Configurazione di AnyConnect Secure Mobility Client con split tunneling su una ASA

Sommario

Introduzione

In questo documento viene descritto come configurare Cisco AnyConnect Secure Mobility Client tramite Cisco Adaptive Security Device Manager (ASDM) su una appliance Cisco Adaptive Security (ASA) con software versione 9.3(2).

Prerequisiti

Requisiti

Il pacchetto di distribuzione Web di Cisco AnyConnect Secure Mobility Client deve essere scaricato sul desktop locale da cui è presente l'accesso ASDM all'appliance ASA. Per scaricare il pacchetto client, consultare la pagina Web Cisco AnyConnect Secure Mobility Client. I pacchetti di distribuzione Web per vari sistemi operativi (OS) possono essere caricati sull'ASA contemporaneamente.

Questi sono i nomi dei file di distribuzione Web per i vari sistemi operativi:

- **Sistemi operativi Microsoft Windows** - *AnyConnect-win-<versione>-k9.pkg*

- **Sistemi operativi Macintosh (MAC)** - *AnyConnect-macosx-i386-<versione>-k9.pkg*
- **Sistemi operativi Linux** - *AnyConnect-linux-<versione>-k9.pkg*

Componenti usati

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

- ASA versione 9.3(2)
- ASDM versione 7.3(1)101
- AnyConnect versione 3.1

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 illustrato come usare la Configurazione guidata Cisco AnyConnect tramite ASDM per configurare il client AnyConnect e abilitare il tunneling suddiviso.

Il tunneling ripartito è usato negli scenari in cui solo il traffico specifico deve essere tunneling, al contrario degli scenari in cui tutto il traffico generato dal client passa attraverso la VPN quando connesso. Per impostazione predefinita, l'uso della Configurazione guidata AnyConnect determina una configurazione *completa* dell'appliance ASA. Il tunneling ripartito deve essere configurato separatamente, come spiegato più in dettaglio nella sezione di questo documento.

Nell'esempio di configurazione, l'intenzione è inviare il traffico per la subnet 10.10.10.0/24, che è la subnet LAN dietro l'ASA, attraverso il tunnel VPN e tutto il resto del traffico proveniente dal computer client viene inoltrato attraverso il proprio circuito Internet.

Informazioni sulla licenza AnyConnect

Di seguito sono riportati alcuni collegamenti a informazioni utili sulle licenze Cisco AnyConnect Secure Mobility Client:

- Per determinare le licenze necessarie per AnyConnect Secure Mobility Client e le funzionalità correlate, consultare il documento AnyConnect Secure Mobility Client Features, Licenze e sistemi operativi versione 3.1.
- Per informazioni sulle licenze AnyConnect Apex e Plus, consultare la Guida agli ordini di Cisco AnyConnect.
- Per ulteriori informazioni, consultare il documento sulla licenza ASA richiesta per le connessioni IP Phone e VPN per dispositivi mobili? nel presente documento vengono fornite

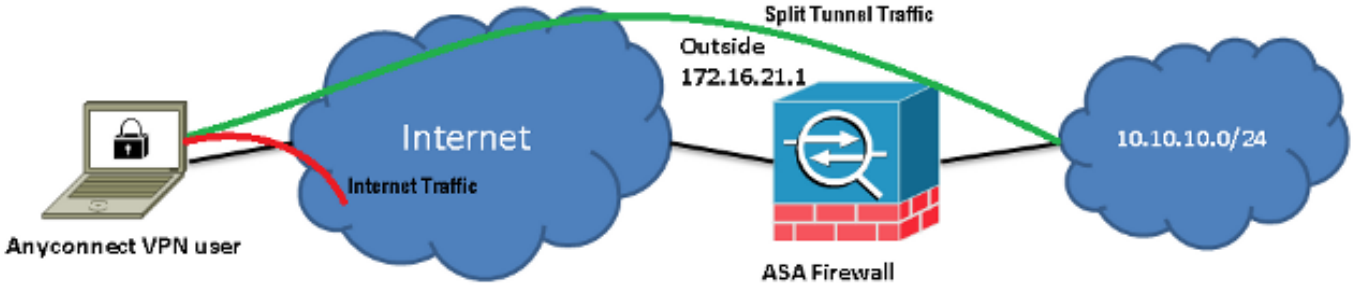
informazioni sui requisiti di licenza aggiuntivi per le connessioni telefoniche e mobili IP.

Configurazione

In questa sezione viene descritto come configurare Cisco AnyConnect Secure Mobility Client sull'appliance ASA.

Esempio di rete

Questa è la topologia utilizzata per gli esempi riportati nel presente documento:

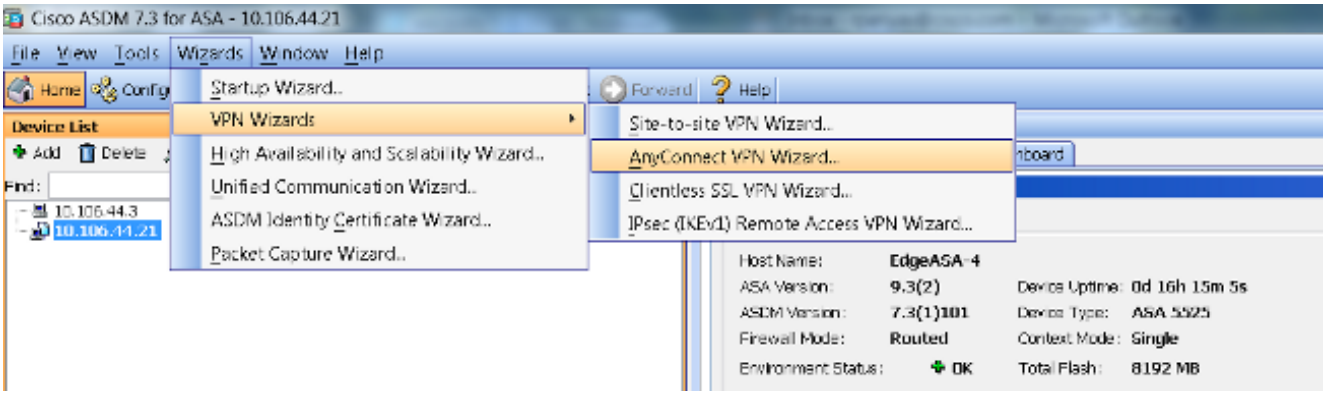


Configurazione guidata AnyConnect ASDM

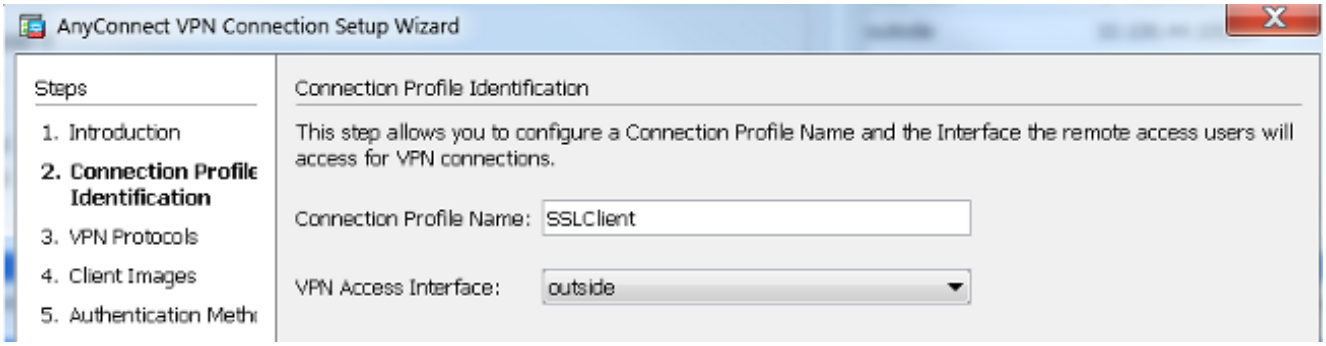
La configurazione guidata AnyConnect può essere usata per configurare il client AnyConnect Secure Mobility. Prima di procedere, verificare che un pacchetto client AnyConnect sia stato caricato nella memoria flash/sul disco del firewall ASA.

Per configurare AnyConnect Secure Mobility Client tramite la Configurazione guidata, completare la procedura seguente:

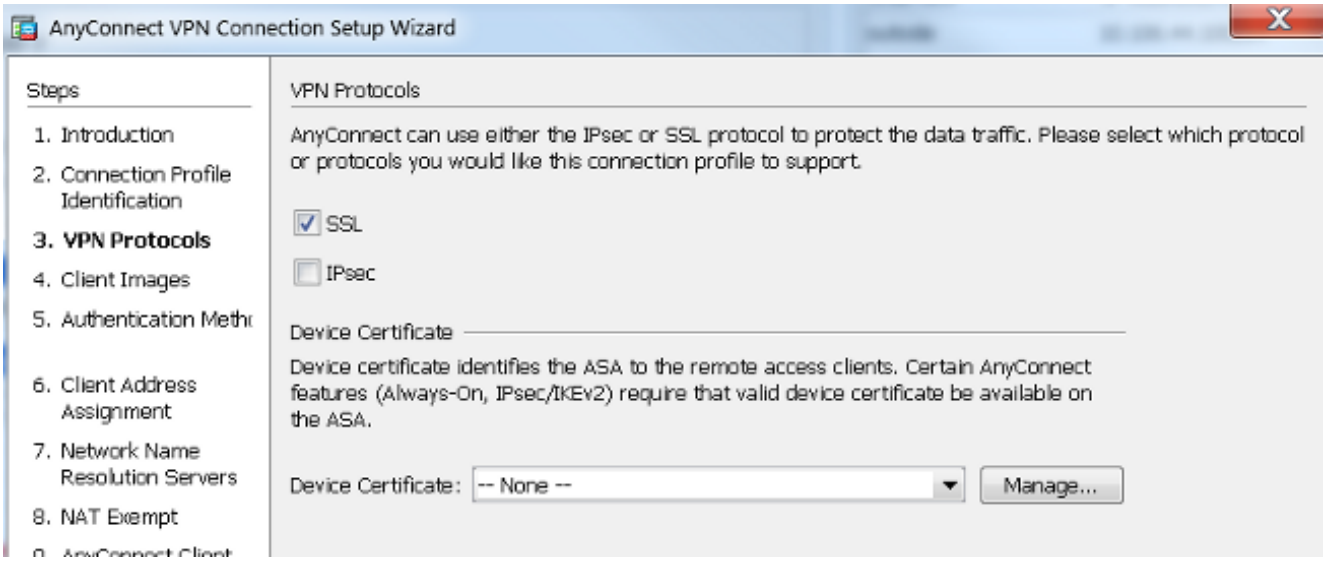
1. Accedere ad ASDM, avviare la **Configurazione guidata** e fare clic su **Avanti**:



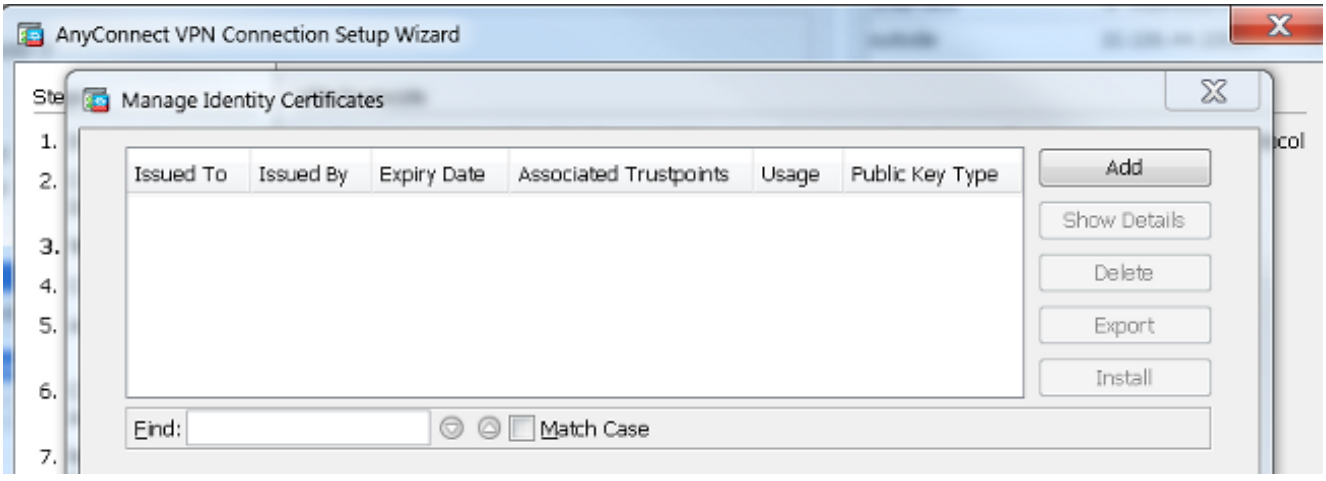
2. Immettere il *nome* del *profilo di connessione*, scegliere l'interfaccia su cui terminare la VPN dal menu a discesa *VPN Access Interface* (Interfaccia di accesso VPN) e fare clic su **Avanti**:



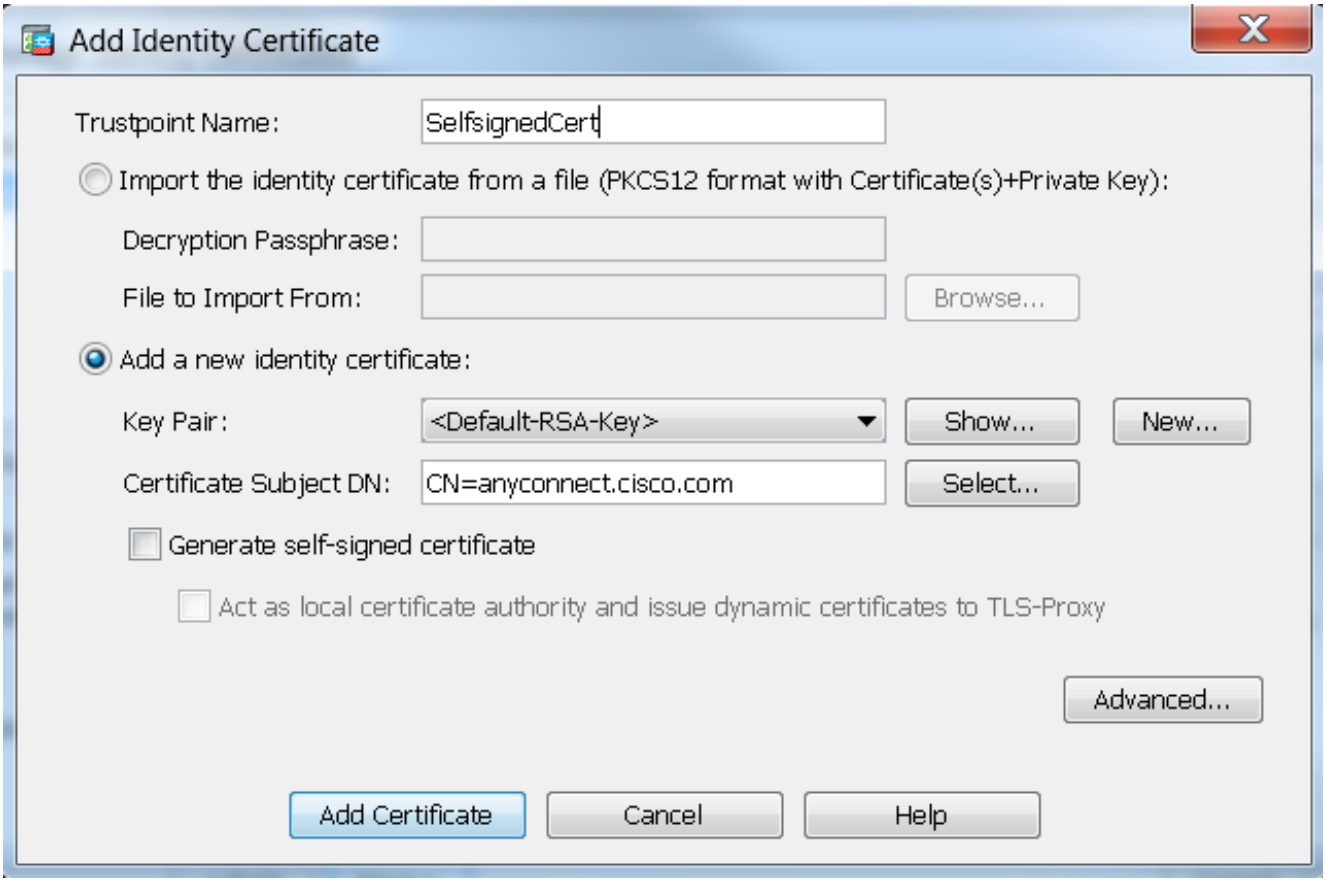
3. Per abilitare SSL (Secure Sockets Layer), selezionare la casella di controllo **SSL**. Il *certificato del dispositivo* può essere un certificato rilasciato da un'Autorità di certificazione (CA) di terze parti attendibile, ad esempio Verisign o Entrust, oppure un certificato autofirmato. Se il certificato è già installato sull'appliance ASA, può essere scelto dal menu a discesa. **Nota:** Questo certificato è il certificato lato server che verrà fornito. Se sull'appliance ASA non è installato alcun certificato ed è necessario generare un certificato autofirmato, fare clic su **Gestisci**.Per installare un certificato di terze parti, completare la procedura descritta nell'ASA 8.x Installazione manuale dei certificati dei fornitori di terze parti da utilizzare con la configurazione di WebVPN nel documento Cisco.



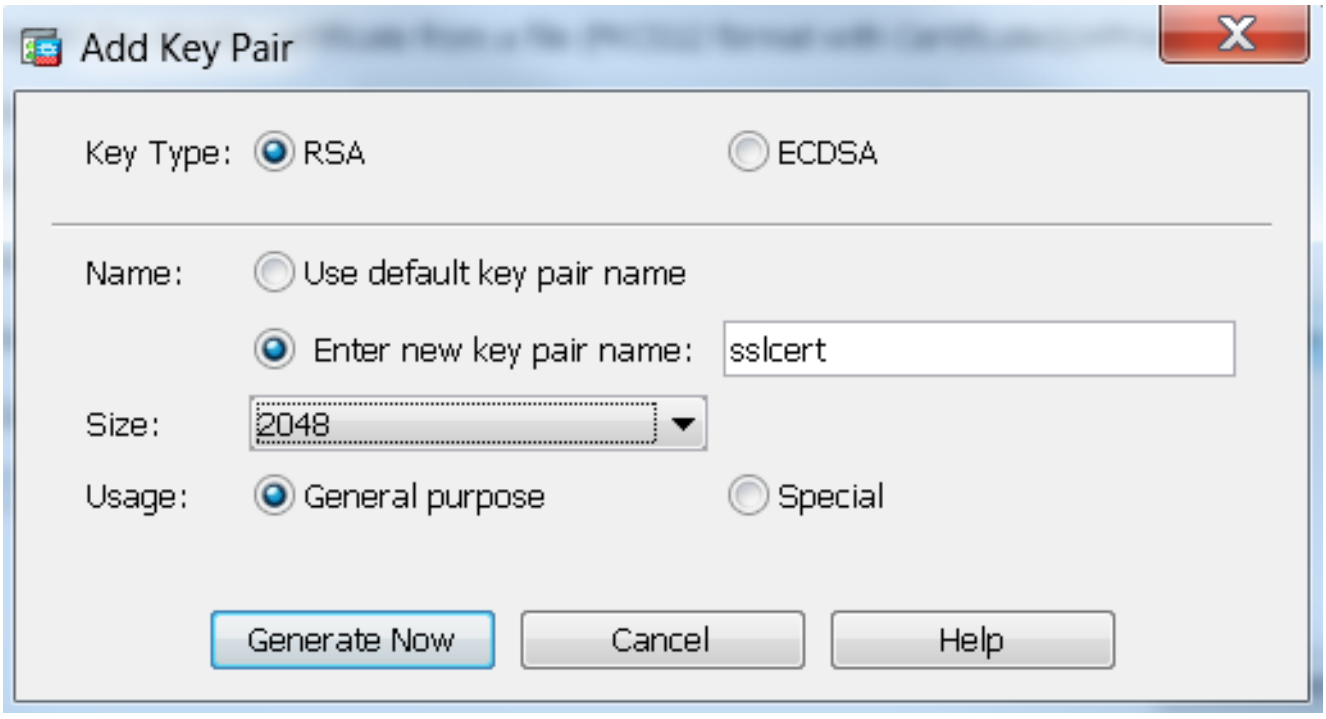
4. Fare clic su **Aggiungi**:



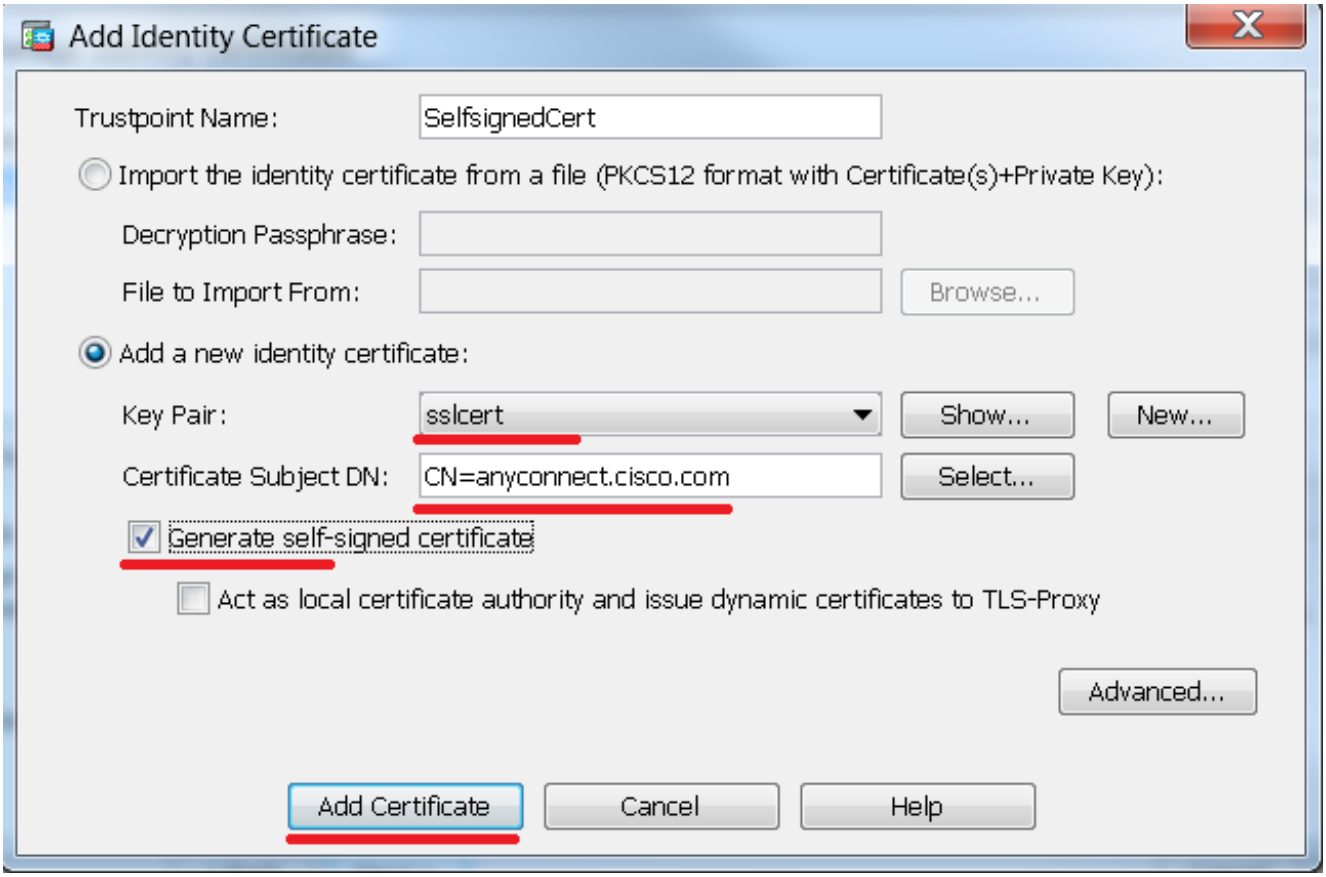
5. Digitare un nome appropriato nel campo *Nome trust* e fare clic sul pulsante di opzione **Aggiungi nuovo certificato di identità**. Se sul dispositivo non sono presenti coppie di chiavi Rivest-Shamir-Addleman (RSA), fare clic su **New (Nuovo)** per generarne una:



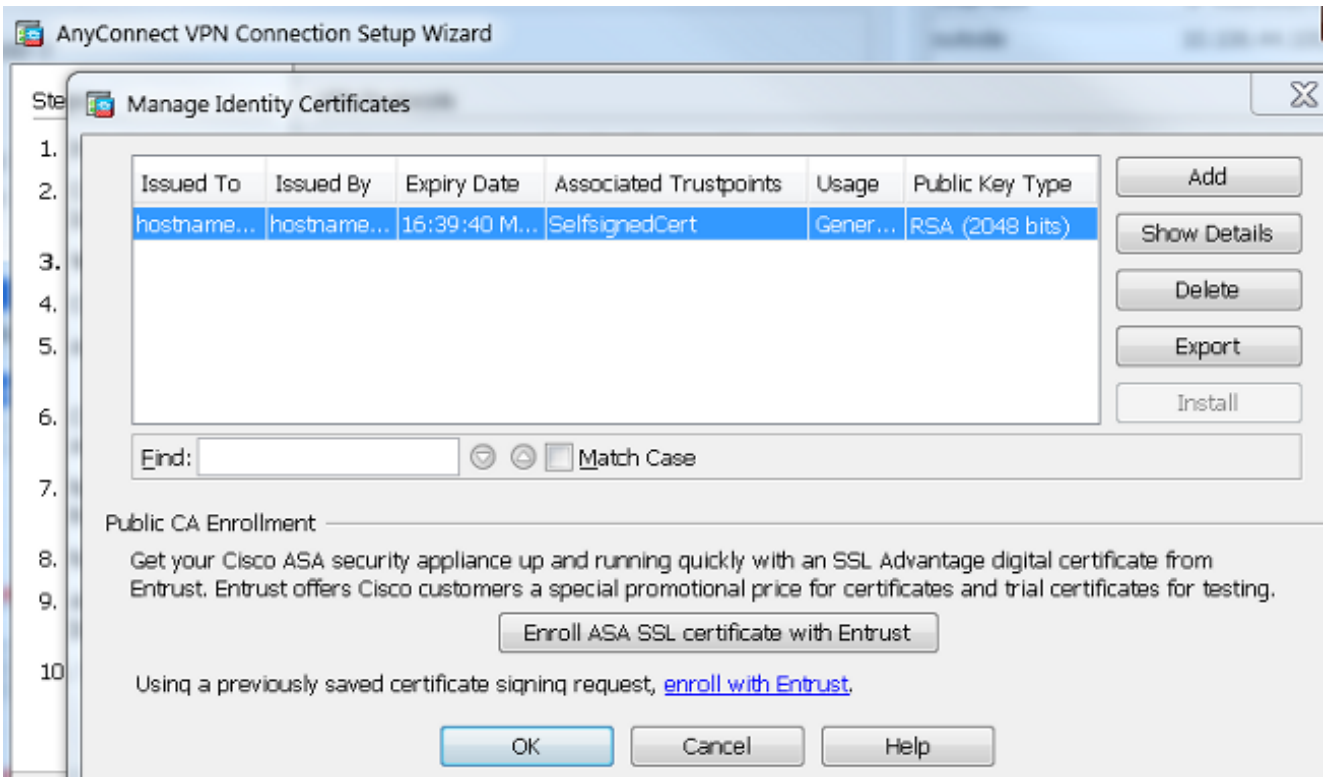
6. Fare clic sul pulsante di scelta **Usa nome coppia di chiavi predefinita** oppure sul pulsante di scelta **Immettere il nuovo nome della coppia di chiavi** e immettere un nuovo nome. Selezionare le dimensioni delle chiavi e quindi fare clic su **Genera ora**:



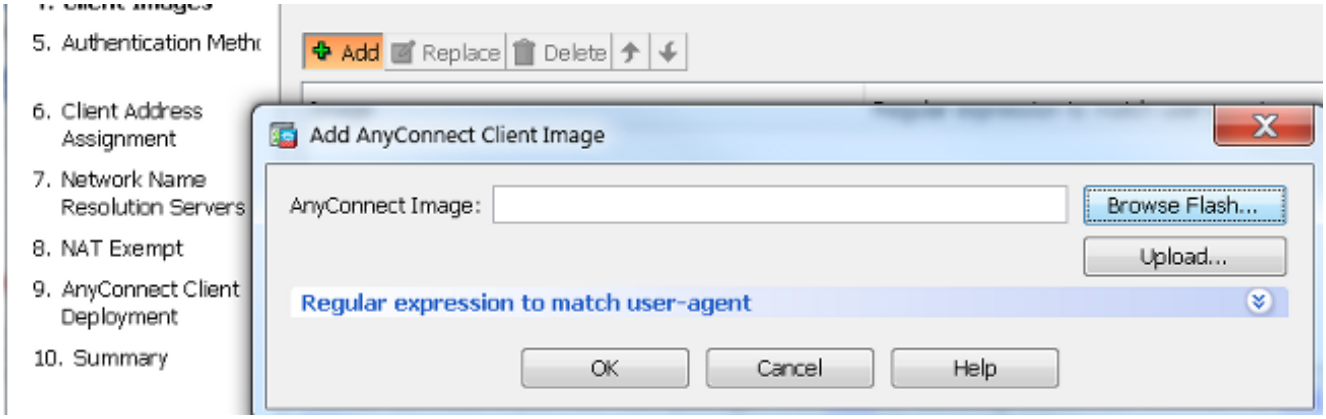
7. Dopo aver generato la coppia di chiavi RSA, scegliere la chiave e selezionare la casella di controllo **Generate self-signed certificate** (Genera certificato autofirmato). Immettere il nome di dominio (DN) del soggetto desiderato nel campo *DN soggetto certificato*, quindi fare clic su **Aggiungi certificato**:

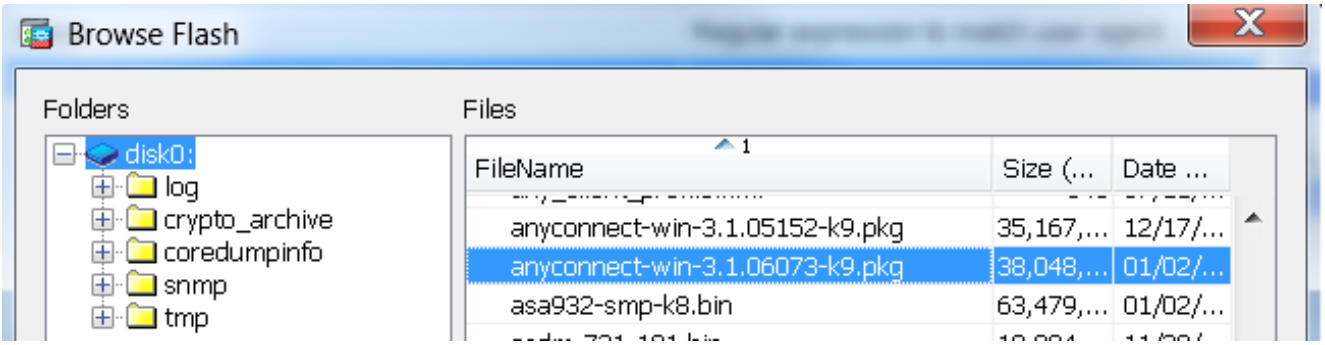


8. Al termine dell'iscrizione, fare clic su **OK**, **OK** e quindi su **Avanti**:

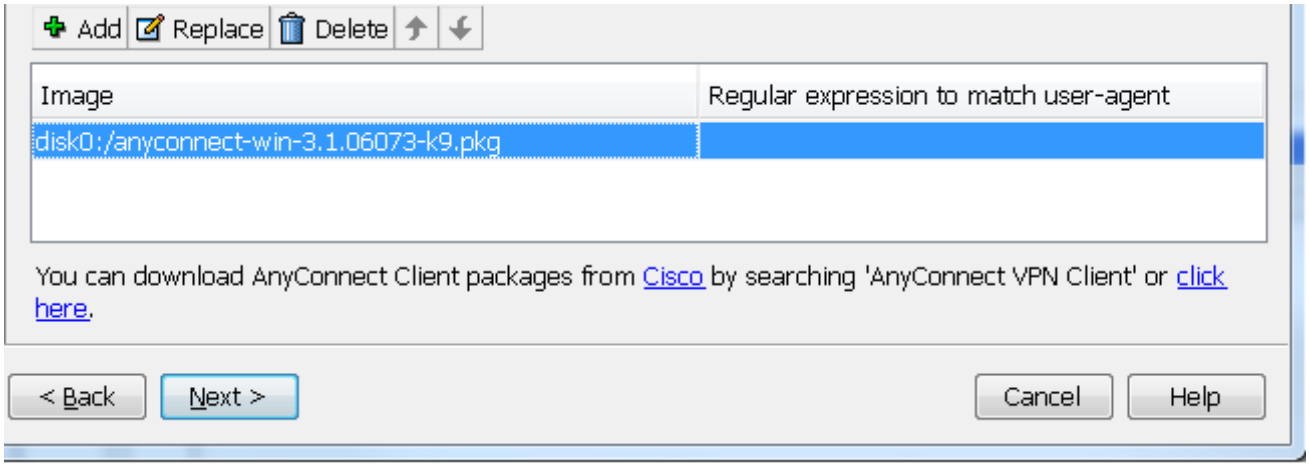


9. Per aggiungere l'immagine del client AnyConnect (il file *.pkg*) dal PC o dalla memoria flash, fare clic su **Add** (Aggiungi). Fare clic su **Browse Flash** (Sfoglia flash) per aggiungere l'immagine dall'unità flash oppure fare clic su **Upload** per aggiungere l'immagine direttamente dal computer host:

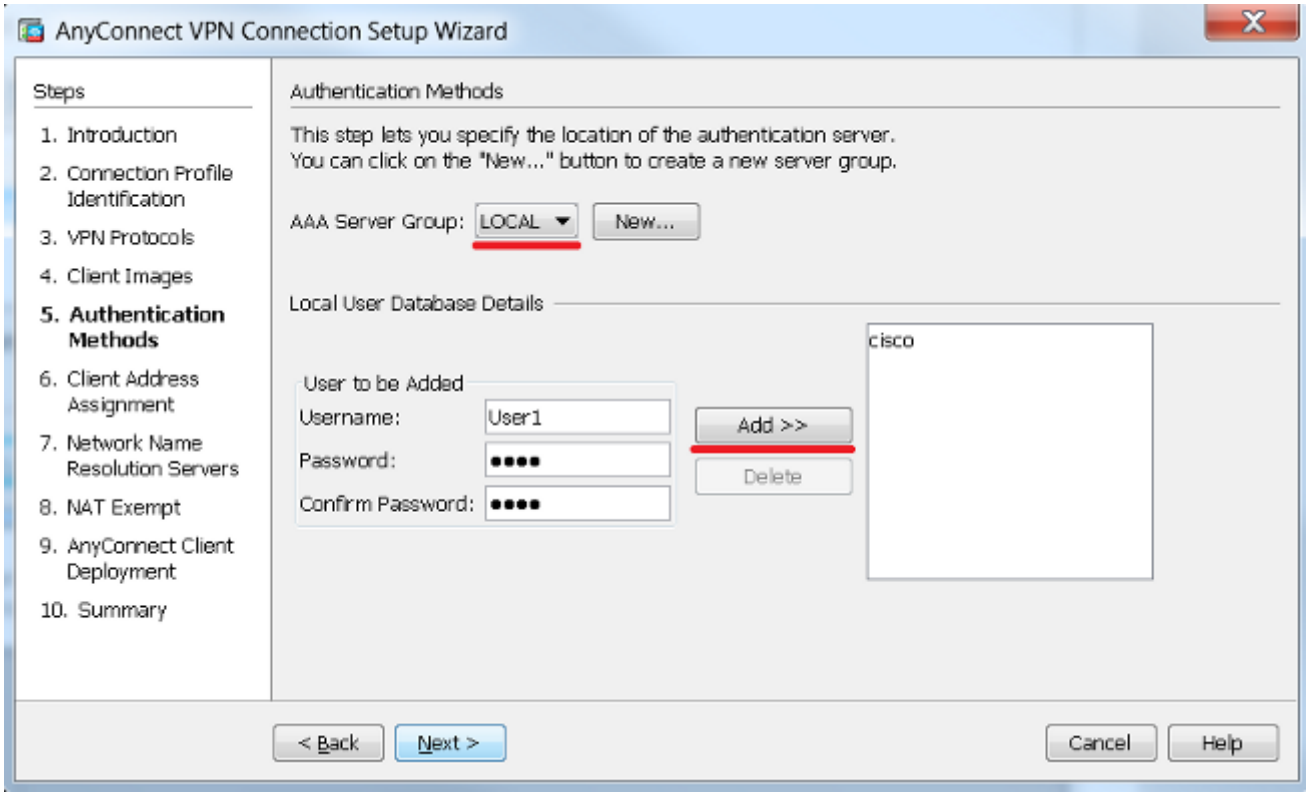




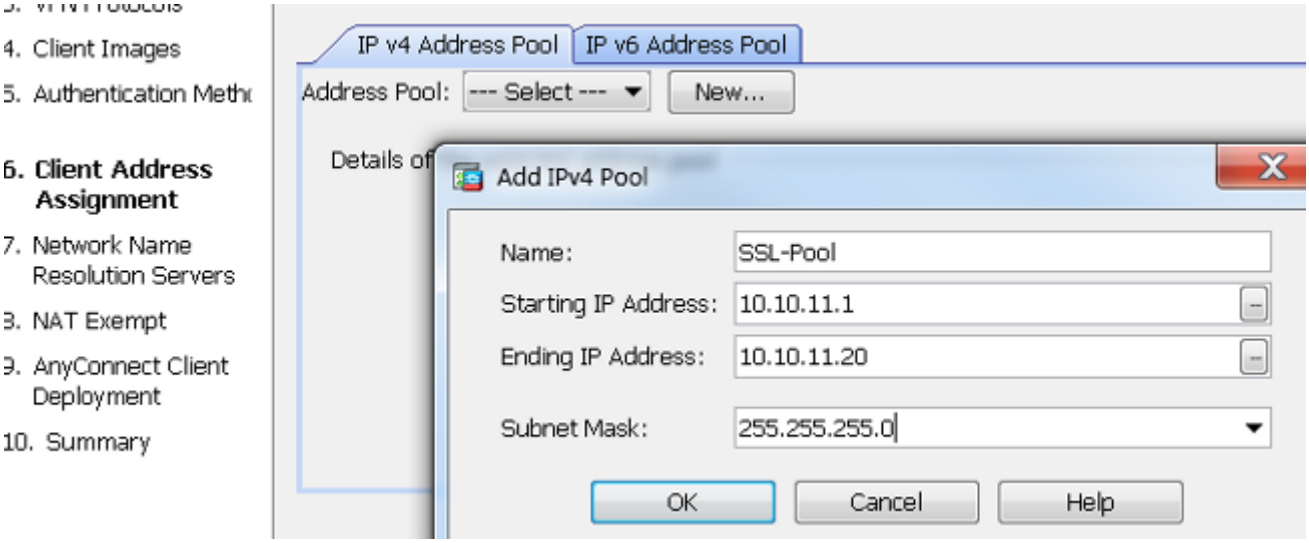
10. Una volta aggiunta l'immagine, fare clic su **Avanti**:



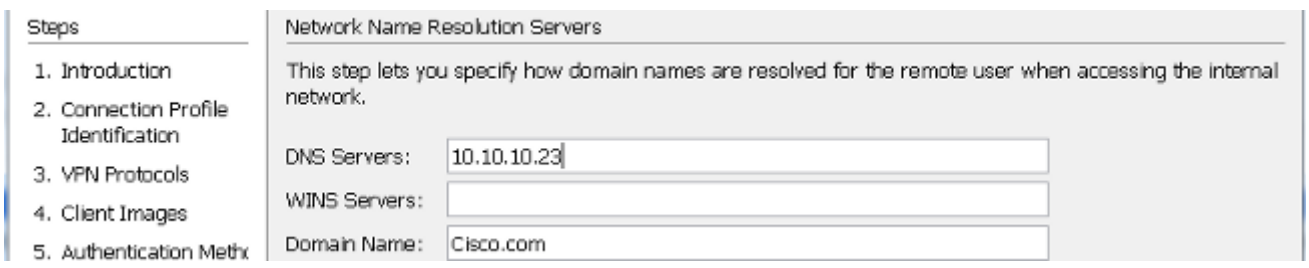
11. L'autenticazione utente può essere completata tramite i gruppi di server Autenticazione, Autorizzazione e Accounting (AAA). Se gli utenti sono già configurati, scegliere **CA locale** e fare clic su **Avanti**. **Nota:** In questo esempio, è configurata l'autenticazione **LOCAL**, ossia il database utenti locale sull'appliance ASA verrà usato per l'autenticazione.



12. Ènecessario configurare il pool di indirizzi per il client VPN. Se ne è già stato configurato uno, selezionarlo dal menu a discesa. In caso contrario, fare clic su **Nuovo** per configurarne uno nuovo. Al termine, fare clic su **Avanti**:

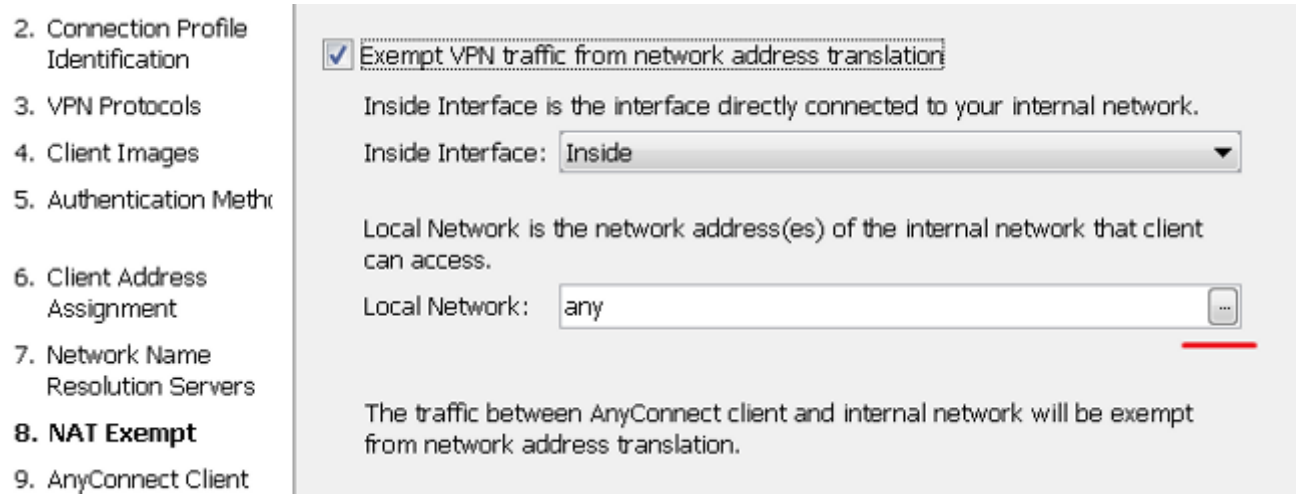


13. Immettere i server DNS (Domain Name System) e i DN nei campi *DNS* e *Nome dominio* in modo appropriato e quindi fare clic su **Avanti**:

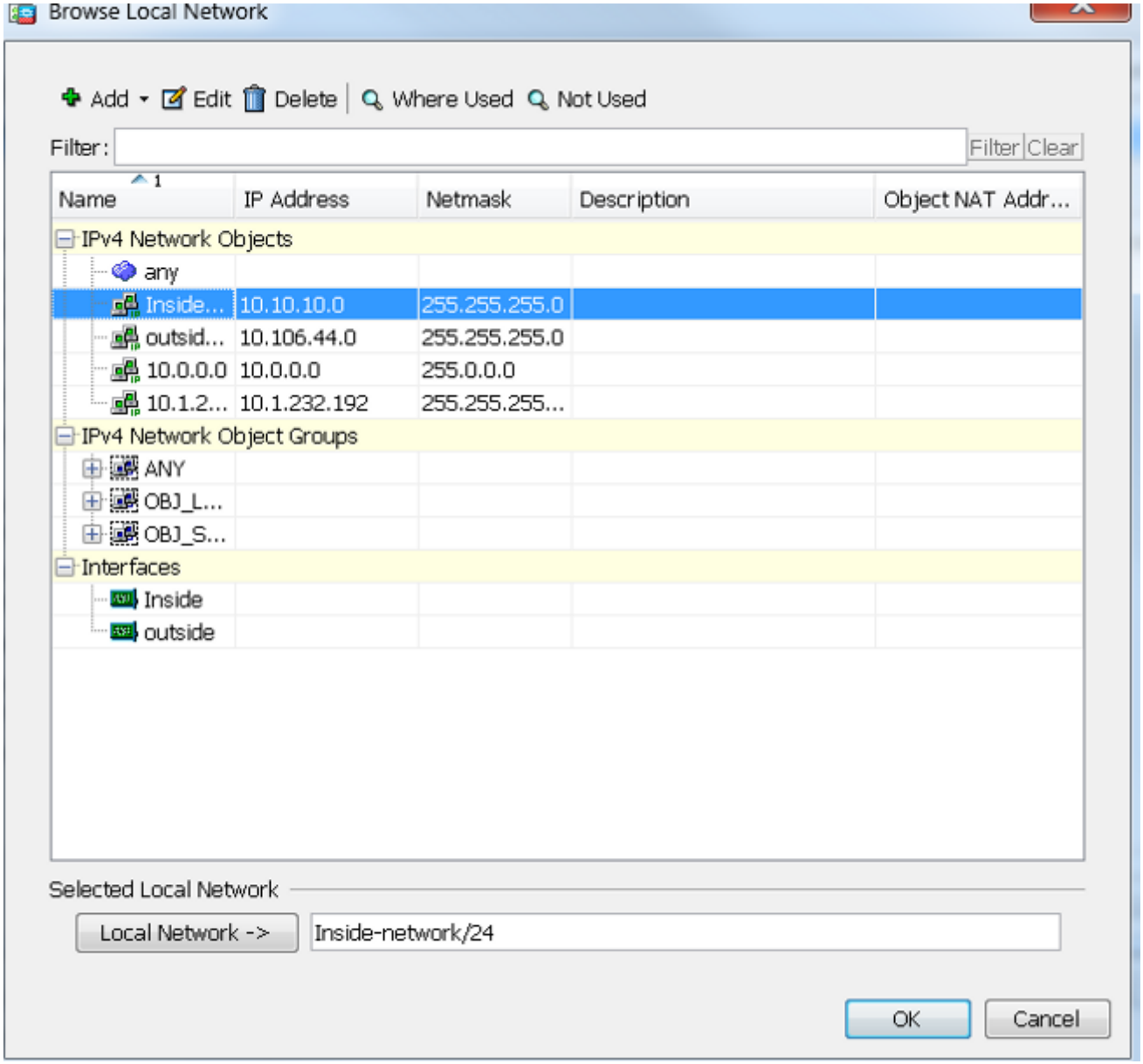


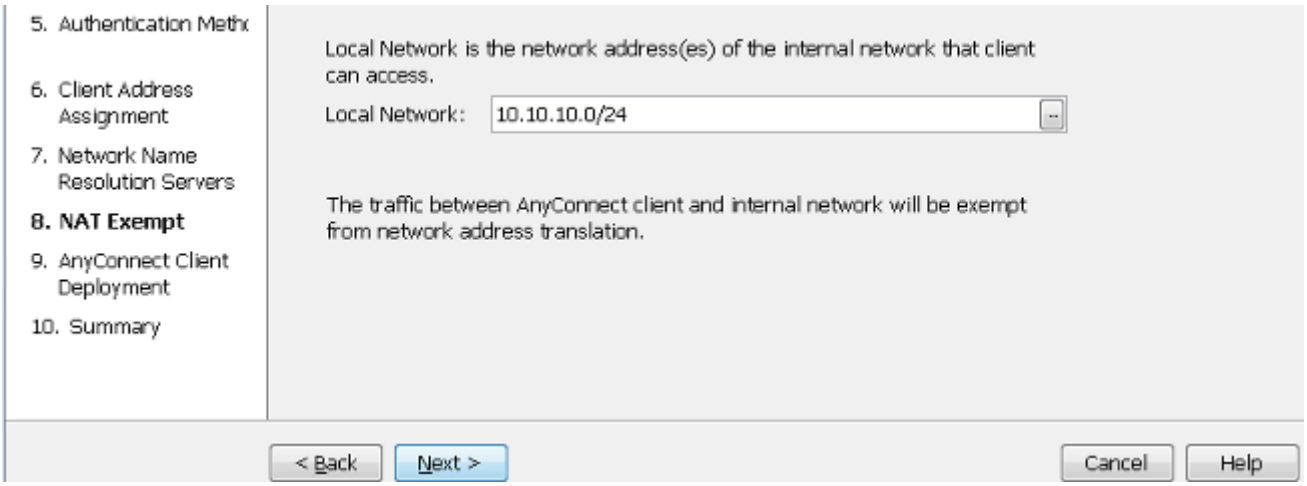
14. In questo scenario, l'obiettivo è limitare l'accesso sulla VPN alla rete **10.10.10.0/24** configurata come subnet *interna* (o LAN) dietro l'ASA. Il traffico tra il client e la subnet interna deve essere esentato da qualsiasi NAT (Network Address Translation) dinamico.

    Selezionare la casella di controllo **Esenzione traffico VPN da conversione indirizzi di rete** e configurare le interfacce LAN e WAN da utilizzare per l'esenzione:



15. Scegliere le reti locali a cui applicare l'esenzione:





16. Fare clic su **Avanti**, **Avanti** e quindi su **Fine**.

La configurazione del client AnyConnect è ora completata. Tuttavia, quando si configura AnyConnect tramite la Configurazione guidata, i criteri del tunnel *suddiviso* vengono configurati come **tunnel** per impostazione predefinita. Per effettuare solo il tunnel del traffico specifico, occorre implementare il *split-tunneling*.

Nota: Se non è configurato il tunneling ripartito, il criterio verrà ereditato dal criterio di gruppo predefinito (DfltGrpPolicy), che per impostazione predefinita è **Tunnel** tutto**.** Ciò significa che quando il client è connesso tramite VPN, tutto il traffico (per includere il traffico verso il Web) viene inviato tramite il tunnel.

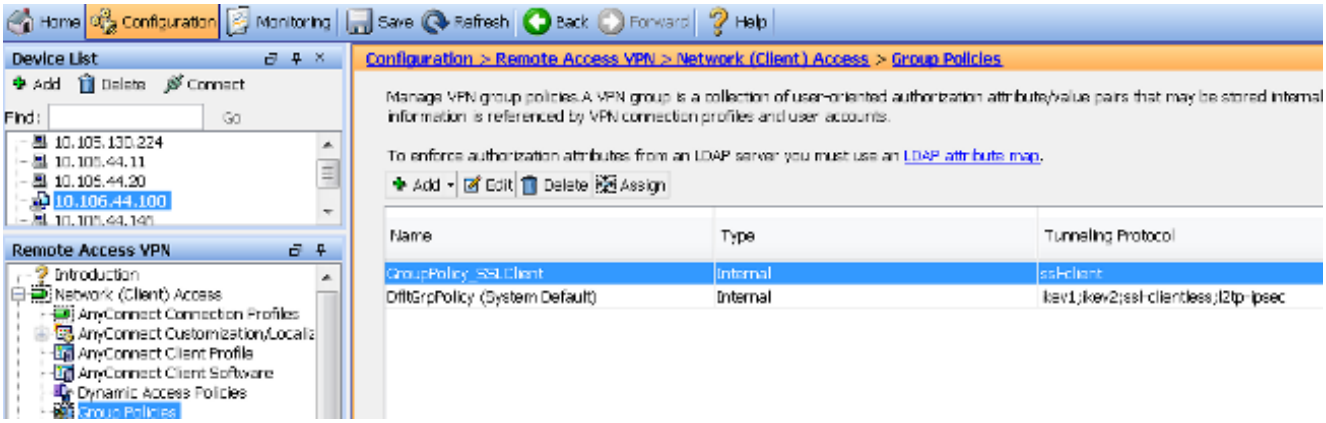
Solo il traffico destinato all'indirizzo IP WAN ASA (o *esterno*) ignorerà il tunneling sul computer client. Questa condizione può essere rilevata nell'output del comando **route print** nei computer Microsoft Windows.

Configurazione tunnel suddiviso

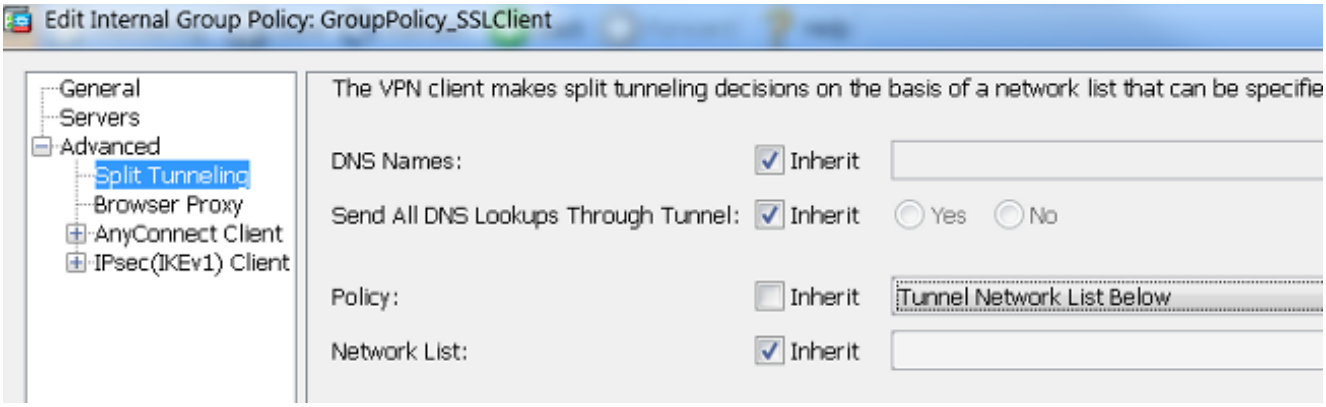
Il tunneling ripartito è una funzione che può essere utilizzata per definire il traffico delle subnet o degli host che devono essere crittografati. Questa operazione richiede la configurazione di un Access Control List (ACL) che verrà associato a questa funzione. Il traffico per le subnet o gli host definiti in questo ACL verrà crittografato sul tunnel dal client-end e le route per queste subnet verranno installate nella tabella di routing del PC.

Completare questa procedura per passare dalla configurazione *Tunnel-all* alla configurazione *Split-tunnel*:

1. Selezionare **Configurazione > VPN ad accesso remoto > Criteri di gruppo**:



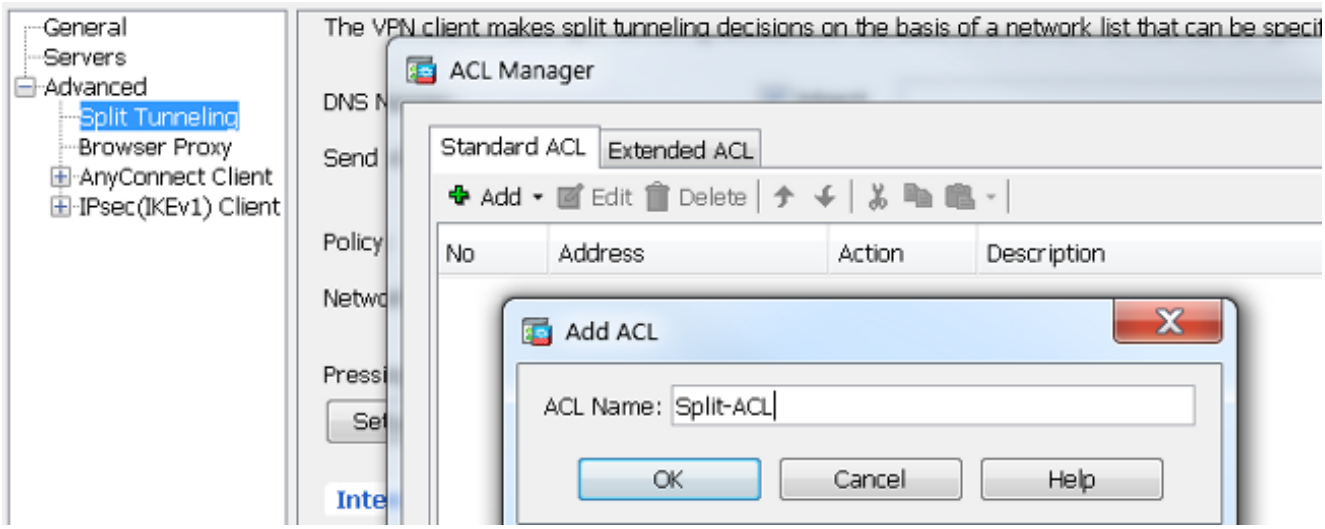
2. Fare clic su **Modifica** e utilizzare la struttura di navigazione per passare a **Avanzate > Tunneling ripartito**. Deselezionare la casella di controllo **Eredita** nella sezione *Criteri* e selezionare **Elenco reti tunnel sottostante** dal menu a discesa:



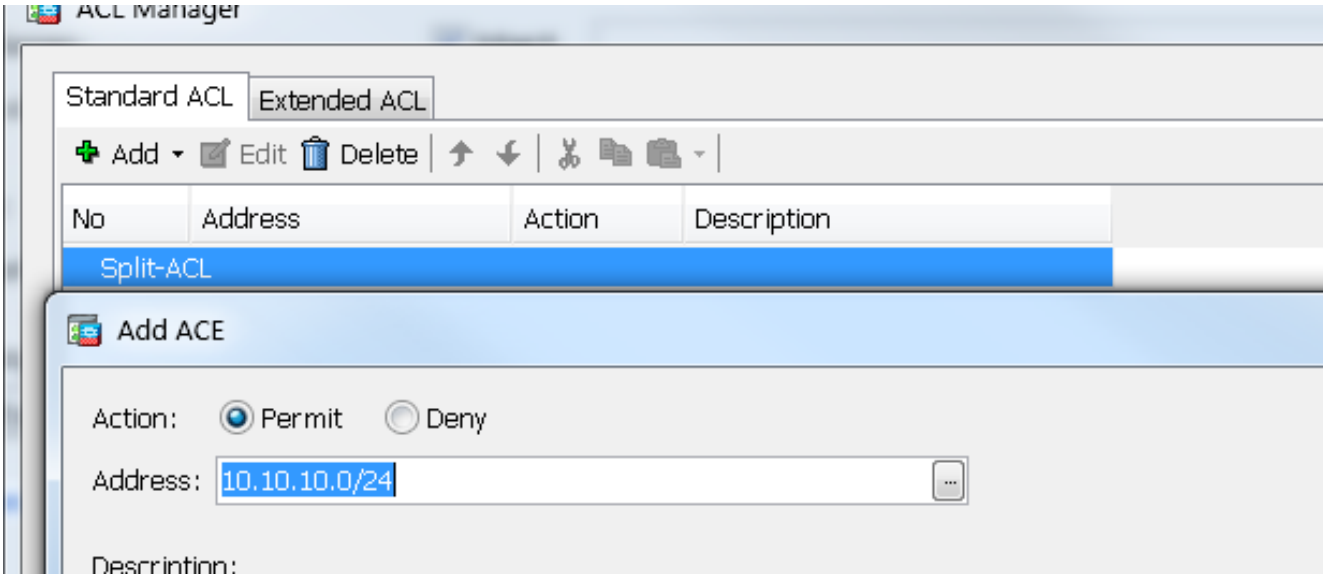
3. Deselezionare la casella di controllo **Inherit** nella sezione *Network List*, quindi fare clic su

Manage per selezionare l'ACL che specifica le reti LAN a cui il client deve accedere:

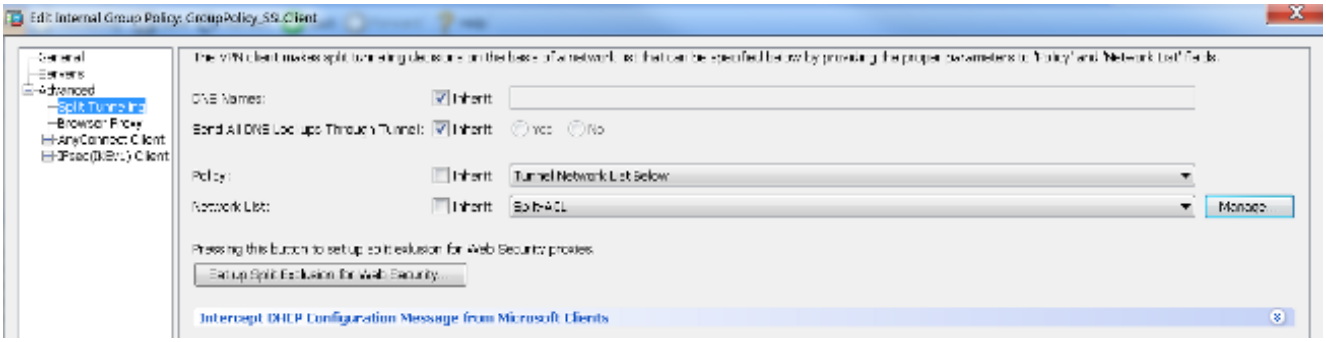
4. Fare clic su **ACL** standard**, Aggiungi**, **Aggiungi ACL**, quindi su **ACL name**:



5. Per aggiungere la regola, fare clic su **Add ACE**:



6. Fare clic su **OK**.



7. Fare clic su **Apply** (Applica).

Una volta connessi, i percorsi per le subnet o gli host sull'ACL suddiviso vengono aggiunti alla tabella di routing del client. Nei computer con sistema operativo Microsoft Windows, è possibile visualizzare questa informazione nell'output del comando **route print**. L'hop successivo per queste route sarà un indirizzo IP dalla subnet del pool IP del client (in genere il primo indirizzo IP della subnet):

```
C:\Users\admin>route print
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination Netmask Gateway Interface Metric
0.0.0.0 0.0.0.0 10.106.44.1 10.106.44.243 261
10.10.10.0      255.255.255.0    10.10.11.2  10.10.11.1     2

!! This is the split tunnel route.

10.106.44.0 255.255.255.0 On-link 10.106.44.243 261
172.16.21.1    255.255.255.255     On-link    10.106.44.243  6

!! This is the route for the ASA Public IP Address.
```

Sui computer MAC OS, immettere il comando **netstat -r** per visualizzare la tabella di routing del PC:

```
$ netstat -r
Routing tables
Internet:
Destination Gateway Flags Refs Use Netif Expire
default hsrp-64-103-236-1. UGSc 34 0 en1
10.10.10/24        10.10.11.2         UGSc    0   44   utun1

!! This is the split tunnel route.

10.10.11.2/32 localhost UGSc 1 0 lo0
172.16.21.1/32     hsrp-64-103-236-1. UGSc    1   0    en1

!! This is the route for the ASA Public IP Address.
```

Scarica e installa il client AnyConnect

Per distribuire Cisco AnyConnect Secure Mobility Client sul computer dell'utente, è possibile procedere in due modi:

- Distribuzione Web
- Distribuzione autonoma

Entrambi i metodi vengono illustrati in modo più dettagliato nelle sezioni seguenti.

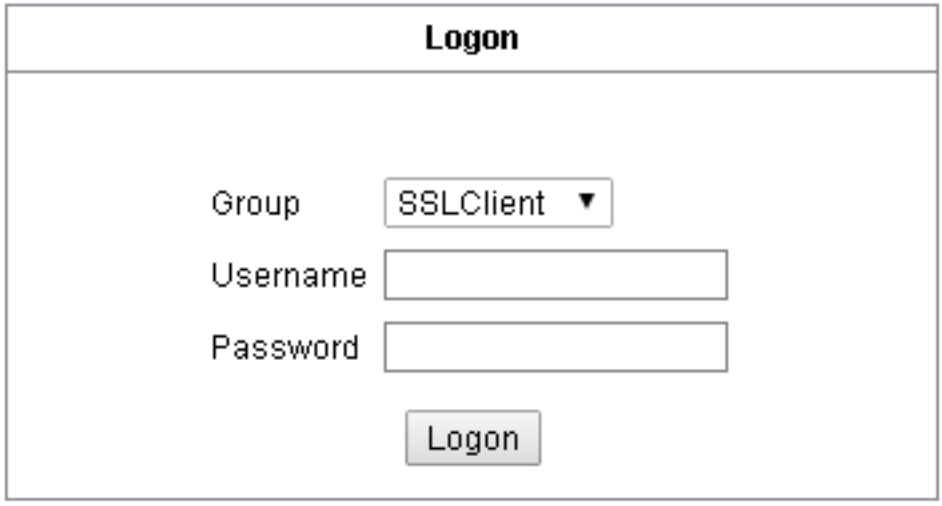
Distribuzione Web

Per utilizzare il metodo di distribuzione Web, immettere l'URL **https://<FQDN dell'ASA>o <IP dell'ASA>** in un browser sul computer client, in modo da visualizzare la pagina del portale *WebVPN*.

Nota: Se si utilizza Internet Explorer (IE), l'installazione viene completata principalmente tramite ActiveX, a meno che non si sia costretti a utilizzare Java. Tutti gli altri browser utilizzano Java.

Dopo aver effettuato l'accesso alla pagina, l'installazione deve iniziare sul computer client e, al termine, il client deve connettersi all'appliance ASA.

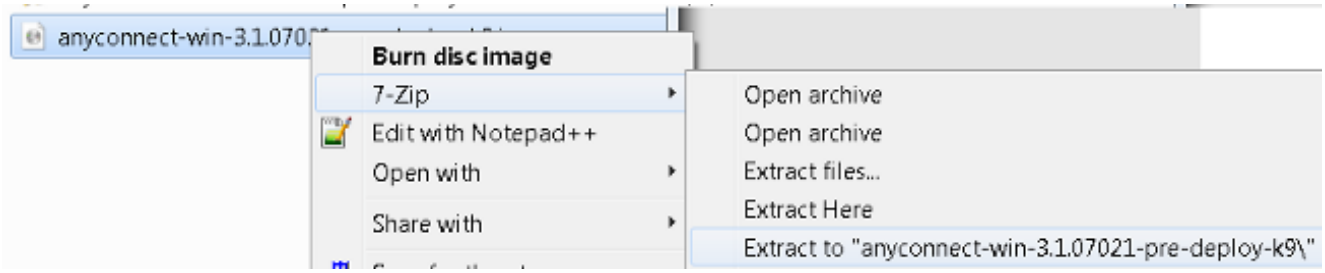
Nota: È possibile che venga richiesta l'autorizzazione per l'esecuzione di ActiveX o Java. Per procedere con l'installazione, è necessario consentire tale operazione.



Distribuzione autonoma

Per utilizzare il metodo di distribuzione standalone, completare i seguenti passaggi:

1. Scaricare l'immagine del client AnyConnect dal sito Web Cisco. Per scegliere l'immagine corretta da scaricare, consultare la pagina Web Cisco AnyConnect Secure Mobility Client. In questa pagina è disponibile un collegamento per il download. Passare alla pagina di download e selezionare la versione appropriata. Eseguire una ricerca del **pacchetto di installazione completa - Windows / Programma di installazione autonomo (ISO)**. **Nota:** Viene quindi scaricata un'immagine del programma di installazione ISO (ad esempio, *anyconnect-win-3.1.06073-pre-deploy-k9.iso*).
2. Usare *WinRar* o *7-Zip* per estrarre il contenuto del pacchetto ISO:



3. Una volta estratto il contenuto, eseguire il file **Setup.exe** e scegliere i moduli da installare con Cisco AnyConnect Secure Mobility Client.

Suggerimento: Per configurare impostazioni aggiuntive per la VPN, fare riferimento alla sezione Configurazione delle connessioni client VPN di AnyConnect della *guida alla configurazione di Cisco ASA serie 5500 dalla CLI, versione 8.4 e 8.6*.

Configurazione CLI

In questa sezione viene fornita la configurazione CLI per Cisco AnyConnect Secure Mobility Client a scopo di riferimento.

```
ASA Version 9.3(2)
!
hostname PeerASA-29
enable password 8Ry2YjIyt7RRXU24 encrypted
ip local pool SSL-Pool 10.10.11.1-10.10.11.20 mask 255.255.255.0
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.21.1 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.10.10.1 255.255.255.0
!
boot system disk0:/asa932-smp-k8.bin
ftp mode passive
object network NETWORK_OBJ_10.10.10.0_24
subnet 10.10.10.0 255.255.255.0
object network NETWORK_OBJ_10.10.11.0_27
subnet 10.10.11.0 255.255.255.224

access-list all extended permit ip any any
```

```
!***********Split ACL configuration***********

access-list Split-ACL standard permit 10.10.10.0 255.255.255.0
no pager
logging enable
logging buffered debugging
mtu outside 1500
mtu inside 1500
mtu dmz 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-721.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected

!************** NAT exemption Configuration *****************
!This will exempt traffic from Local LAN(s) to the
!Remote LAN(s) from getting NATted on any dynamic NAT rule.

nat (inside,outside) source static NETWORK_OBJ_10.10.10.0_24 NETWORK_OBJ_10.10.10.0_24
destination static NETWORK_OBJ_10.10.11.0_27 NETWORK_OBJ_10.10.11.0_27 no-proxy-arp
route-lookup
access-group all in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.21.2 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
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 sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
aaa authentication ssh console LOCAL
http server enable
http 0.0.0.0 0.0.0.0 outside
no snmp-server location
no snmp-server contact

!********** Trustpoint for Selfsigned certificate***********
!Genarate the key pair and then configure the trustpoint
!Enroll the trustpoint genarate the self-signed certificate

crypto ca trustpoint SelfsignedCert
enrollment self
subject-name CN=anyconnect.cisco.com
keypair sslcert
crl configure
crypto ca trustpool policy
crypto ca certificate chain SelfsignedCert
certificate 4748e654
308202f0 308201d8 a0030201 02020447 48e65430 0d06092a 864886f7 0d010105
0500303a 311d301b 06035504 03131461 6e79636f 6e6e6563 742e6369 73636f2e
636f6d31 19301706 092a8648 86f70d01 0902160a 50656572 4153412d 3239301e
170d3135 30343032 32313534 30375a17 0d323530 33333032 31353430 375a303a
311d301b 06035504 03131461 6e79636f 6e6e6563 742e6369 73636f2e 636f6d31
19301706 092a8648 86f70d01 0902160a 50656572 4153412d 32393082 0122300d
06092a86 4886f70d 01010105 00038201 0f003082 010a0282 010100f6 a125d0d0
55a975ec a1f2133f 0a2c3960 0da670f8 bcb6dad7 efefe50a 482db3a9 7c6db7c4
ed327ec5 286594bc 29291d8f 15140bad d33bc492 02f5301e f615e7cd a72b60e0
7877042b b6980dc7 ccaa39c8 c34164d9 e2ddeea1 3c0b5bad 5a57ec4b d77ddb3c
75930fd9 888f92b8 9f424fd7 277e8f9e 15422b40 071ca02a 2a73cf23 28d14c93
```

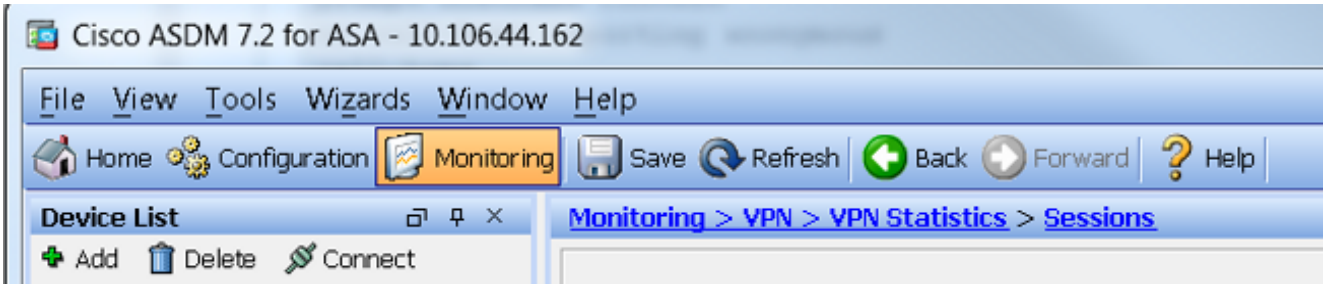
```
5a084cf0 403267a6 23c18fa4 fca9463f aa76057a b07e4b19 c534c0bb 096626a7
53d17d9f 4c28a3fd 609891f7 3550c991 61ef0de8 67b6c7eb 97c3bff7 c9f9de34
03a5e788 94678f4d 7f273516 c471285f 4e23422e 6061f1e7 186bbf9c cf51aa36
19f99ab7 c2bedb68 6d182b82 7ecf39d5 1314c87b ffddff68 8231d302 03010001
300d0609 2a864886 f70d0101 05050003 82010100 d598c1c7 1e4d8a71 6cb43296
c09ea8da 314900e7 5fa36947 c0bc1778 d132a360 0f635e71 400e592d b27e29b1
64dfb267 51e8af22 0a6a8378 5ee6a734 b74e686c 6d983dde 54677465 7bf8fe41
daf46e34 bd9fd20a bacf86e1 3fac8165 fc94fe00 4c2eb983 1fc4ae60 55ea3928
f2a674e1 8b5d651f 760b7e8b f853822c 7b875f91 50113dfd f68933a2 c52fe8d9
4f9d9bda 7ae2f750 313c6b76 f8d00bf5 1f74cc65 7c079a2c 8cce91b0 a8cdd833
900a72a4 22c2b70d 111e1d92 62f90476 6611b88d ff58de5b fdaa6a80 6fe9f206
3fe4b836 6bd213d4 a6356a6c 2b020191 bf4c8e3d dd7bdd8b 8cc35f0b 9ad8852e
b2371ee4 23b16359 ba1a5541 ed719680 ee49abe8
quit
telnet timeout 5
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
management-access inside
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ssl server-version tlsv1-only
ssl encryption des-sha1 3des-sha1 aes128-sha1 aes256-sha1

!******** Bind the certificate to the outside interface********
ssl trust-point SelfsignedCert outside

!********Configure the Anyconnect Image and enable Anyconnect***
webvpn
enable outside
anyconnect image disk0:/anyconnect-win-3.1.06073-k9.pkg 1
anyconnect enable
tunnel-group-list enable

!*******Group Policy configuration*********
!Tunnel protocol, Spit tunnel policy, Split
!ACL, etc. can be configured.

group-policy GroupPolicy_SSLClient internal
group-policy GroupPolicy_SSLClient attributes
wins-server none
dns-server value 10.10.10.23
vpn-tunnel-protocol ikev2 ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value Split-ACL
default-domain value Cisco.com

username User1 password PfeNk7qp9b4LbLV5 encrypted
username cisco password 3USUcOPFUiMCO4Jk encrypted privilege 15

!*******Tunnel-Group (Connection Profile) Configuraiton*****
tunnel-group SSLClient type remote-access
tunnel-group SSLClient general-attributes
address-pool SSL-Pool
default-group-policy GroupPolicy_SSLClient
tunnel-group SSLClient webvpn-attributes
group-alias SSLClient enable
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
```

```
parameters
message-length maximum client auto
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect sip
inspect xdmcp
!
service-policy global_policy global
Cryptochecksum:8d492b10911d1a8fbcc93aa4405930a0
: end
```

Verifica

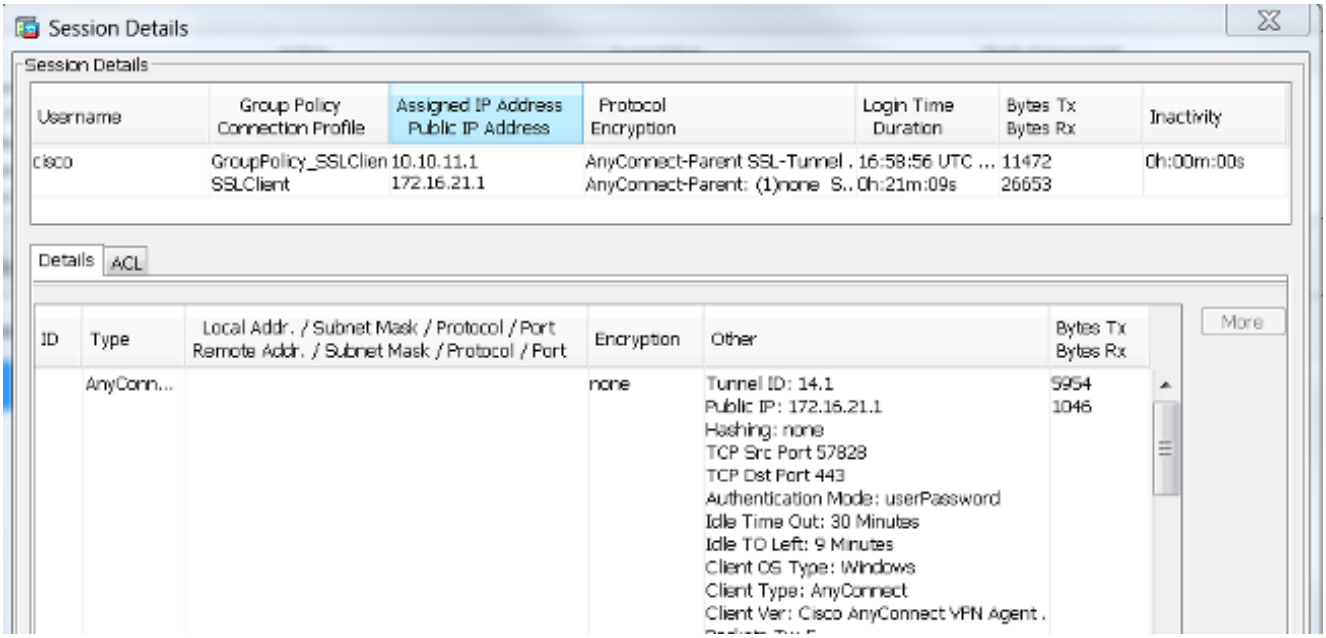
Completare questi passaggi per verificare la connessione client e i vari parametri associati a tale connessione:

1. Selezionare **Monitoraggio > VPN** su ASDM:



2. Per filtrare il tipo di VPN, è possibile utilizzare l'opzione **Filter By**. Selezionare **AnyConnect Client** dal menu a discesa e tutte le sessioni del client AnyConnect. **Suggerimento**: Le sessioni possono essere ulteriormente filtrate in base ad altri criteri, ad esempio *Nome utente* e *indirizzo IP*.

3. Fare doppio clic su una sessione per ottenere ulteriori dettagli su quella particolare sessione:



4. Per ottenere i dettagli della sessione, immettere il comando **show vpn-sessiondb anyconnect** nella CLI:

```
# show vpn-sessiondb anyconnect
Session Type : AnyConnect
Username : cisco Index : 14
Assigned IP : 10.10.11.1   Public IP : 172.16.21.1
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)3DES DTLS-Tunnel: (1)DES
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 11472 Bytes Rx : 39712
Group Policy : GroupPolicy_SSLClient   Tunnel Group : SSLClient
Login Time : 16:58:56 UTC Mon Apr 6 2015
Duration : 0h:49m:54s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
```

5. Per perfezionare i risultati, è possibile utilizzare le altre opzioni di filtro:

```
# show vpn-sessiondb detail anyconnect filter name cisco

Session Type: AnyConnect Detailed

Username : cisco Index : 19
Assigned IP : 10.10.11.1    Public IP : 10.106.44.243
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)3DES DTLS-Tunnel: (1)DES
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 11036 Bytes Rx : 4977
Pkts Tx : 8 Pkts Rx : 60
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : GroupPolicy_SSLClient  Tunnel Group : SSLClient
Login Time   : 20:33:34 UTC Mon Apr 6 2015
Duration : 0h:01m:19s

AnyConnect-Parent Tunnels: 1
```

```
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
Tunnel ID : 19.1
Public IP : 10.106.44.243
Encryption : none Hashing : none
TCP Src Port : 58311 TCP Dst Port : 443
Auth Mode : 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 3.1.06073
Bytes Tx : 5518 Bytes Rx : 772
Pkts Tx : 4 Pkts Rx : 1
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 19.2
Assigned IP : 10.10.11.1 Public IP : 10.106.44.243
Encryption : 3DES Hashing : SHA1
Encapsulation: TLSv1.0 TCP Src Port : 58315
TCP Dst Port : 443 Auth Mode : 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 3.1.06073
Bytes Tx : 5518 Bytes Rx : 190
Pkts Tx : 4 Pkts Rx : 2
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 19.3
Assigned IP : 10.10.11.1 Public IP : 10.106.44.243
Encryption : DES Hashing : SHA1
Encapsulation: DTLSv1.0 UDP Src Port : 58269
UDP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.06073
Bytes Tx : 0 Bytes Rx : 4150
Pkts Tx : 0 Pkts Rx : 59
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

Risoluzione dei problemi

Èpossibile usare lo strumento di diagnostica e segnalazione di AnyConnect (DART) per raccogliere i dati utili per la risoluzione dei problemi di installazione e connessione di AnyConnect. La procedura guidata DART viene usata sul computer su cui è in esecuzione AnyConnect. DART raggruppa i registri, lo stato e le informazioni di diagnostica per l'analisi di Cisco Technical Assistance Center (TAC) e non richiede privilegi di amministratore per l'esecuzione sul computer client.

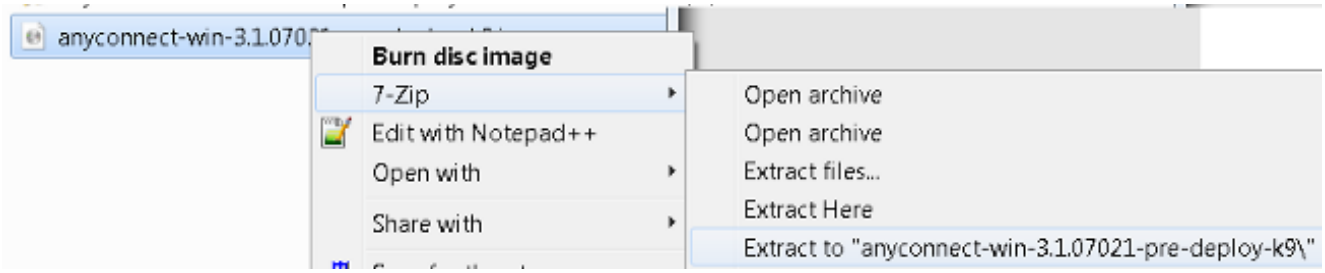
Installare DART

Per installare DART, completare i seguenti passaggi:

1. Scaricare l'immagine del client AnyConnect dal sito Web Cisco. Per scegliere l'immagine

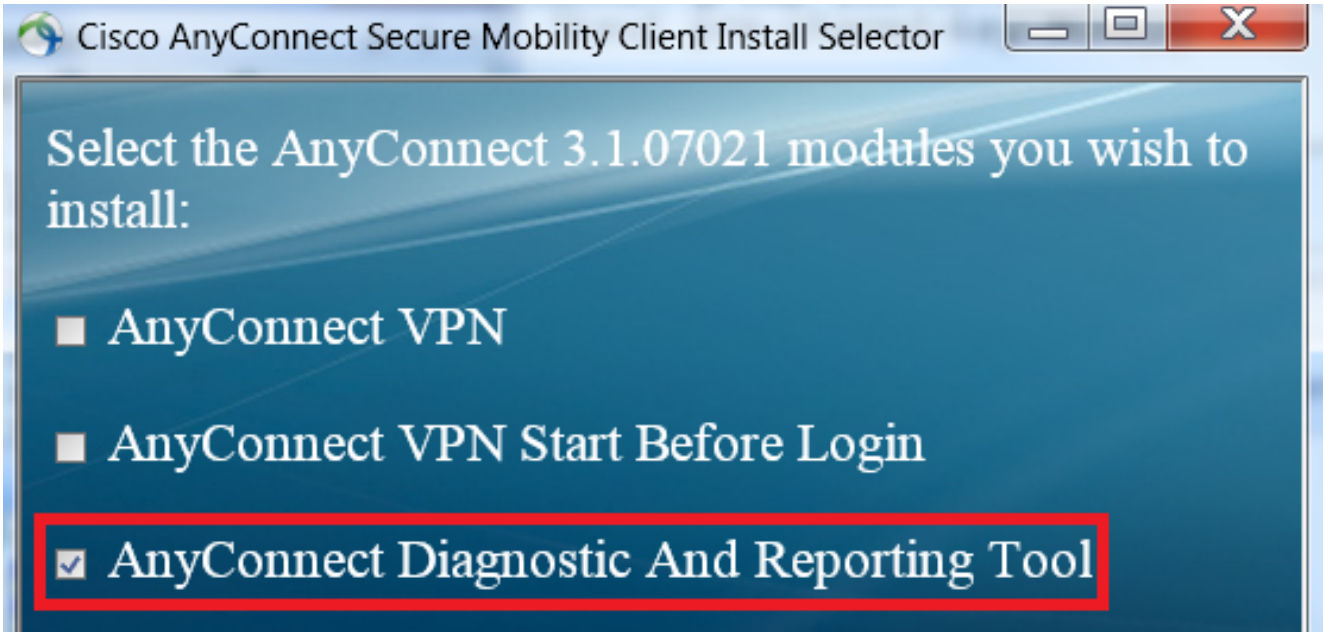
corretta da scaricare, consultare la pagina Web Cisco AnyConnect Secure Mobility Client. In questa pagina è disponibile un collegamento per il download. Passare alla pagina di download e selezionare la versione appropriata. Eseguire una ricerca del **pacchetto di installazione completa - Windows / Programma di installazione autonomo (ISO)**. **Nota:** Viene quindi scaricata un'immagine del programma di installazione ISO (ad esempio, *anyconnect-win-3.1.06073-pre-deploy-k9.iso*).

2. Usare *WinRar* o *7-Zip* per estrarre il contenuto del pacchetto ISO:



3. Selezionare la cartella in cui è stato estratto il contenuto.

4. Eseguire il file **Setup.exe** e selezionare solo **lo strumento di diagnostica e report Anyconnect**:

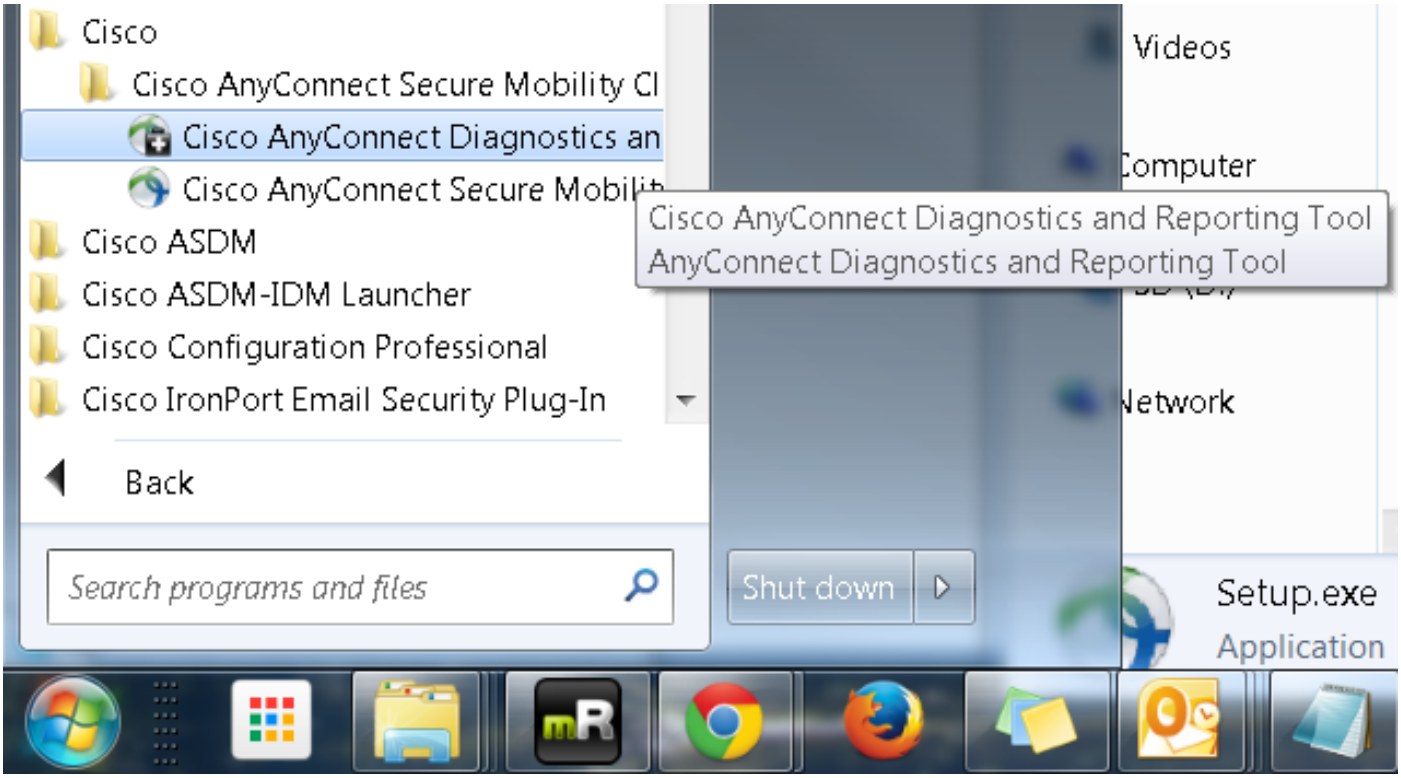


Eseguire il DART

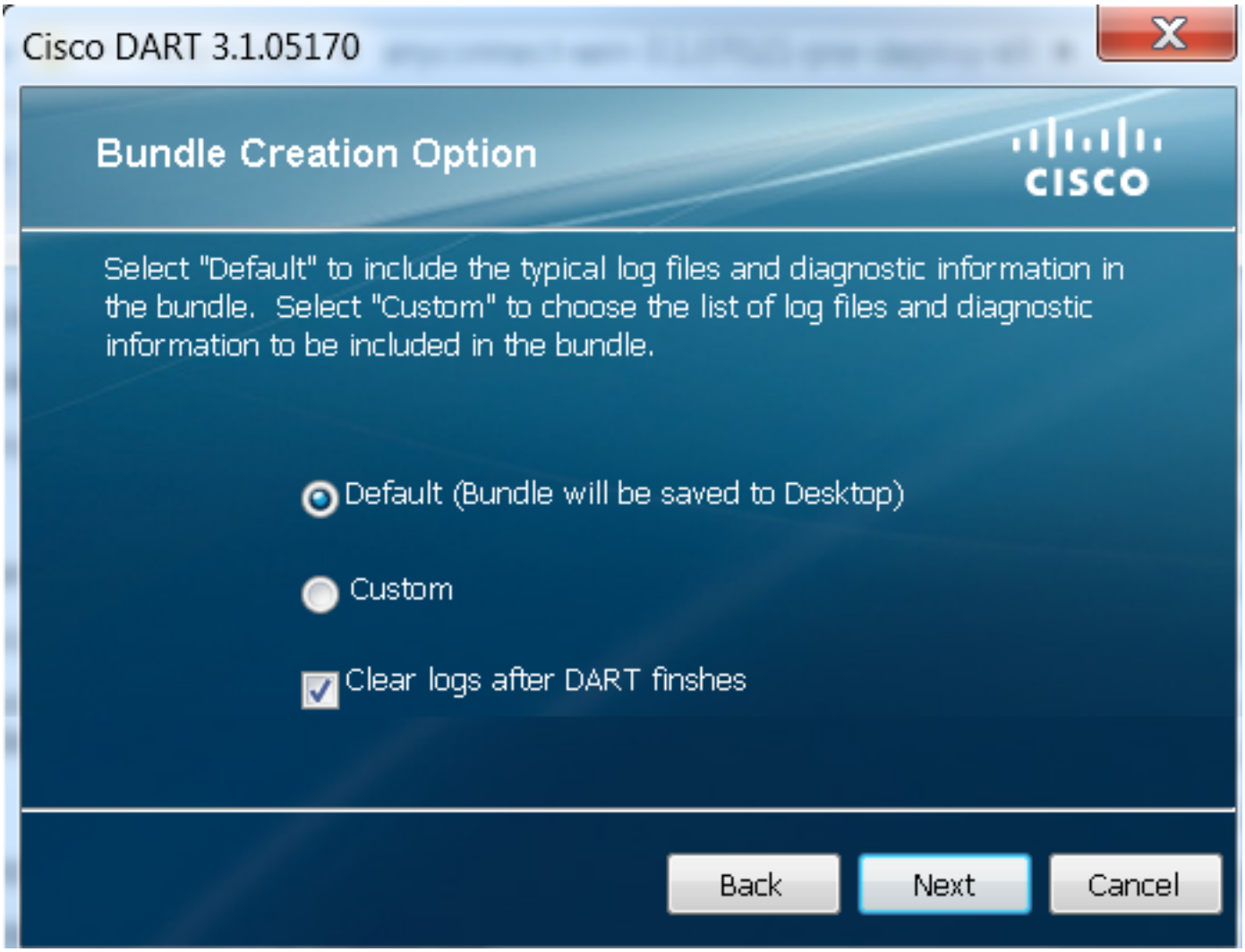
Di seguito sono riportate alcune importanti informazioni da considerare prima di eseguire DART:

- Il problema deve essere ricreato almeno una volta prima di eseguire DART.
- La data e l'ora sul computer dell'utente devono essere annotate quando il problema viene ricreato.

Eseguire il comando DART dal *menu Start* sul computer client:



Èpossibile selezionare la modalità *predefinita* o *personalizzata*. Cisco consiglia di eseguire il comando DART nella modalità predefinita in modo che tutte le informazioni possano essere acquisite in una singola ripresa.



Al termine, lo strumento salva il file DART bundle *.zip* sul desktop del client. Il bundle può quindi essere inviato al TAC (dopo aver aperto una richiesta TAC) per ulteriori analisi.

Informazioni correlate

- Guida alla risoluzione dei problemi dei client VPN AnyConnect - Problemi comuni
- Java 7 - Guida alla risoluzione dei problemi di AnyConnect, CSD/Hostscan e WebVPN
- Documentazione e supporto tecnico – Cisco Systems

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).