VPN de acceso remoto ASA con verificación OCSP en Microsoft Windows 2012 y OpenSSL

Contenido

Introducción

Este documento describe cómo utilizar la validación del Protocolo de estado de certificados en línea (OCSP) en un Cisco Adaptive Security Appliance (ASA) para los certificados presentados por usuarios de VPN. Se presentan ejemplos de configuraciones para dos servidores OCSP (Microsoft Windows Certificate Authority [CA] y OpenSSL). La sección Verificación describe los

flujos detallados en el nivel de paquete, y la sección Resolución de problemas se centra en los errores y problemas típicos.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración de la interfaz de línea de comandos (CLI) del dispositivo de seguridad adaptable de Cisco y configuración de VPN de capa de socket seguro (SSL)
- Certificados X.509
- Servidor de Microsoft Windows
- Linux/OpenSSL

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Software Adaptive Security Appliance de Cisco, versión 8.4 y posteriores
- Microsoft Windows 7 con Cisco AnyConnect Secure Mobility Client, versión 3.1
- Microsoft Server 2012 R2
- Linux con OpenSSL 1.0.0j o posterior

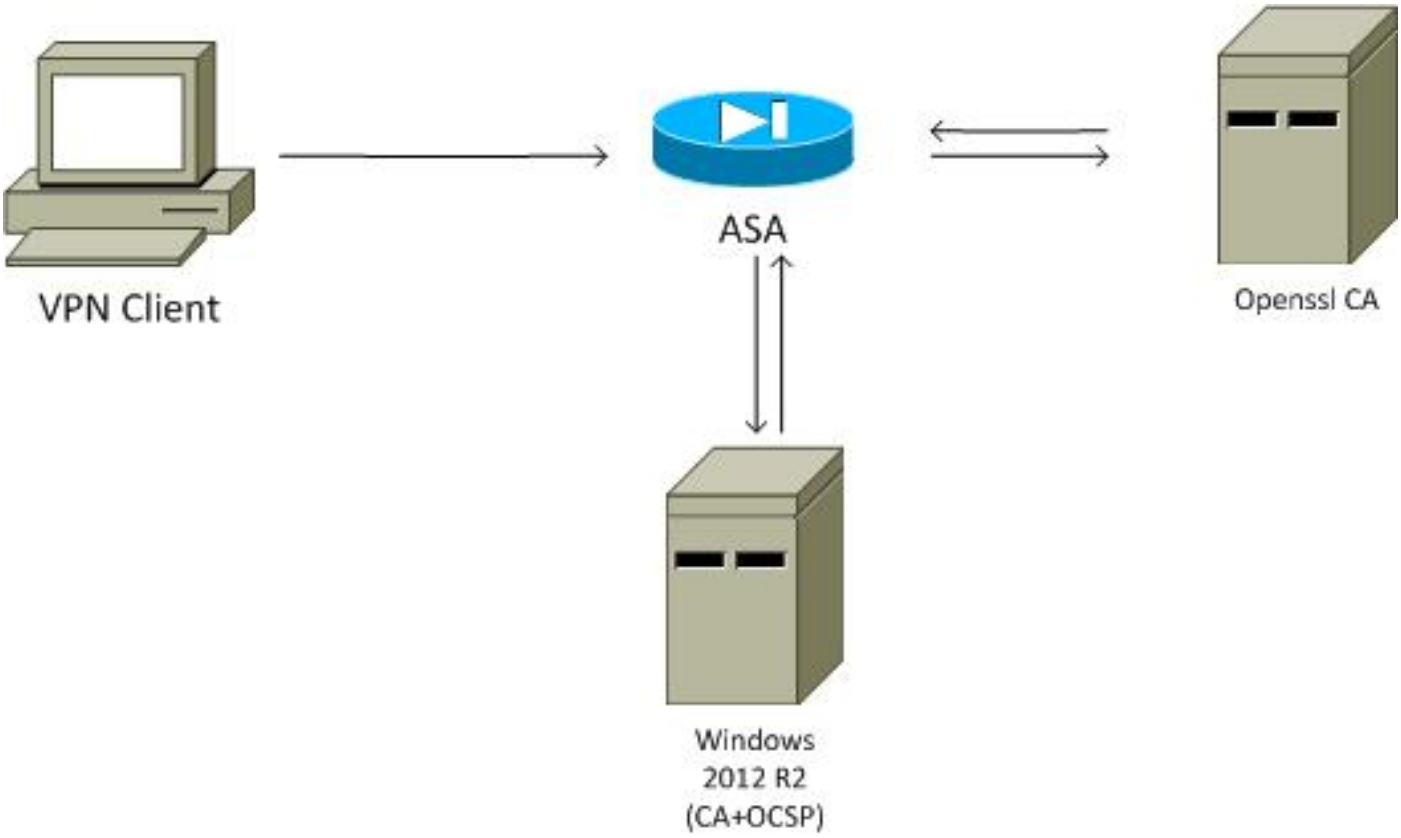
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

Configurar

> **Nota: Use el Command Lookup Tool (únicamente clientes registrados) para obtener más información sobre los comandos que se utilizan en esta sección.**

Diagrama de la red

El cliente utiliza VPN de acceso remoto. Este acceso puede ser Cisco VPN Client (IPSec), Cisco AnyConnect Secure Mobility (SSL/Intercambio de claves de Internet versión 2 [IKEv2]) o WebVPN (portal). Para iniciar sesión, el cliente proporciona el certificado correcto, así como el nombre de usuario/contraseña que se configuraron localmente en el ASA. El certificado de cliente se valida a través del servidor OCSP.



Acceso remoto a ASA con OCSP

ASA está configurado para el acceso SSL. El cliente está usando AnyConnect para iniciar sesión. El ASA utiliza el Protocolo de inscripción de certificado simple (SCEP) para solicitar el certificado:

```
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
```

Se crea un mapa de certificado para identificar a todos los usuarios cuyo nombre de sujeto contiene la palabra administrador (no distingue entre mayúsculas y minúsculas). Estos usuarios están vinculados a un grupo de túnel denominado 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
```

La configuración VPN requiere una autorización correcta (es decir, un certificado validado). También requiere las credenciales correctas para el nombre de usuario definido localmente (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
```

CA de Microsoft Windows 2012

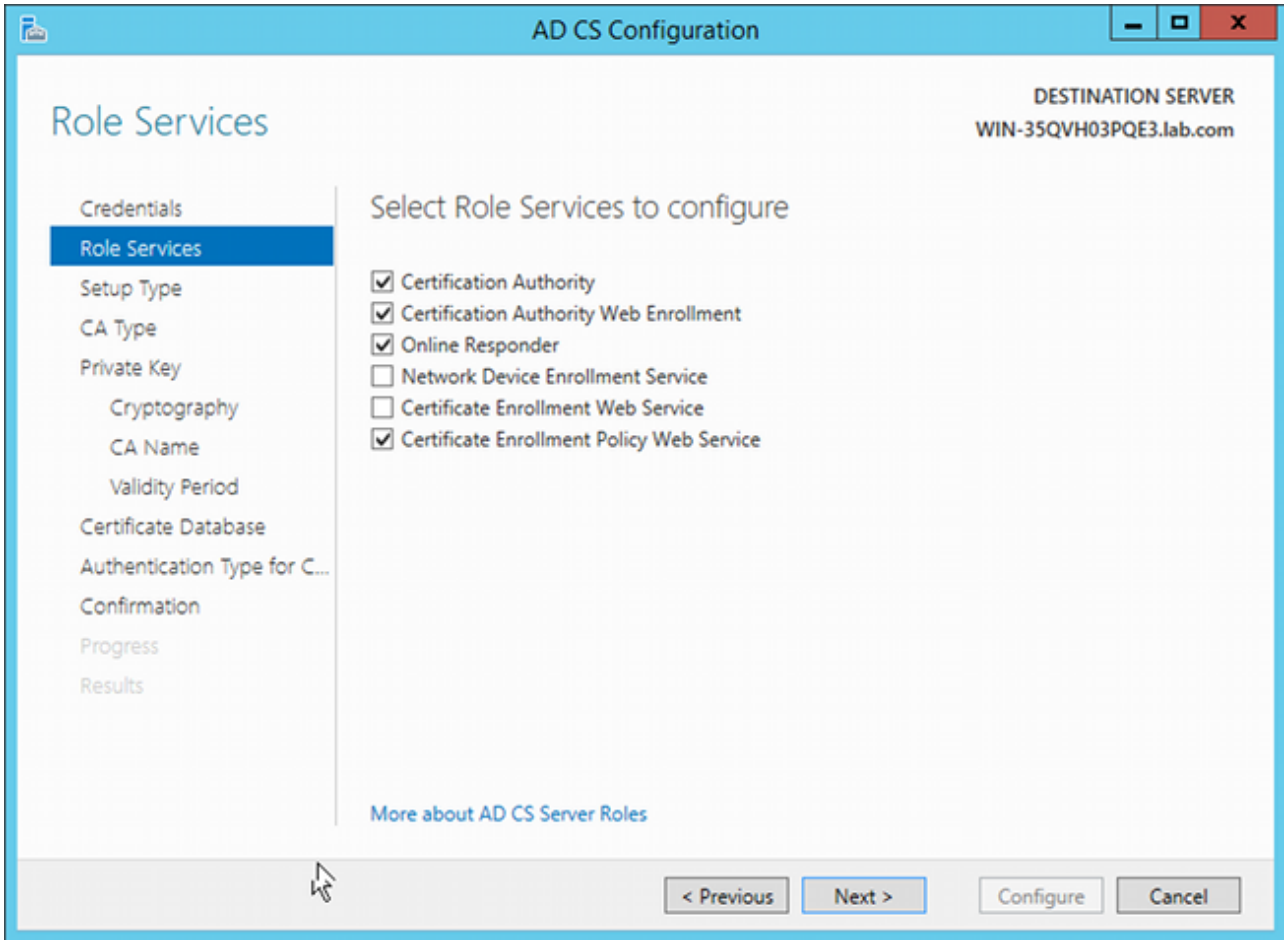
> **Nota**: Consulte la Guía de configuración de Cisco ASA serie 5500 con CLI, 8.4 y 8.6: Configuración de un servidor externo para la autorización de usuario de dispositivos de seguridad para obtener detalles sobre la configuración de ASA a través de CLI.

Instalación de servicios

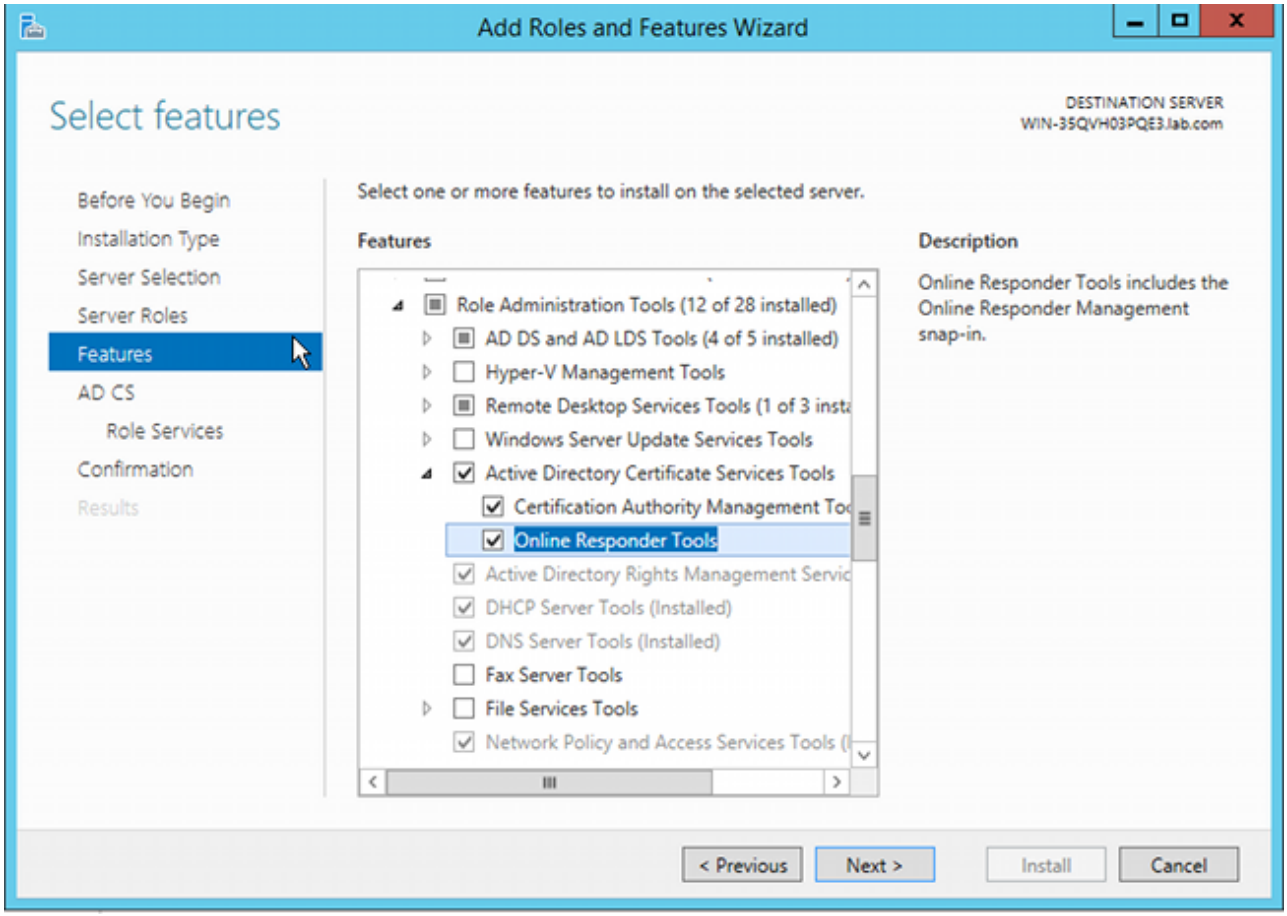
Este procedimiento describe cómo configurar los servicios de función para el servidor de Microsoft:

1. Vaya a **Administrador del servidor > Administrar > Agregar roles y características**. El servidor de Microsoft necesita estos servicios de rol:

   Entidad emisora de certificadosCertification Authority Web Enrollment, que utiliza el clienteRespondedor en línea, necesario para OCSPNetwork Device Enrollment Service, que contiene la aplicación SCEP utilizada por ASA Si es necesario, se puede agregar un servicio Web con directivas.



2.
3.
4. Cuando agregue características, asegúrese de incluir las Herramientas del Respondedor en línea, ya que incluye un complemento de OCSP que se utilizará más adelante:



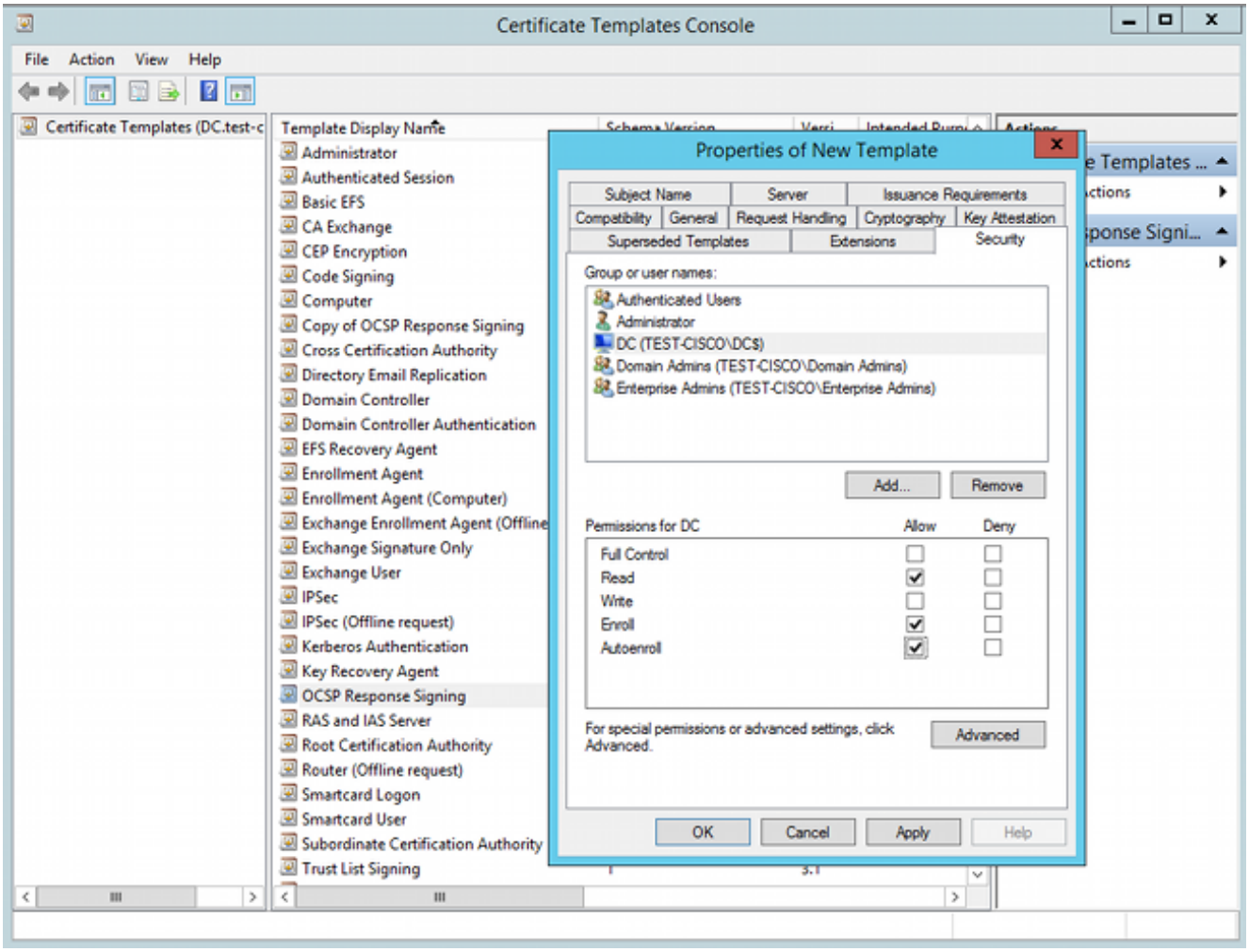
Configuración de CA para la plantilla OCSP

El servicio OCSP utiliza un certificado para firmar la respuesta de OCSP. Se debe generar un certificado especial en el servidor de Microsoft que debe incluir:

- Uso de clave extendido = firma OCSP
- Verificación de no revocación de OCSP

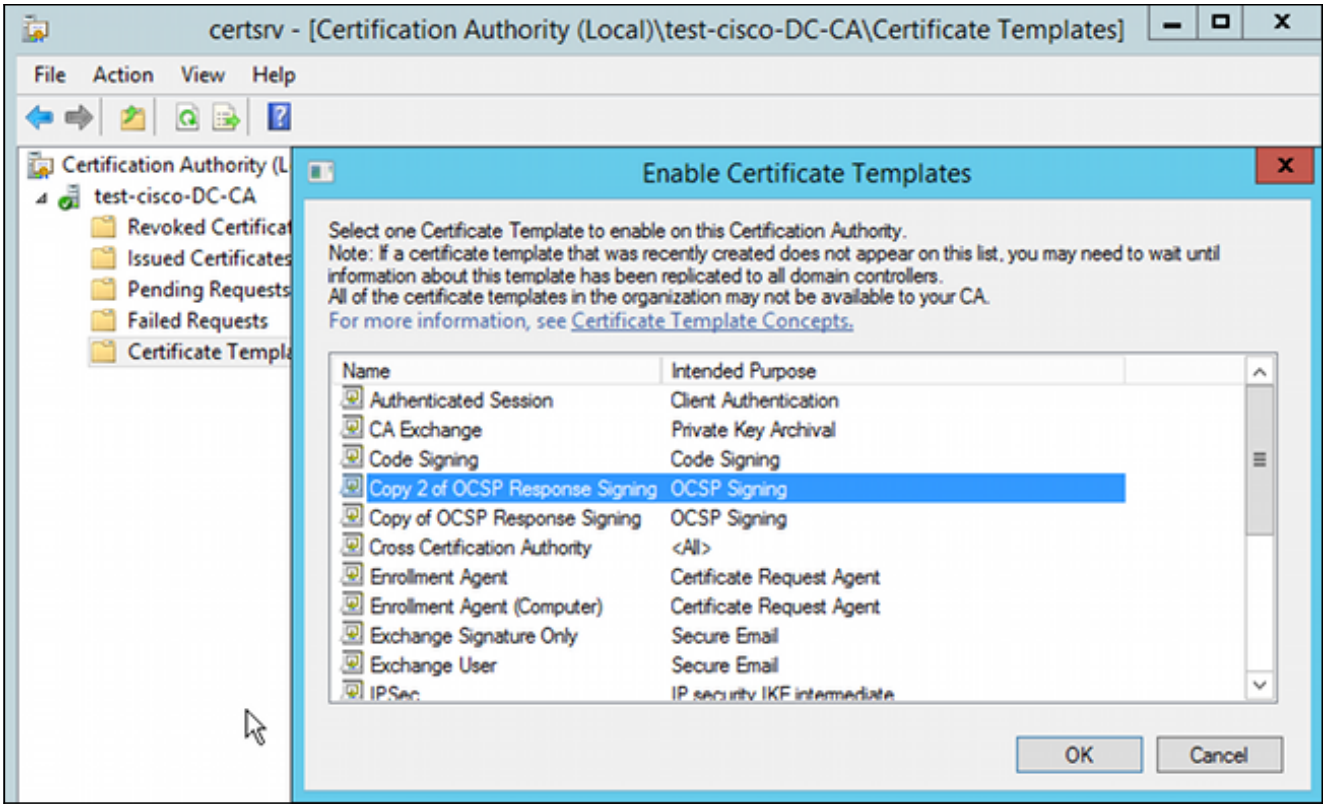
Este certificado es necesario para evitar bucles de validación de OCSP. ASA no utiliza el servicio OCSP para intentar comprobar el certificado presentado por el servicio OCSP.

1. Agregue una plantilla para el certificado en la CA. Navegue hasta **CA > Certificate Template > Manage**, seleccione **OCSP Response Signing** y duplique la plantilla. Vea las propiedades de la plantilla recién creada y haga clic en la pestaña **Seguridad**. Los permisos describen a qué entidad se le permite solicitar un certificado que utiliza esa plantilla, por lo que se requieren los permisos correctos. En este ejemplo, la entidad es el servicio OCSP que se ejecuta en el mismo host (TEST-CISCO\DC) y el servicio OCSP necesita privilegios de inscripción automática:



El resto de la configuración de la plantilla se puede establecer en el valor predeterminado.

2. Active la plantilla. Navegue hasta **CA > Plantilla de certificado > Nuevo > Plantilla de certificado para emitir**, y seleccione la plantilla duplicada:

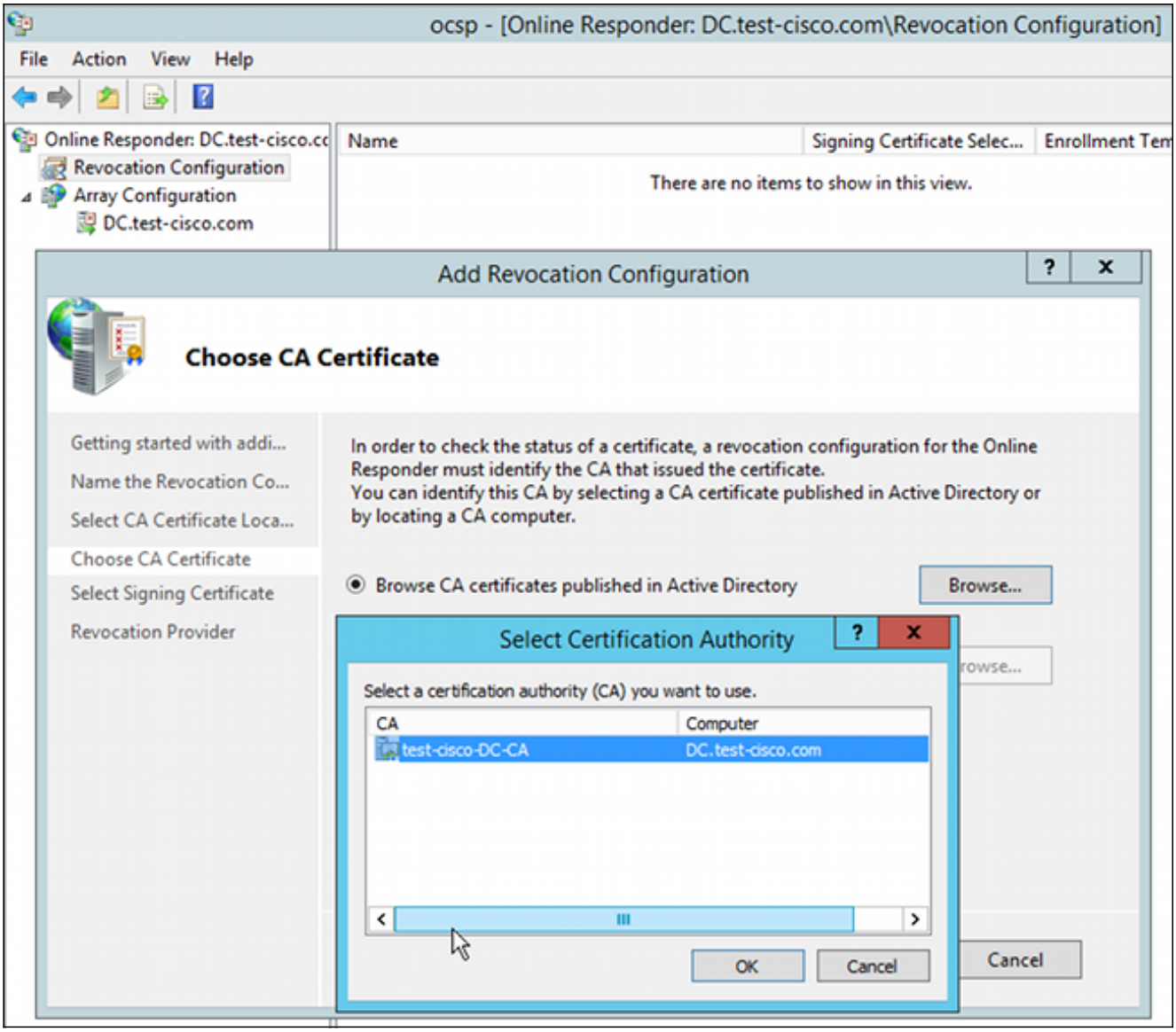


Certificado de servicio OCSP

Este procedimiento describe cómo utilizar Online Configuration Management para configurar OCSP:

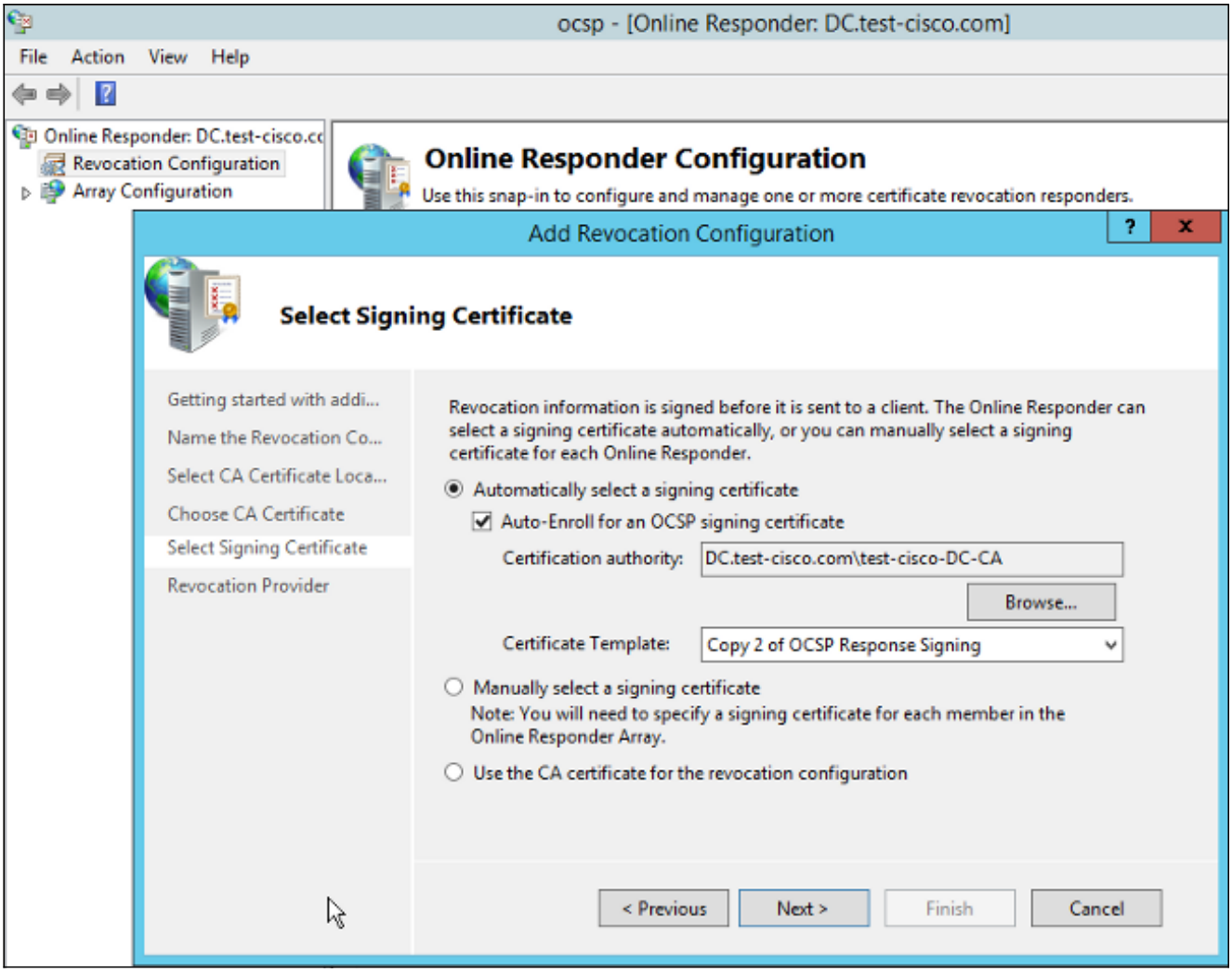
1. Vaya a **Administrador del servidor > Herramientas**.

2. Navegue hasta **Revocation Configuration > Add Revocation Configuration** para agregar una nueva configuración:

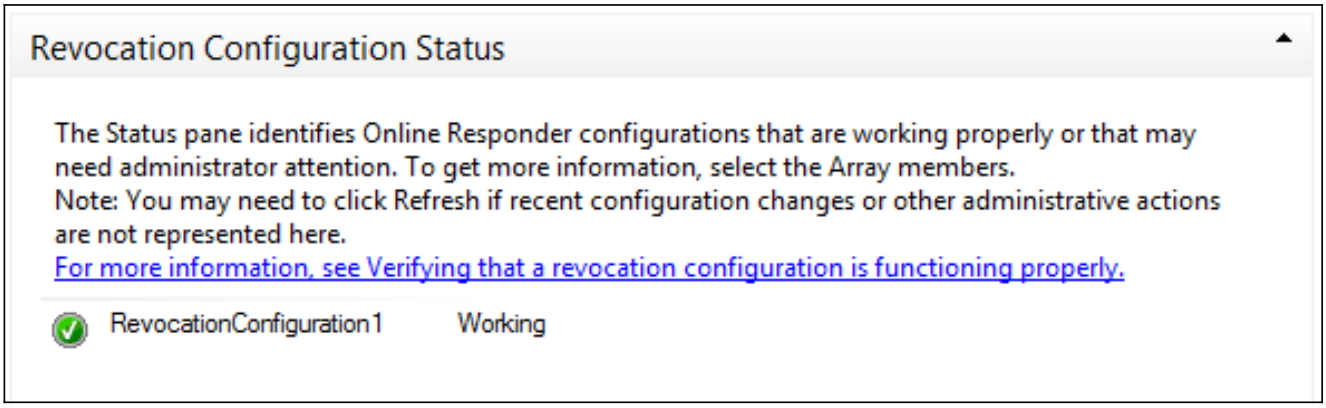


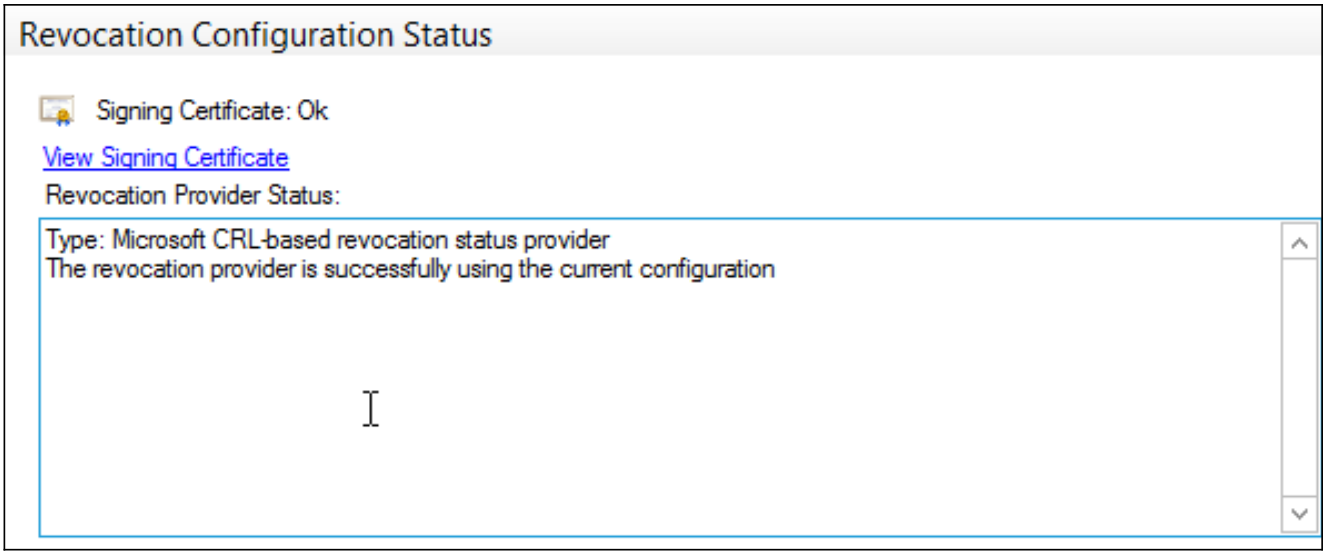
OCSP puede utilizar la misma CA empresarial. Se genera el certificado para el servicio OCSP.

3. Utilice la entidad emisora de certificados de empresa seleccionada y elija la plantilla creada anteriormente. El certificado se inscribe automáticamente:

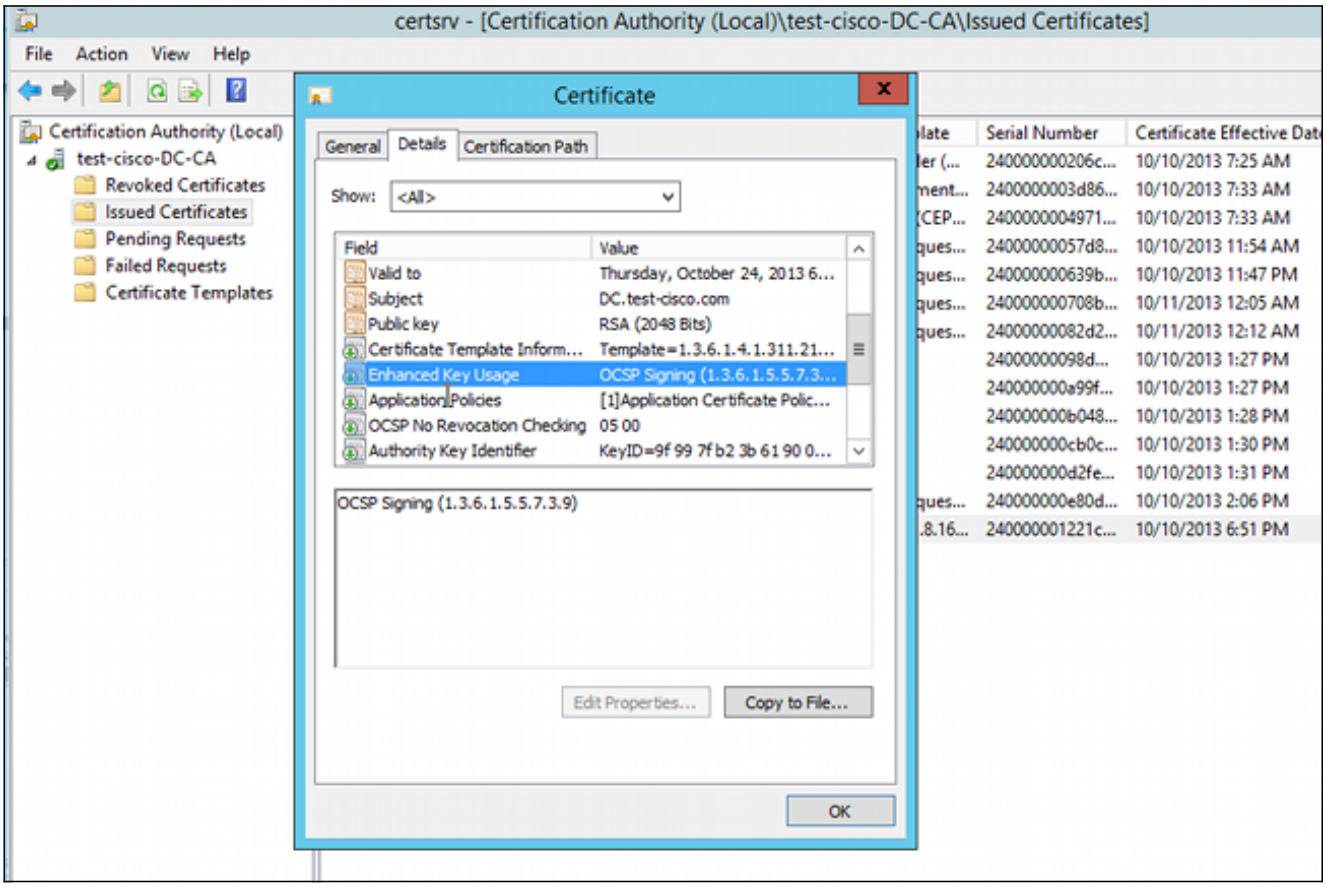


4. Confirme que el certificado está inscrito y que su estado es Working/OK:





5. Navegue hasta **CA > Certificados emitidos** para verificar los detalles del certificado:



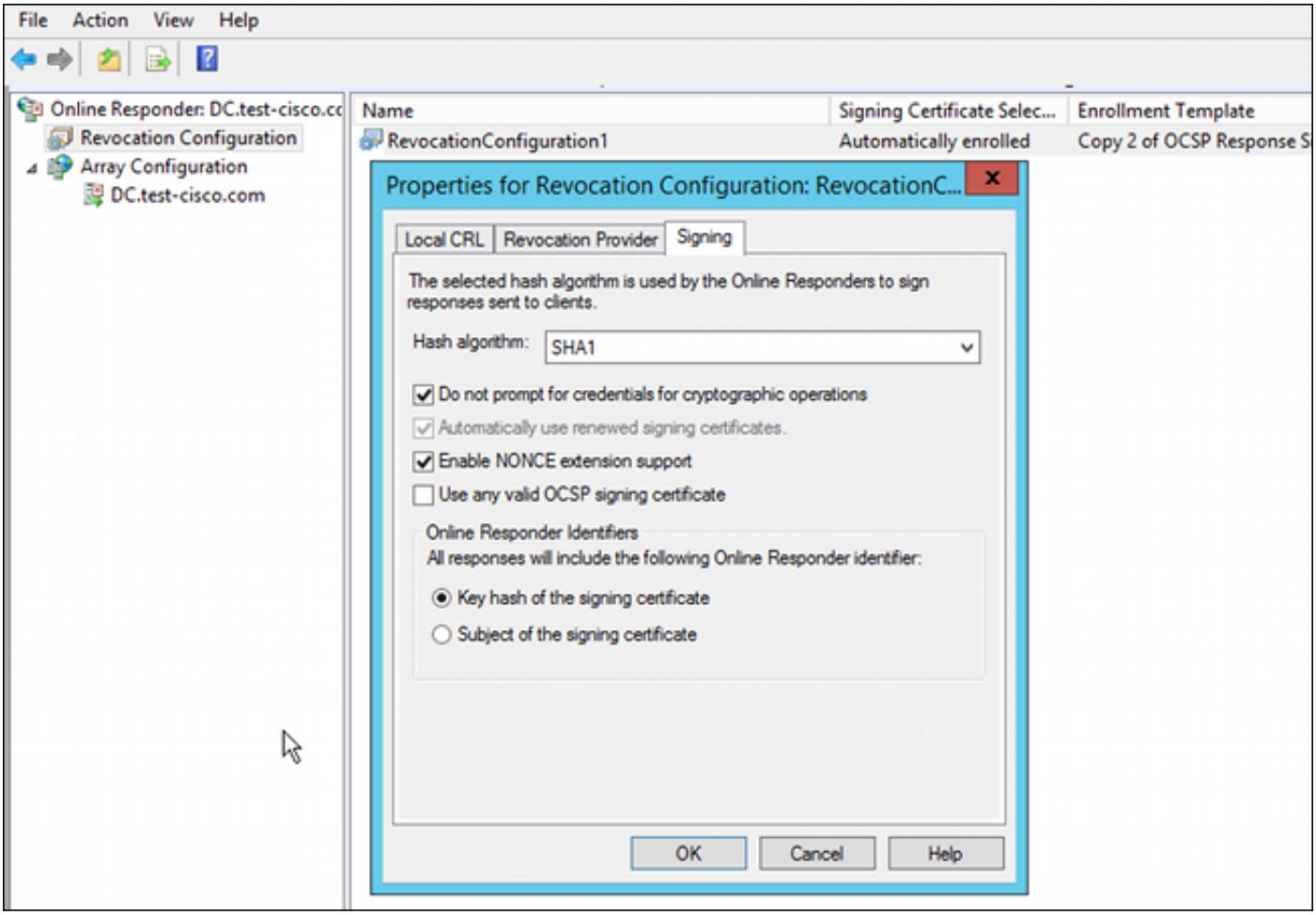
Nonces del servicio OCSP

La implementación de Microsoft de OCSP cumple con RFC 5019 El perfil del protocolo ligero de estado de certificados en línea (OCSP) para entornos de gran volumen , que es una versión simplificada del protocolo de estado de certificados en línea de la infraestructura de clave pública de Internet RFC 2560 X.509 - OCSP .

ASA utiliza RFC 2560 para OCSP. Una de las diferencias entre los dos RFC es que RFC 5019 no acepta solicitudes firmadas enviadas por ASA.

Es posible forzar al servicio OCSP de Microsoft a aceptar esas solicitudes firmadas y responder

con la respuesta firmada correcta. Navegue hasta **Revocation Configuration > RevocationConfiguration1 > Edit Properties**, y seleccione la opción para **Habilitar el soporte de extensión NONCE**.



El servicio OCSP ya está listo para utilizarse.

Aunque Cisco no recomienda esto, los nonces se pueden inhabilitar en el ASA:

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

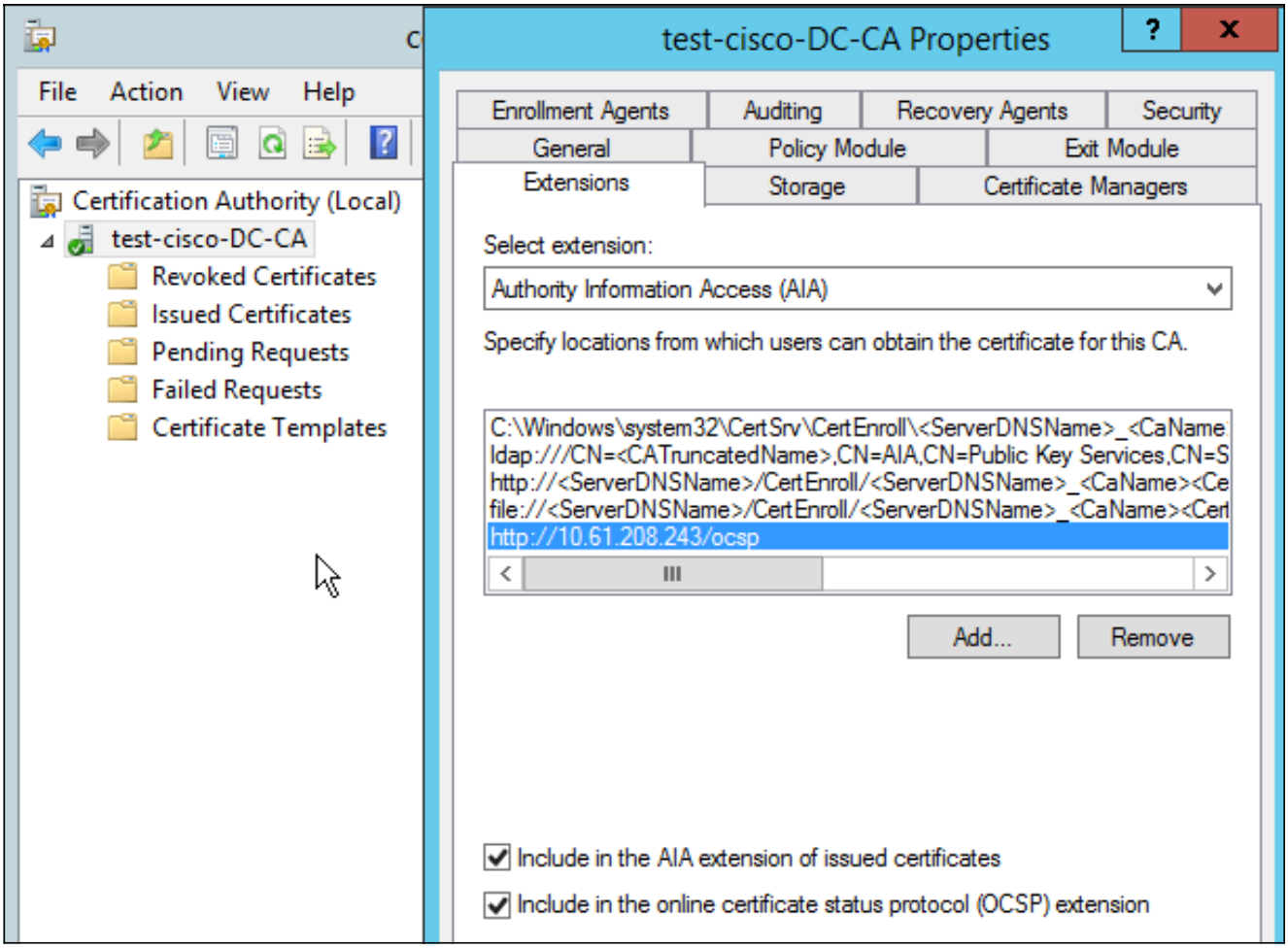
Configuración de CA para extensiones de OCSP

Ahora debe volver a configurar la CA para incluir la extensión de servidor OCSP en todos los certificados emitidos. ASA utiliza la URL de esa extensión para conectarse al servidor OCSP cuando se valida un certificado.

1. Abra el cuadro de diálogo Propiedades del servidor de la CA.

2. Haga clic en la pestaña **Extensions**. Se necesita la extensión Authority Information Access (AIA) que apunta al servicio OCSP; en este ejemplo, es http://10.61.208.243/ocsp. Habilite estas dos opciones para la extensión AIA:

   Incluir en el AIA la extensión de los certificados expedidosIncluir en la extensión del protocolo de estado de certificados en línea (OCSP)



Esto garantiza que todos los certificados emitidos tengan una extensión correcta que apunte al servicio OCSP.

OpenSSL

Nota: Consulte la Guía de configuración de Cisco ASA serie 5500 con CLI, 8.4 y 8.6: Configuración de un servidor externo para la autorización de usuario de dispositivos de seguridad para obtener detalles sobre la configuración de ASA a través de CLI.

Este ejemplo supone que el servidor OpenSSL ya está configurado. Esta sección describe solamente la configuración de OCSP y los cambios necesarios para la configuración de CA.

Este procedimiento describe cómo generar el certificado OCSP:

1. Estos parámetros son necesarios para el respondedor de OCSP:

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

2. Estos parámetros son necesarios para los certificados de usuario:

```
[ UserCerts ]
```

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

3. Los certificados deben ser generados y firmados por la CA.

4. Inicie el servidor OCSP:

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

5. Pruebe el certificado de ejemplo:

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

Hay más ejemplos disponibles en el sitio web de OpenSSL .

OpenSSL, como ASA, soporta nonces de OCSP; los nonces se pueden controlar con el uso de los switches -nonce y -no_nonce.

ASA con varias fuentes de OCSP

ASA puede anular la URL de OCSP. Incluso si el certificado de cliente contiene una URL de OCSP, la configuración del ASA lo sobrescribe:

```
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
```

La dirección del servidor OCSP se puede definir explícitamente. Este ejemplo de comando hace coincidir todos los certificados con administrator en subject name, utiliza un punto de confianza OPENSSL para validar la firma OCSP y utiliza la dirección URL de http://11.11.11.11/ocsp para enviar la solicitud:

```
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
```

El orden utilizado para encontrar la URL de OCSP es:

1. Un servidor OCSP configurado con el comando **match certificate**
2. Un servidor OCSP configurado con el comando **ocsp url**
3. El servidor OCSP en el campo AIA del certificado de cliente

ASA con OCSP firmado por una CA diferente

Una respuesta de OCSP puede estar firmada por una CA diferente. En tal caso, es necesario utilizar el comando **match certificate** para utilizar un punto de confianza diferente en el ASA para

la validación de certificados OCSP.

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

crypto ca certificate map MAP 10
 subject-name co administrator

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

En este ejemplo, ASA utiliza la reescritura de URL de OCSP para todos los certificados con un nombre de sujeto que contiene administrador. ASA se ve obligado a validar el certificado de respondedor OCSP frente a otro punto de confianza, OPENSSL. Los certificados de usuario se siguen validando en el punto de confianza WIN2012.

Dado que el certificado del respondedor de OCSP tiene la extensión 'OCSP sin comprobación de revocación', el certificado no se verifica, incluso cuando OCSP se ve obligado a realizar la validación con el punto de confianza de OPENSSL.

De forma predeterminada, se buscan todos los puntos de confianza cuando el ASA intenta verificar el certificado de usuario. La validación del certificado del respondedor de OCSP es diferente. ASA busca el certificado de usuario sólo en el punto de confianza que ya se ha encontrado (WIN2012 en este ejemplo).

Por lo tanto, es necesario utilizar el comando **match certificate** para forzar al ASA a utilizar un punto de confianza diferente para la validación de certificados OCSP (OPENSSL en este ejemplo).

Los certificados de usuario se validan con respecto al primer punto de confianza coincidente (WIN2012 en este ejemplo), que luego determina el punto de confianza predeterminado para la validación del respondedor de OCSP.

Si no se proporciona ningún punto de confianza específico en el comando **match certificate**, el certificado OCSP se valida con el mismo punto de confianza que los certificados de usuario (WIN2012 en este ejemplo).:

```
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
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

> **Nota**: la herramienta Output Interpreter Tool (sólo clientes registrados) admite ciertos comandos **show**. Utilice la herramienta para ver una análisis de información de salida del comando show.

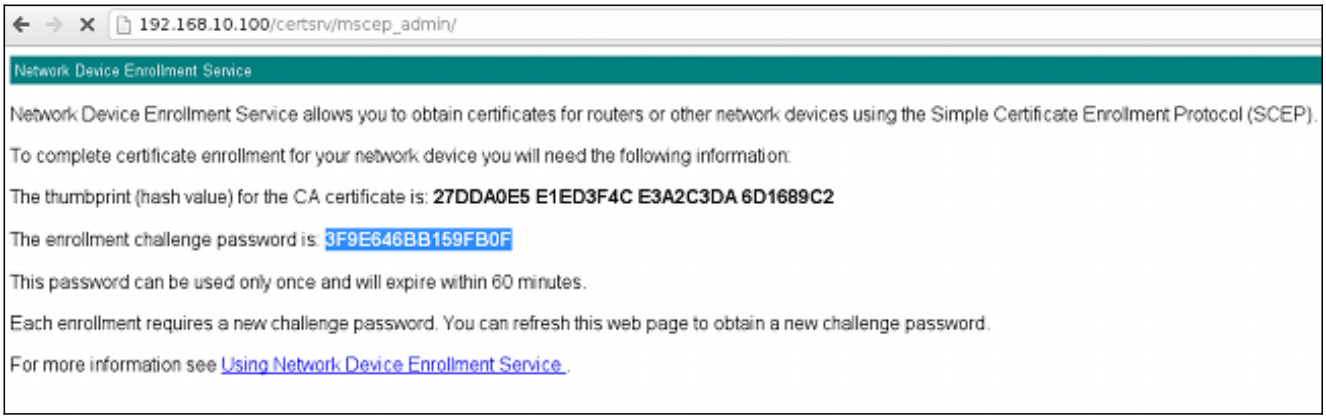
ASA - Obtener certificado a través de SCEP

Este procedimiento describe cómo obtener el certificado mediante el uso de SCEP:

1. Este es el proceso de autenticación de punto de confianza para obtener el certificado de la CA:

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

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

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

CRYPTO_PKI: http connection opened

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

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

Trustpoint CA certificate accepted.
```

2. Para solicitar el certificado, el ASA necesita tener una contraseña SCEP de un solo uso que se puede obtener de la consola de administración en http://IP/certsrv/mscep_admin:



3. Utilice esa contraseña para solicitar el certificado en el 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
```

Algunos resultados se han omitido para mayor claridad.

4. Verifique los certificados de CA y ASA:

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

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

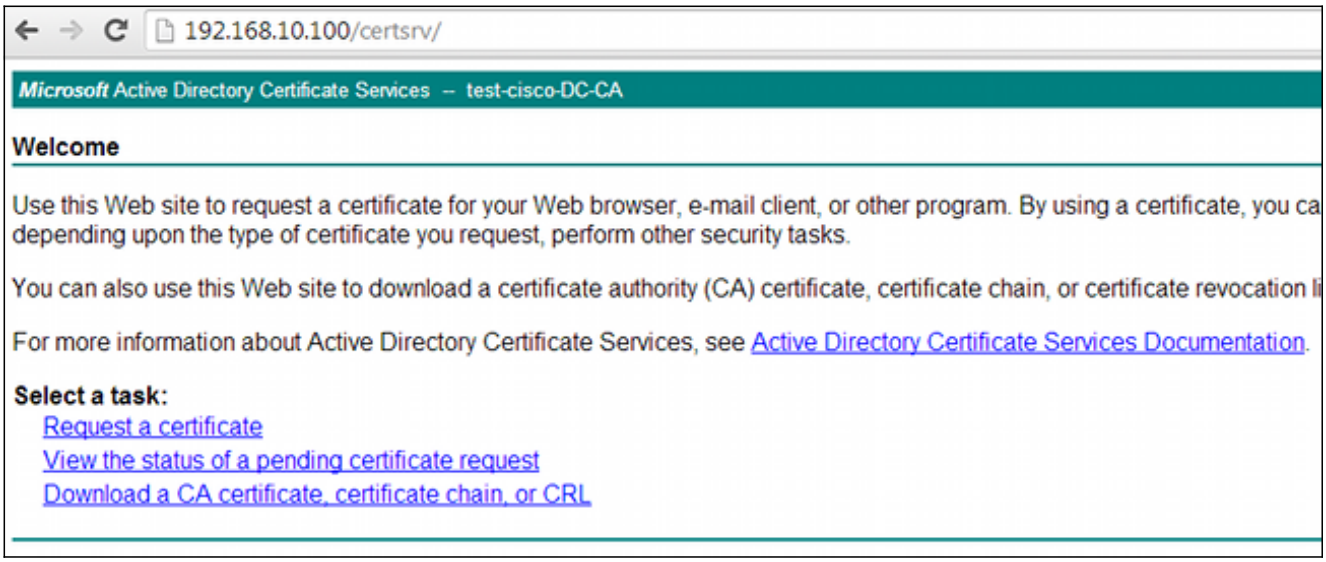
```
Subject Name:
  cn=test-cisco-DC-CA
  dc=test-cisco
  dc=com
Validity Date:
  start date: 07:23:03 CEST Oct 10 2013
  end   date: 07:33:03 CEST Oct 10 2018
Associated Trustpoints: WIN2012
```

ASA no muestra la mayoría de las extensiones de certificado. Aunque el certificado de ASA contiene la extensión 'OCSP URL in AIA', la CLI de ASA no la presenta. La identificación de error de Cisco CSCui44335, "ASA ENH Certificate x509 extensions played," solicita esta mejora.

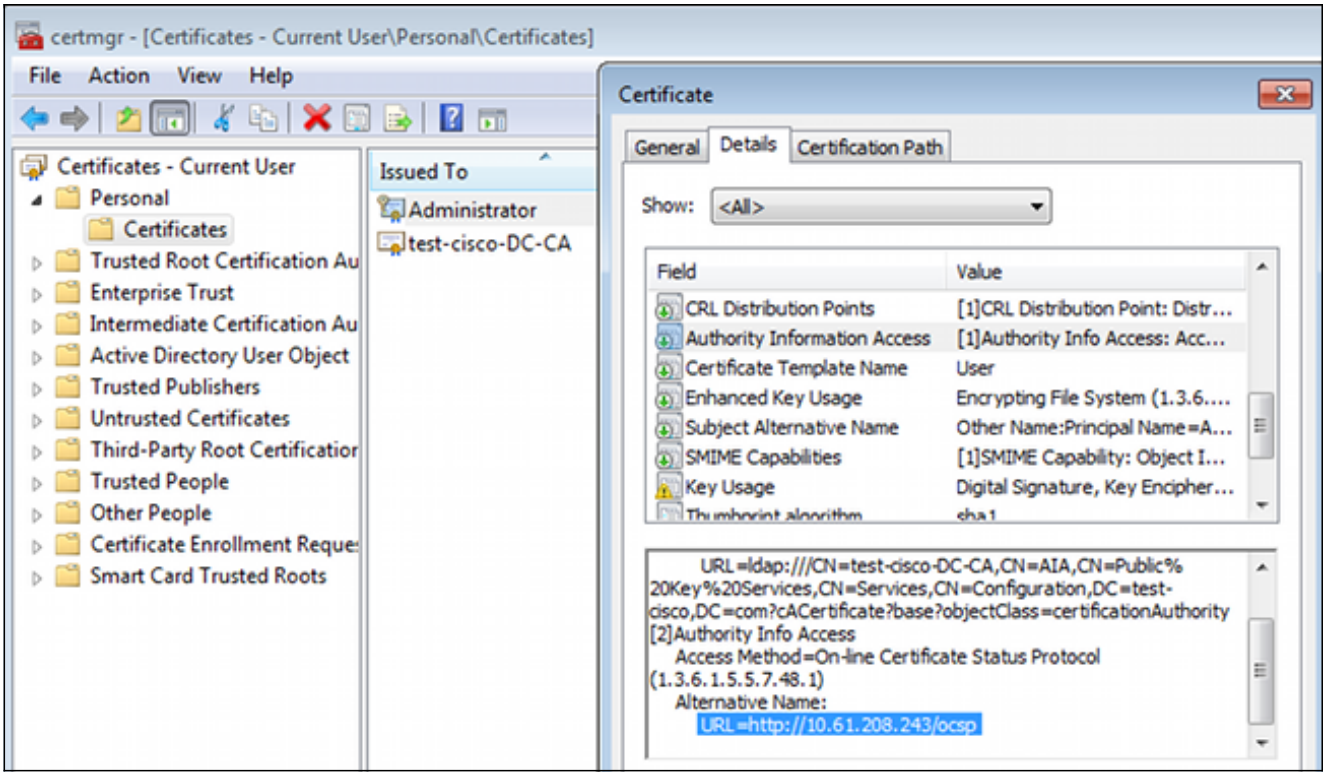
AnyConnect - Obtener certificado a través de la página web

Este procedimiento describe cómo obtener el certificado mediante el uso del explorador web en el cliente:

1. Se puede solicitar un certificado de usuario de AnyConnect a través de la página web. En el equipo cliente, utilice un navegador web para ir a la CA en http://*IP*/certsrv:



2. El certificado de usuario se puede guardar en el almacén del explorador web y, a continuación, exportarse al almacén de Microsoft, en el que AnyConnect realiza la búsqueda. Utilice certmgr.msc para verificar el certificado recibido:



AnyConnect también puede solicitar el certificado siempre que haya un perfil de AnyConnect correcto.

Acceso remoto VPN ASA con validación OCSP

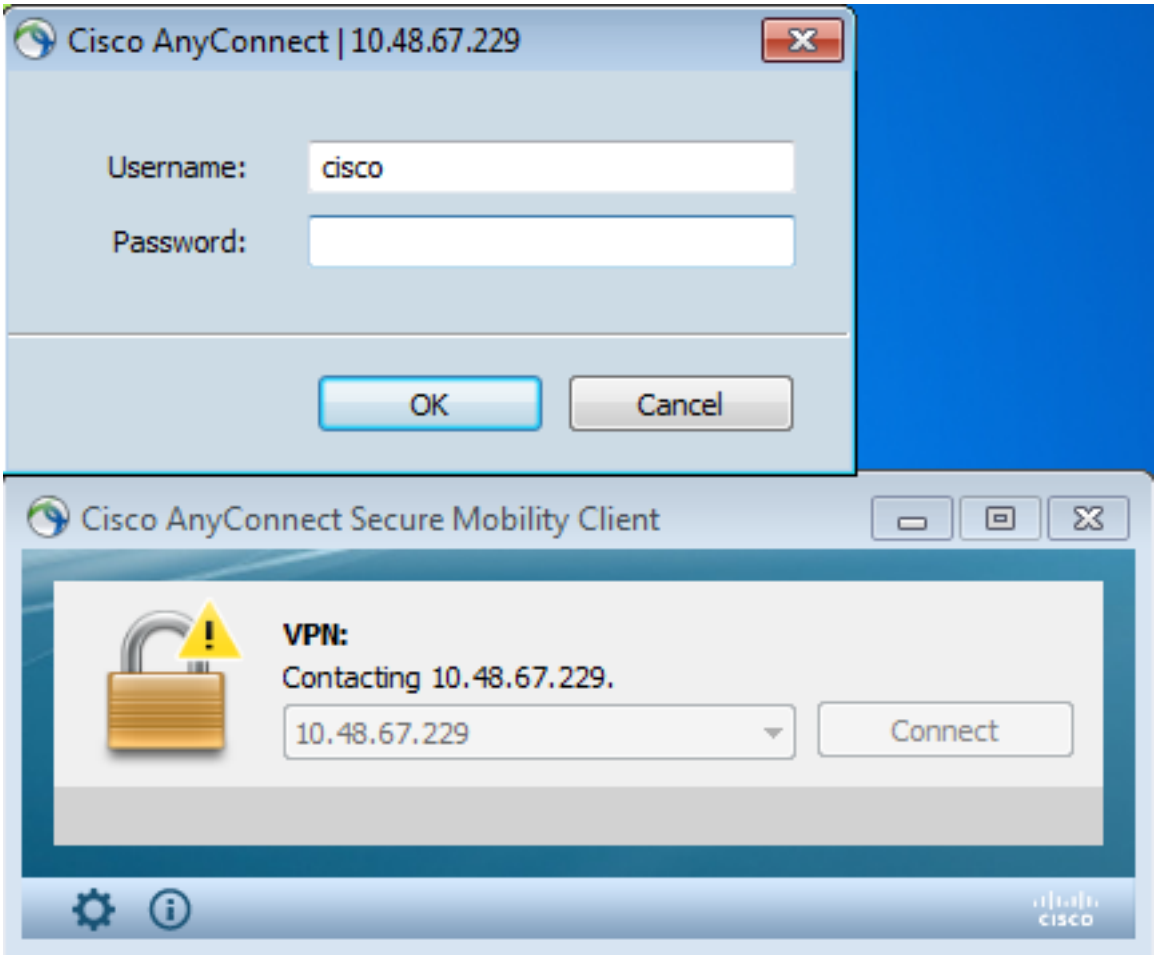
Este procedimiento describe cómo comprobar la validación de OCSP:

1. A medida que intenta conectarse, ASA informa que se está comprobando si el certificado tiene OCSP. Aquí, el certificado de firma de OCSP tiene una extensión sin verificación y no se ha verificado a través de 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.
```

Algunos resultados se han omitido para mayor claridad.

2. El usuario final proporciona las credenciales de usuario:



3. La sesión VPN ha finalizado correctamente:

```
%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. Se crea la sesión:

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

Session Type: AnyConnect Detailed
```

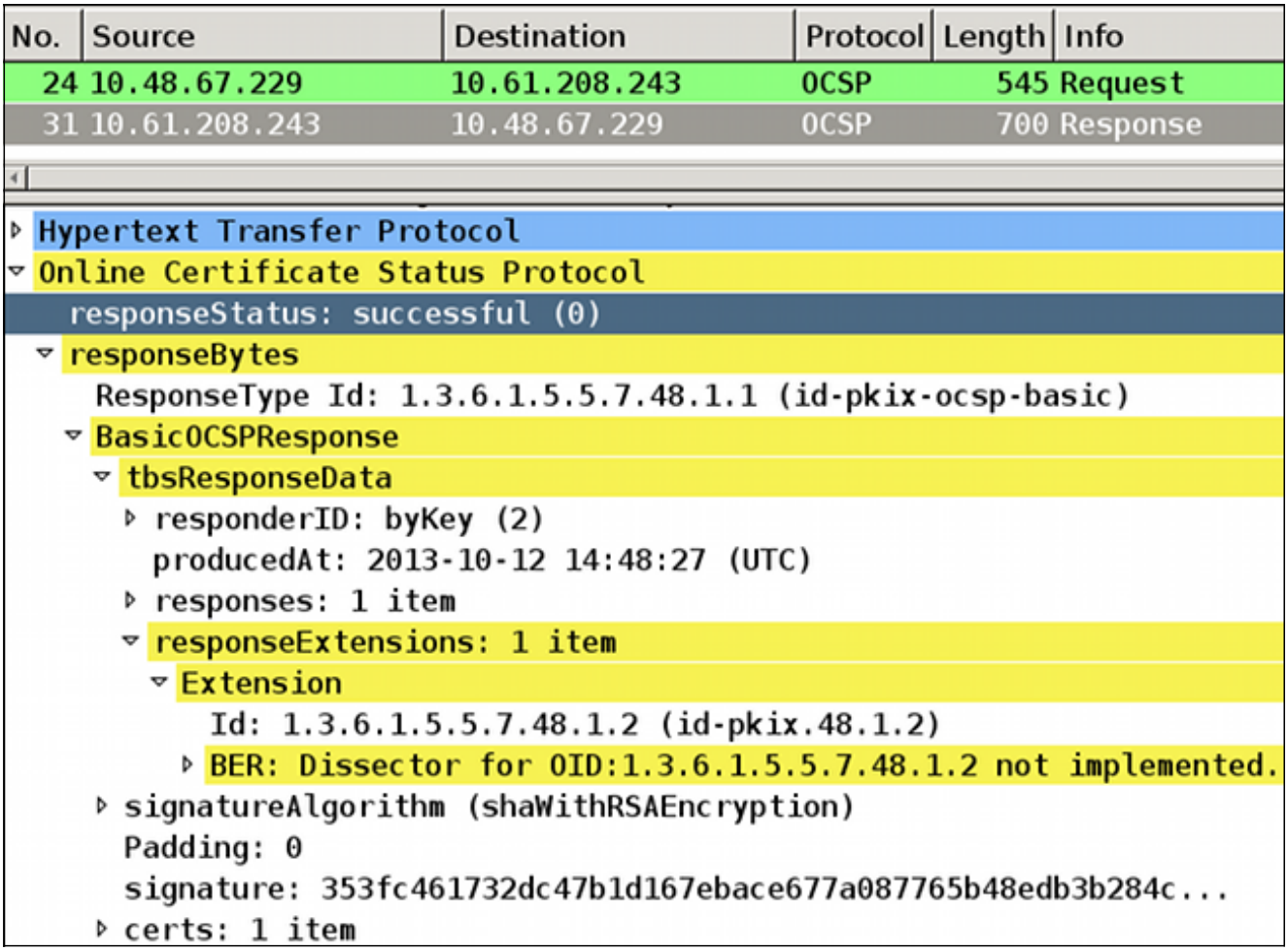
```
Username     : cisco                  Index        : 4
Assigned IP  : 192.168.11.100         Public IP    : 10.61.209.83
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4
DTLS-Tunnel: (1)AES128
Hashing      : 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. Puede utilizar depuraciones detalladas para la validación de OCSP:

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

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

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

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

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

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

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

6. En el nivel de captura de paquetes, esta es la solicitud OCSP y la respuesta OCSP correcta. La respuesta incluye la firma correcta - extensión nonce habilitada en Microsoft OCSP:



Acceso remoto VPN ASA con varias fuentes OCSP

Si se configura un certificado de coincidencia como se explica en ASA con varias fuentes de OCSP, tiene prioridad:

```
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
```

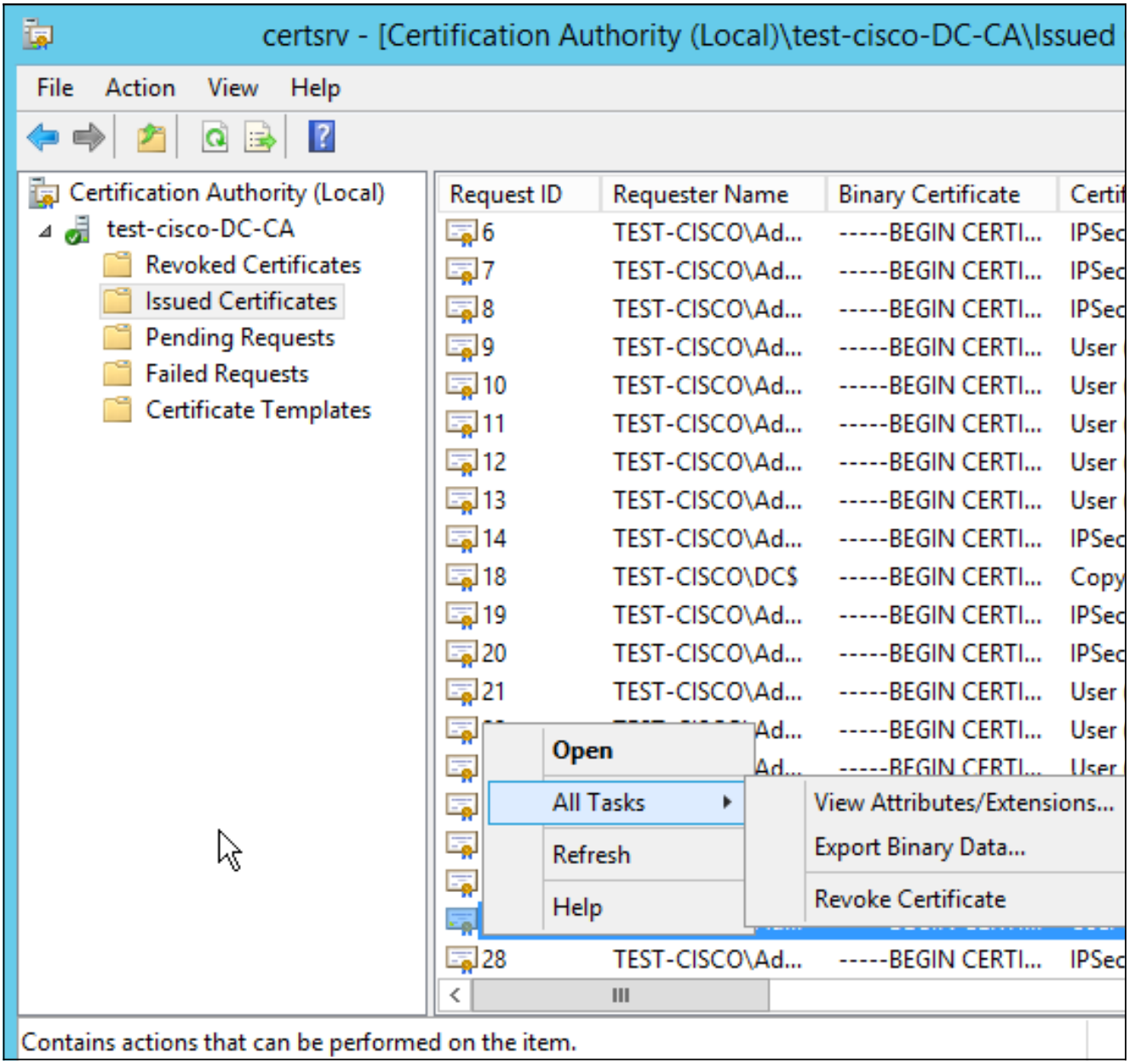
Cuando se utiliza una invalidación de URL de OCSP, los debugs son:

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

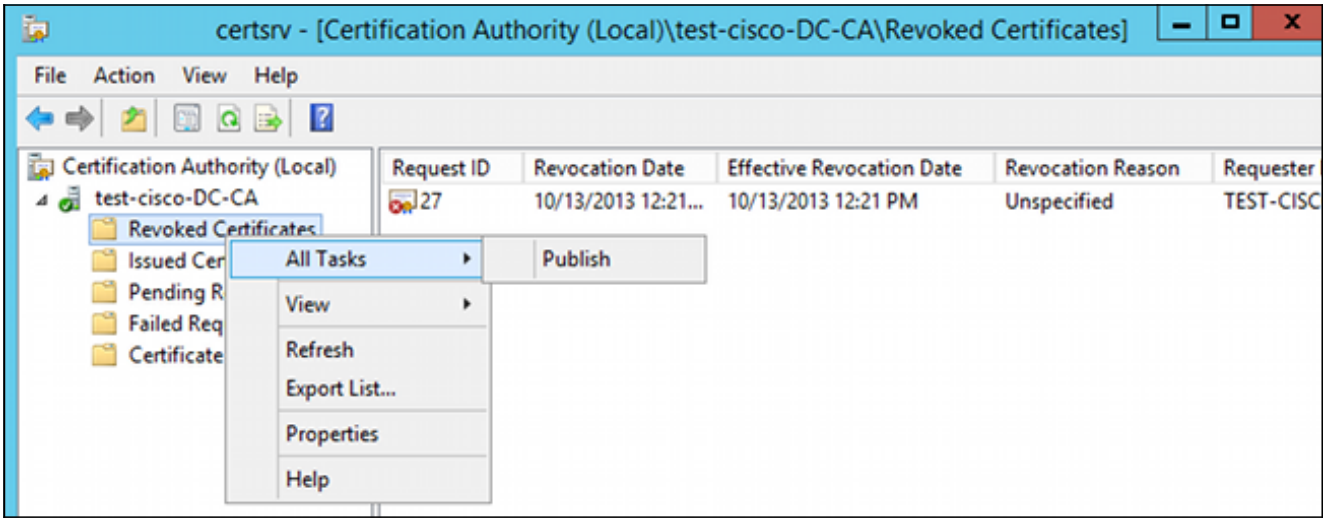
Acceso remoto a VPN ASA con OCSP y certificado revocado

Este procedimiento describe cómo revocar el certificado y confirmar el estado revocado:

1. Revocar el certificado de cliente:



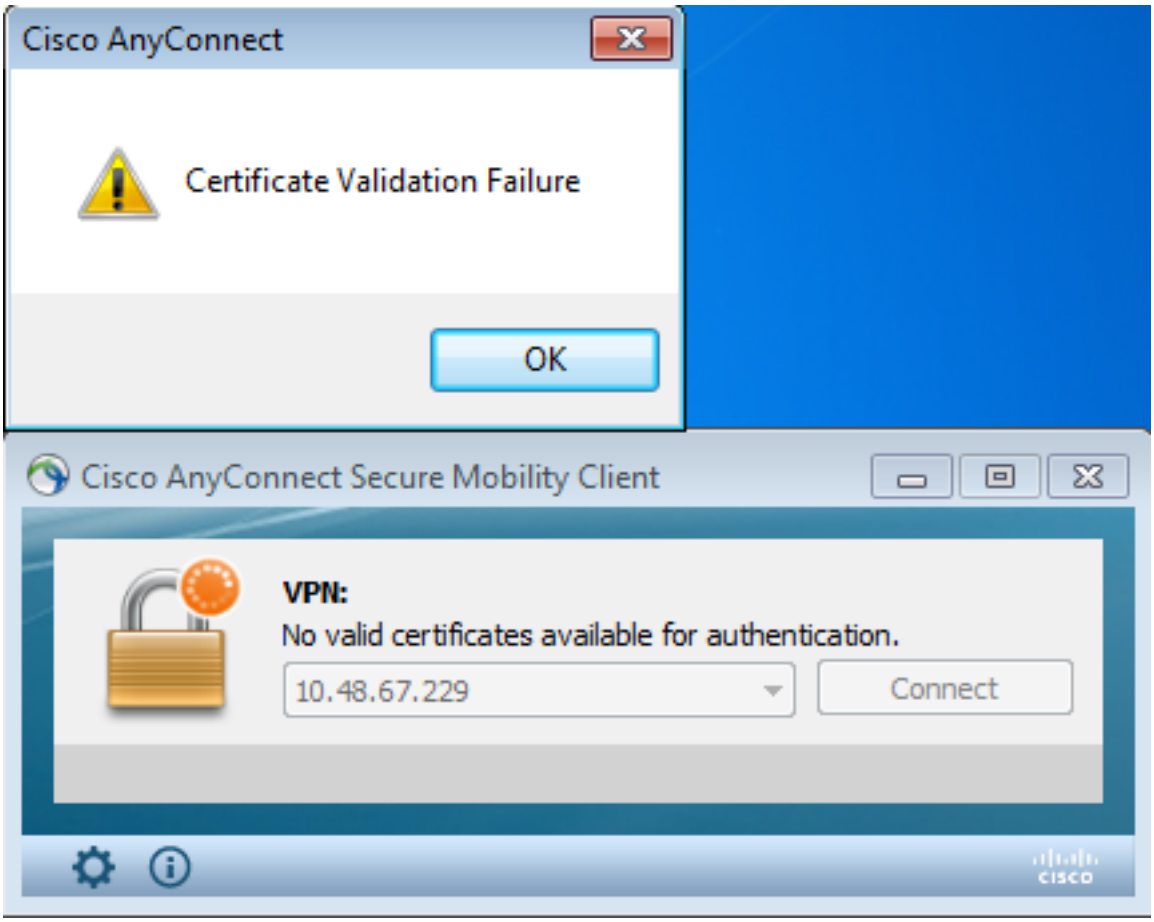
2. Publicar los resultados:



3. [Opcional] Los pasos 1 y 2 también se pueden realizar con la utilidad CLI certutil en Power Shell:

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

4. Cuando el cliente intenta conectarse, hay un error de validación de certificado:



5. Los registros de AnyConnect también indican el error de validación del certificado:

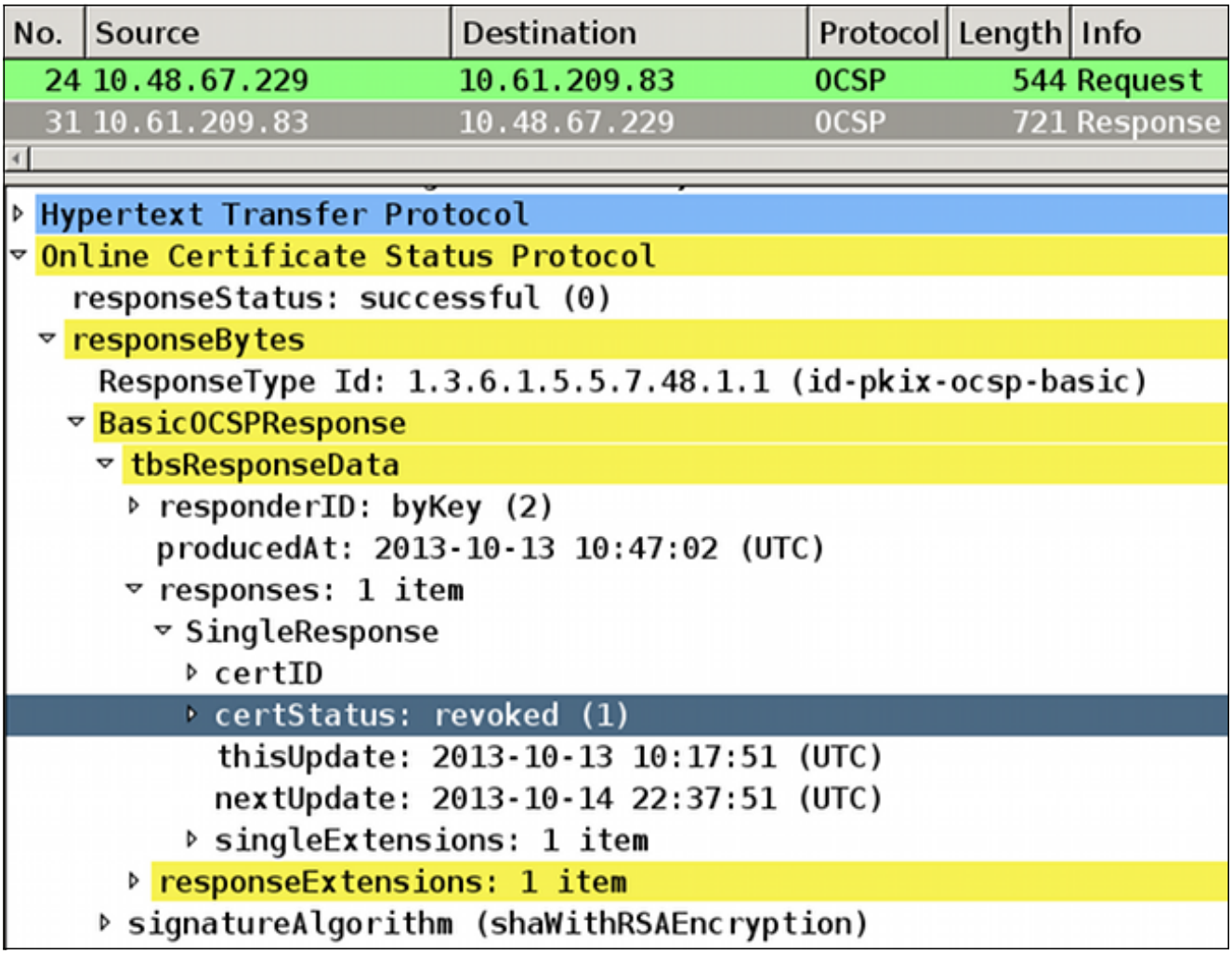
```
[2013-10-13 12:49:53] Contacting 10.48.67.229.
[2013-10-13 12:49:54] No valid certificates available for authentication.
[2013-10-13 12:49:55] Certificate Validation Failure
```

6. El ASA informa que el estado del certificado es revocado:

```
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. Las capturas de paquetes muestran una respuesta de OCSP exitosa con el estado de certificado de revocado:



Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de

configuración.

Servidor OCSP inactivo

ASA informa cuando el servidor OCSP está inactivo:

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

Las capturas de paquetes también pueden ayudar con la resolución de problemas.

Hora no sincronizada

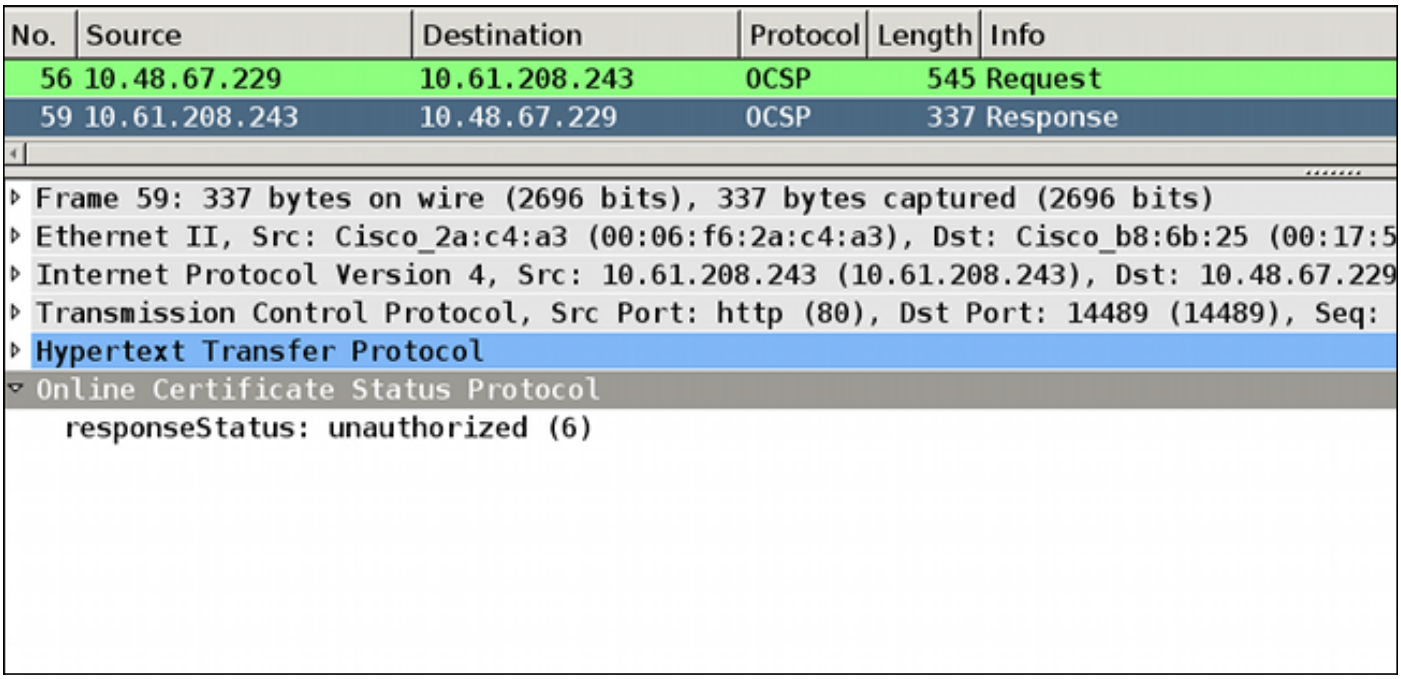
Si la hora actual en el servidor OCSP es anterior a la de ASA (se aceptan pequeñas diferencias), el servidor OCSP envía una respuesta no autorizada y ASA informa de ello:

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

Cuando ASA recibe una respuesta de OCSP de tiempos futuros, también falla.

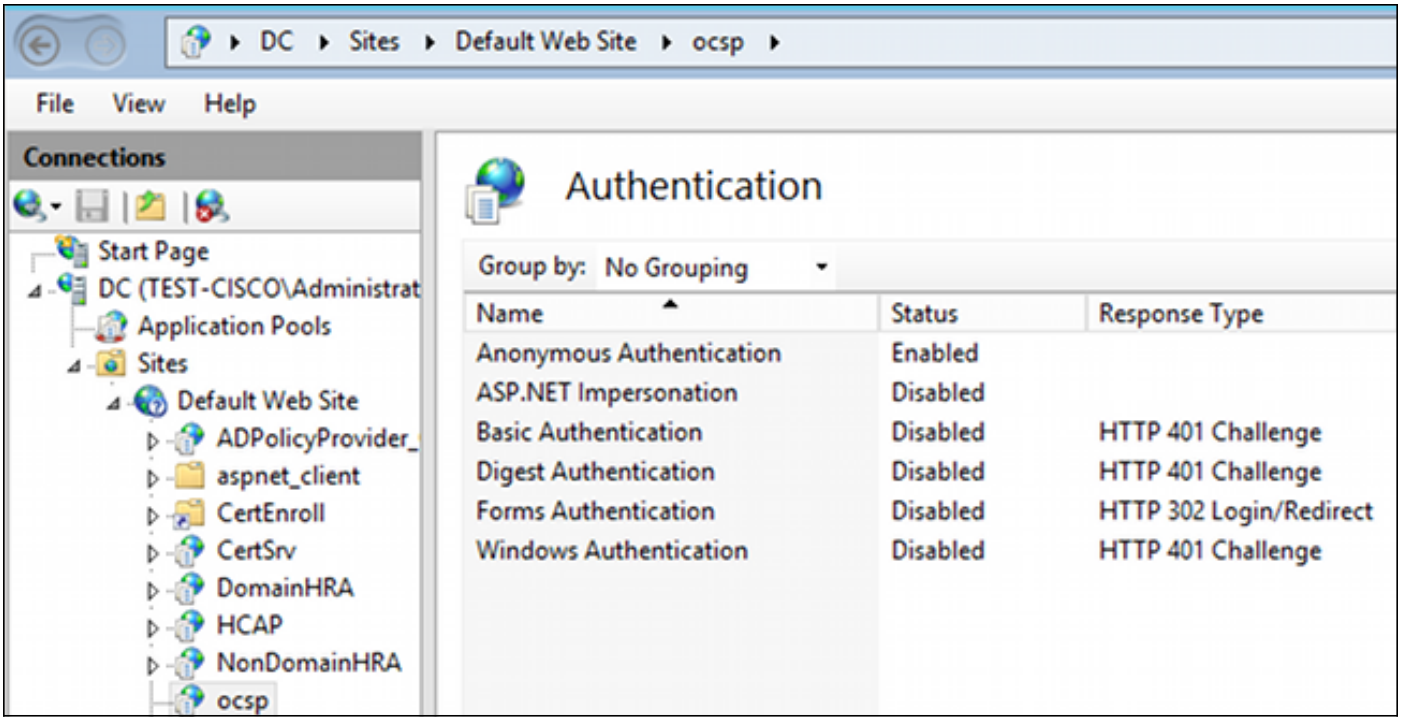
Nonces Firmados No Soportados

Si no se admiten nonces en el servidor (que es el valor predeterminado en Microsoft Windows 2012 R2), se devuelve una respuesta no autorizada:



Autenticación del servidor IIS7

Los problemas con una solicitud SCEP/OCSP suelen ser el resultado de una autenticación incorrecta en Internet Information Services 7 (IIS7). Asegúrese de que el acceso anónimo esté configurado:



Información Relacionada

- Microsoft TechNet: Guía de instalación, configuración y solución de problemas de Online Responder
- Microsoft TechNet: configuración de una CA para admitir responsables de OCSP
- Referencia de Comandos de la Serie ASA de Cisco
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).