Configurazione di SSL AnyConnect Management VPN su FTD

Sommario

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

- Èsupportata 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.

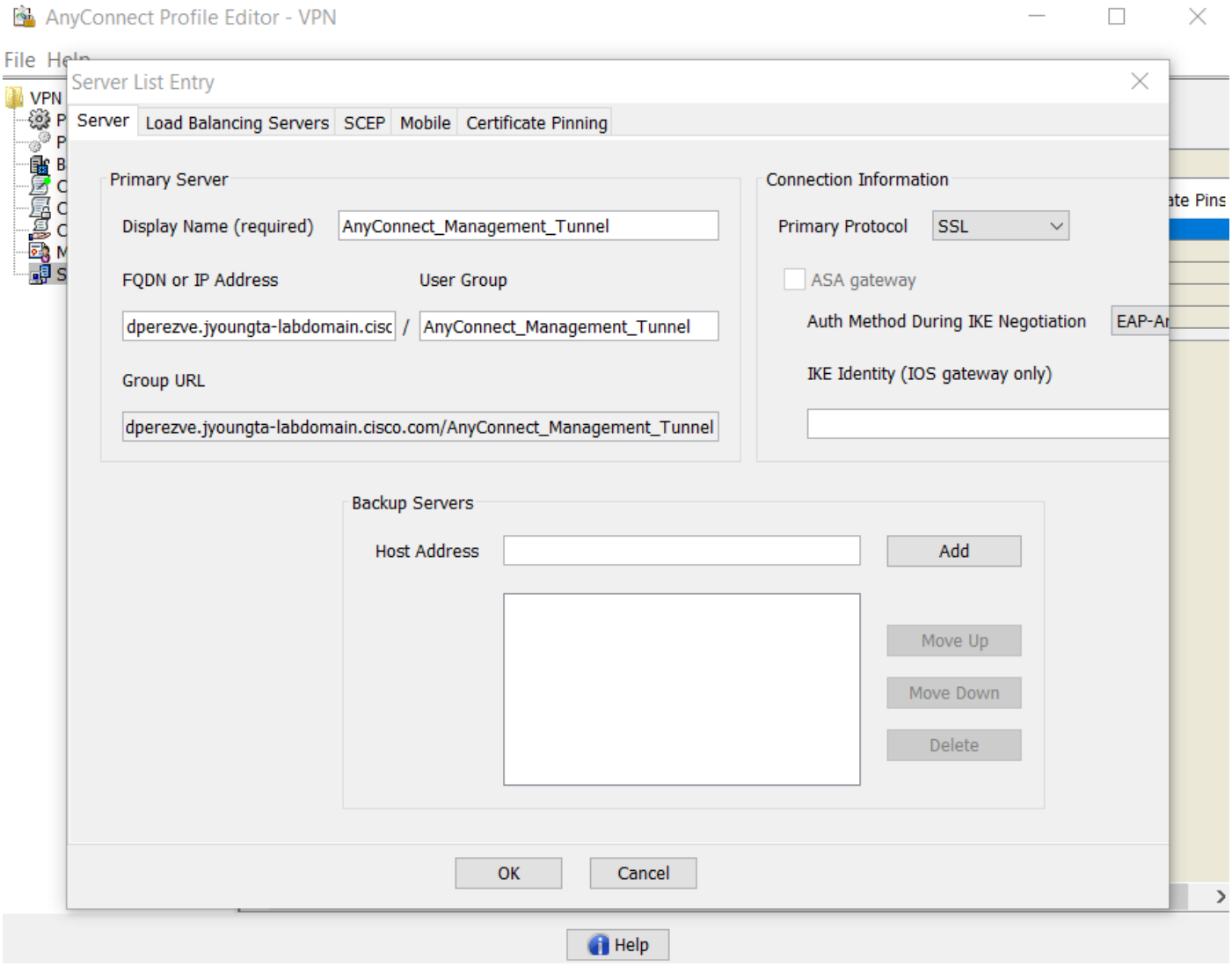
Configurazione

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.

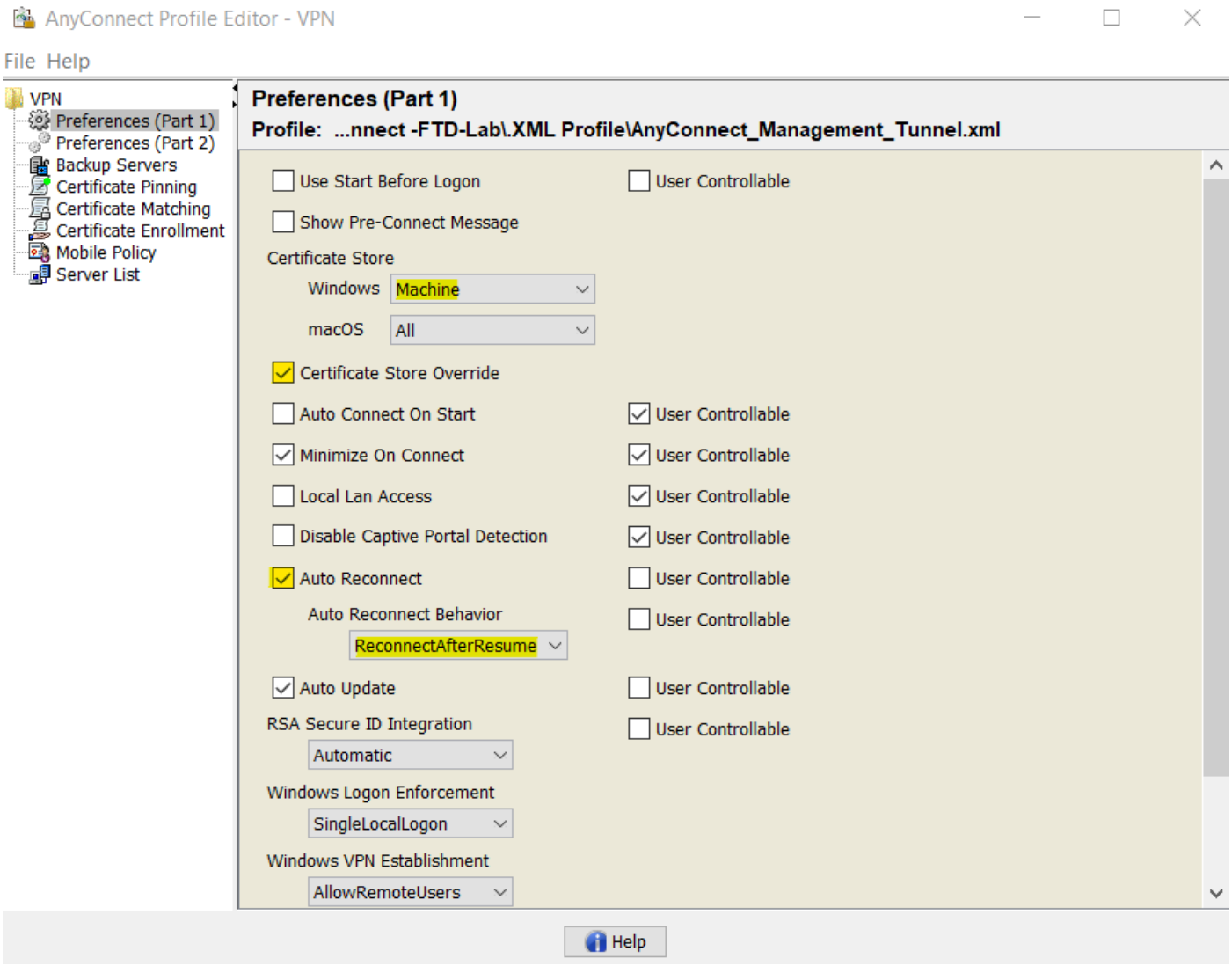
In questo esempio viene definita una voce dell'elenco dei server che punta a FQDN (Fully Qualified Domain Name) dperezve.jyoungta-labdomain.cisco.com e viene selezionato SSL come protocollo primario. Per aggiungere un elenco di server, passare a **Elenco server** e selezionare il pulsante **Aggiungi**,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



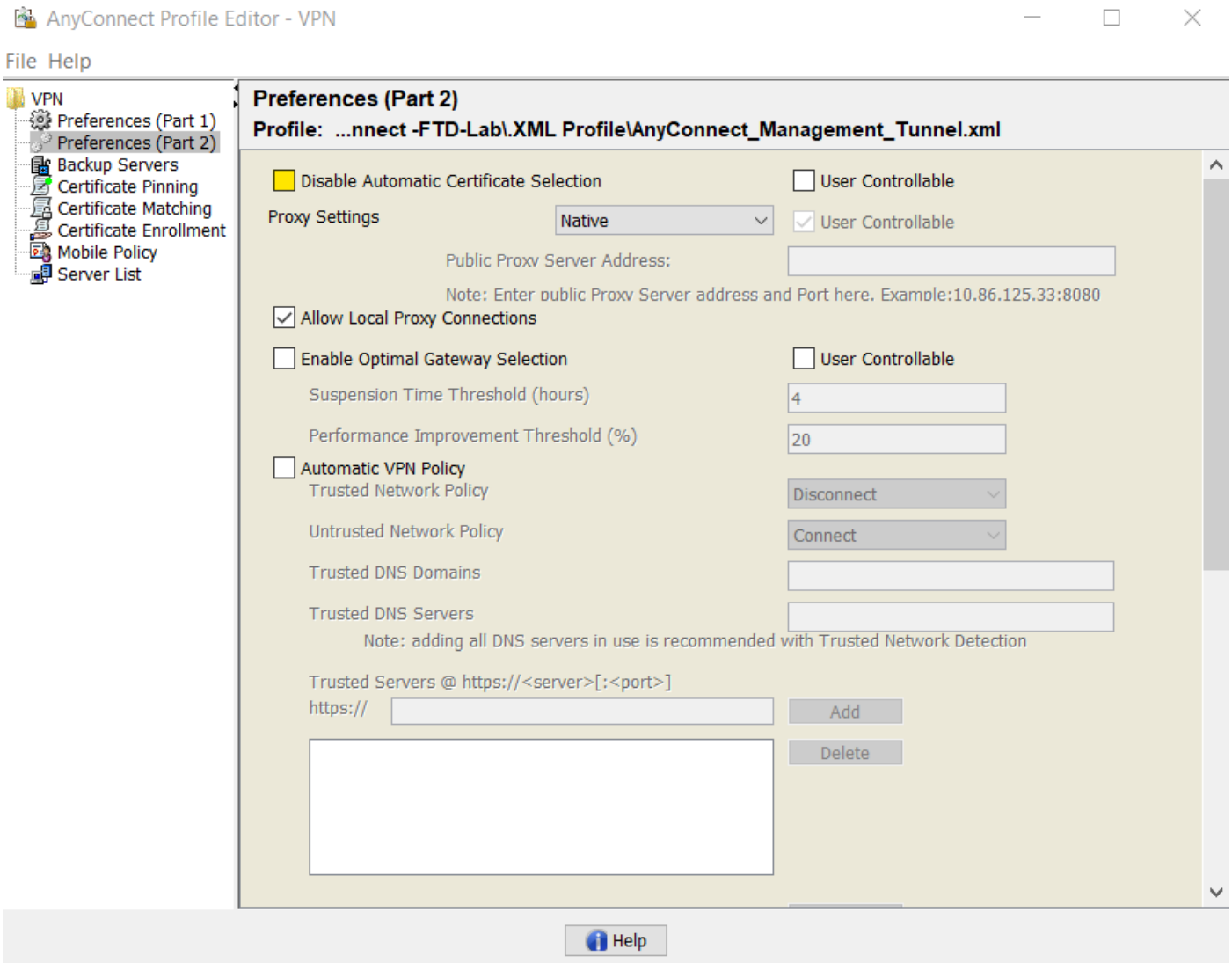
Oltre all'elenco dei server, il profilo VPN di gestione deve contenere alcune preferenze obbligatorie:

- **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:



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



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.

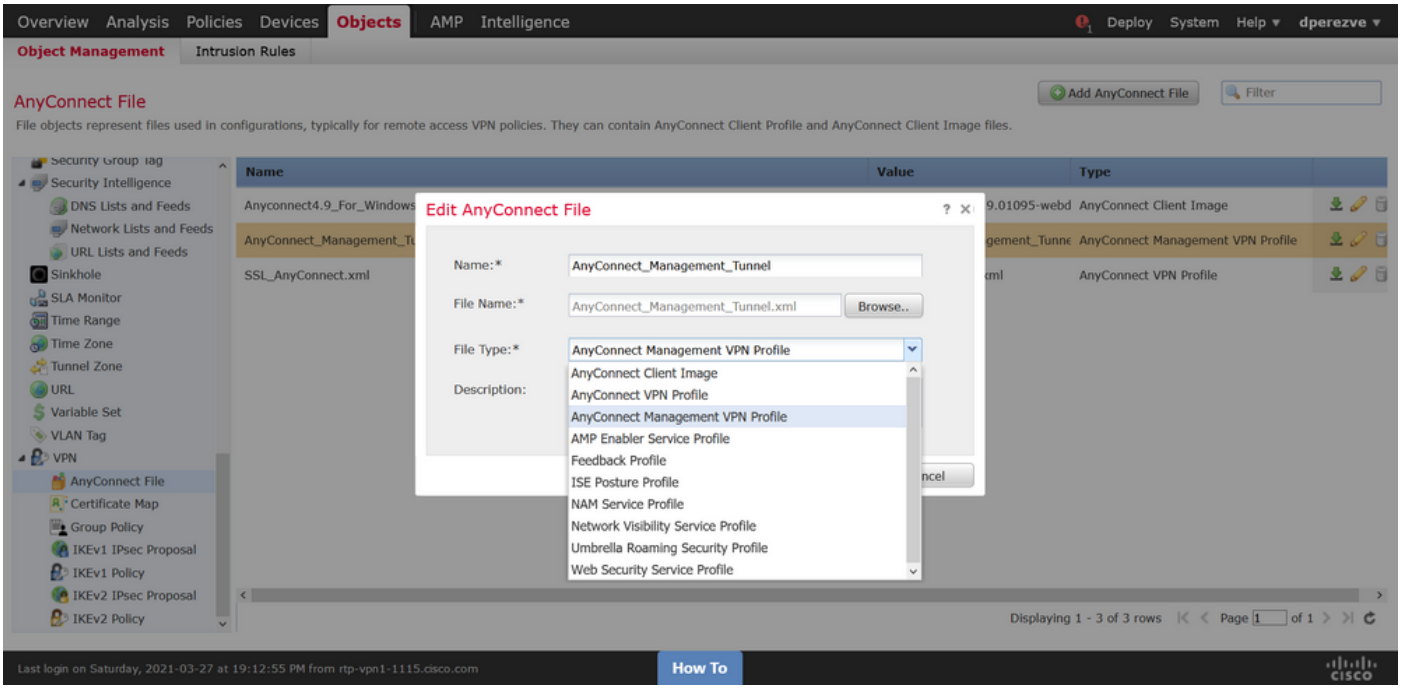
Usare l'Editor dei profili di AnyConnect per creare il profilo VPN di AnyConnect. In questo caso, entrambi i file contengono le stesse impostazioni, quindi è possibile seguire la stessa procedura.

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.

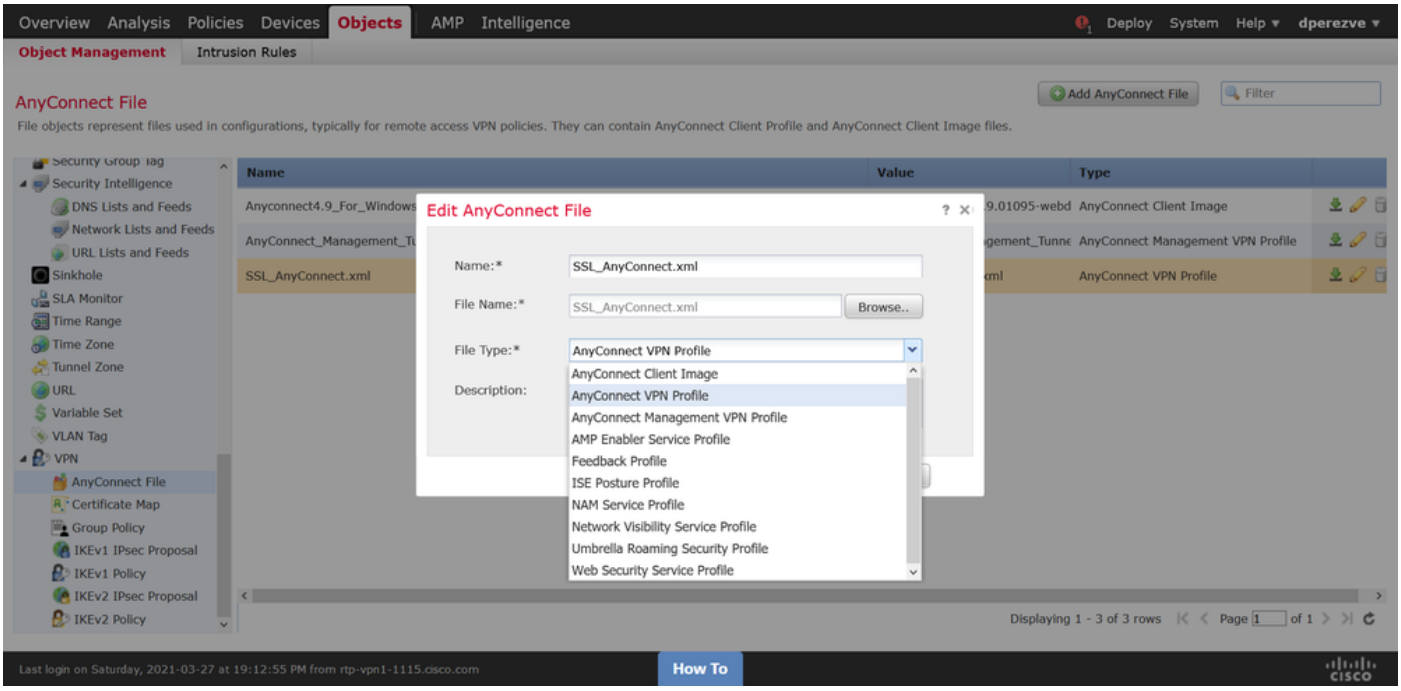
Per caricare il nuovo profilo VPN di AnyConnect Management in FMC, selezionare **Oggetti > Gestione oggetti** e scegliere l'opzione **VPN** dal sommario, quindi selezionare il pulsante **Aggiungi file AnyConnect**.

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

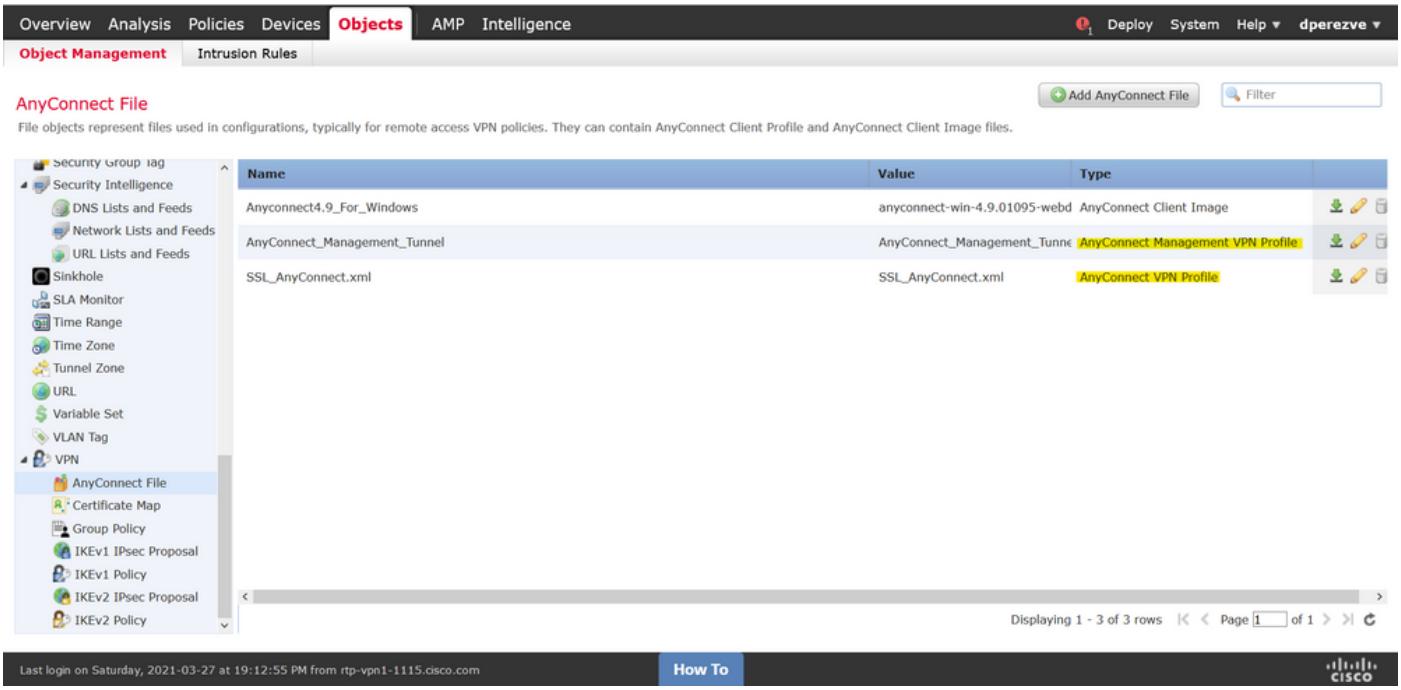


A questo punto, per caricare il profilo VPN AnyConnect, passare nuovamente a **Oggetti > Gestione oggetti** e selezionare l'opzione **VPN** dal sommario, quindi selezionare il pulsante **Add AnyConnect File**.

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



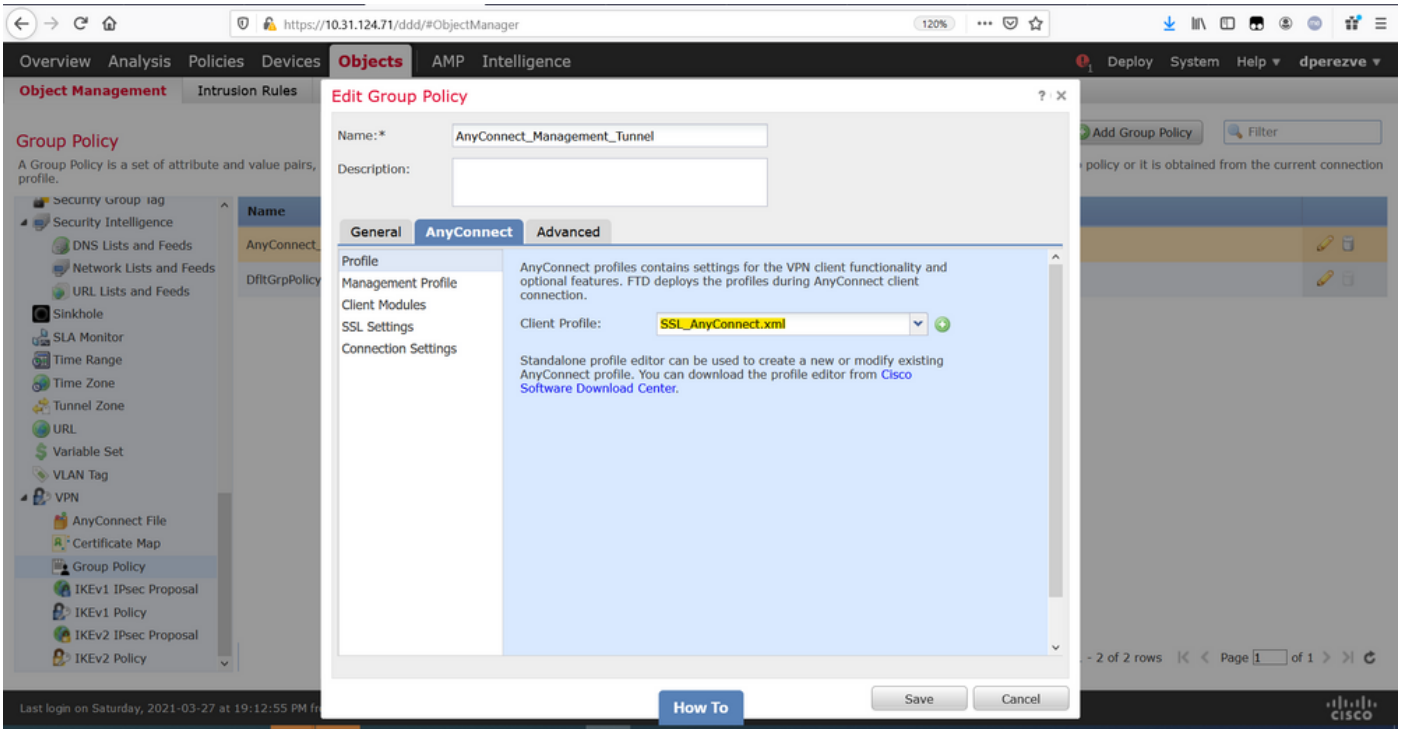
I profili devono essere aggiunti all'elenco degli oggetti e contrassegnati rispettivamente come **profilo VPN di gestione di AnyConnect** e **profilo VPN di AnyConnect**.



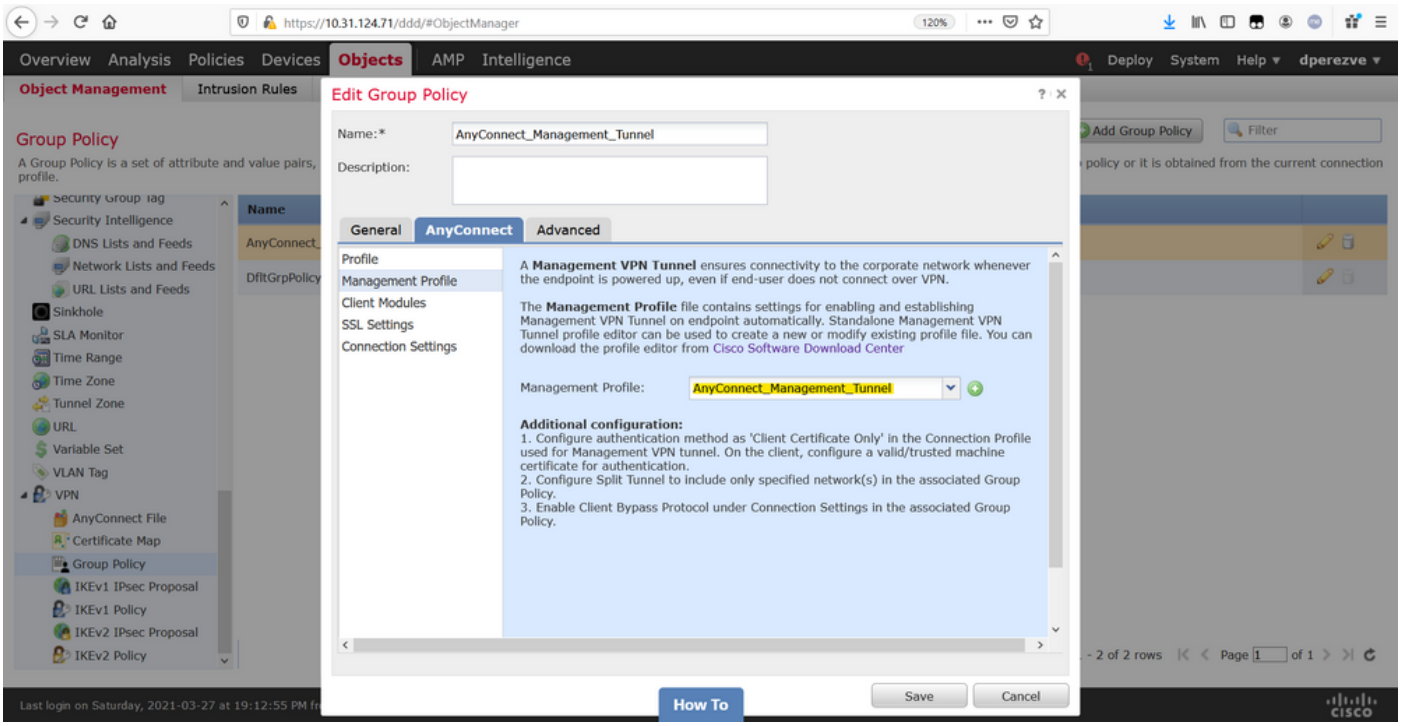
Passaggio 4. Creazione di Criteri di gruppo

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**.

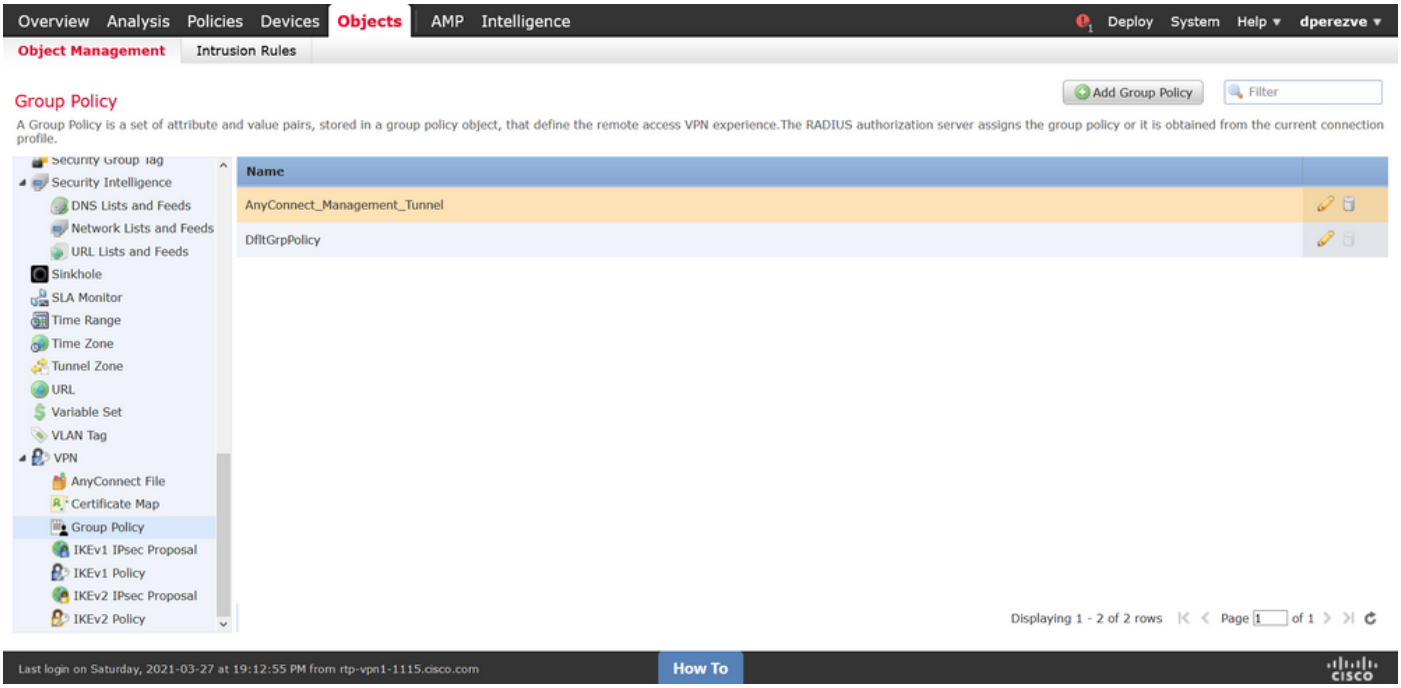
Quando si apre la finestra **Add Group Policy**, assegnare un nome, definire un pool AnyConnect e aprire la scheda **AnyConnect**. Passare a **Profilo** e selezionare l'oggetto che rappresenta il profilo VPN AnyConnect standard nel menu a discesa **Profilo client**.



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**.



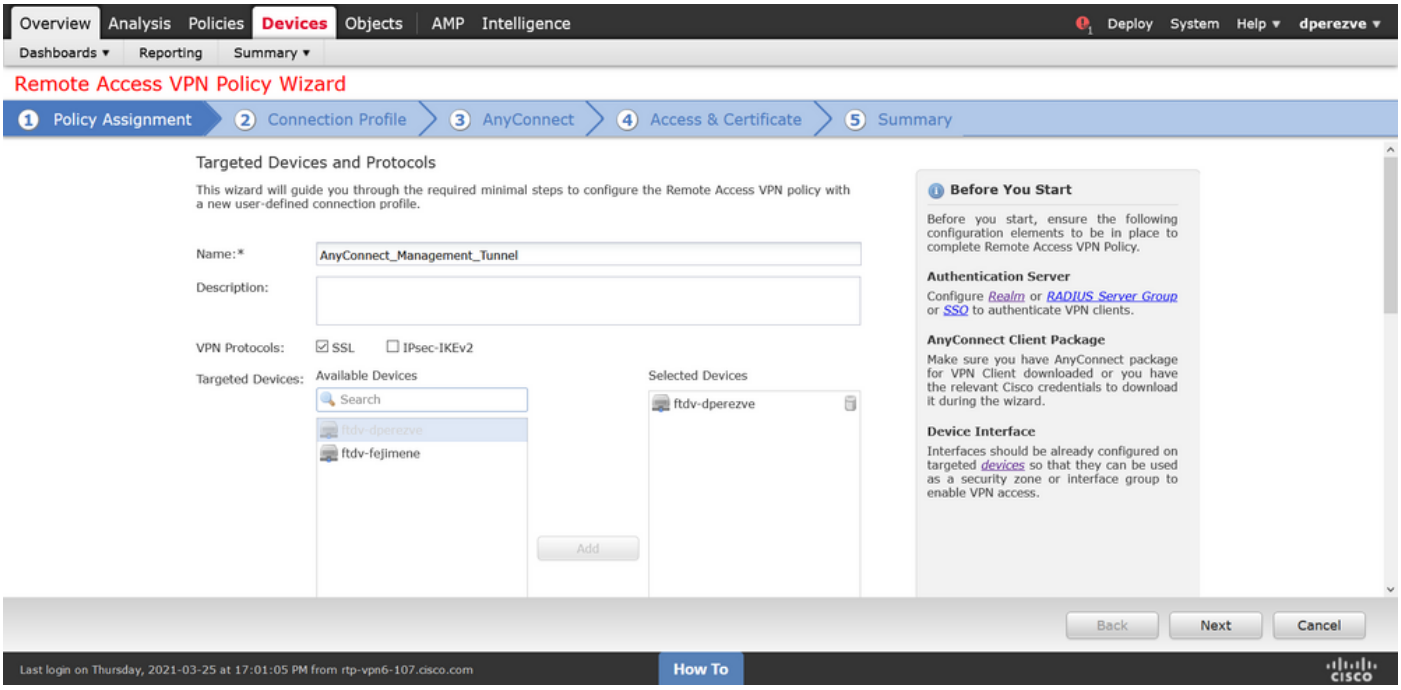
Salvare le modifiche per aggiungere il nuovo oggetto ai Criteri di gruppo esistenti.



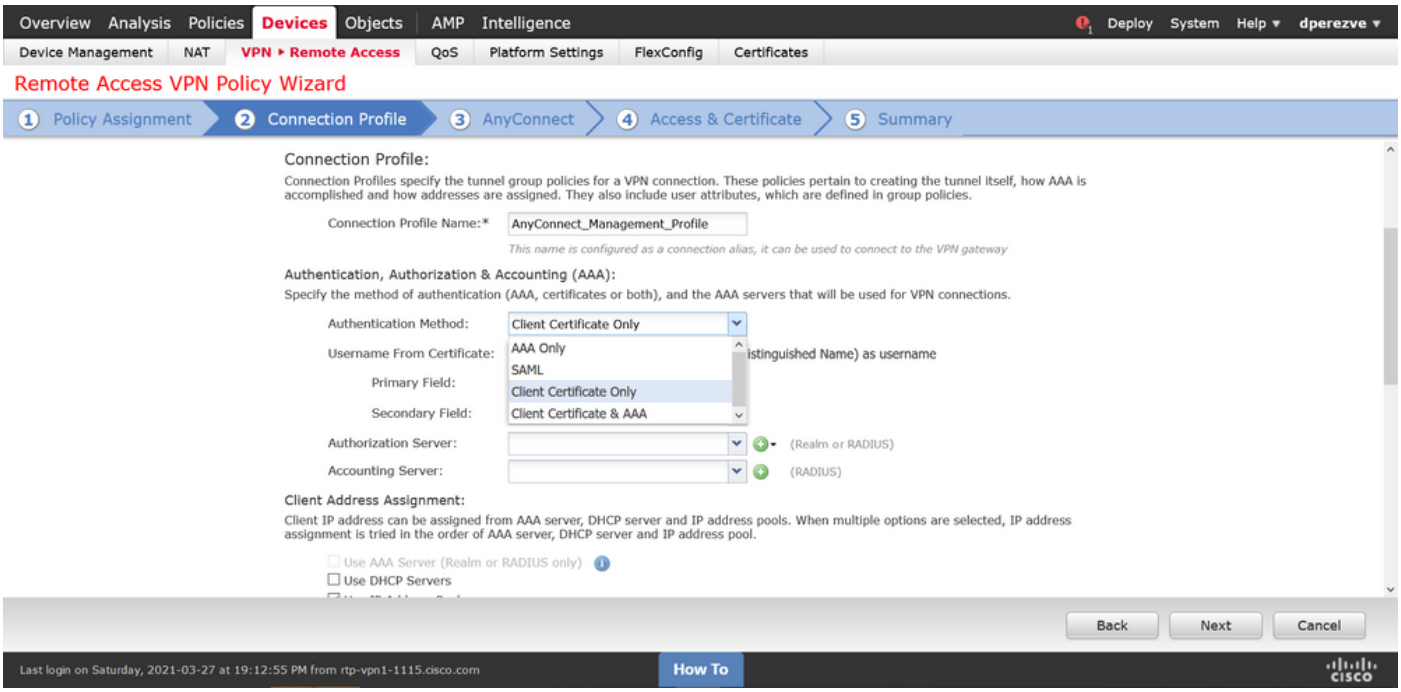
Passaggio 5. Creazione di una nuova configurazione di AnyConnect

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**.

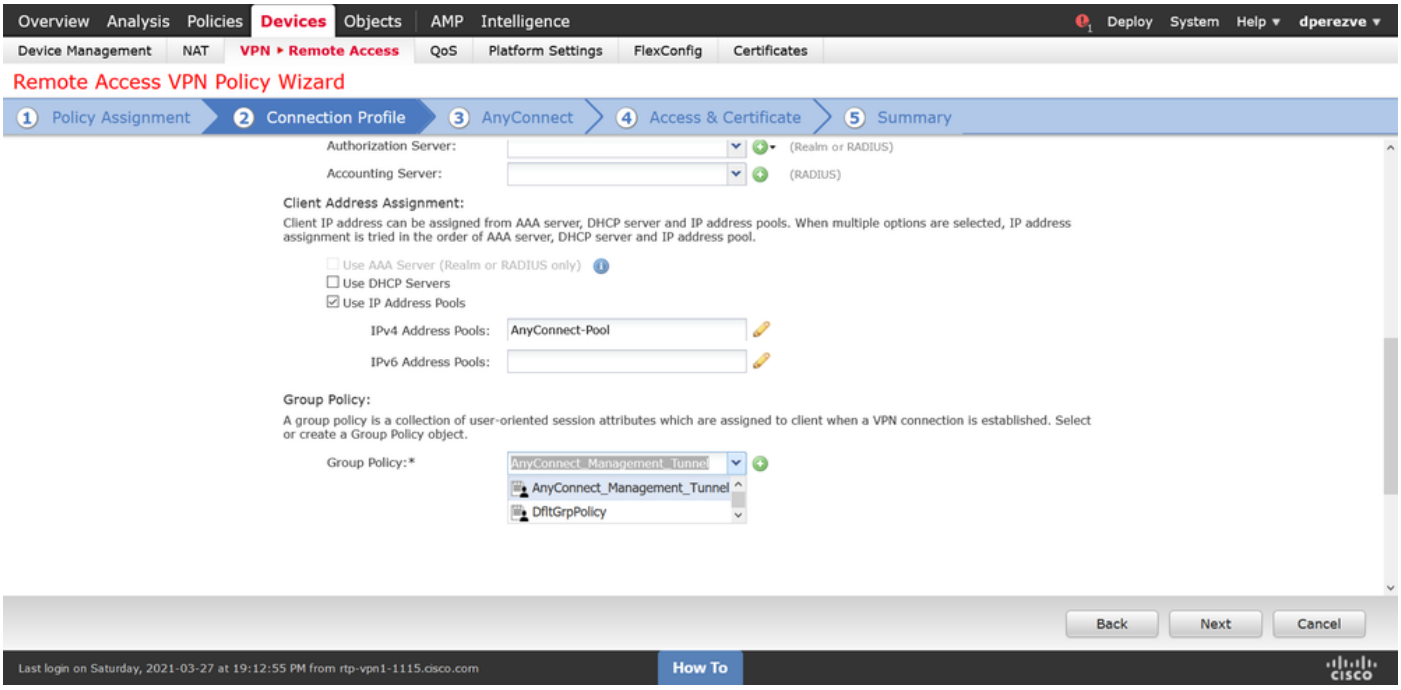
Nella scheda **Assegnazione criteri** selezionare il dispositivo FTD desiderato, definire un nome per il profilo di connessione e selezionare la casella di controllo SSL.



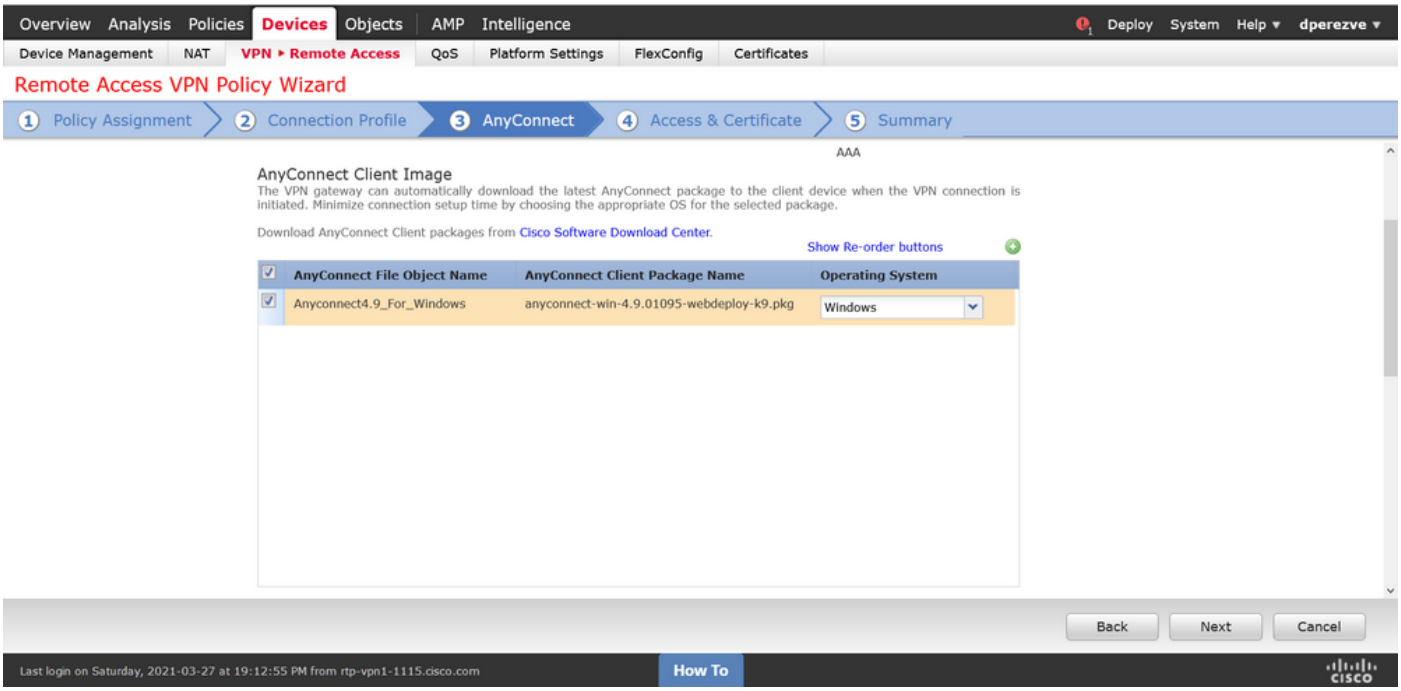
In **Profilo connessione** selezionare **Solo certificato client** come metodo di autenticazione. Questa è l'unica autenticazione supportata per la funzionalità.



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



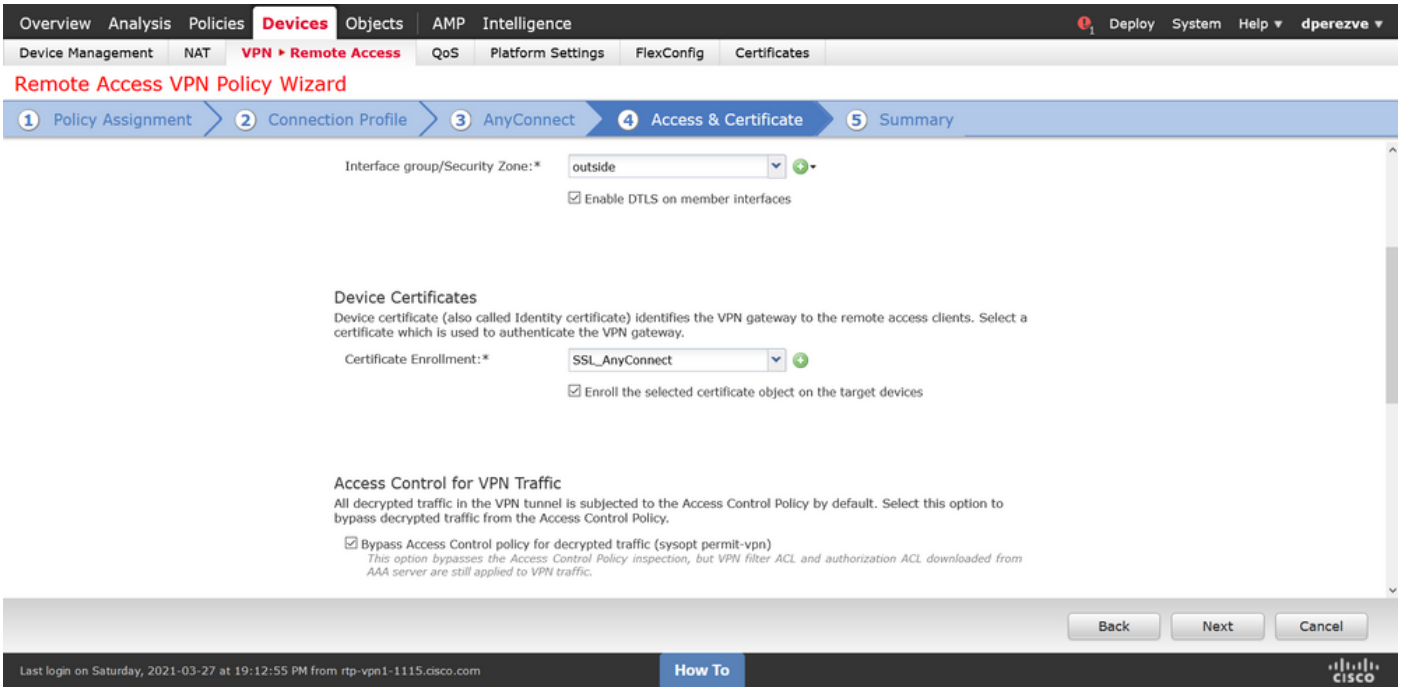
Nella scheda **AnyConnect**, selezionare l'**oggetto file** AnyConnect in base al sistema operativo (OS) sull'endpoint.



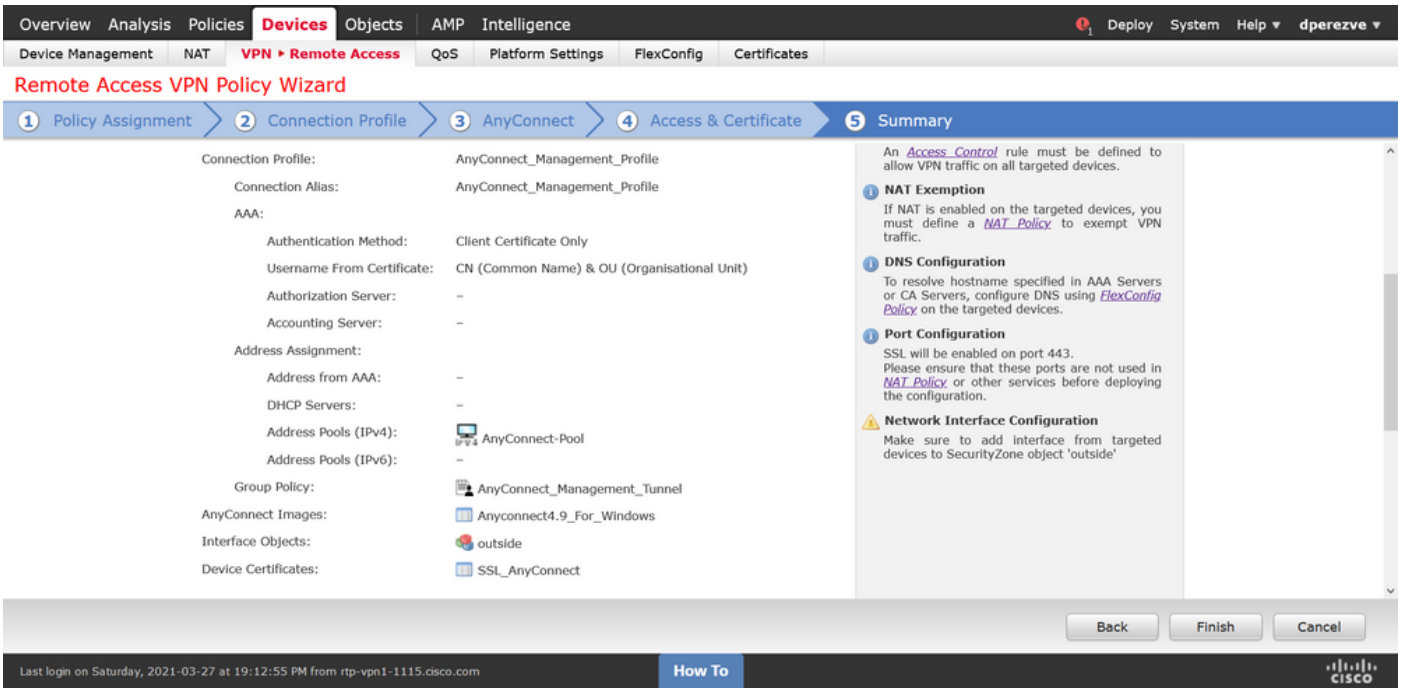
In **Accesso e certificato** specificare il certificato che deve essere utilizzato dall'FTD per verificare la propria identità al client Windows.

> **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).



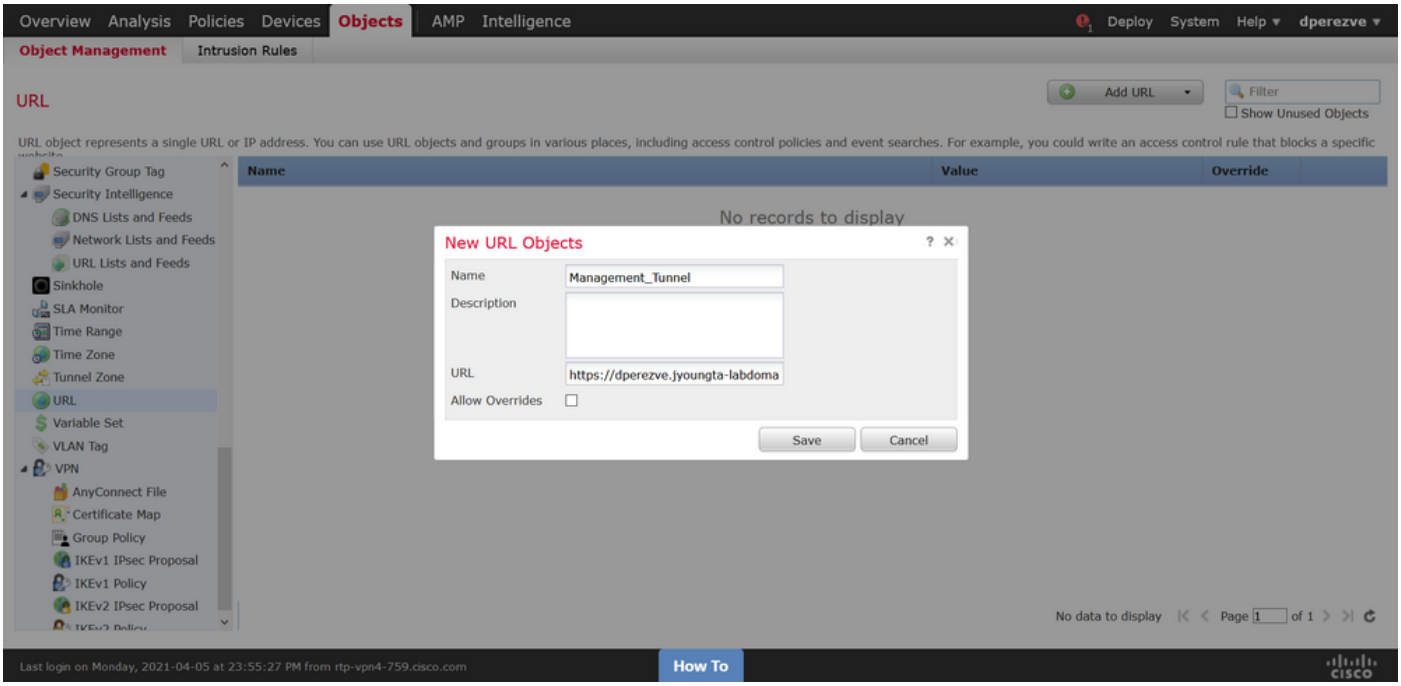
Infine, selezionare il pulsante **Finish** (Fine) nella scheda **Summary** per aggiungere la nuova configurazione AnyConnect.



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.