

Configurazione del mapping dei certificati per l'autenticazione client sicura su FTD tramite FMC

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Esempio di rete](#)

[Configurazioni](#)

[Configurazione in FMC](#)

[Passaggio 1. Configura interfaccia FTD](#)

[Passaggio 2. Conferma licenza Cisco Secure Client](#)

[Passaggio 3. Aggiungi pool di indirizzi IPv4](#)

[Passaggio 4. Aggiungi Criteri di gruppo](#)

[Passaggio 5. Aggiungi certificato FTD](#)

[Passaggio 6. Aggiungi assegnazione criteri per il profilo di connessione del tecnico](#)

[Passaggio 7. Configura dettagli per il profilo di connessione del tecnico](#)

[Passaggio 8. Configura immagine client sicura per il profilo di connessione del tecnico](#)

[Passaggio 9. Configura accesso e certificato per profilo di connessione del tecnico](#)

[Passaggio 10. Conferma riepilogo per il profilo di connessione del tecnico](#)

[Passaggio 11. Aggiungi profilo di connessione per client VPN di gestione](#)

[Passaggio 12. Aggiungi mapping certificati](#)

[Passaggio 13. Associa mappa certificato a profilo di connessione](#)

[Conferma nella CLI FTD](#)

[Conferma in client VPN](#)

[Passaggio 1. Conferma certificato client](#)

[Passaggio 2. Conferma CA](#)

[Verifica](#)

[Passaggio 1. Avvia connessione VPN](#)

[Passaggio 2. Conferma sessioni attive in FMC](#)

[Passaggio 3. Conferma sessioni VPN nella CLI FTD](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive come configurare Cisco Secure Client con SSL su FTD tramite FMC utilizzando la mappatura dei certificati per l'autenticazione.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Firepower Management Center (FMC)
- Virtual Firewall Threat Defense (FTD)
- Flusso di autenticazione VPN

Componenti usati

- Cisco Firepower Management Center per VMWare 7.4.1
- Cisco Firewall Threat Defense Virtual 7.4.1

- Cisco Secure Client 5.1.3.62

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

Il mapping dei certificati è un metodo utilizzato nelle connessioni VPN in cui un certificato client viene mappato a un account utente locale oppure gli attributi all'interno del certificato vengono utilizzati a scopo di autorizzazione. Si tratta di un processo in cui un certificato digitale viene utilizzato per identificare un utente o un dispositivo. Utilizzando il mapping dei certificati, utilizza il protocollo SSL per autenticare gli utenti senza che questi debbano immettere credenziali.

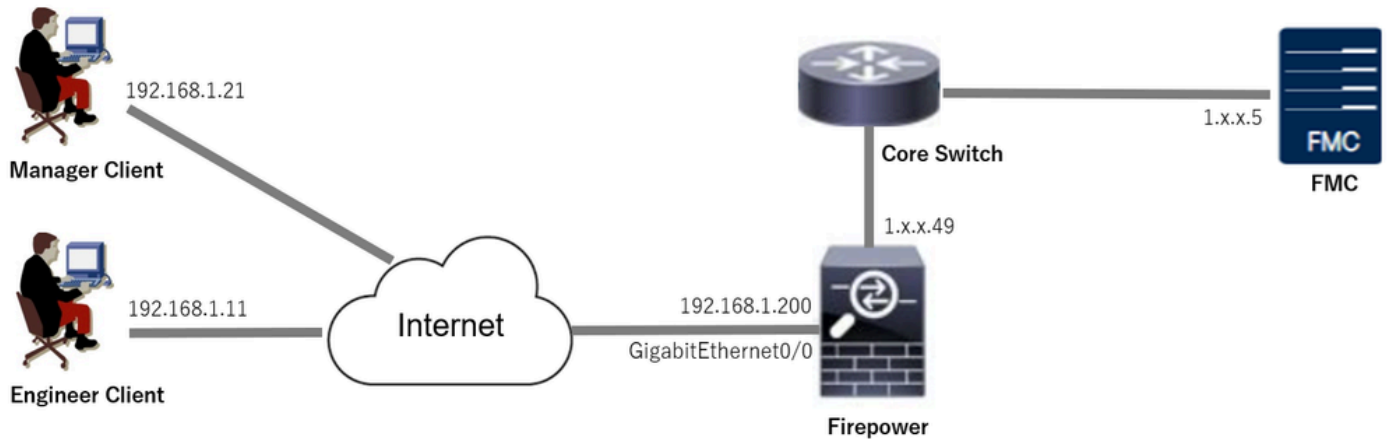
In questo documento viene descritto come autenticare Cisco Secure Client utilizzando il nome comune tratto da un certificato SSL.

Questi certificati contengono un nome comune, utilizzato ai fini dell'autorizzazione.

- CA : ftd-ra-ca-nome-comune
- Certificato client VPN del tecnico: vpnEngineerClientCN
- Certificato client VPN Manager: vpnManagerClientCN
- Certificato server: 192.168.1.200

Esempio di rete

Nell'immagine è illustrata la topologia utilizzata per l'esempio del documento.



Esempio di rete

Configurazioni

Configurazione in FMC

Passaggio 1. Configura interfaccia FTD

Selezionare Dispositivi > Gestione dispositivi, modificare il dispositivo FTD di destinazione, configurare l'interfaccia esterna per FTD nella scheda Interfacce.

Per Gigabit Ethernet0/0,

- Nome: esterno
- Area di sicurezza: area esterna
- Indirizzo IP: 192.168.1.200/24

Firewall Management Center
Devices / Secure Firewall Interfaces

Overview Analysis Policies Devices Objects Integration

Deploy Search admin **SECURE**

1.1.1.1.49
Cisco Firepower Threat Defense for VMware

Device Routing **Interfaces** Inline Sets DHCP VTEP

All Interfaces Virtual Tunnels

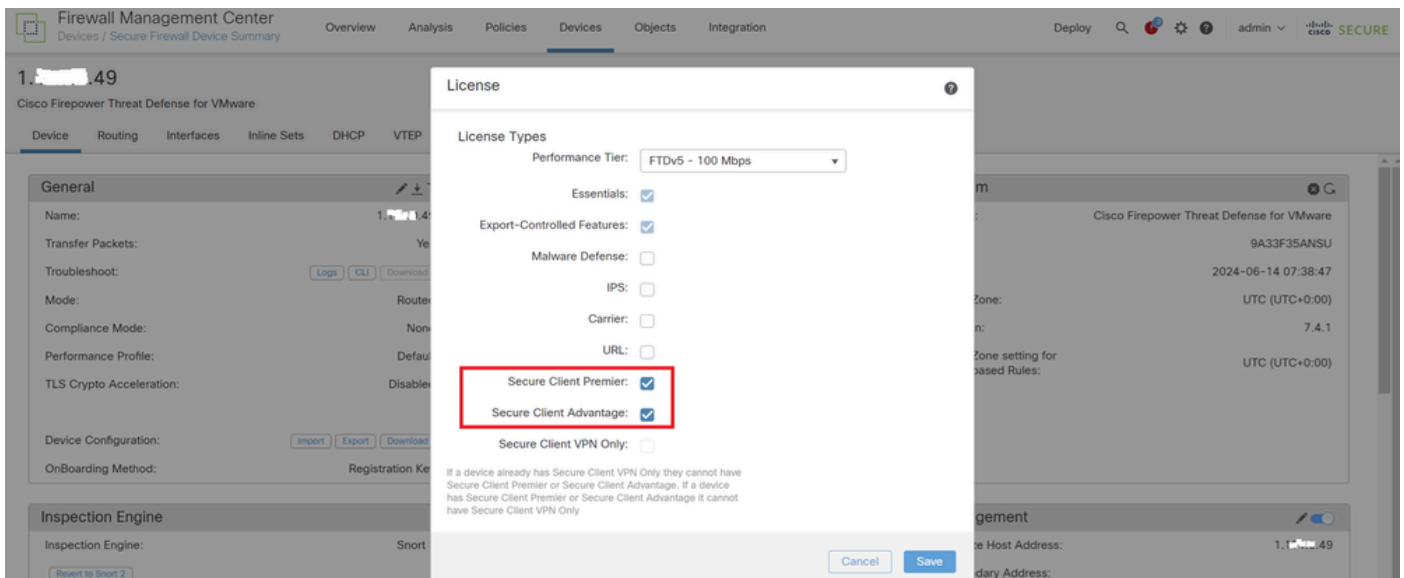
Search by name Sync Device Add Interfaces

| Interface | Logical Name | Type | Security Zones | MAC Address (Active/Standby) | IP Address | Path Monitoring | Virtual Router |
|--------------------|--------------|----------|----------------|------------------------------|--------------------------|-----------------|----------------|
| Management0/0 | management | Physical | | | | Disabled | Global |
| GigabitEthernet0/0 | outside | Physical | outsideZone | | 192.168.1.200/24(Static) | Disabled | Global |

Interfaccia FTD

Passaggio 2. Conferma licenza Cisco Secure Client

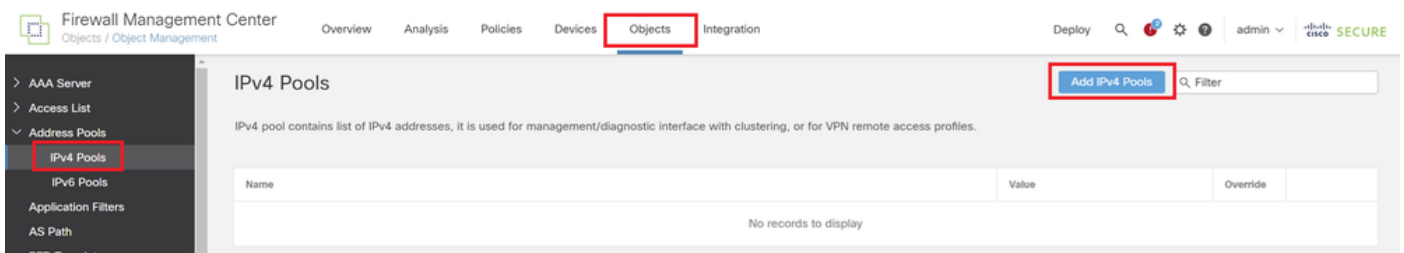
Selezionare Dispositivi > Gestione dispositivi, modificare il dispositivo FTD di destinazione, confermare la licenza Cisco Secure Client nella scheda Dispositivo.



Licenza Secure Client

Passaggio 3. Aggiungo pool di indirizzi IPv4

Selezionare Oggetto > Gestione oggetti > Pool di indirizzi > Pool IPv4, quindi fare clic su Aggiungi pool IPv4.



Aggiungo pool di indirizzi IPv4

Immettere le informazioni necessarie per creare un pool di indirizzi IPv4 per il client VPN del tecnico.

- Nome: ftd-vpn-engineer-pool
- Intervallo di indirizzi IPv4: 172.16.1.100-172.16.1.110
- Maschera: 255.255.255.0

Edit IPv4 Pool



Name*
ftd-vpn-engineer-pool

Description

IPv4 Address Range*
172.16.1.100-172.16.1.110

Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask*
255.255.255.0

Allow Overrides

i Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

► Override (0)

Cancel

Save

Pool di indirizzi IPv4 per client VPN del tecnico

Immettere le informazioni necessarie per creare un pool di indirizzi IPv4 per il client VPN di gestione.

- Nome: ftd-vpn-manager-pool
- Intervallo di indirizzi IPv4: 172.16.1.120-172.16.1.130
- Maschera: 255.255.255.0

Add IPv4 Pool



Name*
ftd-vpn-manager-pool

Description

IPv4 Address Range*
172.16.1.120-172.16.1.130

Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask*
255.255.255.0

Allow Overrides

i Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

► Override (0)

Cancel

Save

Pool di indirizzi IPv4 per client VPN di gestione

Confermare i nuovi pool di indirizzi IPv4.

Firewall Management Center
Objects / Object Management

Overview Analysis Policies Devices **Objects** Integration

Deploy 🔍 ⚙️ ? admin 🔒 Cisco SECURE

Add IPv4 Pools 🔍 Filter

IPv4 Pools

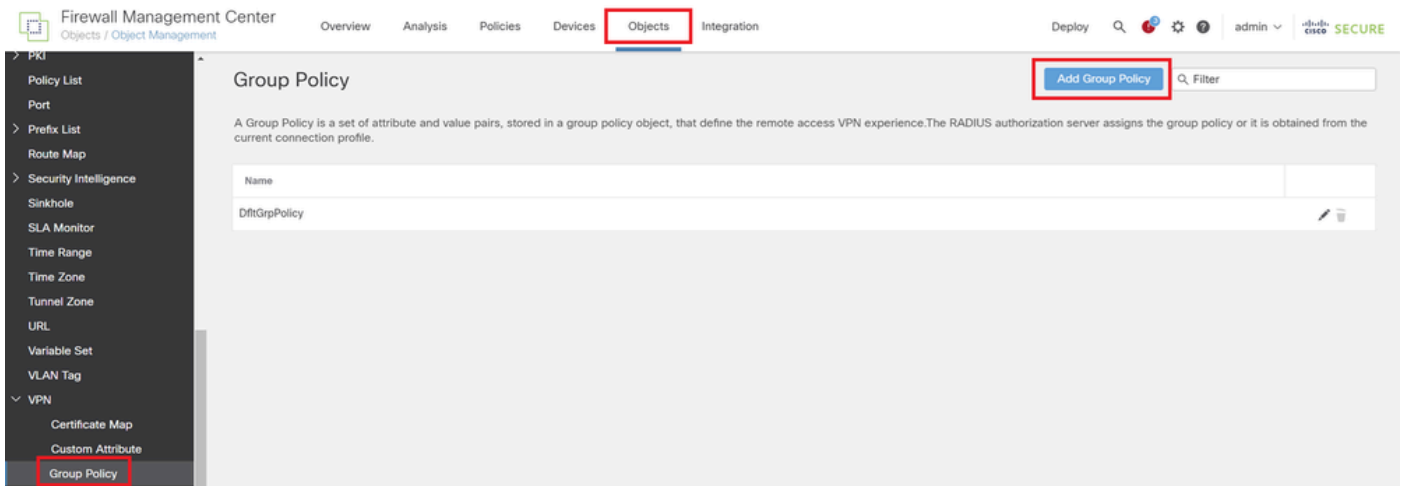
IPv4 pool contains list of IPv4 addresses, it is used for management/diagnostic interface with clustering, or for VPN remote access profiles.

| Name | Value | Override | |
|-----------------------|---------------------------|----------|------|
| ftd-vpn-engineer-pool | 172.16.1.100-172.16.1.110 | ● | ✎ 🗑️ |
| ftd-vpn-manager-pool | 172.16.1.120-172.16.1.130 | ● | ✎ 🗑️ |

Nuovi pool di indirizzi IPv4

Passaggio 4. Aggiungo Criteri di gruppo

Selezionare Oggetto > Gestione oggetti > VPN > Criteri di gruppo, quindi fare clic su Aggiungi criteri di gruppo.



Aggiungi Criteri di gruppo

Immettere le informazioni necessarie per creare un criterio di gruppo per il client VPN del tecnico.

- Nome: ftd-vpn-engineer-grp
- Protocolli VPN: SSL

Add Group Policy

The image shows the 'Add Group Policy' configuration form. The 'Name' field is filled with 'ftd-vpn-engineer-grp'. The 'Description' field is empty. Below the form, there are three tabs: 'General', 'Secure Client', and 'Advanced'. The 'Advanced' tab is selected. Under the 'Advanced' tab, there is a section for 'VPN Tunnel Protocol' with the following options: 'VPN Protocols' (selected), 'IP Address Pools', 'Banner', 'DNS/WINS', and 'Split Tunneling'. The 'VPN Tunnel Protocol' section is expanded, showing 'VPN Tunnel Protocol:' and the instruction 'Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel.' Below this, there are two options: 'SSL' (checked) and 'IPsec-IKEv2' (unchecked).

Criteri di gruppo per il client VPN Engineer

Immettere le informazioni necessarie per creare un criterio di gruppo per il client VPN di gestione.

- Nome: ftd-vpn-manager-grp
- Protocolli VPN: SSL

Add Group Policy



Name:*

Description:

General Secure Client Advanced

VPN Protocols

VPN Tunnel Protocol:
Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel.

SSL

IPsec-IKEv2

IP Address Pools

Banner

DNS/WINS

Split Tunneling

Criteri di gruppo per il client VPN di gestione

Confermare i nuovi criteri di gruppo.

Firewall Management Center

Objects / Object Management

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 SECURE

Group Policy

A Group Policy is a set of attribute and value pairs, stored in a group policy object, that define the remote access VPN experience. The RADIUS authorization server assigns the group policy or it is obtained from the current connection profile.

| Name | |
|----------------------|-----|
| DfltGrpPolicy | ✎ 🗑 |
| ftd-vpn-engineer-grp | ✎ 🗑 |
| ftd-vpn-manager-grp | ✎ 🗑 |

Nuovi Criteri di gruppo

Passaggio 5. Aggiungo certificato FTD

Passare a Oggetto > Gestione oggetti > PKI > Registrazione certificato, quindi fare clic su Aggiungi registrazione certificato.

Firewall Management Center

Overview Analysis Policies Devices **Objects** Integration

Deploy 🔍 ⚙️ ⓘ admin 🔽 Cisco **SECURE**

Cipher Suite List
> Community List
DHCP IPv6 Pool
> Distinguished Name
> DNS Server Group
> External Attributes
File List
> FlexConfig
Geolocation
Interface
Key Chain
Network
PKI
 Cert Enrollment
 External Cert Groups

Cert Enrollment

Add Cert Enrollment 🔍

A certificate enrollment object contains the Certification Authority (CA) server information and enrollment parameters that are required for creating Certificate Signing Requests (CSRs) and obtaining Identity Certificates from the specified CA. These activities occur in your Private Key Infrastructure (PKI).

| Name | Type | Override |
|-----------------------|------|----------|
| No records to display | | |

Aggiungi registrazione certificato

Immettere le informazioni necessarie per il certificato FTD e importare un file PKCS12 dal computer locale.

- Nome: ftd-vpn-cert
- Tipo di registrazione: file PKCS12

Add Cert Enrollment



Name*
ftd-vpn-cert

Description

This certificate is already enrolled on devices. Remove the enrolment from Device>Certificate page to edit/delete this Certificate.

CA Information Certificate Parameters Key Revocation

Enrollment Type: PKCS12 File

PKCS12 File*: ftdCert.pfx [Browse PKCS12 File](#)

Passphrase*:

Validation Usage: IPsec Client SSL Client SSL Server

Skip Check for CA flag in basic constraints of the CA Certificate

Cancel

Save

Dettagli di Registrazione certificato

Confermare la registrazione del nuovo certificato.

Firewall Management Center

Overview Analysis Policies Devices **Objects** Integration

Deploy Search Settings Help admin Cisco SECURE

Cert Enrollment

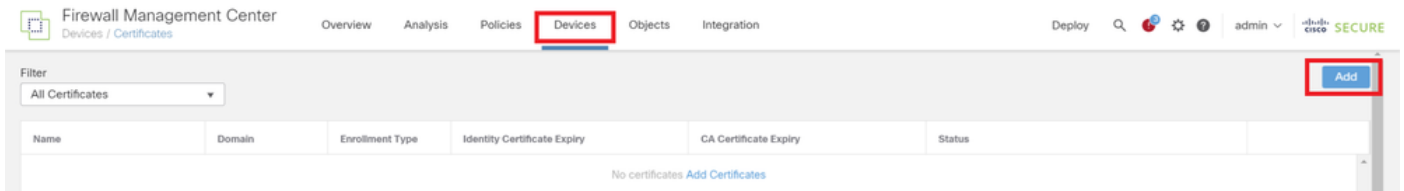
Add Cert Enrollment

A certificate enrollment object contains the Certification Authority (CA) server information and enrollment parameters that are required for creating Certificate Signing Requests (CSRs) and obtaining Identity Certificates from the specified CA. These activities occur in your Private Key Infrastructure (PKI).

| Name | Type | Override |
|--------------|-------------|----------|
| ftd-vpn-cert | PKCS12 File | |

Nuova registrazione certificato

Passare a Dispositivi > Certificati, fare clic su Aggiungi pulsante.



Aggiungi certificato FTD

Immettere le informazioni necessarie per associare la nuova registrazione certificato a FTD.

- Dispositivo: 1.x.x.49
- Registrazione certificato: ftd-vpn-cert

Add New Certificate



Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*:

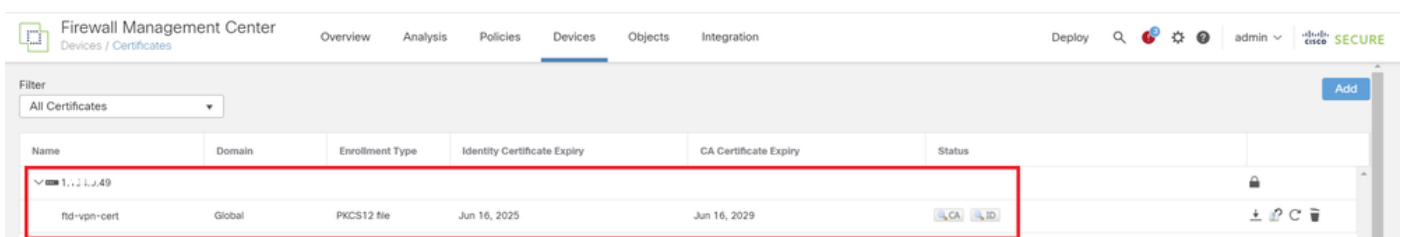
Cert Enrollment*: +

Cert Enrollment Details:

Name: ftd-vpn-cert
Enrollment Type: PKCS12 file
Enrollment URL: N/A

Associa certificato a FTD

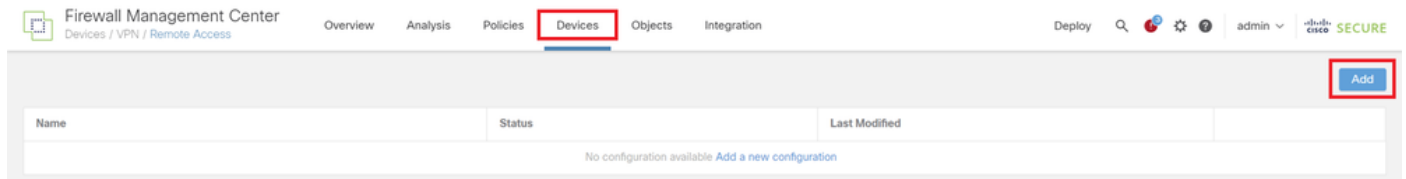
Confermare lo stato dell'associazione certificato.



Stato dell'associazione certificato

Passaggio 6. Aggiungi assegnazione criteri per il profilo di connessione del tecnico

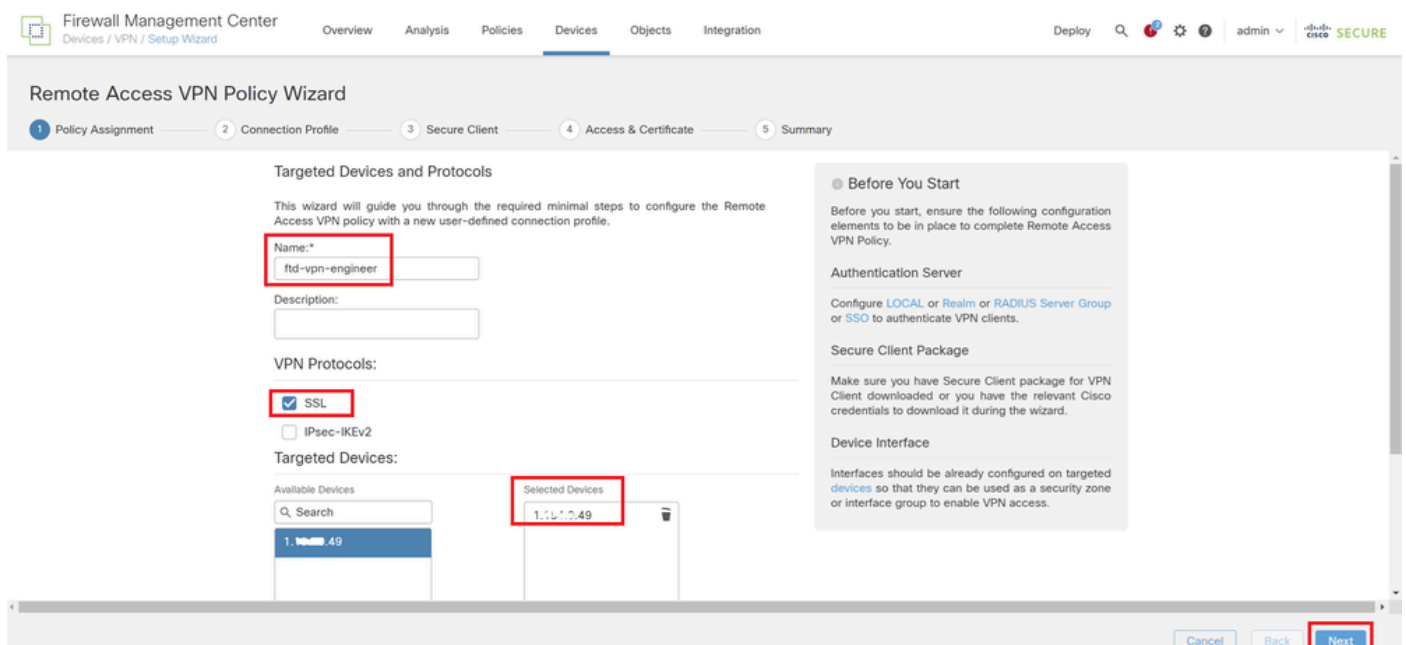
Selezionare Dispositivi > VPN > Accesso remoto, quindi fare clic su Aggiungi pulsante.



Aggiungi VPN di accesso remoto

Immettere le informazioni necessarie e fare clic su Pulsante Avanti.

- Nome: ftd-vpn-engineer
- Protocolli VPN: SSL
- Dispositivi di destinazione: 1.x.x.49



Assegnazione criteri

Passaggio 7. Configura dettagli per il profilo di connessione del tecnico

Immettere le informazioni necessarie e fare clic su Pulsante Avanti.

- Metodo di autenticazione: solo certificato client
- Nome utente da certificato: campo specifico della mappa
- Campo principale: CN (nome comune)
- Campo secondario: unità organizzativa

- Pool di indirizzi IPv4: ftd-vpn-engineer-pool
- Criteri di gruppo: ftd-vpn-engineer-grp

Firewall Management Center
Devices / VPN / Setup Wizard

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 Cisco **SECURE**

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 **Connection Profile** — 3 Secure Client — 4 Access & Certificate — 5 Summary

Connection Profile:

Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.

Connection Profile Name:*

Authentication, Authorization & Accounting (AAA):

Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method:

Username From Certificate: Map specific field Use entire DN (Distinguished Name) as username

Primary Field:

Secondary Field:

Authorization Server: +
(Realm or RADIUS)

Accounting Server: +
(RADIUS)

Client Address Assignment:

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

Use AAA Server (Realm or RADIUS only)

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools:

IPv6 Address Pools:

Group Policy:

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:* +

[Edit Group Policy](#)

Dettagli profilo connessione

Passaggio 8. Configura immagine client sicura per il profilo di connessione del tecnico

Selezionare secure client image file e fare clic su NextButton.

Firewall Management Center
Devices / VPN / Setup Wizard

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 Cisco **SECURE**

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 **Secure Client** — 4 Access & Certificate — 5 Summary

Secure Client Image

The VPN gateway can automatically download the latest Secure Client package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download Secure Client packages from [Cisco Software Download Center](#).

[Show Re-order buttons](#) +

| <input checked="" type="checkbox"/> | Secure Client File Object Name | Secure Client Package Name | Operating System |
|-------------------------------------|------------------------------------|---|------------------|
| <input checked="" type="checkbox"/> | cisco-secure-client-win-5.1.3.6... | cisco-secure-client-win-5.1.3.62-webdepl... | Windows |

Seleziona client protetto

Passaggio 9. Configura accesso e certificato per profilo di connessione del tecnico

Selezionare il valore per gli elementi Gruppo interfaccia/Area di protezione e Registrazione certificato, quindi fare clic su Pulsante Avanti.

- Gruppo di interfacce/Area di sicurezza: outsideZone
- Registrazione certificato: ftd-vpn-cert

The screenshot shows the 'Remote Access VPN Policy Wizard' in the 'Access & Certificate' step. The wizard progress bar indicates steps: 1 Policy Assignment, 2 Connection Profile, 3 Secure Client, 4 Access & Certificate, and 5 Summary. The main configuration area is titled 'Network Interface for Incoming VPN Access' and includes a dropdown menu for 'Interface group/Security Zone:' set to 'outsideZone'. Below this, there is a checkbox for 'Enable DTLS on member interfaces' which is checked. A warning message states: 'All the devices must have interfaces as part of the Interface Group/Security Zone selected.' The 'Device Certificates' section includes a dropdown for 'Certificate Enrollment:' set to 'ftd-vpn-cert'. The 'Access Control for VPN Traffic' section has a checkbox for 'Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)' which is checked. At the bottom right, there are 'Cancel', 'Back', and 'Next' buttons, with 'Next' highlighted in red.

Dettagli di accesso e certificato

Passaggio 10. Conferma riepilogo per il profilo di connessione del tecnico

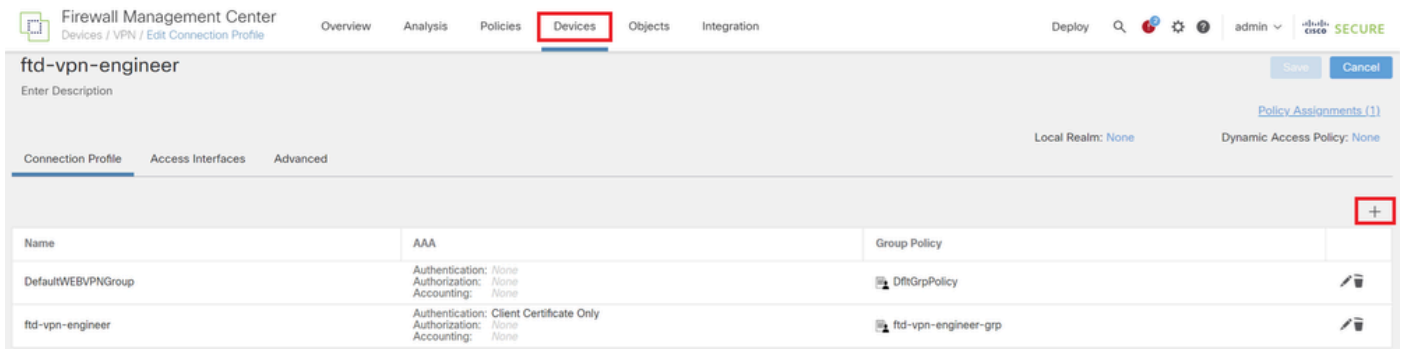
Confermare le informazioni immesse per il criterio VPN di accesso remoto e fare clic sul pulsante Fine.

The screenshot shows the 'Remote Access VPN Policy Wizard' in the 'Summary' step. The wizard progress bar indicates steps: 1 Policy Assignment, 2 Connection Profile, 3 Secure Client, 4 Access & Certificate, and 5 Summary. The main configuration area is titled 'Remote Access VPN Policy Configuration' and lists the following settings: Name: ftd-vpn-engineer, Device Targets: 1.1.1.1-1.1.1.49, Connection Profile: ftd-vpn-engineer, Connection Alias: ftd-vpn-engineer, AAA: Client Certificate Only, Authentication Method: Client Certificate Only, Username From Certificate: -, Authorization Server: -, Accounting Server: -, Address Assignment: -, Address from AAA: -, DHCP Servers: -, Address Pools (IPv4): ftd-vpn-engineer-pool, Address Pools (IPv6): -, Group Policy: ftd-vpn-engineer-grp, Secure Client Images: cisco-secure-client-win-5.1.3.62-webdeploy-k9.pk g, Interface Objects: outsideZone, Device Certificates: ftd-vpn-cert. To the right, there is a section titled 'Additional Configuration Requirements' which lists: Access Control Policy Update, NAT Exemption, DNS Configuration, and Port Configuration. At the bottom right, there are 'Cancel', 'Back', and 'Finish' buttons, with 'Finish' highlighted in red.

Dettagli del criterio VPN di accesso remoto

Passaggio 11. Aggiungi profilo di connessione per client VPN di gestione

Selezionare Dispositivi > VPN > Accesso remoto > Profilo di connessione, quindi fare clic sul pulsante +.



The screenshot shows the Cisco Firewall Management Center interface. The 'Devices' tab is selected. The main content area displays the configuration for a VPN connection profile named 'ftd-vpn-engineer'. Below this, there is a table with columns for Name, AAA, and Group Policy. A red box highlights the '+' button in the top right corner of the table.

| Name | AAA | Group Policy |
|--------------------|--|----------------------|
| DefaultWEBVPNGroup | Authentication: None Authorization: None Accounting: None | DfltGrpPolicy |
| ftd-vpn-engineer | Authentication: Client Certificate Only Authorization: None Accounting: None | ftd-vpn-engineer-grp |

Aggiungi profilo di connessione per client VPN di gestione

Immettere le informazioni necessarie per il profilo di connessione e fare clic su Salva pulsante.

- Nome: ftd-vpn-manager
- Criteri di gruppo: ftd-vpn-manager-grp
- Pool di indirizzi IPv4: ftd-vpn-manager-pool

Add Connection Profile



Connection Profile:*

Group Policy:* +

[Edit Group Policy](#)

Client Address Assignment AAA Aliases

IP Address for the remote clients can be assigned from local IP Address pools/DHCP Servers/AAA Servers. Configure the 'Client Address Assignment Policy' in the Advanced tab to define the assignment criteria.

Address Pools: +

| Name | IP Address Range | |
|-----------------------------|---------------------------|----------------------|
| ftd-vpn-manager-pool | 172.16.1.120-172.16.1.130 | ftd-vpn-manager-pool |

DHCP Servers: +

| Name | DHCP Server IP Address | |
|------|------------------------|--|
|------|------------------------|--|

Dettagli del profilo di connessione per Manager VPN Client

Confermare i nuovi profili di connessione aggiunti.

Firewall Management Center
Devices / VPN / Edit Connection Profile

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 🛡️ admin 🔒 **SECURE**

ftd-vpn-engineer You have unsaved changes

Enter Description

[Policy Assignments \(1\)](#)

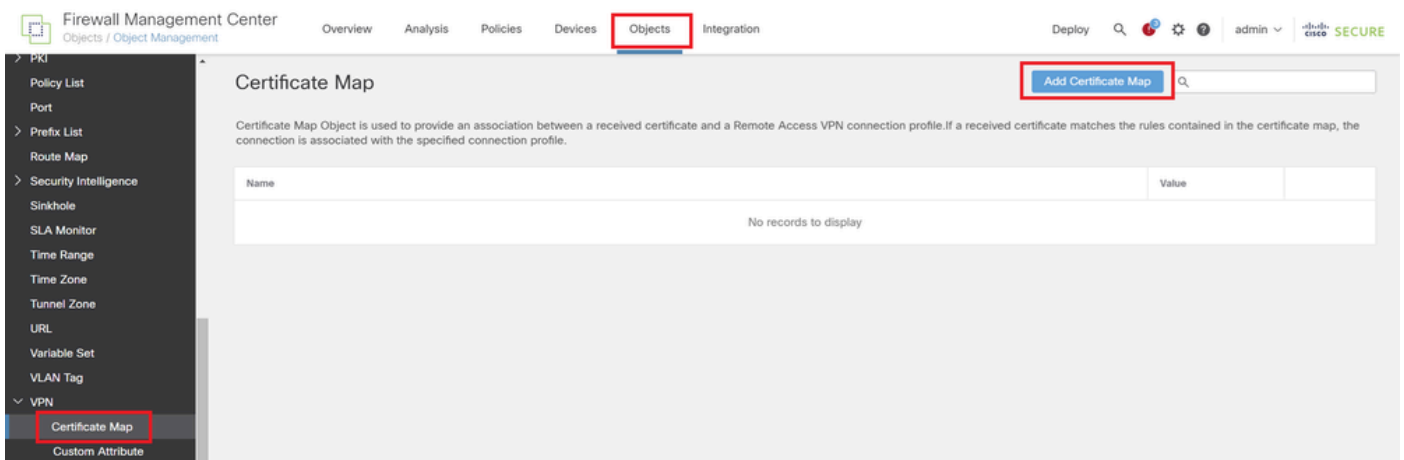
Local Realm: None Dynamic Access Policy: None

| Name | AAA | Group Policy | |
|-------------------------|--|-----------------------------|----|
| DefaultWEBVpnGroup | Authentication: None Authorization: None Accounting: None | DfltGrpPolicy | 🗑️ |
| ftd-vpn-engineer | Authentication: Client Certificate Only Authorization: None Accounting: None | ftd-vpn-engineer-grp | 🗑️ |
| ftd-vpn-manager | Authentication: Client Certificate Only Authorization: None Accounting: None | ftd-vpn-manager-grp | 🗑️ |

Conferma profili di connessione aggiunti

Passaggio 12. Aggiungi mapping certificati

Passare a Oggetti > Gestione oggetti > VPN > Mappa certificati, quindi fare clic sul pulsante Aggiungi mappa certificato.



Firewall Management Center
Objects / Object Management

Overview Analysis Policies Devices **Objects** Integration

Deploy 🔍 ⚙️ ⚠️ admin ▾ **SECURE**

PKI
Policy List
Port
Prefix List
Route Map
Security Intelligence
Sinkhole
SLA Monitor
Time Range
Time Zone
Tunnel Zone
URL
Variable Set
VLAN Tag
VPN
Certificate Map
Custom Attribute

Certificate Map

Add Certificate Map 🔍

Certificate Map Object is used to provide an association between a received certificate and a Remote Access VPN connection profile. If a received certificate matches the rules contained in the certificate map, the connection is associated with the specified connection profile.

| Name | Value |
|-----------------------|-------|
| No records to display | |

Aggiungi mapping certificati

Immettere le informazioni necessarie per la mappa certificati del client VPN del tecnico e fare clic su Pulsante Salva.

- Nome mappa: cert-map-engineer
- Regola di mapping: CN (nome comune) è uguale a vpnEngineerClientCN

Add Certificate Map



Map Name*:

cert-map-engineer

Mapping Rule

Configure the certificate matching rule

Add Rule

| # | Field | Component | Operator | Value | | |
|---|---------|------------------|----------|-------------------|--|--|
| 1 | Subject | CN (Common Name) | Equals | vpnEngineerCle... | | |

Cancel

Save

Mappa certificati per client tecnico

Immettere le informazioni necessarie per la mappa certificati del client VPN di gestione e fare clic su Pulsante Salva.

- Nome mappa: cert-map-manager
- Regola di mapping: CN (nome comune) è uguale a vpnManagerClientCN

Add Certificate Map



Map Name*:

Mapping Rule

Configure the certificate matching rule

Add Rule

| # | Field | Component | Operator | Value | | |
|---|---------|------------------|----------|-------------------|--|--|
| 1 | Subject | CN (Common Name) | Equals | vpnManagerClie... | | |

Cancel

Save

Mappa certificati per clienti di gestione

Confermare le nuove mappe certificati aggiunte.

Firewall Management Center
Objects / Object Management

Overview Analysis Policies Devices Objects Integration

Deploy admin SECURE

Certificate Map

Add Certificate Map

Certificate Map Object is used to provide an association between a received certificate and a Remote Access VPN connection profile. If a received certificate matches the rules contained in the certificate map, the connection is associated with the specified connection profile.

| Name | Value | | |
|-------------------|------------|--|--|
| cert-map-engineer | 1 Criteria | | |
| cert-map-manager | 1 Criteria | | |

Nuove mappe certificati

Passaggio 13. Associa mappa certificato a profilo di connessione

Selezionare Dispositivi > VPN > Accesso remoto, quindi modificare ftd-vpn-engineer. Quindi, passare a Avanzate > Mappe certificati, fare clic su Aggiungi mapping pulsante.

Associa mapping certificati

Associazione del mapping dei certificati al profilo di connessione per il client VPN del tecnico.

- Nome mappa certificati: cert-map-engineer
- Connessione Profile: ftd-vpn-engineer

Add Connection Profile to Certificate Map ?

Choose a Certificate Map and associate Connection Profiles to selected Certificate Map.

Certificate Map Name*:

cert-map-engineer
▼

+

Connection Profile*:

ftd-vpn-engineer
▼

Cancel
OK

Mappa certificati di binding per client VPN del tecnico

Associazione del mapping dei certificati al profilo di connessione per il client VPN di gestione.

- Nome mappa certificati: cert-map-manager
- Profilo connessione: ftd-vpn-manager

Add Connection Profile to Certificate Map



Choose a Certificate Map and associate Connection Profiles to selected Certificate Map.

Certificate Map Name*:
cert-map-manager

+

Connection Profile*:
ftd-vpn-manager

Cancel OK

Associazione mappa certificati per client VPN di gestione

Confermare l'impostazione del binding dei certificati.

Firewall Management Center
Devices / VPN / Edit Advanced

Overview Analysis Policies Devices Objects Integration

Deploy Search Settings Help admin | Cisco SECURE

ftd-vpn-engineer You have unsaved changes Save Cancel

Enter Description Policy Assignments (1)

Local Realm: None Dynamic Access Policy: None

Connection Profile Access Interfaces Advanced

Secure Client Images
Secure Client Customization
GUI Text and Messages
Icons and Images
Scripts
Binaries
Custom Installer Transforms
Localized Installer Transforms
Address Assignment Policy
Certificate Maps
Group Policies

General Settings for Connection Profile Mapping
The device processes the policies in the order listed below until it finds a match

Use group URL if group URL and Certificate Map match different Connection Profiles
 Use the configured rules to match a certificate to a Connection Profile

Certificate to Connection Profile Mapping
Client request is checked against each Certificate Map, associated Connection Profile will be used when rules are matched. If none of the Certificate Map is matched, default connection profile will be chosen.

| Certificate Map | Connection Profile | |
|-------------------|--------------------|--|
| cert-map-engineer | ftd-vpn-engineer | |
| cert-map-manager | ftd-vpn-manager | |

Add Mapping

Conferma associazione certificato

Conferma nella CLI FTD

Confermare le impostazioni della connessione VPN nella CLI FTD dopo la distribuzione dal FMC.

```
// Defines IP of interface  
interface GigabitEthernet0/0
```

```
nameif outside
security-level 0
ip address 192.168.1.200 255.255.255.0

// Defines a pool of addresses
ip local pool ftd-vpn-engineer-pool 172.16.1.100-172.16.1.110 mask 255.255.255.0
ip local pool ftd-vpn-manager-pool 172.16.1.120-172.16.1.130 mask 255.255.255.0

// Defines Trustpoint for Server Certificate
crypto ca trustpoint ftd-vpn-cert
keypair ftd-vpn-cert
crl configure

// Server Certificate Chain
crypto ca certificate chain ftd-vpn-cert
certificate 22413df584b6726c
3082037c 30820264 a0030201 02020822 413df584 b6726c30 0d06092a 864886f7
.....
quit

certificate ca 5242a02e0db6f7fd
3082036c 30820254 a0030201 02020852 42a02e0d b6f7fd30 0d06092a 864886f7
.....
quit

// Defines Certificate Map for Engineer VPN Clients
crypto ca certificate map cert-map-engineer 10
subject-name attr cn eq vpnEngineerClientCN

// Defines Certificate Map for Manager VPN Clients
crypto ca certificate map cert-map-manager 10
subject-name attr cn eq vpnManagerClientCN

// Configures the FTD to allow Cisco Secure Client connections and the valid Cisco Secure Client images
webvpn
enable outside
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
no preload
hsts-client
enable
x-content-type-options
x-xss-protection
content-security-policy
anyconnect image disk0:/csm/cisco-secure-client-win-5.1.3.62-webdeploy-k9.pkg 1 regex "Windows"
anyconnect enable
tunnel-group-list enable
cache
disable
certificate-group-map cert-map-engineer 10 ftd-vpn-engineer
certificate-group-map cert-map-manager 10 ftd-vpn-manager
error-recovery disable

// Configures the group-policy to allow SSL connections from manager VPN clients
group-policy ftd-vpn-manager-grp internal
group-policy ftd-vpn-manager-grp attributes
banner none
wins-server none
dns-server none
```

```
dhcp-network-scope none
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
vpn-tunnel-protocol ikev2 ssl-client
split-tunnel-policy tunnelall
ipv6-split-tunnel-policy tunnelall
split-tunnel-network-list none
default-domain none
split-dns none
split-tunnel-all-dns disable
client-bypass-protocol disable
vlan none
address-pools none
webvpn
anyconnect ssl dtls enable
anyconnect mtu 1406
anyconnect firewall-rule client-interface public none
anyconnect firewall-rule client-interface private none
anyconnect ssl keepalive 20
anyconnect ssl rekey time none
anyconnect ssl rekey method none
anyconnect dpd-interval client 30
anyconnect dpd-interval gateway 30
anyconnect ssl compression none
anyconnect dtls compression none
anyconnect modules value none
anyconnect ask none default anyconnect
anyconnect ssl df-bit-ignore disable
```

```
// Configures the group-policy to allow SSL connections from engineer VPN clients
group-policy ftd-vpn-engineer-grp internal
group-policy ftd-vpn-engineer-grp attributes
banner none
wins-server none
dns-server none
dhcp-network-scope none
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelall
ipv6-split-tunnel-policy tunnelall
split-tunnel-network-list none
default-domain none
split-dns none
split-tunnel-all-dns disable
client-bypass-protocol disable
vlan none
address-pools none
webvpn
anyconnect ssl dtls enable
anyconnect mtu 1406
anyconnect firewall-rule client-interface public none
anyconnect firewall-rule client-interface private none
anyconnect ssl keepalive 20
```

```
anyconnect ssl rekey time none
anyconnect ssl rekey method none
anyconnect dpd-interval client 30
anyconnect dpd-interval gateway 30
anyconnect ssl compression none
anyconnect dtls compression none
anyconnect modules value none
anyconnect ask none default anyconnect
anyconnect ssl df-bit-ignore disable
```

```
// Configures the tunnel-group to use the certificate authentication for engineer VPN clients
tunnel-group ftd-vpn-engineer type remote-access
tunnel-group ftd-vpn-engineer general-attributes
address-pool ftd-vpn-engineer-pool
default-group-policy ftd-vpn-engineer-grp
tunnel-group ftd-vpn-engineer webvpn-attributes
authentication certificate
group-alias ftd-vpn-engineer enable
```

```
// Configures the tunnel-group to use the certificate authentication for manager VPN clients
tunnel-group ftd-vpn-manager type remote-access
tunnel-group ftd-vpn-manager general-attributes
address-pool ftd-vpn-manager-pool
default-group-policy ftd-vpn-manager-grp
tunnel-group ftd-vpn-manager webvpn-attributes
authentication certificate
```

Conferma in client VPN

Passaggio 1. Conferma certificato client

In Engineer VPN client, passare a Certificati - Utente corrente > Personale > Certificati, verificare il certificato client utilizzato per l'autenticazione.



Conferma certificato per il client VPN del tecnico

Fare doppio clic sul certificato client, passare a Dettagli, controllare i dettagli di Oggetto.

- Oggetto: CN = vpnEngineerClientCN

Certificate



General Details Certification Path

Show: <All>

| Field | Value |
|-----------------------|------------------------------------|
| Valid to | Wednesday, June 18, 2025 5:... |
| Subject | vpnEngineerClientCN, vpnEngi... |
| Public key | RSA (2048 Bits) |
| Public key parameters | 05 00 |
| Key Usage | Digital Signature, Key Encipher... |
| Enhanced Key Usage | Client Authentication (1.3.6.1.... |
| Netscape Comment | xca certificate |
| Thumbprint algorithm | sha1 |

CN = vpnEngineerClientCN
O = Cisco
L = Tokyo
S = Tokyo
C = JP

Edit Properties...

Copy to File...

OK

Dettagli del certificato client del tecnico

In Manager VPN client, passare a Certificati - Utente corrente > Personale > Certificati, controllare il certificato client utilizzato per l'autenticazione.



Conferma certificato per client VPN di gestione

Fare doppio clic sul certificato client, passare a Dettagli, controllare i dettagli di Oggetto.

- Oggetto: CN = vpnManagerClientCN

Certificate



General Details Certification Path

Show: <All>

| Field | Value |
|-----------------------|------------------------------------|
| Issued | Thursday, June 19, 2025 9:41... |
| Subject | vpnManagerClientCN, vpnMan... |
| Public Key | RSA (2048 Bits) |
| Public key parameters | 05 00 |
| Key Usage | Digital Signature, Key Encipher... |
| Enhanced Key Usage | Client Authentication (1.3.6.1.... |
| Netscape Comment | xca certificate |
| Thumbprint algorithm | sha1 |

CN = vpnManagerClientCN

O = Cisco
L = Tokyo
S = Tokyo
C = JP

Edit Properties...

Copy to File...

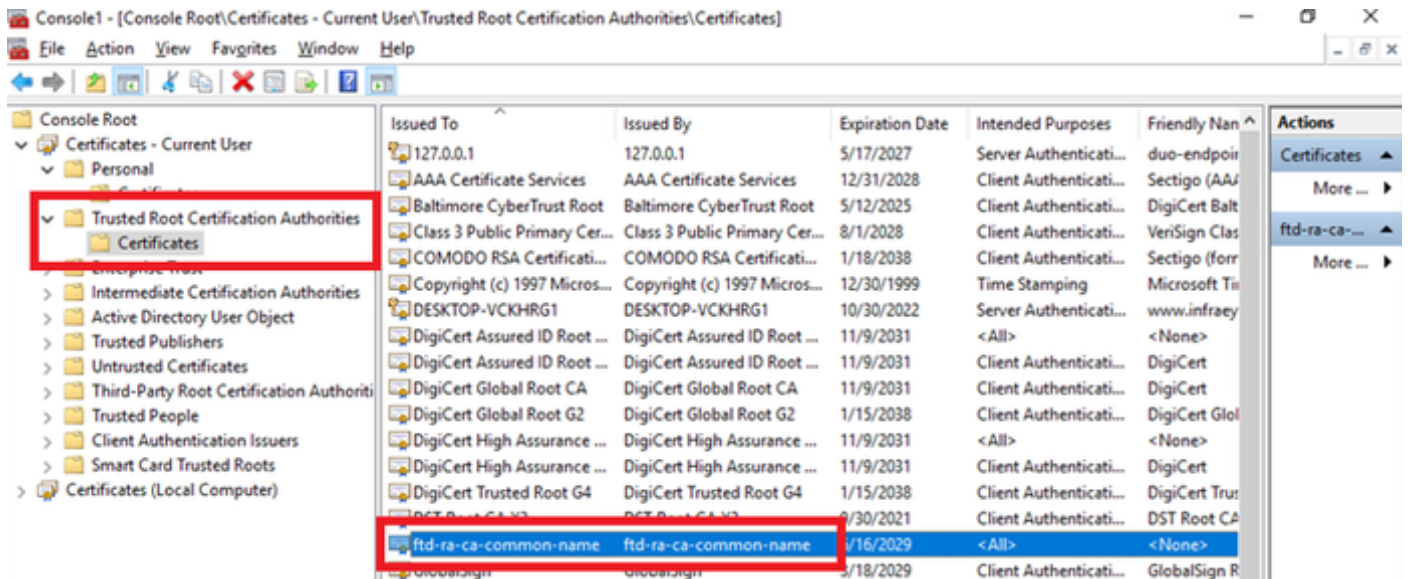
OK

Dettagli del certificato client del gestore

Passaggio 2. Conferma CA

In entrambi i client VPN Engineer e manager, passare a Certificati - Utente corrente > Autorità di certificazione radice attendibili > Certificati, quindi controllare la CA utilizzata per l'autenticazione.

- Rilasciato da: ftd-ra-ca-common-name

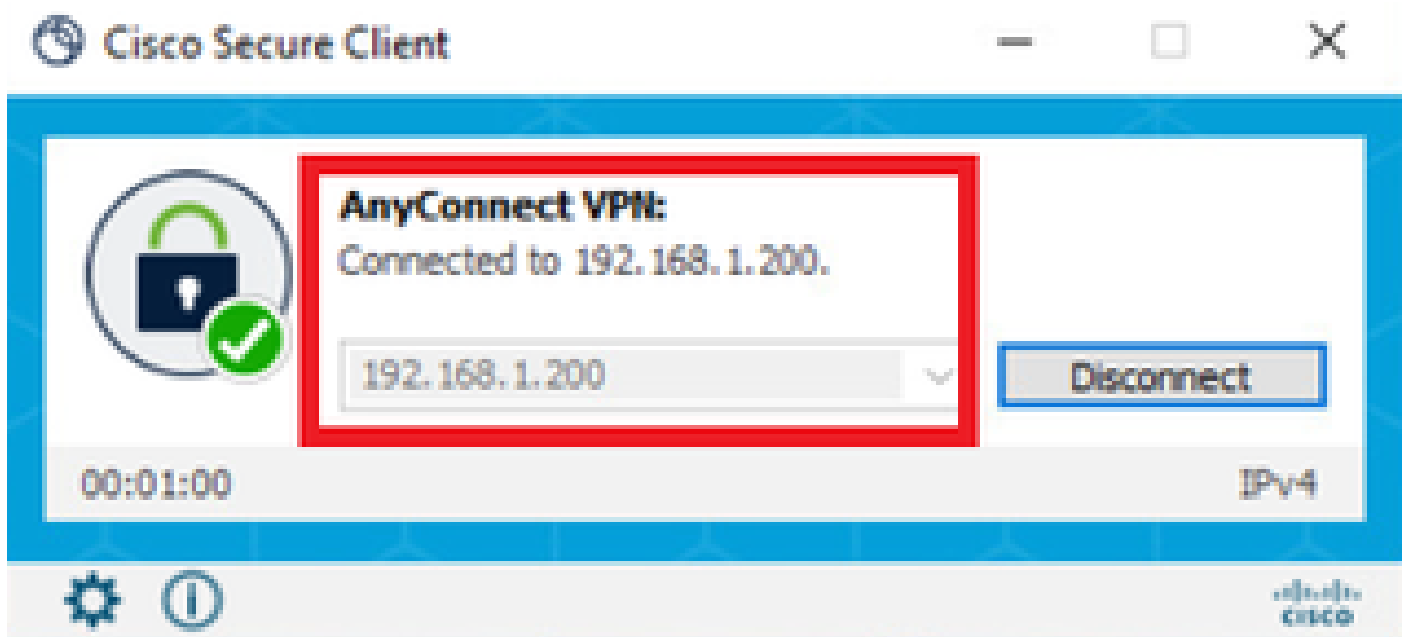


Conferma CA

Verifica

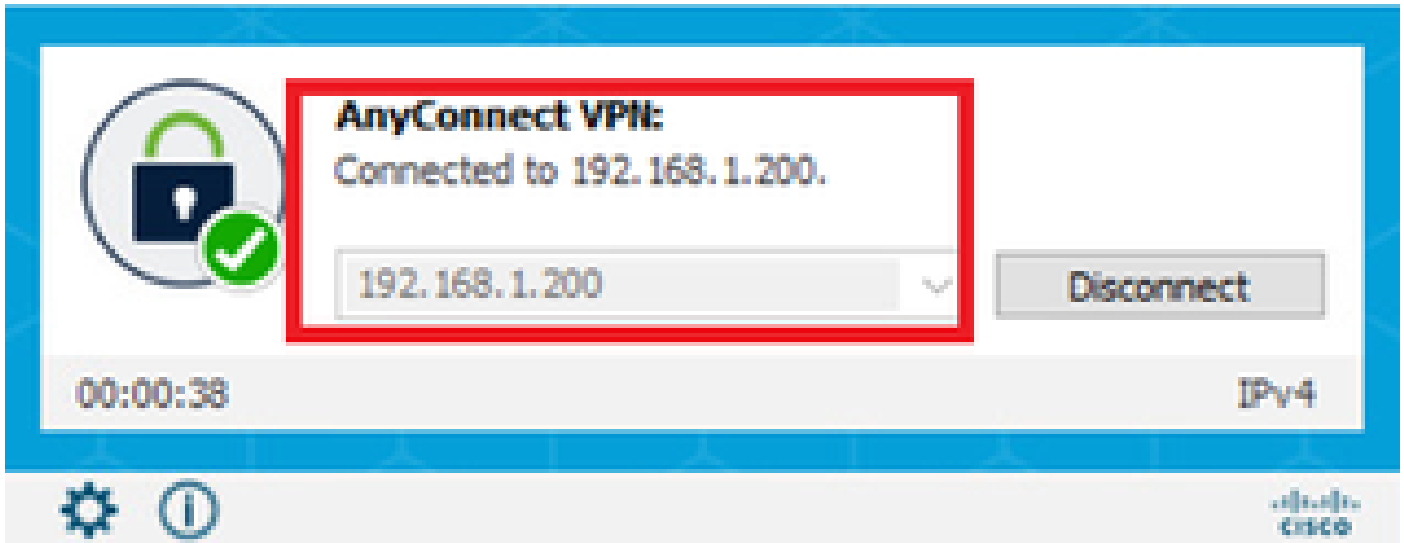
Passaggio 1. Avvia connessione VPN

In Engineer VPN Client, avviare la connessione Cisco Secure Client. Non è necessario immettere il nome utente e la password. La VPN è stata connessa correttamente.



Avvia connessione VPN dal client del tecnico

Nel client VPN di gestione, avviare la connessione Cisco Secure Client. Non è necessario immettere il nome utente e la password. La VPN è stata connessa correttamente.



Avvia connessione VPN dal client di gestione

Passaggio 2. Conferma sessioni attive in FMC

Passare ad Analisi > Utenti > Sessioni attive, verificare la sessione attiva per l'autenticazione VPN.

| Login Time | Realm\Username | Last Seen | Authentication Type | Current IP | Realm | Username ↓ | First Name | Last Name |
|---------------------|---|---------------------|---------------------|--------------|-----------------------|---------------------|------------|-----------|
| 2024-06-19 11:01:19 | Discovered Identities\vpnManagerClientCN | 2024-06-19 11:01:19 | VPN Authentication | 172.16.1.120 | Discovered Identities | vpnManagerClientCN | | |
| 2024-06-19 11:00:35 | Discovered Identities\vpnEngineerClientCN | 2024-06-19 11:00:35 | VPN Authentication | 172.16.1.101 | Discovered Identities | vpnEngineerClientCN | | |

Conferma sessione attiva

Passaggio 3. Conferma sessioni VPN nella CLI FTD

Esegui `show vpn-sessiondb detail anyconnect` il comando nella CLI di FTD (Lina) per confermare le sessioni VPN di Engineer e Manager.

```
ftd702# show vpn-sessiondb detail anyconnect
```

Session Type: AnyConnect Detailed

Username : vpnEngineerClientCN Index : 13

Assigned IP : 172.16.1.101 Public IP : 192.168.1.11

Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel

License : AnyConnect Premium

Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-128 DTLS-Tunnel: (1)AES-GCM-256

Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA256 DTLS-Tunnel: (1)SHA384

Bytes Tx : 14782 Bytes Rx : 12714

Pkts Tx : 2 Pkts Rx : 32

Pkts Tx Drop : 0 Pkts Rx Drop : 0

Group Policy : ftd-vpn-engineer-grp Tunnel Group : ftd-vpn-engineer
Login Time : 02:00:35 UTC Wed Jun 19 2024
Duration : 0h:00m:55s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : cb0071820000d00066723bc3
Security Grp : none Tunnel Zone : 0

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

AnyConnect-Parent:
Tunnel ID : 13.1
Public IP : 192.168.1.11
Encryption : none Hashing : none
TCP Src Port : 50225 TCP Dst Port : 443
Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : win
Client OS Ver: 10.0.15063
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 7391 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 13.2
Assigned IP : 172.16.1.101 Public IP : 192.168.1.11
Encryption : AES-GCM-128 Hashing : SHA256
Ciphersuite : TLS_AES_128_GCM_SHA256
Encapsulation: TLSv1.3 TCP Src Port : 50232
TCP Dst Port : 443 Auth Mode : Certificate
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 5.1.3.62
Bytes Tx : 7391 Bytes Rx : 1775
Pkts Tx : 1 Pkts Rx : 2
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 13.3
Assigned IP : 172.16.1.101 Public IP : 192.168.1.11
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 50825
UDP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 0 Bytes Rx : 10939
Pkts Tx : 0 Pkts Rx : 30
Pkts Tx Drop : 0 Pkts Rx Drop : 0

Username : vpnManagerClientCN Index : 14
Assigned IP : 172.16.1.120 Public IP : 192.168.1.21

Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-128 DTLS-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA256 DTLS-Tunnel: (1)SHA384
Bytes Tx : 14782 Bytes Rx : 13521
Pkts Tx : 2 Pkts Rx : 57
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : ftd-vpn-manager-grp Tunnel Group : ftd-vpn-manager
Login Time : 02:01:19 UTC Wed Jun 19 2024
Duration : 0h:00m:11s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : cb0071820000e00066723bef
Security Grp : none Tunnel Zone : 0

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

AnyConnect-Parent:

Tunnel ID : 14.1
Public IP : 192.168.1.21
Encryption : none Hashing : none
TCP Src Port : 49809 TCP Dst Port : 443
Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : win
Client OS Ver: 10.0.15063
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 7391 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:

Tunnel ID : 14.2
Assigned IP : 172.16.1.120 Public IP : 192.168.1.21
Encryption : AES-GCM-128 Hashing : SHA256
Ciphersuite : TLS_AES_128_GCM_SHA256
Encapsulation: TLSv1.3 TCP Src Port : 49816
TCP Dst Port : 443 Auth Mode : Certificate
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 5.1.3.62
Bytes Tx : 7391 Bytes Rx : 3848
Pkts Tx : 1 Pkts Rx : 25
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:

Tunnel ID : 14.3
Assigned IP : 172.16.1.120 Public IP : 192.168.1.21
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 65501
UDP Dst Port : 443 Auth Mode : Certificate
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 5.1.3.62
Bytes Tx : 0 Bytes Rx : 9673
Pkts Tx : 0 Pkts Rx : 32
Pkts Tx Drop : 0 Pkts Rx Drop : 0

Risoluzione dei problemi

Per informazioni sull'autenticazione VPN, vedere il syslog di debug del motore Lina e il file DART nel computer Windows.

Questo è un esempio di log di debug nel motore Lina durante la connessione VPN da un client di progettazione.

<#root>

Jun 19 2024 02:00:35: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 7AF1C78ADCC8F941, subject name: CN=vpnEngineerClientCN
Jun 19 2024 02:00:35: %FTD-6-717022:

Certificate was successfully validated

. serial number: 7AF1C78ADCC8F941, subject name:

CN=vpnEngineerClientCN

,OU=vpnEngineerClientOU,O=Cisco,L=Tokyo,ST=Tokyo,C=JP.

Jun 19 2024 02:00:35: %FTD-7-717038: Tunnel group match found.

Tunnel Group: ftd-vpn-engineer

, Peer certificate: serial number: 7AF1C78ADCC8F941, subject name: CN=vpnEngineerClientCN,OU=vpnEngineerClientOU,O=Cisco,L=Tokyo,ST=Tokyo,C=JP.

Jun 19 2024 02:00:35: %FTD-6-113009: AAA retrieved default group policy (ftd-vpn-engineer-grp) for user

Jun 19 2024 02:00:46: %FTD-6-725002: Device completed SSL handshake with client outside:192.168.1.11/50

Questo è un esempio di log di debug nel motore Lina durante la connessione VPN dal client di gestione.

<#root>

Jun 19 2024 02:01:19: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 1AD1B5EAE28C6D3C, subject name: CN=vpnManagerClientCN
Jun 19 2024 02:01:19: %FTD-6-717022:

Certificate was successfully validated

. serial number: 1AD1B5EAE28C6D3C, subject name:

CN=vpnManagerClientCN

,OU=vpnManagerClientOU,O=Cisco,L=Tokyo,ST=Tokyo,C=JP.

Jun 19 2024 02:01:19: %FTD-7-717038: Tunnel group match found.

Tunnel Group: ftd-vpn-manager

, Peer certificate: serial number: 1AD1B5EAE28C6D3C, subject name: CN=vpnManagerClientCN,OU=vpnManagerClientOU,O=Cisco,L=Tokyo,ST=Tokyo,C=JP.

Jun 19 2024 02:01:19: %FTD-6-113009: AAA retrieved default group policy (ftd-vpn-manager-grp) for user

Jun 19 2024 02:01:25: %FTD-6-725002: Device completed SSL handshake with client outside:192.168.1.21/65

Informazioni correlate

[Configurazione dell'autenticazione basata sul certificato Anyconnect per l'accesso mobile](#)

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).