Configure Secure Client (AnyConnect) Scripts

Contents

Introduction

This document describes how to configure Cisco Secure Client scripting with Secure Firewall ASA and FTD.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- SSL Cisco Secure Client configuration through Secure Firewall ASA and Secure Firewall Threat Defense managed by Cisco Secure Firewall Management Center (FMC)
- ASDM access
- FTD SSH access
- OnConnect and OnDisconnect scripts

Components Used

- Secure Firewall ASA
- Secure Firewall Threat Defense
- Cisco Secure Firewall Management Center

- Cisco Secure Client 5.0.03072

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

We are covering 2 different configuration examples:

- Setting up Secure Client scripting with Secure Firewall ASA managed by ASDM.
- Setting up Secure Client scripting with Secure Firewall Threat Defense managed by Cisco Secure Firewall Management Center.

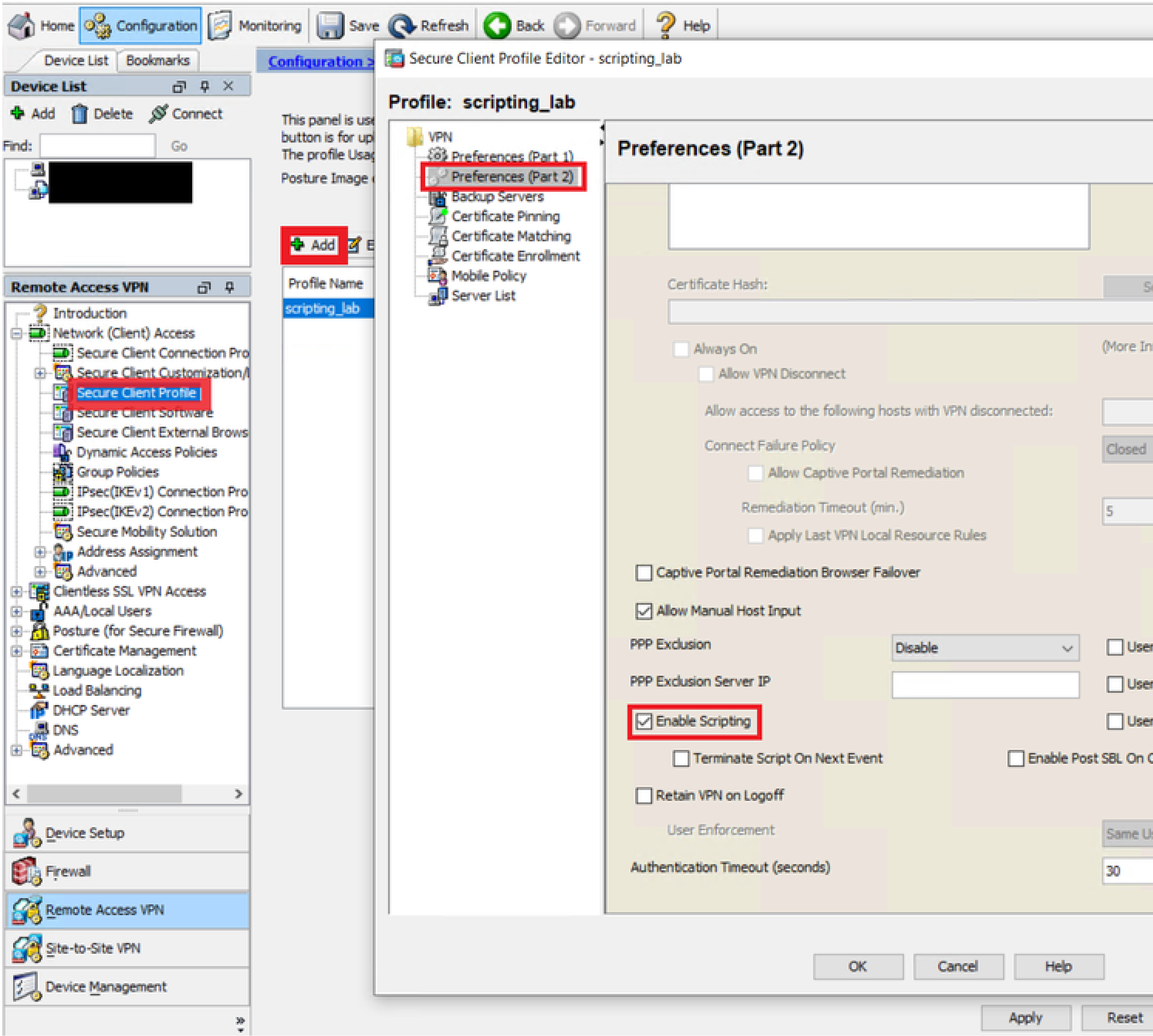
With FTD managed by FMC this is still not officially supported by the FMC so we are going to implement a workaround to the enhancement request Cisco bug ID CSCvt58044 .

Configure

Configurations

Setting up Secure Client scripting with Secure Firewall ASA managed by ASDM configuration example:

Step 1. Create a Secure Client Profile and Enable Scripting in Preferences (Part 2).



[redacted]

Profile: scripting_lab

Preferences (Part 2)

Certificate Hash:

□ Always On (More In

□ Allow VPN Disconnect

Allow access to the following hosts with VPN disconnected:

Connect Failure Policy: Closed

□ Allow Captive Portal Remediation

Remediation Timeout (min.): 5

□ Apply Last VPN Local Resource Rules

□ Captive Portal Remediation Browser Failover

☑ Allow Manual Host Input

PPP Exclusion: Disable □ User

PPP Exclusion Server IP: □ User

☑ Enable Scripting □ User

□ Terminate Script On Next Event □ Enable Post SBL On C

□ Retain VPN on Logoff

User Enforcement: Same U

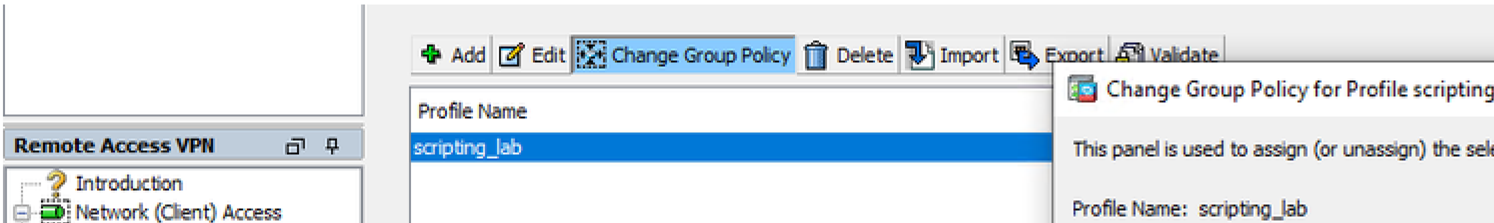
Authentication Timeout (seconds): 30

AnyConnect XML Profile editor

Additional options from the xml profile:

- Check Terminate Script On Next Event to enable the client to terminate a running script process if a transition to another scriptable event occurs. For example, the client terminates a running On Connect script if the VPN session ends and terminates a running OnDisconnect script if Cisco Secure Client starts a new VPN session. On Microsoft Windows, the client also terminates any scripts that the On Connect or OnDisconnect script launched, and all their script descendents. On macOS and Linux, the client terminates only the On Connect or OnDisconnect script; it does not terminate child scripts.
- Check Enable Post SBL On Connect Script (enabled by default) to let the client launch the On Connect script (if present) if SBL establishes the VPN session.

Make sure you assign the AnyConnect Profile to the proper Group Policy:



This panel is used to assign (or unassign) the sel

Profile Name: scripting_lab

```
Err.Clear

Set objShell = CreateObject("WScript.Shell")
objShell.LogEvent 0, "Sample AnyConnect OnConnect script."

Dim strDriveLetter, strRemotePath
strDriveLetter = "REPLACE_WITH_DRIVE_LETTER:"
strRemotePath = "\\REPLACE_WITH_SERVER_NAME\REPLACE_WITH_SHARE"

Set objNetwork = CreateObject("WScript.Network")

' remove old mapping (if any)
objNetwork.RemoveNetworkDrive strDriveLetter

' add new mapping
objNetwork.MapNetworkDrive strDriveLetter, strRemotePath

If Err.Number <> 0 Then
objShell.LogEvent 0, "Failed to map network drive." & vbCrLf & Err.Number & ": " & Err.Description
End If

WScript.Quit
```

OnDisconnect.vbs

```
ON ERROR RESUME NEXT
Err.Clear

Set objShell = CreateObject("WScript.Shell")
objShell.LogEvent 0, "Sample AnyConnect OnDisconnect script."

Dim strDriveLetter
strDriveLetter = "REPLACE_WITH_DRIVE_LETTER:"

Set objNetwork = CreateObject("WScript.Network")

' remove old mapping (if any)
objNetwork.RemoveNetworkDrive strDriveLetter

WScript.Quit
```

2. Script to refresh a windows group policy:

OnConnect.vbs or OnDisconnect.vbs

```
ON ERROR RESUME NEXT
Err.Clear

Set objShell = CreateObject("WScript.Shell")
objShell.LogEvent 0, "Sample AnyConnect OnConnect script."

' refreshes local and Active Directory-based Group Policy settings, including security settings
returnCode = objShell.Run("gpupdate.exe /force", 0, True)
```

```
If returnCode <> 0 Then
objShell.LogEvent 0, "Failed to update Group Policy settings." & vbCrLf & Err.Number & ": " & Err.Descri
End If

objShell.LogEvent 0, "User's Group Policy settings have been updated."

WScript.Quit
```

3. Launching multiple scripts:

Script1.vbs

```
ON ERROR RESUME NEXT
Err.Clear

Set objShell = CreateObject("WScript.Shell")
objShell.LogEvent 0, "Sample script 1."

WScript.Quit
```

Script2.vbs

```
ON ERROR RESUME NEXT
Err.Clear

Set objShell = CreateObject("WScript.Shell")
objShell.LogEvent 0, "Sample script 2."

WScript.Quit 5
```

Script3.vbs

```
ON ERROR RESUME NEXT
Err.Clear

Set objShell = CreateObject("WScript.Shell")
objShell.LogEvent 0, "Sample script 3."

WScript.Quit
```

OnConnect.vbs or OnDisconnect.vbs

```
ON ERROR RESUME NEXT
Err.Clear
```

```
Set objShell = CreateObject("WScript.Shell")
objShell.LogEvent 0, "Sample AnyConnect OnConnect script."

' launch each script after the previous has completed
returnCode = objShell.Run("wscript.exe Script1.vbs", 0, True)
objShell.LogEvent 0, "Script1.vbs returned = " & returnCode

returnCode = objShell.Run("wscript.exe Script2.vbs", 0, True)
objShell.LogEvent 0, "Script2.vbs returned = " & returnCode

returnCode = objShell.Run("wscript.exe Script3.vbs", 0, True)
objShell.LogEvent 0, "Script3.vbs returned = " & returnCode

WScript.Quit
```

> **Note**: **This samples are supplied as is with no implied warranty or support. It is designed to assist you in using the Cisco AnyConnect scripting feature. It is assumed that you are referring to this sample as a reference only.**

Linux Script

1. Launching multiple scripts:

Script1.sh

```
#!/bin/sh
logger "Sample script 1."
```

Script2.sh

```
#!/bin/sh
logger "Sample script 2."
```

Script3.sh

```
#!/bin/sh
logger "Sample script 3."
```

OnConnect.sh or OnDisconnect.sh

```
#!/bin/sh

logger "Sample AnyConnect OnConnect script."
```

```
# launch each script after the previous has completed
./Script1.sh
logger "Script1.sh returned = $?"

./Script2.sh
logger "Script2.sh returned = $?"

./Script3.sh
logger "Script3.sh returned = $?"
```

> **Note**: **This samples are supplied as is with no implied warranty or support. It is designed to assist you in using the Cisco AnyConnect scripting feature. It is assumed that you are referring to this sample as a reference only.**

MacOS scripts

1. Launching AppleScript:

Script1.scpt

```
#!/bin/sh
say "This is a Sample AppleScript"
```

OnConnect.sh

```
#!/bin/sh
logger "Sample AnyConnect OnConnect script."

# launch the AppleScript script
/usr/bin/osascript Script1.scpt
```

2. Launching multiple scripts

Script1.sh

```
#!/bin/sh
logger "Sample script 1."
```

Script2.sh

```
#!/bin/sh
logger "Sample script 2."
```

Script3.sh

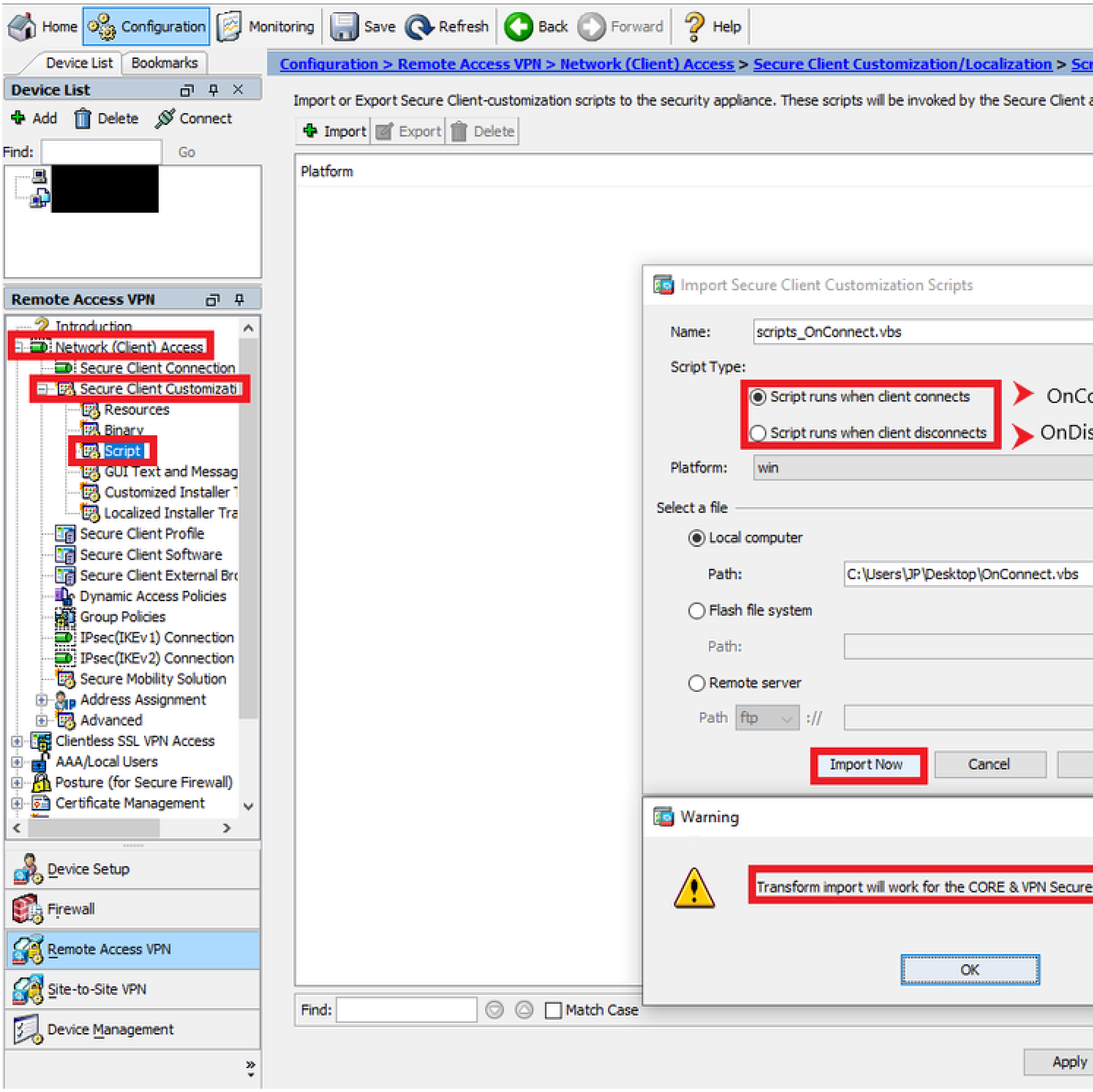
```
#!/bin/sh
logger "Sample script 3."
```

OnConnect.sh

```
#!/bin/sh
logger "Sample AnyConnect OnConnect script."

# launch each script after the previous has completed
./Script1.sh
logger "Script1.sh returned = $?"

./Script2.sh
logger "Script2.sh returned = $?"

./Script3.sh
logger "Script3.sh returned = $?"
```

> **Note: This samples are supplied as is with no implied warranty or support. It is designed to assist you in using the Cisco AnyConnect scripting feature. It is assumed that you are referring to this sample as a reference only.**

Step3. Import the script through ASDM



[redacted]

Configuration > Remote Access VPN > Network (Client) Access > Secure Client Customization/Localization > Scr

Import or Export Secure Client-customization scripts to the security appliance. These scripts will be invoked by the Secure Client a

Import Secure Client Customization Scripts

Name: scripts_OnConnect.vbs

Script Type:

● Script runs when client connects

○ Script runs when client disconnects

Platform: win

Select a file

● Local computer

Path: C:\Users\JP\Desktop\OnConnect.vbs

○ Flash file system

Path:

○ Remote server

Path ftp ://

Import Now | Cancel

Warning

Transform import will work for the CORE & VPN Secure

OK

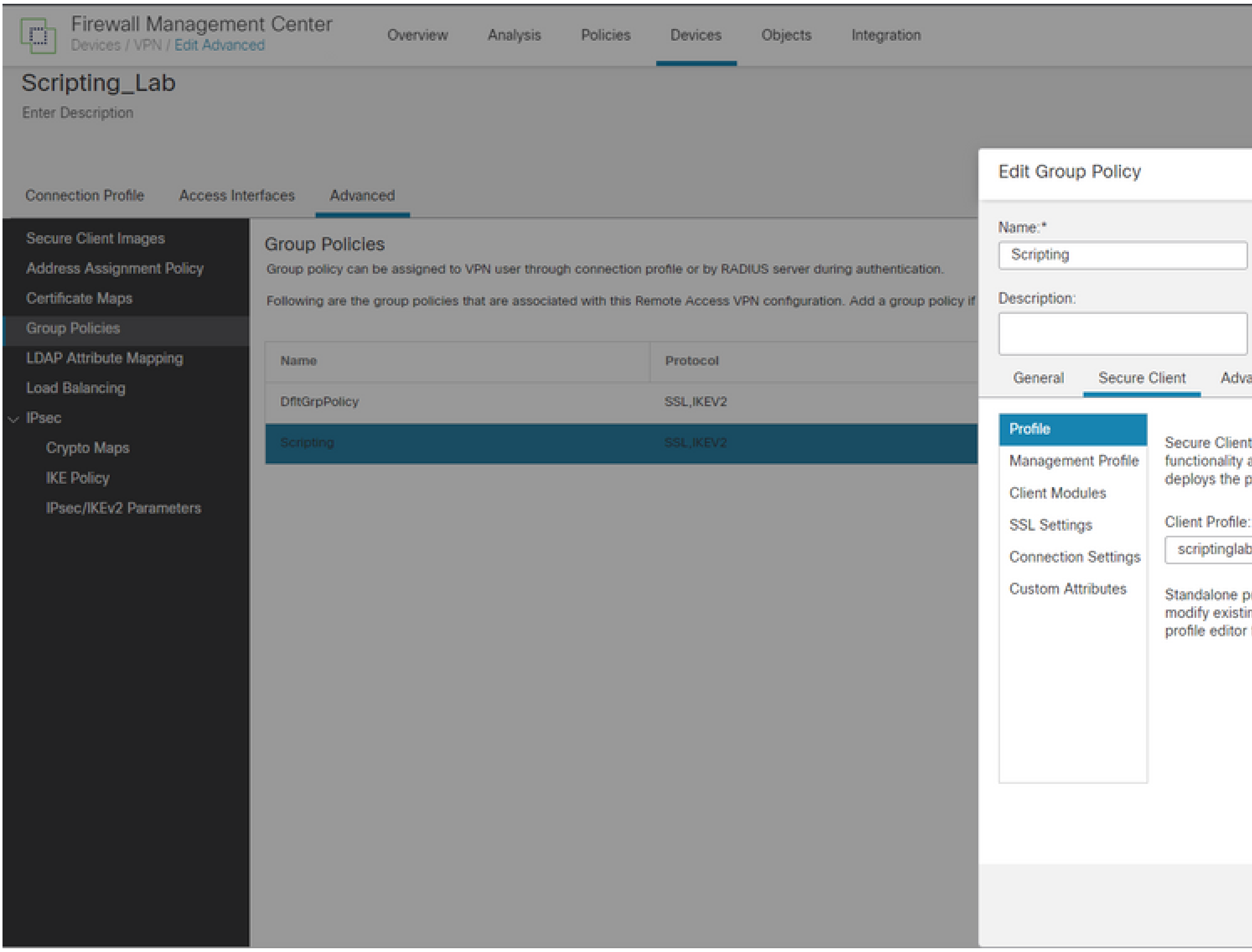
AnyConnect Scripting settings ASDM

Setting up Secure Client scripting with FTD managed by FMC

Currently setting up Secure Client scripting is not supported by the FMC, there is an enhancement request Cisco bug ID CSCvt58044 to support it. Based on that we have a workaround to allow the configuration and deploy of the scripts.

Step 1. Create a Secure Client Profile and Enable Scripting in Preferences (Part 2) with the VPN profile editor.

Devices> Remote Access> select the Connection Profile and Edit> Advanced> Group Policies> edit the Group Policy> Secure Client> Profile> you can select the profile if is already uploaded to the FMC or you can click the plus option and upload the profile from there.



Scripting_Lab

Enter Description

Group Policies

Group policy can be assigned to VPN user through connection profile or by RADIUS server during authentication.

Following are the group policies that are associated with this Remote Access VPN configuration. Add a group policy if

Name	Protocol
DfltGrpPolicy	SSL,IKEV2
Scripting	SSL,IKEV2

Name:* Scripting

Description:

Secure Client
functionality a
deploys the p

Client Profile: scriptinglab

Standalone p
modify existin
profile editor

FMC Group Policy Configuration

Verify

After connecting through the VPN you can confirm the script was sucessfully deployed by checking this path depending on the OS:

Microsoft Windows	%ALLUSERSPROFILE%\Cisco\Cisco Secure Client\VPN\Script
Linux (On Linux, assign execute permissions to the file for User, Group and Other.)	/opt/cisco/secureclient/vpn/script
macOS	/opt/cisco/secureclient/vpn/script

Troubleshoot

1. Make sure that the script has an `OnConnect` or `OnDisconnect`

prefix name, If you use ASDM version 6.3 or later, the Secure Firewall ASA adds the prefix scripts_ and the prefix OnConnect or OnDisconnect to your filename to identify the file as a script. When the client connects, the security appliance downloads the script to the proper target directory on the remote computer, removes the scripts_ prefix and leaves the OnConnect or OnDisconnect prefix. For example, if you import the script myscript.bat, the script appears on the security appliance as scripts_OnConnect_myscript.bat. On the remote computer, the script appears as OnConnect_myscript.bat.

2. Try running the script from the command line. The client cannot run the script if it cannot run from the command line. If the script fails to run on the command line, make sure the application that runs the script is installed, and try rewriting the script on that operating system.

3. Verify that there is only one OnConnect script and only one OnDisconnect script in the scripts directory on the VPN endpoint. If the client downloads an OnConnect script from the Secure Firewall ASA, then downloads a second OnConnect script with a different filename suffix for another Secure Firewall ASA, then the client can not run the script you intended to run. If the script path contains more than one OnConnect or OnDisconnect script, and you are using the Secure Firewall ASA to deploy scripts, then remove the contents of the scripts directory and re-establish a VPN session. If the script path contains more than one OnConnect or OnDisconnect script, and you are using the manual deployment method, then remove the unwanted scripts and re-establish a VPN session.

4. If the operating system is Linux or MacOS, make sure that the script file permissions are set to execute, if the permission is not set to execute you can run this command to make it is executable:

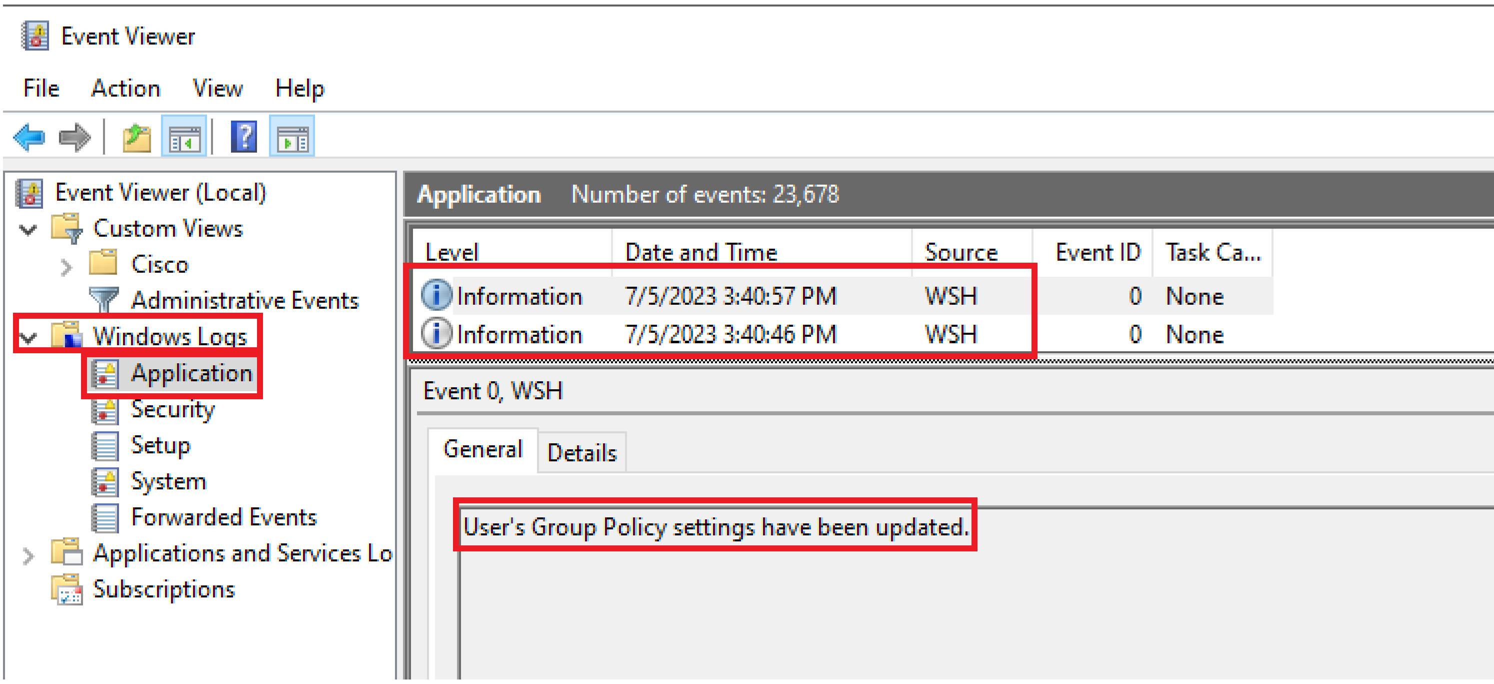
```
$ cd YourScriptDirectory
```

```
$ sudo chmod +755 <scriptname>
```

5. Make sure that the client profile has scripting enabled.

6. Depending on how you are writing your script you need to have an option to log the progress of the script, for example with the .vbs you can use objShell.LogEvent and then you can go to the event viewer of Windows and check if this worked or failed:

Using as an example the script example **Script to refresh a windows group policy**



Application Number of events: 23,678

Level	Date and Time	Source	Event ID	Task Ca...
Information	7/5/2023 3:40:57 PM	WSH	0	None
Information	7/5/2023 3:40:46 PM	WSH	0	None

Event 0, WSH

User's Group Policy settings have been updated.

Event Viewer Logs