

Configurazione dell'autenticazione dei certificati client protetti su FTD Gestito da FMC

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[a. Creazione/importazione di un certificato utilizzato per l'autenticazione server](#)

[b. Aggiungere un certificato CA attendibile/interno](#)

[c. Configurare il pool di indirizzi per gli utenti VPN](#)

[d. Caricamento di immagini client sicure](#)

[e. Crea e carica profilo XML](#)

[Configurazione VPN di accesso remoto](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto il processo di configurazione della VPN ad accesso remoto su Firepower Threat Defense (FTD) gestita da Firepower Management Center (FMC) con autenticazione del certificato.

Contributo di Dolly Jain e Rishabh Aggarwal, Cisco TAC Engineer.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Registrazione manuale dei certificati e nozioni di base di SSL
- FMC
- Conoscenze base di autenticazione per VPN ad accesso remoto
- CA (Certification Authority) di terze parti come Entrust, Geotrust, GoDaddy, Thawte e VeriSign

Componenti usati

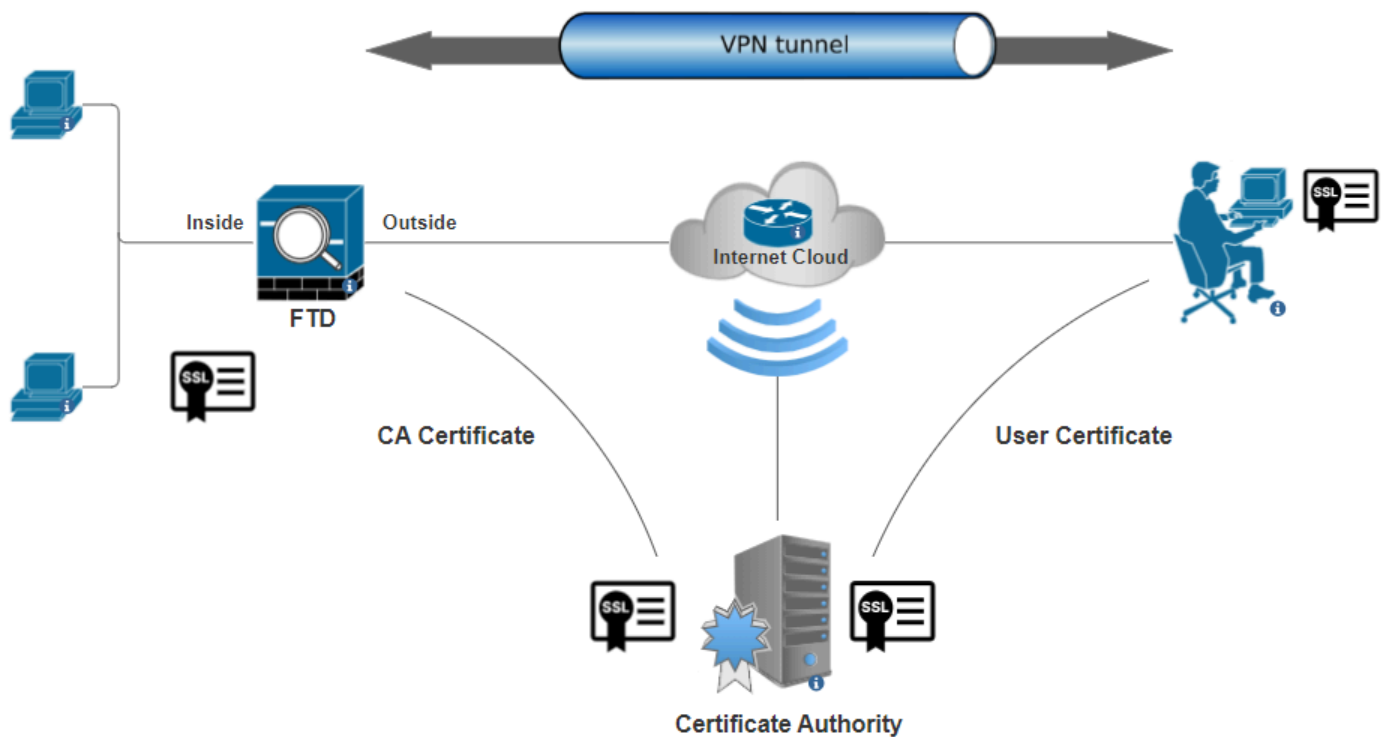
Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

- Secure Firepower Threat Defense versione 7.4.1
- Firepower Management Center (FMC) versione 7.4.1
- Secure Client versione 5.0.05040
- Microsoft Windows Server 2019 come server CA

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.

Configurazione

Esempio di rete



Esempio di rete

Configurazioni

a. Creazione/importazione di un certificato utilizzato per l'autenticazione server



Nota: nel CCP è necessario un certificato CA prima di poter generare il CSR. Se CSR viene generato da un'origine esterna (OpenSSL o di terze parti), il metodo manuale ha esito negativo ed è necessario utilizzare il formato del certificato PKCS12.

Passaggio 1. Individuare Devices > Certificatese fare clic su Add. Selezionare Device (Dispositivo) e fare clic sul segno più (+) in Cert Enrollment (Registrazione certificato).

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*:

Cancel

Add

Aggiungi registrazione certificato

Passaggio 2. In Tipo di registrazione selezionare come CA Information Manual e incollare il certificato dell'Autorità di certificazione (CA) utilizzato per firmare il CSR.

Add Cert Enrollment



Name*

ssl_certificate

Description

CA Information

Certificate Parameters

Key

Revocation

Enrollment Type:

Manual

CA Only

Check this option if you do not require an identity certificate to be created from this CA

CA Certificate:

```
HQYDVQQDEZXIeWRyYXV5S0S
UQgU2VydMvYlENBIE8xMIIBlj
ANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEA6
huZbDVWWMGj7XbFZQWI+uhh
0SleWhO8rI79MV4+7ZSj2
Lxos5e8za0H1JVVzTNPaup2G
o438C5zeaqaGtyUshV8D0xw
UiWyamspTao7PjjuC
h81+tp9z76rp1irjNMh5o/zeJ0
h3Kag5zQG9sfI7J7ihLnTFbArj
N7ID-7zooQw
```

Validation Usage:



IPsec Client



SSL Client



SSL Server



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

Cancel

Save

Aggiungi informazioni sulla CA

Passaggio 3. Per Uso convalida, selezionare IPsec Client, SSL Client e Skip Check for CA flag in basic constraints of the CA Certificate.

Passaggio 4. In Certificate Parameters, immettere i dettagli relativi al nome dell'oggetto.

Add Cert Enrollment



Name*

ssl_certificate

Description

CA Information

Certificate Parameters

Key

Revocation

Include FQDN: Don't use FQDN in certificate ▼

Include Device's IP Address:

Common Name (CN): certauth.cisco.com

Organization Unit (OU): TAC

Organization (O): Cisco

Locality (L): Bangalore

State (ST): KA

Country Code (C): IN

Email (E):

Include Device's Serial Number

Cancel

Save

Aggiungi parametri certificato

Passaggio 5. In Keyselezionare il tipo di chiave come RSA con un nome e una dimensione per la chiave. Fare clic su Save.



Nota: per il tipo di chiave RSA, le dimensioni minime della chiave sono 2048 bit.

Add Cert Enrollment



Name*
ssl_certificate

Description

CA Information Certificate Parameters **Key** Revocation

Key Type:
 RSA ECDSA EdDSA

Key Name:*
rsakey

Key Size:
2048 ▼

▼ Advanced Settings

Ignore IPsec Key Usage

Cancel **Save**

Aggiungi chiave RSA

Passaggio 6. In Cert Enrollment, selezionare il trust point dall'elenco a discesa appena creato e fare clic su Add.

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:

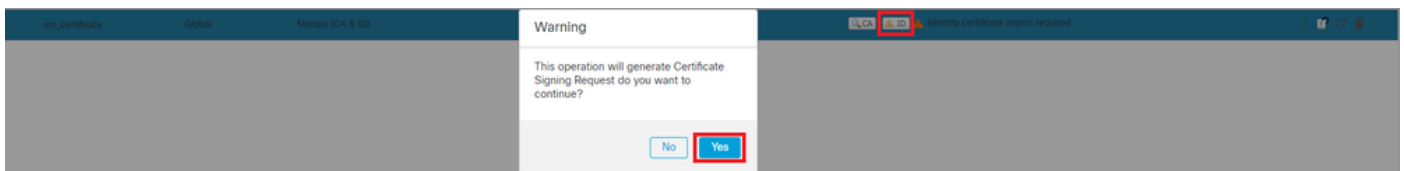
Name: ssl_certificate
Enrollment Type: Manual (CA & ID)
Enrollment URL: N/A

Cancel

Add

Aggiungi nuovo certificato

Passaggio 7. Fare clic su ID, quindi fare clic su inYes un'ulteriore richiesta per generare il CSR.



Genera CSR

Passaggio 8. Copiare il CSR e ottenerne la firma da parte dell'Autorità di certificazione. Una volta che il certificato di identità è stato rilasciato dalla CA, importarlo facendo clic su Browse Identity Certificate e fare clic su Import .

Import Identity Certificate



Step 1

Send Certificate Signing Request (CSR) to the Certificate Authority.

Certificate Signing Request (Copy the CSR below and send to the Certificate Authority):

```
-----BEGIN CERTIFICATE REQUEST-----
MIIEyTCCArECAQAwVTEMMAoGA1UECwwDVVEFDMQ4wDAYDVQQKDAVDaXNjbzEbMBkG
A1UEAwwSY2VydGF1dGguY2lzY28uY29tMQswCQYDVQQIDAJLQTELMakGA1UEBhMC
SU4wggliMA0GCsqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDNZr431mtYG+f1bLFK
WY9Zd9wTaJfqs87FtAW7+n4UuxLDws54R/txe9teX/65uSyY8/bxKfdsgMq5rawO
3dogCVQjtAtel+95np1/myzFOZZRWfeBdK/H1pLEdR4X6ZlnM5fNA/GLV9MnPoP
ppzi0uLlbVmb5iKQexllaur/e3PBccc3eC57e+D3QhKQ9SC7um8ulwueF+70fKYe
```

Step 2

Once certificate authority responds back with identity certificate file, import it to device.

Identity Certificate File:

[Browse Identity Certificate](#)

Cancel

Import

Importa certificato ID



Nota: se il rilascio del certificato ID richiede tempo, è possibile ripetere il passaggio 7 in seguito. In questo modo verrà generato lo stesso CSR e sarà possibile importare il certificato ID.

b. Aggiungere un certificato CA attendibile/interno



Nota: se l'Autorità di certificazione (CA) utilizzata nel passaggio (a), "**Crea/importa un certificato utilizzato per l'autenticazione server**" emette anche certificati utente, è possibile ignorare il **passaggio (b)**, "**Aggiungi un certificato CA attendibile/interno**". Non è necessario aggiungere di nuovo lo stesso certificato CA e deve essere evitato. Se lo stesso certificato CA viene aggiunto di nuovo, il trust point è configurato con "validation-usage none" che può influire sull'autenticazione del certificato per RAVPN.

Passaggio 1. Individuare Devices > Certificates e fare clic su Add.

Selezionare Device (Dispositivo) e fare clic sul segno più (+) in Cert Enrollment (Registrazione certificato).

In questo caso, per il rilascio dei certificati di identità/utente viene utilizzato "auth-risaggar-ca".

General Details Certification Path



Certificate Information

This certificate is intended for the following purpose(s):

- All issuance policies
- All application policies

Issued to: auth-risaggar-ca

Issued by: auth-risaggar-ca

Valid from 04-03-2023 **to** 04-03-2033

Issuer Statement

OK

auth-risaggar-ca

Passaggio 2. Immettere un nome di trust e selezionare Manual come tipo di iscrizione in CA information.

Passaggio 3. Controllare CA Only e incollare il certificato CA attendibile/interna in formato pem.

Passaggio 4. Selezionare **Skip Check for CA flag in basic constraints of the CA Certificate** fare clic su Save.

Add Cert Enrollment ?

Internal_CA

Description

CA InformationCertificate ParametersKeyRevocation

Enrollment Type: Manual

CA Only

Check this option if you do not require an identity certificate to be created from this CA

CA Certificate:

```
-----BEGIN CERTIFICATE-----  
--  
MIIG1jCCBL6gAwIBAgIQQAFu  
+wogXPrr4Y9x1zq7eDANBgk  
qhkiG9w0BAQsFADBK  
MQswCQYDVQQGEwJVUzES  
MBAGA1UEChMJSWRlbiRydX  
N0MScwJQYDVQQDEw5JZGV  
u  
VHJ1c3QgQ29tbWVyY2lhbCB  
Sb290IENBIDUwHhcNMTkxMj
```

Validation Usage: IPsec Client SSL Client SSL Server

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

CancelSave

Aggiungi Trustpoint

Passaggio 5. In Cert Enrollment, selezionare il trust point dall'elenco a discesa appena creato e fare clic su Add.

Add New Certificate



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

Device*:

FTD-A-7.4.1 ▼

Cert Enrollment*:

Internal_CA ▼ +

Cert Enrollment Details:

Name: Internal_CA
Enrollment Type: Manual (CA Only)
Enrollment URL: N/A

Cancel

Add

Aggiungi CA interna

Passaggio 6. Il certificato aggiunto in precedenza viene visualizzato come segue:

Internal_CA	Global	Manual (CA Only)	Mar 4, 2033	CA ID	⌵ ⌵ ⌵ ⌵
-------------	--------	------------------	-------------	-------	---------

Certificato aggiunto

c. Configurare il pool di indirizzi per gli utenti VPN

Passaggio 1. Passare a Objects > Object Management > Address Pools > IPv4 Pools .

Passaggio 2. Immettere il nome e l'intervallo di indirizzi IPv4 con una maschera.

Edit IPv4 Pool



Name*

vpn_pool

Description

IPv4 Address Range*

10.20.20.1-10.20.20.130

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

Aggiungi pool IPv4

d. Caricamento di immagini client sicure

Passaggio 1. Scaricare dal sito [software Cisco](https://www.cisco.com) le immagini client sicure distribuite sul Web in base al sistema operativo.

Passaggio 2. Passare a Objects > Object Management > VPN > Secure Client File > Add Secure Client File .

Passaggio 3. Immettere il nome e selezionare il file Secure Client dal disco.

Passaggio 4. Selezionare il tipo di file Secure Client Image e fare clic su Save.

Edit Secure Client File



Name:*

File Name:*

File Type:*

Description:

Aggiungi immagine client sicura

e. Crea e carica profilo XML

Passaggio 1. Scaricare e installare Secure Client Profile Editor dal sito [software Cisco](#).

Passaggio 2. Creare un nuovo profilo e selezionarlo All dall'elenco a discesa Selezione certificato client. Controlla principalmente gli archivi certificati che Secure Client può utilizzare per archiviare e leggere i certificati.

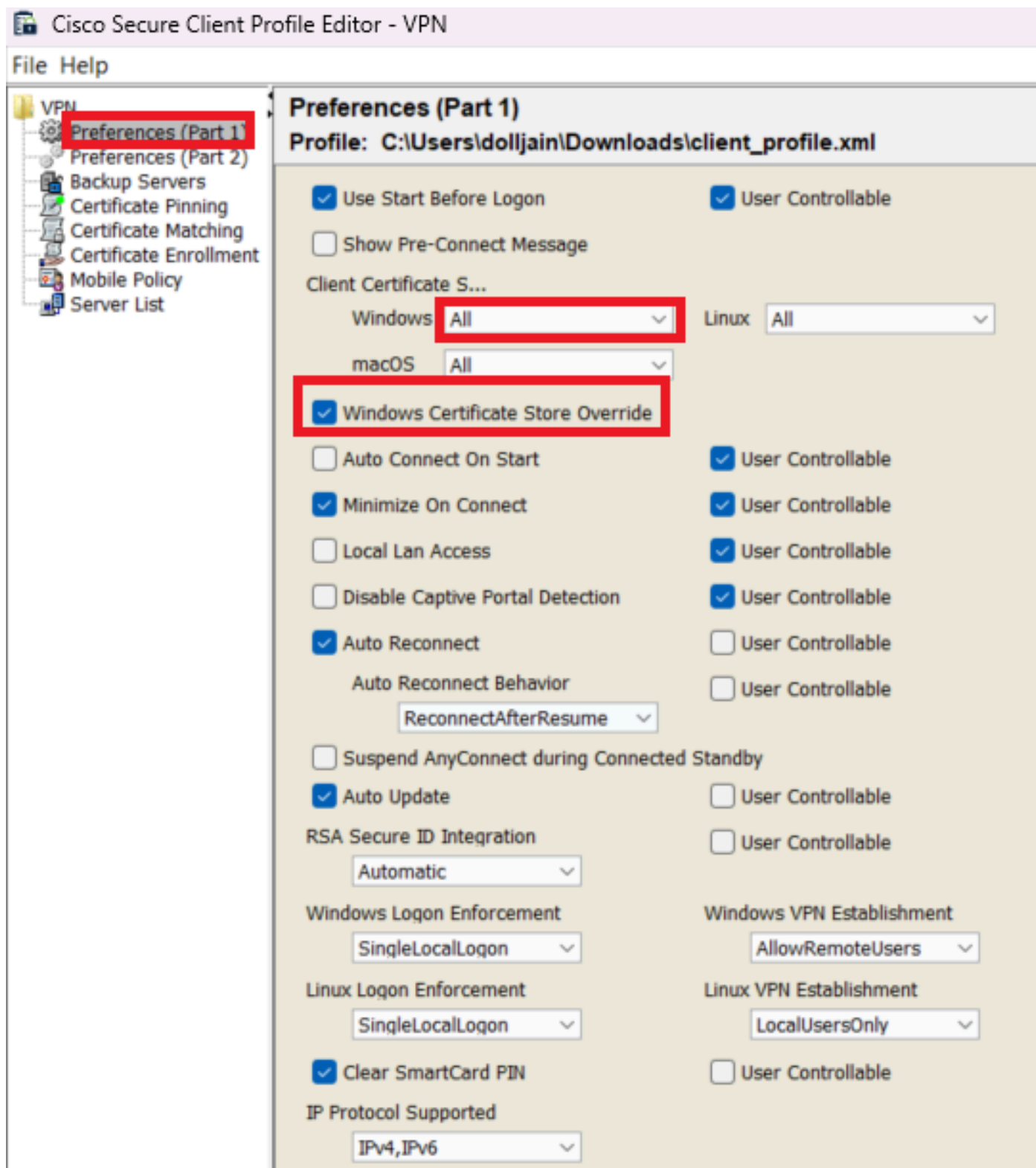
Altre due opzioni disponibili sono:

- **Computer** - Client protetto è limitato alla ricerca di certificati nell'archivio certificati del computer locale di Windows.
- **Utente** - Client protetto è limitato alla ricerca di certificati nell'archivio certificati utente locale di Windows.

Imposta sostituzione archivio certificati come True .

In questo modo un amministratore può indirizzare Secure Client all'utilizzo dei certificati nell'archivio certificati del computer Windows

(sistema locale) per l'autenticazione dei certificati client. L'override dell'archivio certificati si applica solo a SSL, in cui la connessione viene avviata per impostazione predefinita dal processo dell'interfaccia utente. Quando si utilizza IPSec/IKEv2, questa funzionalità del profilo client protetto non è applicabile.



Aggiungi preferenze (Parte 1)

Passaggio 3. (Facoltativo) Deselezionare l'opzione Disable Automatic Certificate Selection in quanto evita la richiesta all'utente di selezionare il certificato di autenticazione.

- VPN
- Preferences (Part 1)
- Preferences (Part 2)**
- Backup Servers
- Certificate Pinning
- Certificate Matching
- Certificate Enrollment
- Mobile Policy
- Server List

Preferences (Part 2)

Profile: C:\Users\dolljain\Downloads\client_profile.xml

Disable Automatic Certificate Selection

User Controllable

Proxy Settings

Native

User Controllable

Public Proxy Server Address:

Note: Enter public Proxy Server address and Port here. Example:10.86.125.33:8080

Allow Local Proxy Connections

Enable Optimal Gateway Selection

User Controllable

Suspension Time Threshold (hours)

Performance Improvement Threshold (%)

Automatic VPN Policy

Trusted Network Policy

Untrusted Network Policy

Bypass connect upon VPN session timeout

Trusted DNS Domains

Trusted DNS Servers

Note: adding all DNS servers in use is recommended with Trusted Network Detection

Trusted Servers @ https://<server>[:<port>]

https://

Add

Delete

Certificate Hash:

Set

Disable interfaces without trusted server connectivity while in truste...

Always On

(More Information)

Allow VPN Disconnect

Allow access to the following hosts with VPN disconn...

Connect Failure Policy

Allow Captive Portal Remediation

Remediation Timeout (min.)

Apply Last VPN Local Resource Rules

Captive Portal Remediation Browser Failover

Allow Manual Host Input

PPP Exclusion

User Controllable

PPP Exclusion Server IP

User Controllable

Enable Scripting

User Controllable

Terminate Script On Next Event

Enable Post SBL On Connect Script

Retain VPN on Logoff

User Enforcement

Authentication Timeout (seconds)

Server List Entry Creare un URL per la configurazione di un profilo nella VPN client sicura fornendo l'alias di gruppo e l'URL di gruppo nell'elenco dei server e salvare il profilo XML.

The screenshot shows the Cisco Secure Client Profile Editor - VPN interface. The main window displays the 'Server List' for a profile named 'C:\Users\dolljain\Downloads\client_profile.xml'. A table lists server entries, with the first entry 'SSL-VPN' highlighted in red. The 'Server List Entry' dialog is open, showing configuration details for the selected server.

Hostname	Host Address	User Group	Backup Serve...	SCEP	Mobile Settings	Certificate Pins
SSL-VPN	https://certaut...	ssl-cert	-- Inherited --			

Note: it is highly recommended that at least one server be defined in a profile.

Buttons: Add..., Delete, Edit..., Details

Server List Entry

Server | Load Balancing Servers | SCEP | Mobile | Certificate Pinning

Primary Server

Display Name (required): SSL-VPN

FQDN or IP Address: https://certauth.cisco.com / User Group: ssl-cert

Group URL: [Empty]

Connection Information

Primary Protocol: SSL

ASA gateway

Auth Method During IKE Negotiation: EAP-AnyConnect

IKE Identity (IOS gateway only): [Empty]

Backup Servers

Host Address: [Empty] Add

Move Up, Move Down, Delete

OK, Cancel

Aggiungi elenco server

Passaggio 5. Infine, il profilo XML è pronto per essere utilizzato.

```

<?xml version="1.0" encoding="UTF-8" ?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
  <ClientInitialization>
    <UseStartBeforeLogon UserControllable="true">true</UseStartBeforeLogon>
    <AutomaticCertSelection UserControllable="false">true</AutomaticCertSelection>
    <ShowPreConnectMessage>false</ShowPreConnectMessage>
    <CertificateStoreAll</CertificateStore>
    <CertificateStoreMac>All</CertificateStoreMac>
    <CertificateStoreLinux>All</CertificateStoreLinux>
    <CertificateStoreOverride>true</CertificateStoreOverride>
    <ProxySettings>Native</ProxySettings>
    <AllowLocalProxyConnections>true</AllowLocalProxyConnections>
    <AuthenticationTimeout>30</AuthenticationTimeout>
    <AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
    <MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
    <LocalLanAccess UserControllable="true">false</LocalLanAccess>
    <DisableCaptivePortalDetection UserControllable="true">false</DisableCaptivePortalDetection>
    <ClearSmartcardPin UserControllable="false">true</ClearSmartcardPin>
    <IPProtocolSupport>IPv4,IPv6</IPProtocolSupport>
    <AutoReconnect UserControllable="false">true
      <AutoReconnectBehavior UserControllable="false">ReconnectAfterResume</AutoReconnectBehavior>
    </AutoReconnect>
    <SuspendOnConnectedStandby>false</SuspendOnConnectedStandby>
    <AutoUpdate UserControllable="false">true</AutoUpdate>
    <RSA SecurIDIntegration UserControllable="false">Automatic</RSA SecurIDIntegration>
    <WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
    <LinuxLogonEnforcement>SingleLocalLogon</LinuxLogonEnforcement>
    <WindowsVFNEstablishment>AllowRemoteUsers</WindowsVFNEstablishment>
    <LinuxVFNEstablishment>LocalUsersOnly</LinuxVFNEstablishment>
    <AutomaticVPNPolicy>false</AutomaticVPNPolicy>
    <PPPEExclusion UserControllable="false">Disable
      <PPPEExclusionServerIP UserControllable="false"></PPPEExclusionServerIP>
    </PPPEExclusion>
    <EnableScripting UserControllable="false">false</EnableScripting>
    <EnableAutomaticServerSelection UserControllable="false">false
      <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
      <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
    </EnableAutomaticServerSelection>
    <RetainVpnOnLogoff>false
      </RetainVpnOnLogoff>
    <CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover>
    <AllowManualHostInput>true</AllowManualHostInput>
  </ClientInitialization>
  <ServerList>
    <HostEntry>
      <HostName>SSL-VPN</HostName>
      <HostAddress>https://certauth.cisco.com</HostAddress>
      <UserGroup>ssl-cert</UserGroup>
    </HostEntry>
  </ServerList>
</AnyConnectProfile>

```

Profilo XML

Posizione dei profili XML per vari sistemi operativi:

- **Windows** - C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile
- **MacOS** - /opt/cisco/anyconnect/profile
- **Linux** - /opt/cisco/anyconnect/profile

Passaggio 6. Passare a Objects > Object Management > VPN > Secure Client File > Add Secure Client Profile .

Immettere il nome del file e fare clic su Browse per selezionare il profilo XML. Fare clic su .Save

Edit Secure Client File



Name:*

File Name:*

File Type:*

Description:

Aggiungi profilo VPN client sicuro

Configurazione VPN di accesso remoto

Passaggio 1. Creare un ACL in base ai requisiti per consentire l'accesso alle risorse interne.

Individuare Objects > Object Management > Access List > Standard e fare clic su Add Standard Access List.

Edit Standard Access List Object



Name

Split_ACL

▼ Entries (1)

Add

Sequence No	Action	Network	
1	Allow	split_acl	

Allow Overrides

Cancel

Save

Aggiungi ACL standard



Nota: questo ACL viene utilizzato da Secure Client per aggiungere route sicure alle risorse interne.

Passaggio 2. Individuare Devices > VPN > Remote Access e fare clic su Add.

Passaggio 3. Immettere il nome del profilo, quindi selezionare il dispositivo FTD e fare clic su Avanti.

Remote Access VPN Policy Wizard

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

Targeted Devices and Protocols

This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.

Name:*

RAVPN

Description:

VPN Protocols:

- SSL
 IPsec-IKEv2

Targeted Devices:

Available Devices	Selected Devices
<input type="text" value="Q Search"/>	FTD-A-7.4.1
FTD-A-7.4.1	
FTD-B-7.4.0	
FTD-ZTNA-7.4.1	
<input type="button" value="Add"/>	

Before You Start

Before you start, ensure the following configuration elements to be in place to complete Remote Access VPN Policy.

Authentication Server

Configure [LOCAL](#) or [Realm](#) or [RADIUS Server Group](#) or [SSO](#) to authenticate VPN clients.

Secure Client Package

Make sure you have Secure Client package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.

Device Interface

Interfaces should be already configured on targeted devices so that they can be used as a security zone or interface group to enable VPN access.

Aggiungi nome profilo

Passaggio 4. Immettere il nome del server Connection Profile Name e selezionare il metodo di autenticazione come Client Certificate Only in Autenticazione, autorizzazione e accounting (AAA).

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:* RAVPN-CertAuth

i This name is configured as a connection alias, it can be used to connect to the VPN gateway

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: Client Certificate Only

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

Primary Field: CN (Common Name)

Secondary Field: OU (Organisational Unit)

Authorization Server: +
(Realm or RADIUS)

Accounting Server: +
(RADIUS)

Seleziona metodo di autenticazione

Passaggio 5. Fare clic su Use IP Address Pools in Assegnazione indirizzo client e selezionare il pool di indirizzi IPv4 creato in precedenza.


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: 

Seleziona assegnazione indirizzo client

Passaggio 6. Modificare i Criteri di gruppo.

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](#)

Modifica Criteri di gruppo

Passaggio 7. Passare a General > Split Tunneling, selezionare Tunnel networks specified below e selezionare Standard Access List in Tipo di elenco reti tunnel suddiviso.

Selezionare l'ACL creato in precedenza.

Edit Group Policy



Name:*

DfltGrpPolicy

Description:

General

Secure Client

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

IPv4 Split Tunneling:

Tunnel networks specified below ▼

IPv6 Split Tunneling:

Allow all traffic over tunnel ▼

Split Tunnel Network List Type:

Standard Access List Extended Access List

Standard Access List:

Split_ACL ▼ +

DNS Request Split Tunneling

DNS Requests:

Send DNS requests as per split t ▼

Domain List:

Cancel

Save

Aggiungi tunneling ripartito

Passaggio 8. Passare a Secure Client > Profile, selezionare Client Profile e fare clic su Save.

Edit Group Policy



Name:*

DfltGrpPolicy

Description:

General

Secure Client

Advanced

Profile

Management Profile

Client Modules

SSL Settings

Connection Settings

Custom Attributes

Secure Client profiles contains settings for the VPN client functionality and optional features. The Firewall Threat Defense deploys the profiles during Secure Client connection.

Client Profile:

Anyconnect_Profile-5-0-05040 ▾ +

Standalone profile editor can be used to create a new or modify existing Secure Client profile. You can download the profile editor from [Cisco Software Download Center](#).

Aggiungi profilo client sicuro

Passaggio 9. Fare clic su Next, quindi selezionare il Secure Client Image e fare clic su Next.

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 type="checkbox"/>	Secure Client File Object Name	Secure Client Package Name	Operating System
<input checked="" type="checkbox"/>	AnyconnectWin-5.0.05040	cisco-secure-client-win-5.0.05040-webde...	Windows ▾


Aggiungi immagine client sicura

Passaggio 10. Selezionare l'interfaccia di rete per l'accesso VPN, scegliere Device Certificates, selezionare syspot allow-vpn e fare clic su Next.

Network Interface for Incoming VPN Access

Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone:* +
 Enable DTLS on member interfaces

 All the devices must have interfaces as part of the Interface Group/Security Zone selected.

Device Certificates

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:* +
 Enroll the selected certificate object on the target devices

Access Control for VPN Traffic

All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

- Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)
This option bypasses the Access Control Policy inspection, but VPN filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

Aggiungi controllo di accesso per traffico VPN

Passaggio 11. Infine, esaminare tutte le configurazioni e fare clic su Finish.

Remote Access VPN Policy Configuration

Firewall Management Center will configure an RA VPN Policy with the following settings

Name:	RAVPN
Device Targets:	FTD-B-7.4.0
Connection Profile:	RAVPN-CertAuth
Connection Alias:	RAVPN-CertAuth
AAA:	
Authentication Method:	Client Certificate Only
Username From Certificate:	-
Authorization Server:	-
Accounting Server:	-
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	vpn_pool
Address Pools (IPv6):	-
Group Policy:	DfltGrpPolicy
Secure Client Images:	AnyconnectWin-5.0.05040
Interface Objects:	outside-zone
Device Certificates:	ssl_certificate

Device Identity Certificate Enrollment

Certificate enrollment object 'ssl_certificate' is not installed on one or more targeted devices. Certificate installation will be initiated on the targeted devices on finishing the wizard. Go to the [Certificates](#) page to check the status of the installation.

Configurazione criteri VPN di Accesso remoto

Passaggio 12. Al termine della configurazione iniziale della VPN ad accesso remoto, modificare il profilo di connessione creato e passare a Aliases.

Passaggio 13. Configurare group-alias facendo clic sull'icona più (+).

Edit Connection Profile

Connection Profile:* RAVPN-CertAuth


Group Policy:* DfltGrpPolicy +

[Edit Group Policy](#)

Client Address Assignment AAA **Aliases**

Alias Names:

Incoming users can choose an alias name upon first login. Aliases from all connections configured on this device can be turned on or off for display.

Name	Status	
ssl-cert	Enabled	

URL Alias:

Configure the list of UR following URLs, system

URL

Edit Alias Name

Alias Name:

 Enabled

Cancel OK

Cancel Save

Modifica alias gruppo

Passaggio 14. Configurare group-url facendo clic sull'icona più (+). Utilizzare lo stesso URL di gruppo configurato in precedenza nel profilo client.

Edit Connection Profile

Connection Profile:* RAVPN-CertAuth

Group Policy:* DfltGrpPolicy

Client Address Assignment AAA **Aliases**

Incoming users can choose an alias name upon first login. Aliases from all connections configured on this device can be turned on or off.

Edit URL Alias

URL Alias:

certauth

Enabled

Cancel OK

URL Alias:

Configure the list of URLs that will be used to log in via this connection profile. If users choose the following URLs, system will automatically log them in via this connection profile.

URL	Status
certauth (https://certauth.cisco.com/ssl-cert)	Enabled

Cancel Save

Modifica URL gruppo

Passaggio 15. Passare a Interfacce di accesso. Selezionare Interface Trustpoint e SSL Global Identity Certificate sotto le impostazioni SSL.

RAVPN

Enter Description

Connection Profile **Access Interfaces** Advanced

Local Realm: cisco-local Policy Assignments (1) Dynamic Access Policy: None

Interfaces of the targeted device which belong to below specified interface groups will support incoming Remote Access VPN connections

Name	Interface Trustpoint	DTLS	SSL	IPsec-IKEv2
outside-zone	ssl_certificate	●	●	●

Access Settings

Allow Users to select connection profile while logging in

SSL Settings

Web Access Port Number:* 443

DTLS Port Number:* 443

SSL Global Identity Certificate: ssl_certificate

Note: Ensure the port used in VPN configuration is not used in other services

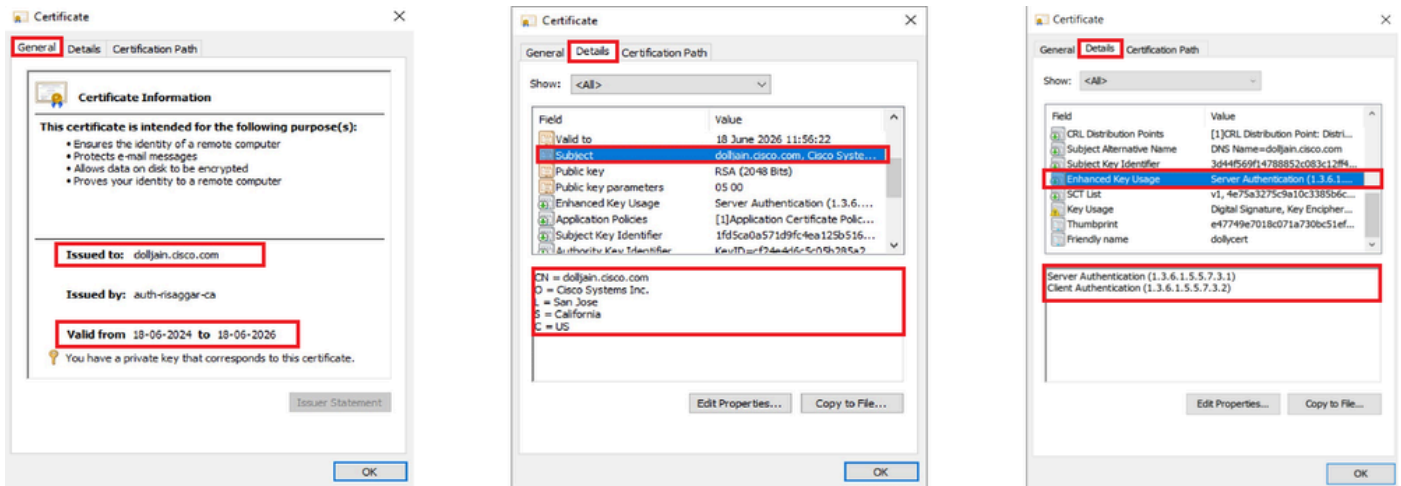
Modifica interfacce di accesso

Passaggio 16. FareSave clic su e distribuire le modifiche.

Verifica

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

1. Sul PC client sicuro deve essere installato il certificato con una data, un oggetto e un utilizzo chiavi avanzato validi sul PC dell'utente. Questo certificato deve essere rilasciato dalla CA il cui certificato è installato sull'FTD, come mostrato in precedenza. In questo caso, l'identità o il certificato utente viene rilasciato da "auth-risaggar-ca".

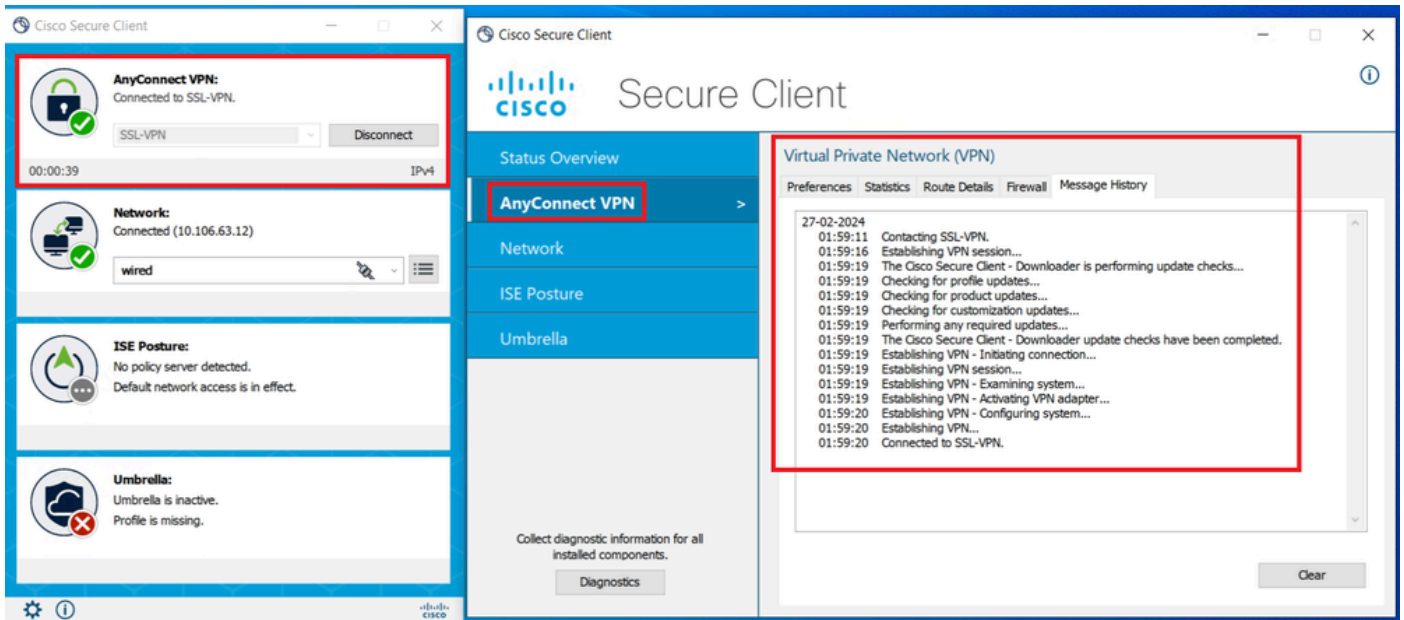


Caratteristiche principali del certificato



Nota: il certificato client deve disporre dell'utilizzo chiavi avanzato per l'autenticazione client.

2. Secure Client deve stabilire la connessione.



Connessione client sicura riuscita

3. Eseguire `show vpn-sessiondb anyconnect` per confermare i dettagli di connessione dell'utente attivo nel gruppo di tunnel utilizzato.

```
firepower# show vpn-sessiondb anyconnect Session Type: AnyConnect Username : dolljain.cisco.com Index :
```

Risoluzione dei problemi

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

1. I debug possono essere eseguiti dalla CLI diagnostica dell'FTD:

```
debug crypto ca 14
```

```
debug webvpn anyconnect 255
```

```
debug crypto ike-common 255
```

2. Fare riferimento a questa [guida](#) per i problemi comuni.

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).