

ASA Remote Access VPN com verificação OCSP no Microsoft Windows 2012 e OpenSSL

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Acesso remoto ASA com OCSP](#)

[CA do Microsoft Windows 2012](#)

[Instalação de serviços](#)

[Configuração de CA para Modelo OCSP](#)

[Certificado de serviço OCSP](#)

[Datas de Serviço OCSP](#)

[Configuração de CA para extensões OCSP](#)

[OpenSSL](#)

[ASA com várias origens OCSP](#)

[ASA com OCSP Assinado por Outra CA](#)

[Verificar](#)

[ASA - Obter Certificado via SCEP](#)

[AnyConnect - Obter certificado através da página da Web](#)

[Acesso remoto ASA VPN com validação OCSP](#)

[Acesso remoto ASA VPN com várias fontes OCSP](#)

[Acesso remoto ASA VPN com OCSP e certificado revogado](#)

[Troubleshoot](#)

[Servidor OCSP inoperante](#)

[Hora Não Sincronizada](#)

[Não Há Suporte Para Datas Assinadas](#)

[Autenticação do Servidor IIS7](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve como usar a validação do Protocolo de Status de Certificados Online (OCSP - Online Certificate Status Protocol) em um Cisco Adaptive Security Appliance (ASA) para certificados apresentados por usuários VPN. São apresentadas configurações de exemplo para dois servidores OCSP (Microsoft Windows Certificate Authority [CA] e OpenSSL). A seção

Verificar descreve os fluxos detalhados no nível do pacote, e a seção Solução de problemas concentra-se em erros e problemas típicos.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração da interface de linha de comando (CLI) do Cisco Adaptive Security Appliance e configuração da VPN Secure Socket Layer (SSL)
- Certificados X.509
- Servidor Microsoft Windows
- Linux/OpenSSL

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Software Cisco Adaptive Security Appliance versão 8.4 e posterior
- Microsoft Windows 7 com Cisco AnyConnect Secure Mobility Client, versão 3.1
- Microsoft Server 2012 R2
- Linux com OpenSSL 1.0.0j ou posterior

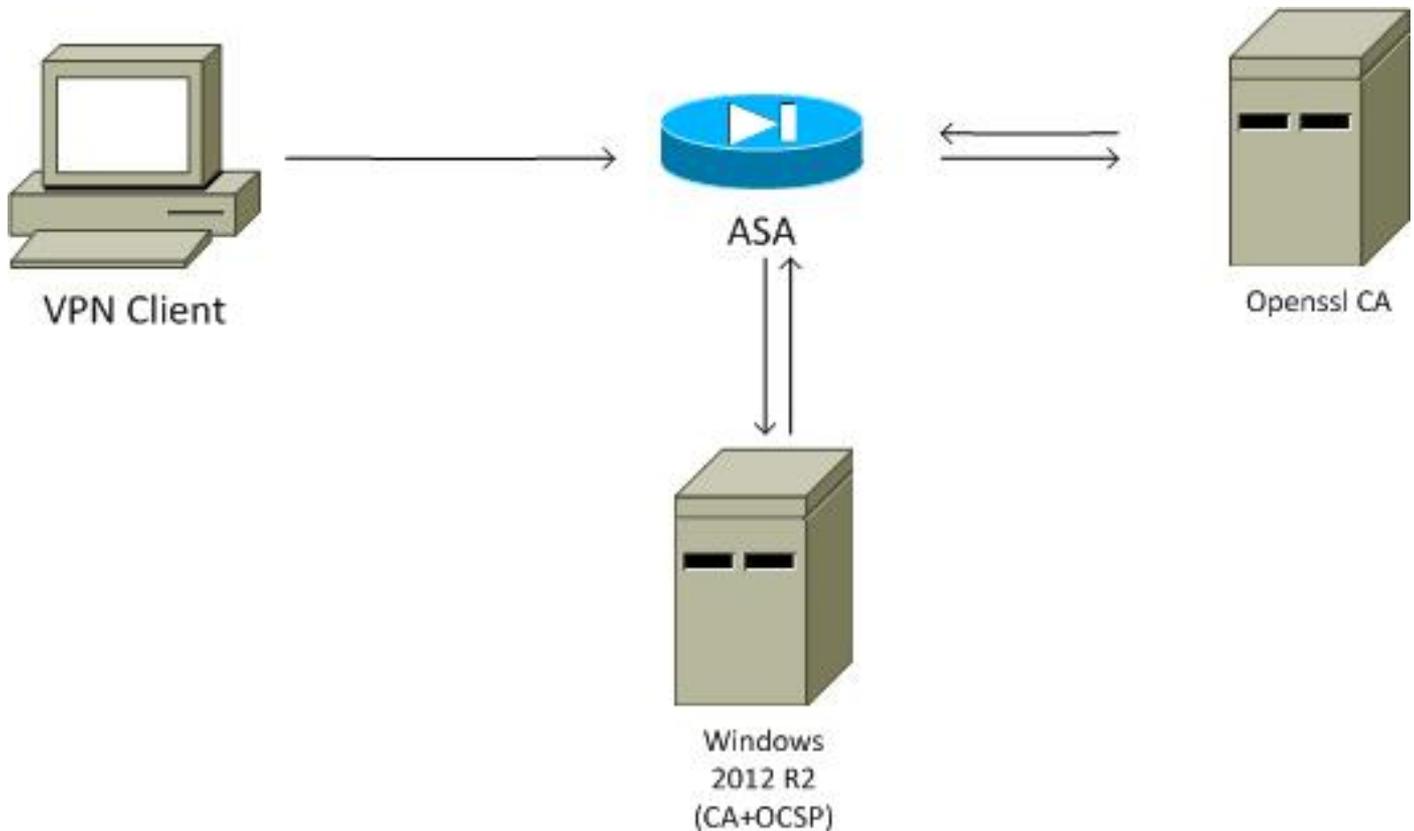
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

O cliente usa VPN de acesso remoto. Esse acesso pode ser o Cisco VPN Client (IPSec), o Cisco AnyConnect Secure Mobility (SSL/Internet Key Exchange versão 2 [IKEv2]) ou WebVPN (portal). Para fazer login, o cliente fornece o certificado correto, bem como o nome de usuário/senha que foram configurados localmente no ASA. O certificado do cliente é validado através do servidor OCSP.



Acesso remoto ASA com OCSP

O ASA está configurado para acesso SSL. O cliente está usando o AnyConnect para fazer login. O ASA usa o Protocolo de Registro de Certificado Simples (SCEP) para solicitar o certificado:

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

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

Um mapa de certificado é criado para identificar todos os usuários cujo nome da entidade contenha a palavra administrador (não diferencia maiúsculas de minúsculas). Esses usuários estão vinculados a um grupo de túneis chamado 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
```

A configuração da VPN requer autorização bem-sucedida (isto é, um certificado validado). Também requer as credenciais corretas para o nome de usuário definido localmente (autenticação aaa):

```
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
```

CA do Microsoft Windows 2012

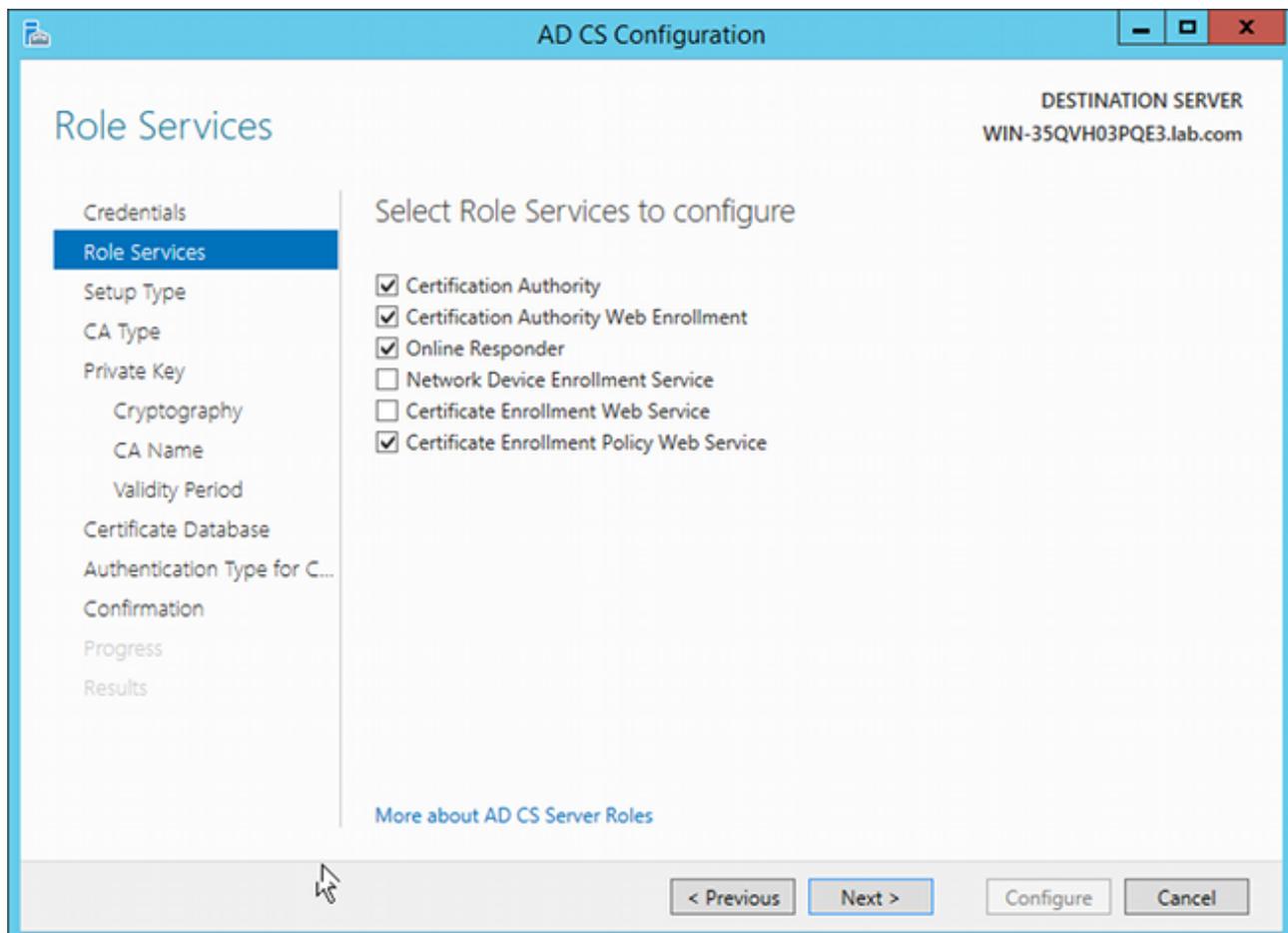
Observação: consulte o [Guia de Configuração do Cisco ASA 5500 Series usando a CLI, 8.4 e 8.6: Configuração de um Servidor Externo para Autorização do Usuário do Security Appliance](#) para obter detalhes sobre a configuração do ASA através da CLI.

Instalação de serviços

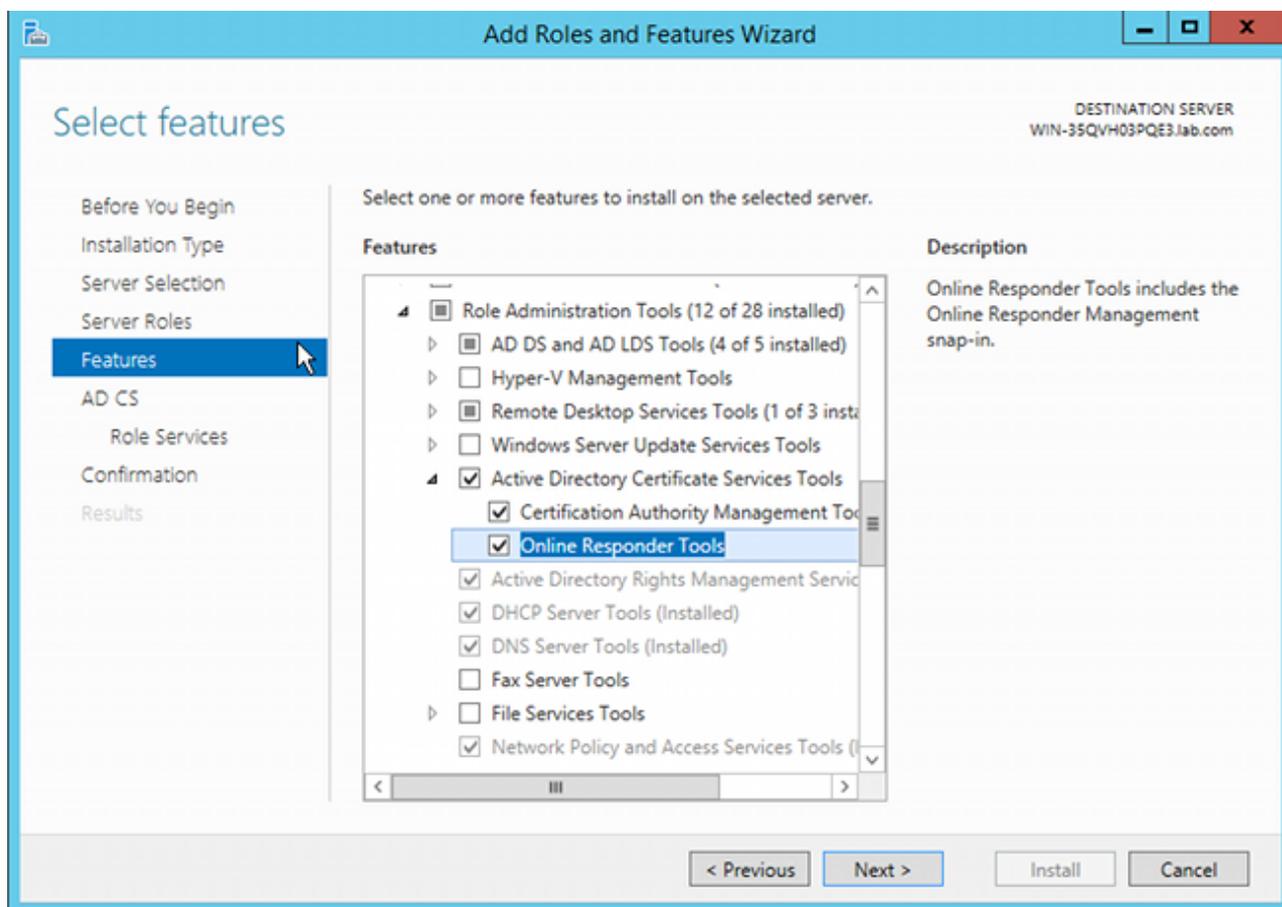
Este procedimento descreve como configurar serviços de função para o servidor Microsoft:

1. Navegue até **Gerenciador de servidores > Gerenciar > Adicionar funções e recursos**. O servidor Microsoft precisa destes serviços de função:

Autoridade de certificaçãoInscrição na Web de Autoridade de Certificação, usada pelo clienteOnline Responder, necessário para OCSPNetwork Device Enrollment Service, que contém o aplicativo SCEP usado pelo ASA O serviço da Web com políticas pode ser adicionado, se necessário.



- 2.
- 3.
4. Ao adicionar recursos, certifique-se de incluir as Ferramentas de Respondente Online, pois elas incluem um snap-in OCSP que será usado posteriormente:



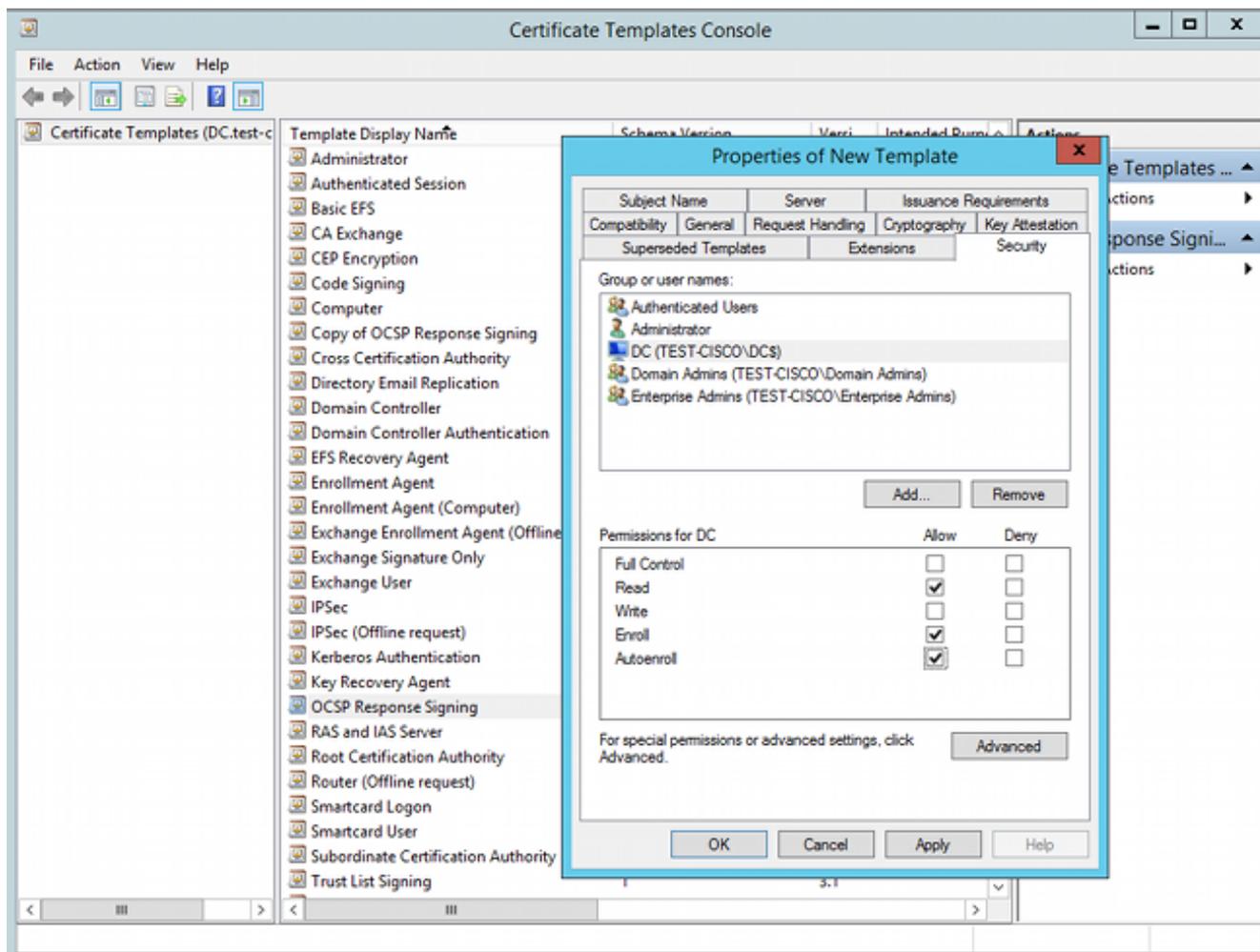
Configuração de CA para Modelo OCSP

O serviço OCSP usa um certificado para assinar a resposta OCSP. Um certificado especial no servidor Microsoft deve ser gerado e deve incluir:

- Uso estendido de chave = assinatura OCSP
- OCSP sem verificação de revogação

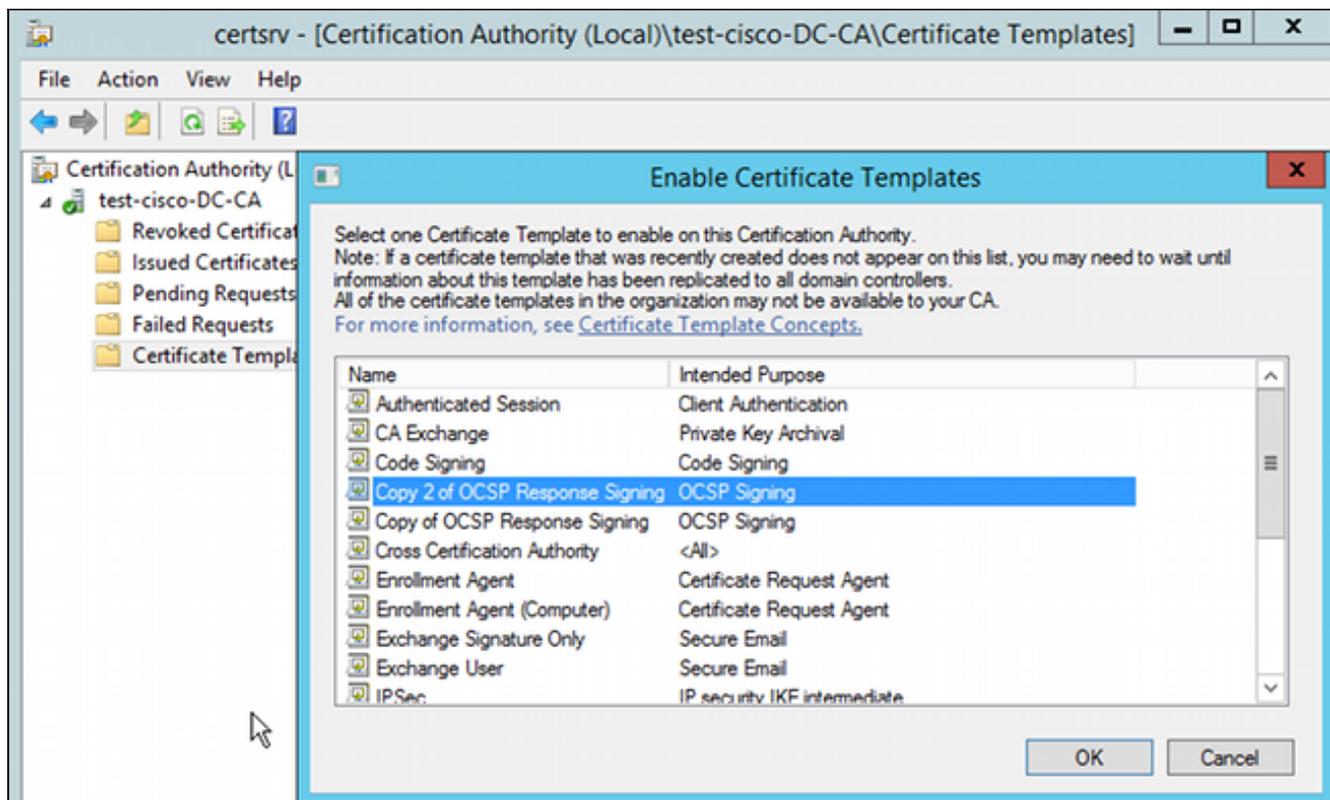
Este certificado é necessário para evitar loops de validação OCSP. O ASA não usa o serviço OCSP para tentar verificar o certificado apresentado pelo serviço OCSP.

1. Adicione um modelo para o certificado na autoridade de certificação. Navegue para **CA > Modelo de certificado > Gerenciar**, selecione **Assinatura de resposta OCSP** e duplique o modelo. Exiba as propriedades do modelo recém-criado e clique na guia **Segurança**. As permissões descrevem qual entidade tem permissão para solicitar um certificado que use esse modelo, portanto, são necessárias permissões corretas. Neste exemplo, a entidade é o serviço OCSP que está sendo executado no mesmo host (TEST-CISCO\DC) e o serviço OCSP precisa de privilégios de Inscrição Automática:



Todas as outras configurações do modelo podem ser definidas como padrão.

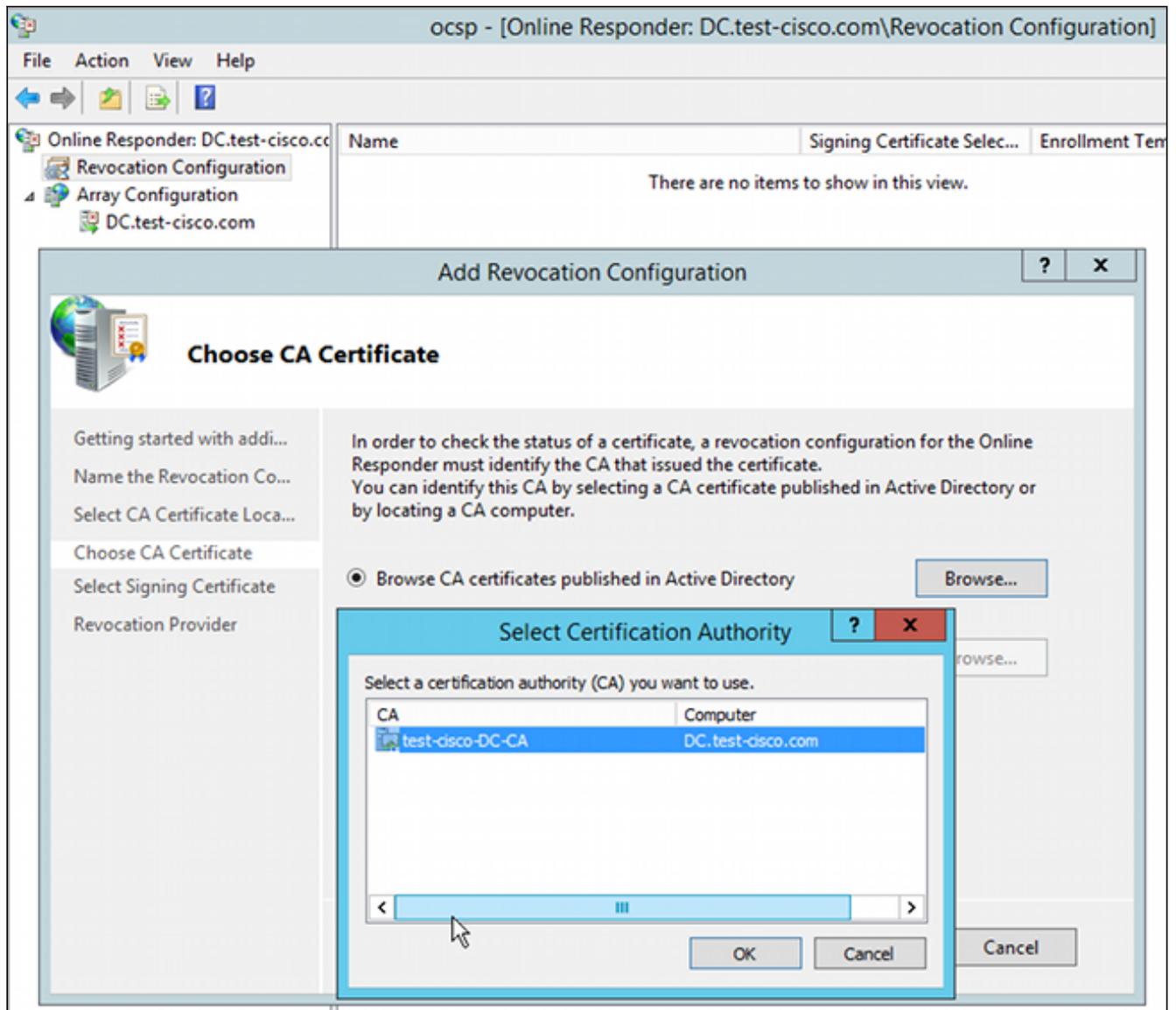
2. Ative o modelo. Navegue até **CA > Modelo de certificado > Novo > Modelo de certificado a ser emitido** e selecione o modelo duplicado:



Certificado de serviço OCSP

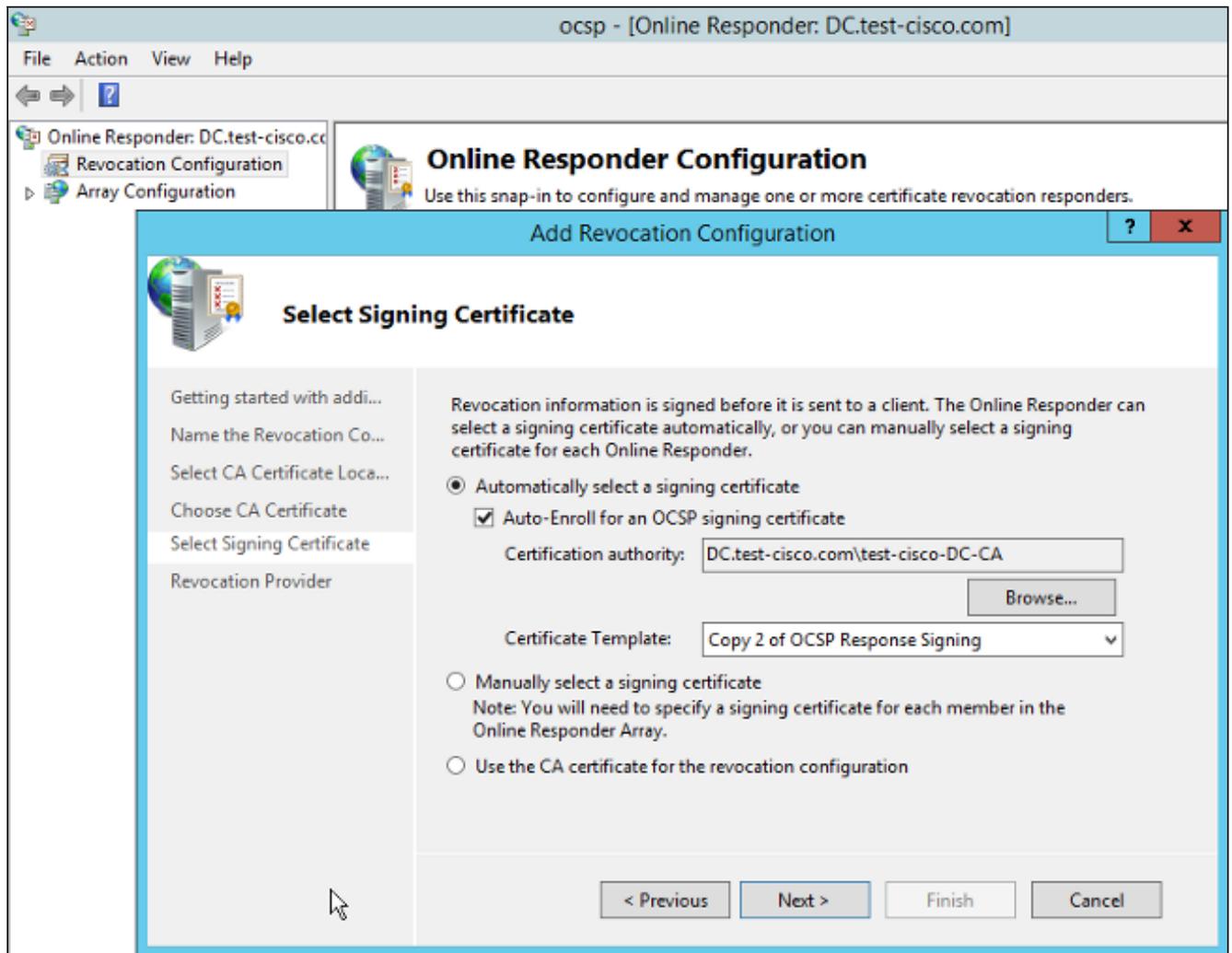
Este procedimento descreve como usar o Gerenciamento de Configuração On-line para configurar o OCSP:

1. Navegue até **Server Manager > Tools**.
2. Navegue para **Revocation Configuration > Add Revocation Configuration** para adicionar uma nova configuração:

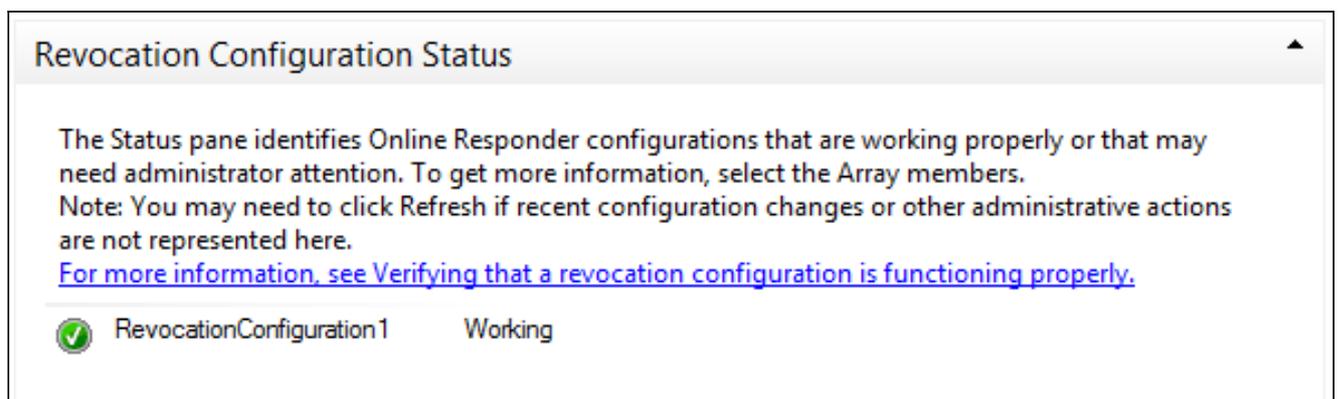


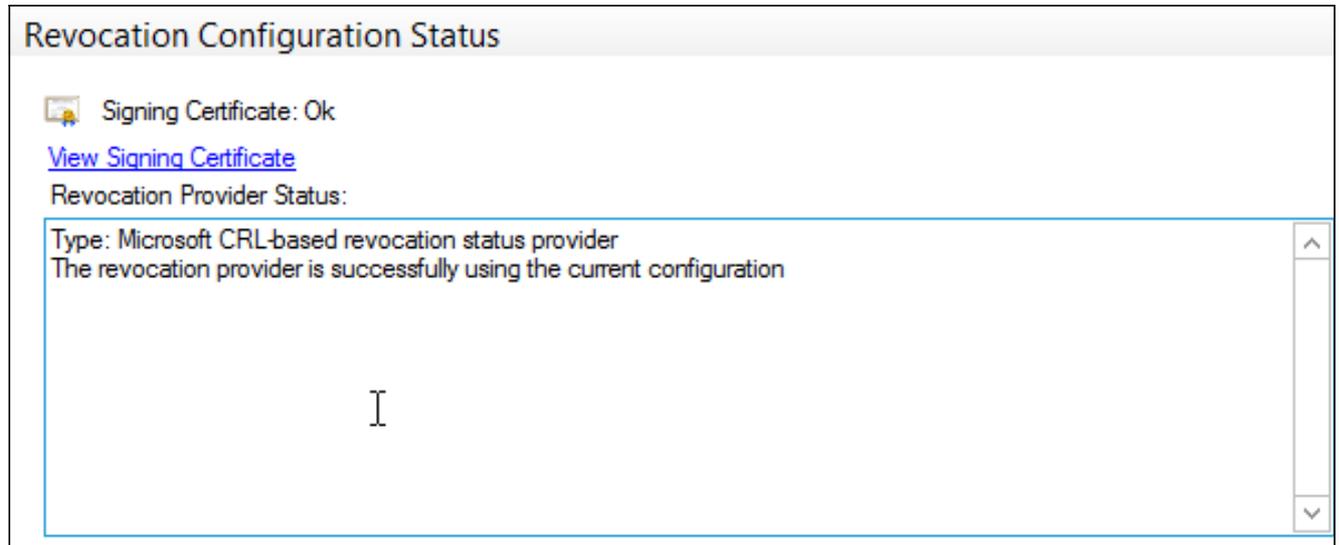
O OCSP pode usar a mesma CA Corporativa. O certificado para o serviço OCSP é gerado.

3. Use a Autoridade de Certificação Corporativa selecionada e escolha o modelo criado anteriormente. O certificado é registrado automaticamente:

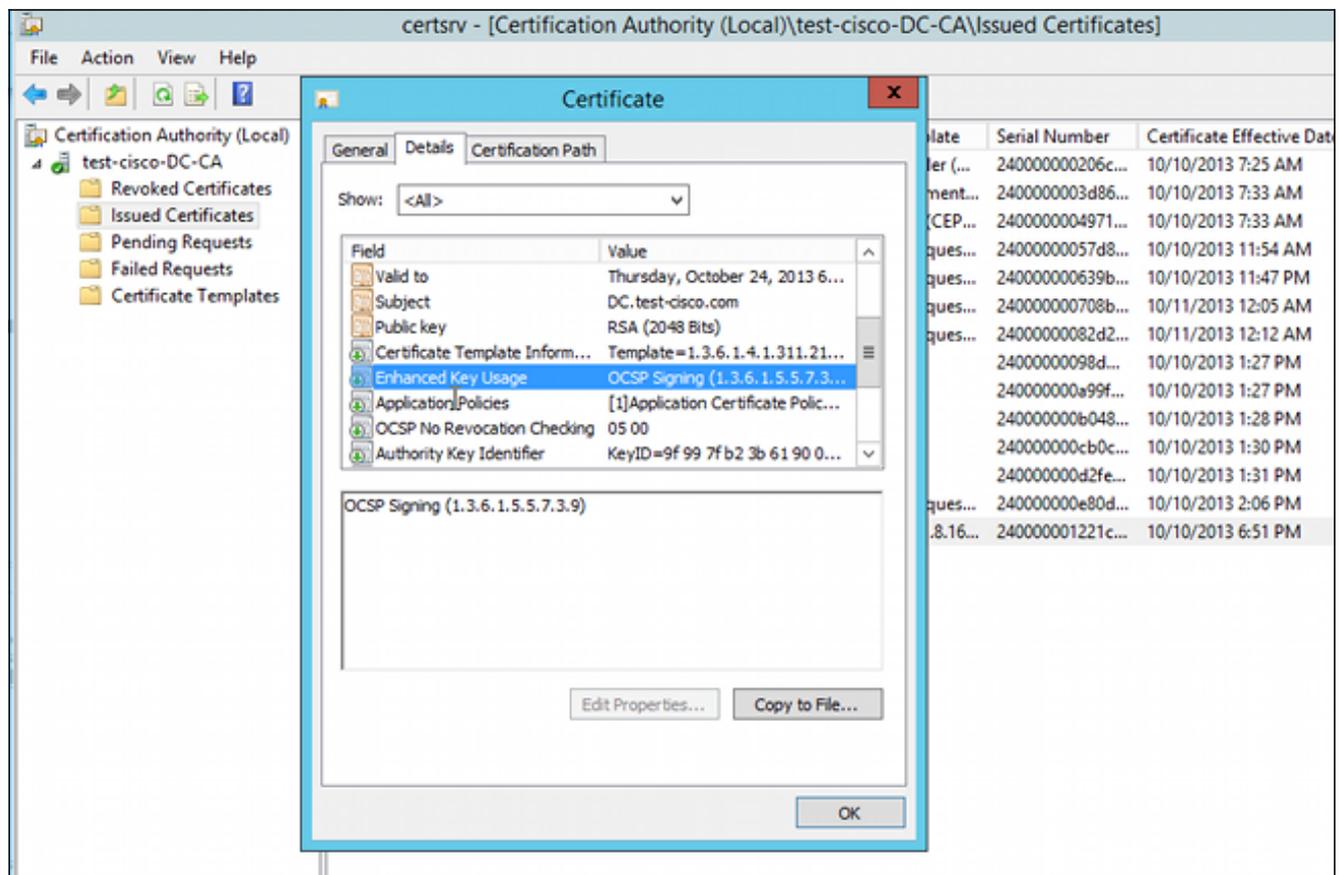


4. Confirme se o certificado está inscrito e se seu status é Processando/OK:





5. Navegue para **CA > Certificados emitidos** para verificar os detalhes do certificado:



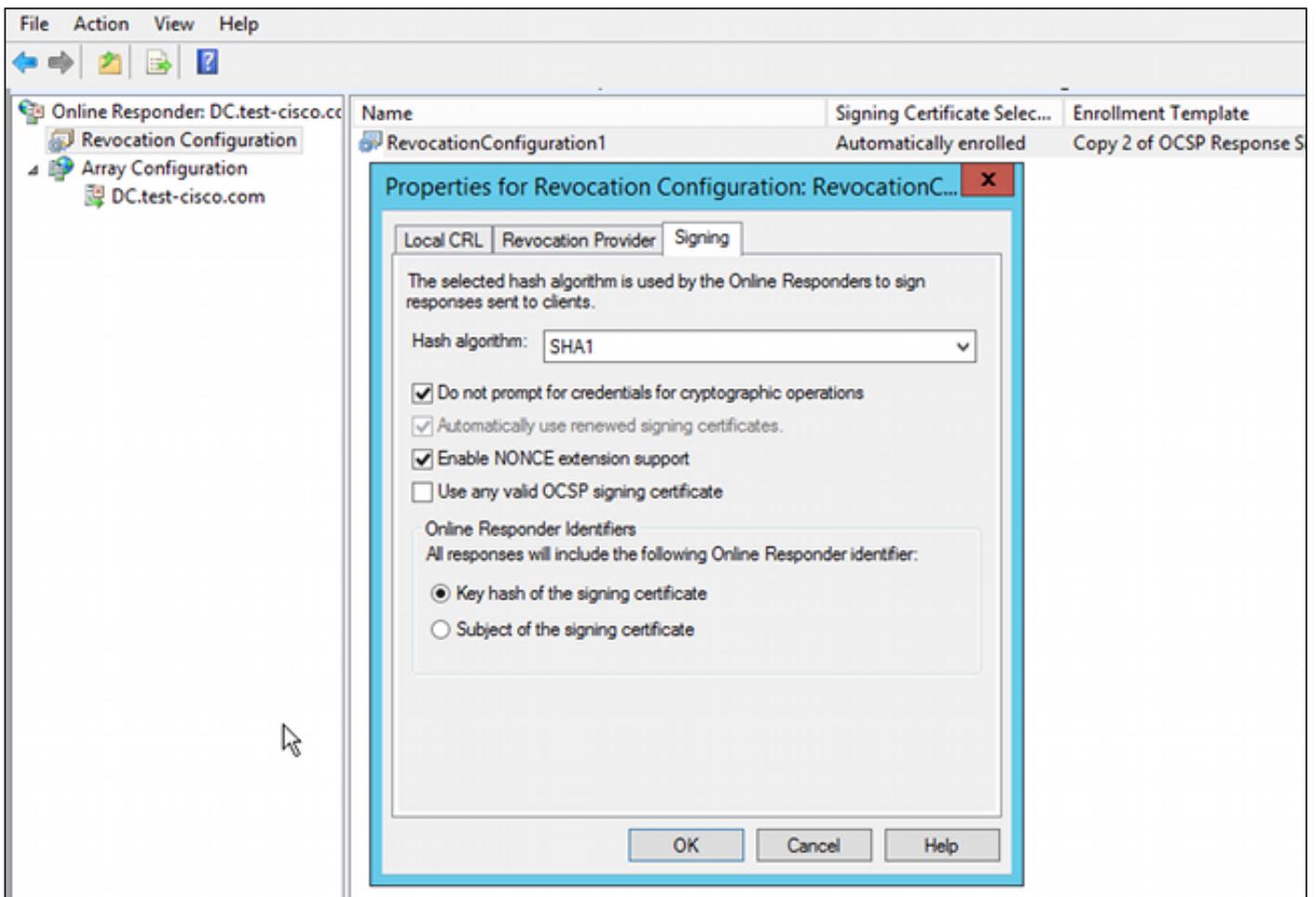
Datas de Serviço OCSP

A implementação do OCSP pela Microsoft está em conformidade com o [RFC 5019 The Lightweight Online Certificate Status Protocol \(OCSP\) Profile for High-Volume Environments](#), que é uma versão simplificada do [RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP](#).

O ASA usa RFC 2560 para OCSP. Uma das diferenças nos dois RFCs é que o RFC 5019 não aceita solicitações assinadas enviadas pelo ASA.

É possível forçar o serviço OCSP da Microsoft a aceitar essas solicitações assinadas e responder

com a resposta assinada correta. Navegue até **Revocation Configuration > RevocationConfiguration1 > Edit Properties** e selecione a opção para **Enable NONCE extension support**.



O serviço OCSP agora está pronto para uso.

Embora a Cisco não recomende isso, as ocorrências podem ser desabilitadas no ASA:

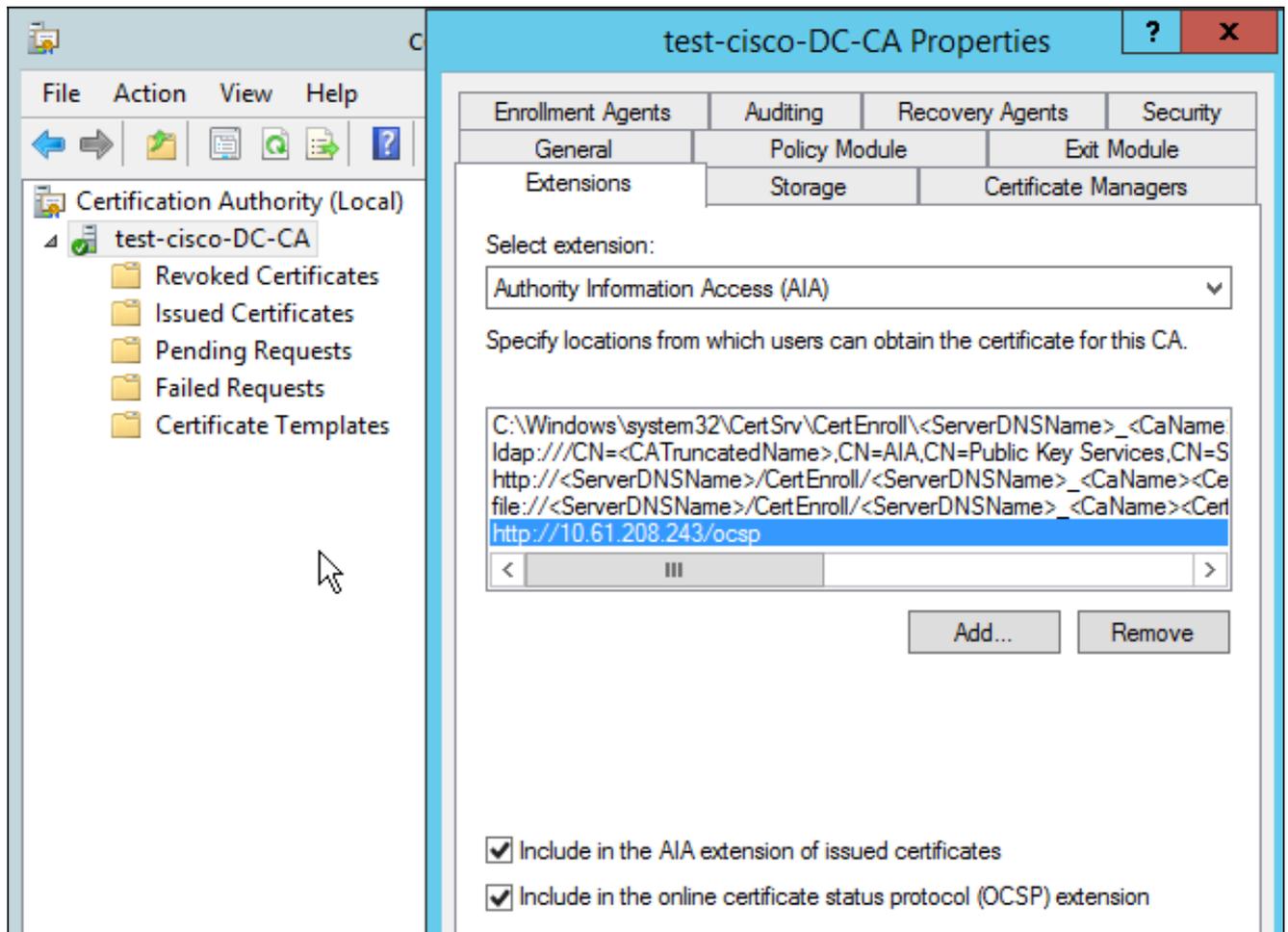
```
BSNS-ASA5510-3(config-ca-trustpoint)# ocsf disable-nonce
```

Configuração de CA para extensões OCSP

Agora você deve reconfigurar a CA para incluir a extensão do servidor OCSP em todos os certificados emitidos. A URL dessa extensão é usada pelo ASA para se conectar ao servidor OCSP quando um certificado é validado.

1. Abra a caixa de diálogo Propriedades do servidor na autoridade de certificação.
2. Clique na guia **Extensions**. É necessário o ramal AIA (Authority Information Access) que aponta para o serviço OCSP; neste exemplo, é <http://10.61.208.243/ocsp>. Habilite ambas as opções para a extensão AIA:

Incluir na extensão AIA de certificados emitidos
Incluir na extensão do protocolo de status de certificados online (OCSP)



Isso garante que todos os certificados emitidos tenham um ramal correto que aponte para o serviço OCSP.

OpenSSL

Observação: consulte o [Guia de Configuração do Cisco ASA 5500 Series usando a CLI, 8.4 e 8.6: Configuração de um Servidor Externo para Autorização do Usuário do Security Appliance](#) para obter detalhes sobre a configuração do ASA através da CLI.

Este exemplo pressupõe que o servidor OpenSSL já esteja configurado. Esta seção descreve apenas a configuração e as alterações OCSP necessárias para a configuração da CA.

Este procedimento descreve como gerar o certificado OCSP:

1. Estes parâmetros são necessários para o respondente OCSP:

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

2. Estes parâmetros são necessários para certificados de usuário:

```
[ UserCerts ]
```

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

3. Os certificados precisam ser gerados e assinados pela autoridade de certificação.

4. Inicie o servidor OCSP:

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

5. Teste o exemplo de certificado:

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

Mais exemplos estão disponíveis no [site do OpenSSL](#) .

O OpenSSL, como o ASA, suporta momentos OCSP; os momentos podem ser controlados com o uso dos switches `-nonce` e `-no_nonce`.

ASA com várias origens OCSP

O ASA pode substituir o URL do OCSP. Mesmo que o certificado do cliente contenha um URL OCSP, ele será substituído pela configuração no ASA:

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

O endereço do servidor OCSP pode ser definido explicitamente. Este exemplo de comando corresponde a todos os certificados com o administrador no nome da entidade, usa um ponto de confiança OPENSSL para validar a assinatura OCSP e usa a URL `http://11.11.11.11/ocsp` para enviar a solicitação:

```
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
```

A ordem usada para localizar o URL do OCSP é:

1. Um servidor OCSP que você define com o comando **match certificate**
2. Um servidor OCSP definido com o comando **ocsp url**
3. O servidor OCSP no campo AIA do certificado do cliente

ASA com OCSP Assinado por Outra CA

Uma resposta OCSP pode ser assinada por uma CA diferente. Nesse caso, é necessário usar o comando **match certificate** para usar um ponto de confiança diferente no ASA para validação do

certificado OCSP.

```
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
```

Neste exemplo, o ASA usa a regravção da URL do OCSP para todos os certificados com um nome de entidade que contenha administrator. O ASA é forçado a validar o certificado do respondente OCSP em relação a outro ponto confiável, o OPENS. Os certificados do usuário ainda são validados no ponto de confiança do WIN2012.

Como o certificado do respondente OCSP tem a extensão 'OCSP no revocation checks', o certificado não é verificado, mesmo quando o OCSP é forçado a validar com base no ponto de confiança OPENS.

Por padrão, todos os pontos confiáveis são pesquisados quando o ASA está tentando verificar o certificado do usuário. A validação do certificado do respondente OCSP é diferente. O ASA pesquisa apenas o ponto confiável que já foi encontrado para o certificado do usuário (WIN2012 neste exemplo).

Assim, é necessário usar o comando **match certificate** para forçar o ASA a usar um ponto de confiança diferente para a validação do certificado OCSP (OPENS neste exemplo).

Os certificados do usuário são validados em relação ao primeiro ponto confiável correspondente (WIN2012 neste exemplo), que determina o ponto confiável padrão para validação do respondente OCSP.

Se nenhum ponto de confiança específico for fornecido no comando **match certificate**, o certificado OCSP será validado em relação ao mesmo ponto de confiança que os certificados do usuário (WIN2012 neste exemplo):

```
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
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Observação: a [Output Interpreter Tool](#) (somente clientes registrados) suporta determinados comandos [show](#). Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show..

ASA - Obter Certificado via SCEP

Este procedimento descreve como obter o certificado através do SCEP:

1. Este é o processo de autenticação de ponto confiável para obter o certificado 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

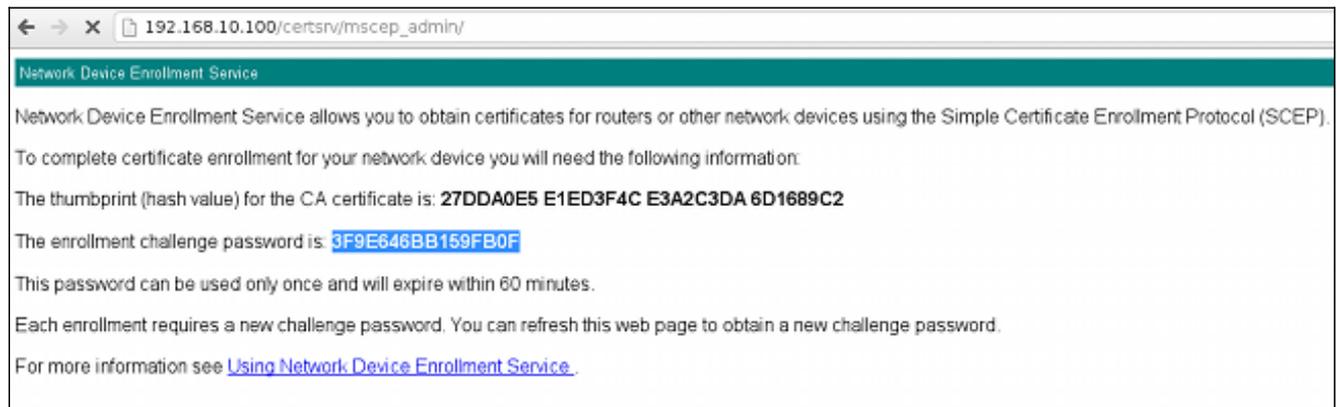
CRYPTO_PKI: http connection opened

INFO: Certificate has the following attributes:
Fingerprint:      27dda0e5 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. Para solicitar o certificado, o ASA precisa ter uma senha SCEP única que pode ser obtida no console do administrador em http://IP/certsrv/mscep_admin/:



3. Use essa senha para solicitar o certificado no 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

Algumas saídas foram omitidas por questões de clareza.

4. Verifique os certificados CA e ASA:

BSNS-ASA5510-3(config)# **show crypto ca certificates**
Certificate
Status: Available
Certificate Serial Number: 240000001cbf2fc89f44fe81970000000001c
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

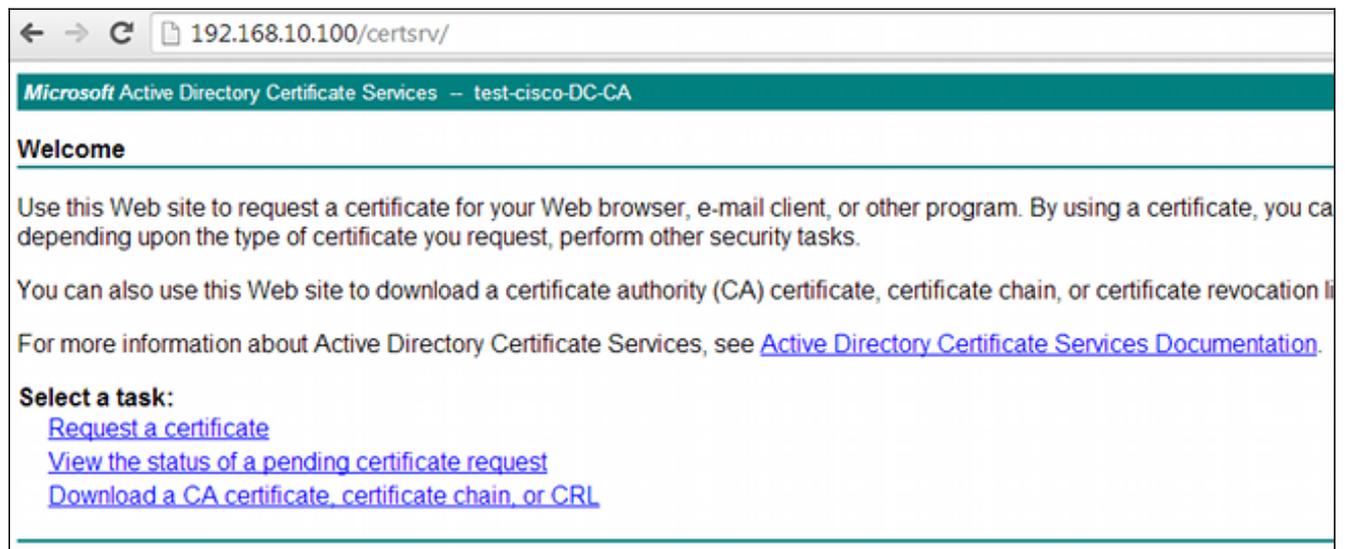
```
dc=test-cisco
dc=com
Validity Date:
  start date: 07:23:03 CEST Oct 10 2013
  end   date: 07:33:03 CEST Oct 10 2018
Associated Trustpoints: WIN2012
```

O ASA não exibe a maioria das extensões de certificado. Mesmo que o certificado ASA contenha a extensão 'URL OCSP no AIA', a CLI do ASA não a apresenta. O bug da Cisco ID [CSCui44335](#), "ASA ENH Certificate x509 extensions displayed" (Extensões x509 do certificado ASA ENH exibidas) solicita essa melhoria.

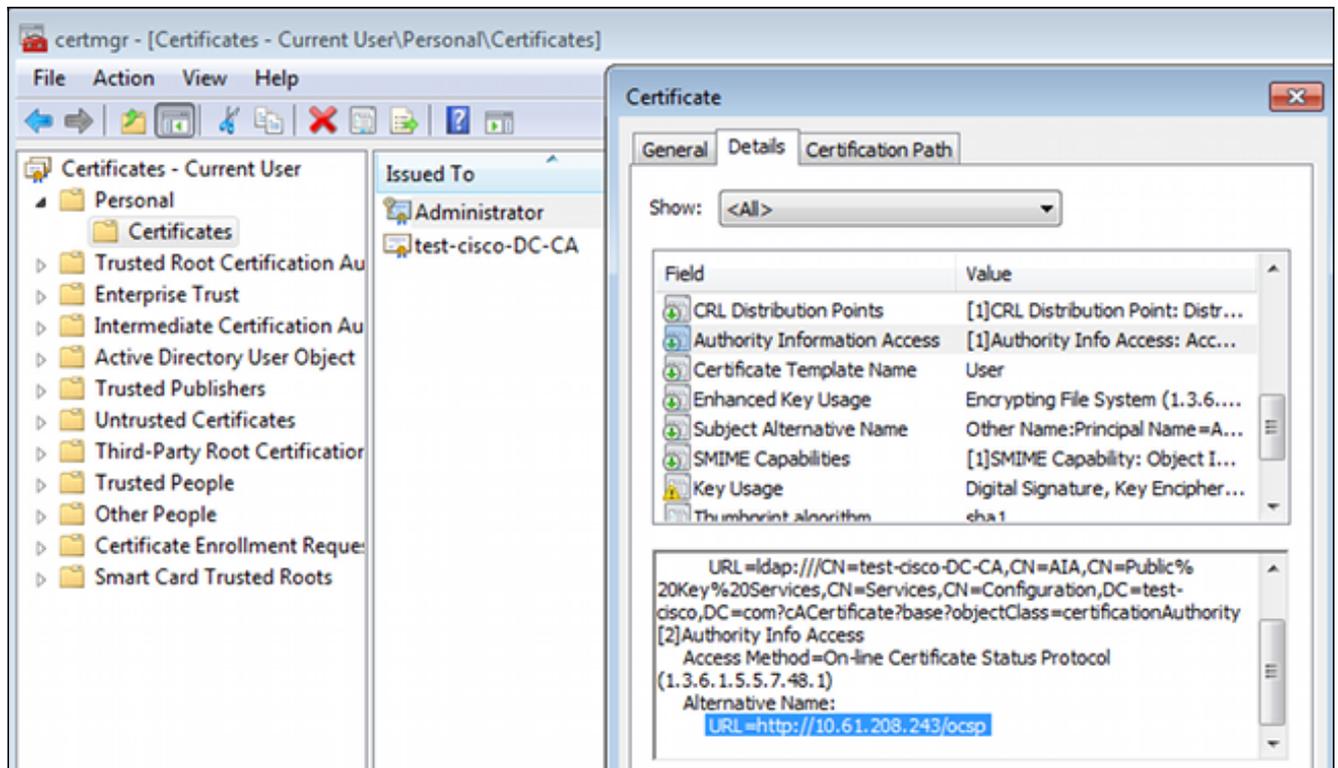
AnyConnect - Obter certificado através da página da Web

Este procedimento descreve como obter o certificado através do uso do navegador da Web no cliente:

1. Um certificado de usuário do AnyConnect pode ser solicitado por meio da página da Web. No PC cliente, use um navegador da Web para acessar a CA em `http://IP/certsrv/`:



2. O certificado do usuário pode ser salvo no armazenamento do navegador da Web e, em seguida, exportado para o armazenamento da Microsoft, que é pesquisado pelo AnyConnect. Use `certmgr.msc` para verificar o certificado recebido:



O AnyConnect também pode solicitar o certificado desde que haja um perfil do AnyConnect correto.

Acesso remoto ASA VPN com validação OCSP

Este procedimento descreve como verificar a validação OCSP:

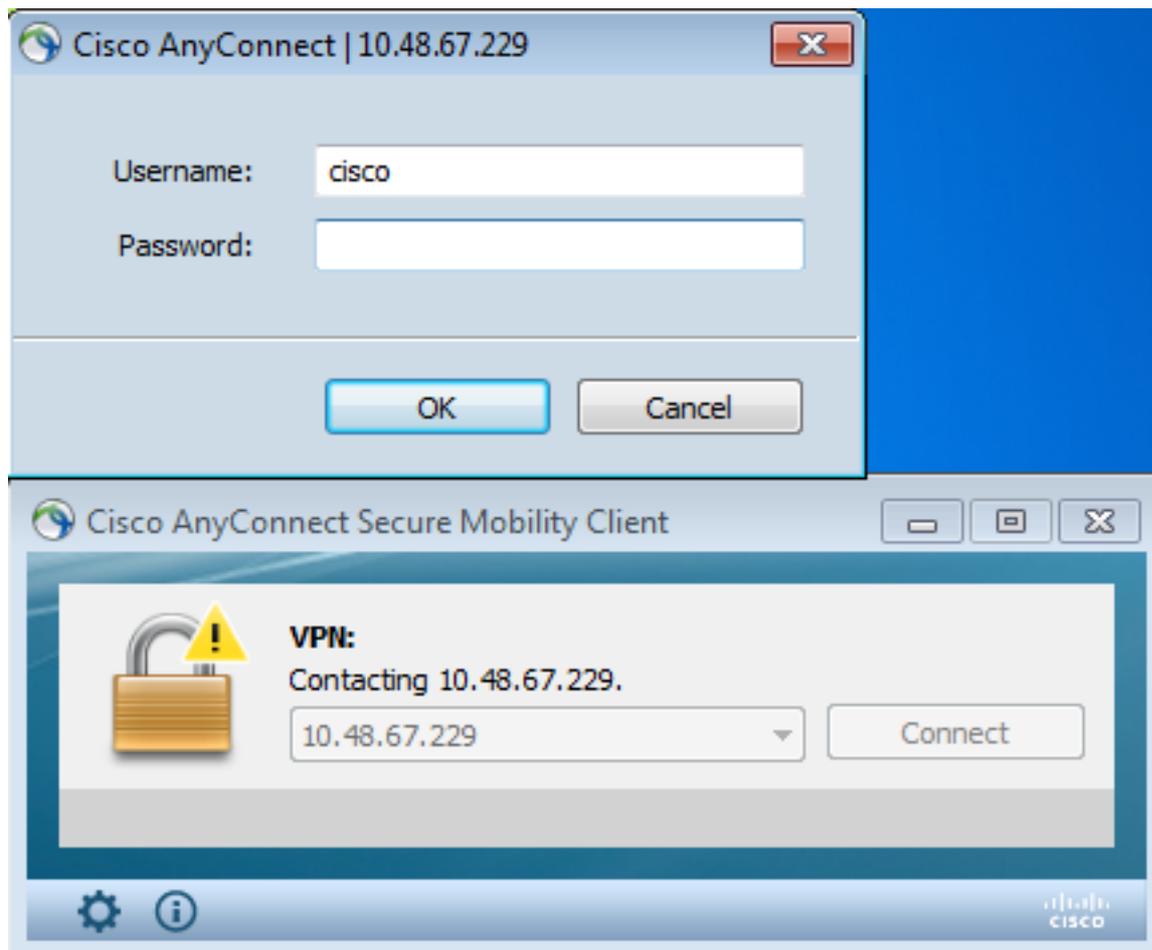
1. Enquanto tenta se conectar, o ASA relata que o certificado está sendo verificado para OCSP. Aqui, o certificado de autenticação OCSP tem uma extensão sem verificação e não foi verificado via OCSP:

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

```
%ASA-6-725001: Starting SSL handshake with client outside:
10.61.209.83/51262 for TLSv1 session.
%ASA-7-717025: Validating certificate chain containing 1 certificate(s).
%ASA-7-717029: Identified client certificate within certificate chain.
serial number: 240000001B2AD208B12811687400000000001B, subject name:
cn=Administrator,cn=Users,dc=test-cisco,dc=com.
Found a suitable trustpoint WIN2012 to validate certificate.
%ASA-7-717035: OCSP status is being checked for certificate. serial
number: 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.
```

Algumas saídas foram omitidas por questões de clareza.

2. O usuário final fornece as credenciais do usuário:



3. A sessão VPN foi concluída corretamente:

```
%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. A sessão é criada:

```
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. Você pode usar depurações detalhadas para validação 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. No nível de captura de pacotes, essa é a solicitação OCSP e a resposta OCSP correta. A resposta inclui a assinatura correta - extensão nonce habilitada no 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

Acesso remoto ASA VPN com várias fontes OCSP

Se um certificado de correspondência for configurado conforme explicado no [ASA com Várias Origens OCSP](#), ele terá precedência:

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

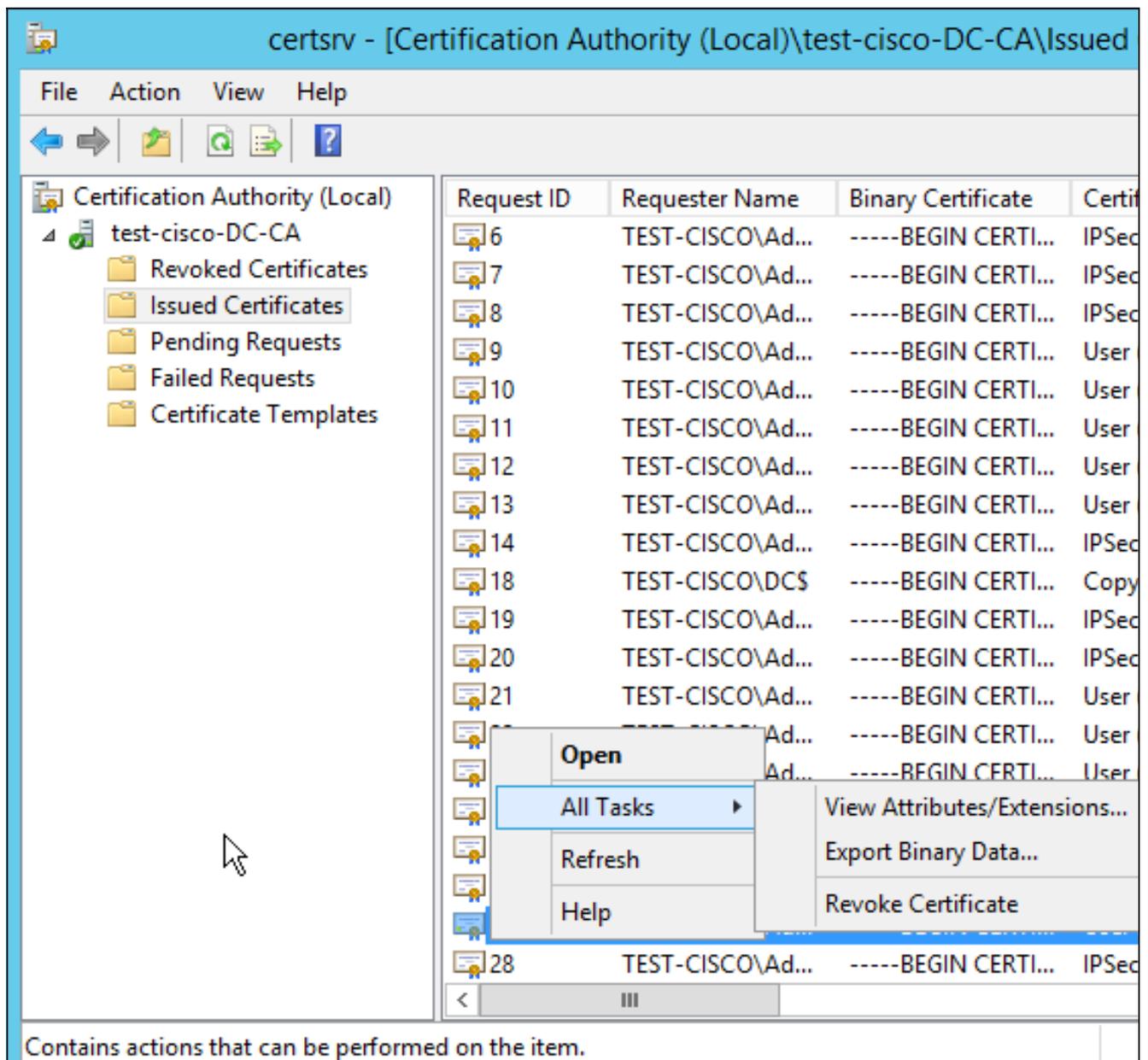
Quando uma substituição de URL OCSP é usada, as depurações são:

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

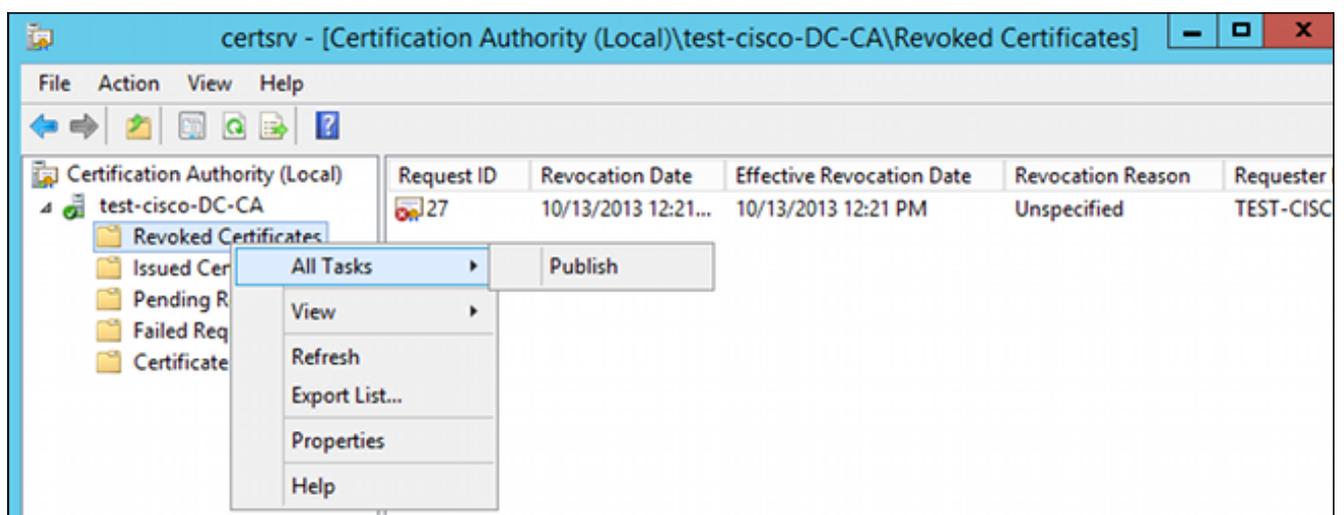
Acesso remoto ASA VPN com OCSP e certificado revogado

Este procedimento descreve como revogar o certificado e confirmar o status revogado:

1. Revogar o certificado do cliente:



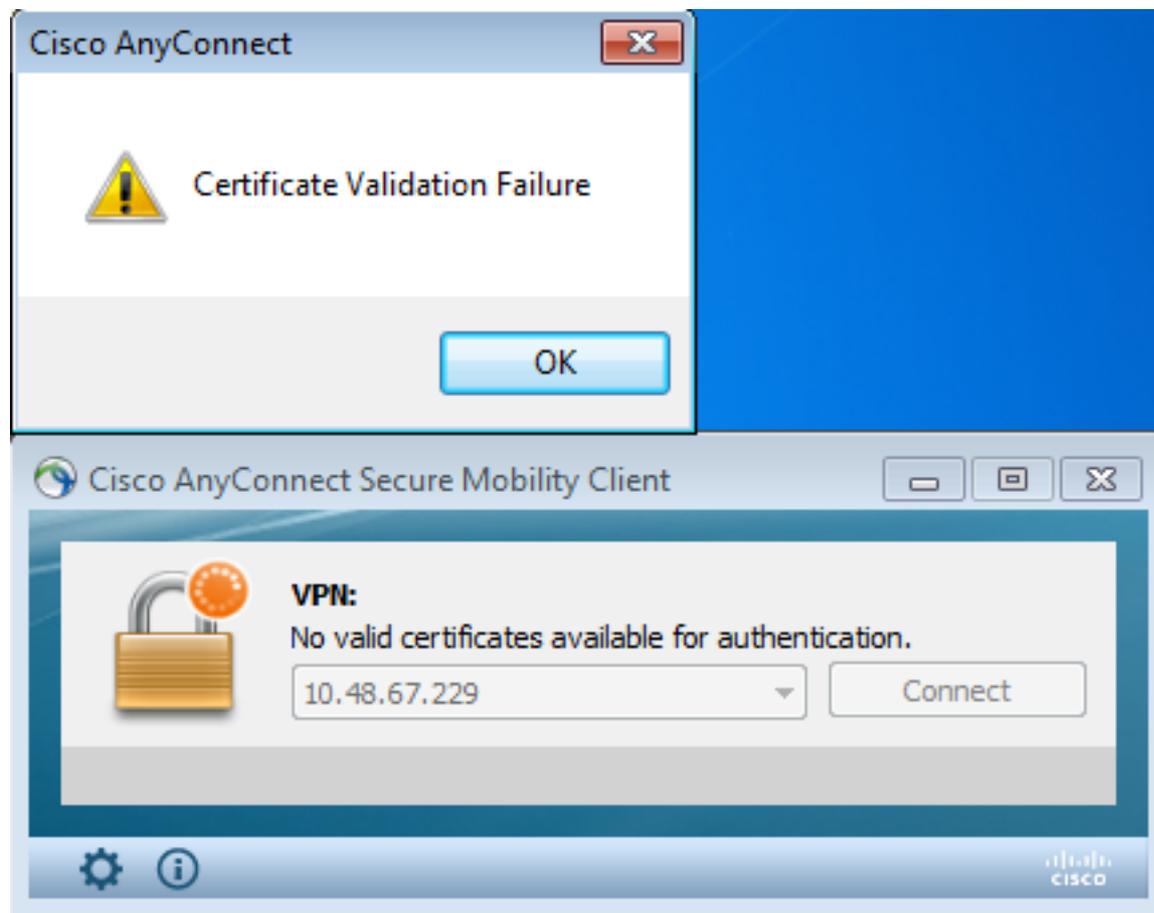
2. Publique os resultados:



3. [Opcional] As etapas 1 e 2 também podem ser executadas com o utilitário certutil CLI no Power Shell:

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

4. Quando o cliente tenta se conectar, há um erro de validação de certificado:



5. Os registros do AnyConnect também indicam o erro de validação do 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. O ASA relata que o status do certificado foi revogado:

```
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 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. As capturas de pacote mostram uma resposta OCSF bem-sucedida com o status de certificado revogado:

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)

Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua

configuração.

Servidor OCSP inoperante

O ASA relata quando o servidor OCSP está inoperante:

```
CRYPTO_PKI: unable to find a valid OCSP server.
```

```
CRYPTO_PKI: OCSP revocation check has failed. Status: 1800.
```

As capturas de pacotes também podem ajudar na solução de problemas.

Hora Não Sincronizada

Se a hora atual no servidor OCSP for mais antiga que no ASA (pequenas diferenças são aceitáveis), o servidor OCSP enviará uma resposta não autorizada e o ASA a relatará:

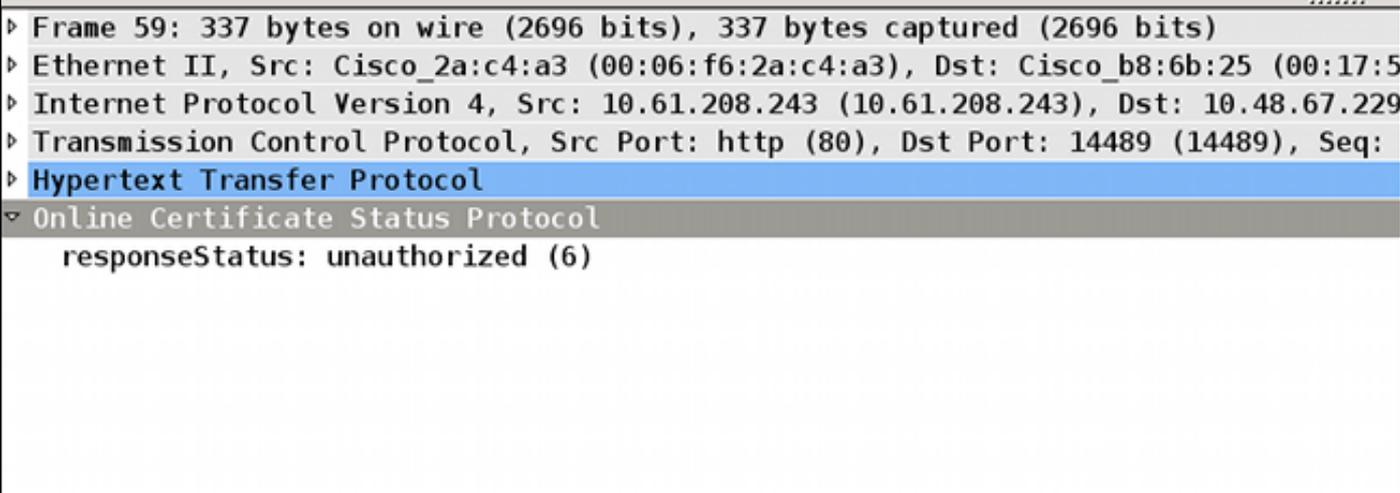
```
CRYPTO_PKI: OCSP response status - unauthorized
```

Quando o ASA recebe uma resposta OCSP de tempos futuros, ele também falha.

Não Há Suporte Para Datas Assinadas

Se não houver suporte para momentos no servidor (que é o padrão no Microsoft Windows 2012 R2), uma resposta não autorizada será retornada:

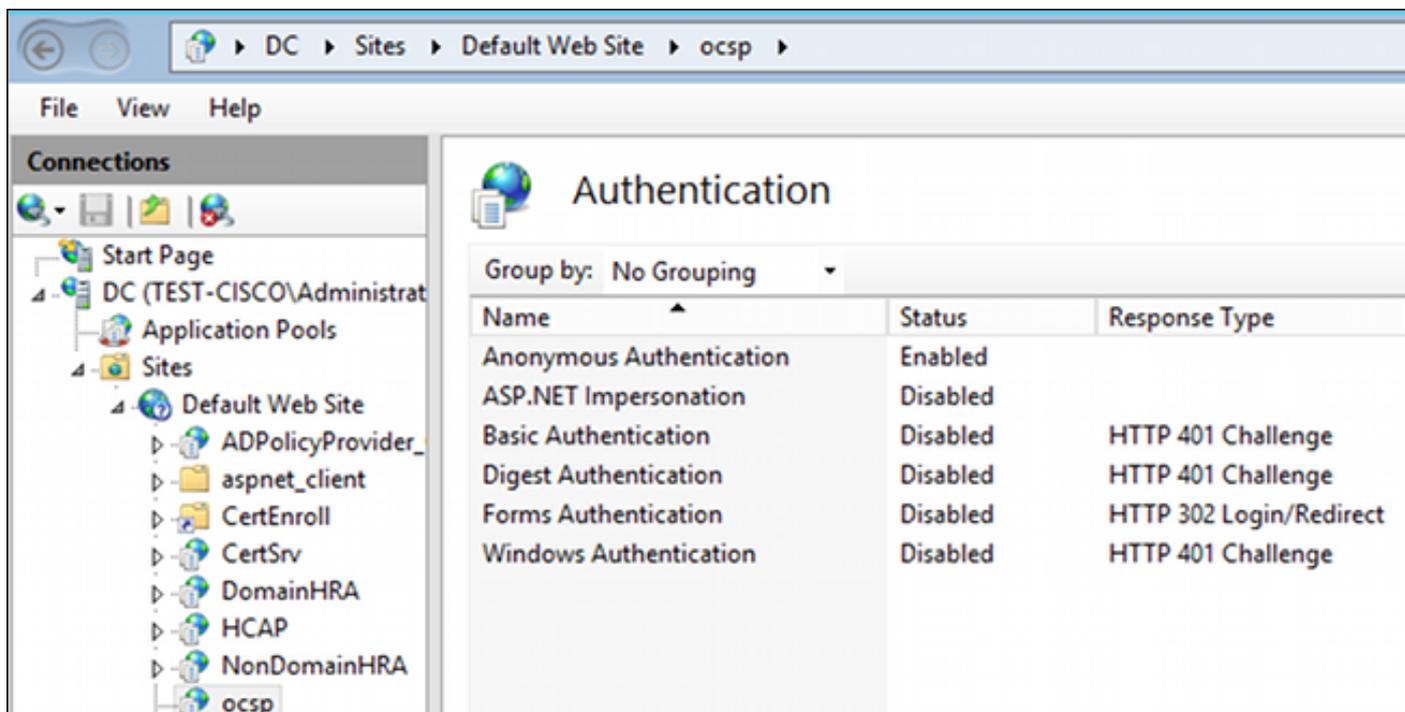
No.	Source	Destination	Protocol	Length	Info
56	10.48.67.229	10.61.208.243	OCSP	545	Request
59	10.61.208.243	10.48.67.229	OCSP	337	Response



```
▶ 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)
```

Autenticação do Servidor IIS7

Os problemas com uma solicitação SCEP/OCSP geralmente são o resultado de autenticação incorreta no Internet Information Services 7 (IIS7). Verifique se o acesso anônimo está configurado:



Informações Relacionadas

- [Microsoft TechNet: Guia de instalação, configuração e solução de problemas do respondente online](#)
- [Microsoft TechNet: Configurar uma CA para oferecer suporte a respondentes OCSP](#)
- [Referência de comandos do Cisco ASA Series](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.