

Esempio di autenticazione IPsec di ASA/PIX 8.x e client VPN con certificati digitali con configurazione CA Microsoft

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Prodotti correlati](#)

[Convenzioni](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Configurazione ASA](#)

[Riepilogo della configurazione dell'ASA](#)

[Configurazione client VPN](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

[Introduzione](#)

In questo documento viene descritto come installare manualmente un certificato digitale di un fornitore terzo su Cisco Security Appliance (ASA/PIX) 8.x e sui client VPN per autenticare i peer IPsec sul server Microsoft Certificate Authority (CA).

[Prerequisiti](#)

[Requisiti](#)

Per questo documento è necessario disporre dell'accesso a un'autorità di certificazione per la registrazione dei certificati. I fornitori di CA di terze parti supportati sono Baltimore, Cisco, Entrust, iPlanet/Netscape, Microsoft, RSA e VeriSign.

in questo documento si presume che non vi sia una configurazione VPN preesistente nell'appliance ASA/PIX.

Nota: in questo documento viene utilizzato un server Microsoft Windows 2003 come server CA per lo scenario.

Nota: per informazioni complete su come configurare un server Windows 2003 come CA, fare riferimento a [Configurazione della CA sul server Windows](#).

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- ASA 5510 con software versione 8.0(2) e ASDM versione 6.0(2)
- Client VPN con software versione 4.x e successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

La configurazione ASA può essere utilizzata anche con i Cisco serie 500 PIX con software versione 8.x.

Convenzioni

Fare riferimento a [Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti](#).

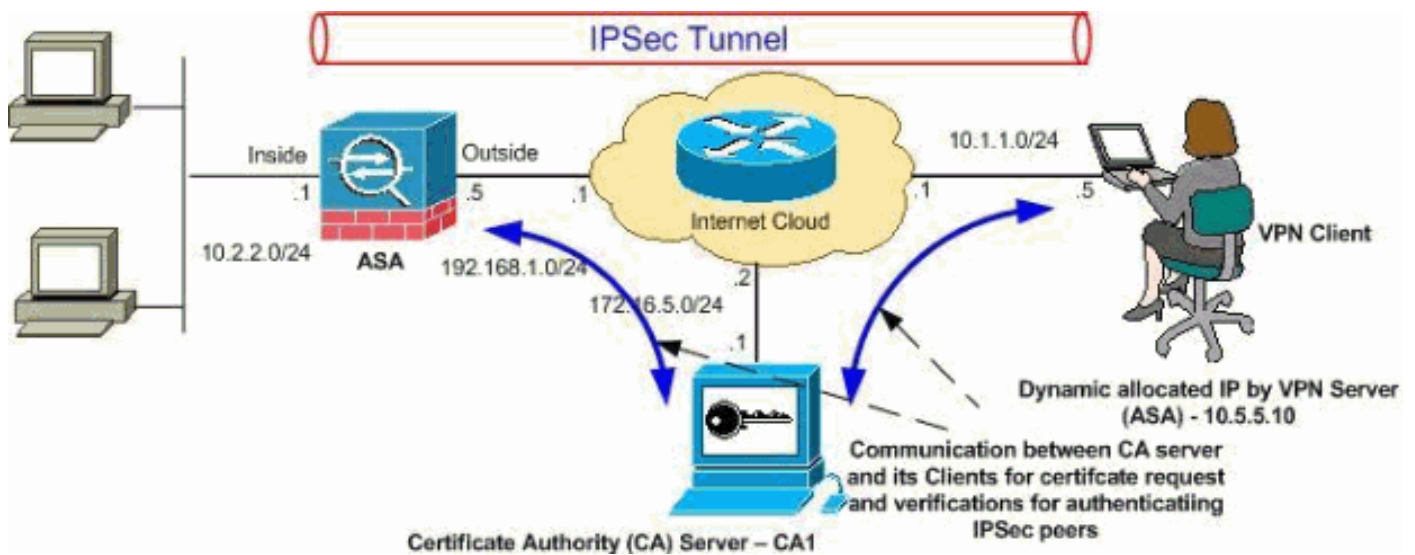
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo [strumento di ricerca](#) dei comandi (solo utenti [registrati](#)).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Nota: gli schemi di indirizzamento IP utilizzati in questa configurazione non sono legalmente instradabili su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

Configurazioni

Nel documento vengono usate queste configurazioni:

- [Configurazione ASA](#)
- [Riepilogo della configurazione dell'ASA](#)
- [Configurazione client VPN](#)

Configurazione ASA

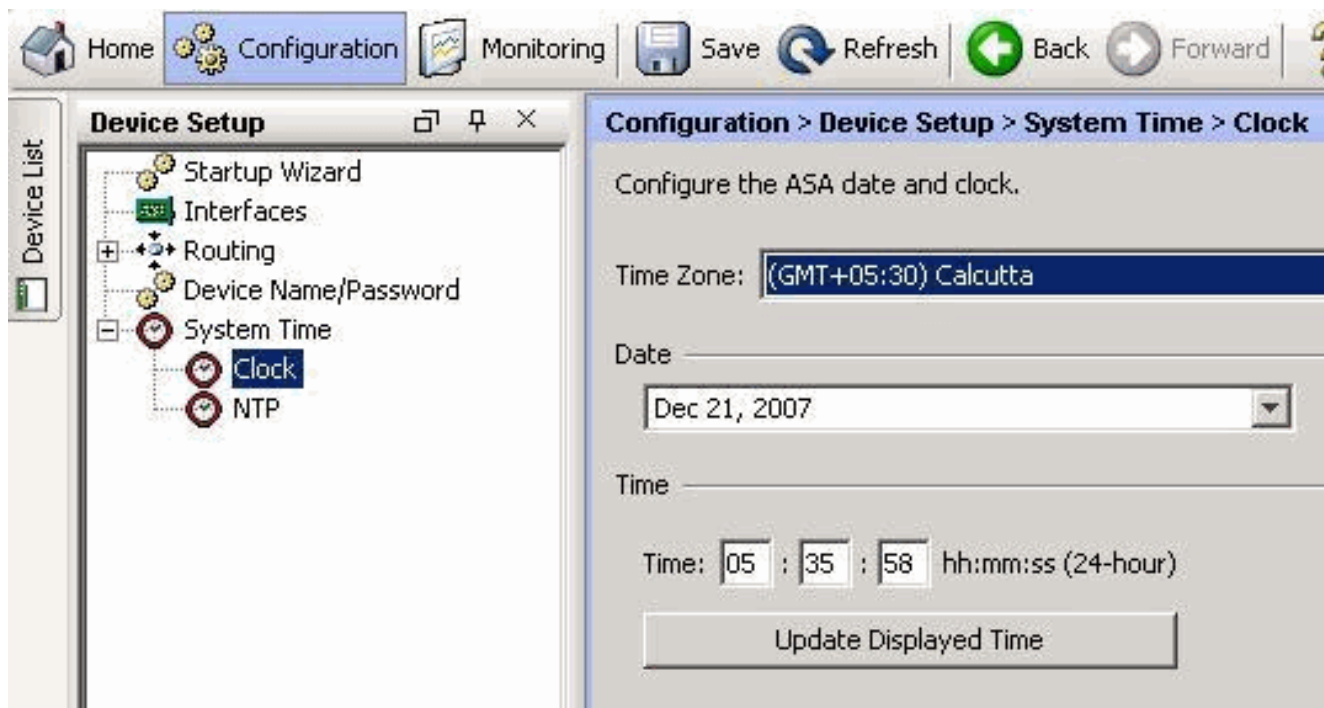
Per installare un certificato digitale di un altro fornitore sull'appliance ASA, attenersi alla seguente procedura:

- [Passaggio 1. Verificare che i valori di Data, Ora e Fuso orario siano accurati](#)
- [Passaggio 2. Generare una richiesta di firma del certificato](#)
- [Passaggio 3. Autenticazione del trust point](#)
- [Passaggio 4. Installare il certificato](#)
- [Passaggio 5. Configurare la VPN di accesso remoto \(IPsec\) per l'utilizzo del nuovo certificato installato](#)

Passaggio 1. Verificare che i valori di Data, Ora e Fuso orario siano accurati

Procedura ASDM

1. Fare clic su **Configurazione** e quindi su **Configurazione dispositivo**.
2. Espandere **Ora di sistema** e scegliere **Orologio**.
3. Verificare che le informazioni elencate siano corrette. I valori di Data, Ora e Fuso orario devono essere accurati per consentire la corretta convalida del certificato.



Esempio della riga di comando

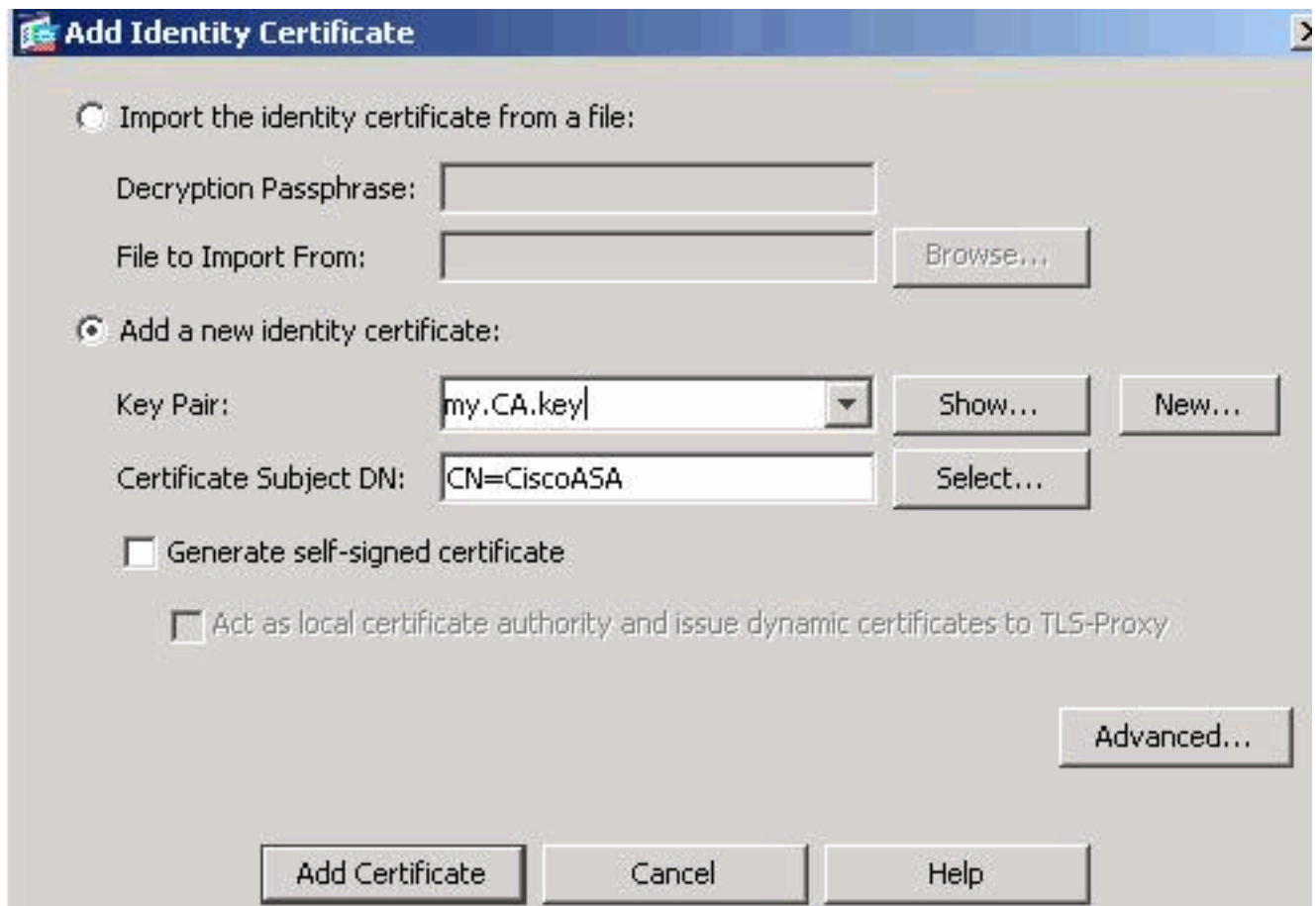
Cisco ASA
<pre>CiscoASA#show clock 05:37:37.904 UTC Fri Dec 21 2007</pre>

[Passaggio 2. Generare una richiesta di firma del certificato](#)

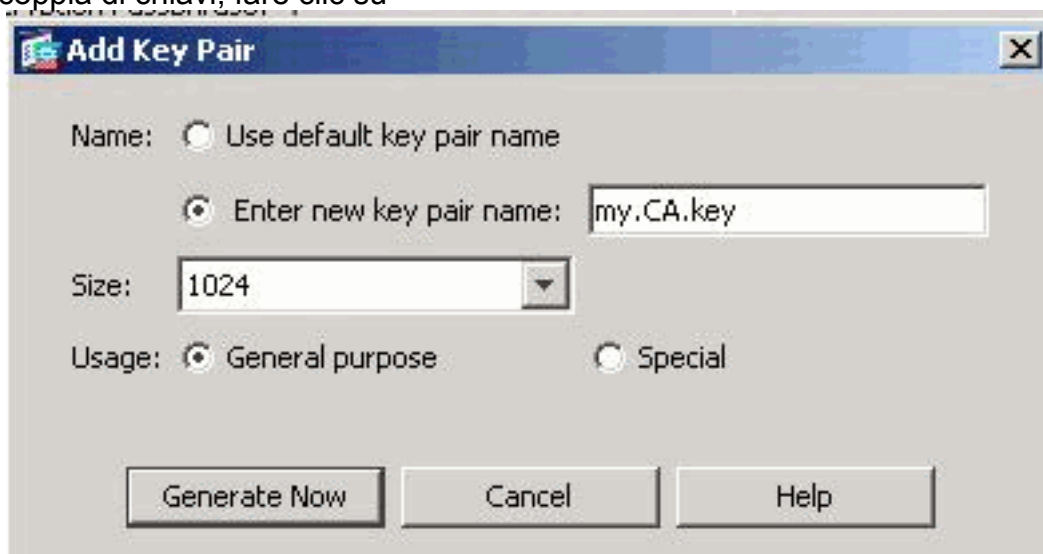
È necessaria una richiesta di firma del certificato (CSR) affinché l'autorità di certificazione di terze parti possa rilasciare un certificato di identità. Il CSR contiene la stringa del nome distinto (DN) dell'ASA e la chiave pubblica generata dall'ASA. L'ASA utilizza la chiave privata generata per firmare digitalmente il CSR.

Procedura ASDM

1. Fare clic su **Configurazione** e quindi su **Gestione dispositivi**.
2. Espandere **Gestione certificati** e scegliere **Certificati di identità**.
3. Fare clic su **Add**.

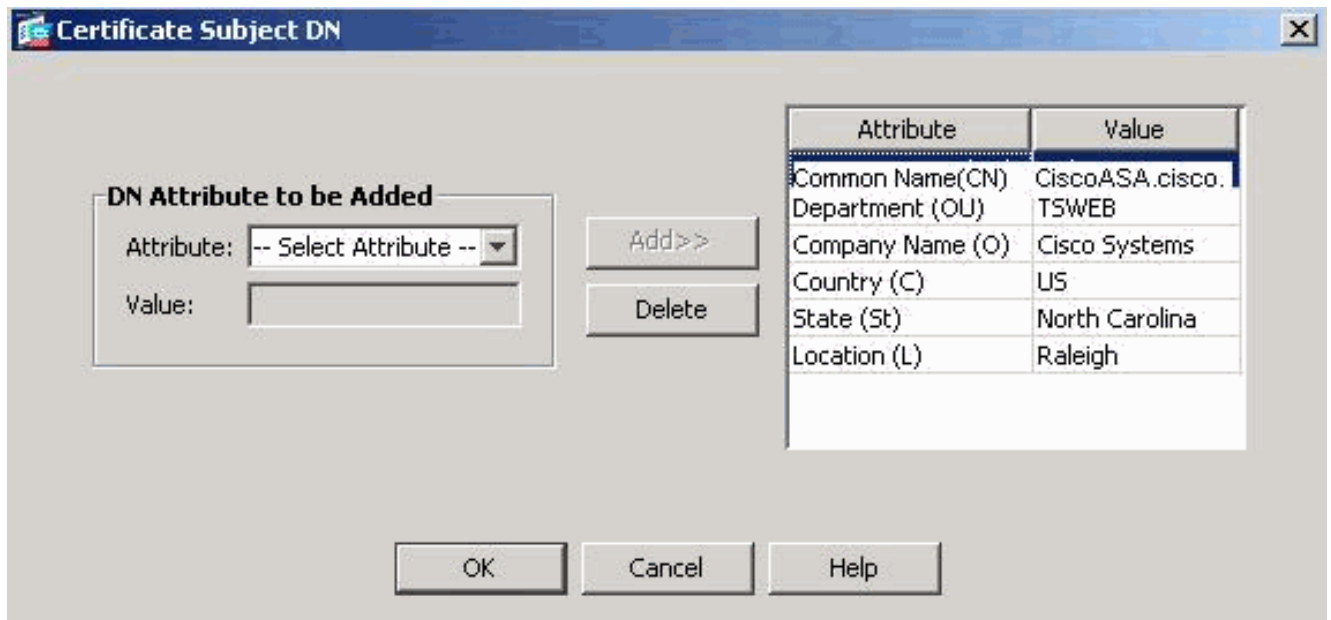


4. Fare clic sul pulsante di opzione **Aggiungi nuovo certificato di identità**.
5. Per la coppia di chiavi, fare clic su



Nuovo.

6. Fare clic sul pulsante di opzione **Immettere il nuovo nome della coppia di chiavi**. È necessario identificare chiaramente il nome della coppia di chiavi ai fini del riconoscimento.
7. Fare clic su **Genera**. È necessario creare la coppia di chiavi.
8. Per definire il DN del soggetto del certificato, fare clic su **Seleziona** e configurare gli attributi elencati nella tabella seguente: Per configurare questi valori, scegliere un valore dall'elenco a discesa Attributo, immettere il valore e fare clic su **Aggiungi**.

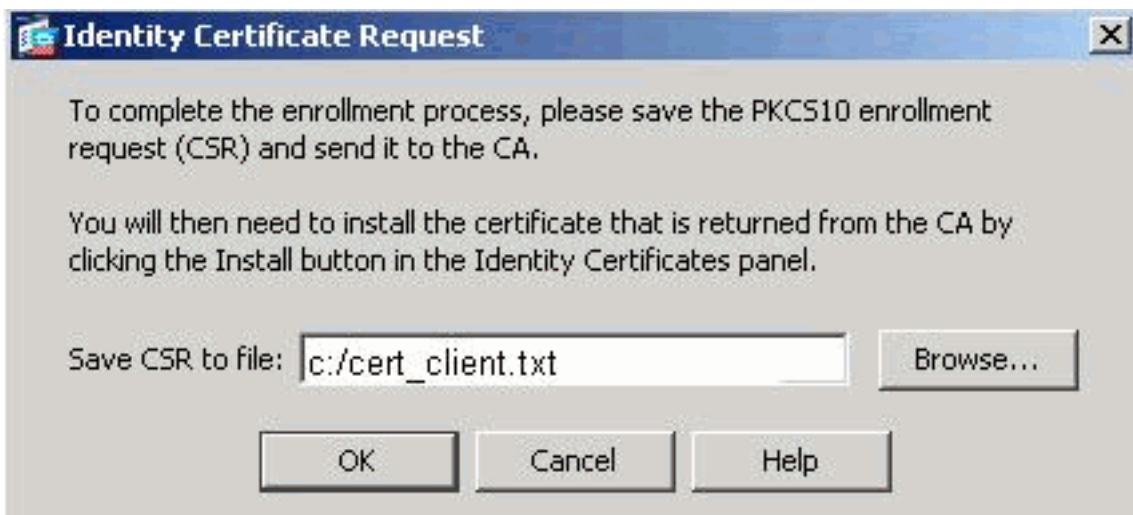


Nota: alcuni fornitori di terze parti richiedono l'inclusione di attributi specifici prima dell'emissione di un certificato di identità. Se non si è certi degli attributi richiesti, rivolgersi al fornitore per ulteriori informazioni.

9. Una volta aggiunti i valori appropriati, fare clic su **OK**. Verrà visualizzata la finestra di dialogo **Aggiungi certificato di identità** con il campo DN soggetto certificato compilato.
10. Fare clic su **Avanzate**.
11. Nel campo FQDN immettere il nome di dominio completo da utilizzare per accedere al dispositivo da Internet. Questo valore deve corrispondere al nome di dominio completo (FQDN) utilizzato per il nome comune (CN).

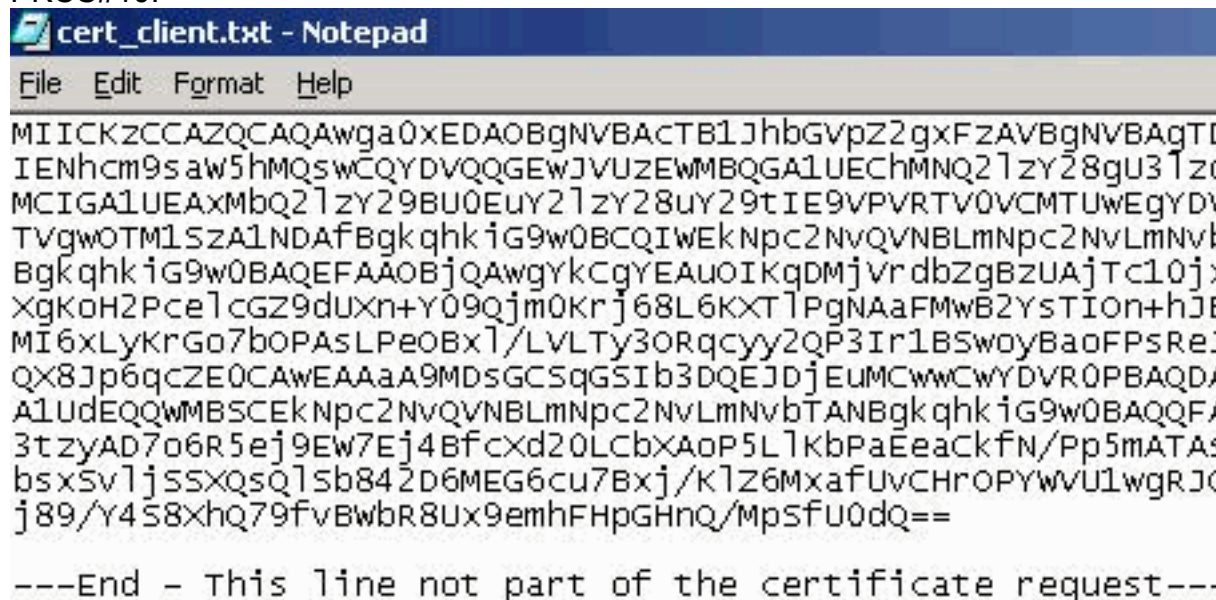


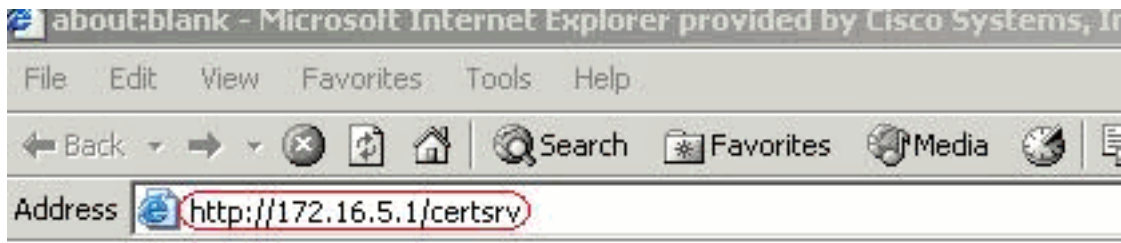
12. Fare clic su **OK** e quindi su **Aggiungi certificato**. Viene richiesto di salvare il CSR in un file sul computer



locale.

13. Fare clic su **Sfogli**a, scegliere il percorso in cui salvare il CSR e salvare il file con estensione .txt. **Nota:** quando si salva il file con estensione .txt, è possibile aprire il file con un editor di testo (ad esempio Blocco note) e visualizzare la richiesta PKCS#10.

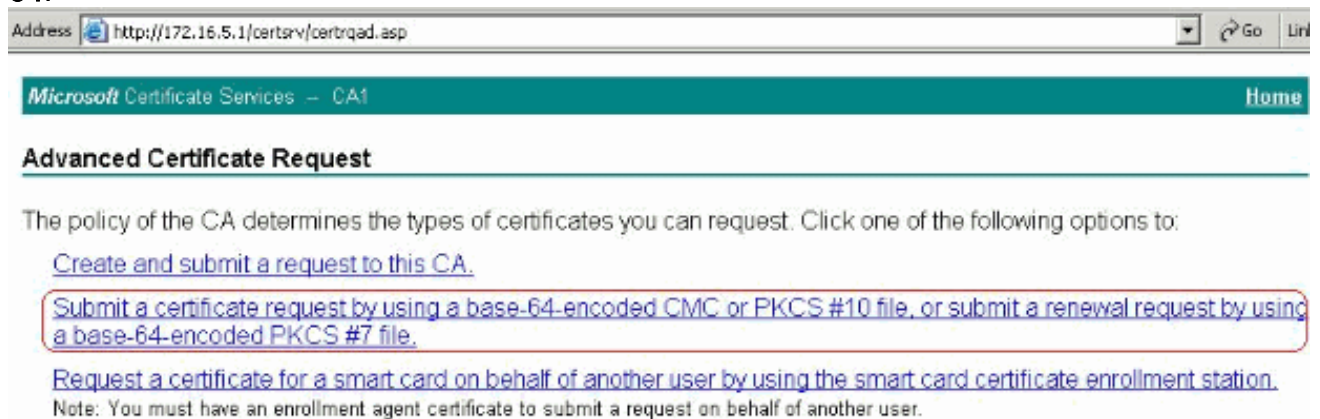


A screenshot of a Windows dialog box titled 'Enter Network Password'. It features a key icon and the text 'Please type your user name and password.' The 'Site:' field is set to '172.16.5.1'. The 'User Name' field contains 'vpnuser' and the 'Password' field contains 'xxxxxxxx'. The 'Domain' field is empty. There is a checkbox for 'Save this password in your password list' which is unchecked. 'OK' and 'Cancel' buttons are at the bottom. A red rectangular box highlights the 'User Name' and 'Password' input fields.

vpn.

Nota:

verificare di disporre di un account utente per l'appliance ASA (server vpn) con il server CA. Fare clic su **Richiedi un certificato > Richiesta avanzata di certificati** per selezionare **Invia una richiesta di certificato utilizzando un file CMC o PKCS#10 con codifica Base 64** oppure inviare una richiesta di rinnovo utilizzando un file PKCS#7 con codifica Base 64.



Copiare e incollare le informazioni codificate nella casella **Richiesta salvata** e quindi fare clic su

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded (source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
fvQVNBmNpc2NvLmNvbTANBgkqhkiG9wOBAQFAAQ  
4BfcXd2OLCbXAoP5L1KbPaEeaCkfN/Pp5mATAsG8  
D6MEG6cu7Bxj/K1Z6MxafUvCHROPYWVU1wgRjGh+  
t8Ux9emhFHpGHnQ/MpSfUOdQ==  
not part of the certificate request---
```

[Browse for a file to insert.](#)

Certificate Template:

IPSEC

Additional Attributes:

Attributes:

Submit >

Invia.

are clic sul pulsante di opzione **Codificato Base 64** e quindi su **Scarica**

Microsoft Certificate Services -- CA1

Certificate Issued

The certificate you requested was issued to you.

DER encoded or Base 64 encoded



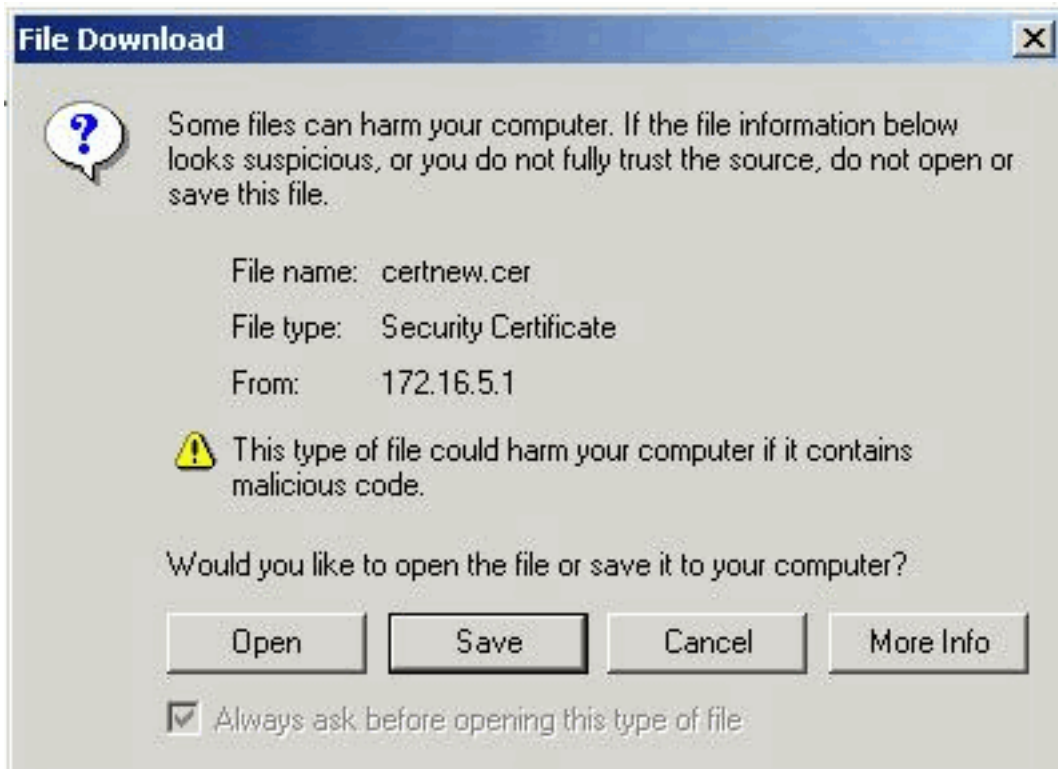
[Download certificate](#)

[Download certificate chain](#)

certificato.

visualizzata la finestra Download file. Salvarlo con il nome **cert_client_id.cer**, che è il certificato di identità da installare sull'appliance

Viene



ASA.

Esempio della riga di comando

```
Cisco ASA

CiscoASA# configure terminal

CiscoASA(config)#crypto key generate rsa label my.ca.key
modulus 1024

!--- Generates 1024 bit RSA key pair. "label" defines
the name of the Key Pair. INFO: The name for the keys
will be: my.CA.key Keypair generation process begin.
Please wait... ciscoasa(config)#crypto ca trustpoint CA1
ciscoasa(config-ca-trustpoint)# subject-name
CN=CiscoASA.cisco.com,OU=TSWEB,
                                O=Cisco
Systems,C=US,St=North Carolina,L=Raleigh

!--- Defines x.500 distinguished name. Use the
attributes defined in table as a guide. CiscoASA(config-
ca-trustpoint)#keypair my.CA.key

!--- Specifies key pair generated in Step 3
CiscoASA(config-ca-trustpoint)#fqdn CiscoASA.cisco.com

!--- Specifies the FQDN (DNS:) to be used as the subject
alternative name CiscoASA(config-ca-
trustpoint)#enrollment terminal

!--- Specifies manual enrollment. CiscoASA(config-ca-
trustpoint)#exit
CiscoASA(config)#crypto ca enroll CA1

!--- Initiates certificate signing request. This is the
request to be !--- submitted via Web or Email to the
third party vendor. % Start certificate enrollment .. %
The subject name in the certificate will be:
cn=CiscoASA.cisco.com OU=TSWEB, O=Cisco Systems,
```

```

C=US,St=North Carolina,L=Raleigh % The fully-qualified
domain name in the certificate will be:
CiscoASA.cisco.com % Include the device serial number in
the subject name? [yes/no]: no
!--- Do not include the device's serial number in the
subject. Display Certificate Request to terminal?
[yes/no]: y
!--- Displays the PKCS#10 enrollment request to the
terminal. You will need to !--- copy this from the
terminal to a text file or web text field to submit to
!--- the third party CA. Certificate Request follows:
MIICKzCCAQQCAQAwga0xEDAObgNVBAcTB1JhbGVpZ2gxZzAVBgNVBAgT
Dk5vcnRo
IENhcm9saW5hMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ21zY28gU31z
dGVtczEk
MCIGA1UEAxMbQ21zY29BU0EuY21zY28uY29tIE9VPVRTV0VCMTUwEgYD
VQQFEwtK
TVgwOTM1SzA1NDafBgkqhkiG9w0BCQIWEkNpc2NvQVNBLmNpc2NvLmNv
bTCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwGyKCGYEAuOIKqDMjVrdbZgBzUAjTc10j
xSlbkkr
XgKoH2PcelcGZ9dUXn+Y09Qjm0Krj68L6KXTlPgNAaFMwB2YsTIOh+hJ
BVq5Sxjv
MI6xLyKrGo7bOPAsLPeOBxl/LVLTy3ORqcy2QP3Ir1BSwoyBaoFPsRe
JGSAYG+O
QX8Jp6qcZE0CAwEAAaA9MDsGCSqGSIb3DQEJJDjEuMCwwCwYDVR0PBAQD
AgWgMB0G
A1UdEQQWMBSEkNpc2NvQVNBLmNpc2NvLmNvbTANBgkqhkiG9w0BAQQF
AAOBgQBM
3tzyAD7o6R5ej9EW7Ej4BfcXd20LCbXAoP5LlKbPaEaCkfn/Pp5mATA
sG832TBm
bsxSvljSSXQsQ1Sb842D6MEG6cu7Bxj/KlZ6MxafUvCHROPYWVU1wgrJ
Gh+ndCZK j89/Y4S8XhQ79fvBwR8Ux9emhFHpGHnQ/MpSfU0dQ== --
--End - This line not part of the certificate request---
Redisplay enrollment request? [yes/no]: n
CiscoASA(config)#

```

[Passaggio 3. Autenticazione del trust point](#)

Una volta ricevuto il certificato di identità dal fornitore di terze parti, è possibile procedere con questo passaggio.

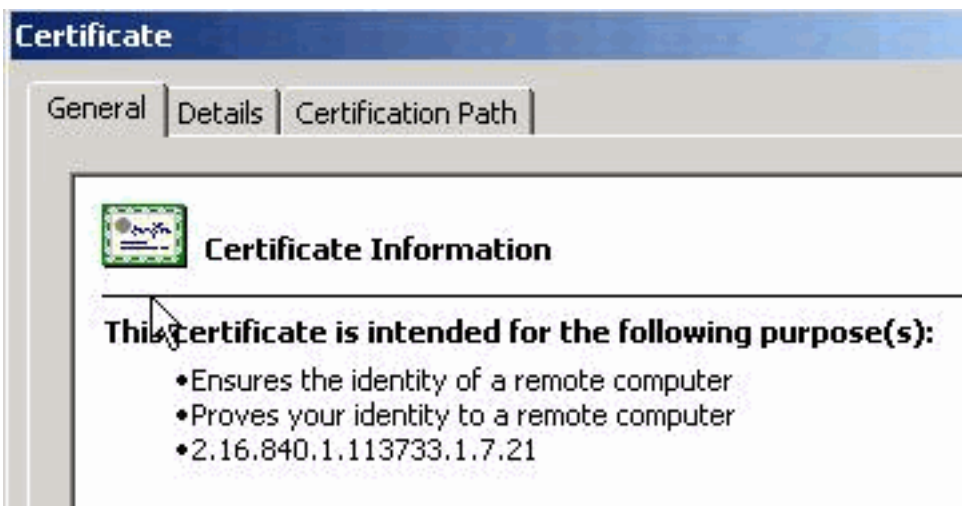
Procedura ASDM

1. Salvare il certificato di identità nel computer locale.
2. Se è stato fornito un certificato con codifica base64 non fornito come file, è necessario copiare il messaggio base64 e incollarlo in un file di testo.
3. Rinominare il file con estensione cer **Nota:** una volta rinominato il file con l'estensione cer,



l'icona del file viene visualizzata come un certificato, come illustrato.

4. Fare doppio clic sul file del



certificato.

Nota: se

Windows non dispone di informazioni sufficienti per verificare che questo messaggio di certificato venga visualizzato nella scheda Generale, è necessario ottenere il certificato CA radice o CA intermedia del fornitore di terze parti prima di continuare con questa procedura. Contattare il fornitore di terze parti o l'amministratore della CA per ottenere la CA radice o il certificato della CA intermedia di emissione.

5. Fare clic sulla scheda **Percorso certificato**.

6. Fare clic sul certificato CA associato al certificato di identità rilasciato e quindi su **Visualizza**



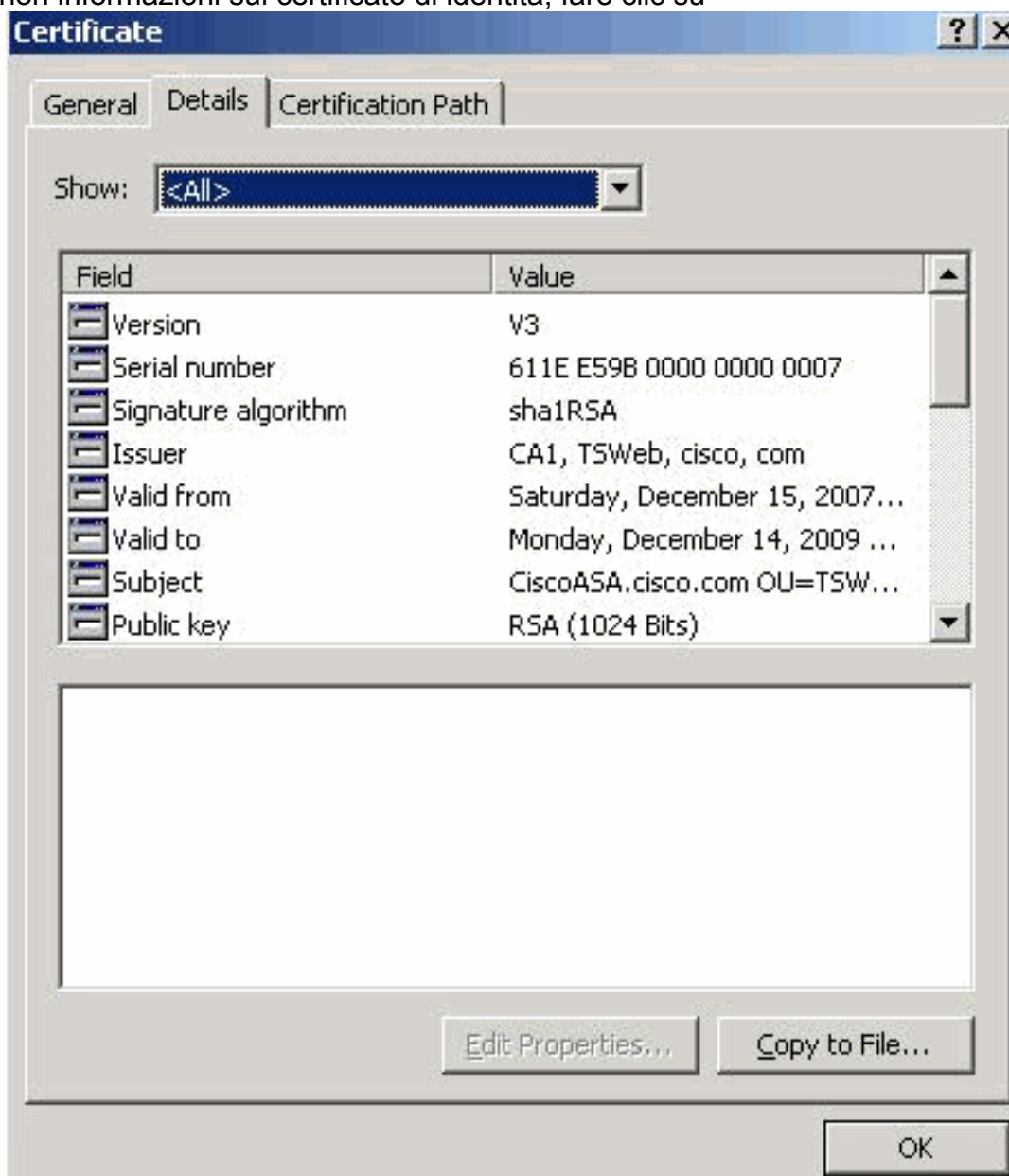
certificato.

OK

Verrann

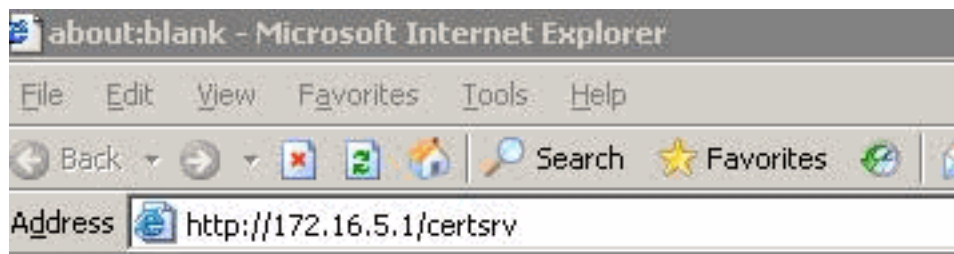
o visualizzate informazioni dettagliate sul certificato CA.

7. Per ulteriori informazioni sul certificato di identità, fare clic su



Dettagli.

8. Prima di installare il certificato di identità, è necessario scaricarlo dal server CA e installarlo nell'appliance ASA, come mostrato. Completare questa procedura per scaricare il certificato CA dal server CA denominato **CA1**. Eseguire l'accesso Web al server CA 172.16.5.1 con l'aiuto delle credenziali fornite al server



VPN.

Fare clic su **Scarica**

un certificato CA, una catena di certificati o un CRL per aprire la finestra, come illustrato.

Fare clic sul pulsante di scelta **Base 64** come metodo di codifica, quindi fare clic su **Scarica**

certificato

CA.

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA cert](#)

To download a CA certificate, certificate chain, or CRL, select the certificate

CA certificate:



Encoding method:

- DER
- Base 64

[Download CA certificate](#)

[Download CA certificate chain](#)

[Download latest base CRL](#)

[Download latest delta CRL](#)

Salvare il certificato CA con il nome **certnew.cer** nel

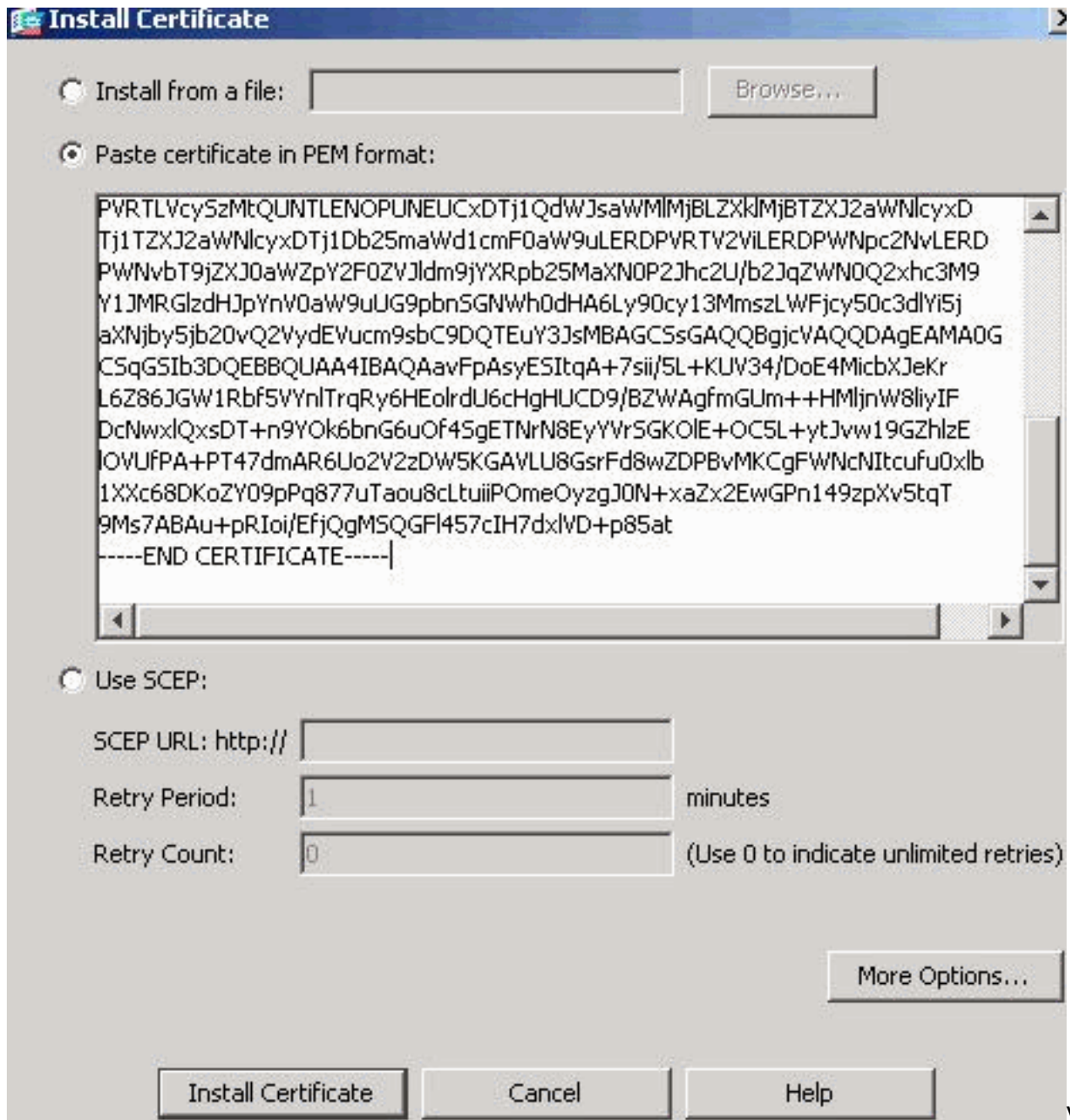


computer.

9. Selezionare il percorso in cui è stato salvato il certificato CA.
10. Aprire il file con un editor di testo, ad esempio Blocco note. Fare clic con il pulsante destro del mouse sul file e scegliere **Invia a > Blocco note**.
11. Viene visualizzato il messaggio con codifica base64 simile al certificato in questa immagine:

```
-----BEGIN CERTIFICATE-----
MIIEHTCCA4wgAwIBAgIQcJnxmUdk4JxGudqAowt0nDANBgkqhkiG9w0BAQUFADBBR
MRMwEQYKZCZImiZPyLQBGGRYDY29tMRUwEwYKZCZImiZPyLQBGGRYFY2IzY28xFTAT
BgoJkiajk/IsZAEZFGVUU1dIYjEMMAoGA1UEAxMDQ0ExMB4XDTA3MTIXNDA2MDE0
Ml0XDTEyMTIXNDA2MTAxNVowUTETMBEGCgmsJomT8ixkARKWA2NvbTEVMBMGCgms
JomT8ixkARKwBWNpc2NvMRUwEwYKZCZImiZPyLQBGGRYFVFNXZWIxDDAKBgnVBAMT
A0NBMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAAOqP7seuvvyiLmA9
BSGZMz3sctR9TCMwOx7qM8mmiD0o7OkGApAvmtHrK431iMuaeKBpo5Zd4TNgntjX
bt6czaHpBuyIsyoZ0OU1PmwAMuIMAD+mL9IqTbndosJfy7Yhh2vweMijcQnwdOq+
Kx+swaenCjslrxeuaHpIBTuaNOckueBUBjxgpJUNPAk1G8YwBfaTV4M7kZf4dbQI
y3GoFGmh8zGx6ys1DEaUQXRvwhdbMivwqYBXWkh4uc04xxQmr//Sct1tdwQcvk2V
uBwCsptw7C1akTqfm5XK/d//z2euuxrHYysQCfoFyk1vE6/qlo+fQessz+Tldhxx
wPXRO18CAwEAAaOCaw8wgGFRMBMGCSSGAQQBgjCUAgQHggQAQwBBMASGA1UddwQE
AwIBhjAPBgnVHRMBAF8EBTADAQH/MB0GA1UdDgQWBBTZrb8I8jqI8RRDL3myfNQJ
pAPlwDCCAQMGA1UdHwSB+zCB+DCB9aCB8qCB74aBtwxkYXA6Ly8vQ049Q0ExLENO
PVRTLvcyszmtQUNTLENOPUNEUCxDTj1QdwJsawMlMjBLZXk1MjBTZXJ2awNlcYxD
Tj1TZXJ2awNlcYxDTj1Db25mawd1cmF0aw9uLERDPVRTV2ViLERDPWNpc2NvLERD
PWNvbT9jZXJ0awZpY2F0ZVJ1dm9jYXRpb25maxN0P2Jhc2U/b2JqZWNOQ2xhc3M9
Y1JMRG1zdHJpYnV0aw9uUG9pbnsGNWh0dHA6Ly90cy13MmszLWFjcy50c3dlYi5j
aXNjby5jb20vQ2vydEVucm9sbc9DQTEuY3JsMBAGCSsGAQQBgjcvAQQDAgEAMA0G
CSqGSIb3DQEBBQUAA4IBAQAavFpAsyESItqa+7sii/5L+KUV34/DoE4MibXJekr
L6Z86JGw1Rbf5vynlTrqRy6HEo1rdU6cHgHUCD9/BZWagfmGUM++HMLjnw8liyIF
DcnwxlQxsDT+n9Yok6bnG6uof4SgETNrN8EyyVrSGK0lE+OC5L+ytJvw19Gzh1ze
lOVUFPA+PT47dmAR6Uo2V2ZDW5KGAVLU8GsrFd8wZDPBVMKCGFWNCNItcufu0x1b
1XXc68DKoZY09pPq877uTaou8cLtuipPomeOyzgJ0N+xaZx2EwGPn149zpxv5tqt
9Ms7ABAU+pRIoi/EfjQgMSQGF1457cIH7dx1VD+p85at
-----END CERTIFICATE-----
```

12. In ASDM, fare clic su **Configurazione**, quindi su **Gestione dispositivi**.
13. Espandere **Gestione certificati** e scegliere **Certificati CA**.
14. Fare clic su **Add**.
15. Fare clic sul pulsante di scelta **Incolla certificato in formato PEM** e incollare nel campo di testo il certificato CA base64 fornito dal fornitore di terze parti.
16. Fare clic su **Installa certificato**.



Vie

ne visualizzata una finestra di dialogo che conferma il completamento dell'installazione.

Esempio della riga di comando

```

Cisco ASA
CiscoASA(config)#crypto ca authenticate CA1
!--- Initiates the prompt for paste-in of base64 CA
intermediate certificate. ! This should be provided by
the third party vendor. Enter the base 64 encoded CA
certificate. End with the word "quit" on a line by
itself -----BEGIN CERTIFICATE-----
MIIE nTCCA4WgAwIBAgIQcJnxmUdk4JxGUdqAoWt0nDANBgkqhkiG9w0B
AQUFADBR
MRMwEQYKCZImiZPyLQG BGRYDY29tMRUwEwYKCZImiZPyLQG BGRYFY21z
Y28xFTAT
BgoJkiaJk/IsZAEZFgVUU1d1YjEMMAoGA1UEAxMDQ0E xMB4XDTA3MTIx
NDA2MDE0
M1oXDTEyMTIxNDA2MTA xNVowUTETMBEGCgmSJomT8ixkARkWA2NvbTEV
MBMGCgmS
JomT8ixkARkWBWNpc2NvMRUwEwYKCZImiZPyLQG BGRYFVFNXZWI xDDAK

```

```

BgNVBAMT
A0NBMTCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOqP7seu
VvyiLmA9
BSGzMz3sCtR9TCMWOx7qM8mmiD0o7OkGAPAvmtHrK431iMuaeKBpo5Zd
4TNgNtjX
bt6czaHpBuyIsyoZ0OU1PmwAMuiMAD+mL9IqTbndosJfy7Yhh2vWeMij
cQnwdOq+
Kx+sWaeNCjs1rxeuAhpIBTuaNOckueBUBjxgPJUNPAk1G8YwBfaTV4M7
kZf4dbQI
y3GoFGmh8zGx6ys1DEaUQxRVwhDbMIvwqYBXWKh4uC04xxQmr//Sct1t
dWQcvk2V
uBwCsptW7C1akTqfm5XK/d//z2eUuXrHYySQcfoFyk1vE6/Q1o+fQeSS
z+TlDhXx
wPXRO18CAwEAAaOCAW8wggFrMBMGCSsGAQQBgjcUAQOQHGAQwBBMAsg
A1UdDwQE
AwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBbTzrb8I8jqI8RRD
L3mYfnQJ
pAP1WDCCAQMGA1UdHwSB+zCB+DCB9aCB8qCB74aBtWxkYXA6Ly8vQ049
Q0ExLENO
PVRTLVcySzMtQUNTLENOPUNEUCxDTj1QdWJsaWMM1mJBLZXk1mJBTZXJ2
aWN1cyxD
Tj1TZXJ2aWN1cyxDTj1Db25maWd1cmF0aW9uLERDPVRTV2ViLERDPWNp
c2NvLERD
PWNvbT9jZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWNO
Q2xhc3M9
Y1JMRG1zdHJpYnV0aW9uUG9pbnsGNWh0dHA6Ly90cy13MmszLWFwcy50
c3dlYi5j
aXNjby5jb20vQ2VydeVucm9sbC9DQTEuY3JsMBAGCSsGAQQBgjcVAQOD
AgEAMA0G
CSqGSIb3DQEBBQUAA4IBAQAavFpAsyESItqA+7sii/5L+KUV34/DoE4M
icbXJeKr
L6Z86JGW1Rbf5VYnlTrqRy6HEolrdU6cHgHUCD9/BZWAghmGUm++HM1j
nW8liYIF
DcNwxlQxsDT+n9YOk6bnG6uOf4SgETNrN8EyYVrSGKOLE+OC5L+ytJvw
19GZhlzE
lOVUfPA+PT47dmAR6Uo2V2zDW5KGAVLU8GsrFd8wZDPBvMKCGFWNcNIt
cufu0x1b
1XXc68DKoZY09pPq877uTaou8cLtuuiPomeOyZgJ0N+xaZx2EwGpN149
zpXv5tqT
9Ms7ABAU+pRIoi/EfjQgMSQGF1457cIH7dxlVD+p85at
-----END CERTIFICATE-----
quit
!--- Manually pasted certificate into CLI. INFO:
Certificate has the following attributes: Fingerprint:
98d66001 f65d98a2 b455fbce d672c24a Do you accept this
certificate? [yes/no]: yes
Trustpoint CA certificate accepted.

% Certificate successfully imported
CiscoASA(config)#

```

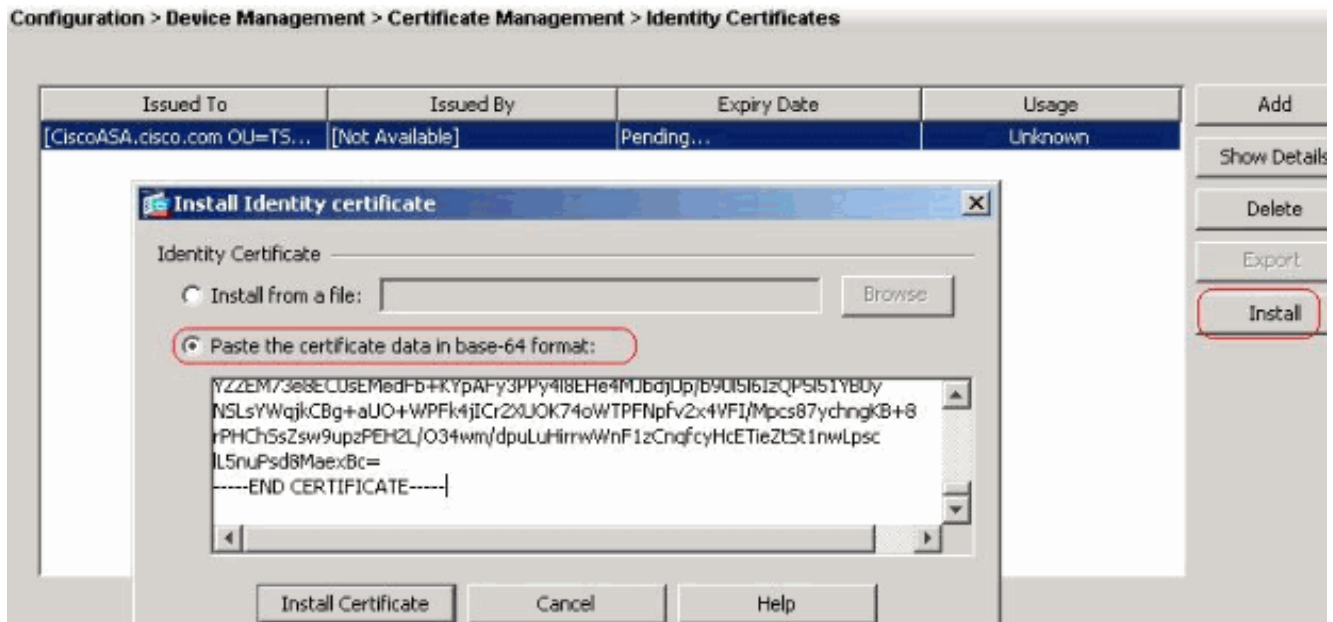
[Passaggio 4. Installare il certificato](#)

Procedura ASDM

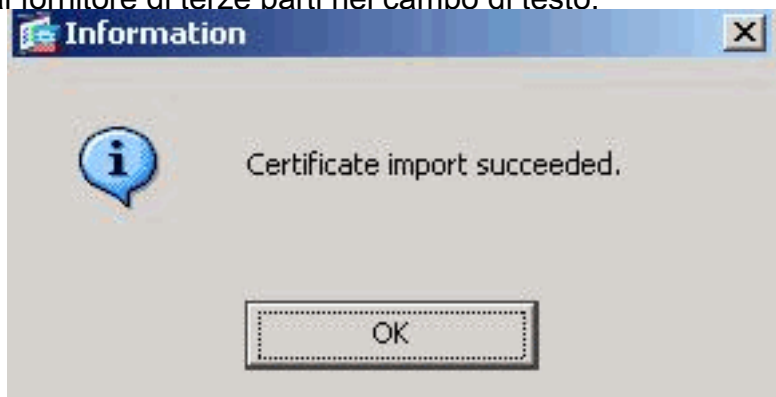
Utilizzare il certificato di identità fornito dal fornitore di terze parti per completare i seguenti passaggi:

1. Fare clic su **Configurazione** e quindi su **Gestione dispositivi**.
2. Espandere **Gestione certificati**, quindi scegliere **Certificati di identità**.

3. Selezionare il certificato di identità creato nel [passaggio 2](#). **Nota:** nella casella Data scadenza viene visualizzato In sospeso.
4. Fare clic su **Installa.**



Fare clic sul pulsante di opzione **Incolla i dati del certificato in formato base 64** e incollare il certificato di identità fornito dal fornitore di terze parti nel campo di testo.



5. Fare clic su **Installa certificato.** Verrà visualizzata una finestra di dialogo per confermare l'importazione.

Esempio della riga di comando

```

Cisco ASA

CiscoASA(config)#crypto ca import CA1 certificate

!--- Initiates prompt to paste the base64 identity !---
certificate provided by the third party vendor. %The
fully-qualified domain name in the certificate will be:
CiscoASA.cisco.com Enter the base 64 encoded
certificate. End with the word "quit" on a line by
itself !--- Paste the base 64 certificate provided by
the third party vendor. -----BEGIN CERTIFICATE-----
MIIFpzCCBI+gAwIBAgIKYR7lmwAAAAAABzANBgkqhkiG9w0BAQUFADBR
MRMwEQYK
CZImiZPyLGQBGRYDY29tMRUwEwYKZImiZPyLGQBGRYFY21zY28xFTAT
BgoJkiaJ
k/IsZAEZFgVUU1dlYjEMMAoGA1UEAxMDQ0EzMB4XDTA3MTIxNTA4MzUz
OV0XDTA5
MTIxNDA4MzUzOVowdjELMAkGA1UEBhMCVVMxFTZAVBgNVBAGTDk5vcnRo
IENhcm9s

```

```
aW5hMRAwDgYDVQQHEwdSYWxlaWdoMRYwFAYDVQKQEW1DaXNjbyBTeXN0
ZW1zMSQw
IgyYDVQQDExtDaXNjb0FTQS5jaXNjby5jb20gT1U9VFNXRUIwgZ8wDQYJ
KoZlhvcN
AQEBBQADgY0AMIGJAoGBALjiCqgzI1a3W2YAc1AI03NdI8UpW5JHK14C
qB9j3HpX
BmfXVF5/mNPUI5tCq4+vC+il05T4DQGhTMAdmLEyDp/oSQVauUsY7zCO
sS8iqxqO
2zjwLcZ3jgcZfy1S08tzkanMstkD9yK9QUUsKMgWqBT7EXiRkgGBvjkF/
CaeqnGRN
AgMBAAGjggLeMIIC2jALBgNVHQ8EBAMCBAAwHQYDVR0RBBywFIISQ21z
Y29BU0Eu
Y21zY28uY29tMB0GA1UdDgQWBbQsJC3bSQzeGv4tY+MeH7KM10xCFjAf
BgNVHSME
GDAWgBTZrb8I8jqI8RRDL3mYfnQJpAP1WDCCAQMGA1UdHwSB+zCB+DCB
9aCB8qCB
74aBtWxkYXA6Ly8vQ049Q0ExLENOPVRTLVcySzMtQUNTLENOPUNEUCxID
Tj1QdWJs
aWM1MjBLZXklMjBTZXJ2aWN1cyxDTj1TZXJ2aWN1cyxDTj1Db25maWd1
cmF0aW9u
LERDPVRTV2ViLERDPWNpc2NvLERDPWNvbT9jZXJ0aWZpY2F0ZVJldm9j
YXRpb25M
aXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRGlzdHJpYnV0aW9uUG9pbmSG
NWh0dHA6
Ly90cy13MmszLWFjcy50c3dlYi5jaXNjby5jb20vQ2VydeVucm9sbC9D
QTEuY3Js
MIIBHQYIKwYBBQUHAQEgEgEPMIIBCzCBQQYIKwYBBQUHMAKGgZxsZGFw
Oi8vL0NO
PUNBMSxDTj1BSUESQ049UHvibG1jJTIwS2V5JTIwU2Vydm1jZXMsQ049
U2Vydm1j
ZXMsQ049Q29uZmlndXJhdG1vbixEQz1UU1dlYixEQz1jaXNjbyxEQz1j
b20/Y0FD
ZXJ0aWZpY2F0ZT9iYXN1P29iamVjdENsYXNzPWN1cnRpZmljYXRpb25B
dXR0b3Jp
dHkwXQYIKwYBBQUHMAKGUWh0dHA6Ly90cy13MmszLWFjcy50c3dlYi5j
aXNjby5j
b20vQ2VydeVucm9sbC9UuY1XmksZLUFDUy5UU1dlYi5jaXNjby5jb21f
Q0ExLmNy
dDAhBgkrBgEEAYI3FAIEFB4SAFcAZQBiAFMAZQByAHYAZQByMAWGA1Ud
EwEB/wQC
MAAwEwYDVR01BAwwCgYIKwYBBQUHAWEdDQYJKoZIhvcNAQEFBQADggEB
AIqCaA9G
+8h+3IS8rfVAGzCWAEVRXCyBlx0NpR/jlocGJ7QbQxkjKEswXq/O2xDB
7wXQaGph
zRq4dxAL111JkIjhfeQY+7VSkZlGEpuBnENTohdhtz5vBjGlcROXIs8
+3Ghg8hy
YZZEM73e8EC0sEMedFb+KYpAFy3PPy418EHe4MJbdjUp/b901516IzQP
5151YB0y
NSLsYWqjkCBg+aUO+WPFk4jICr2XUOK74oWTFPNpFv2x4VFI/Mpcs87y
chngKB+8
rPHChSsZsw9upzPEH2L/O34wm/dpuLuHirrwWnF1zCnqfcyHcETieZtS
tlnwLpsc
lL5nuPsd8MaexBc=
-----END CERTIFICATE-----
quit

INFO: Certificate successfully imported
CiscoASA(config)#
```

[Passaggio 5. Configurare la VPN di accesso remoto \(IPSec\) per l'utilizzo del nuovo certificato installato](#)

Procedura ASDM

Per configurare la VPN di accesso remoto, completare i seguenti passaggi:

1. Scegliere **Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Avanzate > IPSec > Criteri IKE > Aggiungi** per creare una policy ISAKMP 65535, come mostrato.

Add IKE Policy

Priority: Authentication:

Encryption: D-H Group:

Hash: Lifetime: Unlimited

Fare clic su **OK** e su **Applica**.

2. Scegliere **Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Avanzate > IPSec > Set trasformazioni IPSec > Aggiungi** per creare il set di trasformazioni **myset**, come

Add Transform Set

Set Name:

Properties

Mode: Tunnel Transport

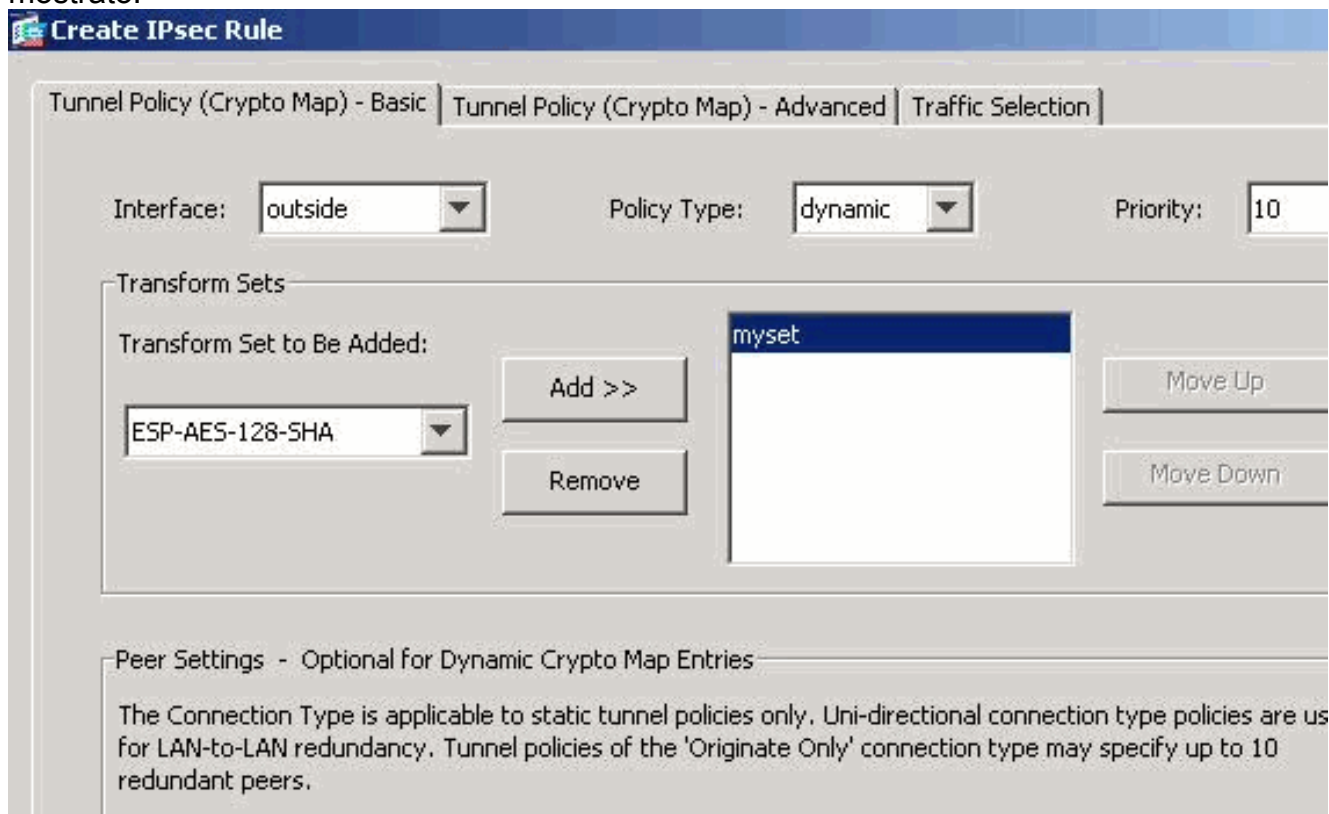
ESP Encryption:

ESP Authentication:

mostrato.
su **Applica**.

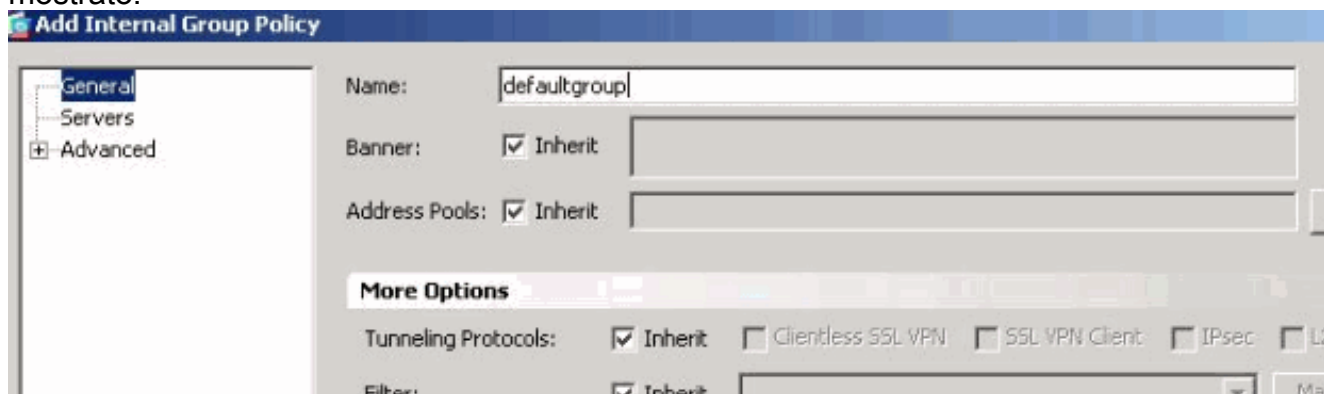
Fare clic su **OK** e

3. Scegliere **Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Avanzate > IPSec > Mappe crittografiche > Aggiungi** per creare una mappa crittografica con criterio dinamico di priorità 10, come mostrato.



Fare clic su **OK** e su **Applica**. **Nota:** ASA 8.0 non supporta SHA 2. Non sono supportati anche i client IPSec che utilizzano certificati con hash 256.

4. Scegliere **Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Avanzate > Criteri di gruppo > Aggiungi** per creare un criterio di gruppo predefinito, come mostrato.



Fare clic su **OK** e su **Applica**.

5. Scegliere **Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Assegnazione indirizzi > Pool di indirizzi > Aggiungi** per configurare il pool di indirizzi **vpnpool** per gli utenti client VPN da assegnare in modo

Add IP Pool

Name: vpnpool

Starting IP Address: 10.5.5.10

Ending IP Address: 10.5.5.20

Subnet Mask: 255.255.255.0

OK Cancel Help

dinamico.

Fare clic su **OK** e su

Applica.

6. Per creare l'account utente **vpnuser** per l'accesso client VPN, scegliere **Configurazione > VPN di accesso remoto > Impostazione AAA > Utenti locali > Aggiungi**. Inoltre, rendere questo utente membro di **DefaultRAGroup**.

Add User Account

Identity
+ VPN Policy

Username:

Password:

Confirm Password:

User authenticated using MSCHAP

Member-of

Member-of:

Access Restriction

Select one of the options below to restrict ASDM, SSH, Telnet and Console access.
Note: All users have network access, regardless of these settings.

Full access(ASDM, SSH, Telnet and Console)
Privilege level is used with command authorization.
Privilege Level:

CLI login prompt for SSH, Telnet and console (no ASDM access)
This setting is effective only if AAA authenticate console command is configured.

No ASDM, SSH, Telnet or Console access
This setting is effective only if AAA authenticate console command is configured.

7. Scegliere **Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Profili di connessione IPSec > Modifica** per modificare il **gruppo predefinito RAGroup**, come mostrato. Scegliere il **certificato di identità** appropriato dal menu a discesa per il campo Autenticazione peer IKE. Scegliere il gruppo di server come **LOCALE** per il campo Autenticazione utente. Scegliere **vpnpool** come pool di indirizzi client per il campo Assegnazione indirizzo client. Scegliere **gruppo predefinito** come Criteri di gruppo per il campo Criteri di gruppo predefinito.

Fare clic su OK e su Applica.

Esempio della riga di comando

```

Cisco ASA

CiscoASA(config)#crypto isakmp enable outside
CiscoASA(config)#crypto isakmp policy 65535
CiscoASA(config-isakmp-policy)#authentication rsa-sig
CiscoASA(config-isakmp-policy)#encryption 3des
CiscoASA(config-isakmp-policy)#hash md5
CiscoASA(config-isakmp-policy)#group 2
CiscoASA(config-isakmp-policy)#lifetime 86400
CiscoASA(config-isakmp-policy)#exit
CiscoASA(config)#crypto isakmp identity auto

!--- Phase 1 Configurations CiscoASA(config)#crypto
ipsec transform-set myset esp-3des esp-md5-hmac
CiscoASA(config)#crypto dynamic-map dynmap 10 set
transform-set myset
CiscoASA(config)#crypto map mymap 10 ipsec-isakmp
dynamic dynmap
CiscoASA(config)#crypto map mymap interface outside

!--- Phase 2 Configurations CiscoASA(config)#group-
policy defaultgroup internal
CiscoASA(config)#group-policy defaultgroup attributes
CiscoASA(config-group-policy)#default-domain value
cisco.com
CiscoASA(config-group-policy)# exit

!--- Create a group policy "defaultgroup" with domain
name !--- cisco.com CiscoASA(config)#username vpnuser
password Cisco123
CiscoASA(config)#username vpnuser attributes
CiscoASA(config-username)#memberof DefaultRAGroup
CiscoASA(config-username)#exit

```

```

!--- Create a user account "vpnuser" and added to !---
"DefaultGroup" CiscoASA(config)#tunnel-group
DefaultRAGroup general-attributes

!--- The Security Appliance provides the default tunnel
groups !--- for remote access (DefaultRAGroup).
CiscoASA(config-tunnel-general)#address-pool vpnpool

!--- Associate the vpnpool to the tunnel group using the
address pool. CiscoASA(config-tunnel-general)#default-
group-policy Defaultgroup

!--- Associate the group policy "Defaultgroup" to the
tunnel group. CiscoASA(config-tunnel-general)# exit
CiscoASA(config)#tunnel-group DefaultRAGroup ipsec-
attributes
CiscoASA(config-tunnel-ipsec)#trust-point CA1
CiscoASA(config-tunnel-ipsec)#exit

!--- Associate the trustpoint CA1 for IPSec peer !---
authentication

```

Riepilogo della configurazione dell'ASA

Cisco ASA

```

CiscoASA#show running-config
: Saved
:
ASA Version 8.0(2)
!
hostname CiscoASA
domain-name cisco.com
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 192.168.1.5 255.255.255.0
!
interface Ethernet0/1
 shutdown
 nameif inside
 security-level 100
 ip address 10.2.2.1 255.255.255.0
!
interface Ethernet0/2
 nameif DMZ
 security-level 90
 ip address 10.77.241.142 255.255.255.192
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!

```

```
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
 !
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name cisco.com
access-list 100 extended permit ip 10.2.2.0
255.255.255.0 10.5.5.0
 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
mtu DMZ 1500
ip local pool vpnpool 10.5.5.10-10.5.5.20
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-602.bin
no asdm history enable
arp timeout 14400
nat (inside) 0 access-list 100
route DMZ 0.0.0.0 0.0.0.0 10.77.241.129 1
route outside 10.1.1.0 255.255.255.0 192.168.1.1 1
route outside 172.16.5.0 255.255.255.0 192.168.1.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 0.0.0.0 0.0.0.0 DMZ
http 0.0.0.0 0.0.0.0 outside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
crypto ipsec transform-set myset esp-3des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap interface outside
crypto ca trustpoint CA1
 enrollment terminal
 subject-name cn=CiscoASA.cisco.com OU=TSWEB, O=Cisco
Systems, C=US,
 St=North Carolina,L=Rale
 serial-number
 keypair my.CA.key
 crl configure
crypto ca certificate chain CA1
 certificate 611ee59b000000000007
 308205a7 3082048f a0030201 02020a61 1ee59b00
00000000 07300d06 092a8648
 86f70d01 01050500 30513113 3011060a 09922689
93f22c64 01191603 636f6d31
 15301306 0a099226 8993f22c 64011916 05636973
636f3115 3013060a 09922689
 93f22c64 01191605 54535765 62310c30 0a060355
```

04031303 43413130 1e170d30
37313231 35303833 3533395a 170d3039 31323134
30383335 33395a30 76310b30
09060355 04061302 55533117 30150603 55040813
0e4e6f72 74682043 61726f6c
696e6131 10300e06 03550407 13075261 6c656967
68311630 14060355 040a130d
43697363 6f205379 7374656d 73312430 22060355
0403131b 43697363 6f415341
2e636973 636f2e63 6f6d204f 553d5453 57454230
819f300d 06092a86 4886f70d
01010105 0003818d 00308189 02818100 b8e20aa8
332356b7 5b660073 5008d373
5d23c529 5b92472b 5e02a81f 63dc7a57 0667d754
5e7f98d3 d4239b42 ab8faf0b
e8a5d394 f80d01a1 4cc01d98 b1320e9f e849055a
b94b18ef 308eb12f 22ab1a8e
db38f02c 2cf78e07 197f2d52 d3cb7391 a9ccb2d9
03f722bd 414b0a32 05aa053e
c45e2464 80606f8e 417f09a7 aa9c644d 02030100
01a38202 de308202 da300b06
03551d0f 04040302 05a0301d 0603551d 11041630
14821243 6973636f 4153412e
63697363 6f2e636f 6d301d06 03551d0e 04160414
2c242ddb 490cdela fe2d63e3
1e1fb28c 974c4216 301f0603 551d2304 18301680
14d9adbf 08f23a88 f114432f
79987cd4 09a403e5 58308201 03060355 1d1f0481
fb3081f8 3081f5a0 81f2a081
ef8681b5 6c646170 3a2f2f2f 434e3d43 41312c43
4e3d5453 2d57324b 332d4143
532c434e 3d434450 2c434e3d 5075626c 69632532
304b6579 25323053 65727669
6365732c 434e3d53 65727669 6365732c 434e3d43
6f6e6669 67757261 74696f6e
2c44433d 54535765 622c4443 3d636973 636f2c44
433d636f 6d3f6365 72746966
69636174 65526576 6f636174 696f6e4c 6973743f
62617365 3f6f626a 65637443
6c617373 3d63524c 44697374 72696275 74696f6e
506f696e 74863568 7474703a
2f2f7473 2d77326b 332d6163 732e7473 7765622e
63697363 6f2e636f 6d2f4365
7274456e 726f6c6c 2f434131 2e63726c 3082011d
06082b06 01050507 01010482
010f3082 010b3081 a906082b 06010505 07300286
819c6c64 61703a2f 2f2f434e
3d434131 2c434e3d 4149412c 434e3d50 75626c69
63253230 4b657925 32305365
72766963 65732c43 4e3d5365 72766963 65732c43
4e3d436f 6e666967 75726174
696f6e2c 44433d54 53576562 2c44433d 63697363
6f2c4443 3d636f6d 3f634143
65727469 66696361 74653f62 6173653f 6f626a65
6374436c 6173733d 63657274
69666963 6174696f 6e417574 686f7269 7479305d
06082b06 01050507 30028651
68747470 3a2f2f74 732d7732 6b332d61 63732e74
73776562 2e636973 636f2e63
6f6d2f43 65727445 6e726f6c 6c2f5453 2d57324b
332d4143 532e5453 5765622e
63697363 6f2e636f 6d5f4341 312e6372 74302106
092b0601 04018237 14020414
1e120057 00650062 00530065 00720076 00650072

300c0603 551d1301 01ff0402
30003013 0603551d 25040c30 0a06082b 06010505
07030130 0d06092a 864886f7
0d010105 05000382 0101008a 82680f46 fbc87edc
84bc45f5 401b3716 0045515c
2c81971d 0da51fe3 96870627 b41b4319 23284b30
5eafcedb 10clef05 d0686a61
cd1ab877 100b965d 499088e1 7de418fb b5529199
46129b81 9c4353a2 1761b61c
f9bc18c6 95c44e5c 8b3cfb71 a183c872 61964433
bddef040 b4b0431e 7456fe29
8a40172d cf3f2e25 f041dee0 c25b7635 29fdbf74
97997a23 340fe65e 75601d32
3522ec61 6aa39020 60f9a50e f963c593 88c80abd
9750e2bb e285933c 53697efd
b1e15148 fc5a5cb3 cef27219 e0281fbc acf1c285
2b19b30f 6ea733c4 1f62ff3b
7e309bf7 69b8bb87 8abaf05a 7175cc29 ea7dcc87
7044e279 9b52b759 f02e9b1c
94be67b8 fb1df0c6 9ec417
quit
certificate ca 7099f1994764e09c4651da80a16b749c
3082049d 30820385 a0030201 02021070 99f19947
64e09c46 51da80a1 6b749c30
0d06092a 864886f7 0d010105 05003051 31133011
060a0992 268993f2 2c640119
1603636f 6d311530 13060a09 92268993 f22c6401
19160563 6973636f 31153013
060a0992 268993f2 2c640119 16055453 57656231
0c300a06 03550403 13034341
31301e17 0d303731 32313430 36303134 335a170d
31323132 31343036 31303135
5a305131 13301106 0a099226 8993f22c 64011916
03636f6d 31153013 060a0992
268993f2 2c640119 16056369 73636f31 15301306
0a099226 8993f22c 64011916
05545357 6562310c 300a0603 55040313 03434131
30820122 300d0609 2a864886
f70d0101 01050003 82010f00 3082010a 02820101
00ea8fee c7ae56fc a22e603d
0521b333 3dec0ad4 7d4c2316 3b1eea33 c9a6883d
28ece906 02902f9a d1eb2b8d
f588cb9a 78a069a3 965de133 6036d8d7 6ede9ccd
ale906ec 88b32a19 38e5353e
6c0032e8 8c003fa6 2fd22a4d b9dda2c2 5fcbb621
876bd678 c8a37109 f074eabe
2b1fac59 a78d0a3b 35af17ae 687a4805 3b9a34e7
24b9e054 063c60a4 9b8d3c09
351bc630 05f69357 833b9197 f875b408 cb71a814
69a1f331 b1eb2b35 0c469443
1455c210 db308bf0 a9805758 a878b82d 38c71426
afffd272 dd6d7564 1cbe4d95
b81c02b2 9b56ec2d 5a913a9f 9b95cafd dfffcf67
94b97ac7 63249009 fa05ca4d
6f13afd0 968f9f41 e492cfe4 e50e15f1 c0f5d13b
5f020301 0001a382 016f3082
016b3013 06092b06 01040182 37140204 061e0400
43004130 0b060355 1d0f0404
03020186 300f0603 551d1301 01ff0405 30030101
ff301d06 03551d0e 04160414
d9adbf08 f23a88f1 14432f79 987cd409 a403e558
30820103 0603551d 1f0481fb
3081f830 81f5a081 f2a081ef 8681b56c 6461703a
2f2f2f43 4e3d4341 312c434e

```
3d54532d 57324b33 2d414353 2c434e3d 4344502c
434e3d50 75626c69 63253230
4b657925 32305365 72766963 65732c43 4e3d5365
72766963 65732c43 4e3d436f
6e666967 75726174 696f6e2c 44433d54 53576562
2c44433d 63697363 6f2c4443
3d636f6d 3f636572 74696669 63617465 5265766f
63617469 6f6e4c69 73743f62
6173653f 6f626a65 6374436c 6173733d 63524c44
69737472 69627574 696f6e50
6f696e74 86356874 74703a2f 2f74732d 77326b33
2d616373 2e747377 65622e63
6973636f 2e636f6d 2f436572 74456e72 6f6c6c2f
4341312e 63726c30 1006092b
06010401 82371501 04030201 00300d06 092a8648
86f70d01 01050500 03820101
001abc5a 40b32112 22da80fb bb228bfe 4bf8a515
df8fc3a0 4e0c89c6 d725e2ab
2fa67ce8 9196d516 dfe55627 953aea47 2e871289
6b754e9c 1e01d408 3f7f0595
8081f986 526fbe1c c9639d6f 258b2205 0dc370c6
5431b034 fe9fd60e 93a6e71b
ab8e7f84 a011336b 37c13261 5ad218a3 a513e382
e4bfb2b4 9bf0d7d1 99865cc4
94e5547c f03e3d3e 3b766011 e94a3657 6cc35b92
860152d4 f06b2b15 df306433
c1bcc282 80558d70 d22d72e7 eed3195b d575dceb
c0caa196 34f693ea f3beee4d
aa2ef1c2 edba288f 3a678ecb 3809d0df b1699c76
13018f9f 5e3dce95 efe6da93
f4cb3b00 102efa94 48a22fc4 7e342031 2406165e
39edc207 eddc6554 3fa9f396 ad
quit
crypto isakmp enable outside
crypto isakmp policy 65535
authentication rsa-sig
encryption 3des
hash md5
group 2
lifetime 86400
crypto isakmp identity auto
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
```

```

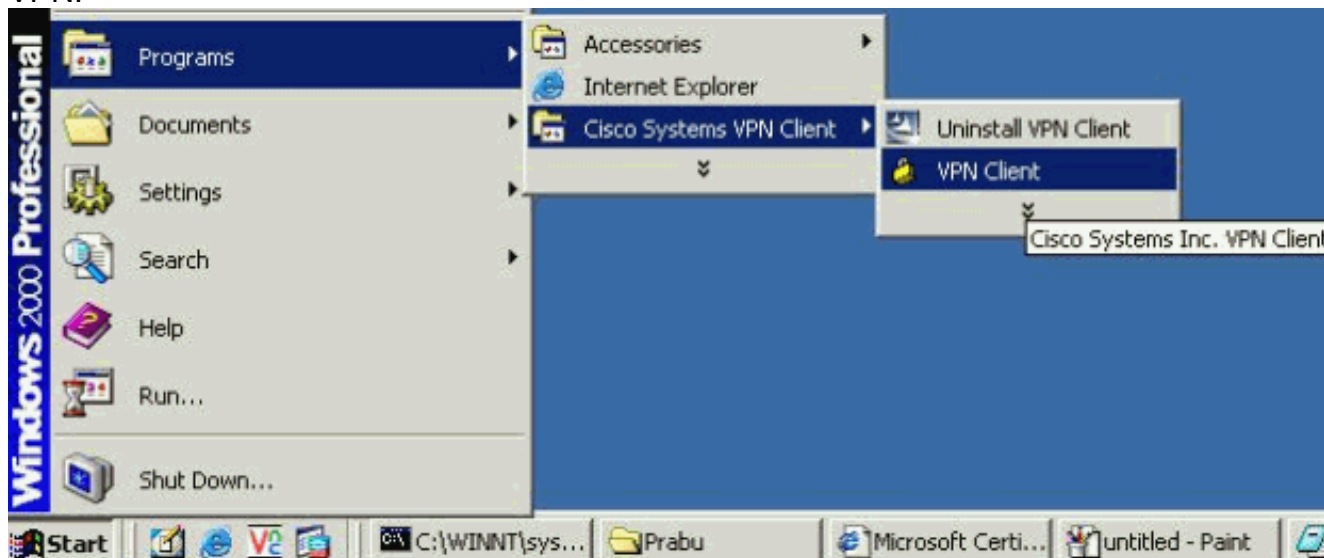
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
!
service-policy global_policy global
group-policy defaultgroup internal
group-policy defaultgroup attributes
  default-domain value cisco.com
username vpnuser password TXttW.eFqbHusJQM encrypted
username vpnuser attributes
  memberof DefaultRAGroup
tunnel-group DefaultRAGroup general-attributes
  address-pool vpnpool
tunnel-group DefaultRAGroup ipsec-attributes
  trust-point CA1
prompt hostname context
Cryptochecksum:dd6f2e3390bf5238815391c13e42cd21
: end
CiscoASA#

```

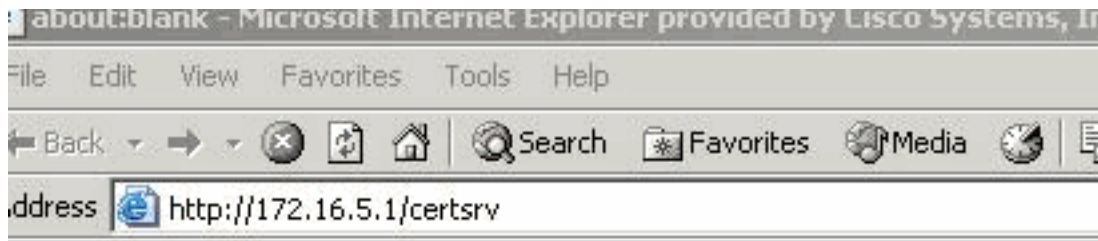
Configurazione client VPN

Completare questa procedura per configurare il client VPN.

1. Scegliere **Start > Programmi > Cisco Systems VPN Client > VPN Client** per avviare il software client VPN.



2. Completare questa procedura per scaricare il certificato CA dal server CA denominato **CA1** e installarlo nel client VPN Cisco. Eseguire l'accesso Web al server CA 172.16.5.1 con l'aiuto delle credenziali fornite all'utente



Enter Network Password

Please type your user name and password.

Site: 172.16.5.1

User Name: vpnuser

Password: *****

Domain:

Save this password in your password list

OK Cancel

vpn.

Nota:
verificare di disporre di un account utente per l'utente client VPN con il server CA. Fare clic su **Scarica un certificato CA, una catena di certificati o un CRL** per aprire la finestra, come illustrato. Fare clic sul pulsante di scelta **Base 64** come metodo di codifica, quindi fare clic su **Scarica certificato CA**.

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA cert](#)

To download a CA certificate, certificate chain, or CRL, select the certificate

CA certificate:



Encoding method:

- DER
- Base 64

[Download CA certificate](#)

[Download CA certificate chain](#)

[Download latest base CRL](#)

[Download latest delta CRL](#)

Salvare il certificato CA con il nome **certnew.cer** nel computer. Per impostazione predefinita, viene archiviato nel percorso `C:\Program Files\Cisco Systems\VPN`



Client.

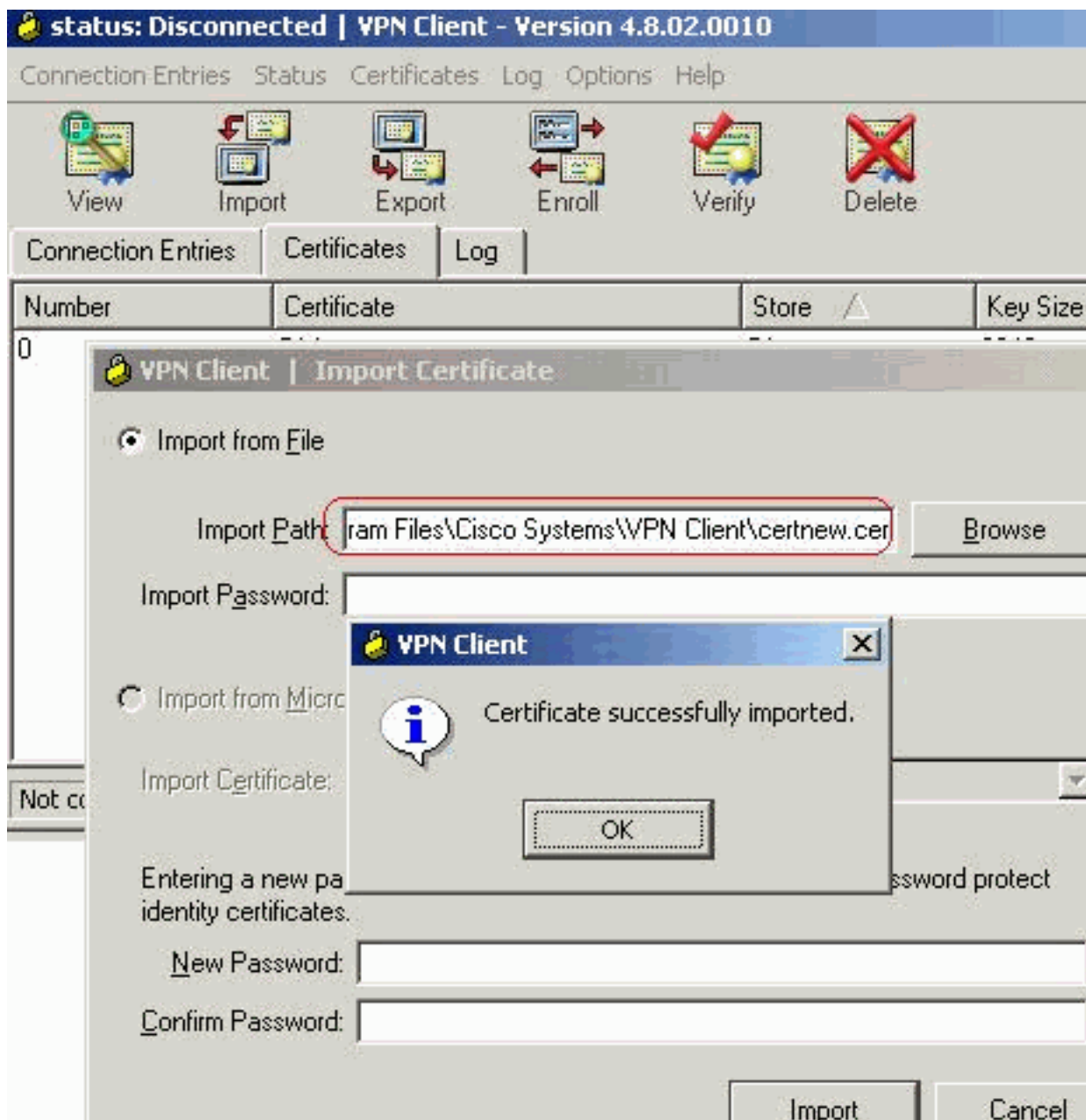
Nel client VPN,

scegliere la **scheda Certificati > Importa**, quindi fare clic sul pulsante **Importa da fileradio**.

Fare clic su **Sfogliare** per importare il certificato CA dal percorso archiviato `C:\Program`

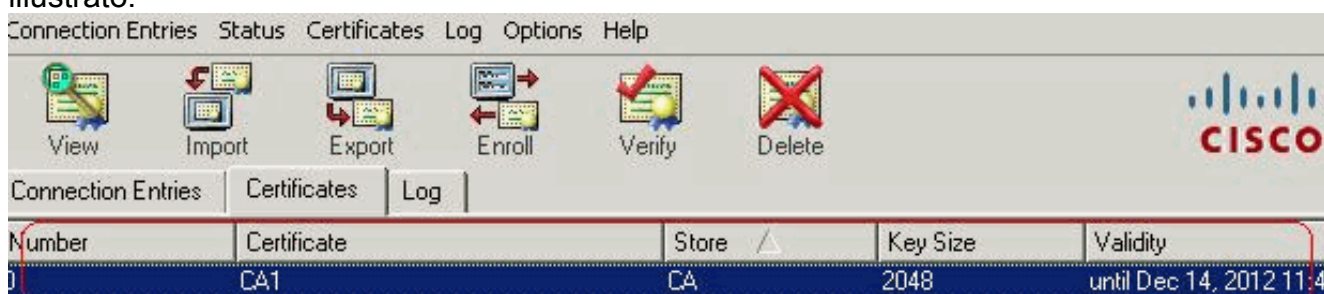
`Files\Cisco Systems\VPN Client`, come mostrato. Fare clic su **Import** (Importa). Viene

visualizzata una finestra di operazione riuscita, come illustrato.

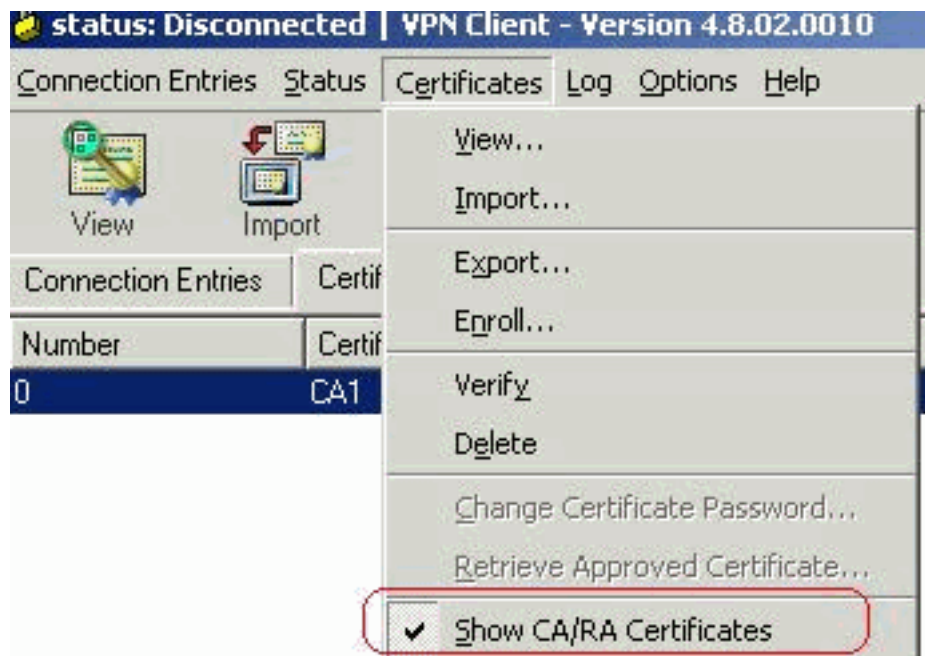


Nella

scheda Certificati viene visualizzata la CA Certificati CA CA1, come illustrato.



Nota: assicurarsi che l'opzione **Mostra certificati CA/RA** sia selezionata, come illustrato, altrimenti i certificati CA non devono essere visualizzati nella finestra dei



certificati.

3. Completare questa procedura per scaricare il certificato di identità e installarlo nel client VPN. Nella CA1 del server CA, scegliere **Richiedi certificato > Richiesta certificato avanzata > Crea e invia una richiesta alla CA** per registrare il certificato di identità. Fare clic su **Invia**.

Certificate Template:

User ▼

Key Options:

Create new key set Use existing key set

CSP: Microsoft Enhanced Cryptographic Provider v1.0 ▼

Key Usage: Exchange

Key Size: 1024 Min: 384 Max: 16384 (common key sizes: [512](#) [1024](#) [2048](#) [4096](#) [8192](#) [16384](#))

Automatic key container name User specified key container name

Mark keys as exportable

Export keys to file

Enable strong private key protection

Store certificate in the local computer certificate store

Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.

Additional Options:

Request Format: CMC PKCS10

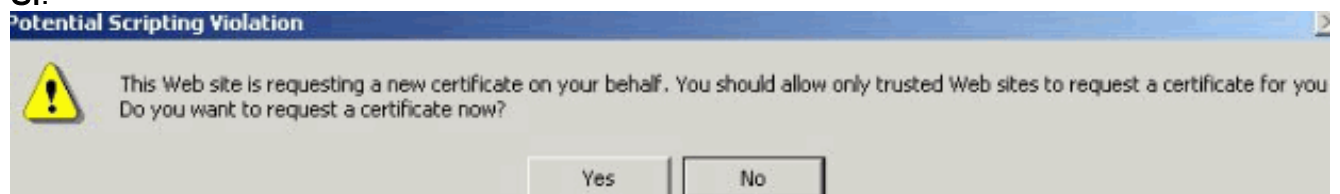
Hash Algorithm: MD5 ▼

Only used to sign request.

Save request to a file

Per continuare, fare clic su

Sì.



Fare clic su **Installa il**

Microsoft Certificate Services -- CA1

Certificate Issued

The certificate you requested was issued to you.

certificato.

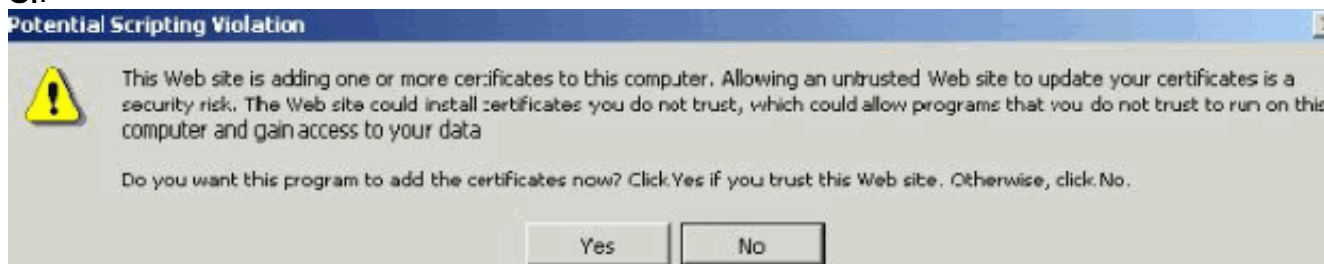


[Install this certificate](#)

Per continuare, fare

clik su

Sì.

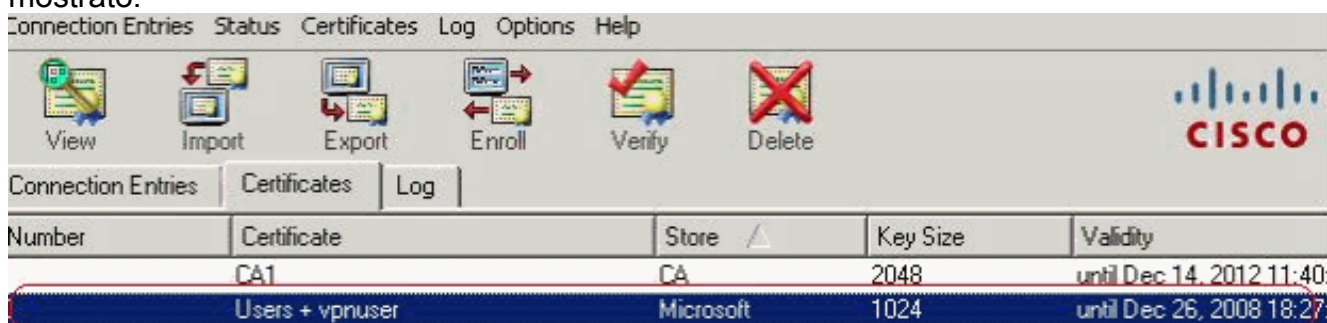


È necessario ricevere il messaggio di installazione certificato, come

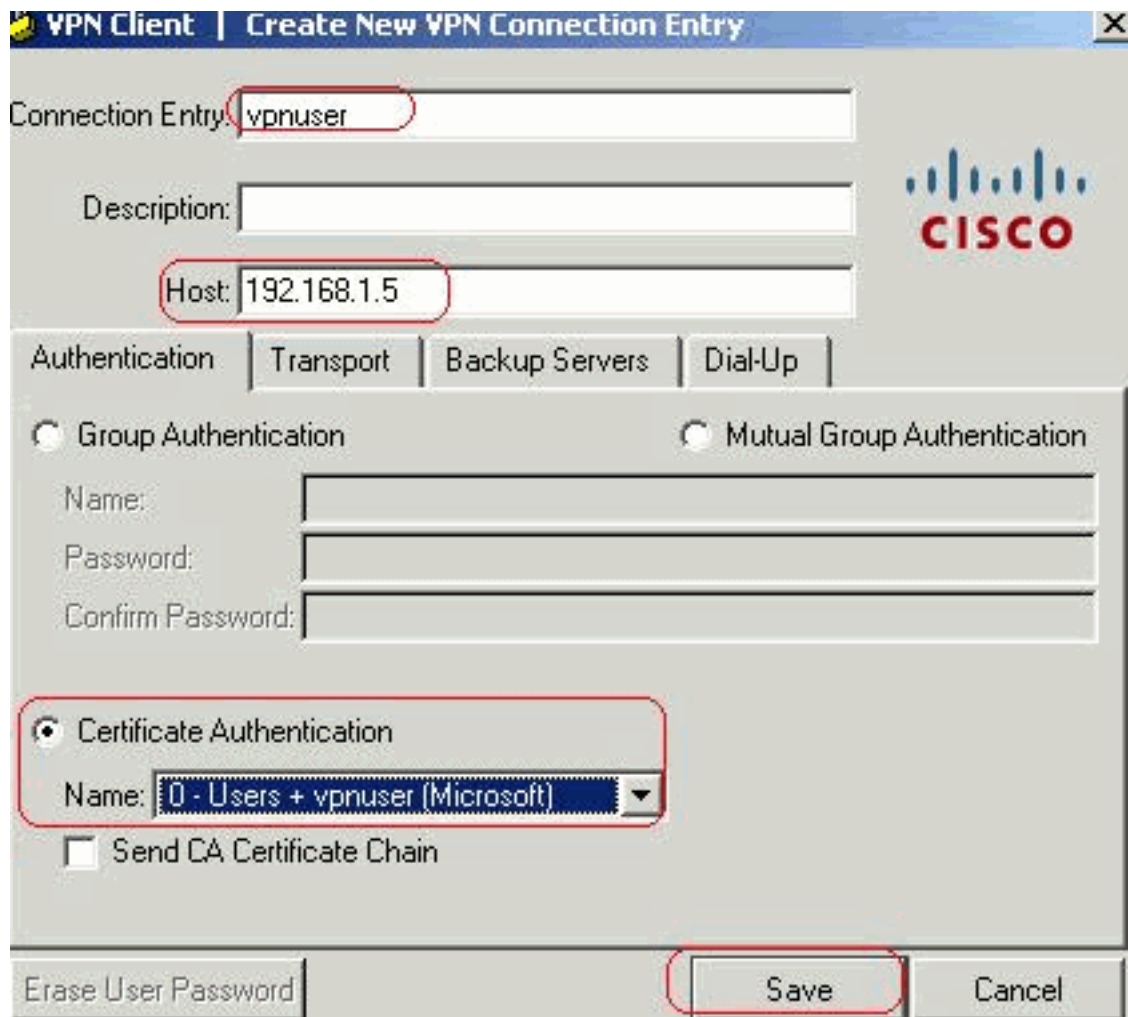
Microsoft Certificate Services -- CA1

Certificate Installed

illustrato. *Your new certificate has been successfully installed.* Uscire dal client VPN e riavviarlo per fare in modo che il certificato di identità installato venga visualizzato nella scheda Certificato del client VPN, come mostrato.

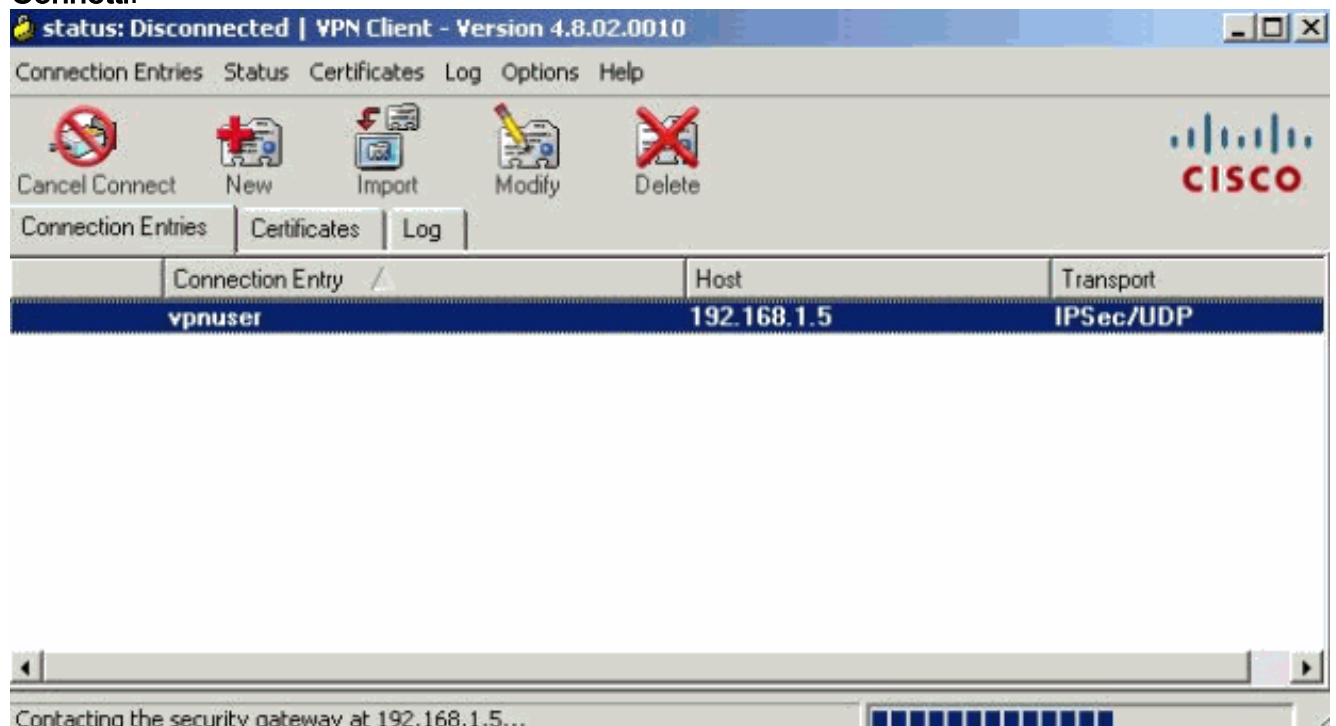


4. Nella scheda Voci di connessione, fare clic su **Nuovo** per creare la voce di connessione **vpnuser**, come mostrato. Immettere l'indirizzo IP peer remoto (intradabile) nel campo Host. Fare clic sul pulsante di scelta **Autenticazione certificato** e scegliere il certificato di identità dall'elenco a discesa, come mostrato. Fare clic su



Salva.

5. Fare clic su **Connetti**.

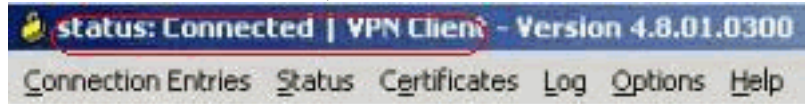


6. Quando richiesto, immettere il nome utente e la password per xauth e fare clic su **OK** per connettersi alla rete



remota.

7. Il client VPN si connette all'ASA, come



mostrato.

Verifica

Sull'appliance ASA, è possibile usare diversi comandi show dalla riga di comando per verificare lo stato di un certificato.

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

- Il comando **show crypto ca trustpoint** visualizza i trust configurati.

```
CiscoASA#show crypto ca trustpoints
```

```
Trustpoint CA1:
```

```
Subject Name:
```

```
cn=CA1
```

```
dc=TSWeb
```

```
dc=cisco
```

```
dc=com
```

```
Serial Number: 7099f1994764e09c4651da80a16b749c
```

```
Certificate configured.
```

- Il comando **show crypto ca certificate** visualizza tutti i certificati installati nel sistema.

```
CiscoASA# show crypto ca certificate
```

```
Certificate
```

```
Status: Available
```

```
Certificate Serial Number: 3f14b70b00000000001f
```

```
Certificate Usage: Encryption
```

```
Public Key Type: RSA (1024 bits)
```

```
Issuer Name:
```

```
cn=CA1
```

```
dc=TSWeb
```

```
dc=cisco
```

```
dc=com
```

```
Subject Name:
```

```
cn=vpnserver
```

```
cn=Users
```

```
dc=TSWeb
```

```
dc=cisco
```

```
dc=com
```

```
PrincipalName: vpnserver@TSWeb.cisco.com
```

```
CRL Distribution Points:
```

```
[1] ldap:///CN=CA1,CN=TS-W2K3-ACS,CN=CDP,CN=Public%20Key%20Services,
CN=Services,CN=Configuration,DC=TSWeb,DC=cisco,
DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint
```

```
[2] http://ts-w2k3-ac.s.tsweb.cisco.com/CertEnroll/CA1.crl
```

```
Validity Date:
```

```
start date: 14:00:36 UTC Dec 27 2007
```

```
end date: 14:00:36 UTC Dec 26 2008
Associated Trustpoints: CA1
```

CA Certificate

```
Status: Available
Certificate Serial Number: 7099f1994764e09c4651da80a16b749c
Certificate Usage: Signature
Public Key Type: RSA (2048 bits)
Issuer Name:
  cn=CA1
  dc=TSWeb
  dc=cisco
  dc=com
Subject Name:
  cn=CA1
  dc=TSWeb
  dc=cisco
  dc=com
CRL Distribution Points:
  [1] ldap:///CN=CA1,CN=TS-W2K3-ACS,CN=CDP,CN=Public%20Key%20Services,
      CN=Services,CN=Configuration,DC=TSWeb,DC=cisco,
      DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint
  [2] http://ts-w2k3-acs.tsweb.cisco.com/CertEnroll/CA1.crl
Validity Date:
  start date: 06:01:43 UTC Dec 14 2007
  end date: 06:10:15 UTC Dec 14 2012
Associated Trustpoints: CA1
```

Certificate

```
Subject Name:
  Name: CiscoASA.cisco.com
Status: Pending terminal enrollment
Key Usage: General Purpose
Fingerprint: 1a022cf2 9771e335 12c3a530 1f9a0345
Associated Trustpoint: CA1
```

- Il comando **show crypto ca crls** visualizza gli elenchi di revoche di certificati (CRL) memorizzati nella cache.
- Il comando **show crypto key mypubkey rsa** visualizza tutte le coppie di chiavi crittografiche generate.

```
CiscoASA# show crypto key mypubkey rsa
Key pair was generated at: 01:43:45 UTC Dec 11 2007
Key name: <Default-RSA-Key>
Usage: General Purpose Key
Modulus Size (bits): 1024
Key Data:

30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00d4a509
99e95d6c b5bdaa25 777aebbe 6ee42c86 23c49f9a bea53224 0234b843 1c0c8541
f5a66eb1 6d337c70 29031b76 e58c3c6f 36229b14 fefd3298 69f9123c 37f6c43b
4f8384c4 a736426d 45765cca 7f04cba1 29a95890 84d2c5d4 adeeb248 a10b1f68
2fe4b9b1 5fa12d0e 7789ce45 55190e79 1364aba4 7b2b21ca de3af74d b7020301 0001
Key pair was generated at: 06:36:00 UTC Dec 15 2007
Key name: my.CA.key
Usage: General Purpose Key
Modulus Size (bits): 1024
Key Data:
```

```
30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00b8e20a
a8332356 b75b6600 735008d3 735d23c5 295b9247 2b5e02a8 1f63dc7a 570667d7
545e7f98 d3d4239b 42ab8faf 0be8a5d3 94f80d01 a14cc01d 98b1320e 9fe84905
5ab94b18 ef308eb1 2f22ab1a 8edb38f0 2c2cf78e 07197f2d 52d3cb73 91a9ccb2
```



```
d903f722 bd414b0a 3205aa05 3ec45e24 6480606f 8e417f09 a7aa9c64 4d020301 0001
Key pair was generated at: 07:35:18 UTC Dec 21 2007
CiscoASA#
```

- Il comando **show crypto isakmp sa** visualizza le informazioni del tunnel IKE 1.

```
CiscoASA#show crypto isakmp sa
```

```
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1
```

```
1 IKE Peer: 10.1.1.5
  Type      : user           Role       : responder
  Rekey     : no            State      : MM_ACTIVE
```

- Per visualizzare le informazioni sul tunnel IPsec, usare il comando **show crypto ipsec sa**.

```
CiscoASA#show crypto ipsec sa
```

```
interface: outside
```

```
  Crypto map tag: dynmap, seq num: 10, local addr: 192.168.1.5
```

```
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (10.5.5.10/255.255.255.255/0/0)
current_peer: 10.1.1.5, username: vpnuser
dynamic allocated peer ip: 10.5.5.10
```

```
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 144, #pkts decrypt: 144, #pkts verify: 144
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors: 0, #recv errors: 0
```

```
local crypto endpt.: 192.168.1.5, remote crypto endpt.: 10.1.1.5
```

```
path mtu 1500, ipsec overhead 58, media mtu 1500
current outbound spi: FF3EEE7D
```

```
inbound esp sas:
```

```
spi: 0xEFDF8BA9 (4024404905)
  transform: esp-3des esp-md5-hmac none
  in use settings = {RA, Tunnel, }
  slot: 0, conn_id: 4096, crypto-map: dynmap
  sa timing: remaining key lifetime (sec): 28314
  IV size: 8 bytes
  replay detection support: Y
```

```
outbound esp sas:
```

```
spi: 0xFF3EEE7D (4282314365)
  transform: esp-3des esp-md5-hmac none
  in use settings = {RA, Tunnel, }
  slot: 0, conn_id: 4096, crypto-map: dynmap
  sa timing: remaining key lifetime (sec): 28314
  IV size: 8 bytes
  replay detection support: Y
```

Lo [strumento Output Interpreter](#) (solo utenti [registrati](#)) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

[Risoluzione dei problemi](#)

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Di seguito sono riportati alcuni possibili errori:

- **ERRORE: Impossibile analizzare o verificare il certificato importato**Questo errore può verificarsi quando si installa il certificato di identità e non si dispone del certificato CA intermedio o radice corretto autenticato con il trust point associato. È necessario rimuovere e rieseguire l'autenticazione con il certificato CA intermedio o radice corretto. Contattare il fornitore di terze parti per verificare di aver ricevuto il certificato CA corretto.
- **Il certificato non contiene la chiave pubblica generica**È possibile che questo errore si verifichi quando si tenta di installare il certificato di identità nel punto di attendibilità errato. Si sta tentando di installare un certificato di identità non valido oppure la coppia di chiavi associata al trust point non corrisponde alla chiave pubblica contenuta nel certificato di identità. Utilizzare il comando **show crypto ca certificates trustpointname** per verificare che il certificato di identità sia stato installato nel trust point corretto. Cercare la riga che indica i **trust point associati**: Se è elencato un trust point errato, utilizzare le procedure descritte in questo documento per rimuovere e reinstallare il trust point appropriato. Verificare inoltre che la coppia di chiavi non sia stata modificata dopo la generazione del CSR.
- **ERRORE: ASA/PIX Sev=Warning/3 IKE/0xE3000081 ID certificato remoto non valido**:Se si verificano problemi di autenticazione con i certificati, questo messaggio di errore può essere visualizzato nel client VPN. Per risolvere il problema, usare il comando **crypto isakmp identity auto** nella configurazione ASA/PIX.

[Informazioni correlate](#)

- [Pagina di supporto di Cisco Adaptive Security Appliance](#)
- [Pagina di supporto per Cisco VPN Client](#)
- [Configurazione di Microsoft Server come Autorità di certificazione \(CA \)](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)