

ASA Remote Access VPN mit OCSP-Verifizierung unter Microsoft Windows 2012 und OpenSSL

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[ASA Remote Access mit OCSP](#)

[Microsoft Windows 2012 CA](#)

[Installation von Services](#)

[CA-Konfiguration für OCSP-Vorlage](#)

[OCSP-Dienstzertifikat](#)

[OCSP-Service-Nichtigkeiten](#)

[CA-Konfiguration für OCSP-Erweiterungen](#)

[OpenSSL](#)

[ASA mit mehreren OCSP-Quellen](#)

[ASA mit OCSP, von anderer Zertifizierungsstelle signiert](#)

[Überprüfung](#)

[ASA - Zertifikat über SCEP abrufen](#)

[AnyConnect - Zertifikat über Webseite abrufen](#)

[ASA VPN Remote Access mit OCSP-Validierung](#)

[ASA VPN-Remote-Zugriff mit mehreren OCSP-Quellen](#)

[ASA VPN-Remote-Zugriff mit OCSP und widerrufenem Zertifikat](#)

[Fehlerbehebung](#)

[OCSP-Server ausgefallen](#)

[Zeit nicht synchronisiert](#)

[Signierte Nonces werden nicht unterstützt](#)

[IIS7-Serverauthentifizierung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird die Verwendung des Online Certificate Status Protocol (OCSP) zur Validierung auf einer Cisco Adaptive Security Appliance (ASA) für Zertifikate von VPN-Benutzern

beschrieben. Es werden Beispielkonfigurationen für zwei OCSP-Server (Microsoft Windows Certificate Authority [CA] und OpenSSL) dargestellt. Im Abschnitt Überprüfen werden detaillierte Abläufe auf Paketebene beschrieben. Im Abschnitt Fehlerbehebung werden typische Fehler und Probleme behandelt.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Konfiguration der Cisco Adaptive Security Appliance über eine Kommandozeile (CLI) und Secure Socket Layer (SSL) VPN
- X.509-Zertifikate
- Microsoft Windows Server
- Linux/OpenSSL

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Adaptive Security Appliance-Software, Version 8.4 und höher
- Microsoft Windows 7 mit Cisco AnyConnect Secure Mobility Client, Version 3.1
- Microsoft Server 2012 R2
- Linux mit OpenSSL 1.0.0j oder höher

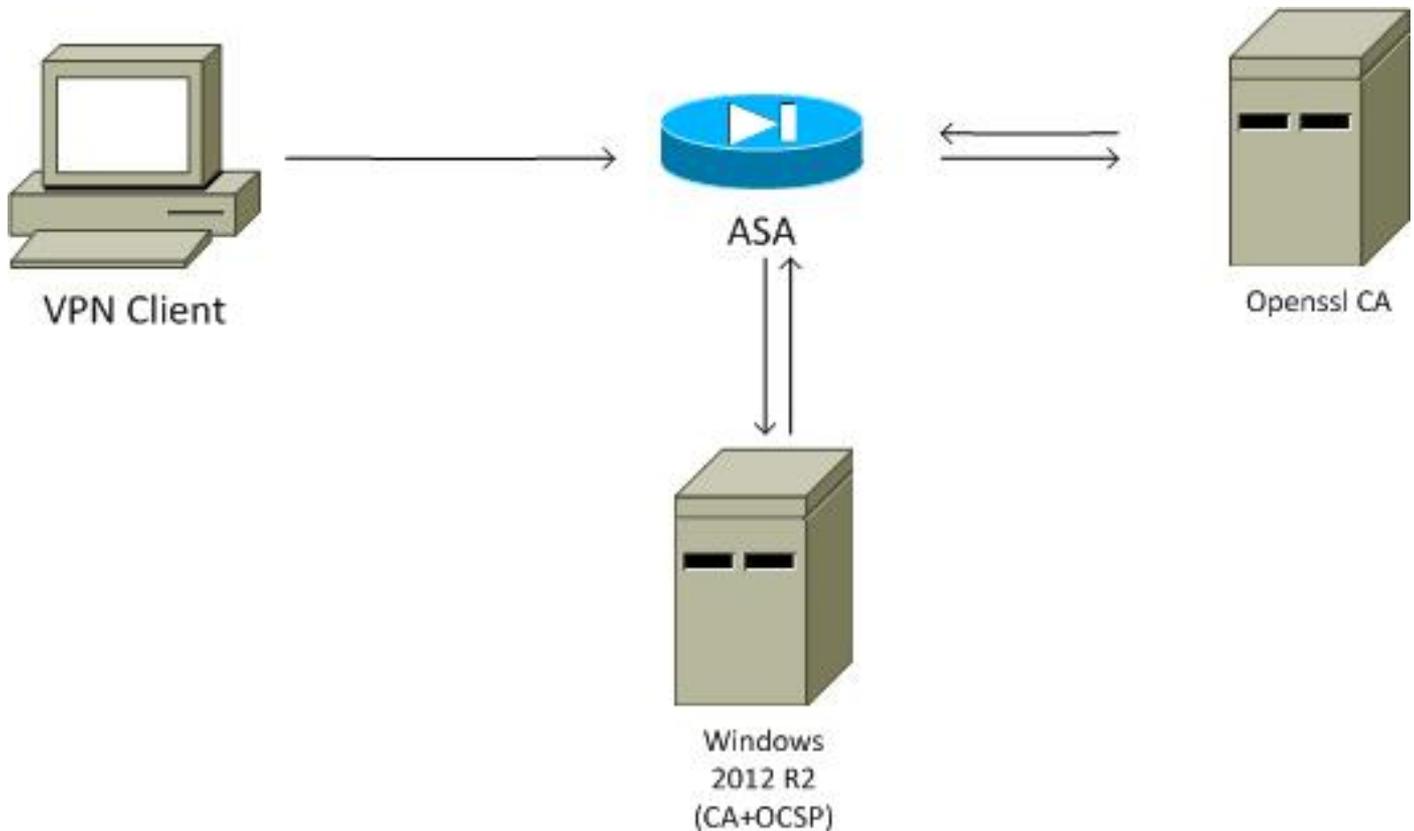
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konfigurieren

Hinweis: Verwenden Sie das [Command Lookup Tool](#) (nur für [registrierte](#) Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

Der Client verwendet das Remotezugriffs-VPN. Dieser Zugriff kann Cisco VPN Client (IPSec), Cisco AnyConnect Secure Mobility (SSL/Internet Key Exchange Version 2 [IKEv2]) oder WebVPN (Portal) sein. Für die Anmeldung stellt der Client das richtige Zertifikat sowie Benutzername und Kennwort bereit, die lokal auf dem ASA-Gerät konfiguriert wurden. Das Client-Zertifikat wird über den OCSP-Server validiert.



ASA Remote Access mit OCSP

Die ASA ist für den SSL-Zugriff konfiguriert. Der Client verwendet AnyConnect für die Anmeldung. Die ASA verwendet das Simple Certificate Enrollment Protocol (SCEP), um das Zertifikat anzufordern:

```
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
```

Eine Zertifikatszuordnung wird erstellt, um alle Benutzer zu identifizieren, deren Antragstellername das Wort Administrator enthält (ohne Berücksichtigung der Groß-/Kleinschreibung). Diese Benutzer sind an eine Tunnelgruppe mit dem Namen RA gebunden:

```
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
```

Die VPN-Konfiguration erfordert eine erfolgreiche Autorisierung (d. h. ein validiertes Zertifikat). Außerdem müssen die richtigen Anmeldeinformationen für den lokal definierten Benutzernamen (Authentifizierung aaa) eingegeben werden:

```
username cisco password xxxxxxxx
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

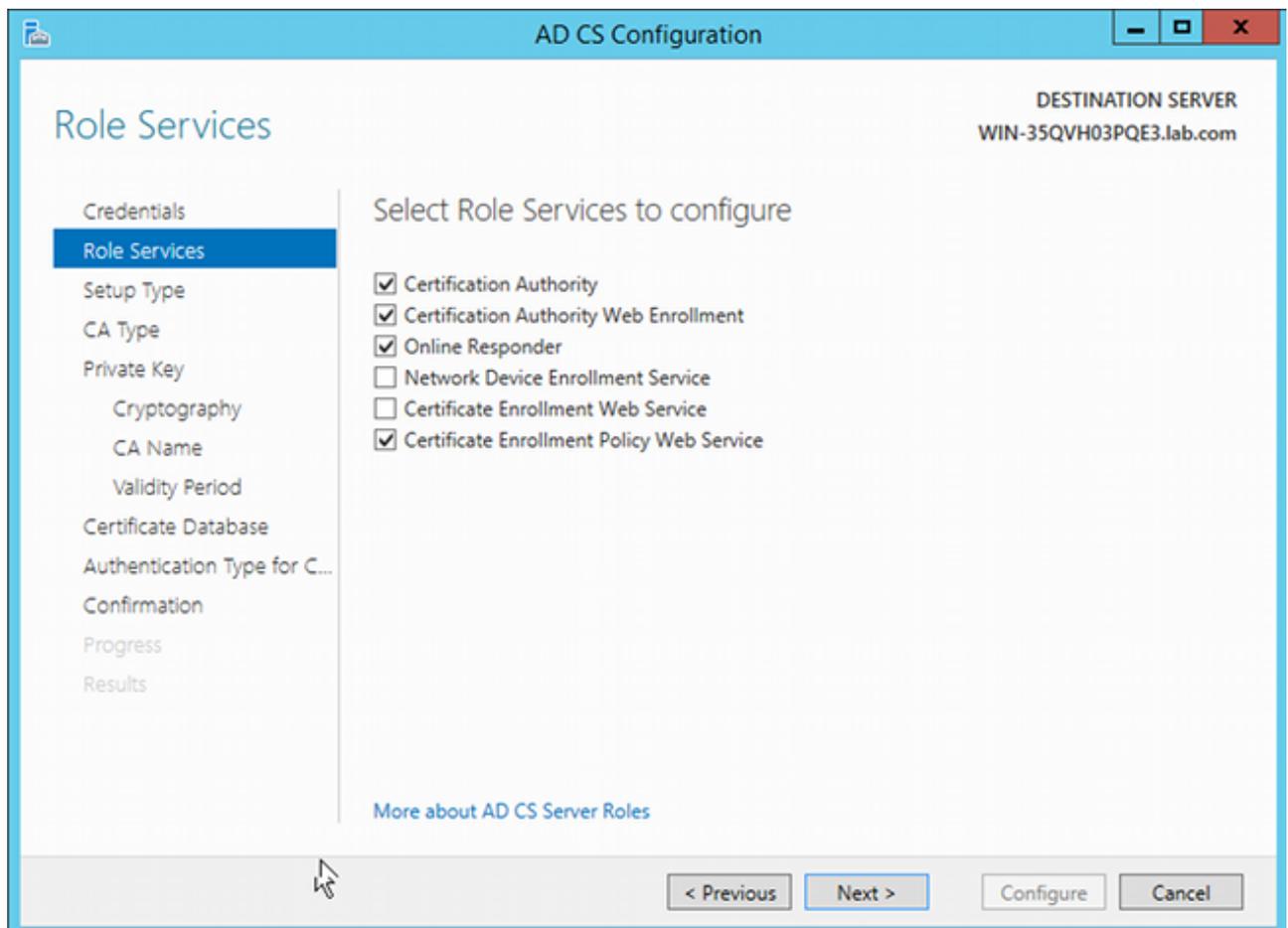
Hinweis: Siehe [Cisco ASA 5500 Series Configuration Guide using the CLI, 8.4 and 8.6: Configuring an External Server for Security Appliance User Authorization \(Konfigurationsanleitung für die Cisco ASA der Serie 5500 unter Verwendung der CLI, 8.4 und 8.6: Konfigurieren eines externen Servers für die Benutzerautorisierung der Security Appliance\)](#).

Installation von Services

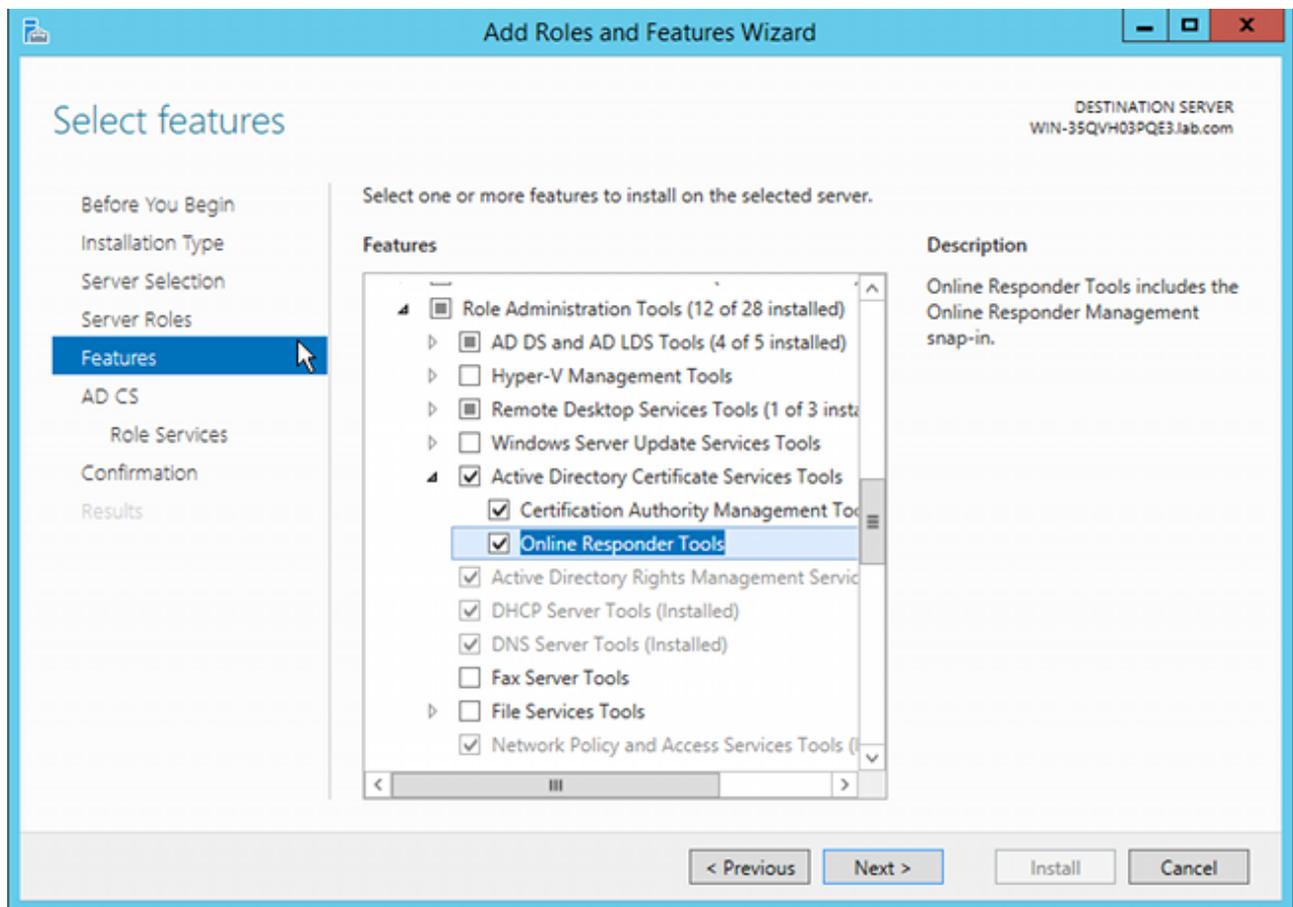
In diesem Verfahren wird beschrieben, wie Sie Rollendienste für den Microsoft-Server konfigurieren:

1. Navigieren Sie zu **Server Manager > Verwalten > Rollen und Funktionen hinzufügen**. Der Microsoft-Server benötigt folgende Rollendienste:

Zertifizierungsstelle Certification Authority Web Enrollment (Webregistrierung der Zertifizierungsstelle), die vom Client verwendet wird Online-Responder für OCSP erforderlich Network Device Enrollment Service, der die von der ASA verwendete SCEP-Anwendung enthält Bei Bedarf kann ein Webdienst mit Richtlinien hinzugefügt werden.



- 2.
- 3.
4. Stellen Sie beim Hinzufügen von Funktionen sicher, dass Sie Online-Responder-Tools verwenden, da diese ein OCSP-Snap-In enthalten, das später verwendet wird:



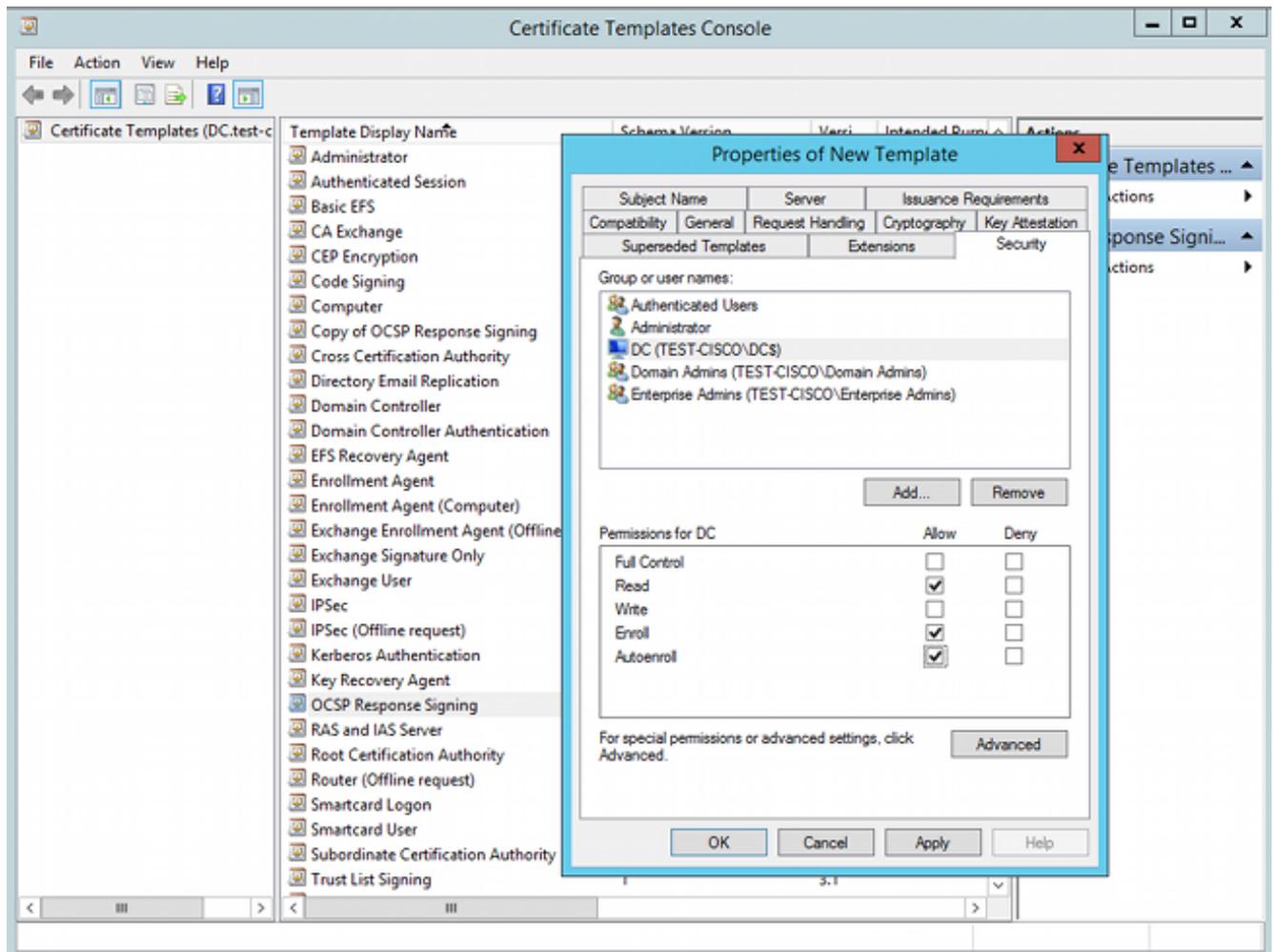
CA-Konfiguration für OCSP-Vorlage

Der OCSP-Dienst verwendet ein Zertifikat, um die OCSP-Antwort zu signieren. Es muss ein spezielles Zertifikat auf dem Microsoft-Server generiert werden, das Folgendes enthalten muss:

- Erweiterte Schlüsselverwendung = OCSP-Signierung
- OCSP - keine Widerrufsprüfung

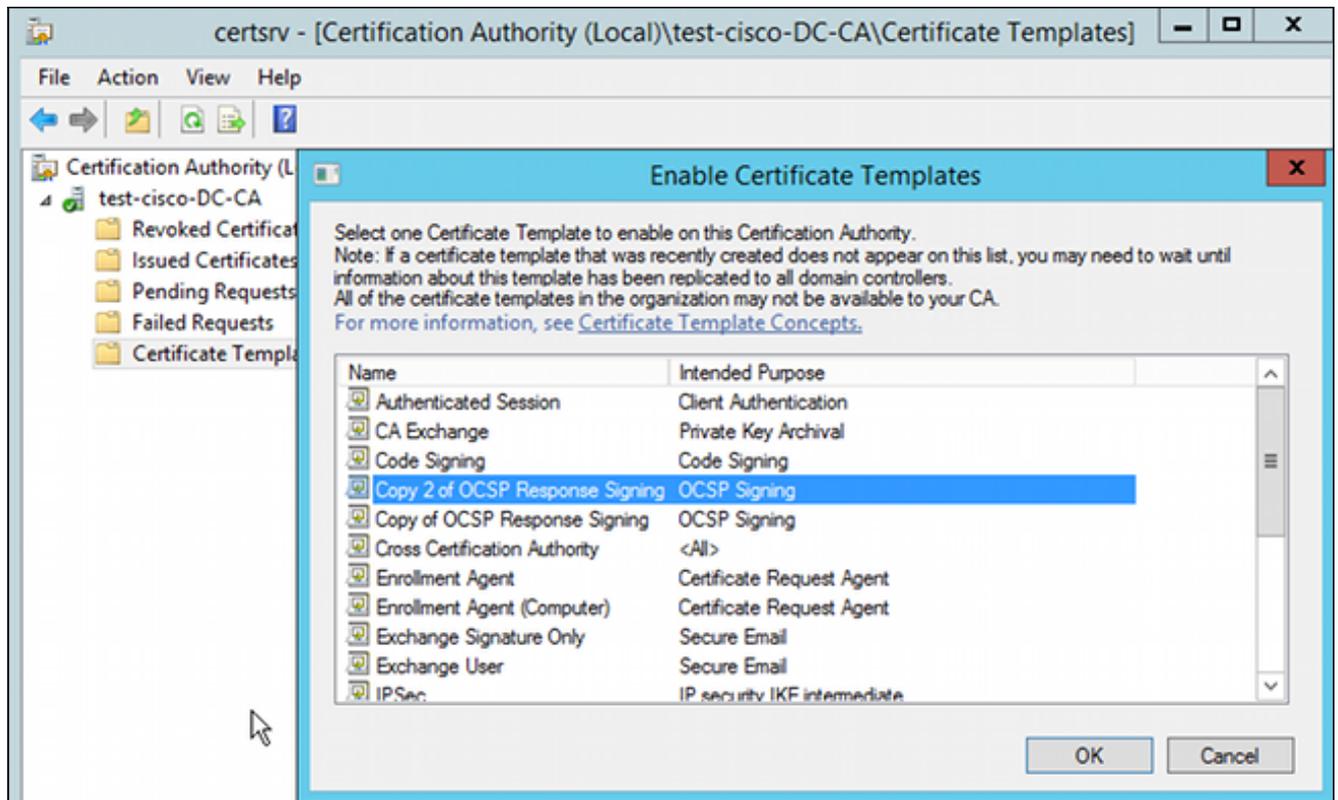
Dieses Zertifikat wird benötigt, um OCSP-Validierungsschleifen zu verhindern. ASA verwendet den OCSP-Dienst nicht, um das vom OCSP-Dienst vorgelegte Zertifikat zu überprüfen.

1. Fügen Sie der Zertifizierungsstelle eine Vorlage für das Zertifikat hinzu. Navigieren Sie zu **CA > Certificate Template > Manage**, wählen Sie **OCSP Response Signing aus**, und duplizieren Sie die Vorlage. Zeigen Sie die Eigenschaften der neu erstellten Vorlage an, und klicken Sie auf die Registerkarte **Sicherheit**. Die Berechtigungen beschreiben, welche Entität ein Zertifikat anfordern darf, das diese Vorlage verwendet. Daher sind die richtigen Berechtigungen erforderlich. In diesem Beispiel ist die Einheit der OCSP-Dienst, der auf demselben Host ausgeführt wird (TEST-CISCO\DC), und der OCSP-Dienst benötigt die Berechtigung zur automatischen Registrierung:



Alle anderen Einstellungen für die Vorlage können auf die Standardeinstellung gesetzt werden.

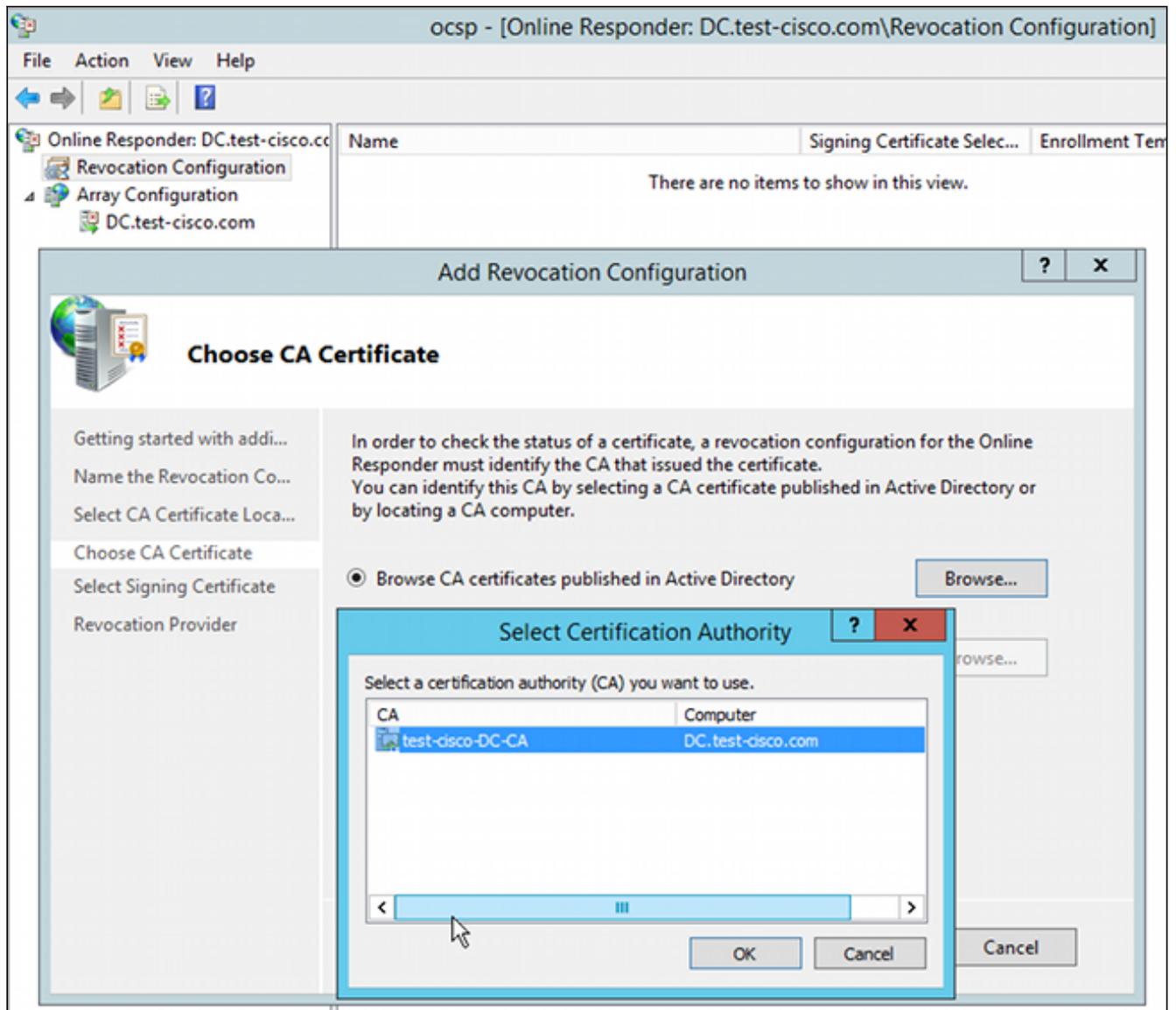
2. Aktivieren der Vorlage Navigieren Sie zu **CA > Certificate Template > New > Certificate Template to Issue**, und wählen Sie die doppelte Vorlage aus:



OCSP-Dienstzertifikat

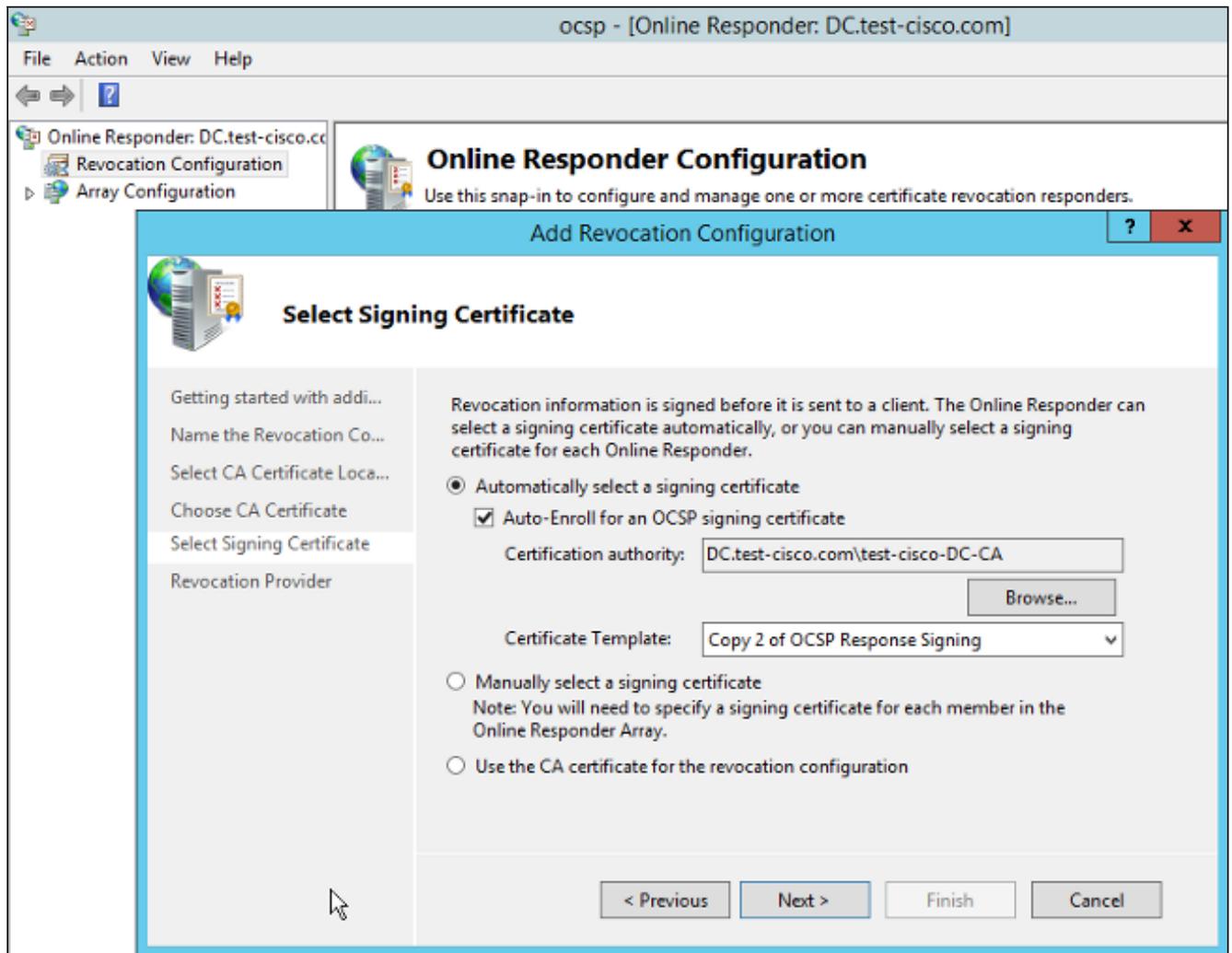
Dieses Verfahren beschreibt die Verwendung von Online Configuration Management zur Konfiguration von OCSP:

1. Navigieren Sie zu **Server Manager > Tools**.
2. Navigieren Sie zu **Sperrkonfiguration > Sperrkonfiguration hinzufügen**, um eine neue Konfiguration hinzuzufügen:

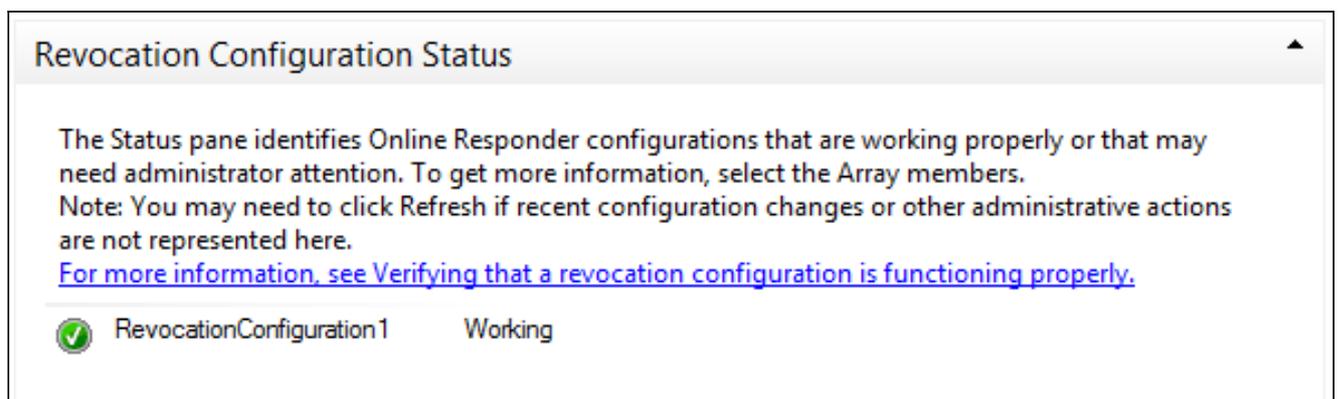


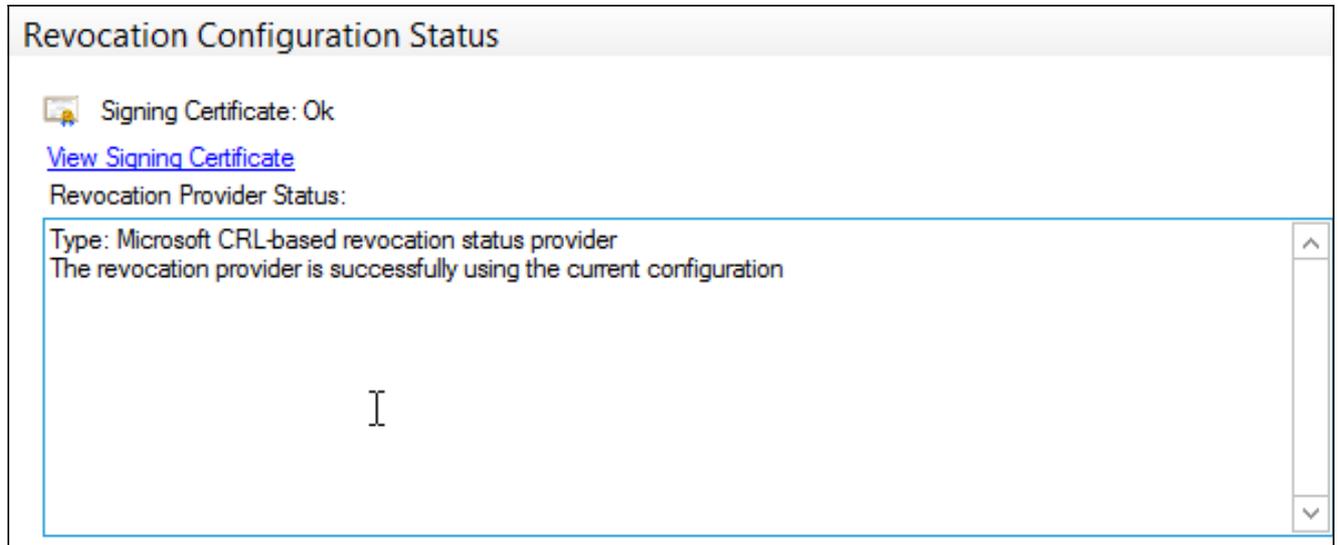
OCSP kann dieselbe Unternehmenszertifizierungsstelle verwenden. Das Zertifikat für den OCSP-Dienst wird generiert.

3. Wählen Sie die ausgewählte Enterprise-CA und die zuvor erstellte Vorlage aus. Das Zertifikat wird automatisch registriert:

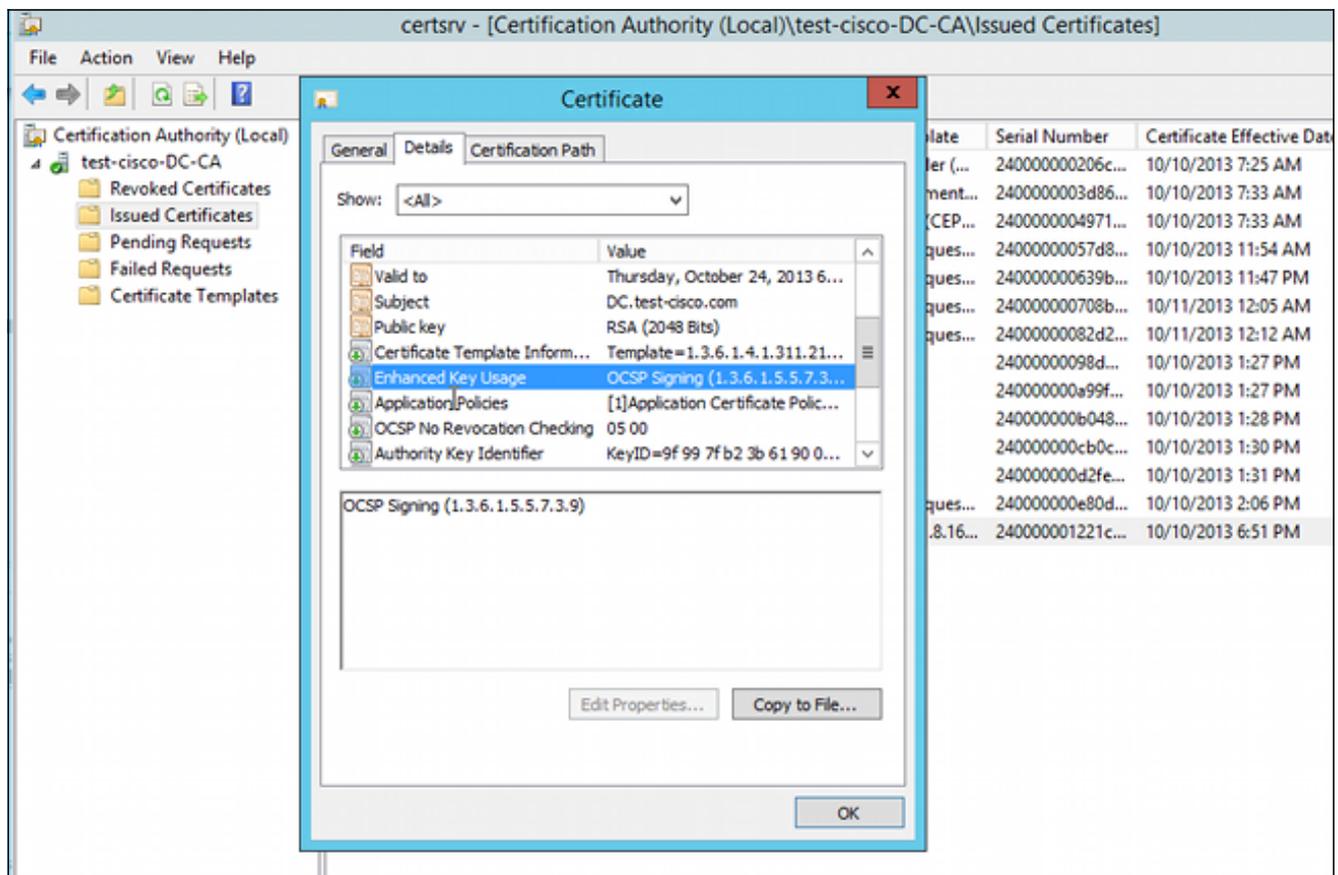


4. Bestätigen Sie, dass das Zertifikat registriert ist und der Status "Working/OK" lautet:





5. Navigieren Sie zu **CA > Ausgestellte Zertifikate**, um die Zertifikatdetails zu überprüfen:

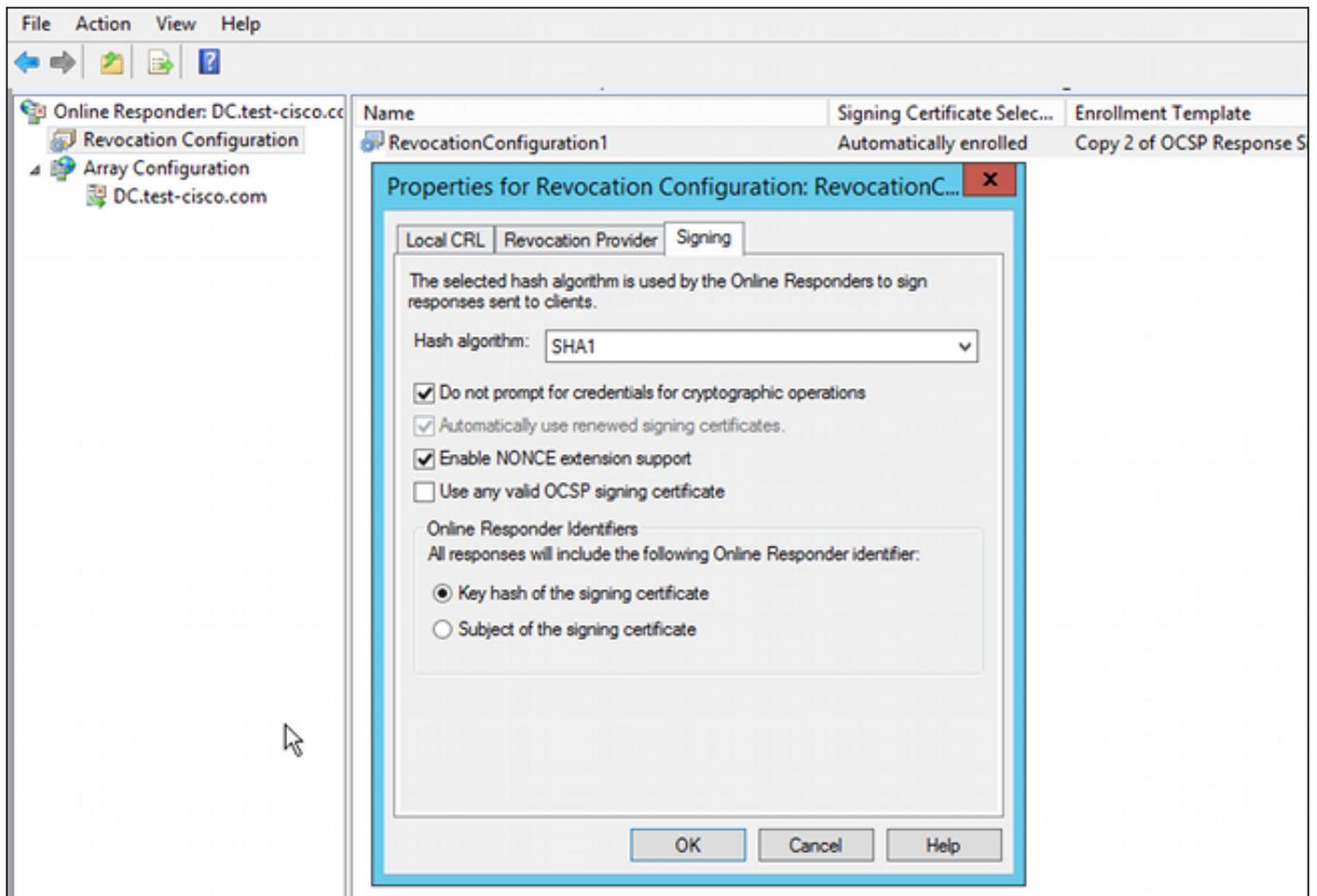


OCSP-Service-Nichtigkeiten

Die Microsoft-Implementierung von OCSP ist mit [RFC 5019 The Lightweight Online Certificate Status Protocol \(OCSP\) Profile for High-Volume Environments](#) konform. Dies ist eine vereinfachte Version des [RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP](#).

Die ASA verwendet RFC 2560 für OCSP. Einer der Unterschiede zwischen den beiden RFCs besteht darin, dass RFC 5019 keine signierten Anfragen akzeptiert, die von der ASA gesendet werden.

Es ist möglich, den Microsoft OCSP-Dienst zu zwingen, diese signierten Anfragen anzunehmen und mit der richtigen signierten Antwort zu antworten. Navigieren Sie zu **Revocation Configuration > RevocationConfiguration1 > Edit Properties**, und wählen Sie die Option zum **Aktivieren der NONCE-Erweiterungsunterstützung** aus.



Der OCSP-Service ist jetzt einsatzbereit.

Obwohl Cisco dies nicht empfiehlt, können Nonces auf dem ASA-Gerät deaktiviert werden:

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

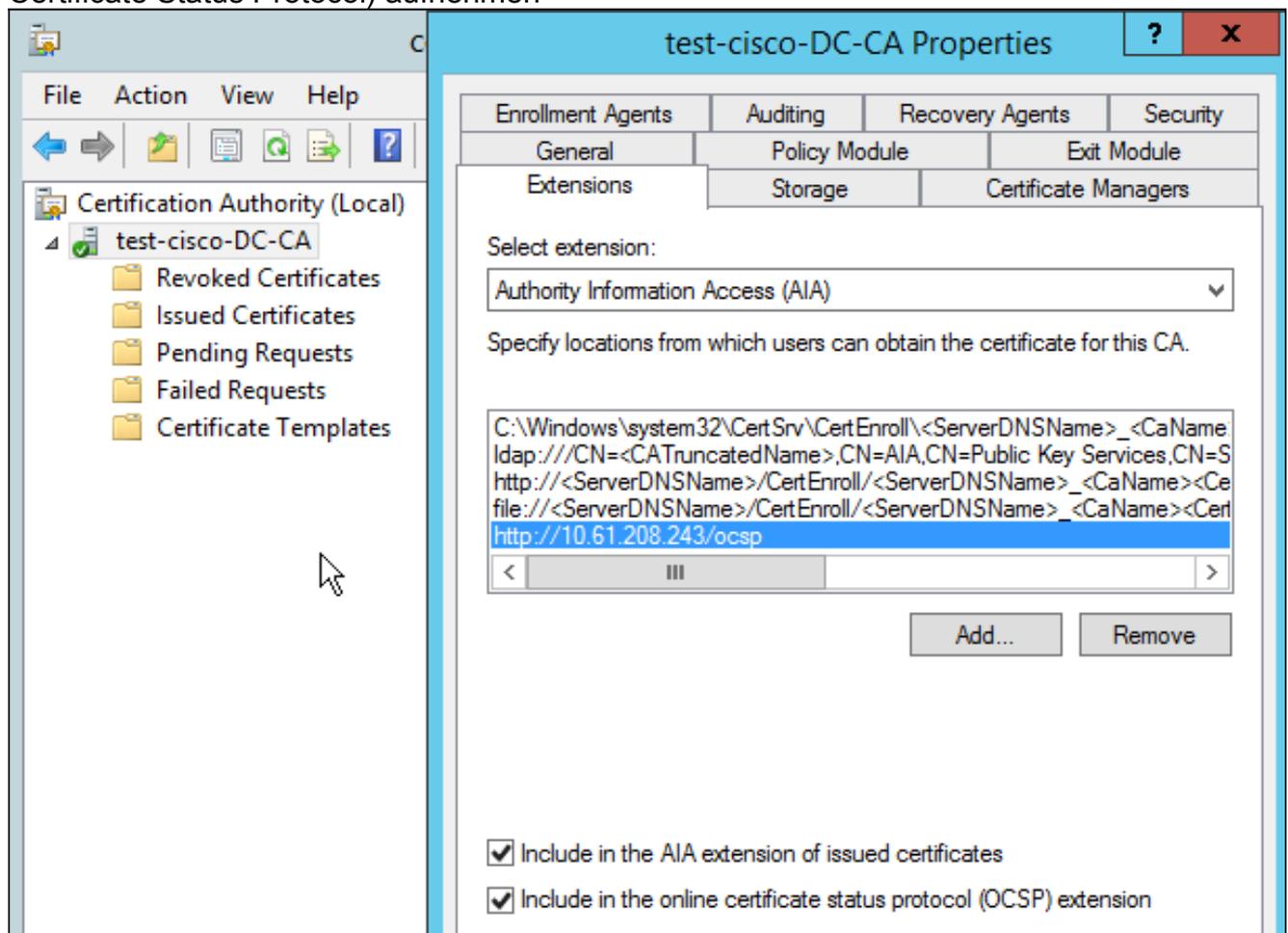
CA-Konfiguration für OCSP-Erweiterungen

Sie müssen nun die CA neu konfigurieren, um die OCSP-Servererweiterung in alle ausgestellten Zertifikate aufzunehmen. Die URL dieser Erweiterung wird von der ASA verwendet, um eine Verbindung zum OCSP-Server herzustellen, wenn ein Zertifikat validiert wird.

1. Öffnen Sie das Dialogfeld Eigenschaften für den Server auf der Zertifizierungsstelle.
2. Klicken Sie auf die Registerkarte **Erweiterungen**. Hierfür ist die Durchwahl "Authority Information Access" (AIA) erforderlich, die auf den OCSP-Service verweist. In diesem Beispiel ist dies "http://10.61.208.243/ocsp". Aktivieren Sie beide Optionen für die AIA-Erweiterung:

In die AIA-Erweiterung ausgestellter Zertifikate aufnehmen In OCSP-Erweiterung (Online

Certificate Status Protocol) aufnehmen



Dadurch wird sichergestellt, dass alle ausgestellten Zertifikate über eine richtige Erweiterung verfügen, die auf den OCSP-Service verweist.

OpenSSL

Hinweis: Siehe [Cisco ASA 5500 Series Configuration Guide using the CLI, 8.4 and 8.6: Configuring an External Server for Security Appliance User Authorization](#) (Konfigurationsanleitung für die Cisco ASA der Serie 5500 unter Verwendung der CLI, 8.4 und 8.6: Konfigurieren eines externen Servers für die Benutzerautorisierung der Security Appliance).

In diesem Beispiel wird davon ausgegangen, dass der OpenSSL-Server bereits konfiguriert ist. In diesem Abschnitt werden nur die OCSP-Konfiguration und die für die CA-Konfiguration erforderlichen Änderungen beschrieben.

In diesem Verfahren wird beschrieben, wie das OCSP-Zertifikat generiert wird:

1. Diese Parameter werden für den OCSP-Responder benötigt:

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

2. Diese Parameter werden für Benutzerzertifikate benötigt:

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

3. Zertifikate müssen von der Zertifizierungsstelle generiert und signiert werden.

4. Starten Sie den OCSP-Server:

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

5. Testen Sie das Beispielzertifikat:

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

Weitere Beispiele finden Sie auf [der OpenSSL-Website](#) .

OpenSSL unterstützt wie ASA OCSP-Nonces; die Nonces können mit den Switches `-nonce` und `-no_nonce` gesteuert werden.

ASA mit mehreren OCSP-Quellen

Die ASA kann die OCSP-URL überschreiben. Selbst wenn das Client-Zertifikat eine OCSP-URL enthält, wird es von der Konfiguration auf dem ASA-Gerät überschrieben:

```
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
```

Die OCSP-Serveradresse kann explizit definiert werden. Dieses Befehlsbeispiel vergleicht alle Zertifikate mit dem Administrator im Antragstellernamen, verwendet einen OPENSSL-Vertrauenspunkt zur Validierung der OCSP-Signatur und verwendet die URL `http://11.11.11.11/ocsp`, um die Anforderung zu senden:

```
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
```

Die verwendete Reihenfolge für die Suche nach der OCSP-URL lautet:

1. Ein OCSP-Server, den Sie mit dem Befehl **match certificate** festlegen
2. Ein OCSP-Server, den Sie mit dem Befehl **ocsp url** festlegen
3. Der OCSP-Server im AIA-Feld des Client-Zertifikats

ASA mit OCSP, von anderer Zertifizierungsstelle signiert

Eine OCSP-Antwort kann von einer anderen Zertifizierungsstelle signiert werden. In diesem Fall muss der Befehl **match certificate** verwendet werden, um einen anderen Vertrauenspunkt auf der ASA für die OCSP-Zertifikatsvalidierung zu verwenden.

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

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

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

In diesem Beispiel verwendet die ASA die OCSP-URL rewrite für alle Zertifikate mit einem Antragstellernamen, der Administrator enthält. Die ASA ist gezwungen, das OCSP-Responder-Zertifikat anhand eines anderen Trustpoints, OPENS, zu validieren. Benutzerzertifikate werden weiterhin im WIN2012 Trustpoint validiert.

Da das OCSP-Responder-Zertifikat die Erweiterung "OCSP no revocation check" aufweist, wird das Zertifikat nicht verifiziert, auch wenn OCSP gezwungen ist, es mit dem OPENS-Trustpoint zu validieren.

Standardmäßig werden alle Vertrauenspunkte durchsucht, wenn die ASA versucht, das Benutzerzertifikat zu überprüfen. Die Validierung für das OCSP-Responder-Zertifikat ist anders. Die ASA durchsucht nur den Vertrauenspunkt, der bereits für das Benutzerzertifikat gefunden wurde (in diesem Beispiel WIN2012).

Daher muss der Befehl **match certificate** verwendet werden, um die ASA zu zwingen, einen anderen Vertrauenspunkt für die OCSP-Zertifikatsvalidierung zu verwenden (in diesem Beispiel OPENS).

Benutzerzertifikate werden anhand des ersten übereinstimmenden Vertrauenspunkts (in diesem Beispiel WIN2012) validiert, der dann den Standardvertrauenspunkt für die OCSP-Antwortvalidierung bestimmt.

Wenn im Befehl **match certificate** kein spezifischer Vertrauenspunkt angegeben wird, wird das OCSP-Zertifikat anhand desselben Vertrauenspunkts wie die Benutzerzertifikate (in diesem Beispiel WIN2012) validiert:

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

Überprüfung

Nutzen Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß

funktioniert.

Hinweis: Das [Output Interpreter Tool](#) (nur für [registrierte](#) Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter-Tool, um eine Analyse der **show**-Befehlsausgabe anzuzeigen.

ASA - Zertifikat über SCEP abrufen

In diesem Verfahren wird beschrieben, wie Sie das Zertifikat mithilfe von SCEP abrufen:

1. Dies ist der Authentifizierungsprozess für den Abruf des Zertifizierungsstellenzertifikats:

```
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

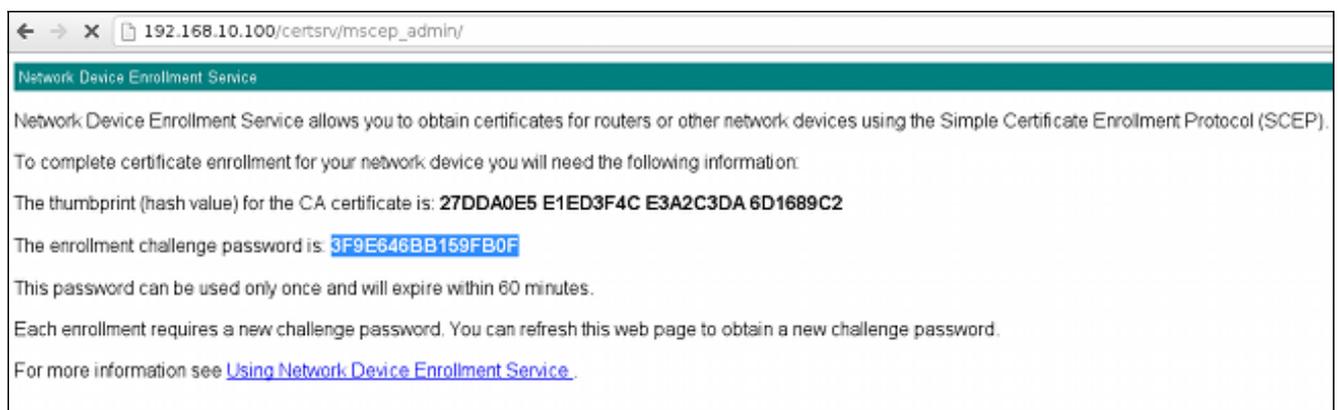
CRYPTO_PKI: http connection opened

INFO: Certificate has the following attributes:
Fingerprint:      27dda0e5 eled3f4c 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. Um das Zertifikat anzufordern, benötigt die ASA ein einmaliges SCEP-Kennwort, das über die Admin-Konsole unter http://IP/certsrv/mscep_admin abgerufen werden kann:



3. Verwenden Sie dieses Kennwort, um das Zertifikat auf der ASA anzufordern:

```

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
Einige Ausgaben wurden der Übersichtlichkeit halber weggelassen.

```

4. Überprüfen Sie die CA- und ASA-Zertifikate:

```

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

```

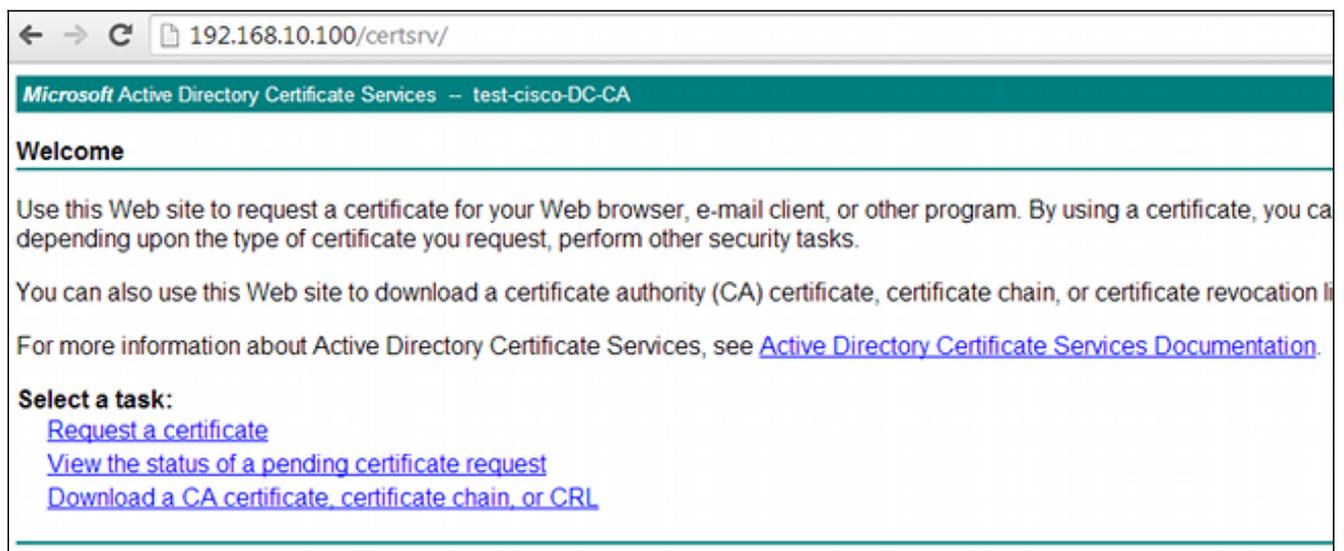
```
Certificate Serial Number: 3d4c0881b04c799f483f4bbe91dc98ae
Certificate Usage: Signature
Public Key Type: RSA (2048 bits)
Signature Algorithm: SHA1 with RSA Encryption
Issuer Name:
  cn=test-cisco-DC-CA
  dc=test-cisco
  dc=com
Subject Name:
  cn=test-cisco-DC-CA
  dc=test-cisco
  dc=com
Validity Date:
  start date: 07:23:03 CEST Oct 10 2013
  end   date: 07:33:03 CEST Oct 10 2018
Associated Trustpoints: WIN2012
```

Die meisten Zertifikatserweiterungen werden auf dem ASA-Gerät nicht angezeigt. Obwohl das ASA-Zertifikat die Erweiterung "OCSP URL in AIA" enthält, wird sie von der ASA CLI nicht angezeigt. Cisco Bug-ID [CSCui44335](#), "Anzeige von ASA ENH-Zertifikat-x509-Erweiterungen", fordert diese Erweiterung an.

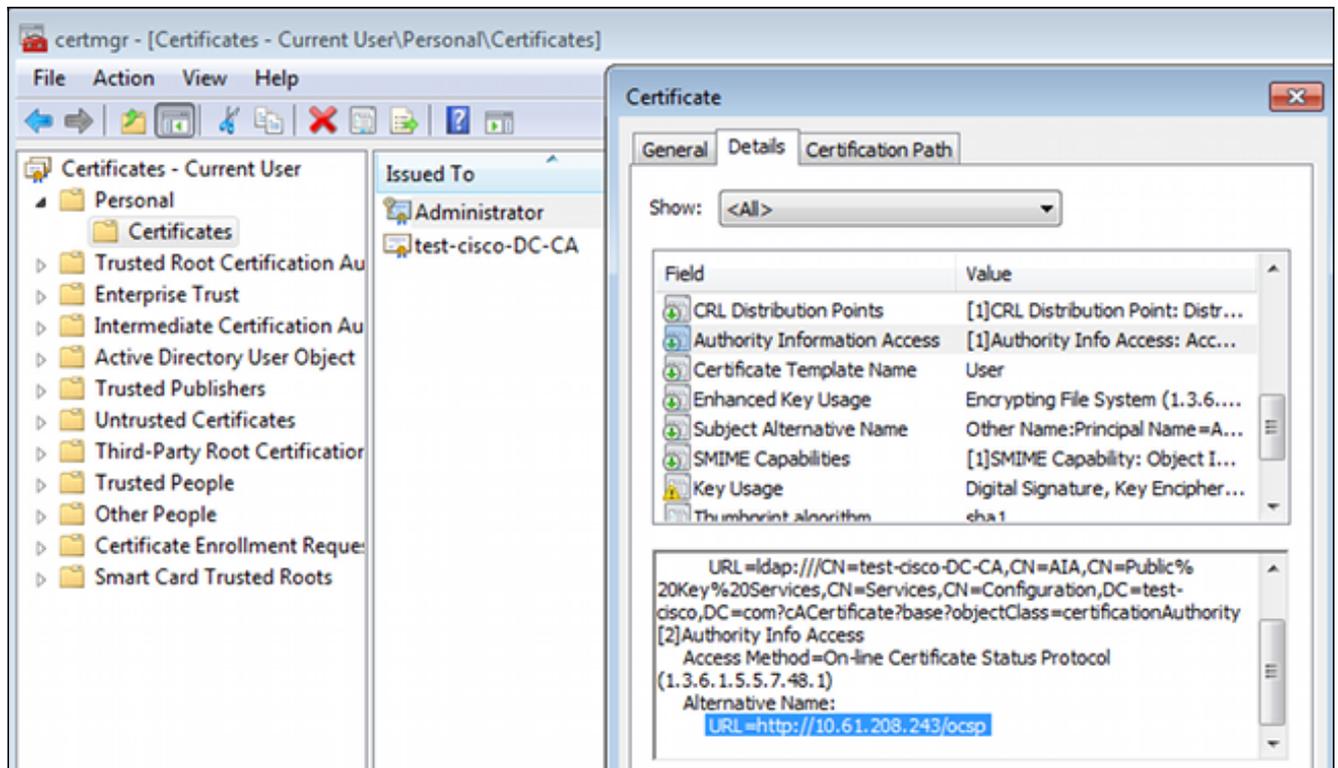
AnyConnect - Zertifikat über Webseite abrufen

In diesem Verfahren wird beschrieben, wie Sie das Zertifikat mithilfe des Webbrowsers auf dem Client abrufen:

1. Ein AnyConnect-Benutzerzertifikat kann über die Webseite angefordert werden. Verwenden Sie auf dem Client-PC einen Webbrowser, um zur Zertifizierungsstelle zu wechseln, die sich unter <http://IP/certsrv> befindet:



2. Das Benutzerzertifikat kann im Webbrowserspeicher gespeichert und dann in den Microsoft-Speicher exportiert werden, der von AnyConnect durchsucht wird. Verwenden Sie `certmgr.msc`, um das empfangene Zertifikat zu überprüfen:



AnyConnect kann das Zertifikat auch anfordern, sofern ein korrektes AnyConnect-Profil vorhanden ist.

ASA VPN Remote Access mit OCSP-Validierung

In diesem Verfahren wird beschrieben, wie die OCSP-Validierung überprüft wird:

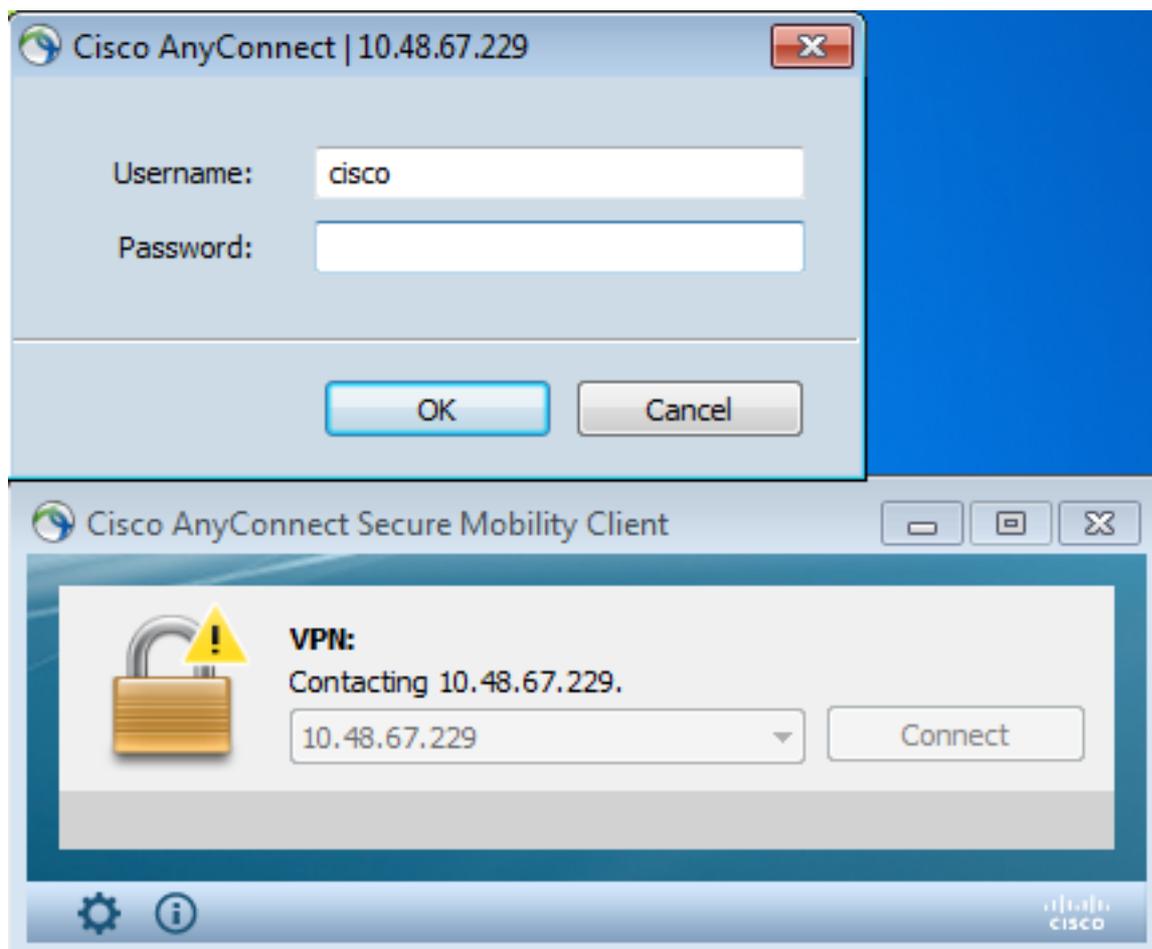
1. Während des Verbindungsversuchs meldet die ASA, dass das Zertifikat auf OCSP überprüft wird. Hier hat das OCSP-Signaturzertifikat eine Nicht-Prüferweiterung und wurde nicht über OCSP geprüft:

```
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: 240000001B2AD208B128116874000000000001B, 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.
```

Einige Ausgaben wurden der Übersichtlichkeit halber weggelassen.

2. Der Endbenutzer gibt die Anmeldeinformationen des Benutzers an:



3. Die VPN-Sitzung wurde ordnungsgemäß beendet:

```
%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. Die Sitzung wird erstellt:

```
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. Für die OCSP-Validierung können Sie detaillierte Debugging-Methoden verwenden:

```
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. Auf der Ebene der Paketerfassung ist dies die OCSP-Anfrage und die richtige OCSP-Antwort. Die Antwort enthält die richtige Signatur - Nonce-Erweiterung aktiviert auf Microsoft OCSP:

No.	Source	Destination	Protocol	Length	Info
24	10.48.67.229	10.61.208.243	OCSP	545	Request
31	10.61.208.243	10.48.67.229	OCSP	700	Response

- Hypertext Transfer Protocol
- ▾ Online Certificate Status Protocol
 - responseStatus: successful (0)
 - ▾ responseBytes
 - ResponseType Id: 1.3.6.1.5.5.7.48.1.1 (id-pkix-ocsp-basic)
 - ▾ BasicOCSPResponse
 - ▾ tbsResponseData
 - responderID: byKey (2)
 - producedAt: 2013-10-12 14:48:27 (UTC)
 - responses: 1 item
 - ▾ responseExtensions: 1 item
 - ▾ Extension
 - Id: 1.3.6.1.5.5.7.48.1.2 (id-pkix.48.1.2)
 - BER: Dissector for OID:1.3.6.1.5.5.7.48.1.2 not implemented.
 - signatureAlgorithm (shaWithRSAEncryption)
 - Padding: 0
 - signature: 353fc461732dc47b1d167ebace677a087765b48edb3b284c...
 - certs: 1 item

ASA VPN-Remote-Zugriff mit mehreren OCSP-Quellen

Wenn ein Übereinstimmungszertifikat wie in [ASA mit mehreren OCSP-Quellen](#) erläutert konfiguriert wird, hat es Vorrang:

```
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: OPENSSEL
```

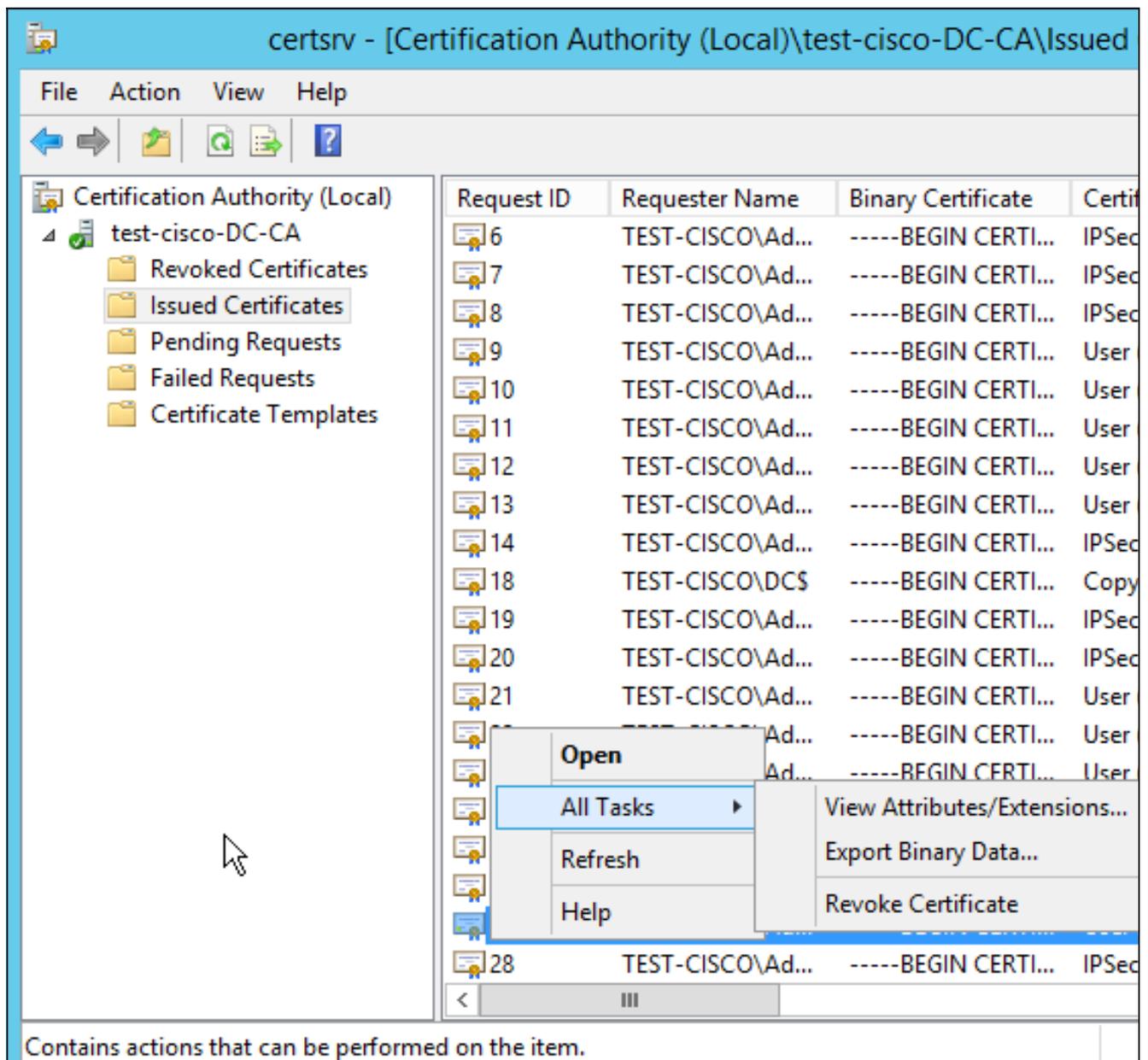
Wenn eine OCSP-URL überschrieben wird, lauten die Fehlerbehebungsschritte:

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

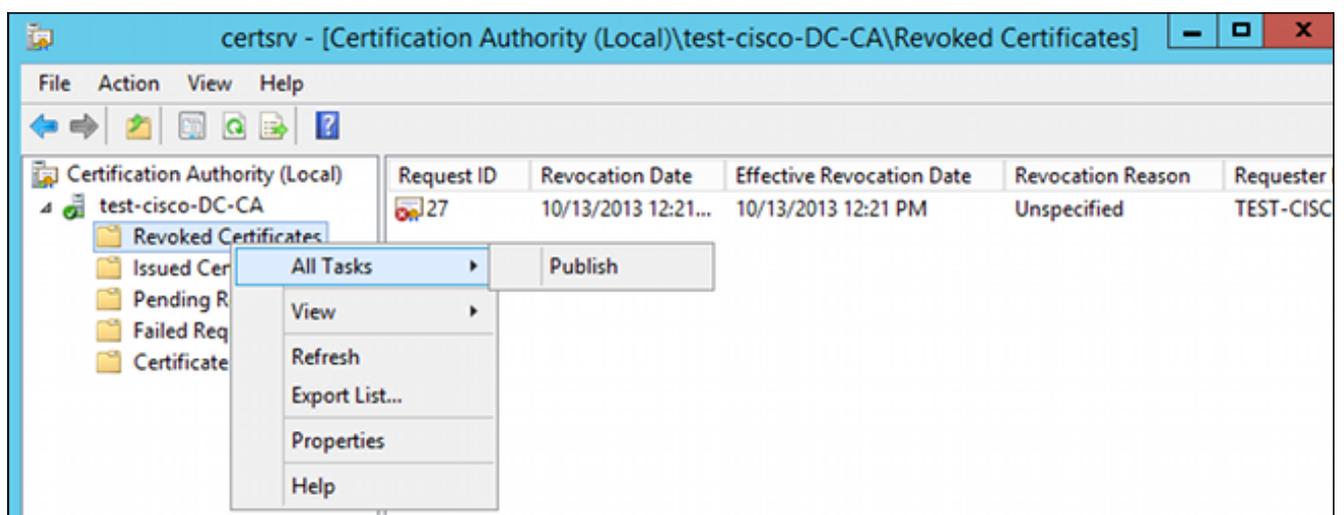
ASA VPN-Remote-Zugriff mit OCSP und widerrufenem Zertifikat

In diesem Verfahren wird beschrieben, wie Sie das Zertifikat widerrufen und den widerrufenen Status bestätigen:

1. Clientzertifikat aufheben:



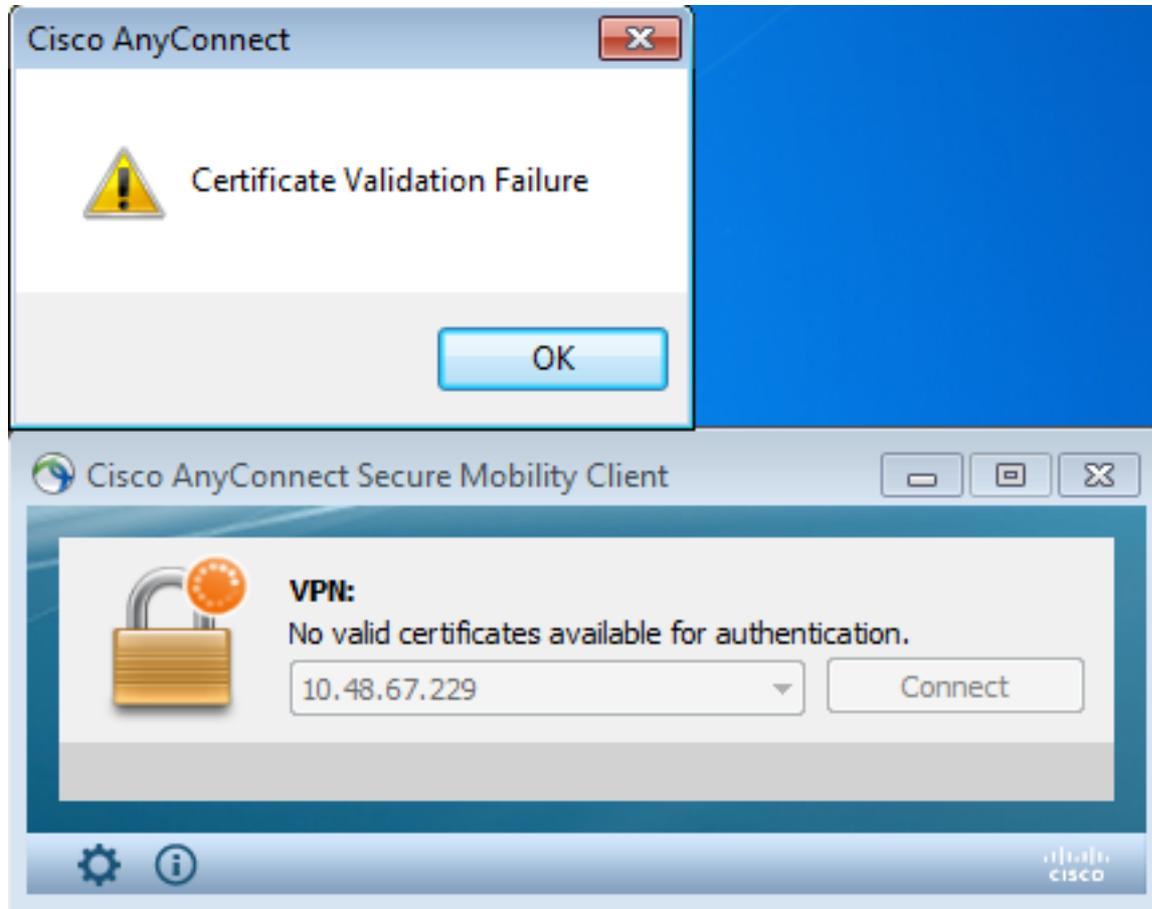
2. Veröffentlichen Sie die Ergebnisse:



3. [Optional] Die Schritte 1 und 2 können auch mit dem Dienstprogramm certutil CLI in Power Shell durchgeführt werden:

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

4. Wenn der Client versucht, eine Verbindung herzustellen, liegt ein Zertifikatüberprüfungsfehler vor:



5. In den AnyConnect-Protokollen wird außerdem der Fehler bei der Zertifikatsvalidierung angezeigt:

```
[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. Die ASA meldet den Widerruf des Zertifikatsstatus:

```
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: **OCSF 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 GetOCSF completed**

CRYPTO_PKI: Received OCSF 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 OCSF response (trustpoint:
 WIN2012, status: 1)
 CRYPTO_PKI: Destroying OCSF data handle 0xae255ac0
 CRYPTO_PKI: OCSF 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. Die Paketerfassungen zeigen eine erfolgreiche OCSF-Antwort mit dem Zertifikatsstatus "Entzogen" an:

No.	Source	Destination	Protocol	Length	Info
24	10.48.67.229	10.61.209.83	OCSF	544	Request
31	10.61.209.83	10.48.67.229	OCSF	721	Response

- Hypertext Transfer Protocol
- ▾ Online Certificate Status Protocol
 - responseStatus: successful (0)
 - ▾ responseBytes
 - ResponseType Id: 1.3.6.1.5.5.7.48.1.1 (id-pkix-ocsp-basic)
 - ▾ BasicOCSPResponse
 - ▾ tbsResponseData
 - responderID: byKey (2)
 - producedAt: 2013-10-13 10:47:02 (UTC)
 - ▾ responses: 1 item
 - ▾ SingleResponse
 - certID
 - certStatus: revoked (1)
 - thisUpdate: 2013-10-13 10:17:51 (UTC)
 - nextUpdate: 2013-10-14 22:37:51 (UTC)
 - singleExtensions: 1 item
 - responseExtensions: 1 item
 - signatureAlgorithm (shaWithRSAEncryption)

Fehlerbehebung

In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

OCSP-Server ausgefallen

ASA meldet bei Ausfall des OCSP-Servers:

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

Paketerfassungen können auch bei der Fehlerbehebung helfen.

Zeit nicht synchronisiert

Wenn die aktuelle Uhrzeit auf dem OCSP-Server älter als auf ASA ist (geringfügige Abweichungen sind akzeptabel), sendet der OCSP-Server eine nicht autorisierte Antwort, und die ASA meldet Folgendes:

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

Wenn die ASA eine OCSP-Antwort aus zukünftigen Zeiten erhält, schlägt sie auch fehl.

Signierte Nonces werden nicht unterstützt

Wenn auf dem Server keine Nicht-Nachrichten unterstützt werden (dies ist die Standardeinstellung unter Microsoft Windows 2012 R2), wird eine nicht autorisierte Antwort zurückgegeben:

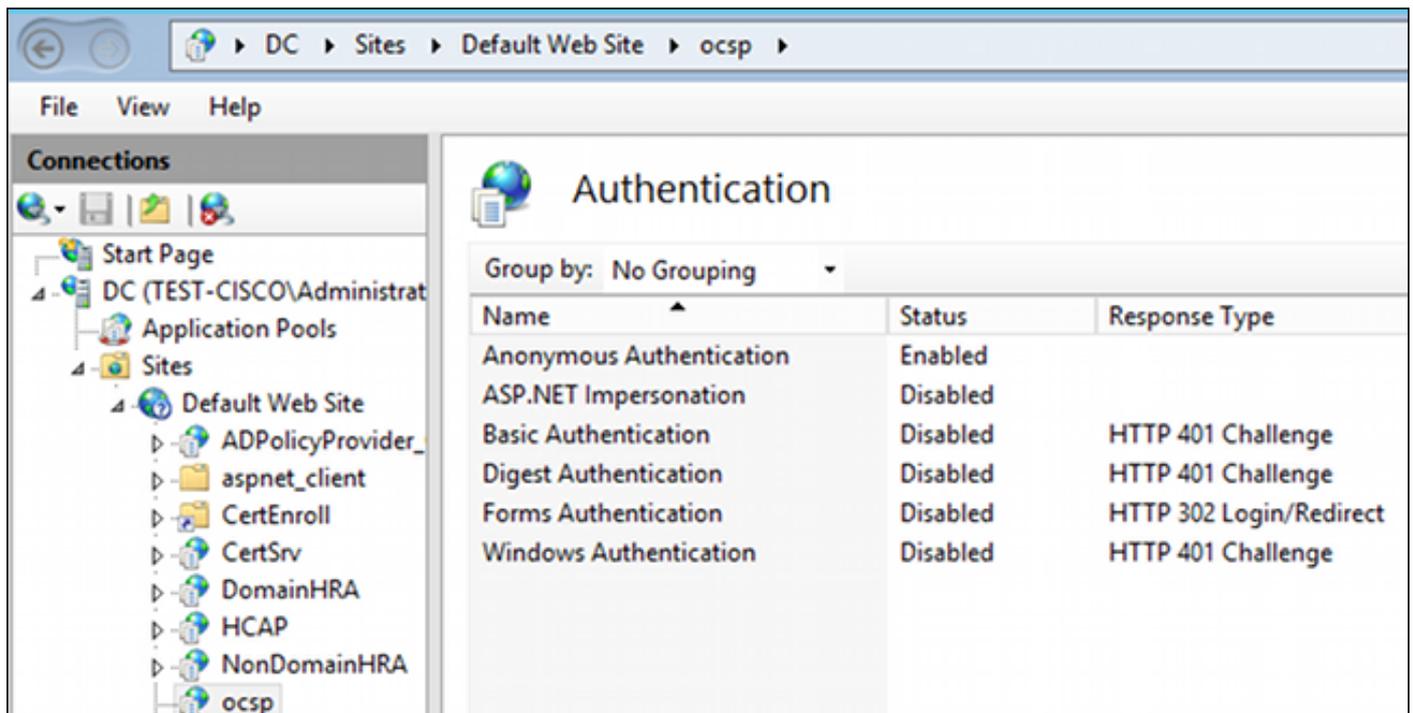
No.	Source	Destination	Protocol	Length	Info
56	10.48.67.229	10.61.208.243	OCSP	545	Request
59	10.61.208.243	10.48.67.229	OCSP	337	Response

▶ Frame 59: 337 bytes on wire (2696 bits), 337 bytes captured (2696 bits)
▶ Ethernet II, Src: Cisco_2a:c4:a3 (00:06:f6:2a:c4:a3), Dst: Cisco_b8:6b:25 (00:17:5
▶ Internet Protocol Version 4, Src: 10.61.208.243 (10.61.208.243), Dst: 10.48.67.229
▶ Transmission Control Protocol, Src Port: http (80), Dst Port: 14489 (14489), Seq:
▶ Hypertext Transfer Protocol
▼ Online Certificate Status Protocol
responseStatus: unauthorized (6)

IIS7-Serverauthentifizierung

Probleme mit einer SCEP-/OCSP-Anforderung sind häufig das Ergebnis einer falschen Authentifizierung in Internetinformationsdiensten 7 (IIS7). Stellen Sie sicher, dass der anonyme

Zugriff konfiguriert ist:



The screenshot shows the IIS Manager interface. The left pane displays the 'Connections' tree with the path: DC (TEST-CISCO\Administrat) > Sites > Default Web Site > ocsip. The right pane shows the 'Authentication' settings for the selected site. A table lists the authentication methods and their status.

Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Digest Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Disabled	HTTP 401 Challenge

Zugehörige Informationen

- [Microsoft TechNet: Online Responder - Installations-, Konfigurations- und Fehlerbehebungshandbuch](#)
- [Microsoft TechNet: Konfigurieren einer Zertifizierungsstelle zur Unterstützung von OCSP-Respondern](#)
- [Befehlsreferenz zur Cisco ASA-Serie](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.