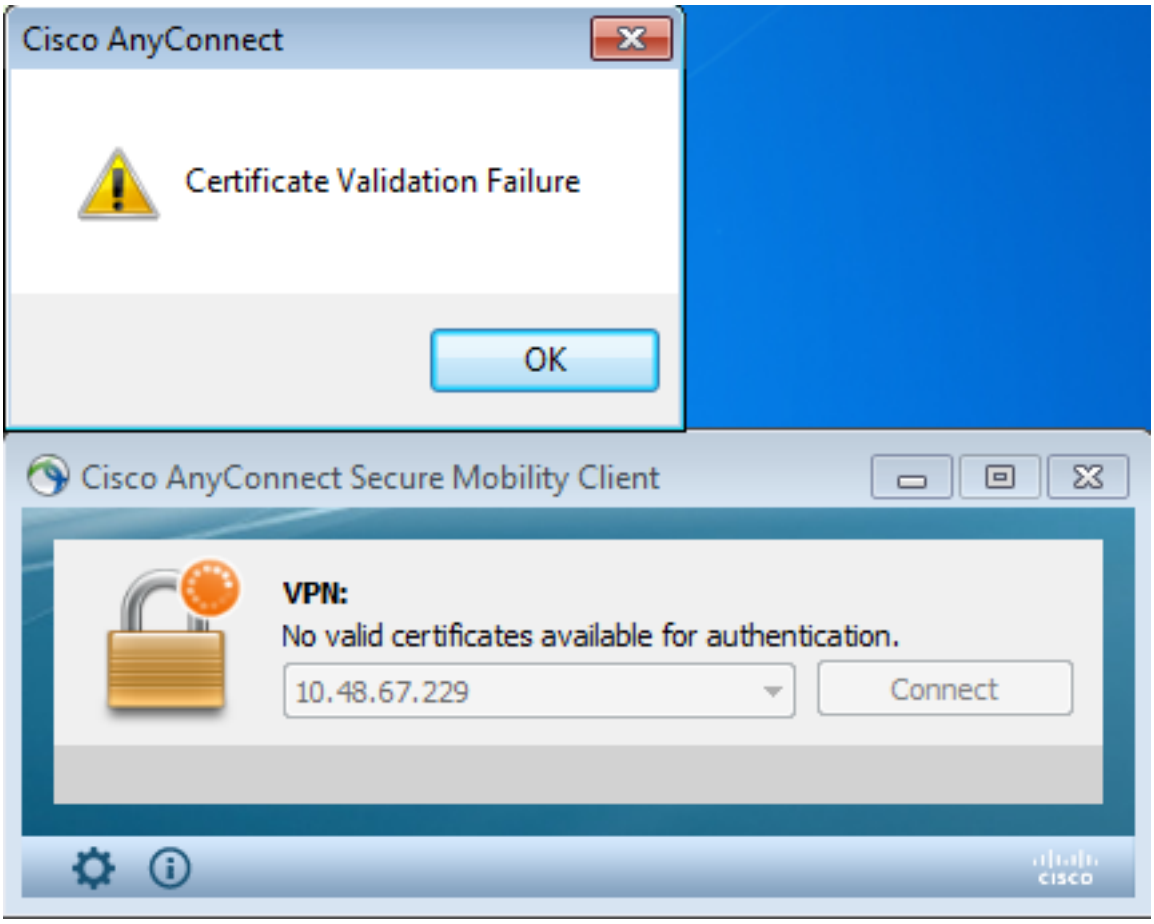
2. 결과를 게시합니다.



3. [선택 사항] 1단계와 2단계는 Power Shell의 certutil CLI 유틸리티로 수행할 수도 있습니다.

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

4. 클라이언트가 연결을 시도할 때 인증서 유효성 검사 오류가 발생합니다.



5. 또한 AnyConnect 로그는 인증서 검증 오류를 나타냅니다.

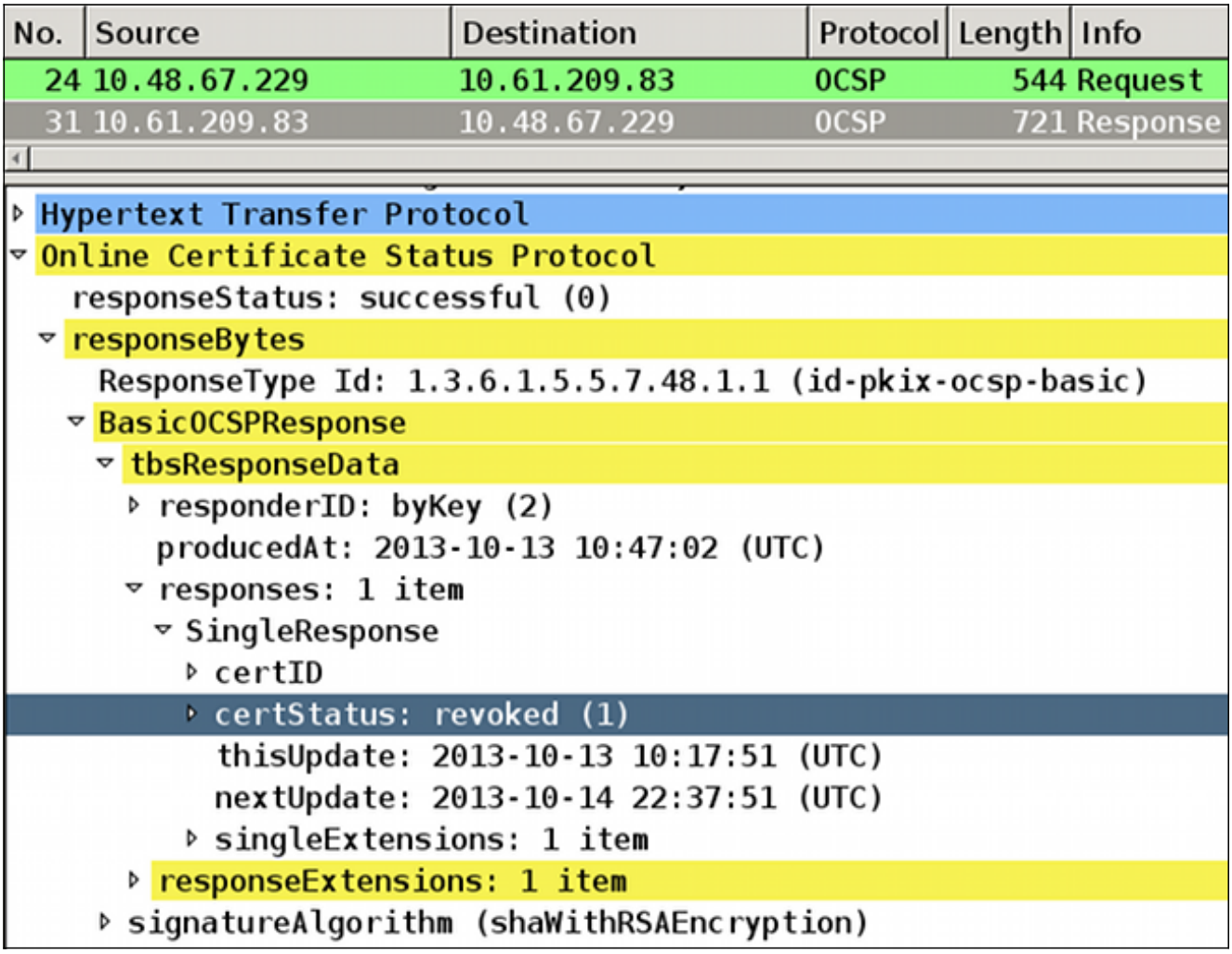
```
[2013-10-13 12:49:53] Contacting 10.48.67.229.
[2013-10-13 12:49:54] No valid certificates available for authentication.
[2013-10-13 12:49:55] Certificate Validation Failure
```

6. ASA에서 인증서 상태가 해지되었음을 보고합니다.

```
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. 패킷 캡처는 인증서 상태가 revoked인 성공적인 OCSP 응답을 표시합니다.



문제 해결

이 섹션에서는 설정 문제 해결에 사용할 수 있는 정보를 제공합니다.

OCSP 서버 작동 중지

ASA는 OCSP 서버가 다운되었을 때 보고합니다.

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

패킷 캡처는 트러블슈팅에도 도움이 됩니다.

시간이 동기화되지 않음

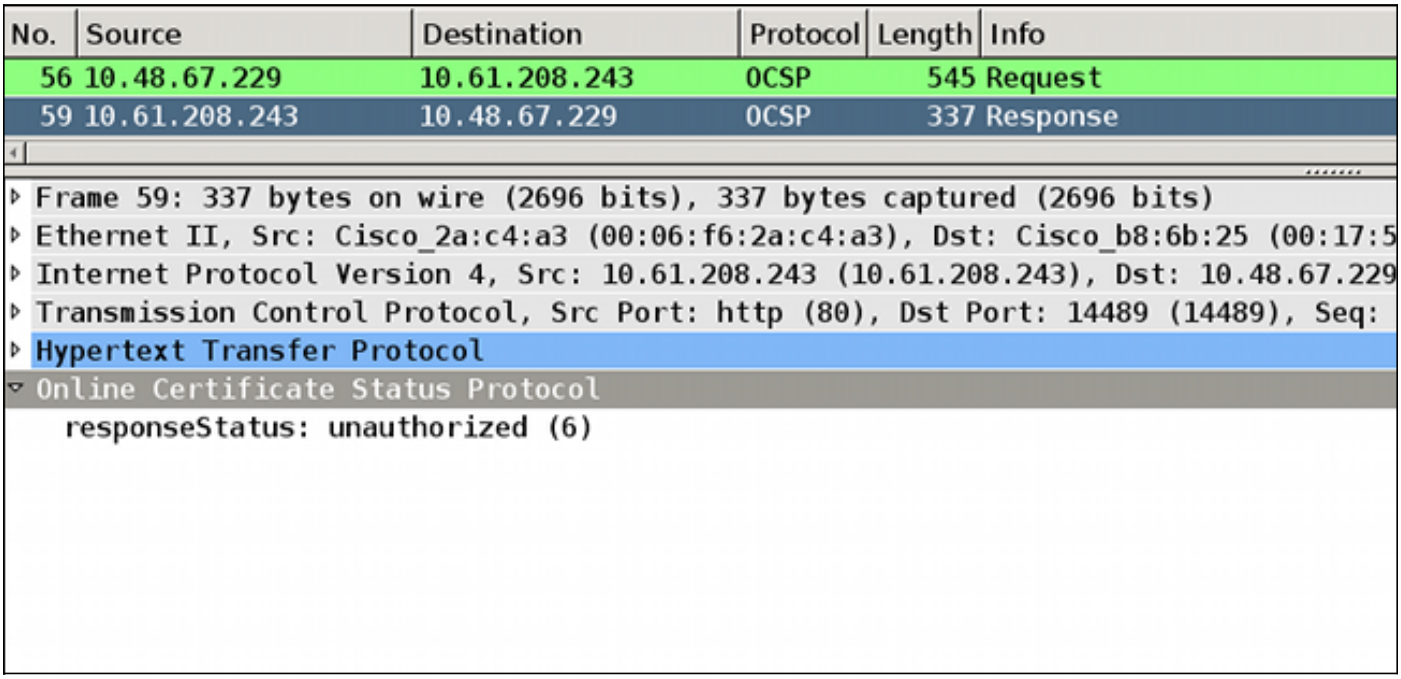
OCSP 서버의 현재 시간이 ASA의 현재 시간보다 오래된 경우(약간의 차이도 허용 가능), OCSP 서버는 무단 응답을 전송하고 ASA는 이를 보고합니다.

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

ASA가 향후 시간으로부터 OCSP 응답을 받으면 역시 실패합니다.

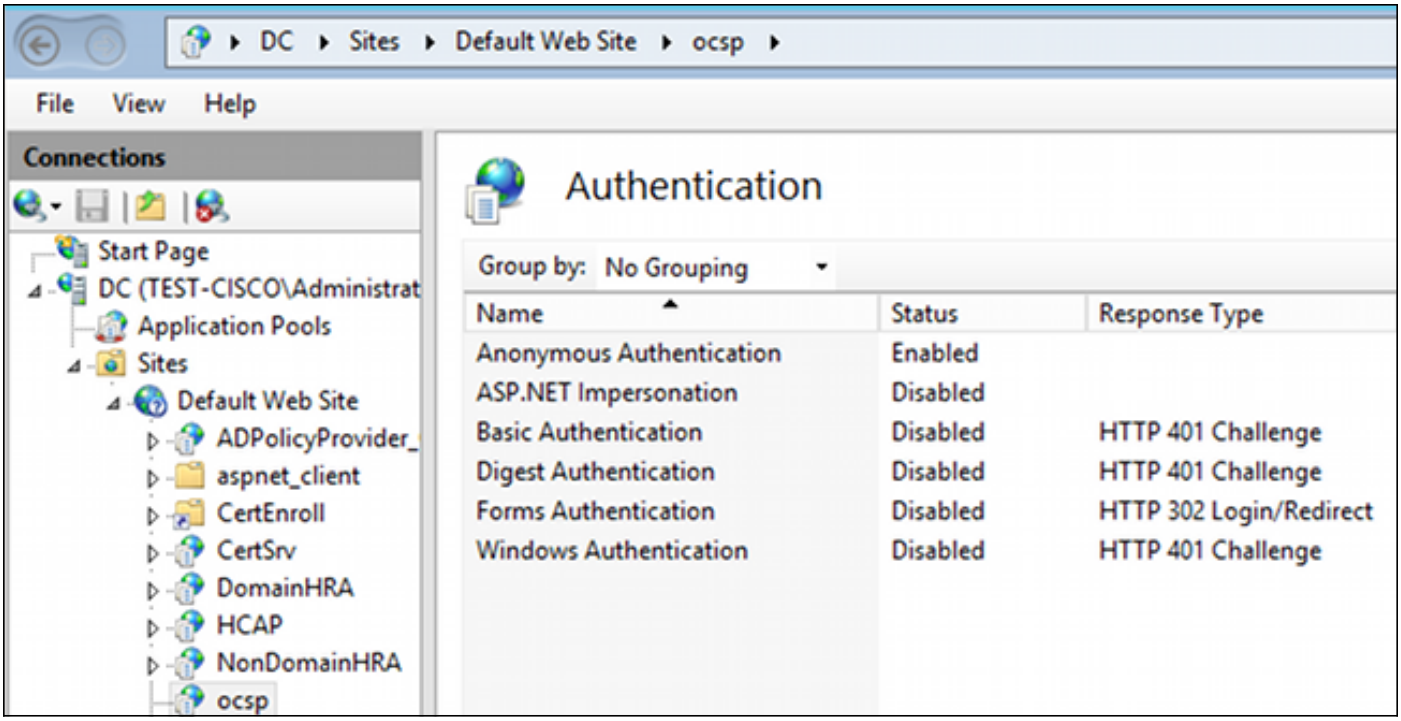
서명된 논스는 지원되지 않음

서버의 nonce가 지원되지 않는 경우(Microsoft Windows 2012 R2의 기본값) 무단 응답이 반환됩니다.



IIS7 서버 인증

SCEP/OCSP 요청 문제는 IIS7(Internet Information Services 7)의 잘못된 인증으로 인해 발생하는 경우가 많습니다. 익명 액세스가 구성되었는지 확인합니다.



관련 정보

- Microsoft TechNet: Online Responder 설치, 구성 및 문제 해결 가이드
- Microsoft TechNet: OCSP 응답자를 지원하도록 CA 구성
- Cisco ASA Series 명령 참조
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.