

# Configurazione dell'autenticazione ASA AnyConnect Secure Mobility Client

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Certificato per AnyConnect](#)

[Installazione certificato su ASA](#)

[Configurazione ASA per autenticazione singola e convalida del certificato](#)

[Test](#)

[Debug](#)

[Configurazione ASA per doppia autenticazione e convalida dei certificati](#)

[Test](#)

[Debug](#)

[Configurazione ASA per doppia autenticazione e precompilazione](#)

[Test](#)

[Debug](#)

[Configurazione ASA per doppia autenticazione e mapping dei certificati](#)

[Test](#)

[Debug](#)

[Risoluzione dei problemi](#)

[Certificato valido non presente](#)

[Informazioni correlate](#)

## Introduzione

In questo documento viene descritta una configurazione per l'accesso ASA AnyConnect Secure Mobility Client che utilizza la doppia autenticazione con convalida del certificato.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di configurazione dell'interfaccia della riga di comando (CLI) ASA e configurazione VPN SSL (Secure Sockets Layer)
- Conoscenze base dei certificati X509

### Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

- Software Cisco Adaptive Security Appliance (ASA), versione 8.4 e successive

- Windows 7 con Cisco AnyConnect Secure Mobility Client 3.1

Si presume che sia stata utilizzata un'Autorità di certificazione (CA) esterna per generare:

- Certificato con codifica PKCS #12 (PKCS #12) base64 per ASA (AnyConnect.pfx)
- Certificato PKCS #12 per AnyConnect

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.

## Premesse

In questo documento viene descritto un esempio di configurazione dell'accesso Cisco AnyConnect Secure Mobility Client di Adaptive Security Appliance (ASA) con autenticazione doppia e convalida del certificato. Per poter accedere alla VPN, gli utenti AnyConnect devono fornire il certificato e le credenziali corretti per l'autenticazione primaria e secondaria. Questo documento fornisce anche un esempio di mappatura dei certificati con la funzione di precompilazione.

## Configurazione

---

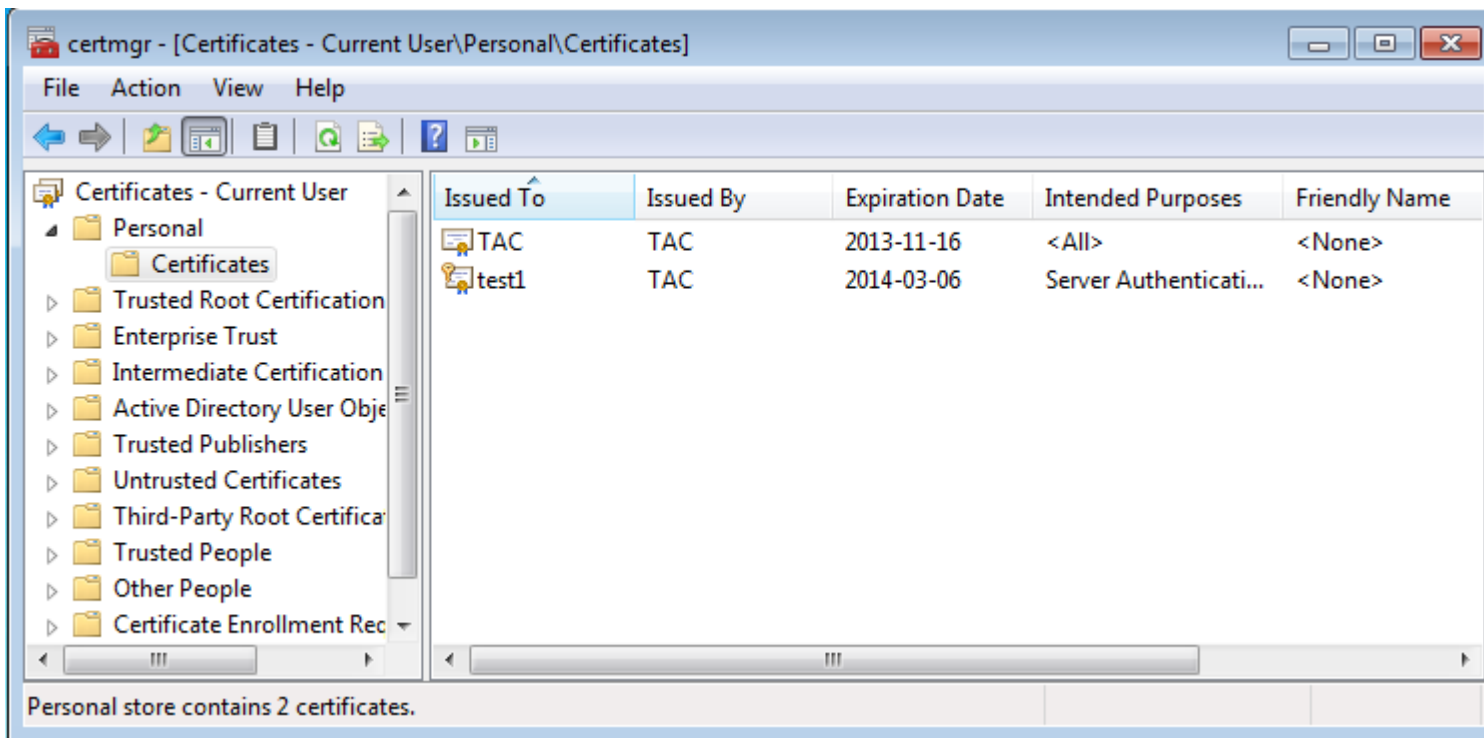
**Nota:** per ulteriori informazioni sui comandi menzionati in questa sezione, usare [lo strumento di ricerca](#) dei comandi. Solo gli utenti Cisco registrati possono accedere agli strumenti e alle informazioni interne di Cisco.

---

### Certificato per AnyConnect

Per installare un certificato di esempio, fare doppio clic sul file AnyConnect.pfx e installare il certificato come certificato personale.

Utilizzare Gestione certificati (certmgr.msc) per verificare l'installazione:



Per impostazione predefinita, AnyConnect cerca un certificato nell'archivio utenti Microsoft. Non è necessario apportare modifiche al profilo AnyConnect.

## Installazione certificato su ASA

Nell'esempio viene mostrato come importare un certificato PKCS #12 base64 da ASA:

<#root>

```
BSNS-ASA5580-40-1(config)# crypto ca import CA pkcs12 123456
```

Enter the base 64 encoded pkcs12.

End with the word "quit" on a line by itself:

```
MIIJAQIBAzCCMcGCSqGSIb3DQEHAaCCCLgEggi0MIIIsDCCBa8GCSqGSIb3DQEH
```

...

<output omitted>

...

```
83EwMTAhMAkGBSs0AwIaBQAEFCS/WBskr0IeT1HARHbLF1FFQvSvBAhu0j9bTtZo
```

```
3AICCAA=
```

```
quit
```

```
INFO: Import PKCS12 operation completed successfully
```

Utilizzare il comando **show crypto ca certificates** per verificare l'importazione:

```
BSNS-ASA5580-40-1(config)# show crypto ca certificates
```

```
CA Certificate
```

```
Status: Available
```

```
Certificate Serial Number: 00cf946de20d0ce6d9
```

```
Certificate Usage: General Purpose
```

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

Signature Algorithm: SHA1 with RSA Encryption  
Issuer Name:  
cn=TAC  
ou=RAC  
o=TAC  
l=Warsaw  
st=Maz  
c=PL  
Subject Name:  
cn=TAC  
ou=RAC  
o=TAC  
l=Warsaw  
st=Maz  
c=PL  
Validity Date:  
start date: 08:11:26 UTC Nov 16 2012  
end date: 08:11:26 UTC Nov 16 2013  
Associated Trustpoints: CA

#### Certificate

Status: Available  
Certificate Serial Number: 00fe9c3d61e131cda9  
Certificate Usage: General Purpose  
Public Key Type: RSA (1024 bits)  
Signature Algorithm: SHA1 with RSA Encryption  
Issuer Name:  
cn=TAC  
ou=RAC  
o=TAC  
l=Warsaw  
st=Maz  
c=PL  
Subject Name:  
cn=IOS  
ou=UNIT  
o=TAC  
l=Wa  
st=Maz  
c=PL  
Validity Date:  
start date: 12:48:31 UTC Nov 29 2012  
end date: 12:48:31 UTC Nov 29 2013  
Associated Trustpoints: CA

---

**Nota:** lo [strumento Output Interpreter](#) supporta alcuni comandi **show**. Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show**. Solo gli utenti Cisco registrati possono accedere agli strumenti e alle informazioni interne di Cisco.

---

## Configurazione ASA per autenticazione singola e convalida del certificato

L'appliance ASA utilizza sia l'autenticazione, l'autorizzazione e l'autenticazione di accounting (AAA) sia l'autenticazione dei certificati. La convalida del certificato è obbligatoria. L'autenticazione AAA utilizza un database locale.

In questo esempio viene illustrata l'autenticazione singola con convalida del certificato.

```
<#root>

ip local pool POOL 10.1.1.10-10.1.1.20
username cisco password cisco

webvpn
enable outside
AnyConnect image disk0:/AnyConnect-win-3.1.01065-k9.pkg 1
AnyConnect enable
tunnel-group-list enable

group-policy Group1 internal
group-policy Group1 attributes
vpn-tunnel-protocol ssl-client ssl-clientless
address-pools value POOL

tunnel-group RA type remote-access
tunnel-group RA general-attributes

  authentication-server-group LOCAL

default-group-policy Group1

authorization-required

tunnel-group RA webvpn-attributes

  authentication aaa certificate

group-alias RA enable
```

Oltre a questa configurazione, è possibile eseguire l'autorizzazione LDAP (Lightweight Directory Access Protocol) con il nome utente da un campo del certificato specifico, ad esempio il nome del certificato (CN). È quindi possibile recuperare attributi aggiuntivi e applicarli alla sessione VPN. Per ulteriori informazioni sull'autenticazione e l'autorizzazione dei certificati, consultare il documento sull'[Esempio di configurazione di ASA AnyConnect VPN e OpenLDAP con schema personalizzato e certificati](#)".

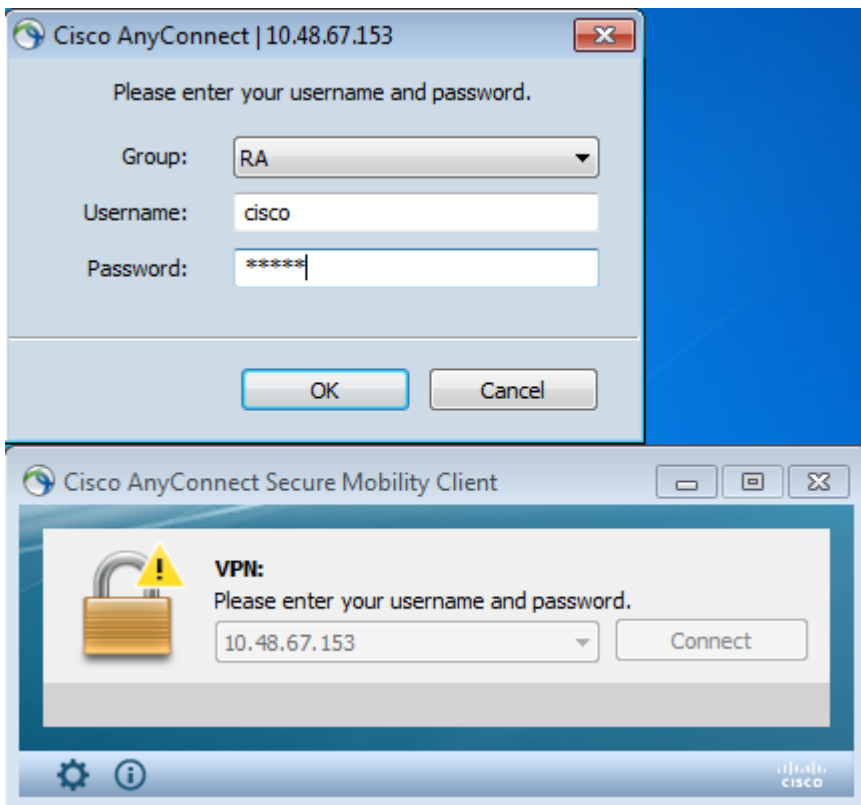
## Test

---

**Nota:** lo [strumento Output Interpreter](#) supporta alcuni comandi **show**. Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show**. Solo gli utenti Cisco registrati possono accedere agli strumenti e alle informazioni interne di Cisco.

---

Per verificare questa configurazione, fornire le credenziali locali (nome utente cisco con password cisco). Il certificato deve essere presente:



Immettere il comando **show vpn-sessiondb detail AnyConnect** sull'appliance ASA:

```
<#root>
```

```
BSNS-ASA5580-40-1(config-tunnel-general)# show vpn-sessiondb detail AnyConnect  
Session Type: AnyConnect Detailed
```

```
Username      :
```

```
cisco
```

```
Index        : 10
```

```
Assigned IP  :
```

```
10.1.1.10
```

```
Public IP    : 10.147.24.60
```

```
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
```

```
License      : AnyConnect Premium
```

```
Encryption   : RC4 AES128           Hashing      : none SHA1
```

```
Bytes Tx     : 20150                 Bytes Rx    : 25199
```

```
Pkts Tx      : 16                    Pkts Rx    : 192
```

```
Pkts Tx Drop : 0                     Pkts Rx Drop : 0
```

```
Group Policy : Group1                 Tunnel Group : RA
```

```
Login Time   : 10:16:35 UTC Sat Apr 13 2013
```

```
Duration     : 0h:01m:30s
```

```
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 : 10.1  
Public IP : 10.147.24.60  
Encryption : none  
TCP Dst Port : 443  
TCP Src Port : 62531  
Auth Mode :

**Certificate**  
and userPassword

Idle Time Out: 30 Minutes  
Client Type : AnyConnect  
Client Ver : 3.1.01065  
Bytes Tx : 10075  
Pkts Tx : 8  
Pkts Tx Drop : 0  
Idle TO Left : 28 Minutes  
Bytes Rx : 1696  
Pkts Rx : 4  
Pkts Rx Drop : 0

**SSL-Tunnel:**

Tunnel ID : 10.2  
Assigned IP : 10.1.1.10  
Encryption : RC4  
Encapsulation: TLSv1.0  
TCP Dst Port : 443  
Public IP : 10.147.24.60  
Hashing : SHA1  
TCP Src Port : 62535  
Auth Mode :

**Certificate**  
and userPassword

Idle Time Out: 30 Minutes  
Client Type : SSL VPN Client  
Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.01065  
Bytes Tx : 5037  
Pkts Tx : 4  
Pkts Tx Drop : 0  
Idle TO Left : 28 Minutes  
Bytes Rx : 2235  
Pkts Rx : 11  
Pkts Rx Drop : 0

**DTLS-Tunnel:**

Tunnel ID : 10.3  
Assigned IP : 10.1.1.10  
Encryption : AES128  
Encapsulation: DTLSv1.0  
UDP Dst Port : 443  
Public IP : 10.147.24.60  
Hashing : SHA1  
UDP Src Port : 52818  
Auth Mode :

**Certificate**  
and userPassword

Idle Time Out: 30 Minutes  
Client Type : DTLS VPN Client  
Client Ver : 3.1.01065  
Bytes Tx : 0  
Pkts Tx : 0  
Pkts Tx Drop : 0  
Idle TO Left : 29 Minutes  
Bytes Rx : 21268  
Pkts Rx : 177  
Pkts Rx Drop : 0

**NAC:**

Reval Int (T): 0 Seconds  
SQ Int (T) : 0 Seconds  
Hold Left (T): 0 Seconds  
Redirect URL :  
Reval Left(T): 0 Seconds  
EoU Age(T) : 92 Seconds  
Posture Token:

**Debug**

---

**Nota:** consultare le [informazioni importanti sui comandi di debug](#) prima di usare i comandi di **debug**.

---

In questo esempio, il certificato non è stato memorizzato nella cache del database, è stata trovata una CA corrispondente, è stato utilizzato l'utilizzo corretto della chiave (ClientAuthentication) e il certificato è stato convalidato:

```
<#root>
```

```
debug aaa authentication
debug aaa authorization
debug webvpn 255
```

```
debug webvpn AnyConnect 255
```

```
debug crypto ca 255
```

I comandi di debug dettagliati, come il comando **debug webvpn 255**, possono generare molti log in un ambiente di produzione e sottoporre un'ASA a un carico elevato. Alcuni debug WebVPN sono stati rimossi per maggiore chiarezza:

```
<#root>
```

```
CERT_API: Authenticate session 0x0934d687, non-blocking cb=0x0000000012cfc50
CERT_API thread wakes up!
CERT_API: process msg cmd=0, session=0x0934d687
CERT_API: Async locked for session 0x0934d687
CRYPTO_PKI:
```

```
Checking to see if an identical cert is
```

```
already in the database
```

```
...
CRYPTO_PKI: looking for cert in handle=0x00007ffd8b80ee90, digest=
ad 3d a2 da 83 19 e0 ee d9 b5 2a 83 5c dd e0 70 | .=.....*.\..p
CRYPTO_PKI: Cert record not found, returning E_NOT_FOUND
CRYPTO_PKI:
```

```
Cert not found in database
```

```
.
CRYPTO_PKI:
```

```
Looking for suitable trustpoints
```

```
...
CRYPTO_PKI: Storage context locked by thread CERT_API
CRYPTO_PKI:
```

```
Found a suitable authenticated trustpoint CA
```

```
.
CRYPTO_PKI(make trustedCerts list)CRYPTO_PKI:check_key_usage: ExtendedKeyUsage
OID = 1.3.6.1.5.5.7.3.1
CRYPTO_PKI:
```



check\_key\_usage:Key Usage check OK

CRYPTO\_PKI:

Certificate validation: Successful, status: 0

. Attempting to

retrieve revocation status if necessary

CRYPTO\_PKI:Certificate validated. serial number: 00FE9C3D61E131CDB1, subject name: cn=test1,ou=Security,o=Cisco,l=Krakow,st=PL,c=PL.

CRYPTO\_PKI: Storage context released by thread CERT API

CRYPTO\_PKI: Certificate validated without revocation check

Tentativo di trovare un gruppo di tunnel corrispondente. Non esistono regole di mapping dei certificati specifiche e viene utilizzato il gruppo di tunnel specificato:

<#root>

CRYPTO\_PKI: Attempting to find tunnel group for cert with serial number:

00FE9C3D61E131CDB1, subject name: cn=test1,ou=Security,o=Cisco,l=Krakow,st=PL, c=PL, issuer\_name: cn=TAC,ou=RAC,o=TAC,l=Warsaw,st=Maz,c=PL.

CRYPTO\_PKI:

No Tunnel Group Match for peer certificate

.  
CERT\_API: Unable to find tunnel group for cert using rules (SSL)

Di seguito sono riportati i debug SSL e della sessione generale:

<#root>

%ASA-7-725012: Device chooses cipher : RC4-SHA for the SSL session with client outside:10.147.24.60/64435

%ASA-7-717025:

Validating certificate chain containing 1 certificate(s).

%ASA-7-717029:

Identified client certificate

within certificate chain. serial number: 00FE9C3D61E131CDB1, subject name:

cn=test1,ou=Security,o=Cisco,l=Krakow, st=PL,c=PL

.  
%ASA-7-717030:

Found a suitable trustpoint CA to validate certificate

.  
%ASA-6-717022:

Certificate was successfully validated

```

. serial number:
00FE9C3D61E131CDB1, subject name: cn=test1,ou=Security,o=Cisco,l=Krakow,st=PL,
c=PL.
%ASA-6-717028: Certificate chain was successfully validated with warning,
revocation status was not checked.
%ASA-6-725002: Device completed SSL handshake with client outside:
10.147.24.60/64435
%ASA-7-717036:

Looking for a tunnel group match based on certificate maps

for
peer certificate with serial number: 00FE9C3D61E131CDB1, subject name: cn=test1,
ou=Security,o=Cisco,l=Krakow,st=PL,c=PL, issuer_name: cn=TAC,ou=RAC,o=TAC,
l=Warsaw,st=Maz,c=PL.
%ASA-4-717037:

Tunnel group search using certificate maps failed for peer
certificate

: serial number: 00FE9C3D61E131CDB1, subject name: cn=test1,
ou=Security,o=Cisco,l=Krakow,st=PL,c=PL, issuer_name: cn=TAC,ou=RAC,o=TAC,
l=Warsaw,st=Maz,c=PL.
%ASA-6-113012:

AAA user authentication Successful : local database : user = cisco

%ASA-6-113009:

AAA retrieved default group policy (Group1) for user = cisco

%ASA-6-113008: AAA transaction status ACCEPT : user = cisco
%ASA-7-734003: DAP: User cisco, Addr 10.147.24.60:
Session Attribute aaa.cisco.grouppolicy = Group1
%ASA-7-734003: DAP: User cisco, Addr 10.147.24.60:
Session Attribute aaa.cisco.username = cisco
%ASA-7-734003: DAP: User cisco, Addr 10.147.24.60:
Session Attribute aaa.cisco.username1 = cisco
%ASA-7-734003: DAP: User cisco, Addr 10.147.24.60:
Session Attribute aaa.cisco.username2 =
%ASA-7-734003: DAP: User cisco, Addr 10.147.24.60:
Session Attribute aaa.cisco.tunnelgroup = RA
%ASA-6-734001: DAP: User cisco, Addr 10.147.24.60, Connection AnyConnect: The
following DAP records were selected for this connection: DfltAccessPolicy
%ASA-6-113039: Group <Group1> User <cisco> IP <10.147.24.60> AnyConnect parent
session started.

```

## **Configurazione ASA per doppia autenticazione e convalida dei certificati**

Questo è un esempio di doppia autenticazione, in cui il server di autenticazione primario è LOCAL e il server di autenticazione secondario è LDAP. La convalida del certificato è ancora abilitata.

L'esempio mostra la configurazione LDAP:

```

aaa-server LDAP protocol ldap
aaa-server LDAP (outside) host 10.147.24.60
ldap-base-dn DC=test-cisco,DC=com

```

```
ldap-scope subtree
ldap-naming-attribute uid
ldap-login-password *****
ldap-login-dn CN=Manager,DC=test-cisco,DC=com
server-type openldap
```

Di seguito è riportato l'aggiunta di un server di autenticazione secondario:

```
<#root>
```

```
tunnel-group RA general-attributes
```

```
authentication-server-group LOCAL
secondary-authentication-server-group LDAP
```

```
default-group-policy Group1
```

```
authorization-required
```

```
tunnel-group RA webvpn-attributes
```

```
authentication aaa certificate
```

'authentication-server-group LOCAL' non visualizzato nella configurazione perché è un'impostazione predefinita.

Per 'authentication-server-group' è possibile usare qualsiasi altro server AAA. Per il 'gruppo-server-autenticazione-secondaria', è possibile utilizzare tutti i server AAA ad eccezione di un server Security Dynamics International (SDI); in tal caso, l'SDI potrebbe ancora essere il server di autenticazione primario.

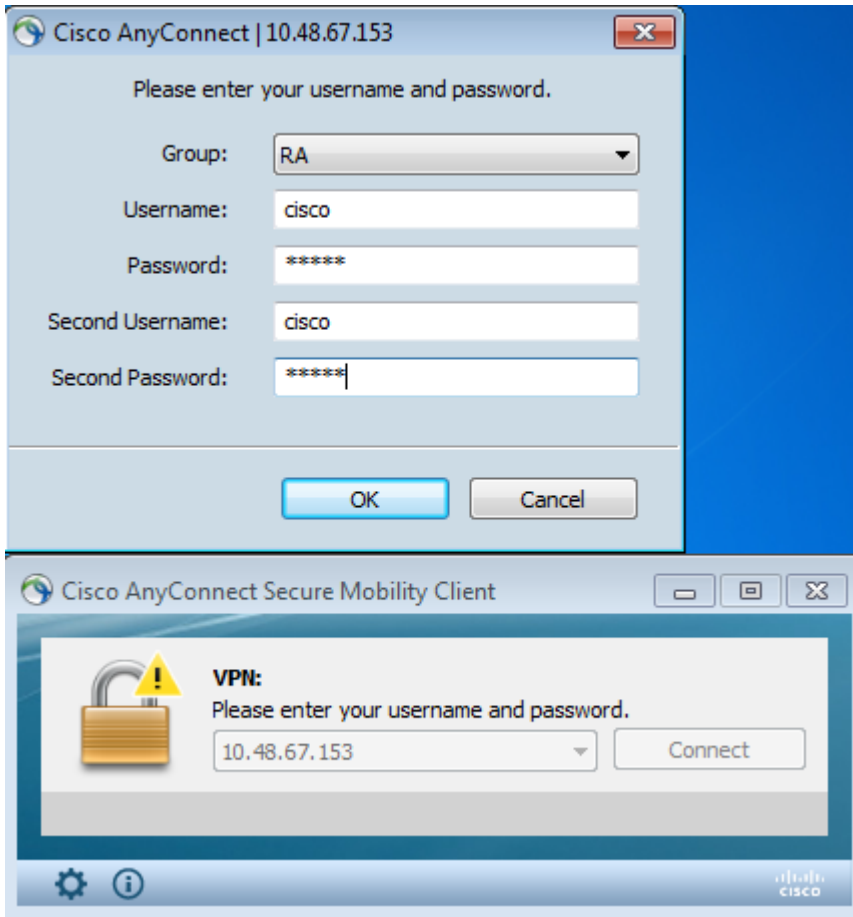
## Test

---

**Nota:** lo [strumento Output Interpreter](#) supporta alcuni comandi **show**. Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show**. Solo gli utenti Cisco registrati possono accedere agli strumenti e alle informazioni interne di Cisco.

---

Per verificare questa configurazione, fornire le credenziali locali (nome utente cisco con password cisco) e le credenziali LDAP (nome utente cisco con password LDAP). Il certificato deve essere presente:



Immettere il comando **show vpn-sessiondb detail AnyConnect** sull'appliance ASA.

I risultati sono simili a quelli relativi all'autenticazione singola. Fare riferimento alla sezione ["Configurazione ASA per autenticazione singola e convalida certificato, test"](#).

## Debug

I debug per la sessione WebVPN e l'autenticazione sono simili. Fare riferimento alla sezione ["Configurazione ASA per autenticazione singola e convalida del certificato, debug"](#). Viene visualizzato un ulteriore processo di autenticazione:

```
<#root>
```

```
%ASA-6-113012:
```

```
AAA user authentication Successful : local database : user = cisco
```

```
%ASA-6-302013: Built outbound TCP connection 1936 for outside:10.147.24.60/389  
(10.147.24.60/389) to identity:10.48.67.153/54437 (10.48.67.153/54437)
```

```
%ASA-6-113004:
```

```
AAA user authentication Successful : server = 10.147.24.60 :  
user = cisco
```

```
%ASA-6-113009: AAA retrieved default group policy (Group1) for user = cisco
```

```
%ASA-6-113008: AAA transaction status ACCEPT : user = cisco
```

I debug per LDAP mostrano dettagli che possono variare in base alla configurazione LDAP:

```
[34] Session Start
[34] New request Session, context 0x00007ffd8d7dd828, reqType = Authentication
[34] Fiber started
[34] Creating LDAP context with uri=ldap://10.147.24.60:389
[34] Connect to LDAP server: ldap://10.147.24.60:389, status = Successful
[34] supportedLDAPVersion: value = 3
[34] Binding as Manager
[34] Performing Simple authentication for Manager to 10.147.24.60
[34] LDAP Search:
      Base DN = [DC=test-cisco,DC=com]
      Filter  = [uid=cisco]
      Scope   = [SUBTREE]
[34] User DN = [uid=cisco,ou=People,dc=test-cisco,dc=com]
[34] Server type for 10.147.24.60 unknown - no password policy
[34] Binding as cisco
[34] Performing Simple authentication for cisco to 10.147.24.60
[34] Processing LDAP response for user cisco
[34] Authentication successful for cisco to 10.147.24.60
[34] Retrieved User Attributes:
[34]   cn: value = John Smith
[34]   givenName: value = John
[34]   sn: value = cisco
[34]   uid: value = cisco
[34]   uidNumber: value = 10000
[34]   gidNumber: value = 10000
[34]   homeDirectory: value = /home/cisco
[34]   mail: value = name@dev.local
[34]   objectClass: value = top
[34]   objectClass: value = posixAccount
[34]   objectClass: value = shadowAccount
[34]   objectClass: value = inetOrgPerson
[34]   objectClass: value = organizationalPerson
[34]   objectClass: value = person
[34]   objectClass: value = CiscoPerson
[34]   loginShell: value = /bin/bash
[34]   userPassword: value = {SSHA}pndf5sfjscTPuyrhL+/QUqhK+i1UCUTy
[34] Fiber exit Tx=315 bytes Rx=911 bytes, status=1
[34] Session End
```

## Configurazione ASA per doppia autenticazione e precompilazione

È possibile mappare determinati campi del certificato al nome utente utilizzato per l'autenticazione primaria e secondaria:

```
<#root>
```

```
username test1 password cisco
```

```
tunnel-group RA general-attributes
```

```
  authentication-server-group LOCAL
```

`secondary-authentication-server-group LDAP`

`default-group-policy Group1`  
`authorization-required`

`username-from-certificate CN`

`secondary-username-from-certificate OU`

`tunnel-group RA webvpn-attributes`  
`authentication aaa certificate`

`pre-fill-username ssl-client`

`secondary-pre-fill-username ssl-client`

`group-alias RA enable`

In questo esempio, il client utilizza il certificato: `cn=test1,ou=Security,o=Cisco,l=Cracovia,st=PL,c=PL`.

Per l'autenticazione primaria, il nome utente viene ricavato dalla CN, motivo per cui è stato creato l'utente locale 'test1'.

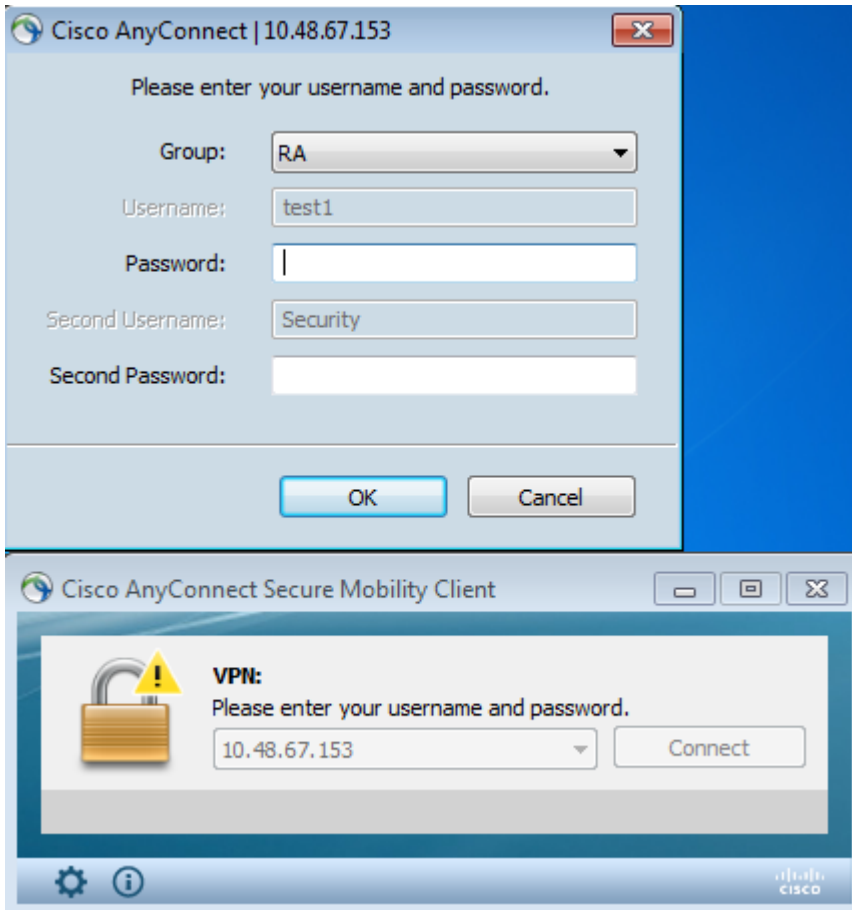
Per l'autenticazione secondaria, il nome utente viene ricavato dall'unità organizzativa (OU), motivo per cui sul server LDAP è stata creata l'opzione di protezione utente.

Inoltre, è possibile forzare AnyConnect a usare i comandi di precompilazione per precompilare il nome utente principale e secondario.

In uno scenario reale, il server di autenticazione primario è in genere un server AD o LDAP, mentre il server di autenticazione secondario è il server Rivest, Shamir e Adelman (RSA) che utilizza password token. In questo scenario, l'utente deve fornire credenziali AD/LDAP (note all'utente), una password token RSA (di cui l'utente dispone) e un certificato (sul computer utilizzato).

## **Test**

Si noti che non è possibile modificare il nome utente primario o secondario perché è precompilato dai campi CN e OU del certificato:



## Debug

Nell'esempio viene mostrata la richiesta di precompilazione inviata ad AnyConnect:

```
%ASA-7-113028: Extraction of username from VPN client certificate has been requested. [Request 5]
%ASA-7-113028: Extraction of username from VPN client certificate has started. [Request 5]
%ASA-7-113028: Extraction of username from VPN client certificate has finished successfully. [Request 5]
%ASA-7-113028: Extraction of username from VPN client certificate has completed. [Request 5]
%ASA-7-113028: Extraction of username from VPN client certificate has been requested. [Request 6]
%ASA-7-113028: Extraction of username from VPN client certificate has started. [Request 6]
%ASA-7-113028: Extraction of username from VPN client certificate has finished successfully. [Request 6]
%ASA-7-113028: Extraction of username from VPN client certificate has completed. [Request 6]
```

Nell'esempio, l'autenticazione utilizza i nomi utente corretti:

```
<#root>
```

```
%ASA-6-113012:
```

```
AAA user authentication Successful : local database : user = test1
```

```
%ASA-6-302013: Built outbound TCP connection 2137 for outside:10.147.24.60/389  
(10.147.24.60/389) to identity:10.48.67.153/46606 (10.48.67.153/46606)  
%ASA-6-113004:
```

```
AAA user authentication Successful : server = 10.147.24.60 :  
user = Security
```

## Configurazione ASA per doppia autenticazione e mapping dei certificati

È inoltre possibile mappare certificati client specifici a gruppi di tunnel specifici, come mostrato nell'esempio seguente:

```
crypto ca certificate map CERT-MAP 10  
  issuer-name co tac
```

```
webvpn  
  certificate-group-map CERT-MAP 10 RA
```

In questo modo, tutti i certificati utente firmati dall'autorità di certificazione Cisco Technical Assistance Center (TAC) vengono mappati a un gruppo di tunnel denominato 'RA'.

---

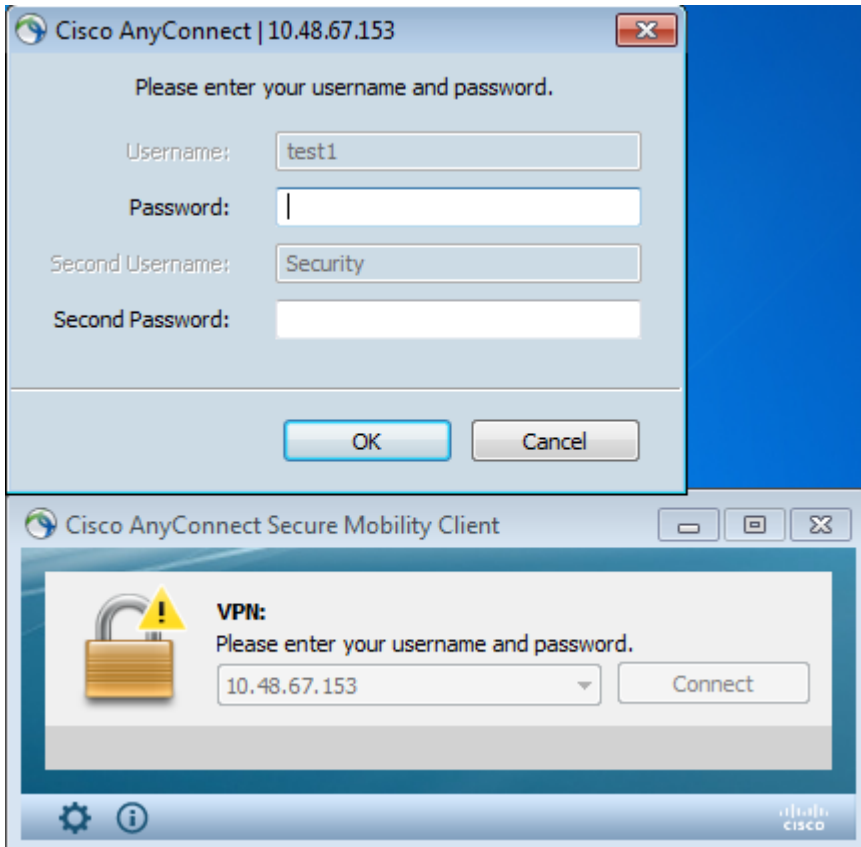
**Nota:** il mapping dei certificati per SSL è configurato in modo diverso rispetto al mapping dei certificati per IPsec. Per IPsec, è configurato con le regole 'tunnel-group-map' nella modalità di configurazione globale. Per SSL, è configurato con 'certificate-group-map' nella modalità di configurazione webvpn.

---

## Test

Una volta abilitato il mapping dei certificati, non è più necessario scegliere un gruppo di tunnel:





## Debug

In questo esempio, la regola di mapping dei certificati consente di trovare il gruppo di tunnel:

```
<#root>
```

```
%ASA-7-717036:
```

```
Looking for a tunnel group match based on certificate maps
```

```
for
```

```
peer certificate with serial number: 00FE9C3D61E131CDB1, subject name: cn=test1,  
ou=Security,o=Cisco,l=Krakow,st=PL,c=PL, issuer_name: cn=TAC,ou=RAC,o=TAC,  
l=Warsaw,st=Maz,c=PL.
```

```
%ASA-7-717038:
```

```
Tunnel group match found. Tunnel Group: RA
```

```
, Peer certificate:
```

```
serial number: 00FE9C3D61E131CDB1, subject name: cn=test1,ou=Security,o=Cisco,  
l=Krakow,st=PL,c=PL, issuer_name: cn=TAC,ou=RAC,o=TAC,l=Warsaw,st=Maz,c=PL.
```

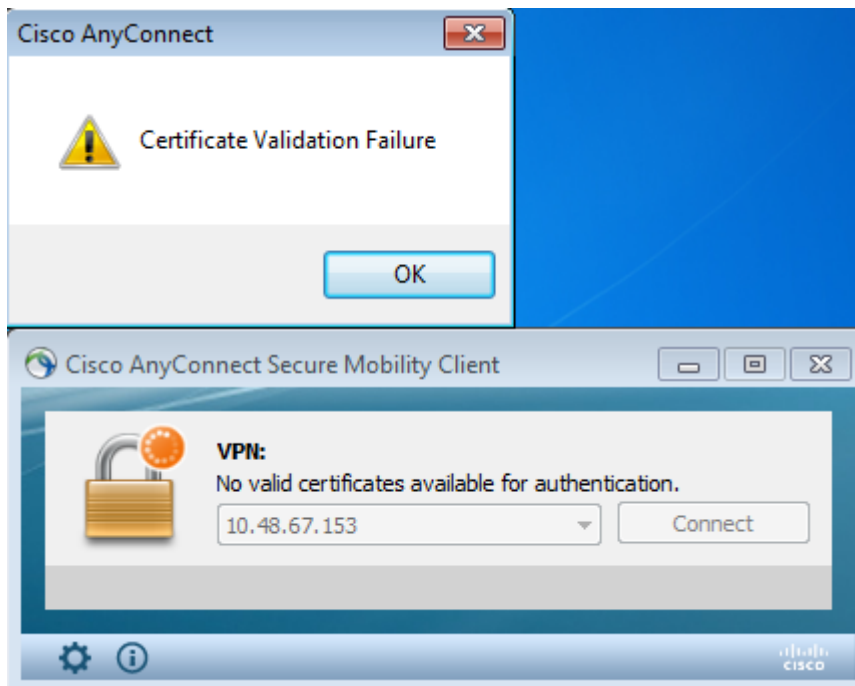
## Risoluzione dei problemi

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

### Certificato valido non presente

Dopo aver rimosso un certificato valido da Windows7, AnyConnect non riesce a trovare alcun certificato

valido:



Sull'appliance ASA, la sessione sembra essere terminata dal client (Reset-I):

<#root>

```
%ASA-6-302013: Built inbound TCP connection 2489 for outside:10.147.24.60/52838
(10.147.24.60/52838) to identity:10.48.67.153/443 (10.48.67.153/443)
%ASA-6-725001: Starting SSL handshake with client outside:10.147.24.60/52838 for
TLSv1 session.
%ASA-7-725010: Device supports the following 4 cipher(s).
%ASA-7-725011: Cipher[1] : RC4-SHA
%ASA-7-725011: Cipher[2] : AES128-SHA
%ASA-7-725011: Cipher[3] : AES256-SHA
%ASA-7-725011: Cipher[4] : DES-CBC3-SHA
%ASA-7-725008: SSL client outside:10.147.24.60/52838 proposes the following 8
cipher(s).
%ASA-7-725011: Cipher[1] : AES128-SHA
%ASA-7-725011: Cipher[2] : AES256-SHA
%ASA-7-725011: Cipher[3] : RC4-SHA
%ASA-7-725011: Cipher[4] : DES-CBC3-SHA
%ASA-7-725011: Cipher[5] : DHE-DSS-AES128-SHA
%ASA-7-725011: Cipher[6] : DHE-DSS-AES256-SHA
%ASA-7-725011: Cipher[7] : EDH-DSS-DES-CBC3-SHA
%ASA-7-725011: Cipher[8] : RC4-MD5
%ASA-7-725012: Device chooses cipher : RC4-SHA for the SSL session with client
outside:10.147.24.60/52838
%ASA-6-302014:

Teardown TCP connection 2489 for outside:10.147.24.60/52838 to
identity:10.48.67.153/443 duration 0:00:00 bytes 1448 TCP Reset-I
```

## Informazioni correlate

- [Configura gruppi di tunnel, criteri di gruppo e utenti: Configura doppia autenticazione](#)

- [Configurazione di un server esterno per l'autorizzazione utente di Security Appliance](#)
- [Supporto tecnico e download Cisco](#)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).