

# Configurazione di SSL AnyConnect Management VPN su FTD

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Limitazioni](#)

[Configurazione](#)

[Configurazioni](#)

[Passaggio 1. Creazione del profilo VPN di gestione di AnyConnect](#)

[Passaggio 2. Creazione del profilo VPN AnyConnect](#)

[Passaggio 3. Caricare il profilo VPN di gestione di AnyConnect e il profilo VPN di AnyConnect in FMC](#)

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

[Passaggio 5. Creazione di una nuova configurazione di AnyConnect](#)

[Passaggio 6. Creazione dell'oggetto URL](#)

[Passaggio 7. Definizione dell'alias dell'URL](#)

[Verifica](#)

[Risoluzione dei problemi](#)

## Introduzione

In questo documento viene descritto come configurare un tunnel di gestione di Cisco AnyConnect su un Cisco Firepower Threat Defense (FTD) gestito da Cisco Firepower Management Center (FMC). Nell'esempio seguente viene utilizzato SSL (Secure Sockets Layer) per creare una rete VPN (Virtual Private Network) tra FTD e un client Windows 10.

Contributo di Daniel Perez Vertti Vazquez, Cisco TAC Engineer.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco AnyConnect Profile Editor
- Configurazione di AnyConnect SSL tramite FMC.
- Autenticazione certificato client

### Componenti usati

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

- Cisco FTD versione 6.7.0 (Build 65)
- Cisco FMC versione 6.7.0 (build 65)
- Cisco AnyConnect 4.9.01095 installato sul computer Windows 10

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

Dalla versione 6.7, Cisco FTD supporta la configurazione dei tunnel di gestione di AnyConnect. Questa procedura consente di correggere la richiesta di miglioramento precedentemente aperta [CSCvs78215](#).

La funzionalità di gestione di AnyConnect consente di creare un tunnel VPN subito dopo il completamento dell'avvio dell'endpoint. Non è necessario che gli utenti avviino manualmente l'app AnyConnect, non appena il sistema viene acceso, il servizio agente VPN di AnyConnect rileva la funzionalità VPN di gestione e avvia una sessione AnyConnect utilizzando la voce host definita nell'elenco dei server del profilo VPN di gestione di AnyConnect.

## Limitazioni

- È supportata solo l'autenticazione del certificato client.
- Per i client Windows è supportato solo l'archivio certificati del computer.
- Non supportato in Cisco Firepower Device Manager (FDM) [CSCvx90058](#).
- Non supportato sui client Linux.

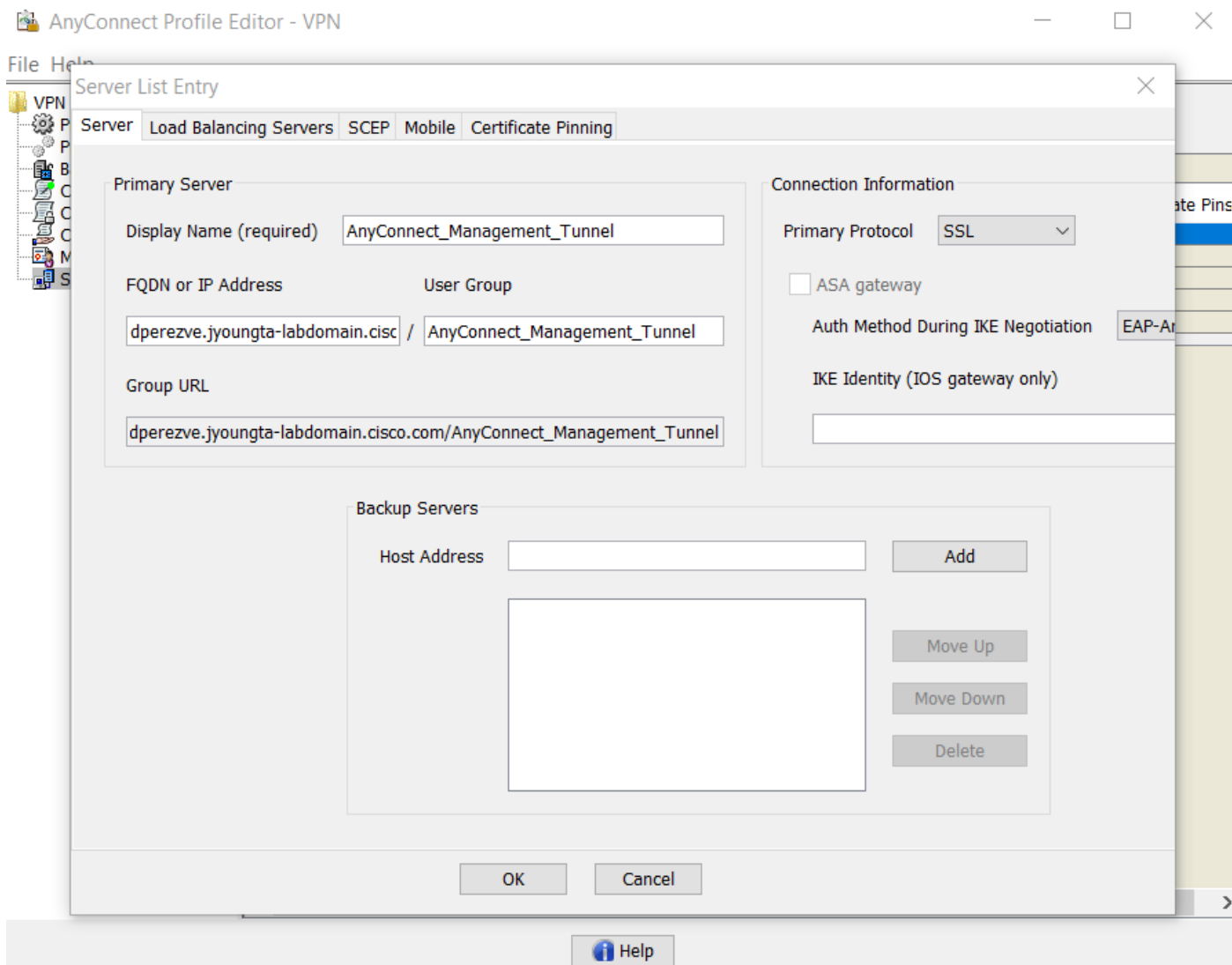
## Configurazione

### Configurazioni

#### Passaggio 1. Creazione del profilo VPN di gestione di AnyConnect

Aprire l'Editor profili AnyConnect per creare il profilo VPN di gestione di AnyConnect. Il profilo di gestione contiene tutte le impostazioni utilizzate per stabilire il tunnel VPN dopo l'avvio dell'endpoint.

In questo esempio viene definita una voce dell'elenco dei server che punta a FQDN (Fully Qualified Domain Name) `dperezve.jyoungta-labdomain.cisco.com` e viene selezionato SSL come protocollo primario. Per aggiungere un elenco di server, passare a **Elenco server** e selezionare il pulsante **Aggiungi**, compilare i campi obbligatori e salvare le modifiche.



Oltre all'elenco dei server, il profilo VPN di gestione deve contenere alcune preferenze obbligatorie:

- **AutomaticCertSelection** deve essere impostato su **true**.
- **La riconnessione automatica** deve essere impostata su **true**.
- È necessario configurare **AutoReconnectBehavior** per **ReconnectAfterResume**.
- **AutoUpdate** deve essere impostato su **false**.
- **BlockUntrustedServers** deve essere impostato su **true**.
- **CertificateStore** deve essere configurato per **MachineStore**.
- **CertificateStoreOverride** deve essere impostato su **true**.
- **EnableAutomaticServerSelection** deve essere impostato su **false**.
- **EnableScripting** deve essere impostato su **false**.
- **RetainVPNOnLogoff** deve essere impostato su **true**.

In AnyConnect Profile Editor passare a **Preferenze (Parte 1)** e regolare le impostazioni come segue:

File Help

**Preferences (Part 1)**  
Profile: ...nnect -FTD-Lab1.XML Profile\AnyConnect\_Management\_Tunnel.xml

Use Start Before Logon  User Controllable

Show Pre-Connect Message

Certificate Store

Windows **Machine** ▾

macOS **All** ▾

Certificate Store Override

Auto Connect On Start  User Controllable

Minimize On Connect  User Controllable

Local Lan Access  User Controllable

Disable Captive Portal Detection  User Controllable

Auto Reconnect  User Controllable

Auto Reconnect Behavior

**ReconnectAfterResume** ▾

Auto Update  User Controllable

RSA Secure ID Integration  User Controllable

**Automatic** ▾

Windows Logon Enforcement

**SingleLocalLogon** ▾

Windows VPN Establishment

**AllowRemoteUsers** ▾

Help

Passare quindi a **Preferenze (Parte 2)** e deselezionare l'opzione **Disabilita selezione automatica certificati**.

File Help

**Preferences (Part 2)**  
Profile: ...nnect -FTD-Lab1.XML ProfileAnyConnect\_Management\_Tunnel.xml

Disable Automatic Certificate Selection  User Controllable

Proxy Settings: Native  User Controllable

Public Proxv Server Address:

Note: Enter public Proxv 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: Disconnect

Untrusted Network Policy: Connect

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://

## Passaggio 2. Creazione del profilo VPN AnyConnect

Oltre al profilo VPN di gestione, è necessario configurare il profilo VPN AnyConnect standard. Il profilo VPN AnyConnect viene usato al primo tentativo di connessione. Durante questa sessione, il profilo VPN di gestione viene scaricato da FTD.

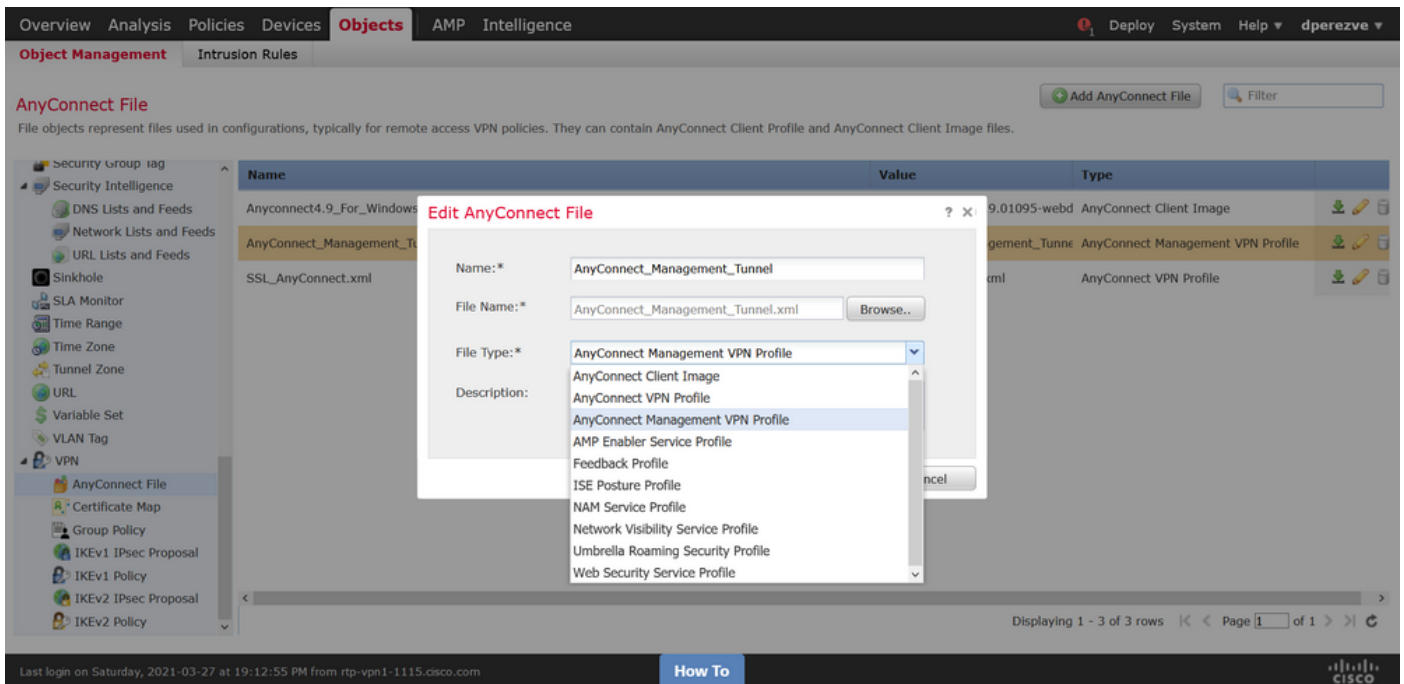
Usare l'Editor dei profili di AnyConnect per creare il profilo VPN di AnyConnect. In questo caso, entrambi i file contengono le stesse impostazioni, quindi è possibile seguire la stessa procedura.

## Passaggio 3. Caricare il profilo VPN di gestione di AnyConnect e il profilo VPN di AnyConnect in FMC

Dopo aver creato i profili, caricarli nel FMC come oggetti AnyConnect File.

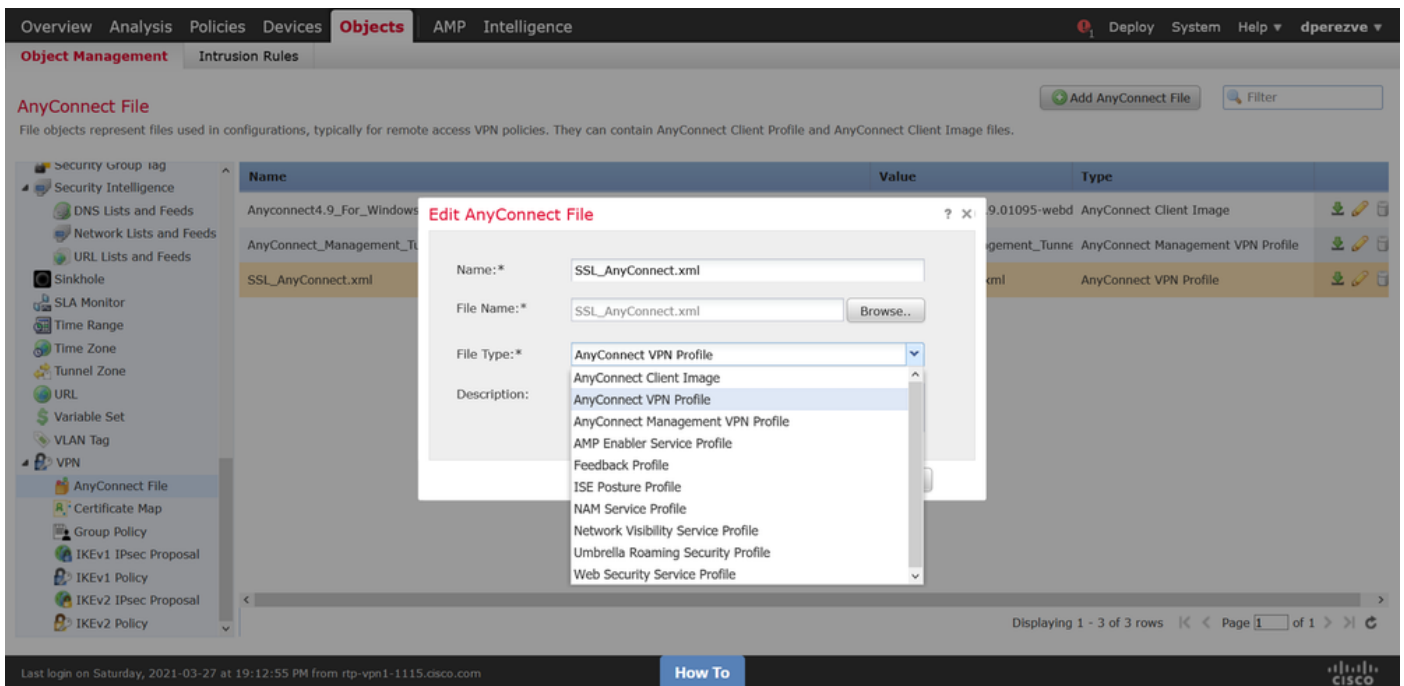
Per caricare il nuovo profilo VPN di AnyConnect Management in FMC, selezionare **Oggetti > Gestione oggetti** e scegliere l'opzione **VPN** dal sommario, quindi selezionare il pulsante **Aggiungi file AnyConnect**.

Fornire un nome per il file, scegliere **AnyConnect Management VPN Profile** come tipo di file e salvare l'oggetto.



A questo punto, per caricare il profilo VPN AnyConnect, passare nuovamente a **Oggetti > Gestione oggetti** e selezionare l'opzione **VPN** dal sommario, quindi selezionare il pulsante **Add AnyConnect File**.

Fornire un nome per il file, ma questa volta scegliere **AnyConnect VPN Profile** come tipo di file e salvare il nuovo oggetto.



I profili devono essere aggiunti all'elenco degli oggetti e contrassegnati rispettivamente come **profilo VPN di gestione di AnyConnect** e **profilo VPN di AnyConnect**.

The screenshot shows the Cisco AnyConnect configuration interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'Objects' tab is active, and the 'Object Management' section is selected. A sidebar on the left lists various object types, with 'VPN' expanded to show 'AnyConnect File'. The main area displays a table of AnyConnect files:

Name	Value	Type
Anyconnect4.9_For_Windows	anyconnect-win-4.9.01095-webd	AnyConnect Client Image
AnyConnect_Management_Tunnel	AnyConnect_Management_Tunne	AnyConnect Management VPN Profile
SSL_AnyConnect.xml	SSL_AnyConnect.xml	AnyConnect VPN Profile

At the bottom of the interface, there is a 'How To' button and a Cisco logo.

## Passaggio 4. Creazione di Criteri di gruppo

Per creare un nuovo criterio di gruppo, passare a **Oggetti > Gestione oggetti** e scegliere l'opzione **VPN** dal sommario, quindi selezionare **Criteri di gruppo** e fare clic sul pulsante **Aggiungi criterio di gruppo**.

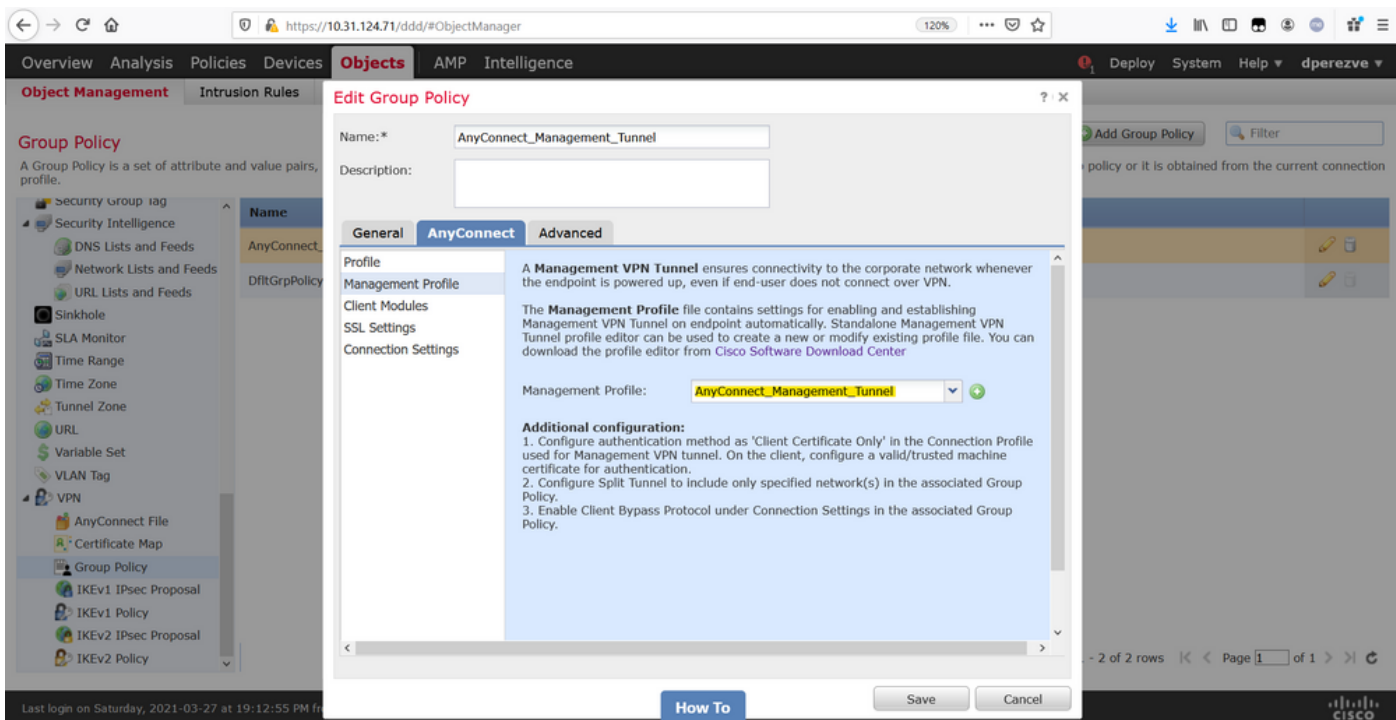
Quando si apre la finestra **Add Group Policy**, assegnare un nome, definire un pool AnyConnect e aprire la scheda **AnyConnect**. Passare a **Profilo** e selezionare l'oggetto che rappresenta il profilo VPN AnyConnect standard nel menu a discesa **Profilo client**.

The screenshot shows the Cisco AnyConnect configuration interface with the 'Edit Group Policy' dialog box open. The dialog box has the following fields and tabs:

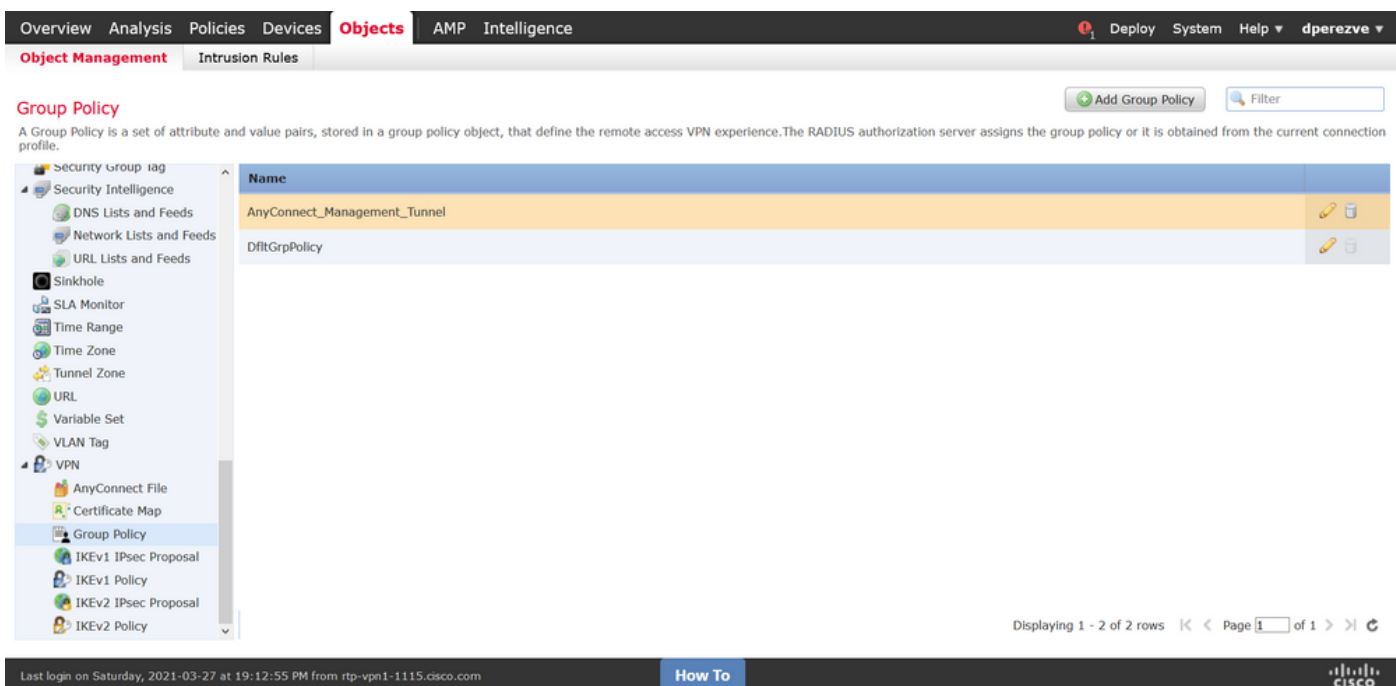
- Name:** AnyConnect\_Management\_Tunnel
- Description:** (empty)
- Tabs:** General, AnyConnect (selected), Advanced
- Profile:** Management Profile, Client Modules, SSL Settings, Connection Settings
- Client Profile:** SSL\_AnyConnect.xml (selected)

The 'AnyConnect' tab is active, and the 'Client Profile' dropdown menu is open, showing 'SSL\_AnyConnect.xml' as the selected option. The dialog box also includes a 'Save' button and a 'Cancel' button.

Passare quindi alla scheda **Profilo di gestione** e selezionare l'oggetto che contiene il Profilo VPN di gestione nel menu a discesa **Profilo di gestione**.



Salvare le modifiche per aggiungere il nuovo oggetto ai Criteri di gruppo esistenti.



## Passaggio 5. Creazione di una nuova configurazione di AnyConnect

La configurazione di SSL AnyConnect in FMC è composta da 4 passaggi diversi. Per configurare AnyConnect, selezionare **Devices > VPN > Remote Access** (Dispositivi > Accesso remoto) e selezionare il pulsante **Add** (Aggiungi). È necessario aprire la **Creazione guidata criteri VPN di Accesso remoto**.

Nella scheda **Assegnazione criteri** selezionare il dispositivo FTD desiderato, definire un nome per il profilo di connessione e selezionare la casella di controllo SSL.



Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help dperezve

Dashboards Reporting Summary

### Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 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:\* AnyConnect\_Management\_Tunnel

Description:

VPN Protocols:  SSL  IPsec-IKEv2

Targeted Devices:

Available Devices: Search ftdv-dperezve ftdv-fejimene

Selected Devices: ftdv-dperezve

Buttons: Back Next Cancel

Last login on Thursday, 2021-03-25 at 17:01:05 PM from rtp-vpn6-107.cisco.com [How To](#)

In **Profilo connessione** selezionare **Solo certificato client** come metodo di autenticazione. Questa è l'unica autenticazione supportata per la funzionalità.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help dperezve

Device Management NAT **VPN Remote Access** QoS Platform Settings FlexConfig Certificates

### Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 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:\* AnyConnect\_Management\_Profile  
*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: AAA Only (Distinguished Name) as username

Primary Field: SAML

Secondary Field: Client Certificate Only

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

Buttons: Back Next Cancel

Last login on Saturday, 2021-03-27 at 19:12:55 PM from rtp-vpn1-1115.cisco.com [How To](#)

Selezionare quindi l'oggetto Criteri di gruppo creato al passaggio 3 nell'elenco a discesa **Criteri di gruppo**.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help dperezve

Device Management NAT **VPN Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 **AnyConnect** 4 Access & Certificate 5 Summary

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) i

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:\*

AnyConnect\_Management\_Tunnel  
 AnyConnect\_Management\_Tunnel  
 DfltGrpPolicy

Back Next Cancel

Last login on Saturday, 2021-03-27 at 19:12:55 PM from rtp-vpn1-1115.cisco.com How To

Nella scheda **AnyConnect**, selezionare l'oggetto file AnyConnect in base al sistema operativo (OS) sull'endpoint.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help dperezve

Device Management NAT **VPN Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 **Access & Certificate** 5 Summary

AAA

**AnyConnect Client Image**  
 The VPN gateway can automatically download the latest AnyConnect 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 AnyConnect Client packages from [Cisco Software Download Center](#).

Show Re-order buttons

<input checked="" type="checkbox"/>	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
<input checked="" type="checkbox"/>	Anyconnect4.9_For_Windows	anyconnect-win-4.9.01095-webdeploy-k9.pkg	Windows <input type="text"/>

Back Next Cancel

Last login on Saturday, 2021-03-27 at 19:12:55 PM from rtp-vpn1-1115.cisco.com How To

In **Accesso e certificato** specificare il certificato che deve essere utilizzato dall'FTD per verificare la propria identità al client Windows.

**Nota:** Poiché gli utenti non devono interagire con l'app AnyConnect quando usano la funzionalità VPN di gestione, il certificato deve essere completamente attendibile e non deve stampare alcun messaggio di avviso.

**Nota:** Per evitare errori di convalida del certificato, il campo Nome comune (CN) incluso nel Nome soggetto del certificato deve corrispondere al nome di dominio completo (FQDN) definito nell'Elenco server di profili XML (Passaggio 1 e Passaggio 2).

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help dperezve

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary

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

**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.*

Back Next Cancel

Last login on Saturday, 2021-03-27 at 19:12:55 PM from rtp-vpn1-1115.cisco.com **How To** CISCO

Infine, selezionare il pulsante **Finish** (Fine) nella scheda **Summary** per aggiungere la nuova configurazione AnyConnect.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help dperezve

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary

Connection Profile: AnyConnect\_Management\_Profile  
 Connection Alias: AnyConnect\_Management\_Profile  
 AAA:  
 Authentication Method: Client Certificate Only  
 Username From Certificate: CN (Common Name) & OU (Organisational Unit)  
 Authorization Server: -  
 Accounting Server: -  
 Address Assignment:  
 Address from AAA: -  
 DHCP Servers: -  
 Address Pools (IPv4): AnyConnect-Pool  
 Address Pools (IPv6): -  
 Group Policy: AnyConnect\_Management\_Tunnel  
 AnyConnect Images: Anyconnect4.9\_For\_Windows  
 Interface Objects: outside  
 Device Certificates: SSL\_AnyConnect

**Warnings:**  
 An [Access Control](#) rule must be defined to allow VPN traffic on all targeted devices.  
 1 **NAT Exemption**  
 If NAT is enabled on the targeted devices, you must define a [NAT Policy](#) to exempt VPN traffic.  
 1 **DNS Configuration**  
 To resolve hostname specified in AAA Servers or CA Servers, configure DNS using [FlexConfig Policy](#) on the targeted devices.  
 1 **Port Configuration**  
 SSL will be enabled on port 443. Please ensure that these ports are not used in [NAT Policy](#) or other services before deploying the configuration.  
 ⚠ **Network Interface Configuration**  
 Make sure to add interface from targeted devices to SecurityZone object 'outside'

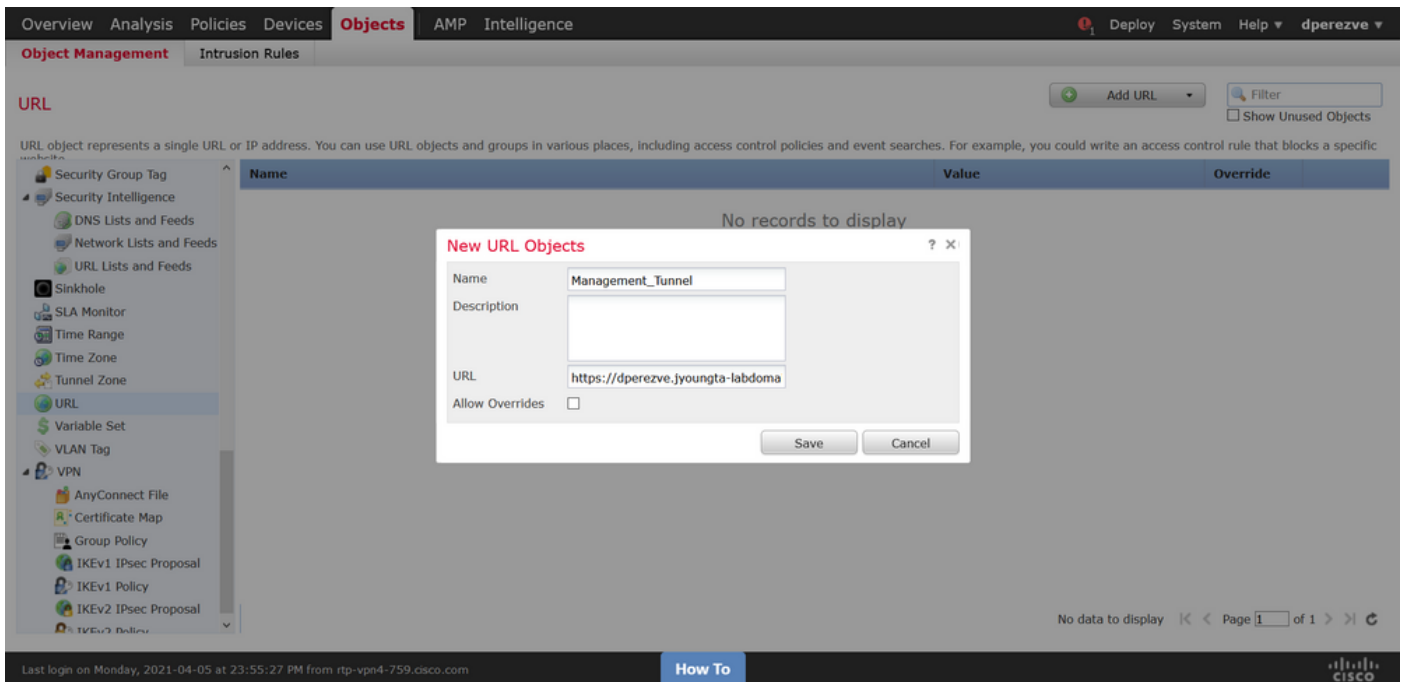
Back Finish Cancel

Last login on Saturday, 2021-03-27 at 19:12:55 PM from rtp-vpn1-1115.cisco.com **How To** CISCO

## Passaggio 6. Creazione dell'oggetto URL

Passare a **Oggetti > Gestione oggetti** e selezionare **URL** dal sommario. Quindi selezionare **Add Object** (Aggiungi oggetto) nell'elenco a discesa **Add URL** (Aggiungi URL).

Fornire un nome per l'oggetto e definire l'URL utilizzando lo stesso FQDN/gruppo di utenti specificato nell'elenco dei server dei profili VPN di gestione (passaggio 2). Nell'esempio, l'URL deve essere `dperezve.jyoungta-labdomain.cisco.com/AnyConnect_Management_Tunnel`.

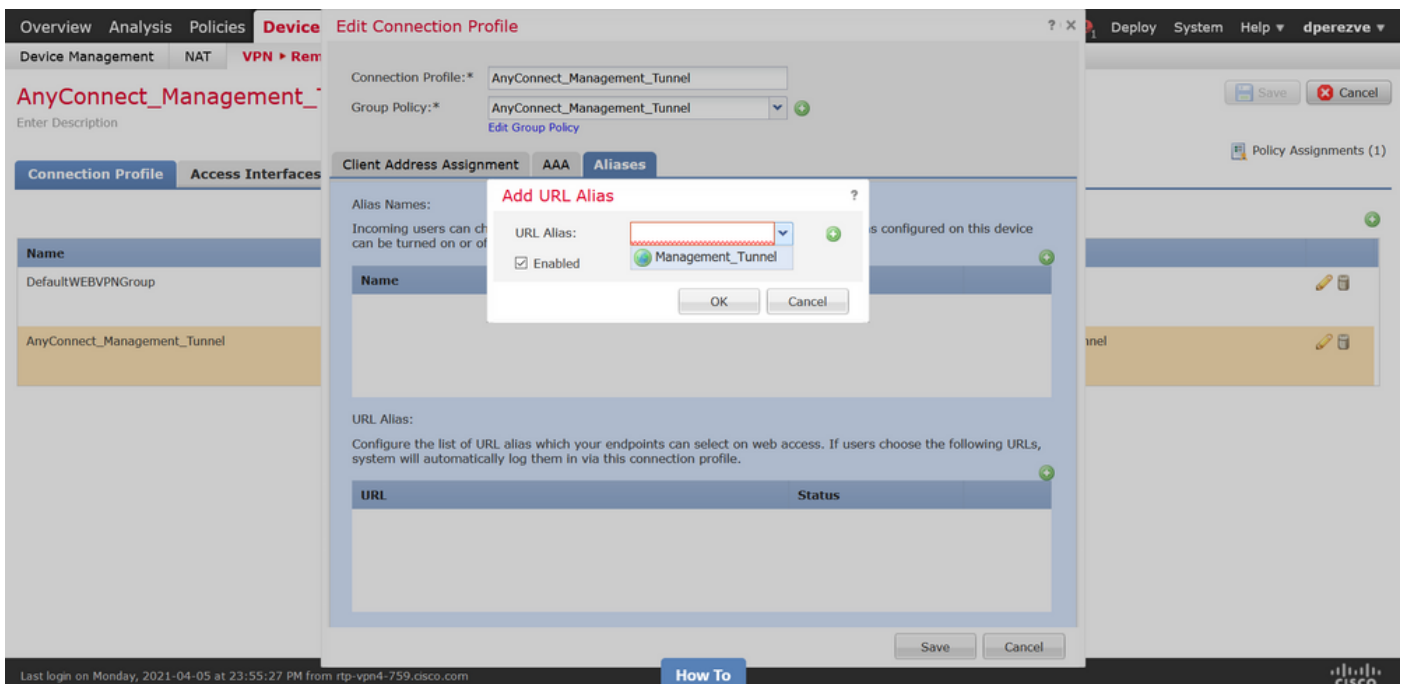


Salvare le modifiche per aggiungere l'oggetto all'elenco degli oggetti.

### Passaggio 7. Definizione dell'alias dell'URL

Per abilitare l'alias URL nella configurazione AnyConnect, selezionare **Dispositivi > VPN > Accesso remoto** e fare clic sull'icona a forma di matita per apportare le modifiche.

Nella scheda Profilo connessione selezionare la configurazione desiderata, passare ad **Alias**, fare clic sul pulsante **Aggiungi** e selezionare l'oggetto URL nell'**elenco a discesa Alias URL**. Verificare che la casella di controllo **Abilitato** sia selezionata.



Salvare le modifiche e distribuire le configurazioni in FTD.

## Verifica

Al termine dell'implementazione, è necessaria una prima connessione AnyConnect manuale con il profilo VPN di AnyConnect. Durante questa connessione, il profilo VPN di gestione viene scaricato da FTD e archiviato in **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun**. Da questo punto, le connessioni successive devono essere avviate tramite il profilo VPN di gestione senza alcuna interazione da parte dell'utente.

## Risoluzione dei problemi

Per gli errori di convalida del certificato:

- Verificare che il certificato radice per CA (Certification Authority) sia installato nell'FTD.
- Verificare che in Windows Machine Store sia installato un certificato di identità firmato dalla stessa CA.
- Verificare che il campo CN sia incluso nel certificato e che corrisponda all'FQDN definito nell'elenco dei server del profilo VPN di gestione e all'FQDN definito nell'alias URL.

Per il tunnel di gestione non avviato:

- Verificare che il profilo VPN di gestione sia stato scaricato e archiviato in **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun**.
- Verificare che il nome del profilo VPN di gestione sia **VpnMgmtTunProfile.xml**.

Per problemi di connettività, raccogliere il bundle DART e contattare Cisco TAC per ulteriori ricerche.