Configure Secure Client VPN Management Tunnel on Secure Firewall

Contents

Introduction

This document describes how to configure a Secure Client VPN Management tunnel on a Secure Firewall Threat Defense that is managed by the Cisco FMC.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco AnyConnect Profile Editor
- SSL AnyConnect configuration through Firewall Management Center (FMC)
- Client Certificate authentication

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Firewall Threat Defense (FTD) version 6.7.0 (Build 65)
- Cisco FMC version 6.7.0 (Build 65)
- Cisco AnyConnect 4.9.01095 installed on Windows 10 machine

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

In the example, Secure Sockets Layer (SSL) is used to create a Virtual Private Network (VPN) between FTD and a Windows 10 client.

From release 6.7, Cisco FTD supports configuration of AnyConnect Management tunnels. This fixes previously opened enhancement request Cisco bug ID CSCvs78215.

The AnyConnect Management feature allows you to create a VPN tunnel immediately after the endpoint finishes its startup. There is no need that the users manually launch the AnyConnect app. As soon as their system is powered up, the AnyConnect VPN agent service detects the Management VPN feature and initiates an AnyConnect session using theHost Entry defined in the Server List of the AnyConnect Management VPN Profile.

Limitations

- Only Client Certificate authentication is supported.
- Only Machine Certificate Store is supported for Windows clients.
- Not supported on Cisco Firepower Device Manager (FDM) Cisco bug ID CSCvx90058.
- Not supported on Linux clients.

Full limitations are described in the Cisco Secure Client Administrator Guide, Release 5.

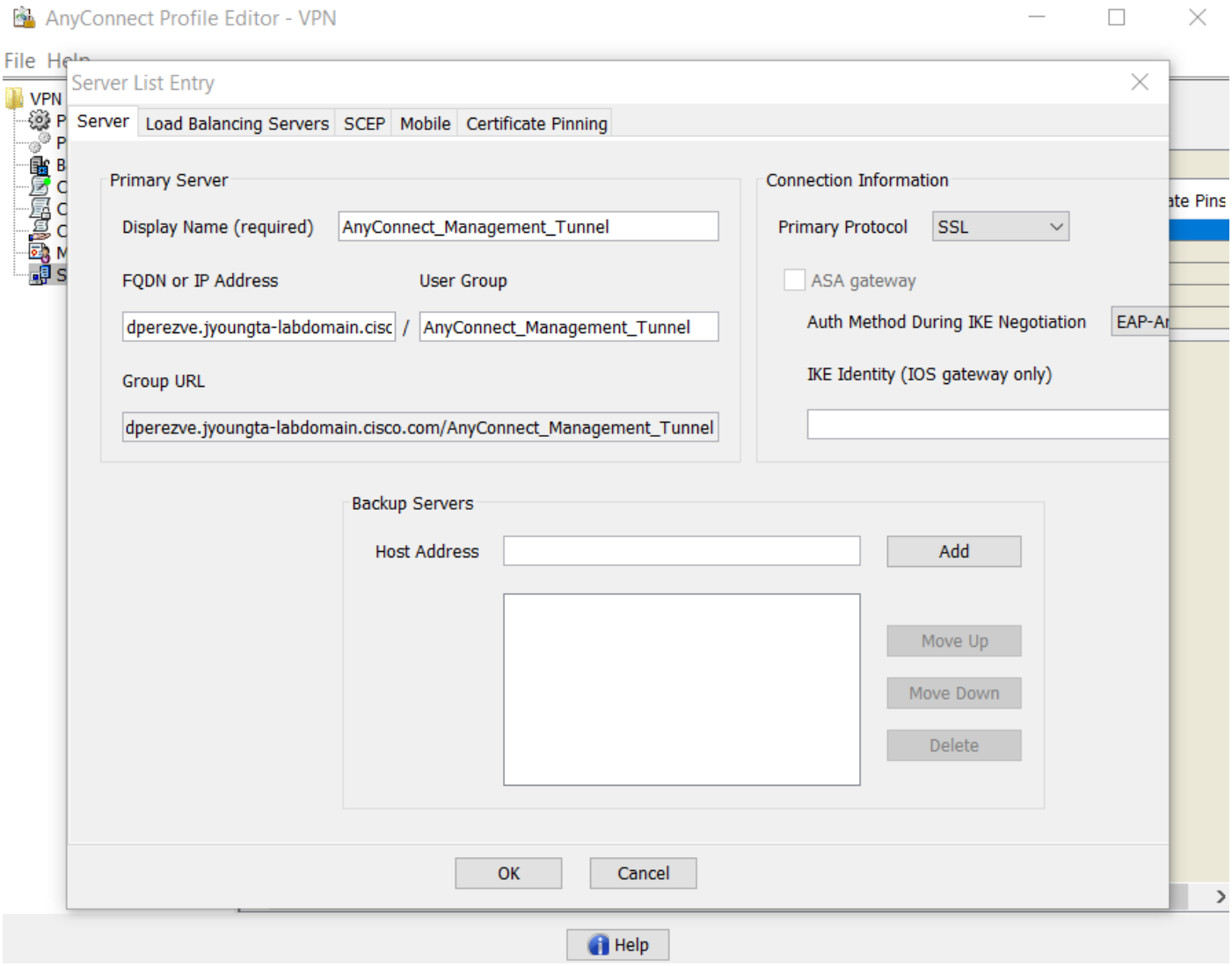
Configure

Configurations

Step 1. Create AnyConnect Management VPN Profile

Open the AnyConnect Profile Editor to create AnyConnect Management VPN Profile. The Management Profile contains all the settings used to establish the VPN tunnel after the endpoint boots up.

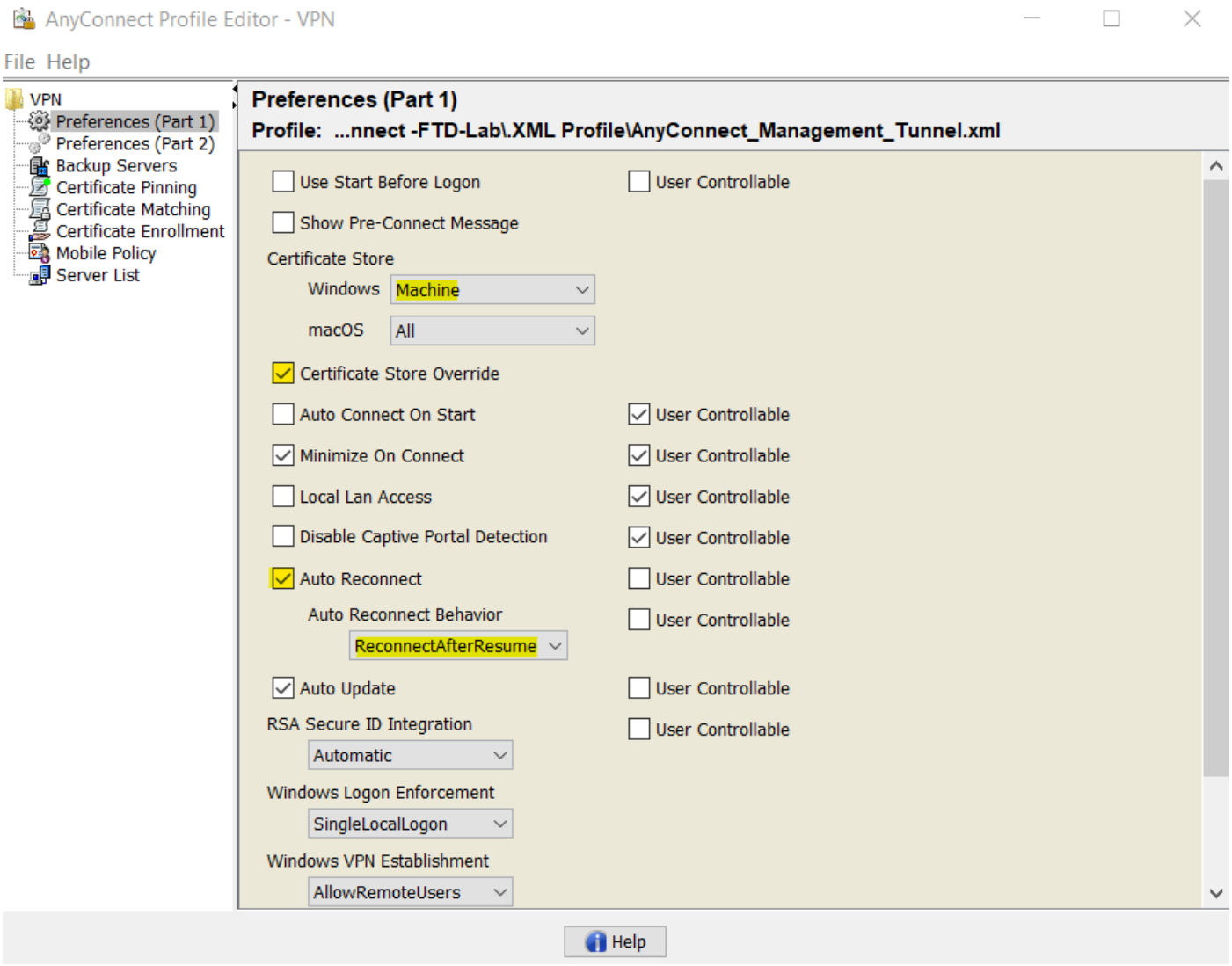
In this example, a Server List entry that points to Fully Qualified Domain Name (FQDN) dperezve.jyoungta-labdomain.cisco.com is defined and SSL is selected as the primary protocol. To add a Server List, navigate to **Server List** and select **Add** button. Fill the required fields and save changes.



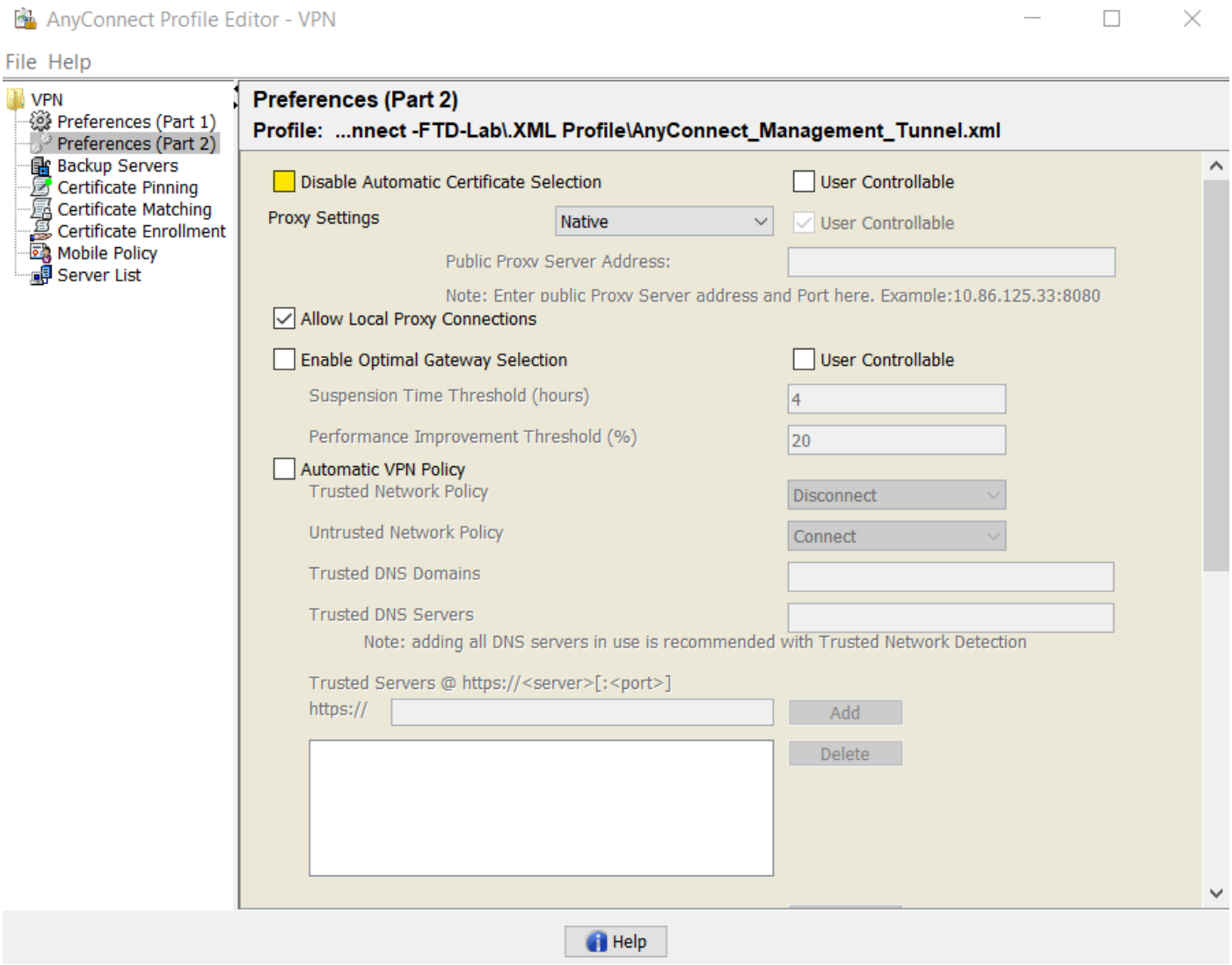
Besides the Server List, the Management VPN Profile must contain some mandatory preferences:

- AutomaticCertSelection must be set to true.
- AutoReconnect must be set to true.
- AutoReconnectBehavior must be configured for ReconnectAfterResume.
- AutoUpdate must be set to false.
- BlockUntrustedServers must be set to true.
- CertificateStore must be configured for MachineStore.
- CertificateStoreOverride must be set to true.
- EnableAutomaticServerSelection must be set to false.
- EnableScripting must be set to false.
- RetainVPNOnLogoff must be set to true.

In AnyConnect Profile Editor, navigate to **Preferences (Part 1)** and adjust settings as follows:



Then navigate to **Preferences (Part 2)** and uncheck the **Disable Automatic Certificate Selection** option.



Step 2. Create AnyConnect VPN Profile

As an addition to the Management VPN Profile, the regular AnyConnect VPN Profile needs to be configured. The AnyConnect VPN Profile is used in the first connection try. During this session, the Management VPN Profile is downloaded from FTD.

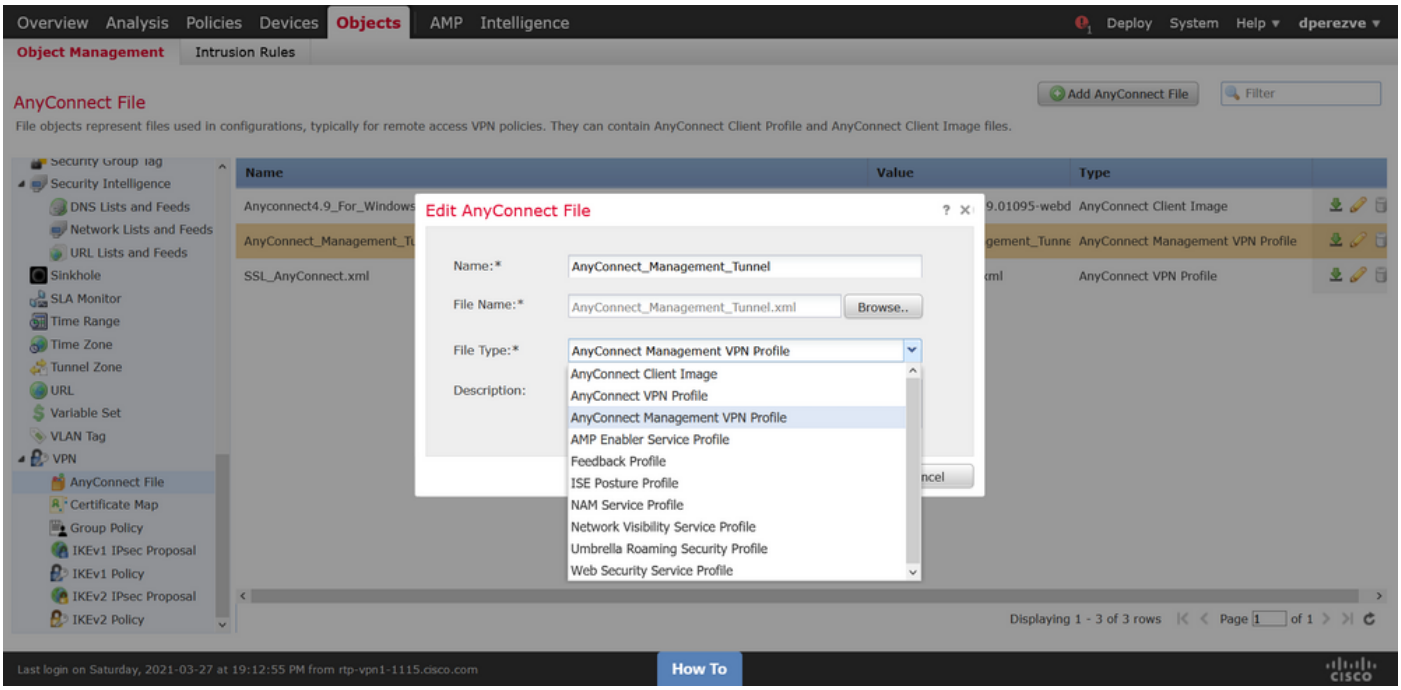
Use the AnyConnect Profile Editor to create the AnyConnect VPN Profile. In this case, both files contain the same settings so the same procedure can be follow.

Step 3. Upload AnyConnect Management VPN Profile and AnyConnect VPN Profile to FMC

Once the profiles are created, the next step is upload them to the FMC as AnyConnect File objects.

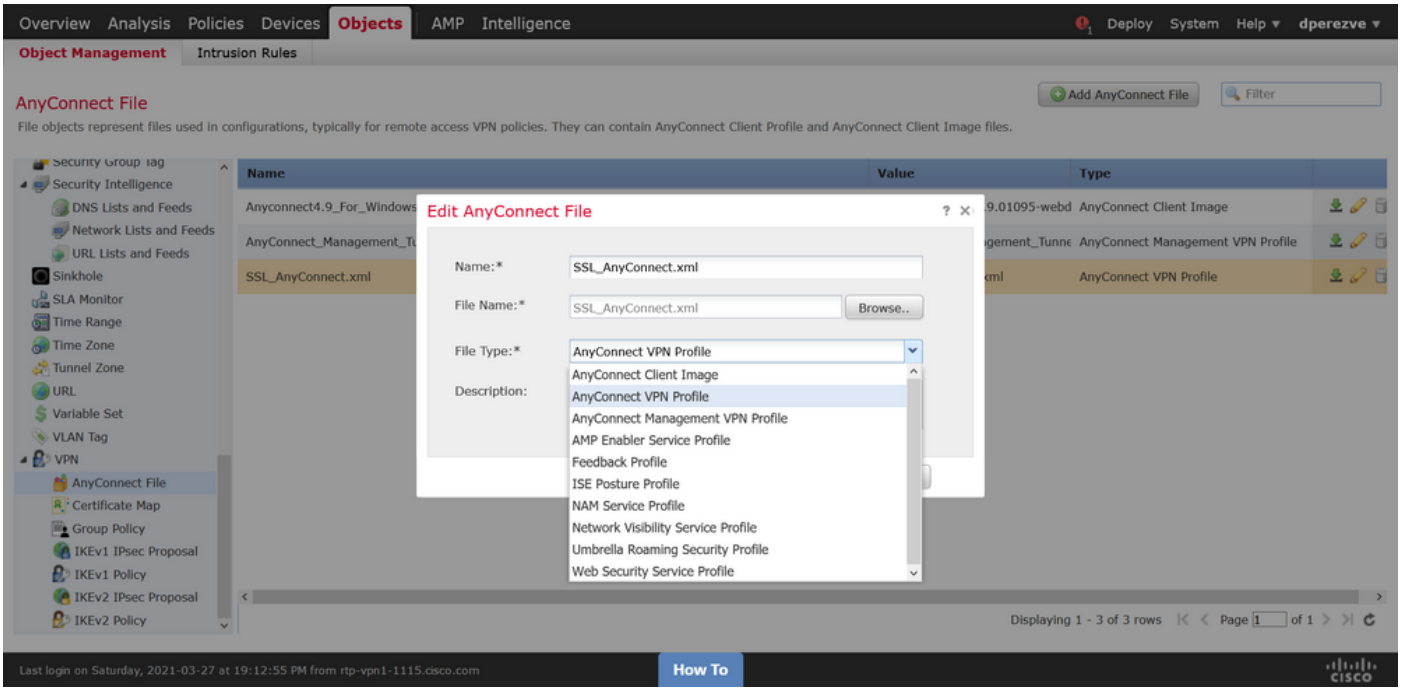
In order to upload the new AnyConnect Management VPN Profile to FMC, navigate to **Objects > Object Management** and choose **VPN** option from the table of contents, then select the **Add AnyConnect File** button.

Provide a name for the file. Choose **AnyConnect Management VPN Profile** as the file type and save the object.

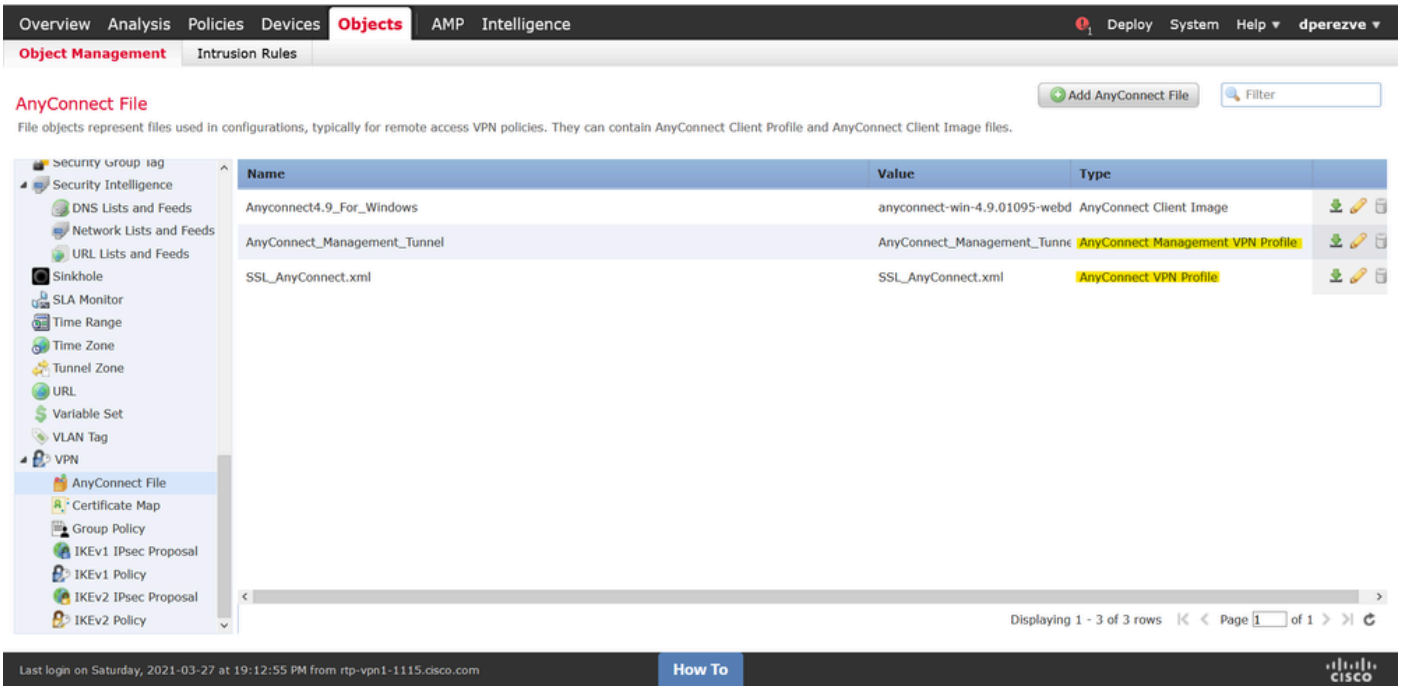


Now, in order to upload the AnyConnect VPN Profile navigate again to **Objects > Object Management** and choose **VPN** option from the table of contents, then select the **Add AnyConnect File** button.

Provide a name for the file but this time choose **AnyConnect VPN Profile** as the file type and save the new object.



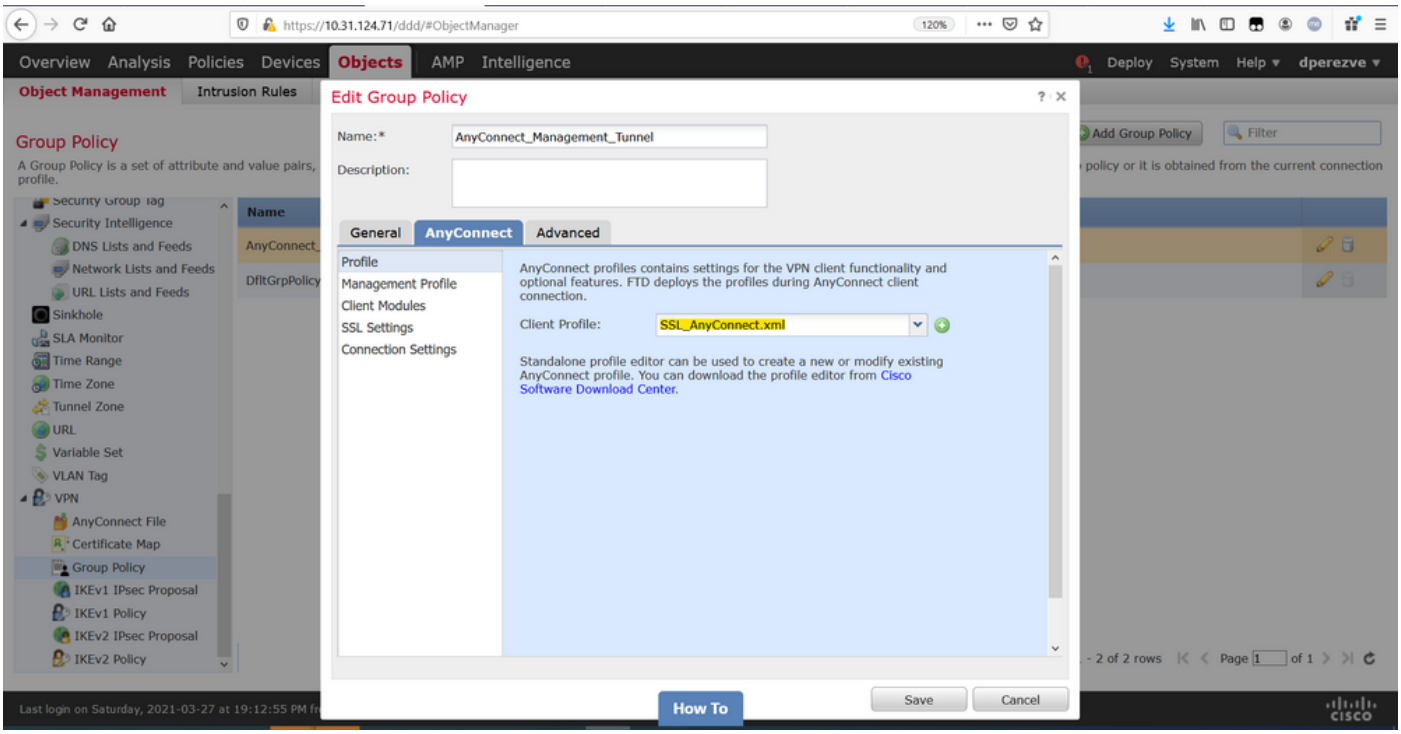
Profiles must be added to the object list and marked as **AnyConnect Management VPN Profile** and **AnyConnect VPN Profile** respectively.



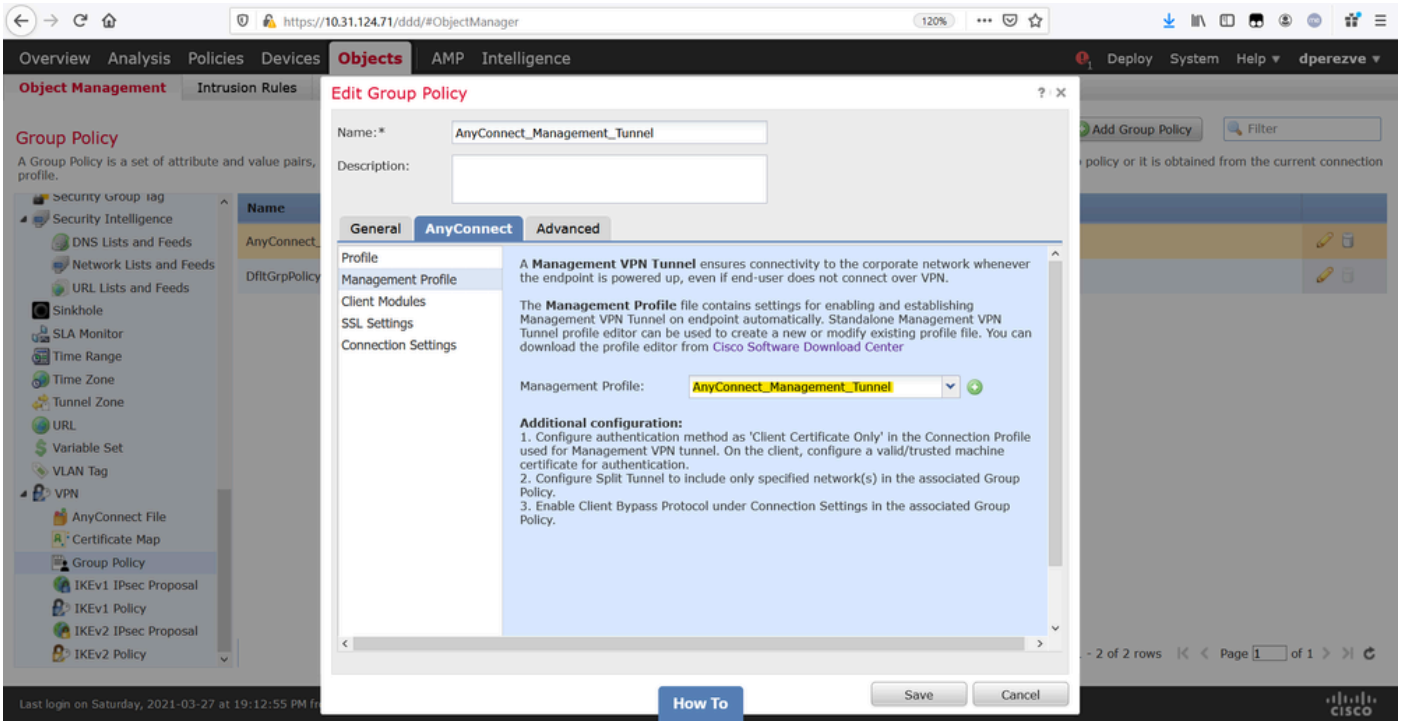
Step 4. Create Group Policy

In order to create a new Group Policy navigate to **Objects > Object Management** and choose **VPN** option from the table of contents, then select **Group Policy** and clic on the **Add Group Policy** button.

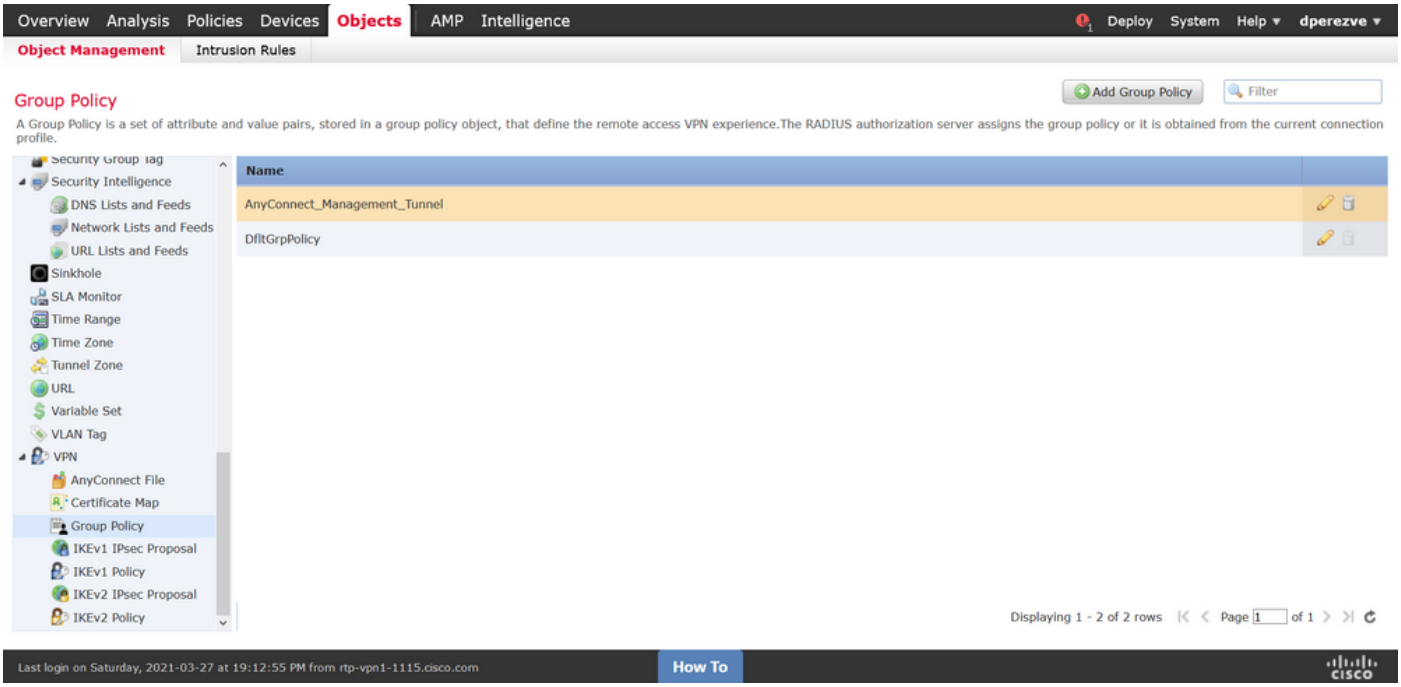
Once the **Add Group Policy** window opens, assign a name, define an AnyConnect pool and open the **AnyConnect** tab. Navigate to **Profile** and select the object that represents the regular AnyConnect VPN Profile in the **Client Profile** drop down menu.



Then, navigate to **Management Profile** tab and select the object that contains the Management VPN Profile in the **Management Profile** drop down menu.



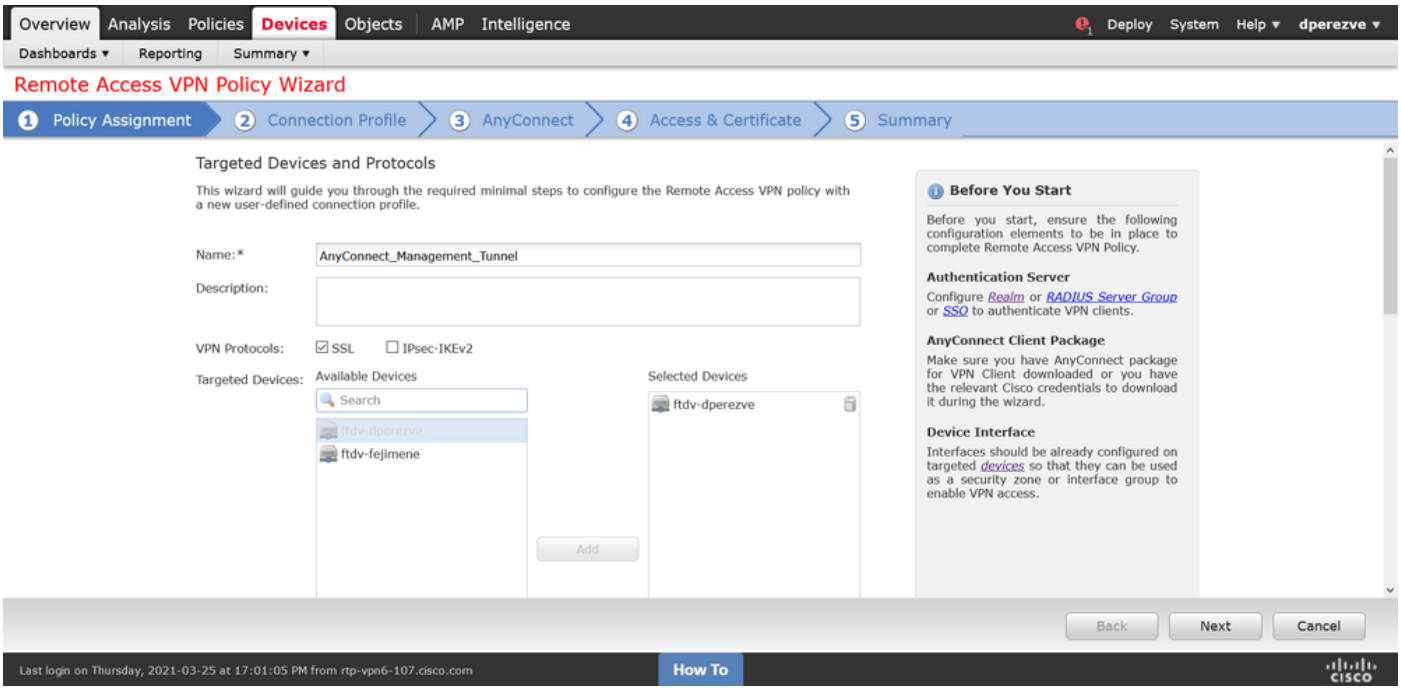
Save the changes to add the new object to the existing Group Policies.



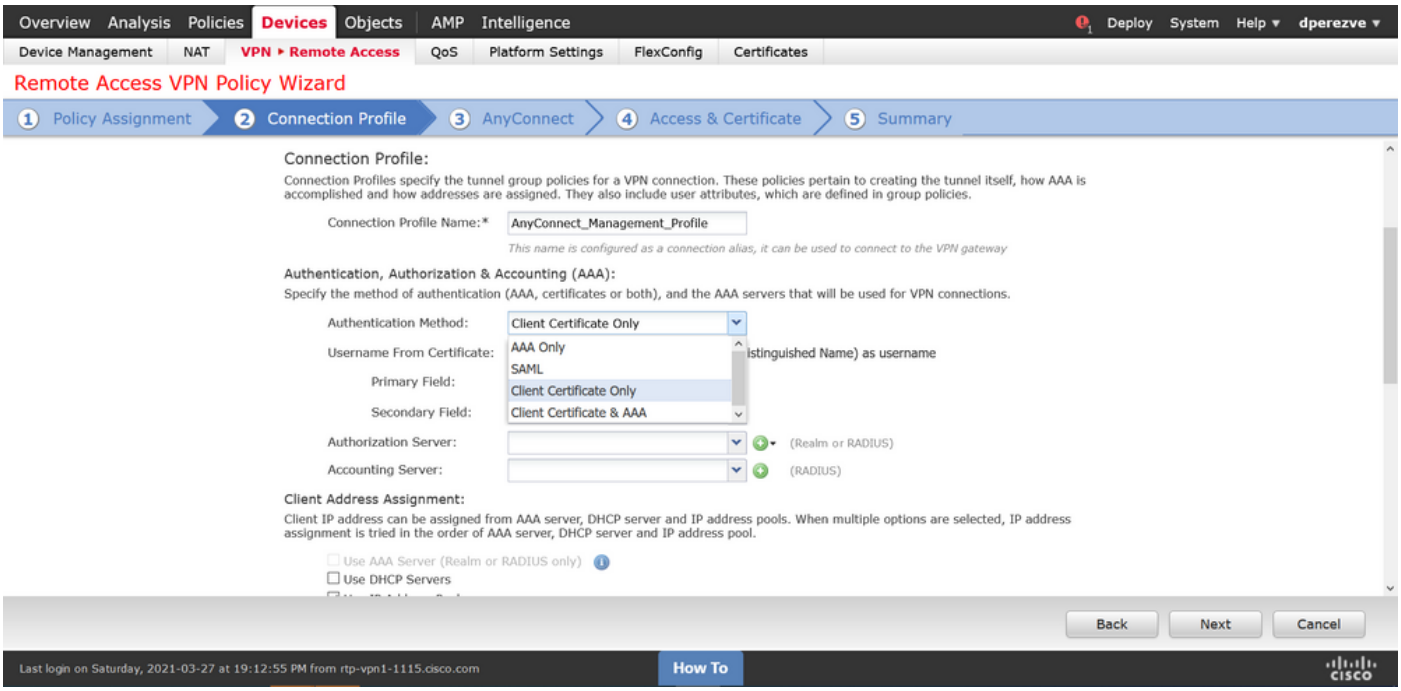
Step 5. Create New AnyConnect Configuration

The configuration of SSL AnyConnect in FMC is composed of 4 different steps. To configure AnyConnect navigate to **Devices > VPN > Remote Access** and select the **Add** button. This must open the **Remote Access VPN Policy Wizard**.

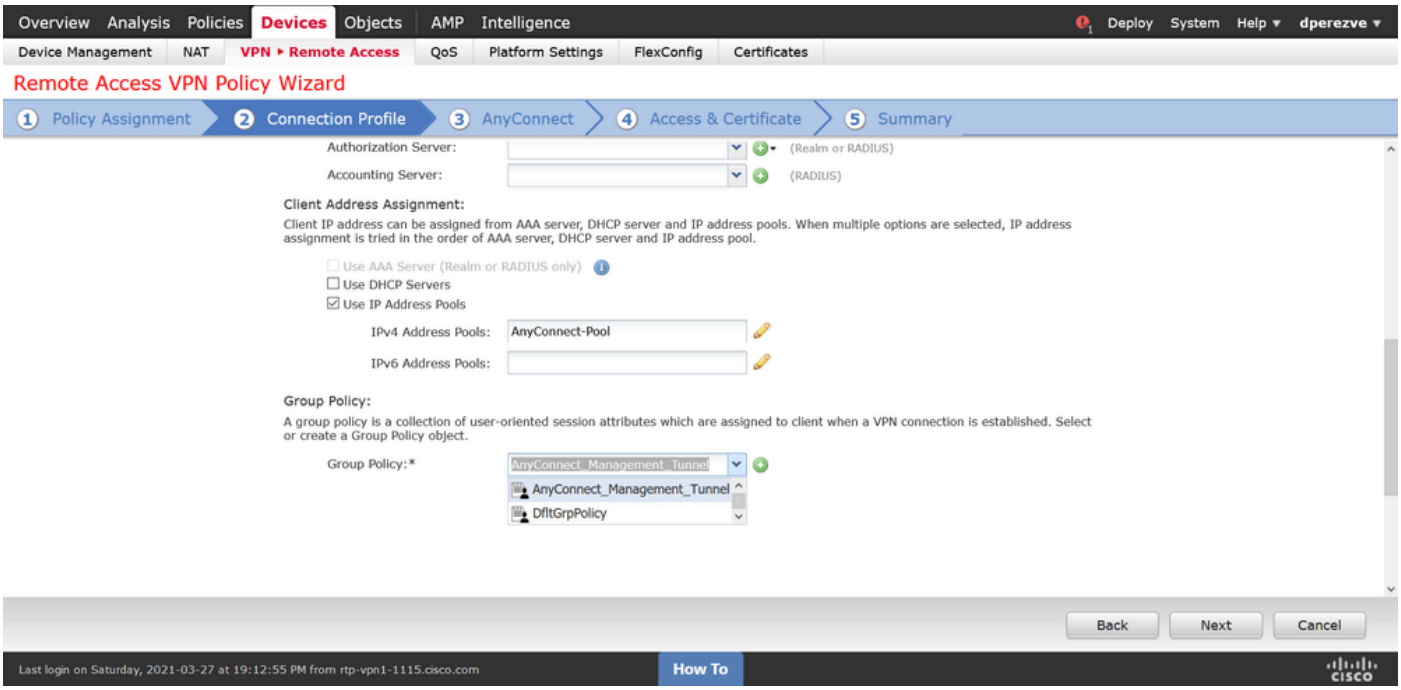
On **Policy Assignment** tab, select the FTD device at hand, define a name for the Connection Profile, and check the SSL checkbox.



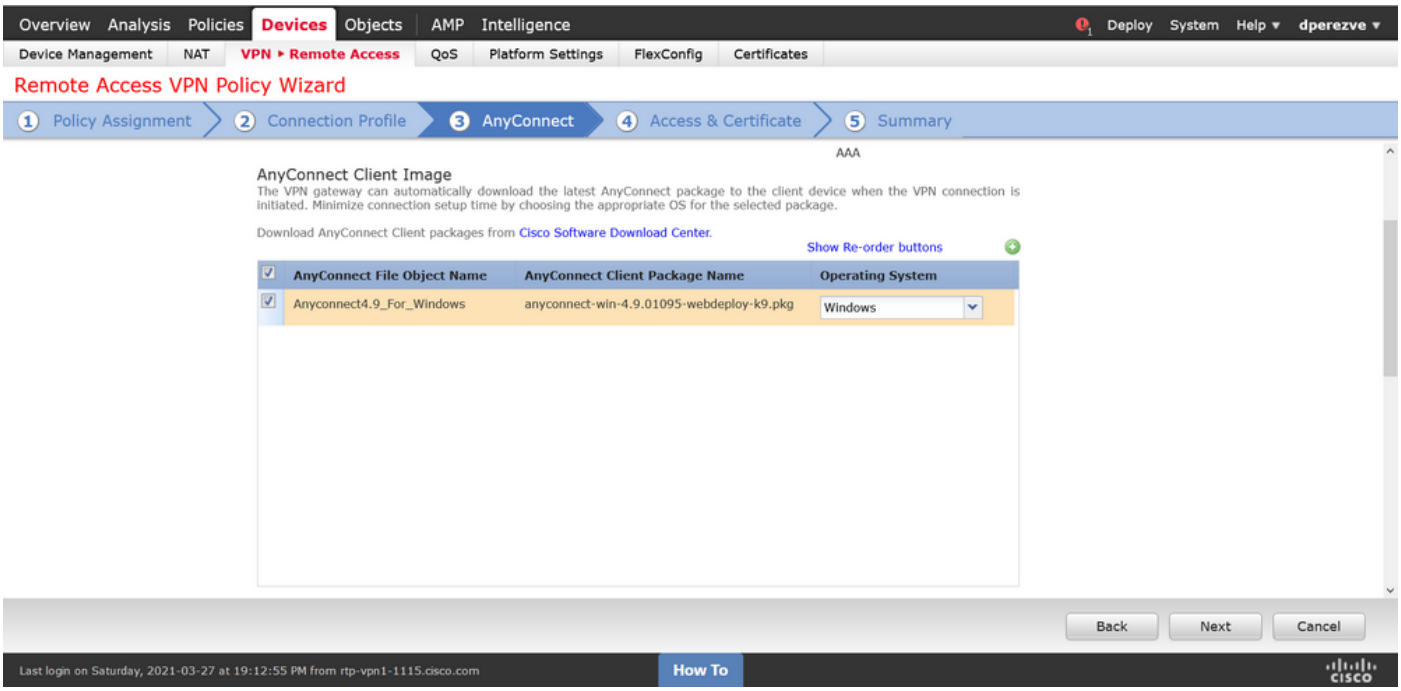
On **Connection Profile**, select **Client Certificate Only** as the authentication method. This is the only authentication supported for the feature.



Then select the Group Policy object created in step 3 in the **Group Policy** drop down.



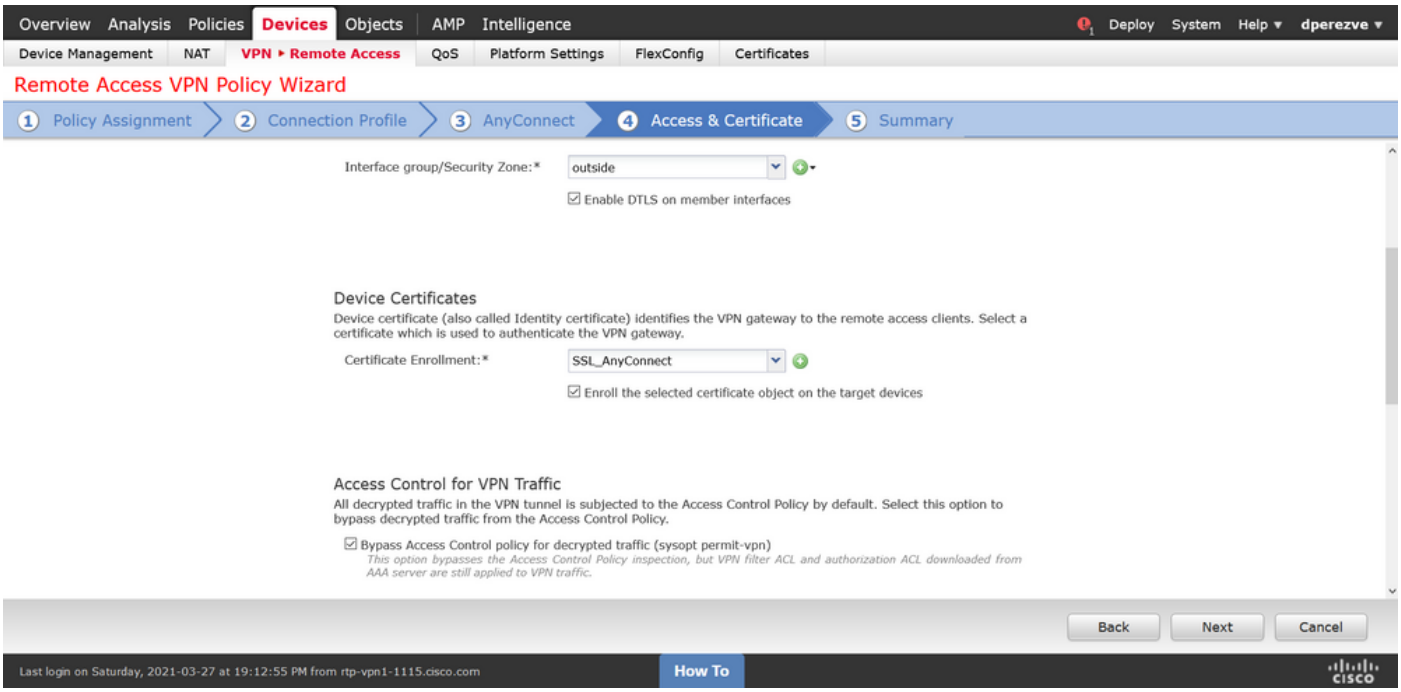
On **AnyConnect** tab, select the **AnyConnect File Object** according to the Operating System (OS) on the endpoint.



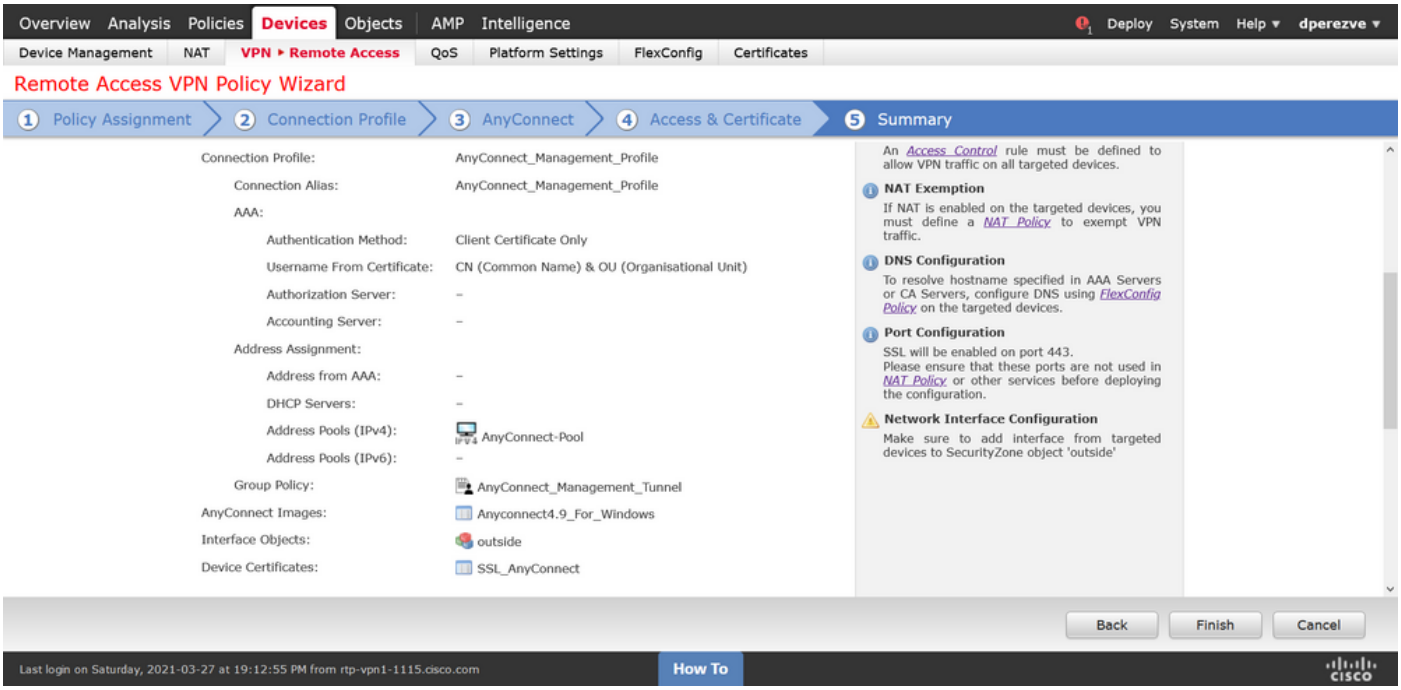
On **Access & Certificate**, specify the certificate that must be used by the FTD to probe its identity to the Windows client.

Note: Since users cannot interact with AnyConnect app when using the Management VPN feature, the certificate needs to be fully trusted and must not print any Warning message.

Note: In order to prevent certificate validation errors, the Common Name (CN) field included in the Subject Name of the certificate must match the FQDN defined in the Server List of XML profiles (Step 1 and Step 2).



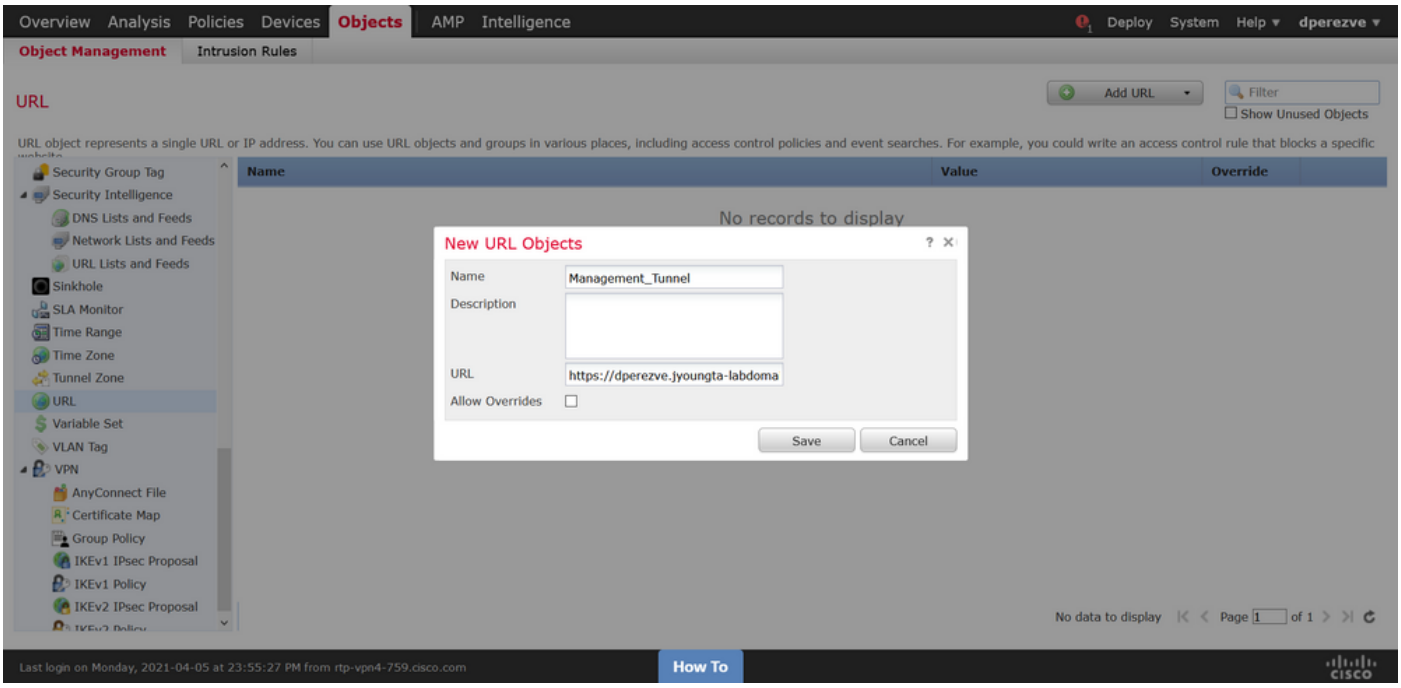
Finally, select **Finish** button on the **Summary** tab to add the new AnyConnect Configuration.



Step 6. Create URL Object

Navigate to **Objects > Object Management** and select **URL** from the table of contents. Then select **Add Object** in the **Add URL** drop down.

Provide a name for the object and define the URL using the same FQDN/User Group specified in the Management VPN Profile Server List (Step 2). In this example, URL must be dperezve.jyoungta-labdomain.cisco.com/AnyConnect_Management_Tunnel.

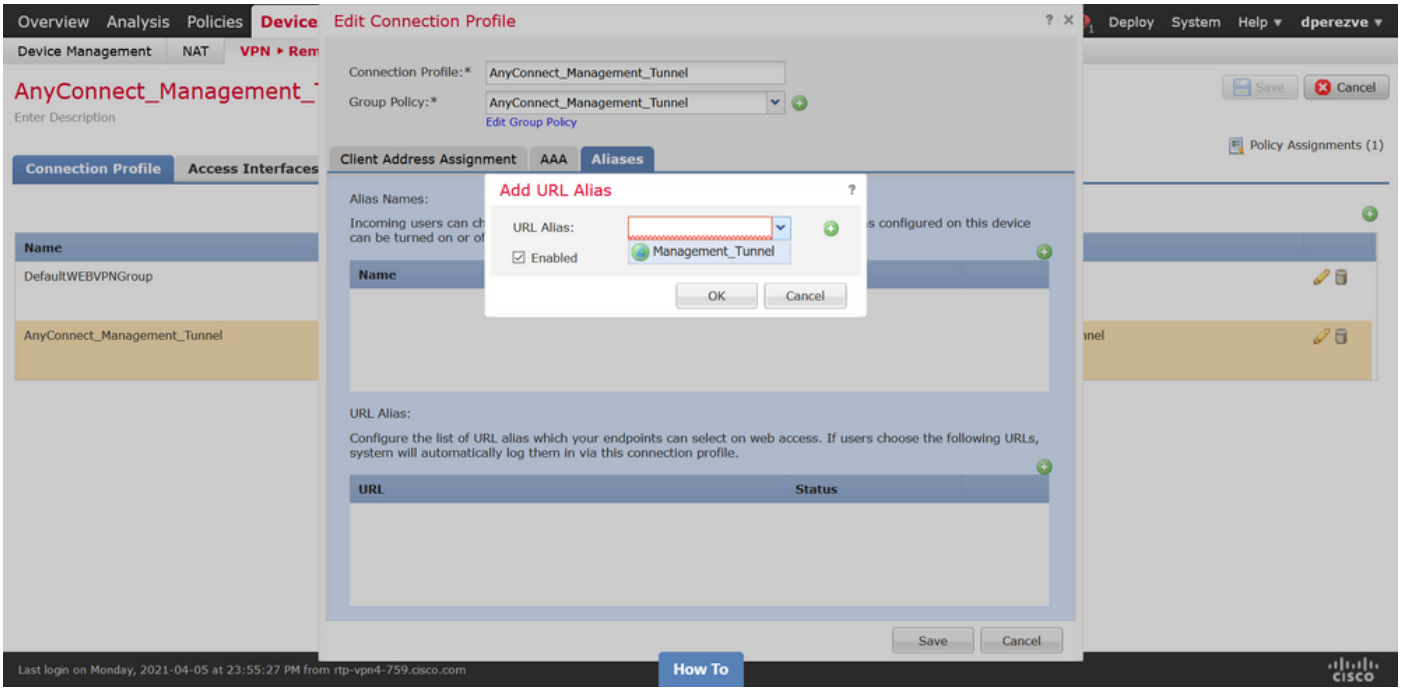


Save the changes to add the object to the object list.

Step 7. Define URL Alias

In order to enable the URL Alias in the AnyConnect configuration, navigate to **Devices > VPN > Remote Access** and click on the pencil icon to edit.

Then, on the **Connection Profile** tab, select the configuration at hand, navigate to **Aliases**, click on **Add** button, and select the **URL Object** in the **URL Alias** drop down . Ensure the **Enabled** check box is selected.



Save changes and deploy configurations to FTD.

Verify

After the deployment finishes, a first manual AnyConnect connection with the AnyConnect VPN Profile is needed. During this connection the Management VPN Profile is downloaded from FTD and stored in **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun**. From this point, subsequent connections must be initiated through the Management VPN profile without any user interaction.

Troubleshoot

For certificate validation errors:

- Ensure the root certificate for Certificate Authority (CA) is installed on the FTD.
- Ensure an identity certificate signed by the same CA is installed on Windows Machine Store.
- Ensure the CN field is included in the certificate and is the same as the FQDN defined in the Server List of the Management VPN Profile and FQDN defined in URL alias.

For Management tunnel not initiated:

- Ensure the Management VPN Profile has been downloaded and stored in **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun**.

- Ensure the name for the Management VPN Profile is **VpnMgmtTunProfile.xml**.

For connectivity problems, collect DART bundle and contact Cisco TAC for further research.