

# 在FTD上配置由FMC管理的安全客户端证书身份验证

## 目录

---

### [简介](#)

### [先决条件](#)

#### [要求](#)

#### [使用的组件](#)

### [配置](#)

#### [网络图](#)

#### [配置](#)

##### [a.创建/导入用于服务器身份验证的证书](#)

##### [b.添加受信任/内部CA证书](#)

##### [c.配置VPN用户的地址池](#)

##### [d.上传安全客户端映像](#)

##### [e.创建和上传XML配置文件](#)

#### [远程访问VPN配置](#)

### [验证](#)

### [故障排除](#)

---

## 简介

本文档介绍在由Firepower管理中心(FMC)通过证书身份验证管理的Firepower威胁防御(FTD)上配置远程访问VPN的过程。

作者：Dolly Jain和Rishabh Aggarwal，思科TAC工程师。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- 手动证书注册和SSL基础知识
- FMC
- 远程访问VPN的基本身份验证知识
- 第三方证书颁发机构(CA)，如Entrust、Geotrust、GoDaddy、Thawte和VeriSign

### 使用的组件

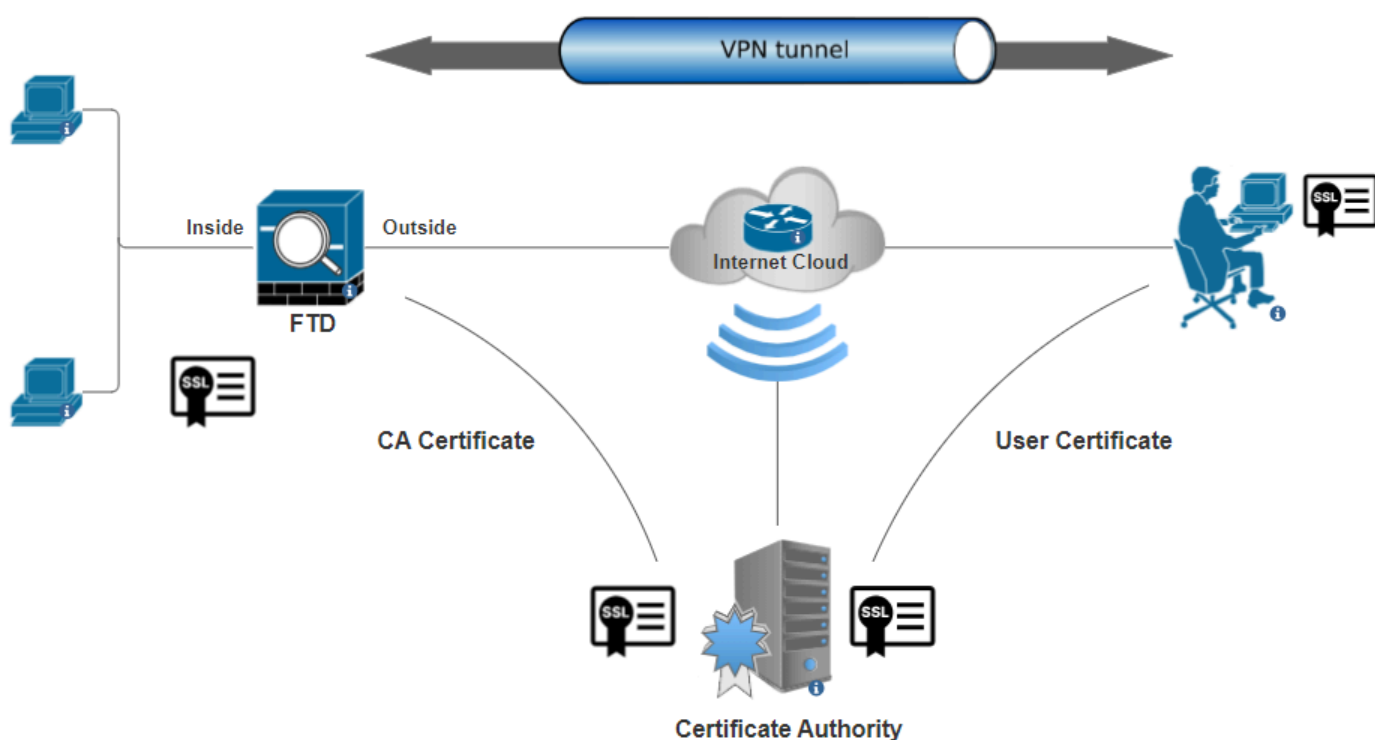
本文档中的信息基于以下软件版本：

- 安全Firepower威胁防御7.4.1版
- Firepower管理中心(FMC)版本7.4.1
- 安全客户端5.0.05040版
- Microsoft Windows Server 2019作为CA服务器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 配置

### 网络图



网络图

## 配置

a. 创建/导入用于服务器身份验证的证书



注意：在FMC上，需要先获取CA证书，然后才能生成CSR。如果从外部源（OpenSSL或第三方）生成CSR，则手动方法失败，必须使用PKCS12证书格式。

---

步骤1:导航到Devices > Certificates并单击Add。选择Device，然后单击Cert Enrollment下的加号(+)。

## 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

添加证书注册

第二步：在CA Information下，选择“Enrollment Type”作为Manual，并粘贴用于签署CSR的证书颁发机构(CA)证书。

## 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:

```
HQYDVQQDEZXIeWRyYRw50S
UQgU2VydmVyeLENBIE8xMIIBlj
ANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEA6
huZbDVWWMGj7XbFZQWI+uhh
0SleWhO8rI79MV4+7ZSj2
Lxos5e8za0H1JVVzTNPaup2G
o438C5zeaqaGtyUshV8D0xw
UiWyamspTao7PjjuC
h81+tp9z76rp1irjNMh5o/zeJ0
h3Kag5zQG9sfI7J7ihLnTFbArj
N7ID=ZeeQw
```

Validation Usage:



IPsec Client



SSL Client



SSL Server



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

Cancel

Save

添加认证中心信息

第三步：对于验证用法，选择IPsec Client, SSL Client和Skip Check for CA flag in basic constraints of the CA Certificate。

第四步：在Certificate Parameters下，填写主题名称详细信息。

## 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):

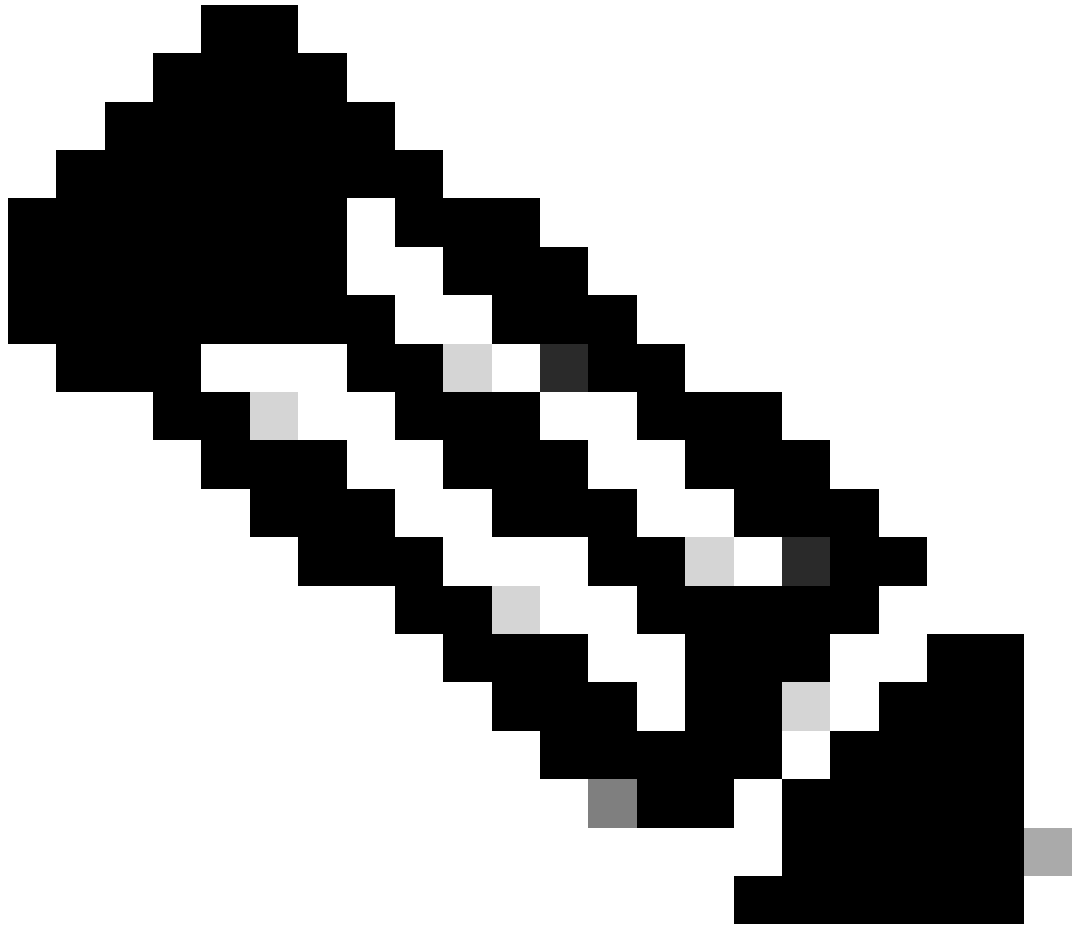
Include Device's Serial Number

Cancel

Save

添加证书参数

第五步：在Key下，选择密钥类型为RSA并具有密钥名称和大小。单击Save。



注意：对于RSA密钥类型，最小密钥大小为2048位。



## 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**

添加RSA密钥

第六步：在Cert Enrollment下，从刚创建的下拉列表中选择信任点，然后单击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\*:

 +

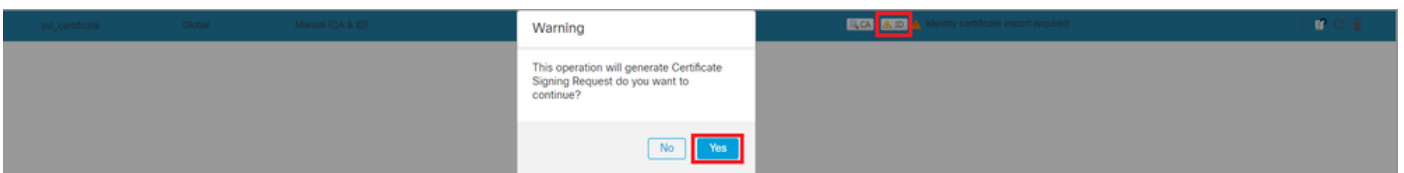
Cert Enrollment Details:

Name: ssl\_certificate  
Enrollment Type: Manual (CA & ID)  
Enrollment URL: N/A

添加新证书

步骤 7. 点击ID，然后点击Yes进一步的提示，生成CSR。



生成 CSR

步骤 8 复制CSR并由证书颁发机构对其进行签名。身份证书由CA颁发之后，请通过单击Browse Identity Certificate并单击Import导入它。

# 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/e3PDeee3eC57e+D3QhKQ9SC7um8ulwueF+70fKYe
```

## Step 2

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

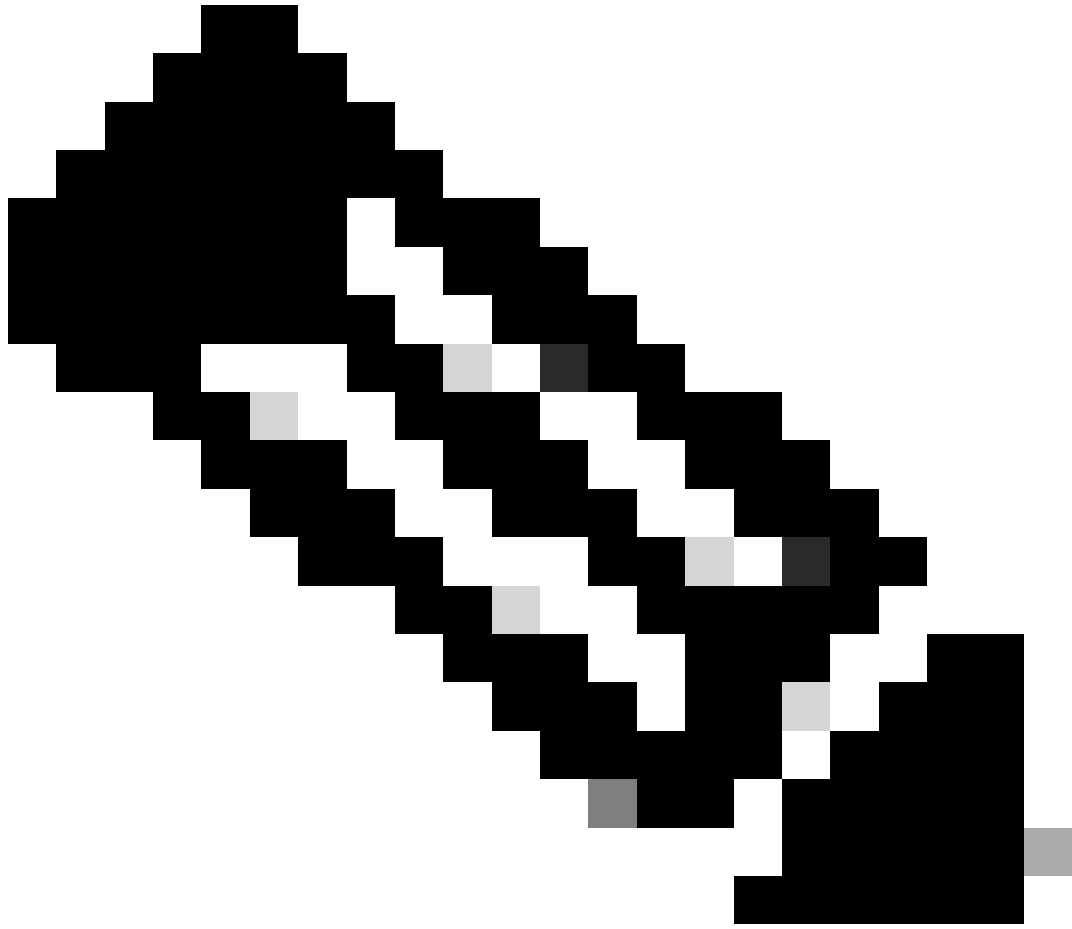
Identity Certificate File:

[Browse Identity Certificate](#)

[Cancel](#)

[Import](#)

导入ID证书



注意：如果ID证书的颁发需要时间，您可以在以后重复第7步。这将生成相同的CSR，我们可以导入ID证书。

---

#### b. 添加受信任/内部CA证书



**注意：**如果第(a)步“创建/导入用于服务器身份验证的证书”中使用的证书颁发机构(CA)也颁发用户证书，您可以跳过第(b)步，“添加受信任/内部CA证书”。无需再次添加相同的CA证书，也必须避免这种情况。如果再次添加同一CA证书，信任点配置为“validation-usage none”，这可能会影响RAVPN的证书身份验证。

---

步骤1:导航到Devices > Certificates，然后单击Add。

选择Device，然后单击Cert Enrollment下的加号(+)

此处，“auth-risagar-ca”用于颁发身份/用户证书。

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*

第二步：输入信任点名称，然后选择ManualCA information下的注册类型。

第三步：选中CA Only并粘贴pem格式的受信任/内部CA证书。

第四步：选中Skip Check for CA flag in basic constraints of the CA Certificate并单击Save。

### Add Cert Enrollment ?

Internal\_CA

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:

```
-----BEGIN CERTIFICATE-----  
--  
MIIG1jCCBL6gAwIBAgIQQAFu  
+wogXPrr4Y9x1zq7eDANBgk  
qhkiG9w0BAQsFADBK  
MQswCQYDVQQGEwJVUzES  
MBAGA1UEChMJSWRlbiRydX  
N0MScwJQYDVQQDEw5JZGV  
u  
VHJ1c3QgQ29tbWV5Y2lhbCB  
Sb290IENBIDUwHhcNMTkxMj
```

Validation Usage:  IPsec Client    SSL Client    SSL Server

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

Cancel   Save

添加信任点

第五步：在Cert Enrollment下方，从刚创建的下拉列表中选择信任点，然后单击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: Internal\_CA  
Enrollment Type: Manual (CA Only)  
Enrollment URL: N/A

Cancel

Add

添加内部Ca

第六步：之前添加的证书显示如下：

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

已添加证书

### c.配置VPN用户的地址池

步骤1:导航到Objects > Object Management > Address Pools > IPv4 Pools。

第二步：输入名称和带掩码的IPv4地址范围。

## 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

添加IPv4池

### d.上传安全客户端映像

步骤1:从[Cisco软件](#)站点按操作系统下载webdeploy安全客户端映像。

第二步：导航到Objects > Object Management > VPN > Secure Client File > Add Secure Client File。

第三步：输入名称，然后从磁盘中选择Secure Client文件。

第四步：将文件类型选择为Secure Client Image，然后单击Save。



# Edit Secure Client File



Name:\*

File Name:\*

File Type:\*

Description:

添加安全客户端映像

## e.创建和上传XML配置文件

步骤1:从[思科软件](#)站点下载并安装安全客户端Profile Editor。

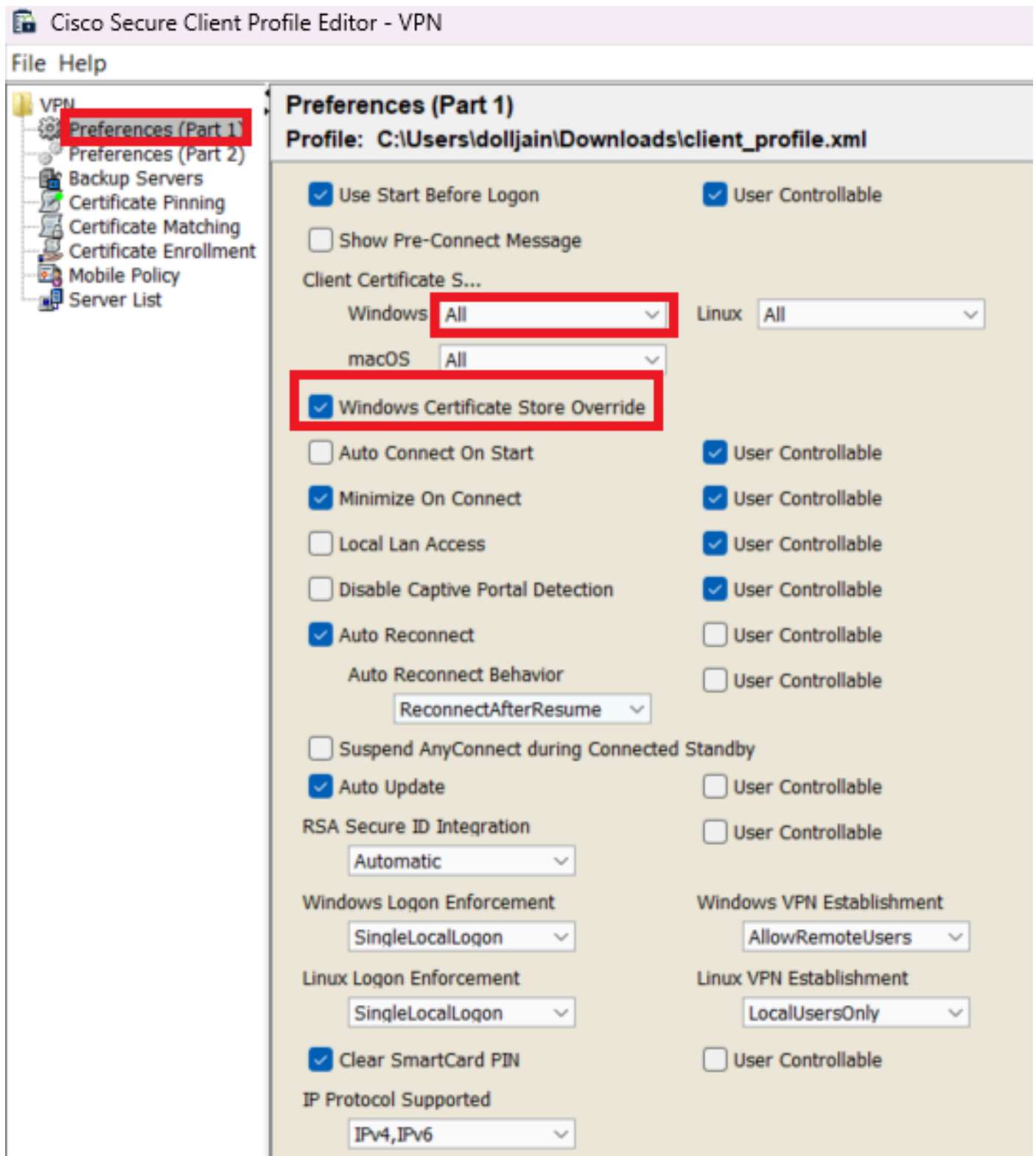
第二步：创建新配置文件并从Client Certificate Selection下拉列表中选择All。它主要控制Secure Client可以使用哪些证书存储区来存储和读取证书。

另外两个可用选项是：

- 计算机 - 安全客户端仅限于Windows本地计算机证书存储区中的证书查找。
- 用户 - 安全客户端仅限于在本地Windows用户证书存储区查找证书。

将“证书存储区覆盖”设置为True。

这允许管理员指示安全客户端使用Windows计算机（本地系统）证书存储中的证书进行客户端证书身份验证。证书存储区覆盖仅适用于SSL，默认情况下，UI进程在此启动连接。使用IPSec/IKEv2时，安全客户端配置文件中的此功能不适用。



添加首选项（第1部分）

第3步：（可选）取消选中Disable Automatic Certificate Selection，因为它会避免提示用户选择身份验证证书。

- 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

Disconnect

Untrusted Network Policy

Connect

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

Closed

Allow Captive Portal Remediation

Remediation Timeout (min.)

Apply Last VPN Local Resource Rules

Captive Portal Remediation Browser Failover

Allow Manual Host Input

PPP Exclusion

Disable

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

Same User Only

Authentication Timeout (seconds)

注意：安全客户端使用此ACL向内部资源添加安全路由。

第二步：导航到Devices > VPN > Remote Access，然后单击Add。

第三步：输入配置文件的名称，然后选择FTD设备并点击Next。

The screenshot shows the 'Remote Access VPN Policy Wizard' interface. At the top, there is a progress bar with five steps: 1. Policy Assignment, 2. Connection Profile, 3. Secure Client, 4. Access & Certificate, and 5. Summary. The current step is 'Targeted Devices and Protocols'. Below the progress bar, there is a section titled 'Targeted Devices and Protocols' with a sub-header 'Before You Start'. The main content area includes a 'Name:\*' field with 'RAVPN' entered and highlighted by a red box. Below it is a 'Description:' field. The 'VPN Protocols:' section has two checked options: 'SSL' and 'IPsec-IKEv2'. The 'Targeted Devices:' section is divided into 'Available Devices' and 'Selected Devices'. 'Available Devices' lists 'FTD-A-7.4.1', 'FTD-B-7.4.0', and 'FTD-ZTNA-7.4.1'. 'FTD-A-7.4.1' is selected and highlighted in blue. 'Selected Devices' shows 'FTD-A-7.4.1' with a trash icon. An 'Add' button is located between the two device lists. On the right side, there is a 'Before You Start' panel with instructions: 'Before you start, ensure the following configuration elements to be in place to complete Remote Access VPN Policy.' It lists '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.), and '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.).

添加配置文件名称

第四步：输入Connection Profile Name并在“Authentication，Authorization and Accounting (AAA)”下选择“Authentication Method”作为Client Certificate Only。

## 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:\*

**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:

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

Primary Field:

Secondary Field:

Authorization Server:  +  
(Realm or RADIUS)

Accounting Server:  +  
(RADIUS)

选择身份验证方法

第五步：点击Client Address Assignment下的Use IP Address Pools 并选择之前创建的IPv4地址池。


## 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:  

选择客户端地址分配

第六步：编辑组策略。

## 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](#)

编辑组策略

步骤 7. 导航到 General > Split Tunneling , 选择 Tunnel networks specified below 并在 Split Tunnel Network List Type 下选择 Standard Access List。

选择之前创建的 ACL。

## 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

添加拆分隧道

步骤 8 导航到 Secure Client > Profile (仅路由器), 选择 Client Profile (默认), 然后单击 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](#).

添加安全客户端配置文件

步骤 9 点击Next，然后选择Secure Client Image选项，再点击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

添加安全客户端映像

步骤 10 选择VPN访问的网络接口，选择Device Certificates并选中sysopt permit-vpn，然后单击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.*

为VPN流量添加访问控制

步骤 11最后，查看所有配置并单击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.

远程访问VPN策略配置

步骤 12完成远程访问VPN的初始设置后，编辑创建的连接配置文件并转到Aliases。

步骤 13通过点击加号图标(+)配置group-alias。


### 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:  
ssl-cert

Enabled

Cancel   OK

Cancel   Save

编辑组别名

步骤 14通过点击加号图标(+)配置group-url。使用之前在客户端配置文件中配置的不同组URL。

## 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 URL aliases. 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

编辑组URL

步骤 15 导航至 Access Interfaces。选择 SSL settings 下的 Interface Trustpoint 和 SSL Global Identity Certificate。

## 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

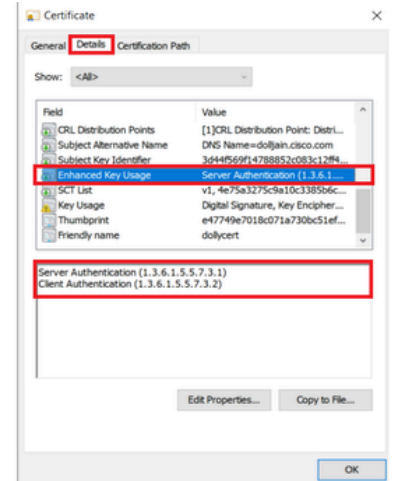
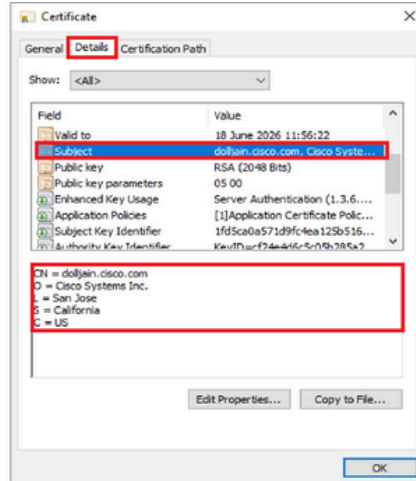
编辑访问接口

步骤 16 点击 Save，部署这些更改。

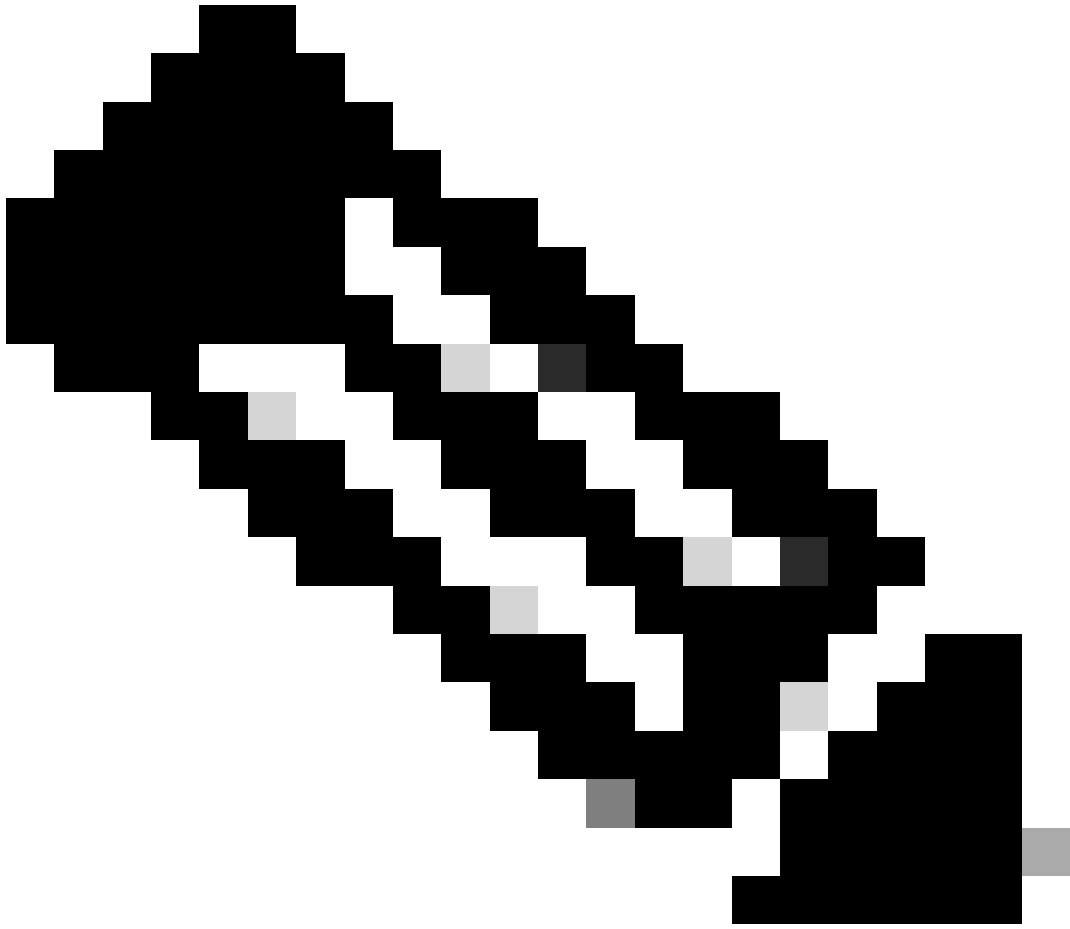
## 验证

使用本部分可确认配置能否正常运行。

1. 安全客户端 PC 必须在用户 PC 上安装带有有效日期、主题和 EKU 的证书。此证书必须由在 FTD 上安装证书的 CA 颁发，如前所示。此处，身份或用户证书由“auth-risaggar-ca”颁发。



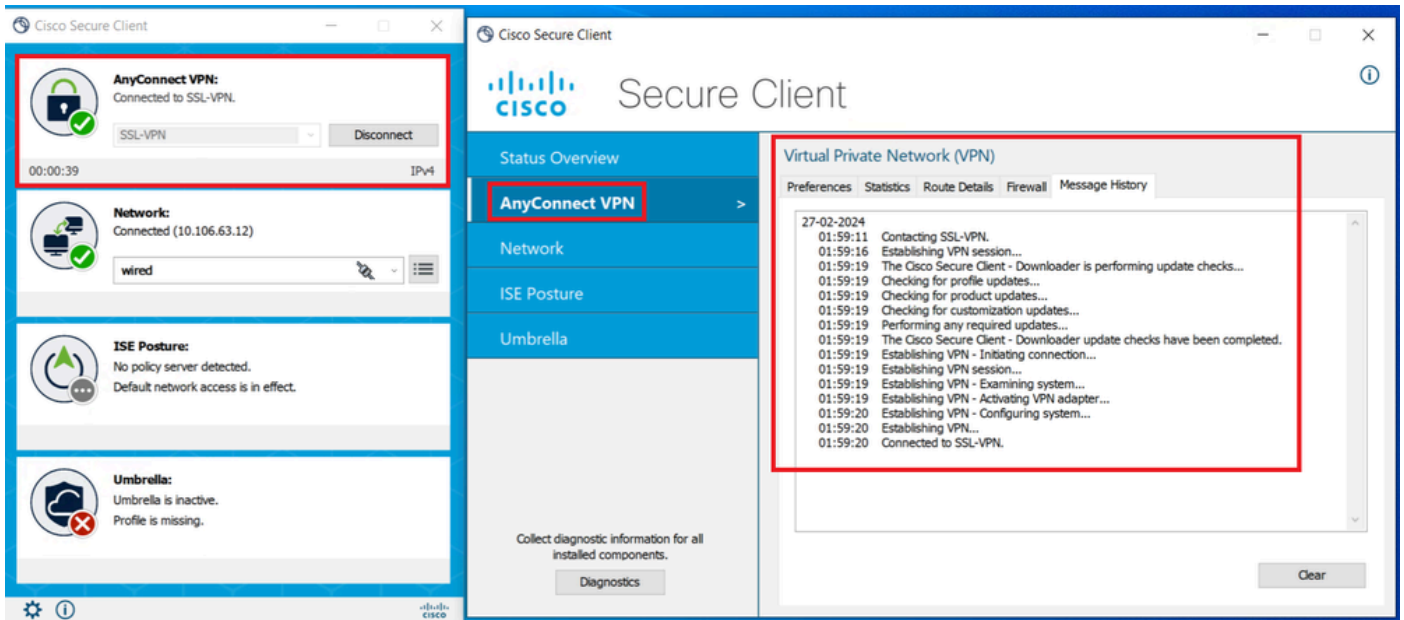
证书亮点



注意：客户端证书必须具有“客户端身份验证”(Client Authentication)增强型密钥使用(EKU)。

---

2. 安全客户端必须建立连接。



成功的安全客户端连接

3. 运行show vpn-sessiondb anyconnect以确认所用隧道组下活动用户的连接详细信息。

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

## 故障排除

本部分提供了可用于对配置进行故障排除的信息。

1. 可以从FTD的诊断CLI运行调试：

```
debug crypto ca 14
debug webvpn anyconnect 255
debug crypto ike-common 255
```

2. 有关常见问题，请参阅本[指南](#)。

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。