Microsoft Windows 2012 および OpenSSL で OCSP 検証を使用した ASA リモート アクセス VPN

内容

概要

このドキュメントでは、VPN ユーザが提示した証明書に対して、Cisco 適応型セキュリティ アプライアンス（ASA）の Online Certificate Status Protocol（OCSP）検証を使用する方法について

説明します。2 台の OCSP サーバ（Microsoft Windows 認証局（CA）と OpenSSL）の設定例を示します。「確認」セクションでは、パケット レベルでの詳細なフローについて説明し、「トラブルシューティング」セクションでは、一般的なエラーや問題について重点的に説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco 適応型セキュリティ アプライアンス コマンドライン インターフェイス（CLI）の設定および Secure Socket Layer（SSL）VPN の設定
- X.509 証明書
- Microsoft Windows Server
- Linux/OpenSSL

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco 適応型セキュリティ アプライアンス ソフトウェア バージョン 8.4 以降
- Cisco AnyConnect セキュア モビリティ クライアント リリース 3.1 を備えた Microsoft Windows 7
- Microsoft SQL Server 2012 R2
- OpenSSL 1.0.0j 以降を備えた Linux

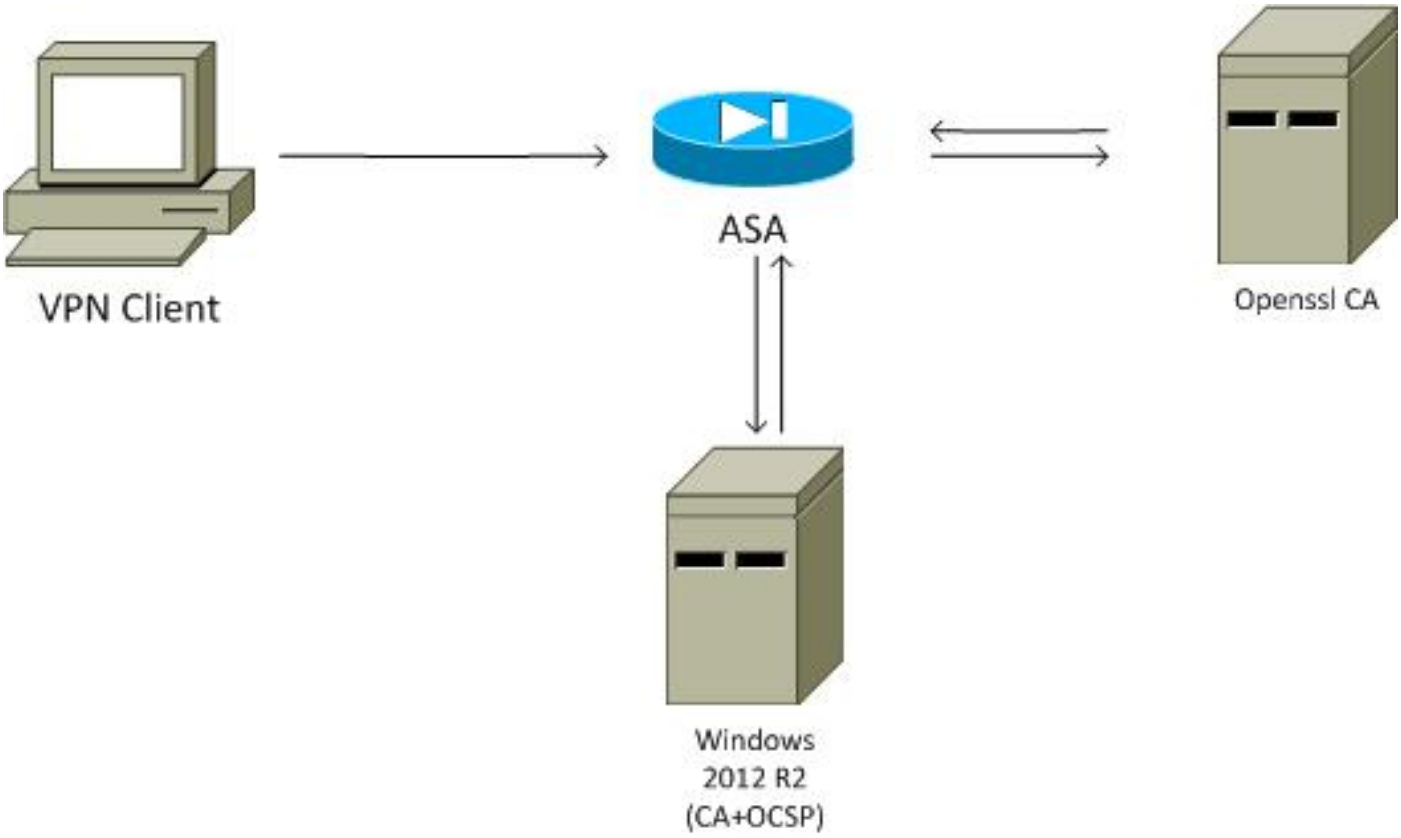
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

設定

> **注**：このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool(登録ユーザ専用)を使用してください。

ネットワーク図

クライアントはリモート アクセス VPN を使用します。このアクセス VPN には、Cisco VPN Client（IPSec）、Cisco AnyConnect セキュア モビリティ（SSL/Internet Key Exchange バージョン 2（IKEv2）、または WebVPN（ポータル））を使用できます。ログインするために、クライアントは、正しい証明書を提供し、ASA でローカルに設定されたユーザ名/パスワードを入力します。クライアント証明書は OCSP サーバ経由で検証されます。



OCSP による ASA リモート アクセス

ASA は SSL アクセス用に設定されています。クライアントは、AnyConnect を使用してログインします。ASA は、Simple Certificate Enrollment Protocol（SCEP）を使用して証明書を要求します。

```
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
```

証明書マップが作成され、これによって、administrator（大文字と小文字が区別されます）という単語がサブジェクト名に含まれるすべてのユーザが識別されます。これらのユーザは、RA という名前のトンネル グループにバインドされます。

```
webvpn
 enable outside
 anyconnect image disk0:/anyconnect-win-3.1.02040-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable
 certificate-group-map MAP 10 RA
```

VPN 設定には、認証に成功すること（つまり、検証された証明書）が必要です。また、ローカルに定義されたユーザ名（認証 aaa）用の正しいクレデンシャルも必要です。

```
username cisco password xxxxxxx
ip local pool POOL 192.168.11.100-192.168.11.105 mask 255.255.255.0

aaa authentication LOCAL
```

```
aaa authorization LOCAL

group-policy MY internal
group-policy MY attributes
 vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless

tunnel-group RA type remote-access
tunnel-group RA general-attributes
 address-pool POOL
 default-group-policy MY
 authorization-required
tunnel-group RA webvpn-attributes
 authentication aaa certificate
 group-alias RA enable
```

Microsoft Windows 2012 CA

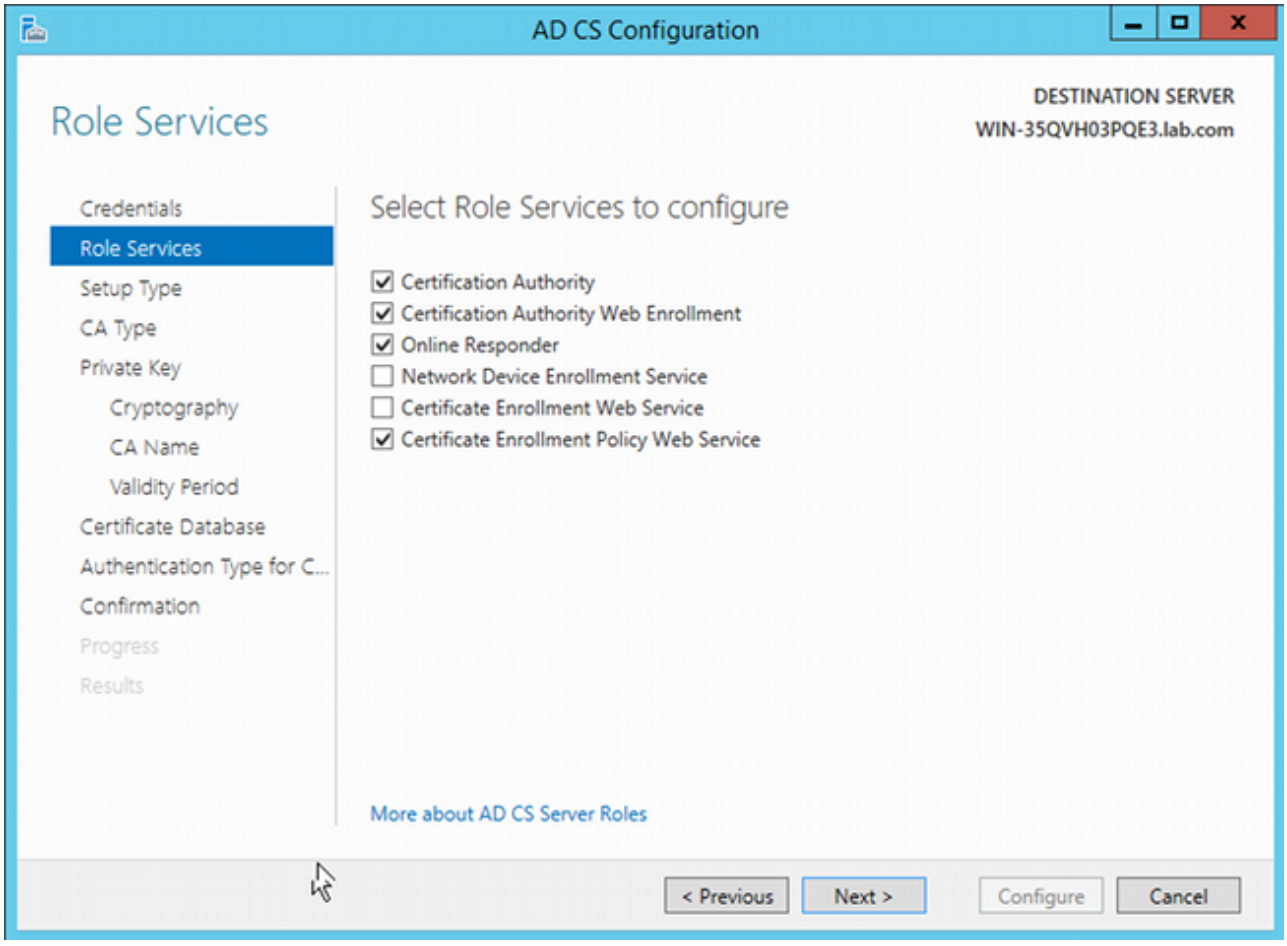
> **注：CLIを使用したASAの設定の詳細については、**『CLIを使用したCisco ASA 5500シリーズ設定ガイド、8.4および8.6：セキュリティアプライアンスユーザ許可のための外部サーバの設定』を参照してください。

サービスのインストール

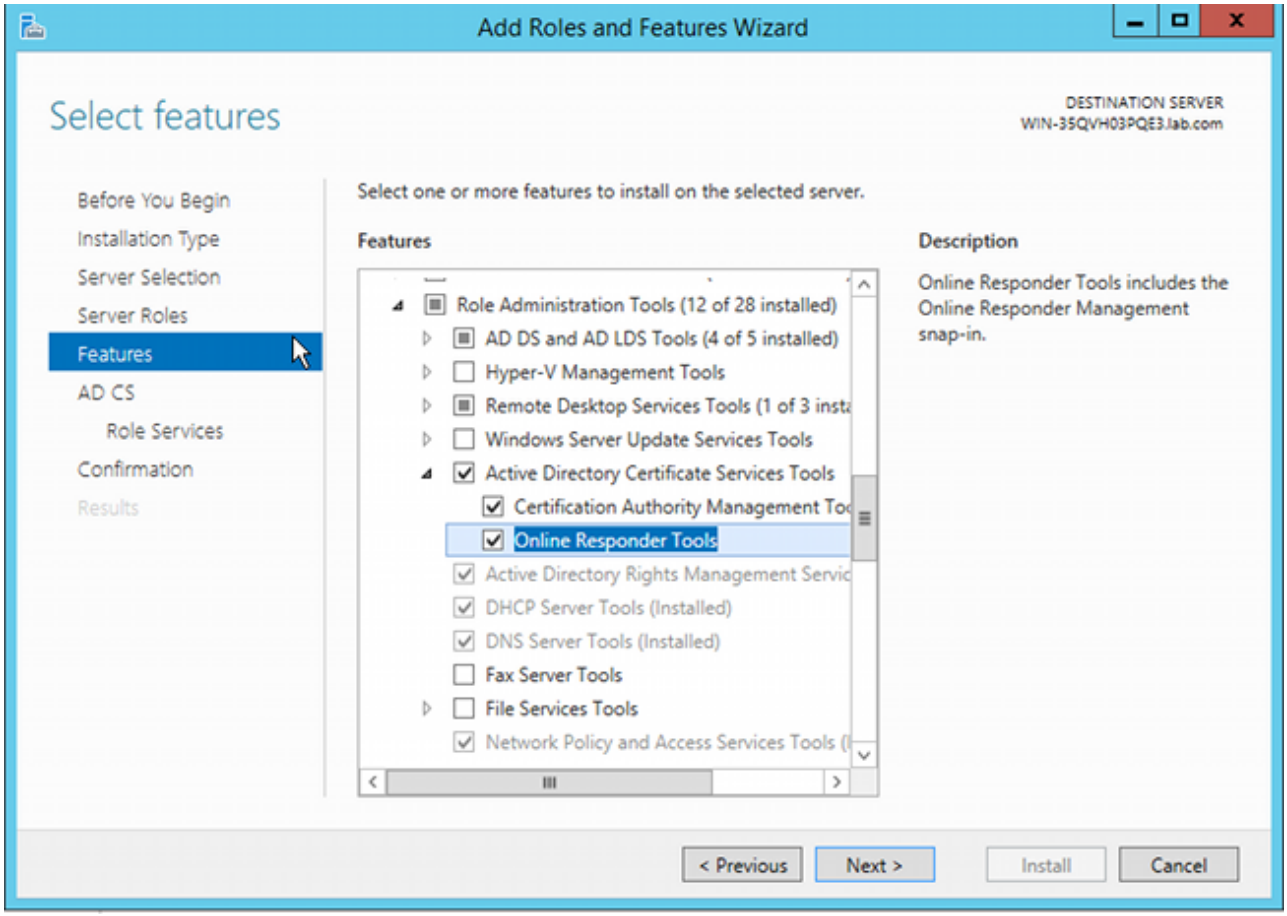
この手順では、Microsoft サーバのロール サービスの設定方法を説明します。

1. [Server Manager] **> [Manage] > [Add Roles and Features]** に移動します。Microsoft サーバには、次のロール サービスが必要です。

   認証局（CA）認証局 Web 登録（クライアントで使用される）Online Responder（OCSP に必要）Network Device Enrollment Service（ASA が使用する SCEP アプリケーションが含まれる） ポリシーを含む Web サービスを、必要に応じて追加できます。



2.
3.
4. 機能を追加する場合は、Online Responder Tool を必ず含めてください。これには、後で使用する OCSP スナップインが含まれるためです。



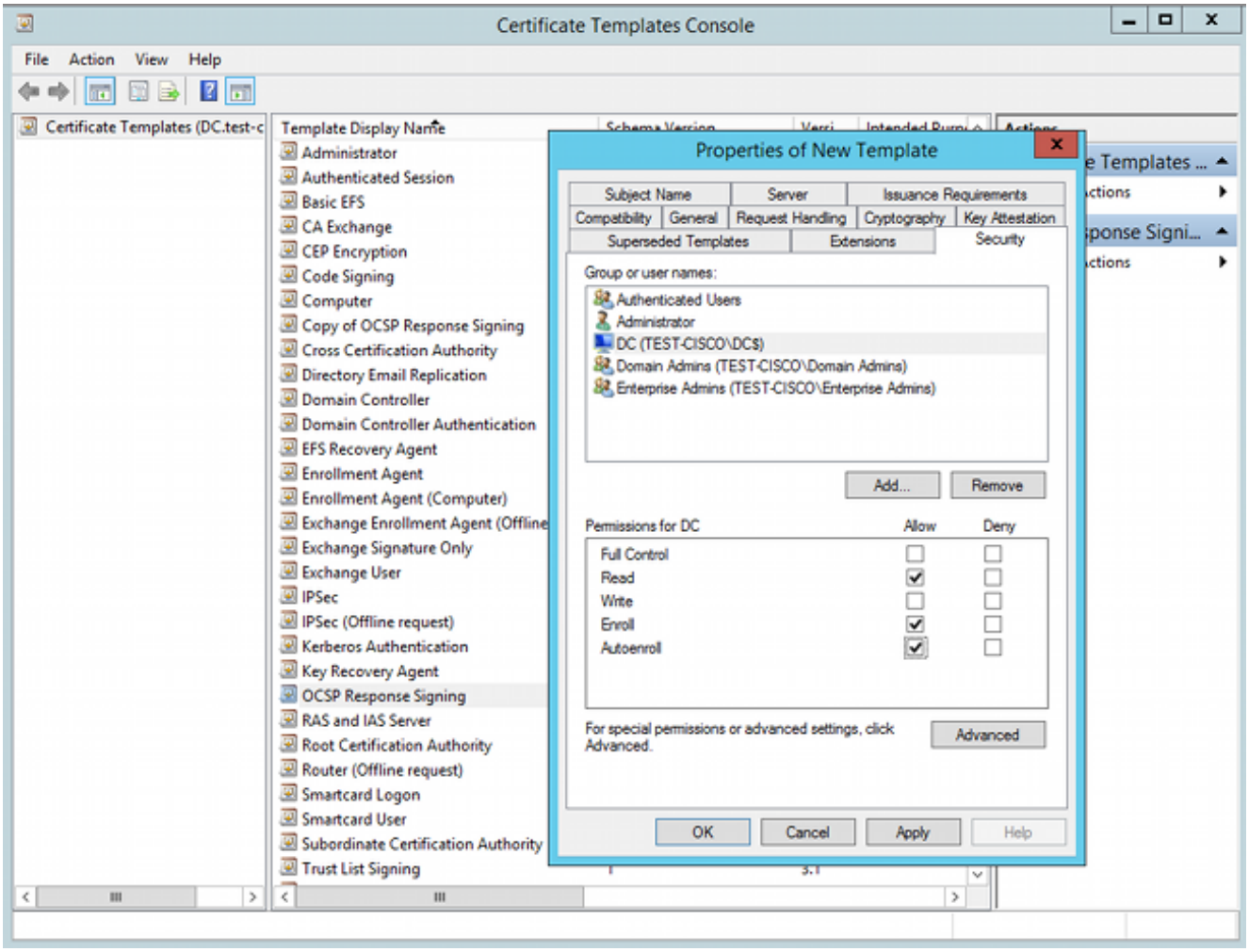
OCSP テンプレートの CA 設定

OCSP サービスは、証明書を使用して OCSP 応答に署名します。Microsoft サーバでは、次のものを含む特別な証明書を生成する必要があります。

- 拡張キー使用法 = OCSP 署名
- OCSP 失効チェック

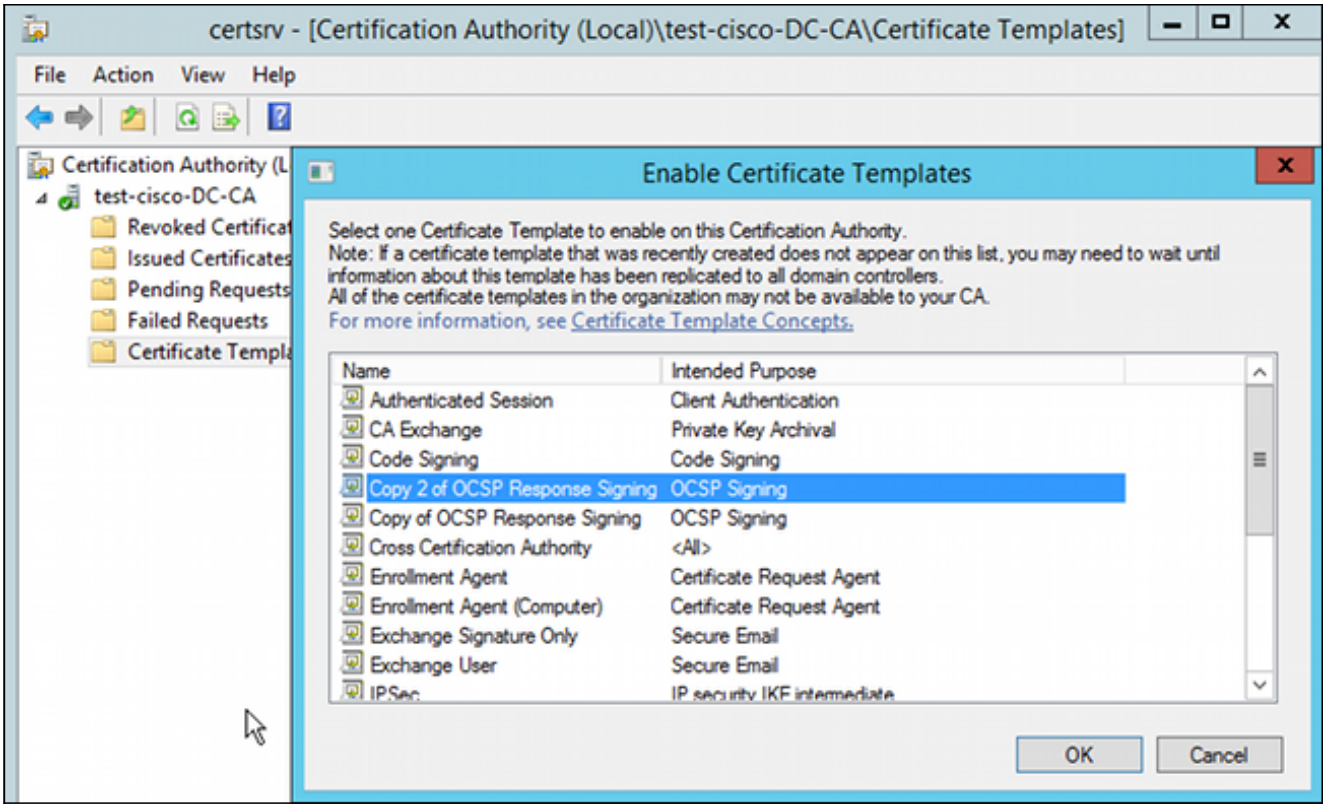
この証明書は、OCSP 検証のループを防ぐために必要です。ASA は、OCSP サービスが提示する証明書を確認しようとする場合に、証明書サービスは使用しません。

1. CAで証明書のテンプレートを追加します。[CA] > [Certificate Template] > [Manage] に移動し、[OCSP Response Signing] を選択してテンプレートを複製します。新しく作成したテンプレートのプロパティを確認し、[Security] **タブをクリックします。**権限では、そのテンプレートを使用して証明書を要求できるエンティティはどれかが説明されています。したがって、正しい権限が必要です。この例では、そのエンティティは、同じホスト（TEST-CISCO\DC）で動作している OCSP サービスであり、この OCSP サービスには Autoenroll 権限が必要です。



テンプレートのその他の設定はすべて、デフォルトに設定できます。

2. テンプレートをアクティブにします。[CA] > **[Certificate Template] > [New] > [Certificate Template to Issue]** に移動し、複製したテンプレートを選択します。

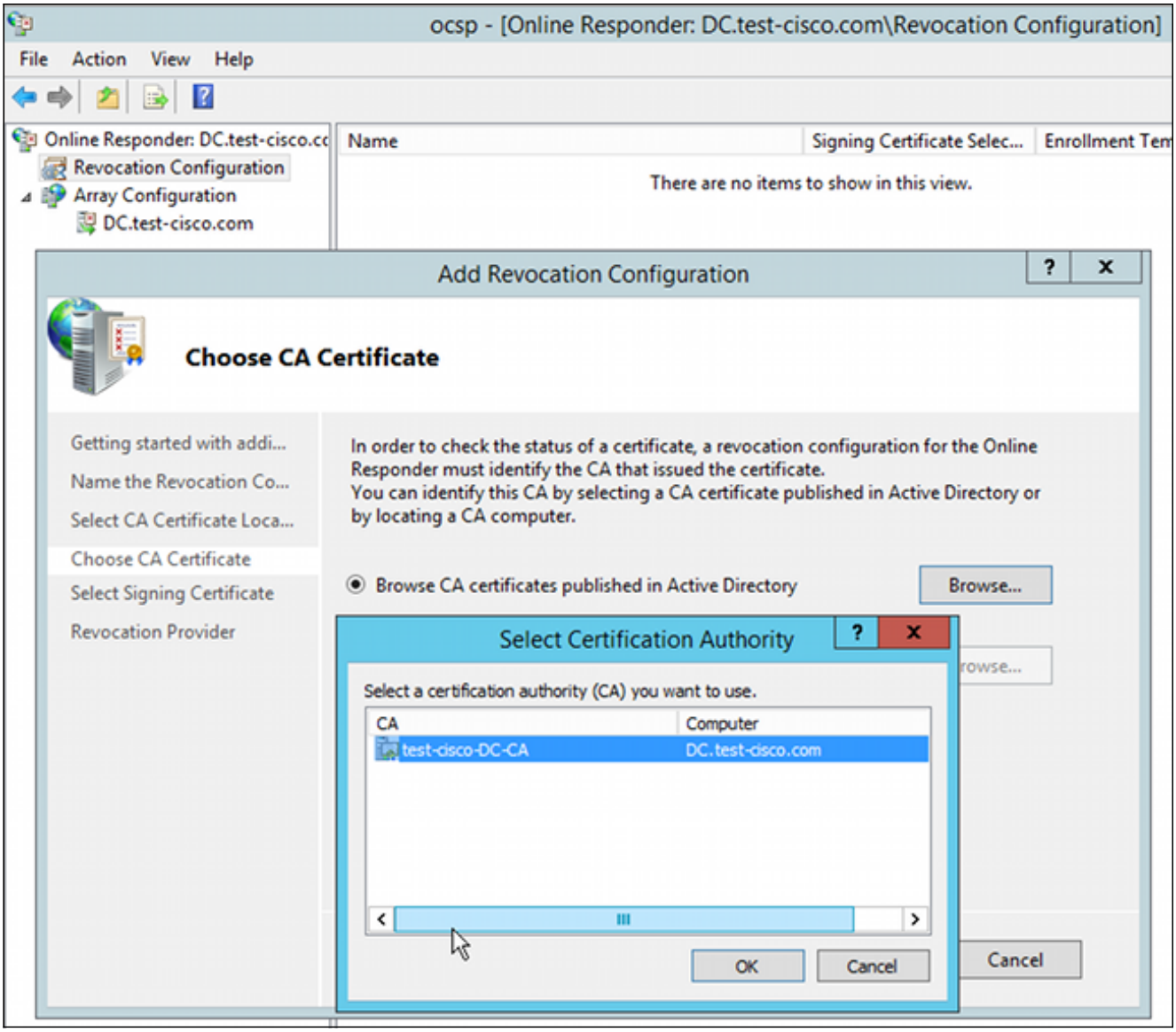


OCSP サービス証明書

この手順では、オンライン構成管理を使用して OCSP を設定する方法について説明します。

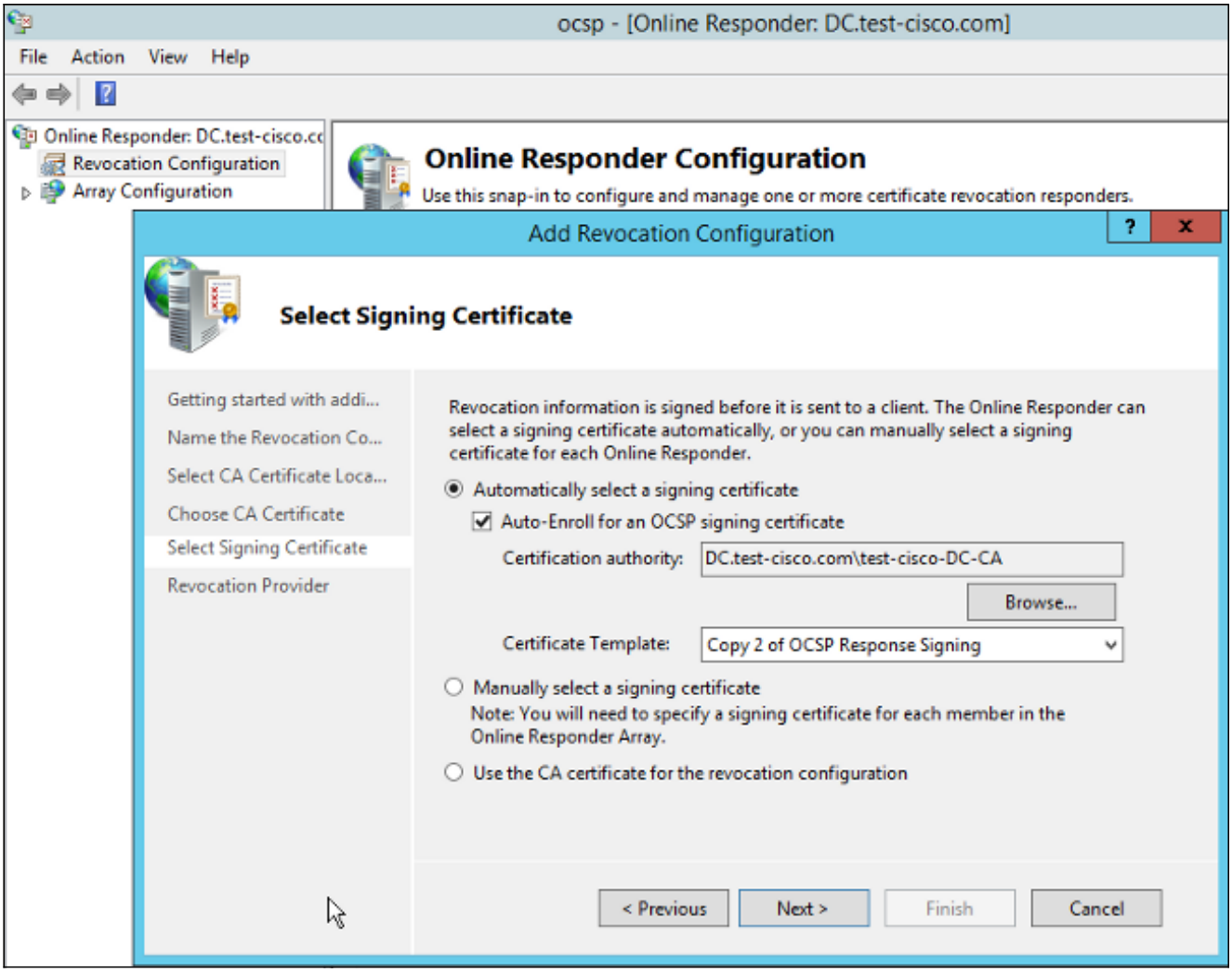
1. [Server Manager] **> [Tools]** に移動します。

2. [Revocation Configuration] **> [Add Revocation Configuration] に移動して、新しい証明書を追加します。**

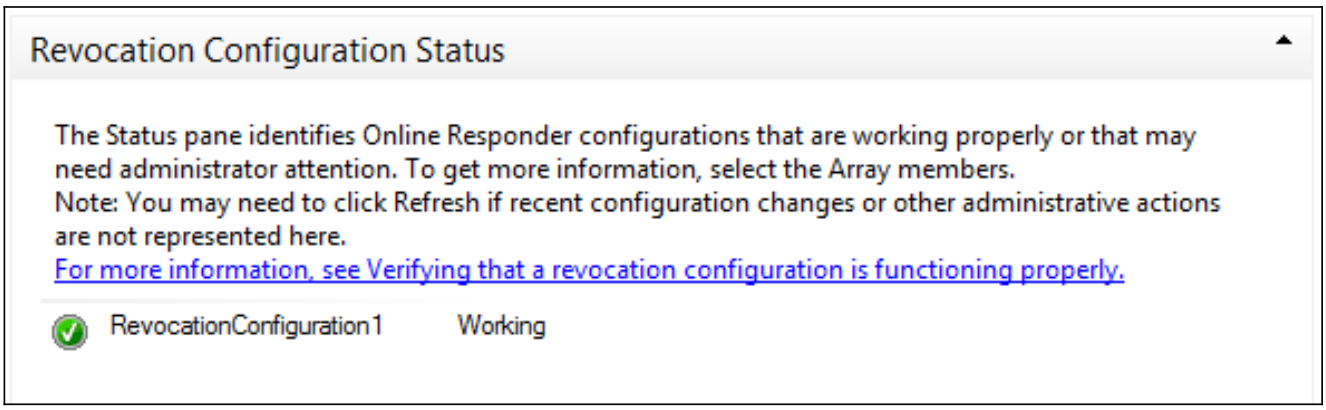


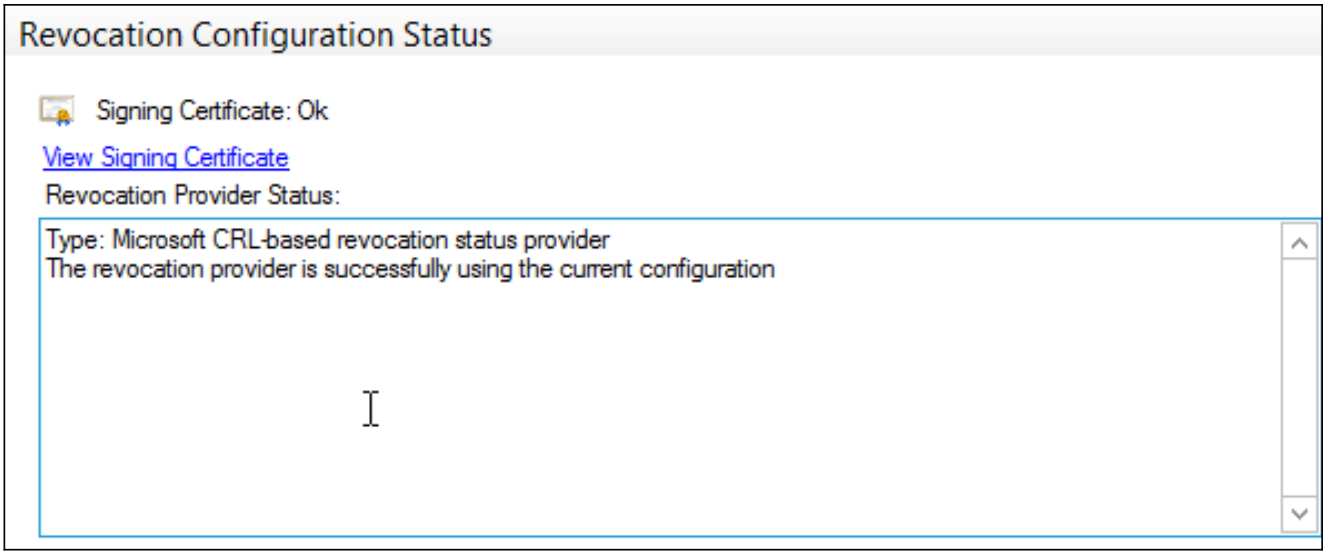
OCSP は、同じエンタープライズ CA を使用できます。OCSP サービスの証明書が生成されます。

3. 選択したエンタープライズ CA を使用し、前に作成したテンプレートを選択します。証明書が自動的に登録されます。

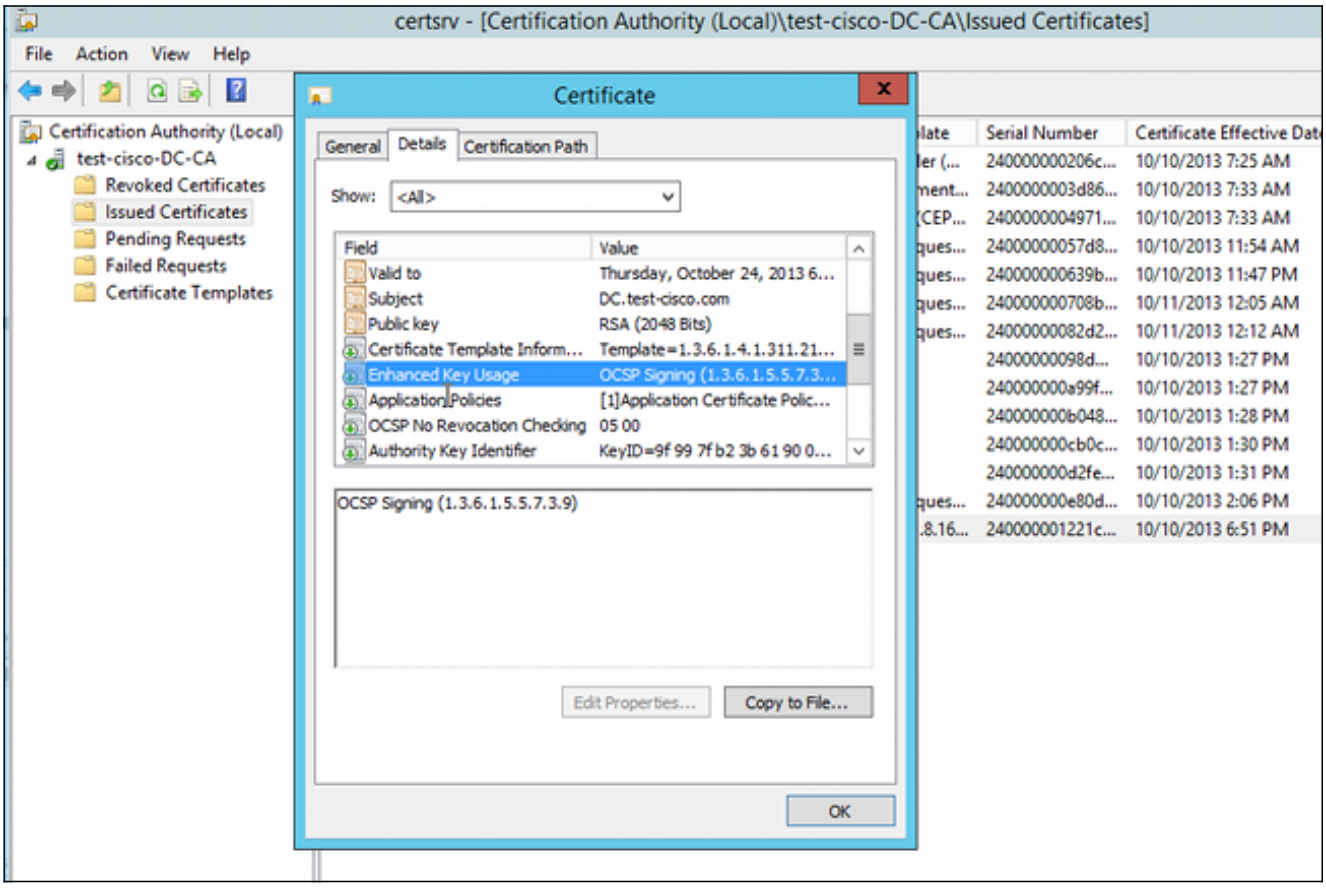


4. 証明書が登録され、状態が Working/OK であることを確認します。





5. [CA] **> [Issued Certificates] に移動して、証明書の詳細を確認します。**



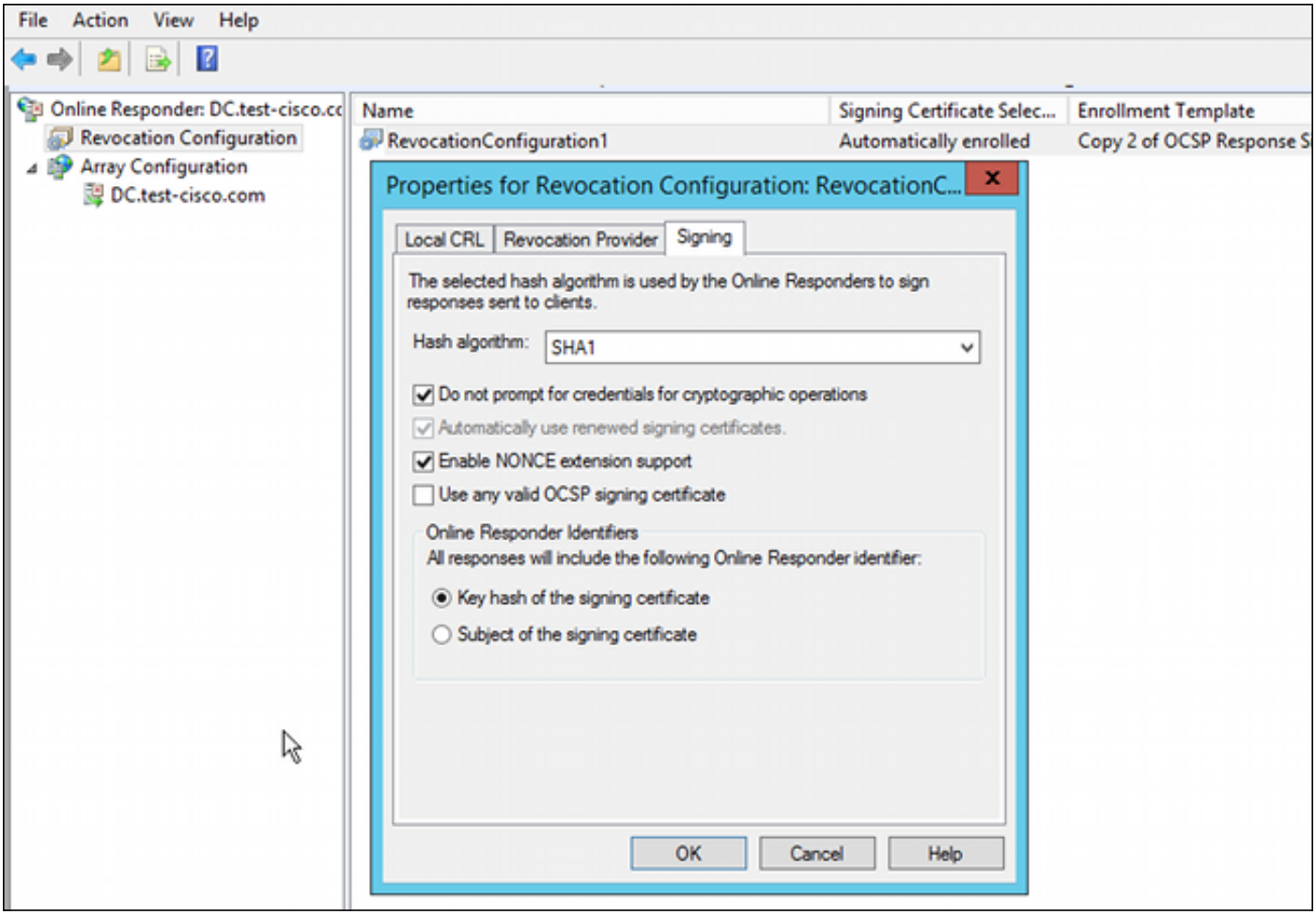
OCSP サービス ナンス

Microsoft による OCSP の実装は、[RFC 5019 The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments に準拠しています。これは、RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP の簡易バージョンです。]

ASA は、OCSP に RFC 2560 を使用します。2 つの RFC の相違点の 1 つは、RFC 5019 では、ASA によって送信された署名済み要求を受け入れないことです。

このような署名済み要求を Microsoft 証明書サービスで強制的に受け入れ、適切な署名済み応答

で応答させることができます。[Revocation Configuration] **> [RevocationConfiguration1] > [Edit Properties] に移動し、[Enable NONCE extension support]** オプションを選択して NONCE 拡張のサポートを有効にします。



これで、OCSP サービスが使用可能になりました。

シスコでは推奨していませんが、ナンスは ASA で無効にすることができます。

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

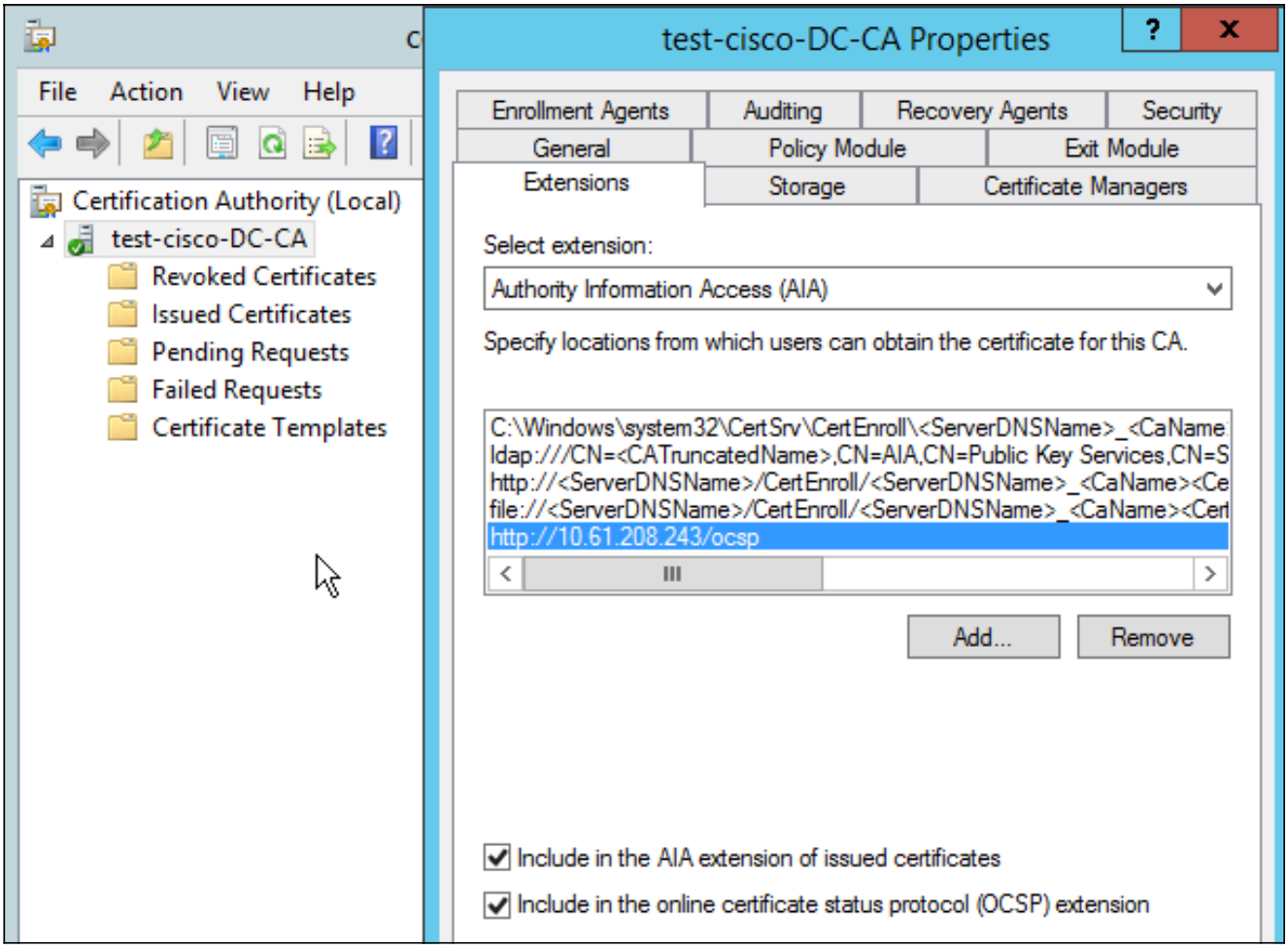
OCSP 拡張の CA 設定

今度は、すべての発行済み証明書に OCSP サーバ拡張が含まれるように CA を再設定する必要があります。ASA は、この拡張からの URL を使用して、証明書の検証時に OCSP サーバに接続します。

1. CA で、サーバの [Properties] ダイアログボックスを開きます。

2. [Extensions] **タブをクリックします。**OCSPサービスをポイントするAuthority Information Access(AIA)拡張が必要です。この例では、http://10.61.208.243/ocspです。AIA 拡張の両方のオプションを有効にします。

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



これで、すべての発行済み証明書に、OCSP サービスをポイントする正しい拡張が確実に含まれます。

OpenSSL

注：CLIを使用したASAの設定の詳細については、『CLIを使用したCisco ASA 5500シリーズ設定ガイド、8.4および8.6：セキュリティアプライアンスユーザ許可のための外部サーバの設定』を参照してください。

この例では、OpenSSL サーバがすでに設定されていると想定しています。このセクションでは、OSCP 設定と、CA 設定に必要な変更についてのみ説明します。

次の手順では、OCSP 証明書の生成方法について説明します。

1. 次のパラメータが、OCSP レスポンダに必要です。

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

2. 次のパラメータが、ユーザ証明書に必要です。

```
[ UserCerts ]
```

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

3. 証明書は、CA によって生成され、署名される必要があります。

4. OCSP サーバを起動します。

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

5. サンプル証明書をテストします。

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

[OpenSSL Web サイトには、さらに多くのサンプルが用意されています。]

OpenSSLは、ASAと同様にOCSPナンスをサポートします。ナンスは、-nonceおよび –no_nonceスイッチを使用して制御できます。

複数の OCSP ソースを含む ASA

ASA は、OCSP URL をオーバーライドできます。クライアント証明書に OCSP の URL が含まれていても、ASA での設定によって上書きされます。

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

OCSP サーバ アドレスは、明示的に定義できます。次のコマンド例では、すべての証明書をサブジェクト名の管理者に照合し、OPENSSL トラストポイントを使用して OCSP 署名を検証します。また、http://11.11.11.11/ocsp の URL を使用して要求を送信します。

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

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

OCSP URL の検索で使用される順序は次のとおりです。

1. match certificate コマンドで設定した OCSP サーバ
2. ocsp url コマンドで設定した OCSP サーバ
3. クライアント証明書の AIA フィールドに指定された OCSP サーバ

異なる CA によって署名された OCSP を含む ASA

OCSP応答は、別のCAによって署名できます。このような場合、ASAでOCSP証明書の検証に別のトラストポイントを使用するには、match certificateコマンドを使用する必要があります。

```
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
```

この例では、ASA が、administrator を含むサブジェクト名を持つすべての証明書に対して、OCSP URL の書き換えを使用します。ASA では強制的に、別のトラストポイント、OPENSSL に対して OCSP レスポンダ証明書が検証されます。この場合でも、ユーザ証明書は WIN2012 トラストポイントで検証されます。

OCSP レスポンダ証明書には「OCSP を失効チェック」拡張があるため、OCSP で強制的に OPENSSL トラストポイントに対して検証される場合でも、この証明書は検証されません。

デフォルトでは、すべてトラストポイントが、ASA がユーザ証明書を検証しようとしているときに検索されます。これは、OCSP レスポンダ証明書の検証では異なります。ASA は、ユーザ証明書（この例では WIN2012）用にすでに見つかっているトラストポイントだけを検索します。

したがって、**match certificate コマンドを使用して、OCSP 証明書の検証に、ASA で別のトラストポイント（この例では OPENSSL）を強制的に使用する必要があります。**

ユーザ証明書は、最初に一致したトラストポイント（この例では WIN2012）に対して検証されます。これにより、OCSP レスポンダの検証用のデフォルト トラストポイントが決定されます。

match certificate コマンドで特定のトラストポイントを指定しない場合は、OCSP 証明書が、ユーザ証明書（この例では WIN2012）と同じトラストポイントに対して検証されます。

```
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
```

確認

ここでは、設定が正常に機能しているかどうかを確認します。

> **注：**特定のshowコマンドは、Output Interpreter Tool(登録ユーザ専用)でサポートされています。show コマンドの出力の分析を表示するには、Output Interpreter Tool を使用します。

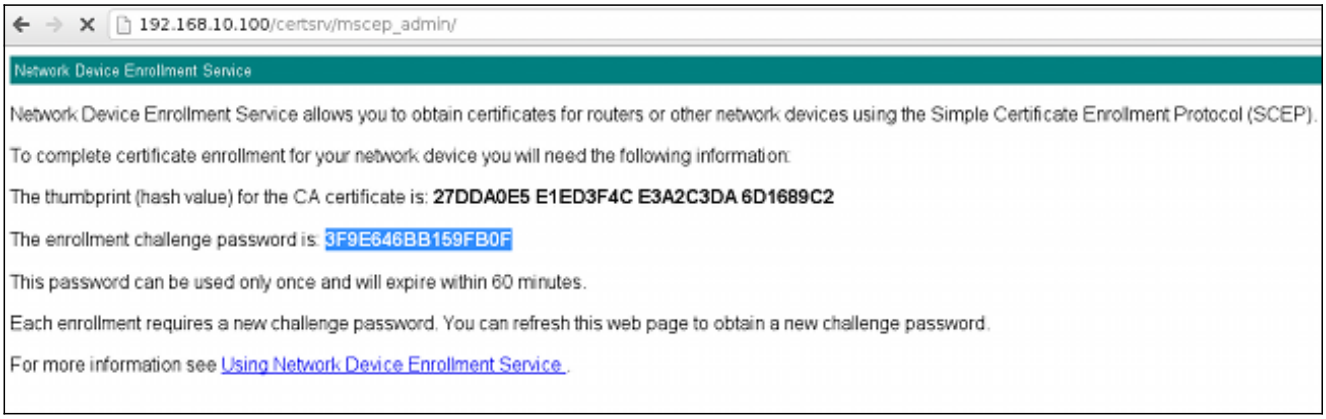
ASA:SCEP経由での証明書の取得

この手順では、SCEP を使用して証明書を取得する方法を説明しています。

1. 次に示すのは、CA 証明書を取得するためのトラストポイント認証プロセスです。

```
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. 証明書を要求するために ASA は、1 度だけ使用する SCEP パスワードを必要とします。これは、http://IP/certsrv/mscep_admin で管理コンソールから入手できます。



3. このパスワードを使用して、ASA で証明書を要求します。

```
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
```

一部の出力は、分かりやすくするために省略されています。

4. CA 証明書と ASA 証明書を両方とも確認します。

```
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
```

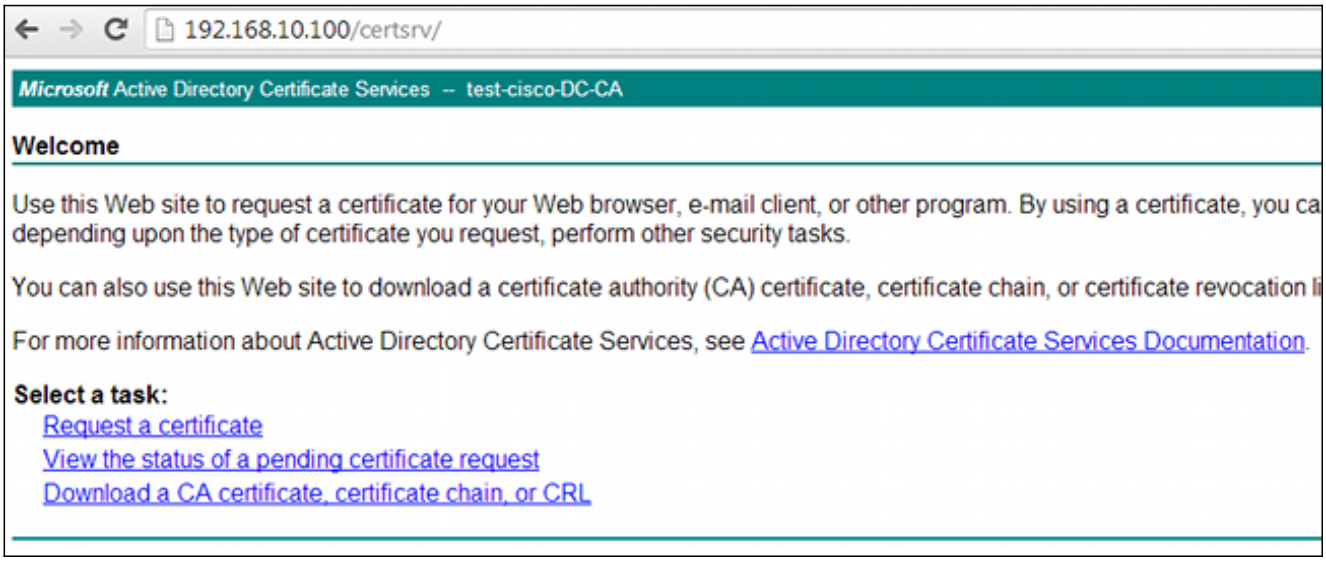
ASA では、証明書拡張のほとんどの部分が表示されません。ASA 証明書に「AIA の OCSP

URL」拡張が含まれる場合でも、ASA CLI には表示されません。Cisco Bug ID CSCui44335、「ASA ENH 証明書 x509 拡張が表示される」では、この機能拡張を依頼しています。

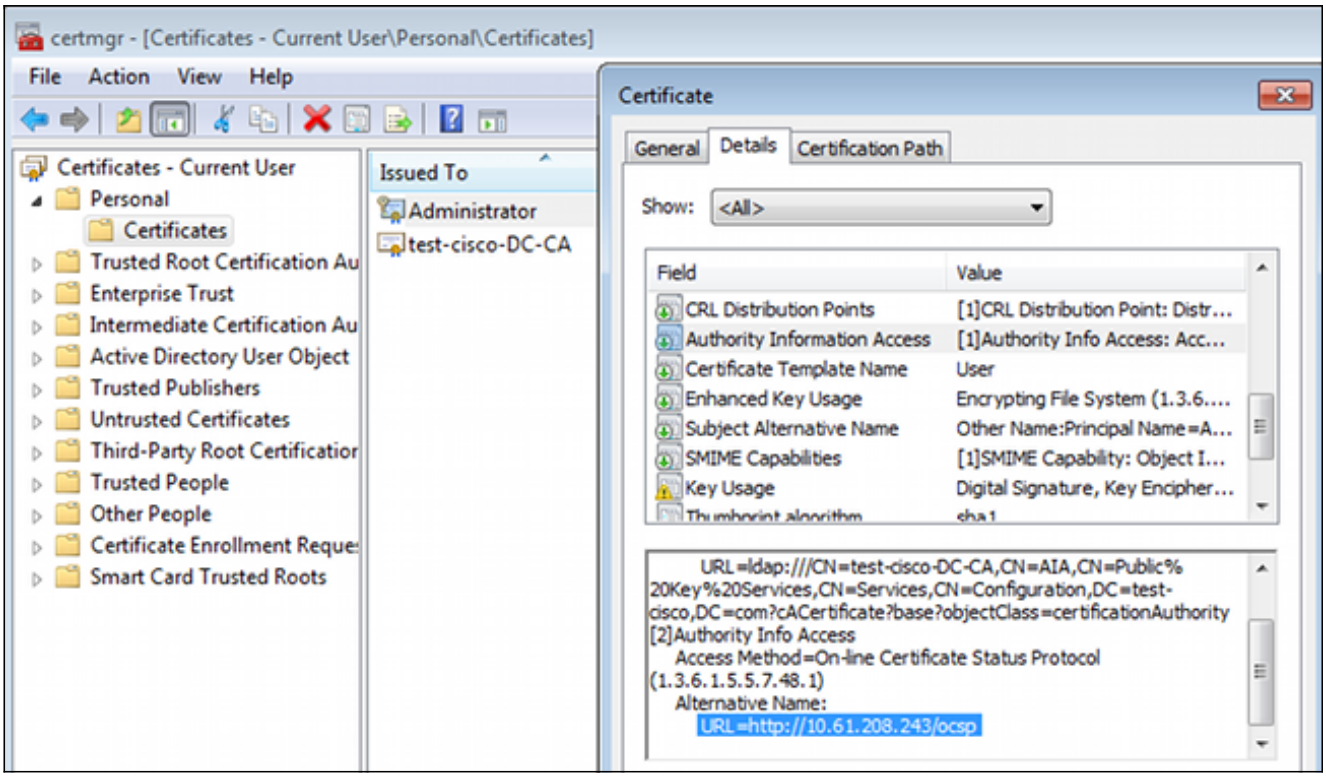
AnyConnect：Web ページによる証明書の取得

この手順では、クライアントの Web ブラウザを使用して証明書を取得する方法を説明しています。

1. AnyConnect ユーザ証明書は、Web ページを使用して要求できます。クライアント PC で Web ブラウザを使用して、http://*IP/certsrv にアクセスします。*



2. ユーザ証明書は、Web ブラウザのストアに保存した後、Microsoft ストアにエクスポートできます。この Microsoft ストアを AnyConnect が検索します。certmgr.msc を使用して、受け取った証明書を確認します。



正しい AnyConnect プロファイルがある場合は、AnyConnect も証明書を要求できます。

OCSP 検証による ASA VPN リモート アクセス

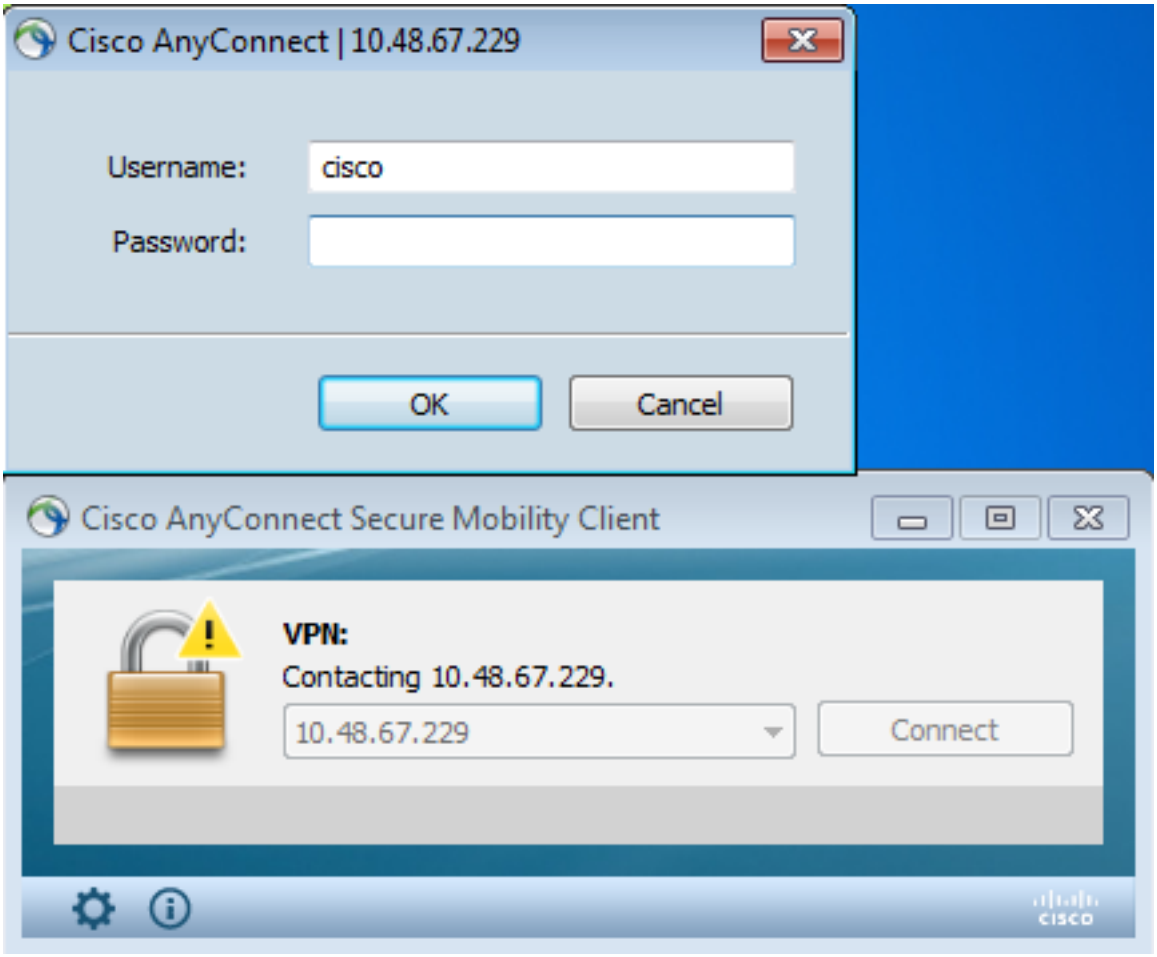
次の手順では、OCSP 検証のチェック方法について説明します。

1. 接続しようとするときに ASA は、証明書が OCSP に対してチェックされていることを報告します。この場合、OCSP 署名証明書にはチェックなし拡張があるため、OCSP によってチェックされていません。

```
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.
```

一部の出力は、分かりやすくするために省略されています。

2. エンド ユーザは、ユーザ クレデンシャルを入力します。



3. VPN のセッションは正常に終了します。

```
%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. セッションが作成されます。

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

Session Type: AnyConnect Detailed

Username     : cisco                  Index        : 4
Assigned IP  : 192.168.11.100         Public IP    : 10.61.209.83
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4
DTLS-Tunnel: (1)AES128
```

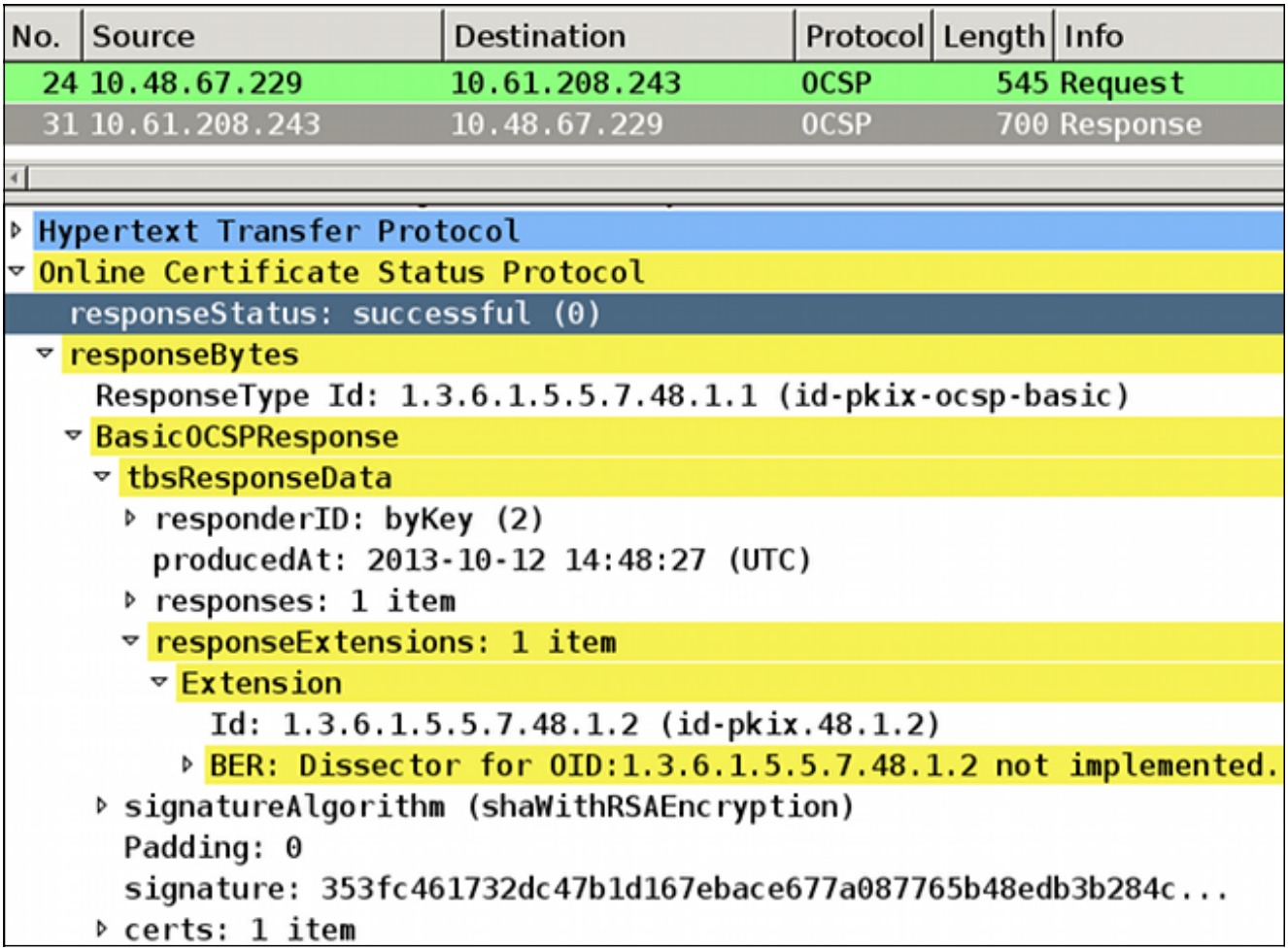
```
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1
DTLS-Tunnel: (1)SHA1
Bytes Tx     : 10540                 Bytes Rx     : 32236
Pkts Tx      : 8                     Pkts Rx      : 209
Pkts Tx Drop : 0                     Pkts Rx Drop : 0
Group Policy : MY                    Tunnel Group : RA
Login Time   : 11:30:31 CEST Sun Oct 13 2013
Duration     : 0h:01m:05s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                   VLAN         : none

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
 Tunnel ID    : 4.1
 Public IP    : 10.61.209.83
 Encryption   : none                  Hashing      : none
 TCP Src Port : 51401                 TCP Dst Port : 443
 Auth Mode    : Certificate and userPassword
 Idle Time Out: 30 Minutes            Idle TO Left : 29 Minutes
 Client OS    : Windows
 Client Type  : AnyConnect
 Client Ver   : Cisco AnyConnect VPN Agent for Windows 3.1.02040
 Bytes Tx     : 5270                  Bytes Rx     : 788
 Pkts Tx      : 4                     Pkts Rx      : 1
 Pkts Tx Drop : 0                     Pkts Rx Drop : 0

SSL-Tunnel:
 Tunnel ID    : 4.2
 Assigned IP  : 192.168.11.100        Public IP    : 10.61.209.83
 Encryption   : RC4                   Hashing      : SHA1
 Encapsulation: TLSv1.0               TCP Src Port : 51406
 TCP Dst Port : 443                   Auth Mode    : Certificate and
userPassword
 Idle Time Out: 30 Minutes            Idle TO Left : 29 Minutes
 Client OS    : Windows
 Client Type  : SSL VPN Client
 Client Ver   : Cisco AnyConnect VPN Agent for Windows 3.1.02040
 Bytes Tx     : 5270                  Bytes Rx     : 1995
 Pkts Tx      : 4                     Pkts Rx      : 10
 Pkts Tx Drop : 0                     Pkts Rx Drop : 0

DTLS-Tunnel:
 Tunnel ID    : 4.3
 Assigned IP  : 192.168.11.100        Public IP    : 10.61.209.83
 Encryption   : AES128                Hashing      : SHA1
 Encapsulation: DTLSv1.0              UDP Src Port : 58053
 UDP Dst Port : 443                   Auth Mode    : Certificate and
userPassword
 Idle Time Out: 30 Minutes            Idle TO Left : 29 Minutes
 Client OS    : Windows
 Client Type  : DTLS VPN Client
 Client Ver   : Cisco AnyConnect VPN Agent for Windows 3.1.02040
 Bytes Tx     : 0                     Bytes Rx     : 29664
 Pkts Tx      : 0                     Pkts Rx      : 201
 Pkts Tx Drop : 0                     Pkts Rx Drop : 0
```

5. OCSP 検証には、詳細なデバッグを使用できます。

```
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. パケット キャプチャ レベルでは、OCSP 要求および正しい OCSP 応答は、次のようになります。応答には、正しい署名が含まれており、Microsoft OCSP でナンス拡張が有効になっています。



複数の OCSP ソースによる ASA VPN リモート アクセス

「複数の OCSP ソースを含む ASA」で説明されているように一致証明書が設定されている場合は、それが優先されます。

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

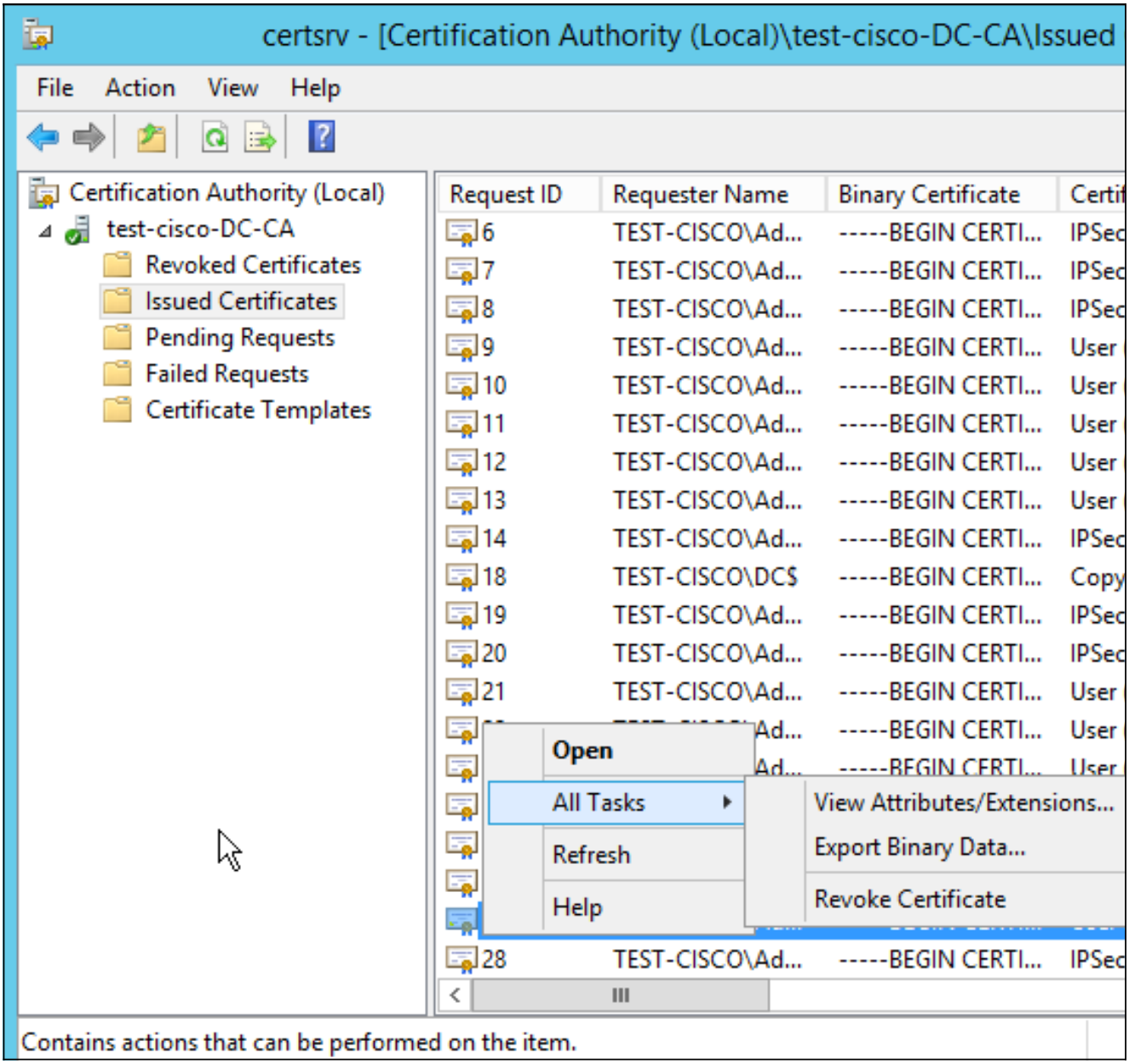
OCSP URL オーバーライドを使用した場合のデバッグは次のとおりです。

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

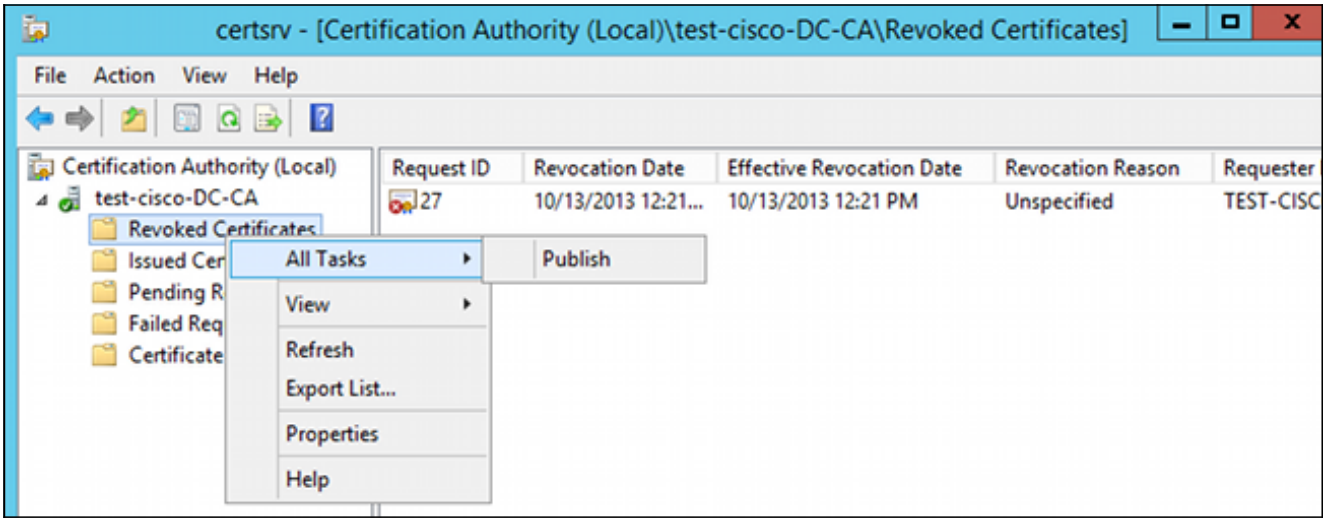
OCSP および無効な証明書による ASA VPN リモート アクセス

この手順では、証明書を無効化し、無効状態を確認する方法を説明します。

1. クライアント証明書を無効にします。



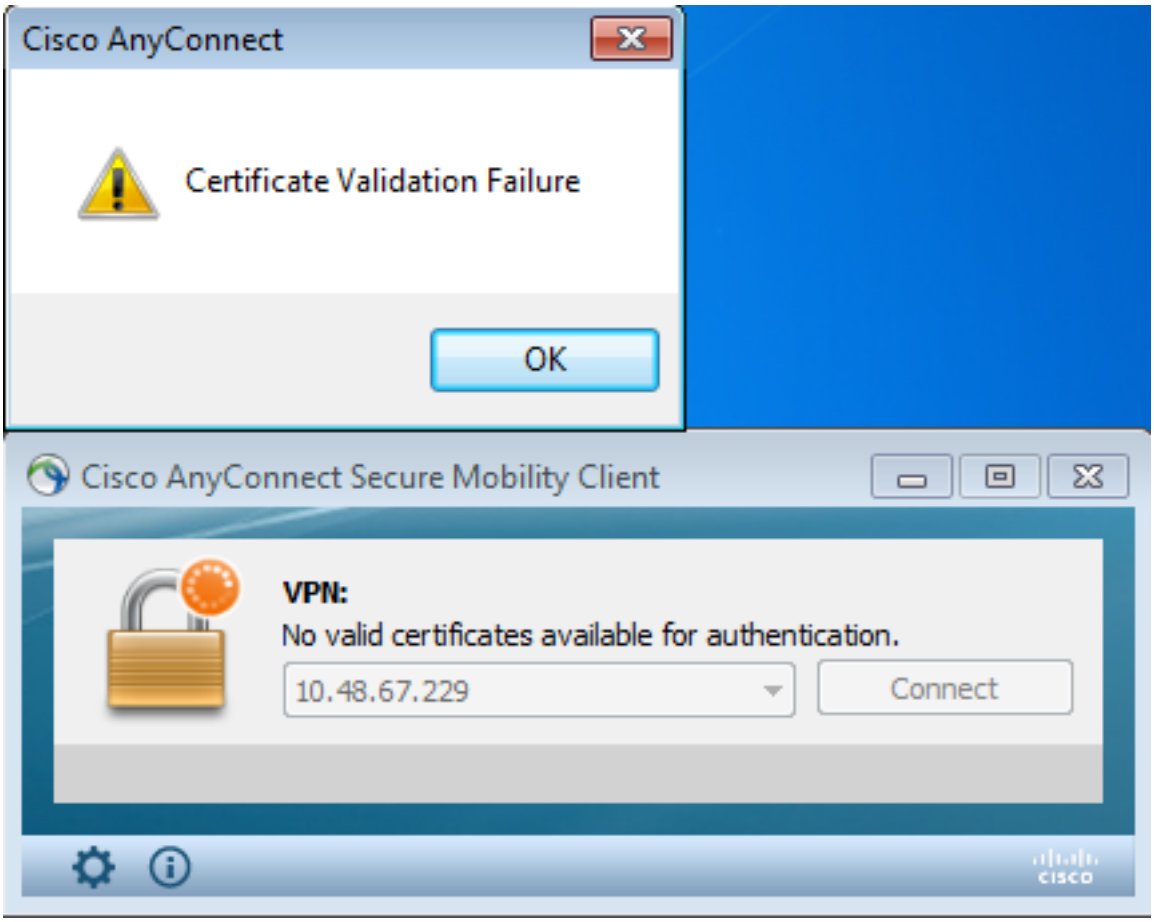
2. 結果を公開します。



3. （オプション）ステップ 1 と 2 は、Power Shell の certutil CLI ユーティリティで実行できます。

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

4. クライアントが接続しようとすると、証明書検証エラーが発生します。



5. AnyConnect ログも証明書検証エラーを示しています。

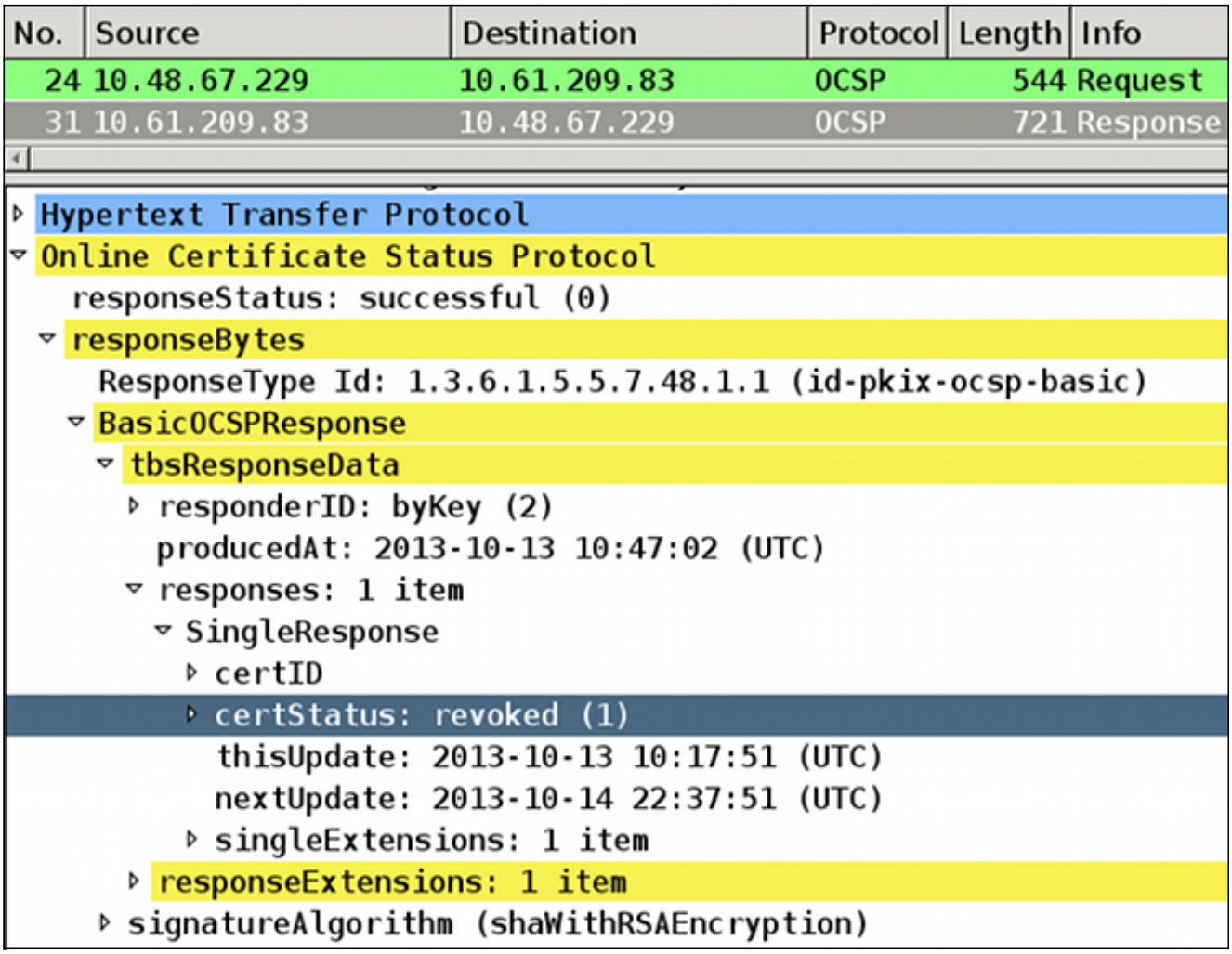
```
[2013-10-13 12:49:53] Contacting 10.48.67.229.
[2013-10-13 12:49:54] No valid certificates available for authentication.
[2013-10-13 12:49:55] Certificate Validation Failure
```

6. ASA は、証明書のステータスが「無効」であることを報告します。

```
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. パケット キャプチャは、証明書の「無効」ステータスを含む、正常な OCSP 応答を示しています。



トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

OCSP サーバのダウン

ASA は、OCSP サーバがダウンすると報告します。

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

パケット キャプチャもトラブルシューティングに役立ちます。

時間が同期されない

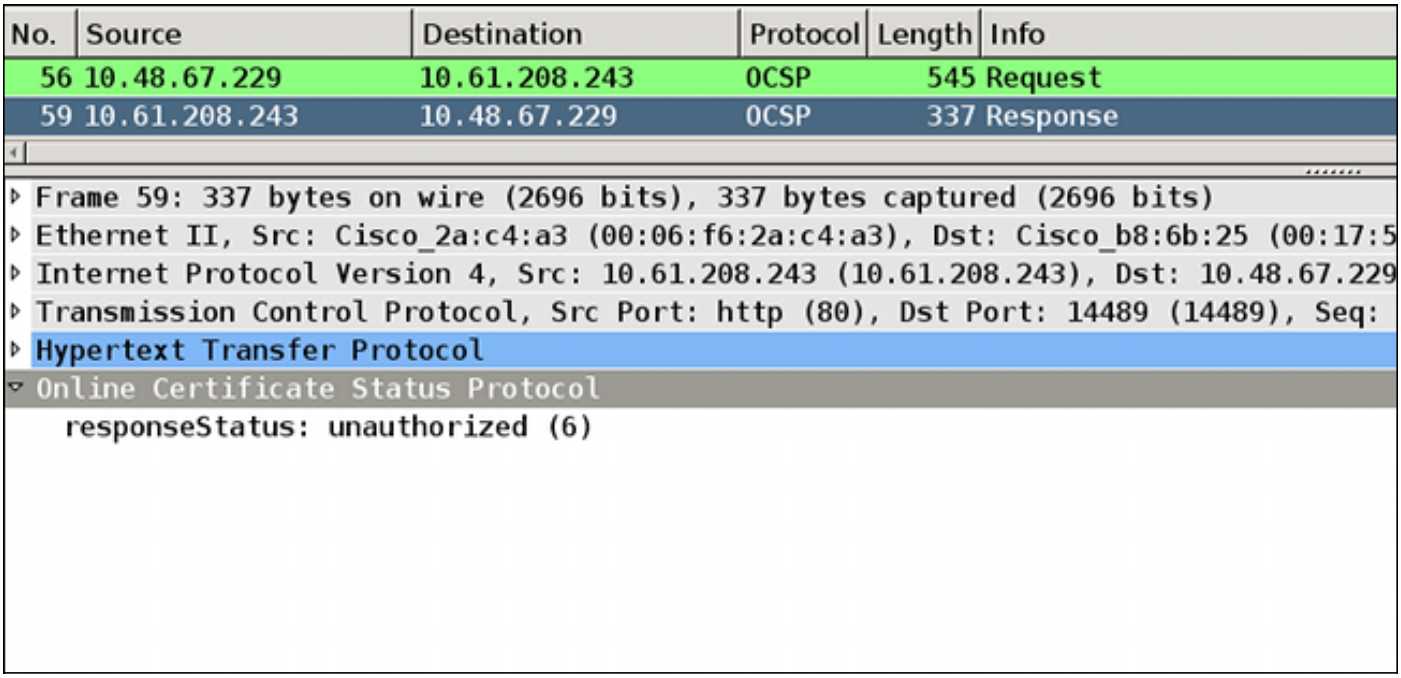
OCSP サーバの現在の時刻が ASA より古い（わずかな差は許容されます）場合は、OCSP サーバが不正な応答を送信し、ASA はそれを報告します。

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

ASA が、将来の時刻から OCSP 応答を受信した場合も、エラーが発生します。

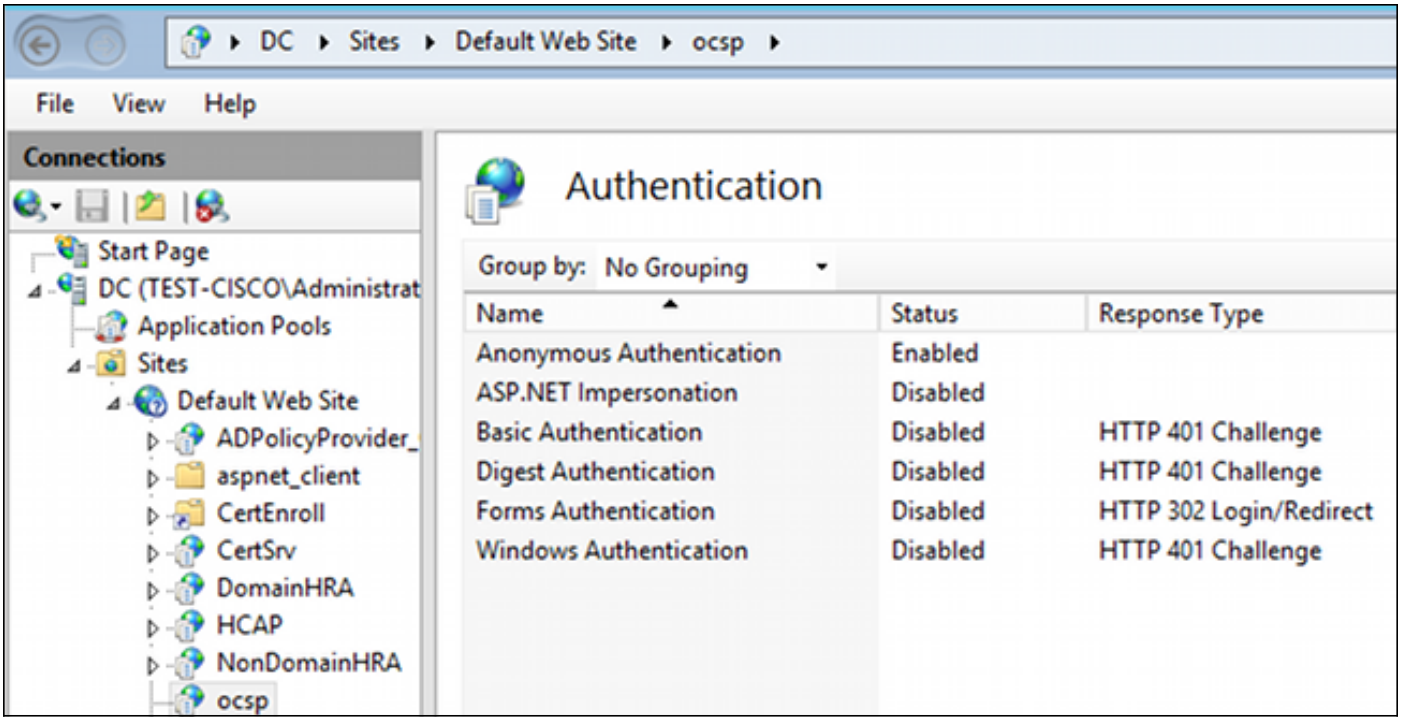
サポートされていない署名済みナンス

サーバのナンスがサポートされていない（Microsoft Windows 2012 R2 でのデフォルト）場合は、不正な応答が返されます。



IIS7 サーバ認証

SCEP/OCSP 要求での問題は、多くの場合、Internet Information Services 7（IIS7）での不正な認証により発生しています。匿名アクセスが設定されていることを確認してください。



関連情報

- Microsoft TechNet：オンラインレスポンダのインストール、設定、およびトラブルシューティングガイド
- Microsoft TechNet:OCSPレスポンダをサポートするためのCAの設定
- Cisco ASA シリーズ コマンド リファレンス
- テクニカル サポートとドキュメント – Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。