使用ISE終端安全評估將Duo SAML SSO與Anyconnect安全遠端訪問整合

目錄

簡介

本文檔介紹將Duo SAML SSO與利用思科ISE進行詳細狀態評估的自適應安全裝置(ASA)Cisco AnyConnect安全移動客戶端訪問相整合的配置示例。Duo SAML SSO使用Duo Access Gateway(DAG)實現，DAG與Active Directory通訊以進行初始使用者身份驗證，然後與Duo Security(Cloud)通訊以進行多重身份驗證。思科ISE用作授權伺服器，用於使用狀態評估提供終端驗證。

作者：Dinesh Moudgil和Pulkit Saxena，Cisco HTTS工程師。

必要條件

需求

本文檔假定ASA已完全正常運行並配置為允許Cisco Adaptive Security Device Manager(ASDM)或命令列介面(CLI)進行配置更改。

思科建議您瞭解以下主題：

- Duo Access Gateway和Duo Security的基礎知識
- ASA上遠端訪問VPN配置的基本知識
- ISE和狀態服務基礎知識

採用元件

本檔案中的資訊是根據以下軟體版本：

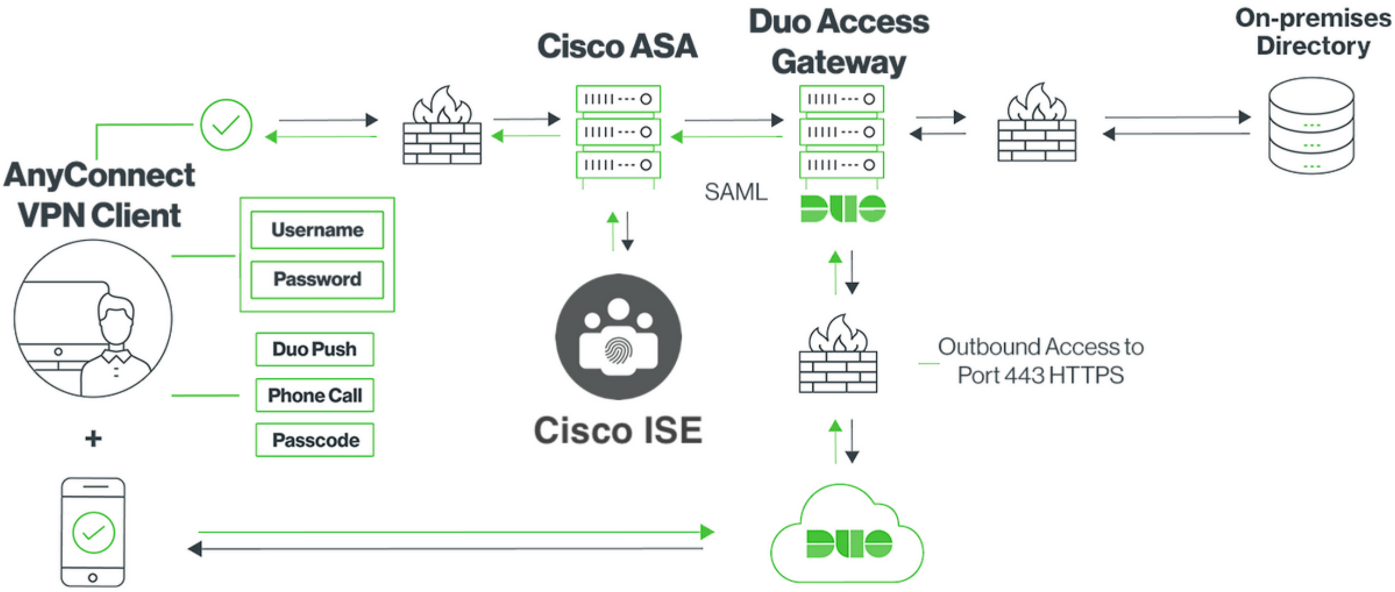
- 思科調適型安全裝置軟體版本9.12(3)12
- Duo Access Gateway
- Duo Security
- 思科身份服務引擎2.6版及更高版本
- Microsoft Windows 10與AnyConnect版本4.8.03052

> 註：此實施中使用的Anyconnect嵌入式瀏覽器要求每個版本在9.7(1)24、9.8(2)28、9.9(2)1或更高版本以及AnyConnect 4.6或更高版本上安裝ASA。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

網路圖表



流量

1. Anyconnect客戶端發起到Cisco ASA的SSL VPN連線

2. Cisco ASA配置為使用Duo Access Gateway(DAG)進行主要身份驗證，將Anyconnect客戶端中的嵌入式瀏覽器重定向到DAG進行SAML身份驗證

3. Anyconnect客戶端已重定向至Duo接入網關

4. AnyConnect客戶端輸入憑證後，會生成SAML身份驗證請求，並從Cisco ASA向Duo Access Gateway發出該請求

5. Duo Access Gateway利用與現場Active Directory的整合來執行Anyconnect客戶端的主要身份驗證

6. 主身份驗證成功後，Duo接入網關會通過TCP埠443向Duo Security傳送請求以開始雙因素身份驗證

7. AnyConnect客戶端已顯示「Duo Interactive Prompt」（Duo互動式提示），使用者使用他們的首選方法（推送或密碼）完成Duo二元身份驗證

8. Duo Security收到身份驗證響應並將資訊返回到Duo接入網關

9. Duo Access Gateway根據身份驗證響應構建SAML身份驗證響應，該響應包含SAML斷言並響應Anyconnect客戶端

10. Anyconnect客戶端成功通過Cisco ASA的SSL VPN連線進行身份驗證

11. 身份驗證成功後，Cisco ASA向Cisco ISE傳送授權請求

✎ 注意：思科ISE僅配置為授權，因為Duo訪問網關提供必需的身份驗證

12. 思科ISE處理授權請求，並且由於客戶端狀態狀態為未知，返回狀態重定向（通過思科ASA有限訪問Anyconnect客戶端）

13. 如果Anyconnect客戶端沒有合規性模組，系統會提示其下載以繼續進行狀態評估

14. 如果Anyconnect客戶端具有合規性模組，則會與Cisco ASA建立TLS連線，並啟動狀態流程

15. 根據ISE上配置的終端安全評估條件，終端安全評估檢查完成，詳細資訊從Anyconnect客戶端傳送到思科ISE

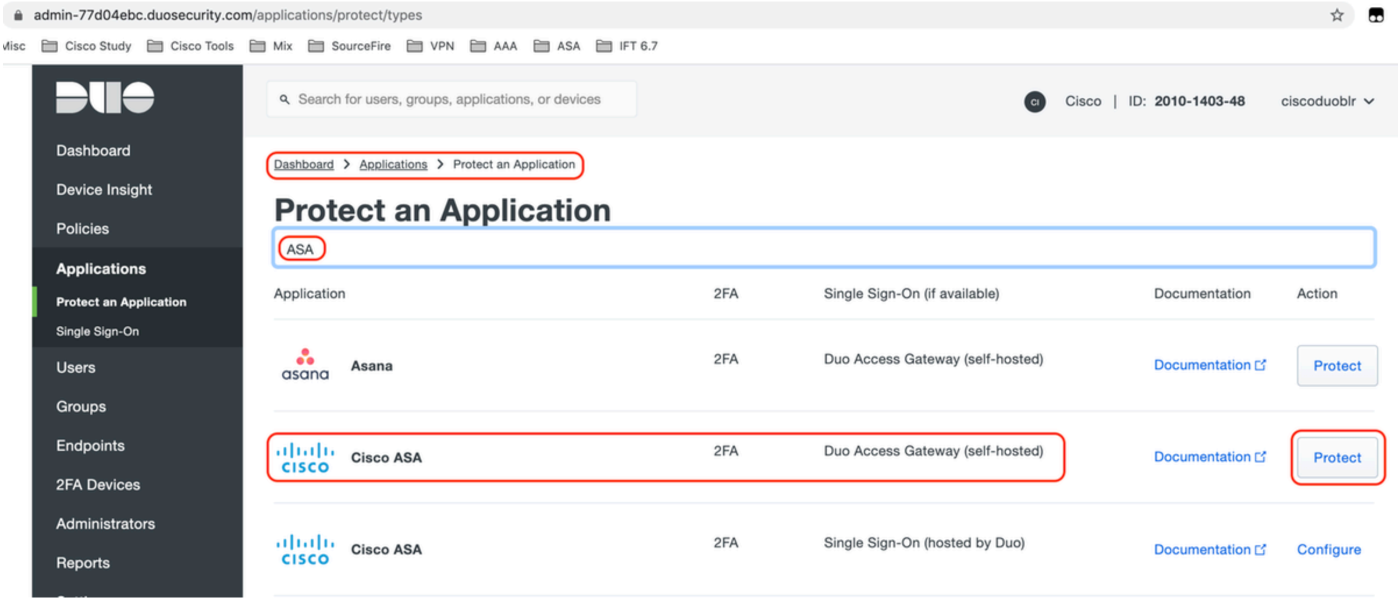
16. 如果客戶端狀態從Unknown更改為Compliant，則授權更改(CoA)請求會從Cisco ISE傳送到Cisco ASA以授予對客戶端的完全訪問許可權，並且VPN完全建立

組態

- Duo Admin Portal配置

在本節中，在Duo Admin Portal上配置ASA應用程式。

1.登入「Duo Admin Portal」並導航至「Applications > Protect an Application」，然後搜尋保護型別為「2FA with Duo Access Gateway， self-hosted」的「ASA」。按一下最右邊的「保護」以配置Cisco ASA



Protect an Application

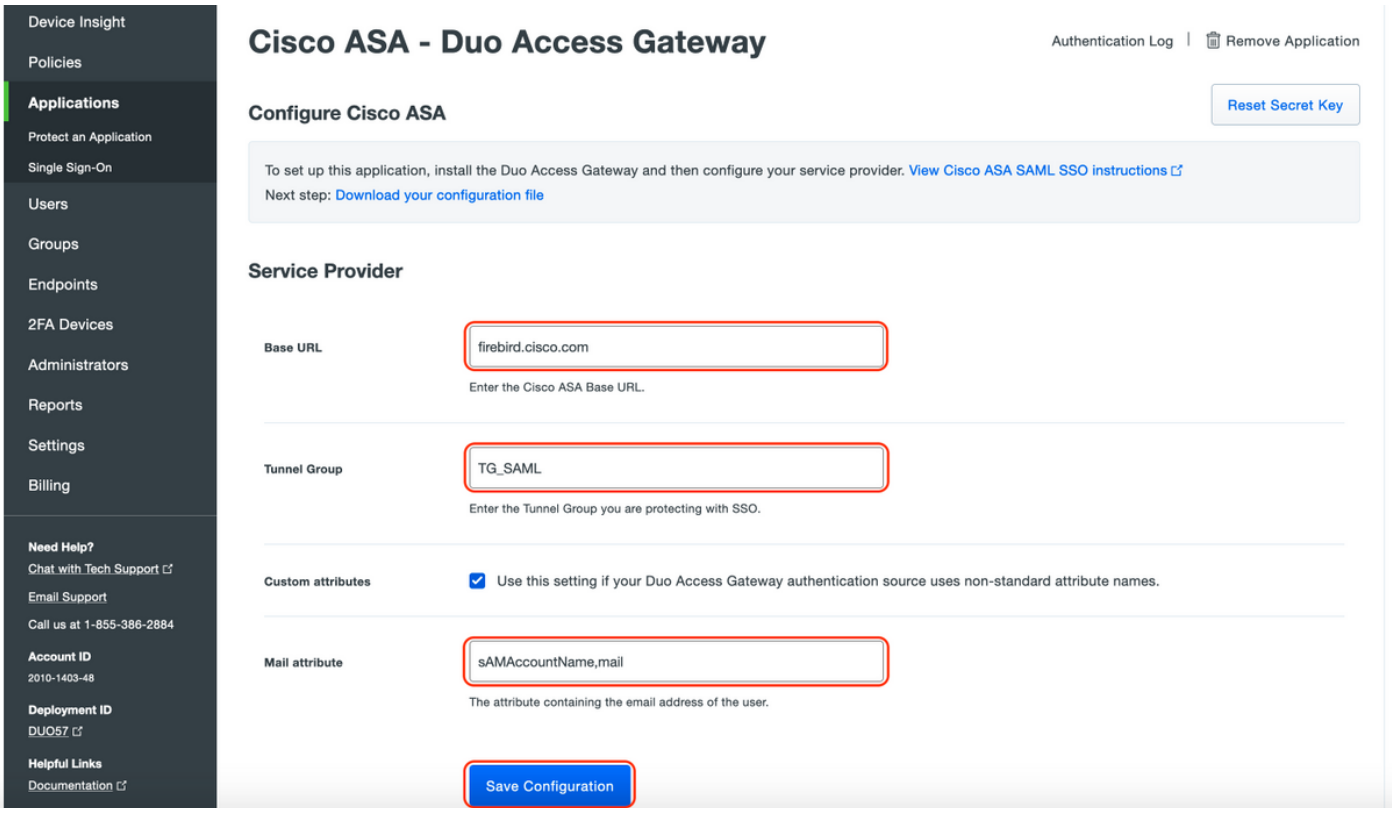
ASA

Application	2FA	Single Sign-On (if available)	Documentation	Action
Asana	2FA	Duo Access Gateway (self-hosted)	Documentation	Protect
Cisco ASA	2FA	Duo Access Gateway (self-hosted)	Documentation	Protect
Cisco ASA	2FA	Single Sign-On (hosted by Duo)	Documentation	Configure

2.為受保護的應用程式ASA在「服務提供商」下配置以下屬性

基本URL	firebird.cisco.com
通道組	TG_SAML
郵件屬性	sAMAccountName，mail

按一下頁面底部的「Save（儲存）」



Cisco ASA - Duo Access Gateway

Configure Cisco ASA

To set up this application, install the Duo Access Gateway and then configure your service provider. View Cisco ASA SAML SSO instructions
Next step: Download your configuration file

Service Provider

Base URL: firebird.cisco.com
Enter the Cisco ASA Base URL.

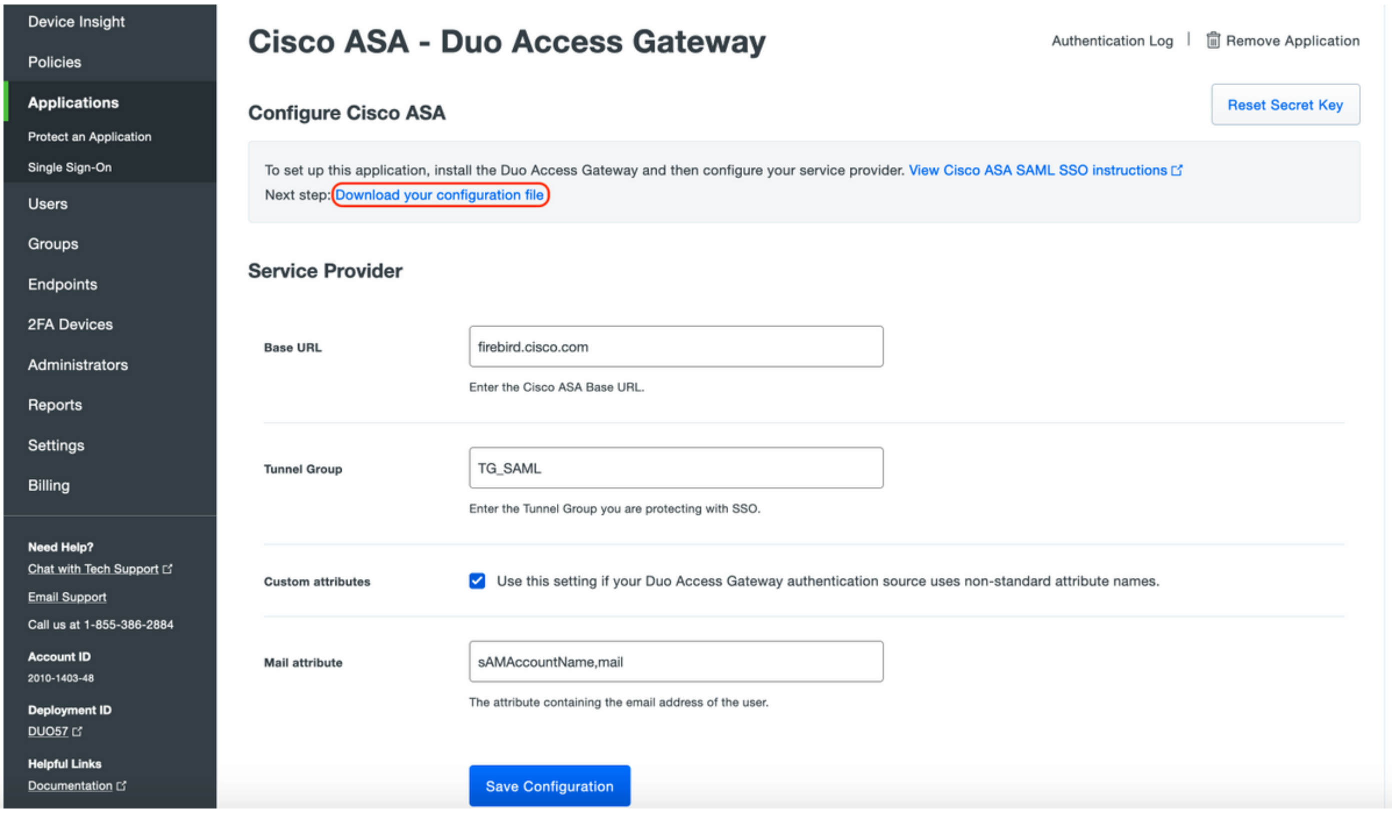
Tunnel Group: TG_SAML
Enter the Tunnel Group you are protecting with SSO.

Custom attributes: ☑ Use this setting if your Duo Access Gateway authentication source uses non-standard attribute names.

Mail attribute: sAMAccountName,mail
The attribute containing the email address of the user.

在本文檔中，其餘配置使用預設引數，但可以根據客戶要求進行設定。
此時可以為新SAML應用程式調整其他設定，例如從預設值更改應用程式名稱、啟用自助服務或分配組策略。

3.按一下「下載配置檔案」連結以獲取Cisco ASA應用程式設定（作為JSON檔案）。在後續步驟中，此檔案將被上傳到Duo Access Gateway



Cisco ASA - Duo Access Gateway

Configure Cisco ASA

To set up this application, install the Duo Access Gateway and then configure your service provider. View Cisco ASA SAML SSO instructions
Next step: Download your configuration file

Service Provider

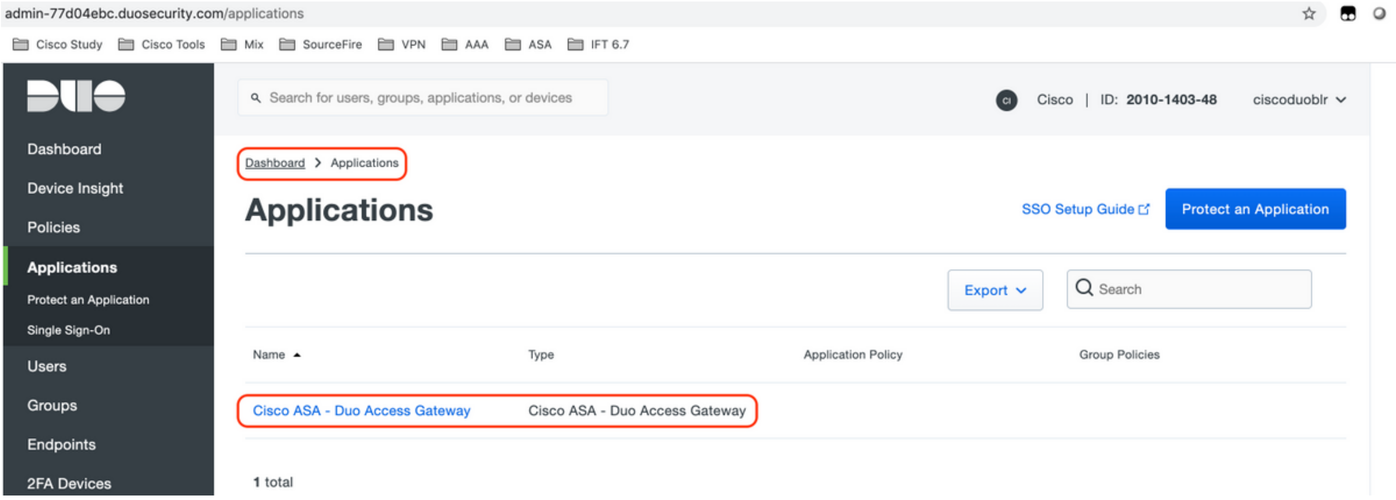
Base URL: firebird.cisco.com
Enter the Cisco ASA Base URL.

Tunnel Group: TG_SAML
Enter the Tunnel Group you are protecting with SSO.

Custom attributes: ☑ Use this setting if your Duo Access Gateway authentication source uses non-standard attribute names.

Mail attribute: sAMAccountName,mail
The attribute containing the email address of the user.

4.在「Dashboard > Applications」下，新建立的ASA應用程式如下圖所示：



Dashboard > Applications

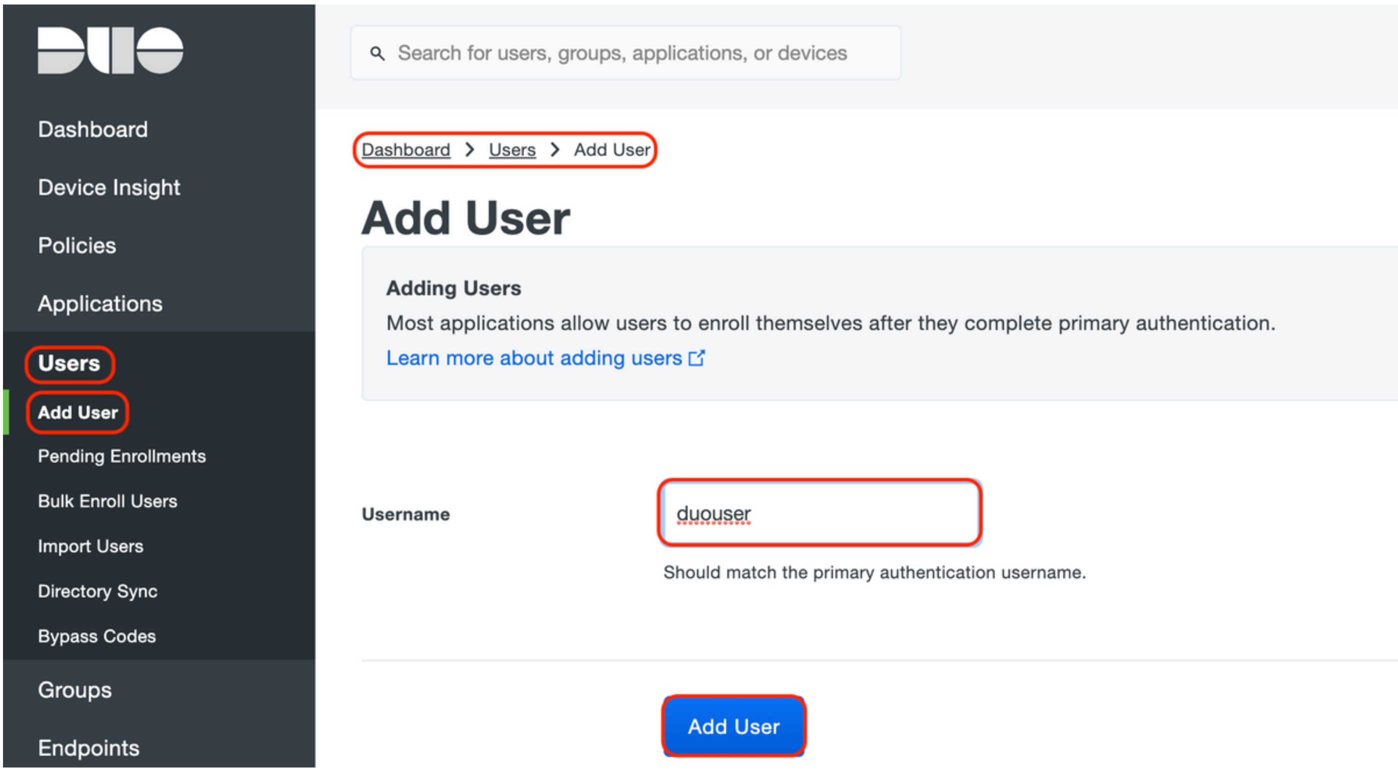
Applications

Name ▲	Type	Application Policy	Group Policies
Cisco ASA - Duo Access Gateway	Cisco ASA - Duo Access Gateway		

1 total

5.導覽至「Users > Add User」，如下圖所示：

建立一個名為「duouser」的使用者用於Anyconnect遠端訪問身份驗證，並在終端使用者裝置上啟用Duo Mobile



Dashboard > Users > Add User

Add User

Adding Users

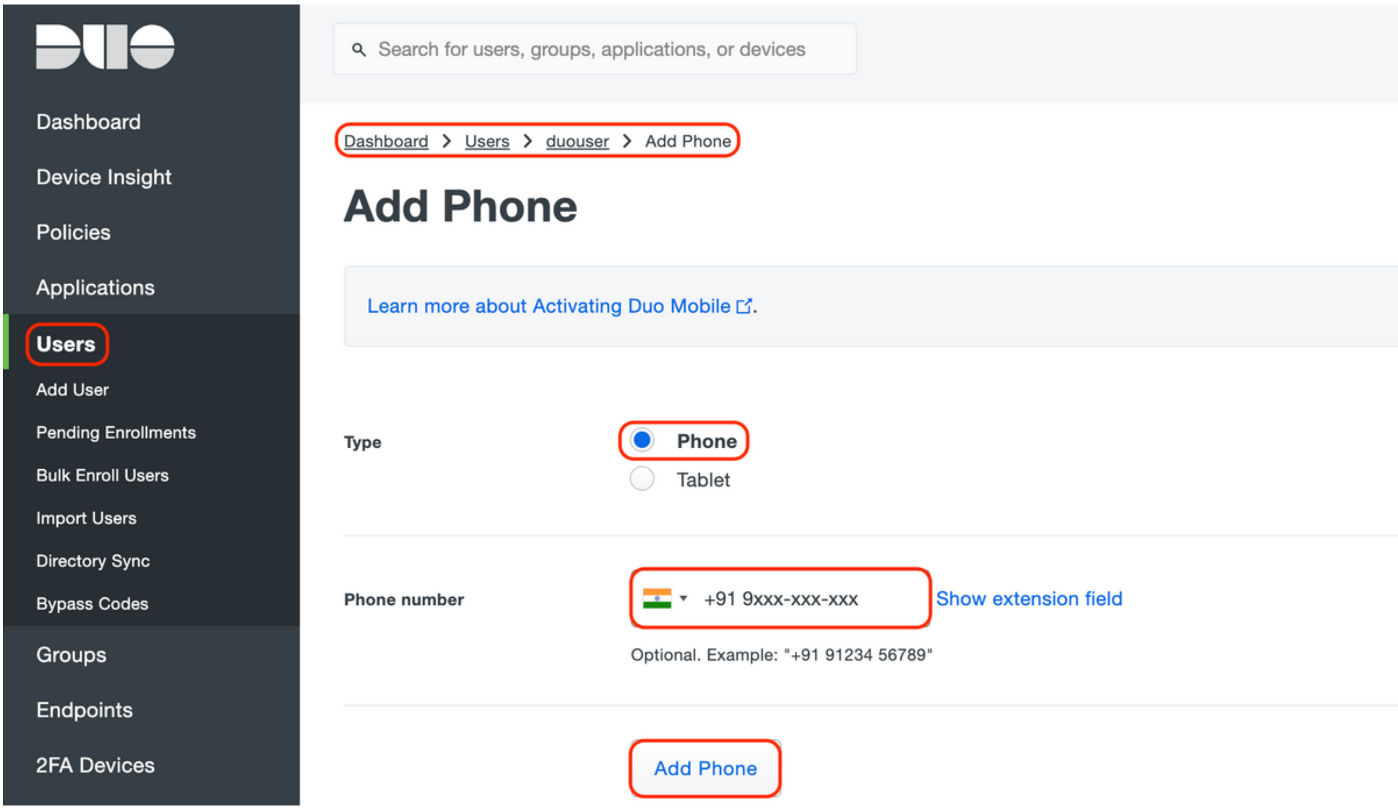
Most applications allow users to enroll themselves after they complete primary authentication.

Learn more about adding users

Username: duouser

Should match the primary authentication username.

要新增電話號碼（如圖所示），請選擇「Add Phone」選項。



Search for users, groups, applications, or devices

Dashboard > Users > duouser > Add Phone

Add Phone

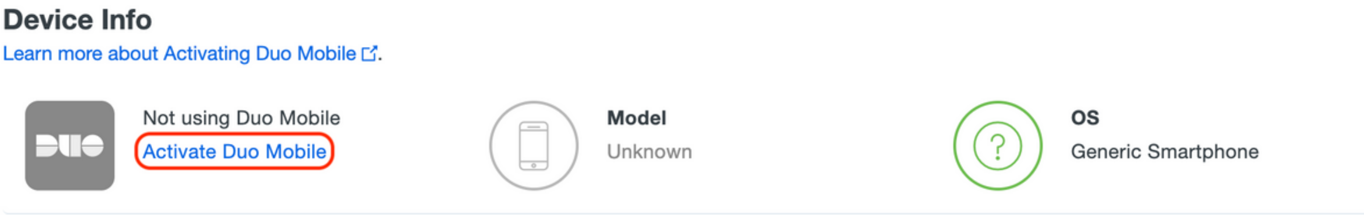
Learn more about Activating Duo Mobile.

Type: ● Phone ○ Tablet

Phone number: +91 9xxx-xxx-xxx Show extension field

Optional. Example: "+91 91234 56789"

為特定使用者啟用「Duo Mobile」



Device Info

Learn more about Activating Duo Mobile.

Not using Duo Mobile

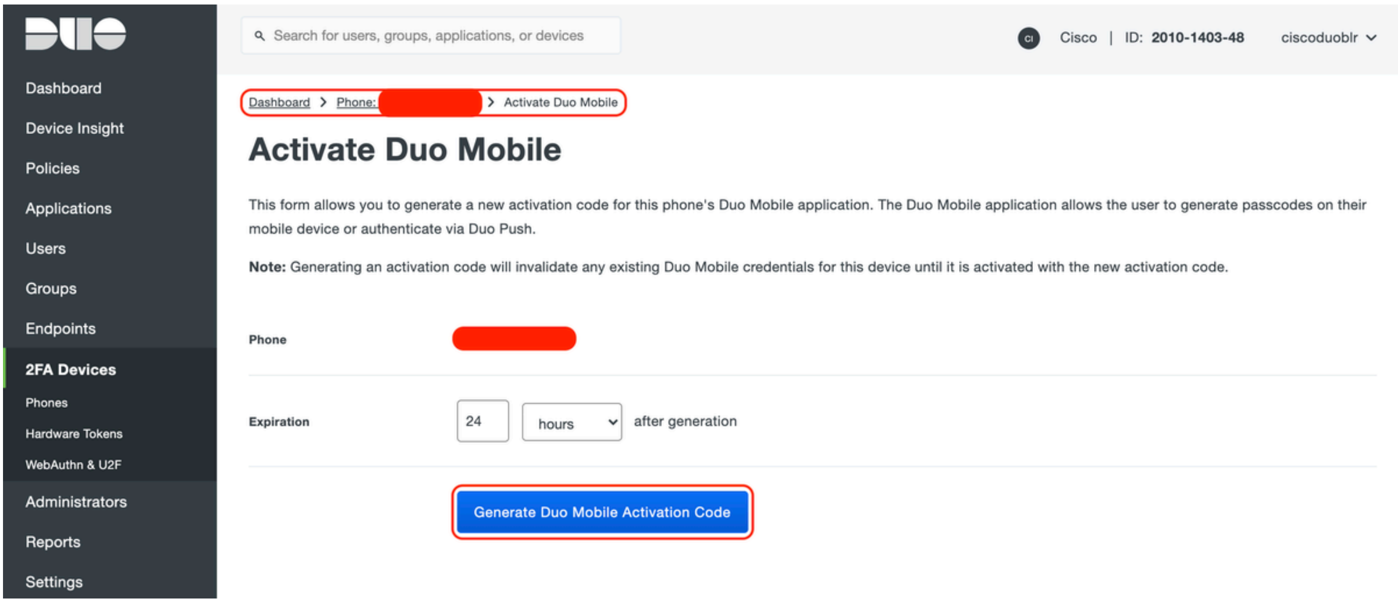
Activate Duo Mobile

Model: Unknown

OS: Generic Smartphone

註：確保在終端使用者裝置上安裝「Duo Mobile」。
[手動安裝用於IOS裝置的Duo應用程式]
[手動安裝用於Android裝置的Duo應用程式]

選擇「Generate Duo Mobile Activation Code」，如下圖所示：



Dashboard > Phone: [redacted] > Activate Duo Mobile

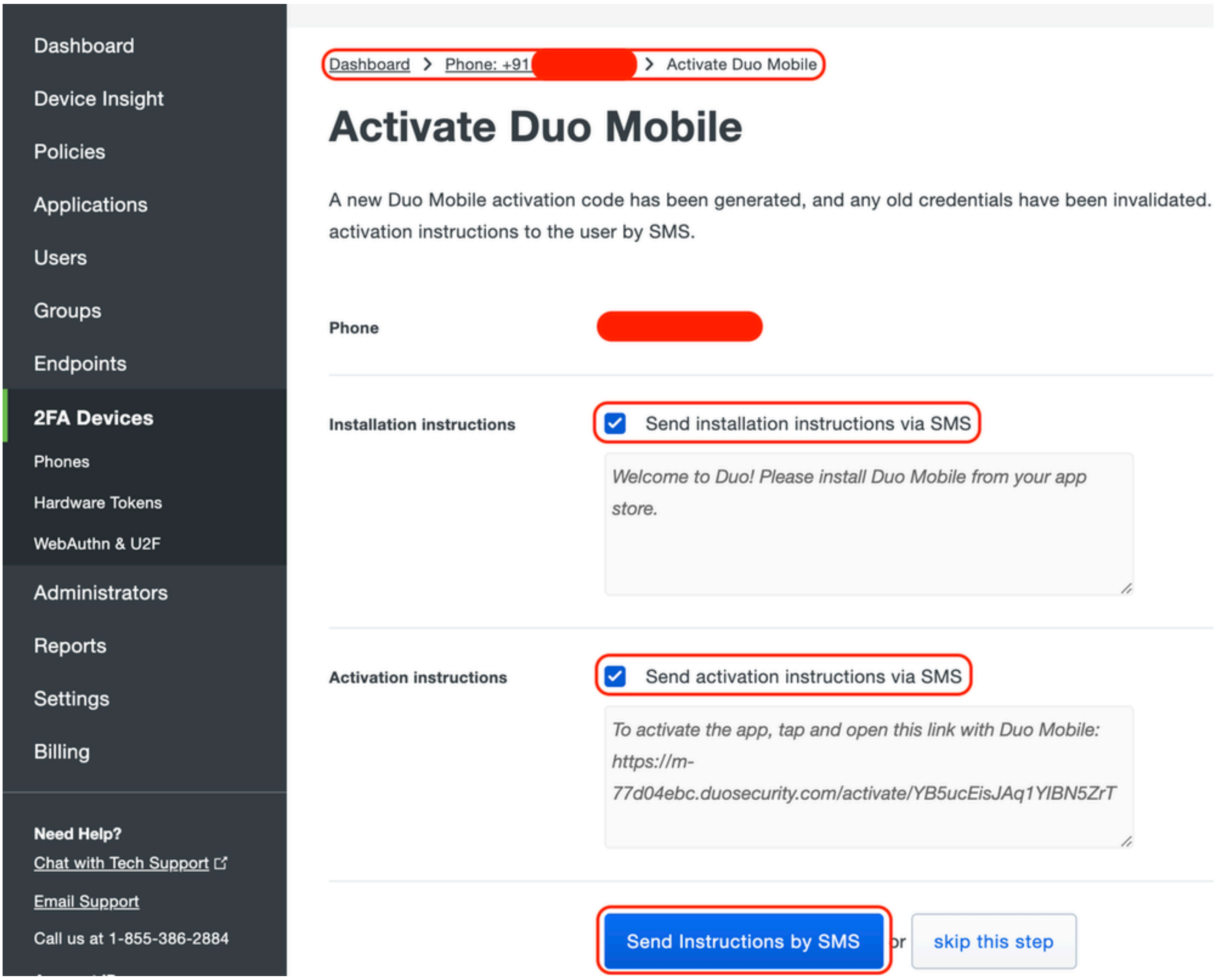
Activate Duo Mobile

This form allows you to generate a new activation code for this phone's Duo Mobile application. The Duo Mobile application allows the user to generate passcodes on their mobile device or authenticate via Duo Push.

Note: Generating an activation code will invalidate any existing Duo Mobile credentials for this device until it is activated with the new activation code.

Phone	[redacted]
Expiration	24 hours after generation

選擇「Send Instructions by SMS」（通過SMS傳送說明），如下圖所示：



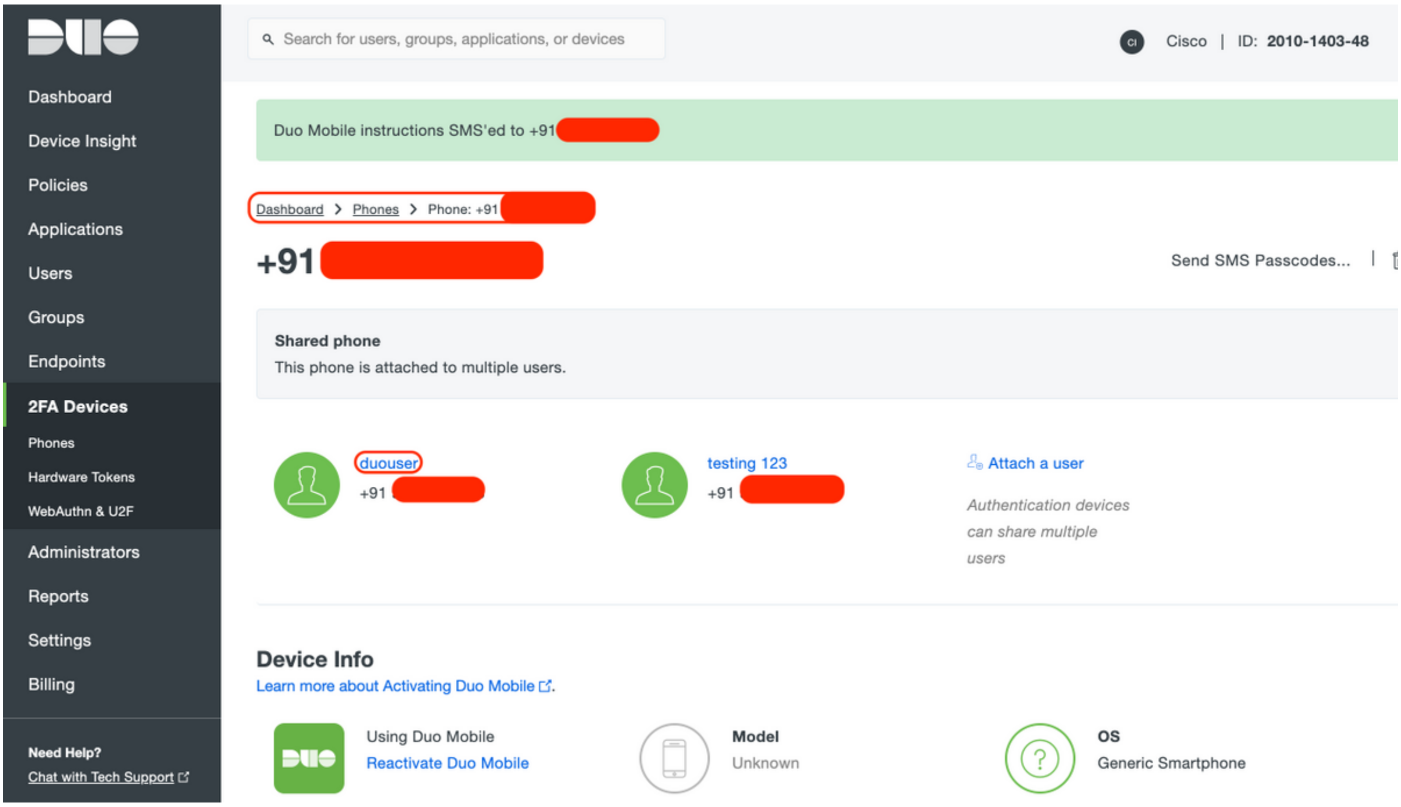
Dashboard > Phone: +91[redacted] > Activate Duo Mobile

Activate Duo Mobile

A new Duo Mobile activation code has been generated, and any old credentials have been invalidated. activation instructions to the user by SMS.

Phone	[redacted]
Installation instructions	☑ Send installation instructions via SMS *Welcome to Duo! Please install Duo Mobile from your app store.*
Activation instructions	☑ Send activation instructions via SMS *To activate the app, tap and open this link with Duo Mobile: https://m-77d04ebc.duosecurity.com/activate/YB5ucEisJAq1YIBN5ZrT*

點選SMS中的連結，Duo應用將連結到「裝置資訊」部分中的使用者帳戶，如下圖所示：



Duo Mobile instructions SMS'ed to +91[redacted]

Dashboard > Phones > Phone: +91[redacted]

+91[redacted]

Shared phone
This phone is attached to multiple users.

duouser
+91[redacted]

testing 123
+91[redacted]

Authentication devices can share multiple users

Device Info
Learn more about Activating Duo Mobile.

Using Duo Mobile

Model
Unknown

OS
Generic Smartphone

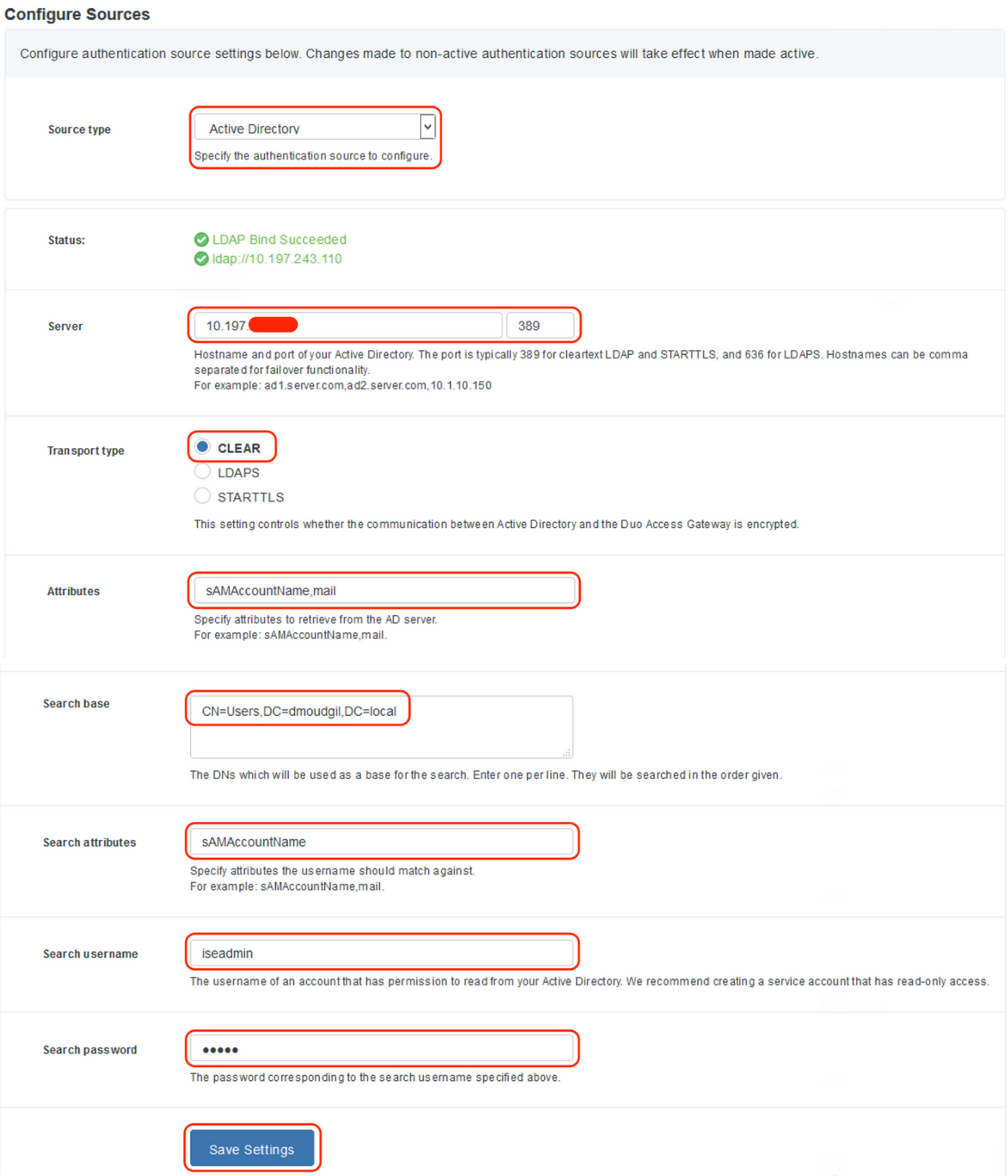
- Duo Access Gateway(DAG)配置

1. 在網路中的伺服器上部署Duo Access Gateway(DAG)

> 注意：請按照以下文檔進行部署：
>
> Linux版Duo存取閘道
> https://duo.com/docs/dag-linux
>
> 適用於Windows的Duo存取閘道
> https://duo.com/docs/dag-windows

2. 在Duo Access Gateway首頁上，導航至「Authentication Source」

3. 在「Configure Sources」下，輸入您的Active Directory的以下屬性，然後按一下「Save Settings」



Configure Sources

Configure authentication source settings below. Changes made to non-active authentication sources will take effect when made active.

Source type: Active Directory
Specify the authentication source to configure.

Status:
✓ LDAP Bind Succeeded
✓ ldap://10.197.243.110

Server: 10.197.[redacted] 389
Hostname and port of your Active Directory. The port is typically 389 for cleartext LDAP and STARTTLS, and 636 for LDAPS. Hostnames can be comma separated for failover functionality.
For example: ad1.server.com,ad2.server.com,10.1.10.150

Transport type:
● CLEAR
○ LDAPS
○ STARTTLS
This setting controls whether the communication between Active Directory and the Duo Access Gateway is encrypted.

Attributes: sAMAccountName,mail
Specify attributes to retrieve from the AD server.
For example: sAMAccountName,mail.

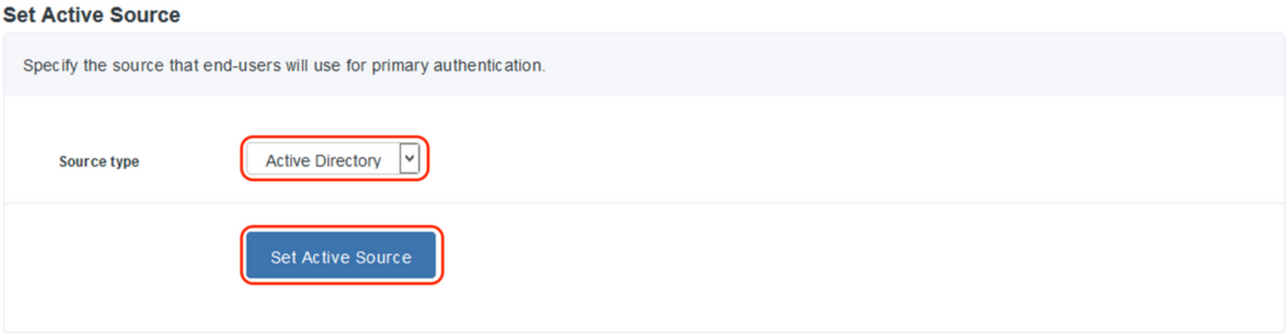
Search base: CN=Users,DC=dmoudgil,DC=local
The DNs which will be used as a base for the search. Enter one per line. They will be searched in the order given.

Search attributes: sAMAccountName
Specify attributes the username should match against.
For example: sAMAccountName,mail.

Search username: iseadmin
The username of an account that has permission to read from your Active Directory. We recommend creating a service account that has read-only access.

Search password: •••••
The password corresponding to the search username specified above.

4. 在「Set Active Source」下，選擇源型別為「Active Directory」，然後按一下「Set Active Source」

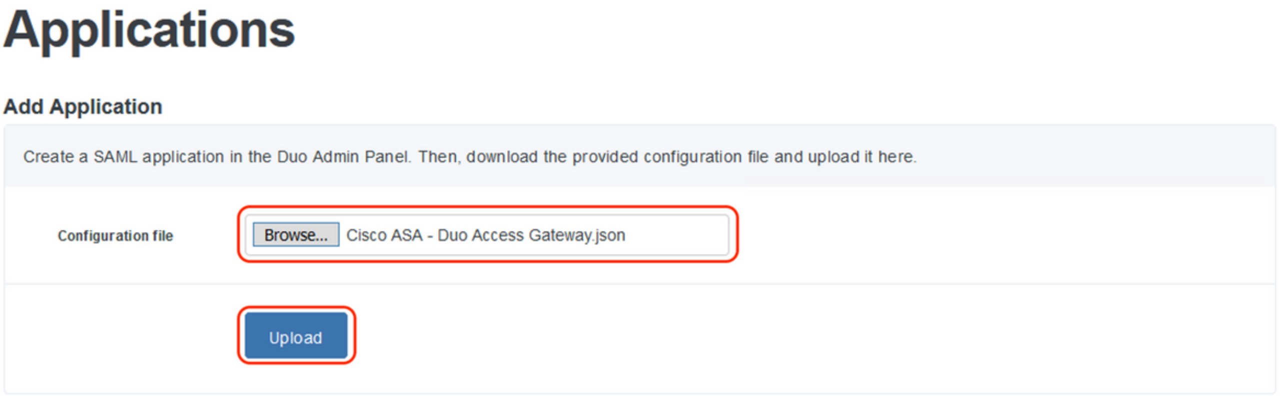


Set Active Source

Specify the source that end-users will use for primary authentication.

Source type: Active Directory

5. 導航至「Applications」，在「Add Application」子選單下上傳從「Configuration file」部分的Duo Admin Console下載的.json檔案。相應的.json檔案已在步驟3的Duo Admin Portal Configuration下下載



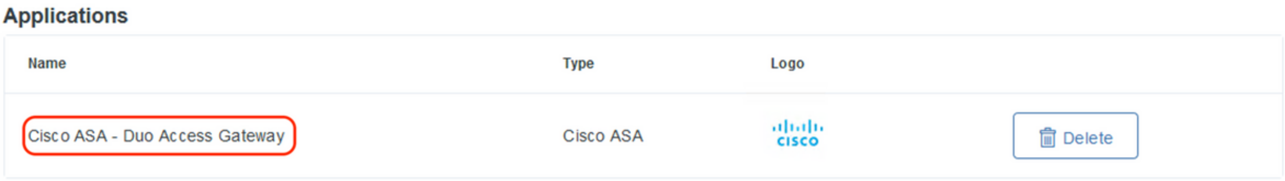
Applications

Add Application

Create a SAML application in the Duo Admin Panel. Then, download the provided configuration file and upload it here.

Configuration file: Browse... Cisco ASA - Duo Access Gateway.json

6. 成功新增應用程式後，該應用程式將顯示在「應用程式」子選單下

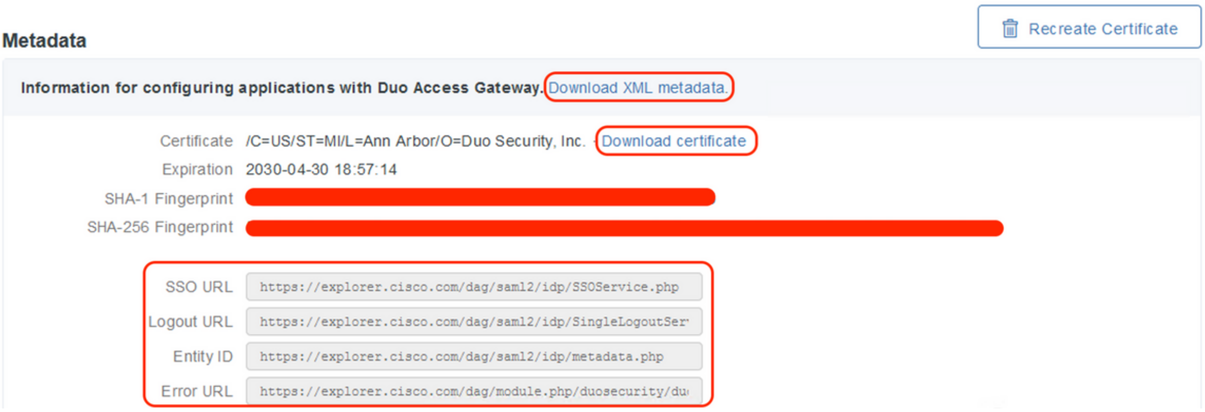


Applications

Name	Type	Logo	
Cisco ASA - Duo Access Gateway	Cisco ASA	cisco	Delete

7. 在「後設資料」子選單下，下載XML後設資料和IdP證書，並記下隨後在ASA上配置的以下URL

   1. SSO URL
   2. 註銷URL
   3. 實體Id
   4. 錯誤Url



Metadata

Recreate Certificate

Information for configuring applications with Duo Access Gateway. Download XML metadata.

Certificate /C=US/ST=MI/L=Ann Arbor/O=Duo Security, Inc. Download certificate

Expiration 2030-04-30 18:57:14

SHA-1 Fingerprint [redacted]

SHA-256 Fingerprint [redacted]

SSO URL https://explorer.cisco.com/dag/saml2/idp/SSOService.php

Logout URL https://explorer.cisco.com/dag/saml2/idp/SingleLogoutSer

Entity ID https://explorer.cisco.com/dag/saml2/idp/metadata.php

Error URL https://explorer.cisco.com/dag/module.php/duosecurity/du

- ASA配置

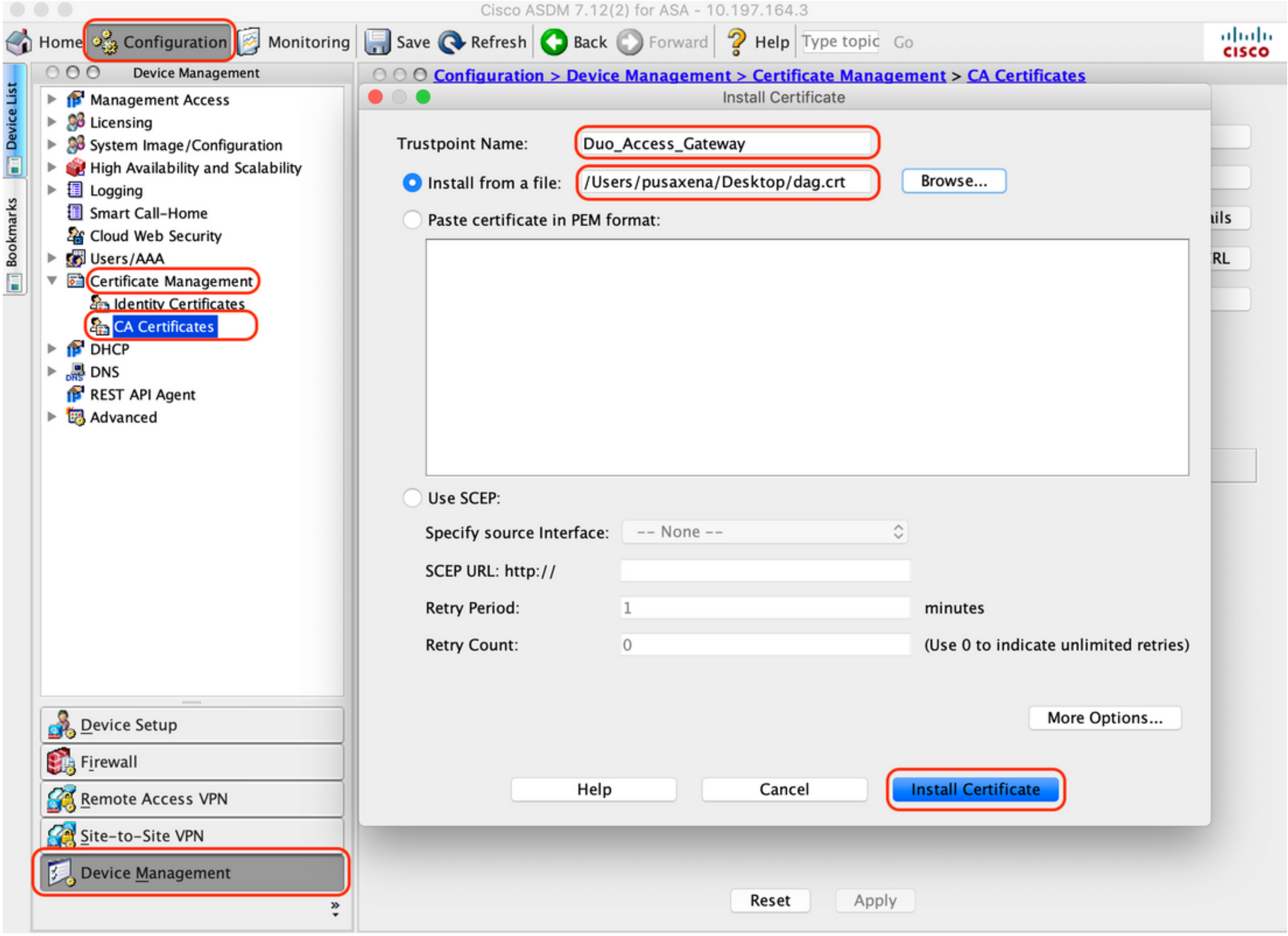
本節提供有關配置ASA以進行SAML IDP身份驗證和基本AnyConnect配置的資訊。本文檔提供了ASDM配置步驟和CLI運行配置以供概述。

1.上傳Duo接入網關證書

A.導航到「Configuration > Device Management > Certificate Management > CA Certificates」，然後按一下「Add」

B.在「Install Certificate Page」上，配置信任點名稱：Duo_Access_Gateway

C.按一下「瀏覽」選擇與DAG證書關聯的路徑，選擇後，按一下「安裝證書」



Trustpoint Name: Duo_Access_Gateway

● Install from a file: /Users/pusaxena/Desktop/dag.crt

○ Paste certificate in PEM format:

○ Use SCEP:

Specify source Interface: -- None --

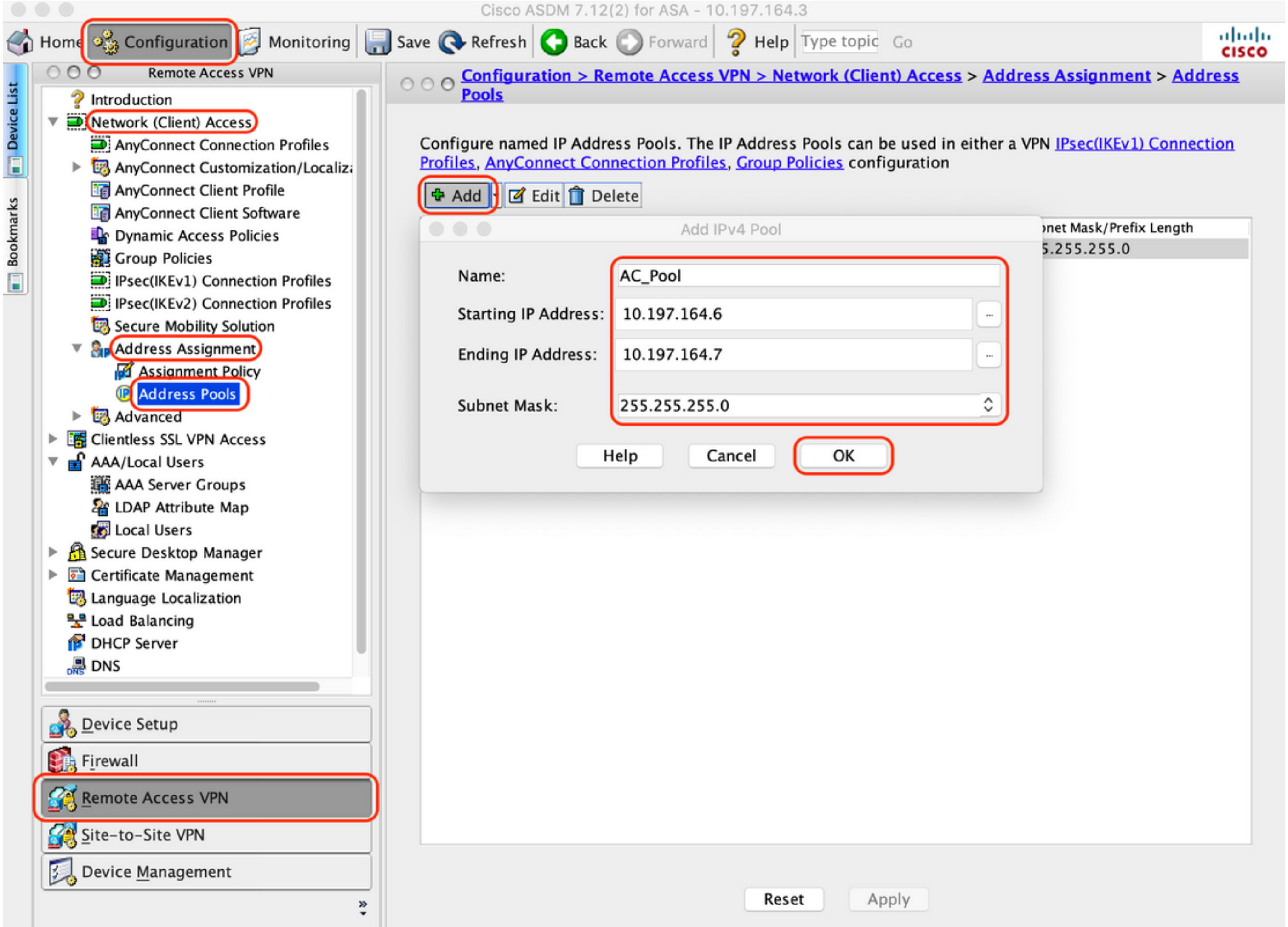
SCEP URL: http://

Retry Period: 1 minutes

Retry Count: 0 (Use 0 to indicate unlimited retries)

2.為AnyConnect使用者建立IP本地池

導航到「Configuration > Remote Access VPN > Network(Client)Access > Address Assignment > Address Pools」，按一下「Add」



Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools

Configure named IP Address Pools. The IP Address Pools can be used in either a VPN IPsec(IKEv1) Connection Profiles, AnyConnect Connection Profiles, Group Policies configuration

Name: AC_Pool

Starting IP Address: 10.197.164.6

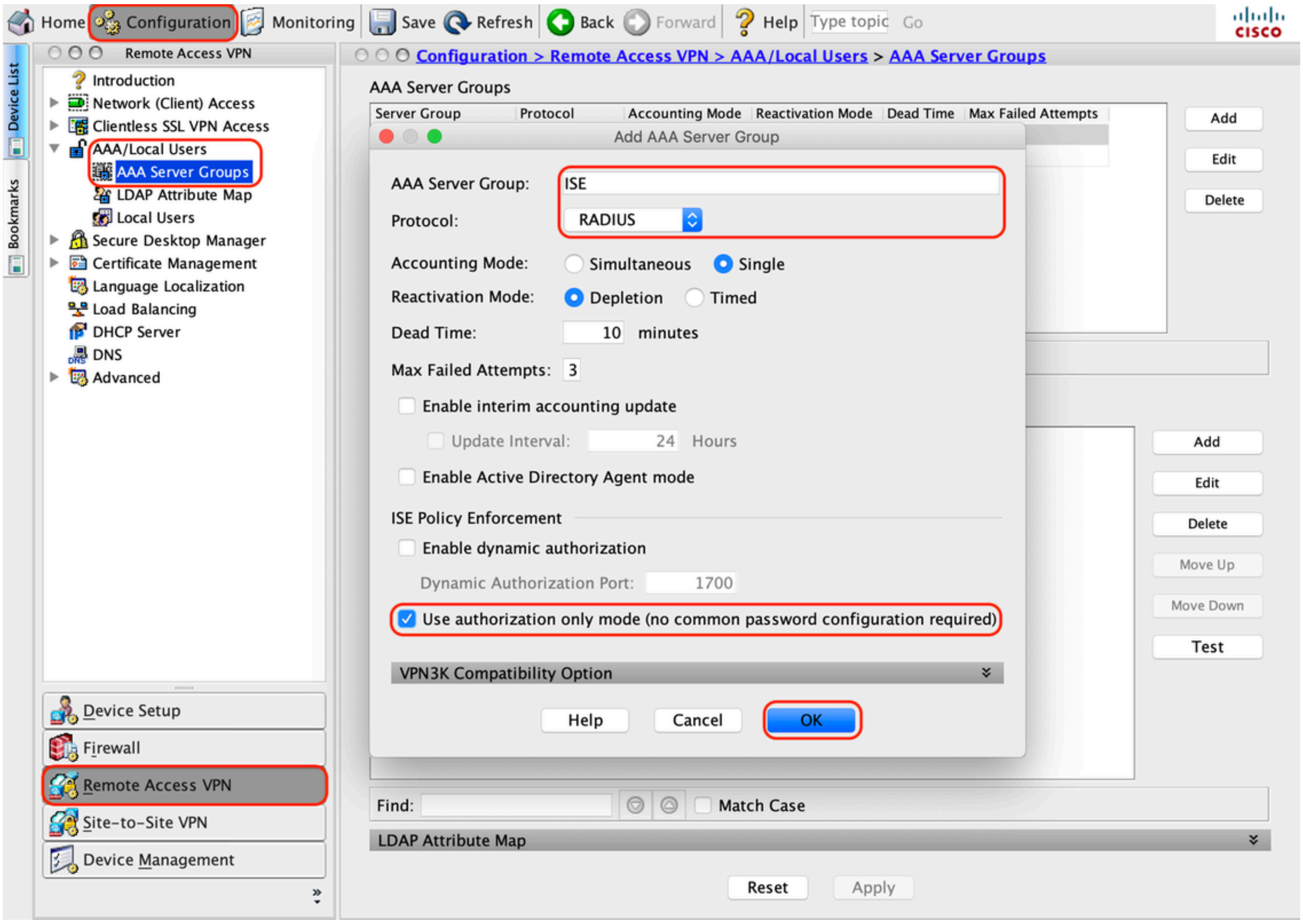
Ending IP Address: 10.197.164.7

Subnet Mask: 255.255.255.0

3.配置AAA伺服器組

A.在此部分，配置AAA伺服器組並提供執行授權的特定AAA伺服器的詳細資訊

B.導航到「Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups」，然後按一下「Add」



AAA Server Group: ISE

Protocol: RADIUS

Accounting Mode: ○ Simultaneous ● Single

Reactivation Mode: ● Depletion ○ Timed

Dead Time: 10 minutes

Max Failed Attempts: 3

□ Enable interim accounting update

□ Update Interval: 24 Hours

□ Enable Active Directory Agent mode

ISE Policy Enforcement

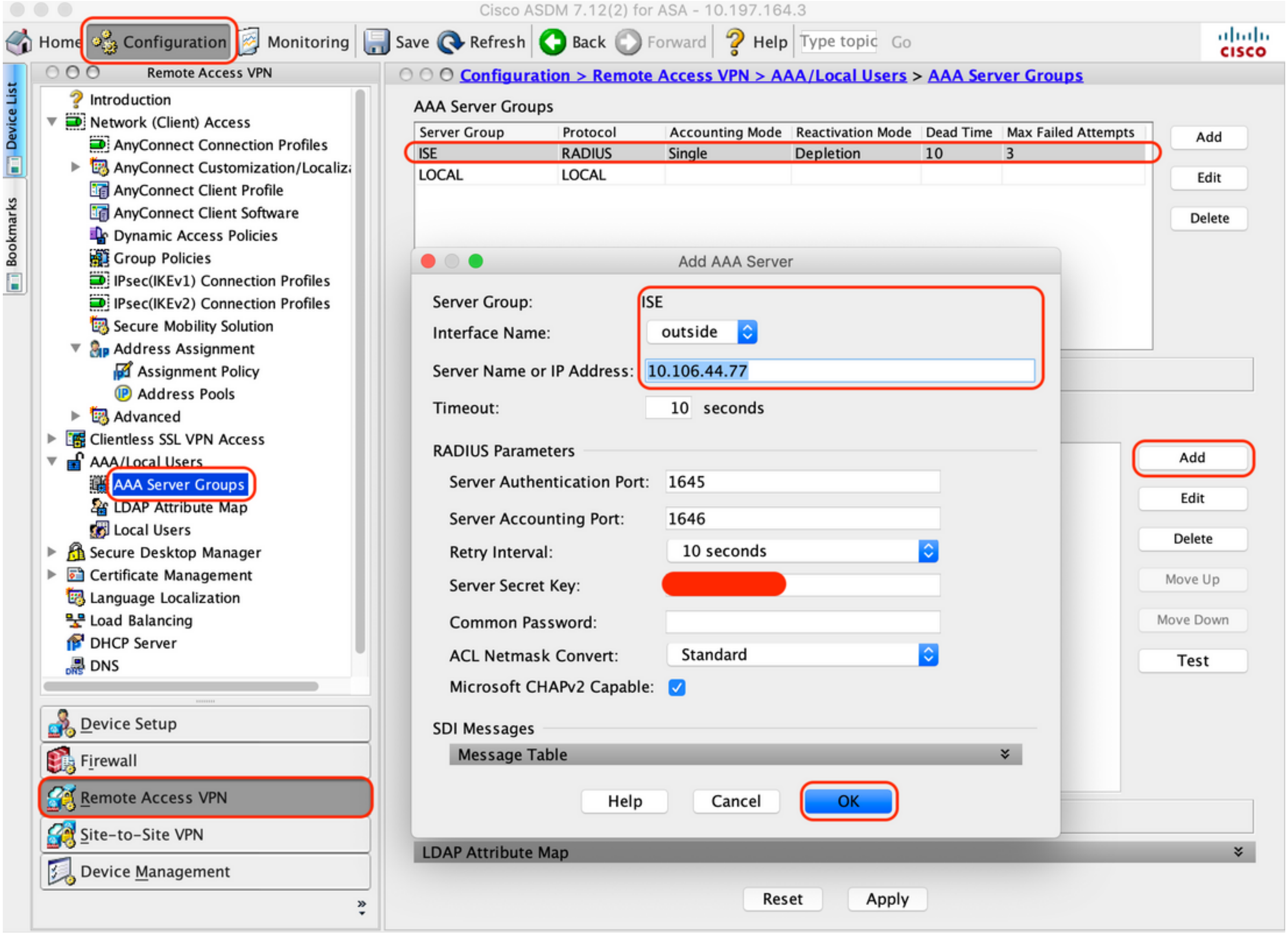
□ Enable dynamic authorization

Dynamic Authorization Port: 1700

☑ Use authorization only mode (no common password configuration required)

VPN3K Compatibility Option

C.在同一頁的「Servers in the Selected group」部分下，按一下「Add」並提供AAA伺服器的IP地址詳細資訊



Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups

AAA Server Groups

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
ISE	RADIUS	Single	Depletion	10	3
LOCAL	LOCAL				

Add AAA Server

Server Group: ISE

Interface Name: outside

Server Name or IP Address: 10.106.44.77

Timeout: 10 seconds

RADIUS Parameters

Server Authentication Port: 1645

Server Accounting Port: 1646

Retry Interval: 10 seconds

Server Secret Key: [redacted]

Common Password:

ACL Netmask Convert: Standard

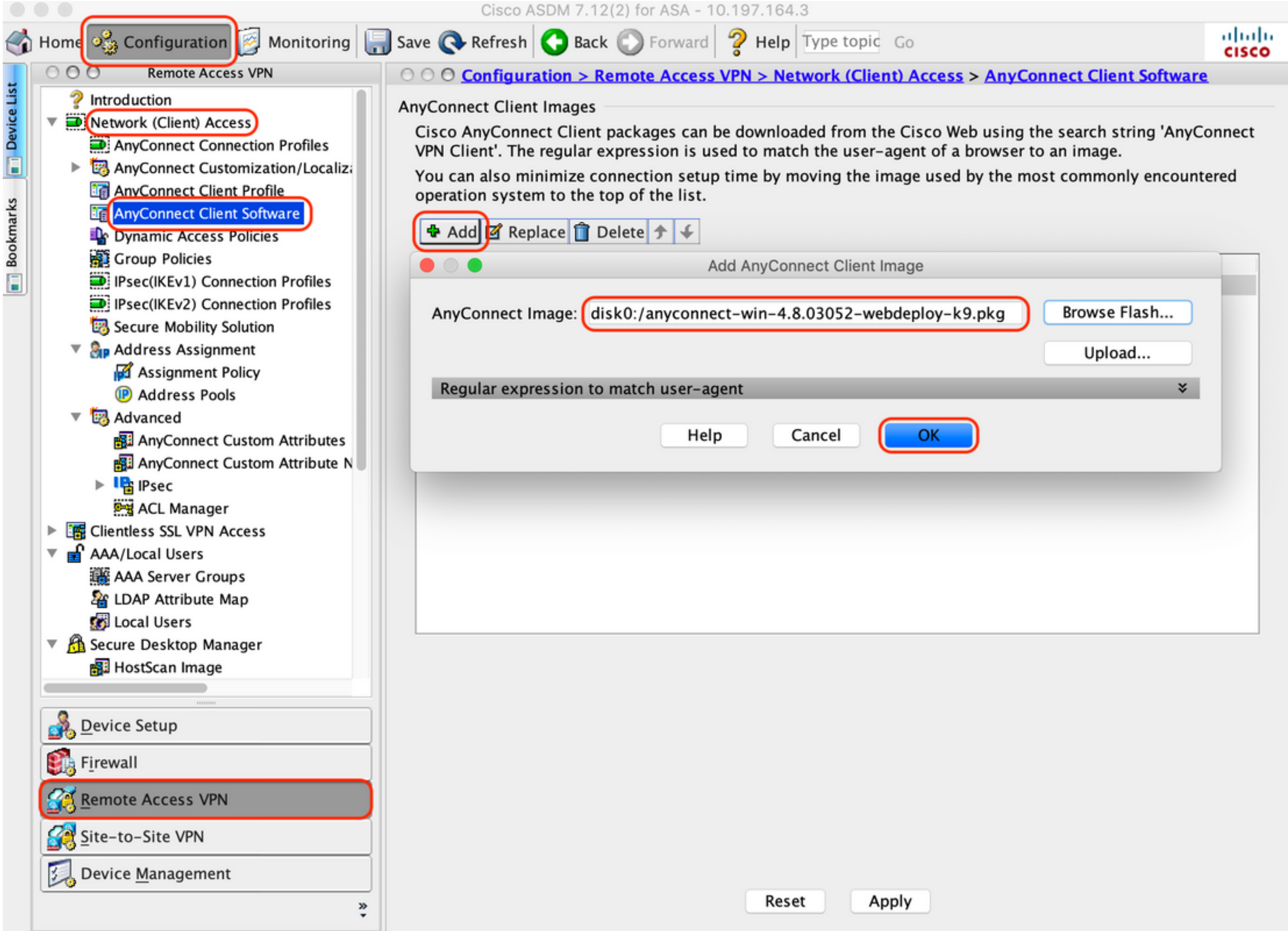
Microsoft CHAPv2 Capable: ☑

SDI Messages

4.對映AnyConnect客戶端軟體

A.對映用於WebVPN的Windows的AnyConnect客戶端軟體webdeploy映像4.8.03052

B.導航到「Configuration > Remote Access VPN > Network(Client)Access > AnyConnect Client Software」，按一下「Add」



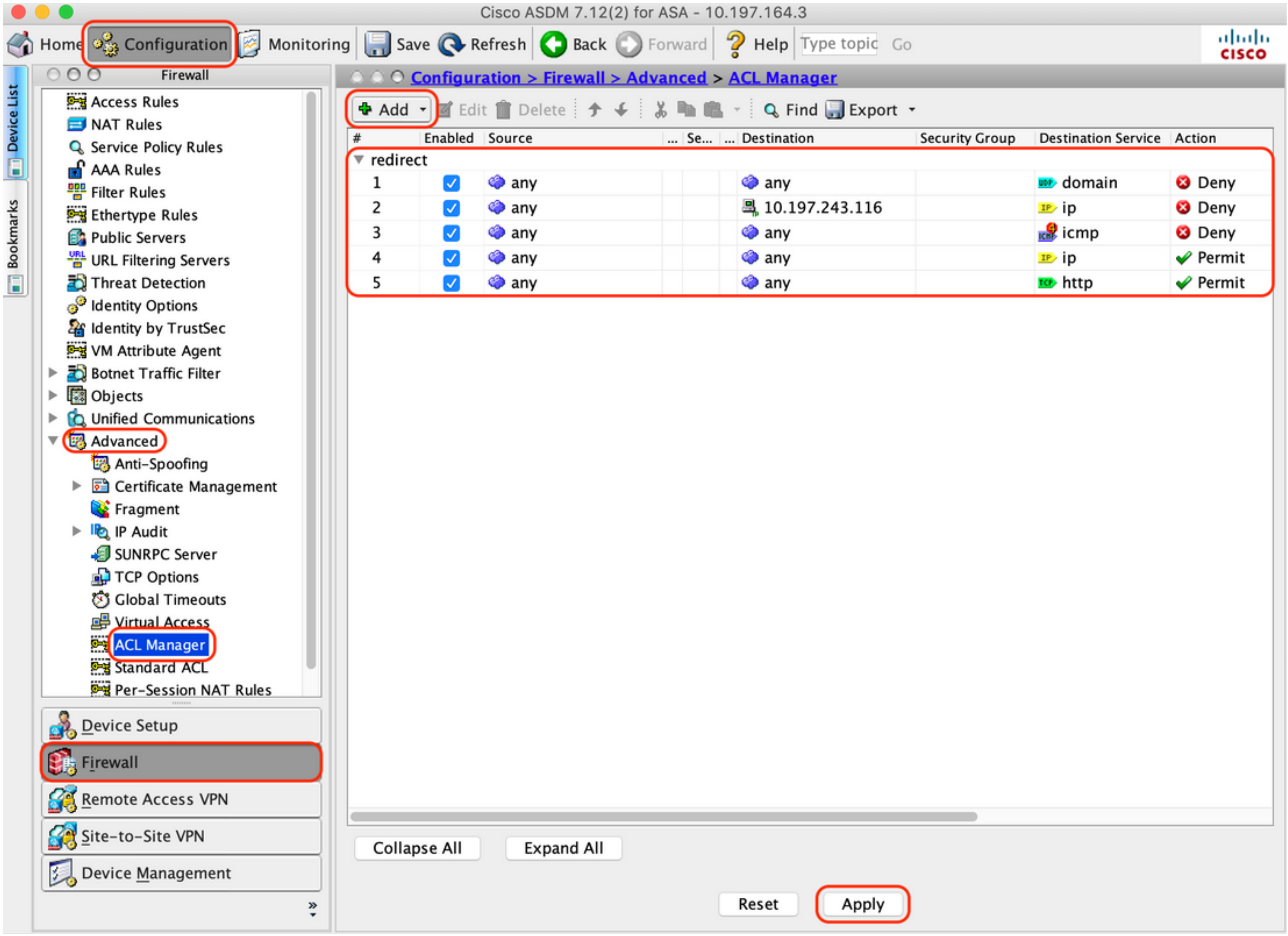
Cisco AnyConnect Client packages can be downloaded from the Cisco Web using the search string 'AnyConnect VPN Client'. The regular expression is used to match the user-agent of a browser to an image.

You can also minimize connection setup time by moving the image used by the most commonly encountered operation system to the top of the list.

AnyConnect Image: disk0:/anyconnect-win-4.8.03052-webdeploy-k9.pkg

5.配置從ISE推送的重定向ACL

A.導覽至「Configuration > Firewall > Advanced > ACL Manager」，然後按一下Add以新增重新導向ACL。條目一旦配置，如下圖所示：

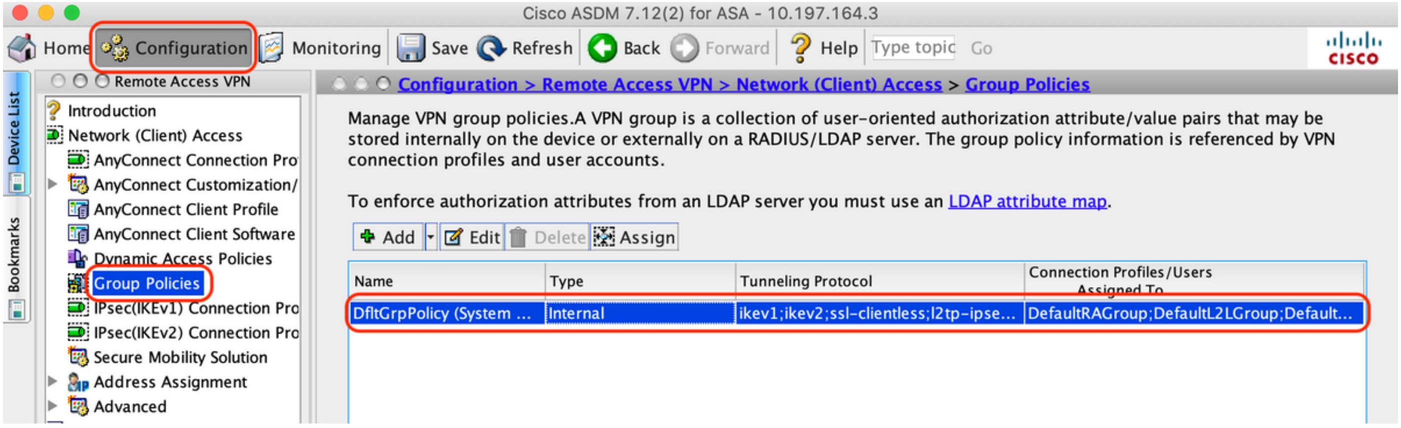


redirect

#	Enabled	Source	Se...	Destination	Security Group	Destination Service	Action
1	☑	any		any		domain	Deny
2	☑	any		10.197.243.116		ip	Deny
3	☑	any		any		icmp	Deny
4	☑	any		any		ip	Permit
5	☑	any		any		http	Permit

6.驗證現有組策略

A.此設定使用預設組策略，可以在以下位置檢視：「Configuration > Remote Access VPN > Network(Client)Access > Group Policies」


Cisco ASDM 7.12(2) for ASA - 10.197.164.3
Home
Configuration
Monitoring
Save
Refresh
Back
Forward
Help
Type topic
Go
Remote Access VPN
Introduction
Network (Client) Access
AnyConnect Connection Pro
AnyConnect Customization/
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connection Pro
IPsec(IKEv2) Connection Pro
Secure Mobility Solution
Address Assignment
Advanced
Configuration > Remote Access VPN > Network (Client) Access > Group Policies
Add
Edit
Delete
Assign

Manage VPN group policies.A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts.

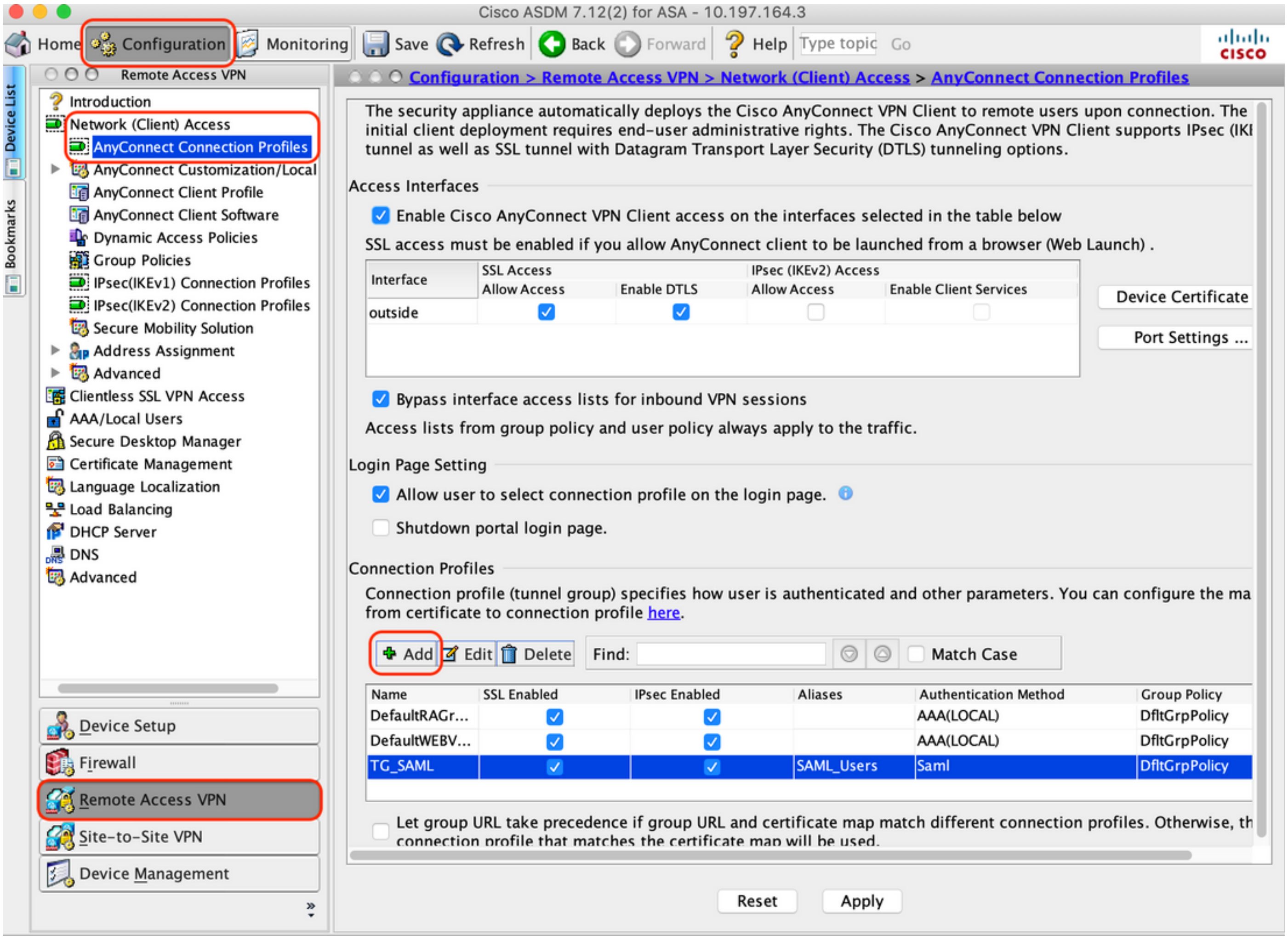
To enforce authorization attributes from an LDAP server you must use an LDAP attribute map.

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
DfltGrpPolicy (System ...	Internal	ikev1;ikev2;ssl-clientless;l2tp-ipse...	DefaultRAGroup;DefaultL2LGroup;Default...

7.配置連線配置檔案

A.建立AnyConnect使用者連線的新連線配置檔案

B.導航到「Configuration > Remote Access VPN > Network(Client)Access > Anyconnect Connection Profiles」，按一下「Add」



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports IPsec (IKE tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.

Access Interfaces

☑ Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below

SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch) .

Interface	SSL Access		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow Access	Enable Client Services
outside	☑	☑	□	□

☑ Bypass interface access lists for inbound VPN sessions

Access lists from group policy and user policy always apply to the traffic.

Login Page Setting

☑ Allow user to select connection profile on the login page.

□ Shutdown portal login page.

Connection Profiles

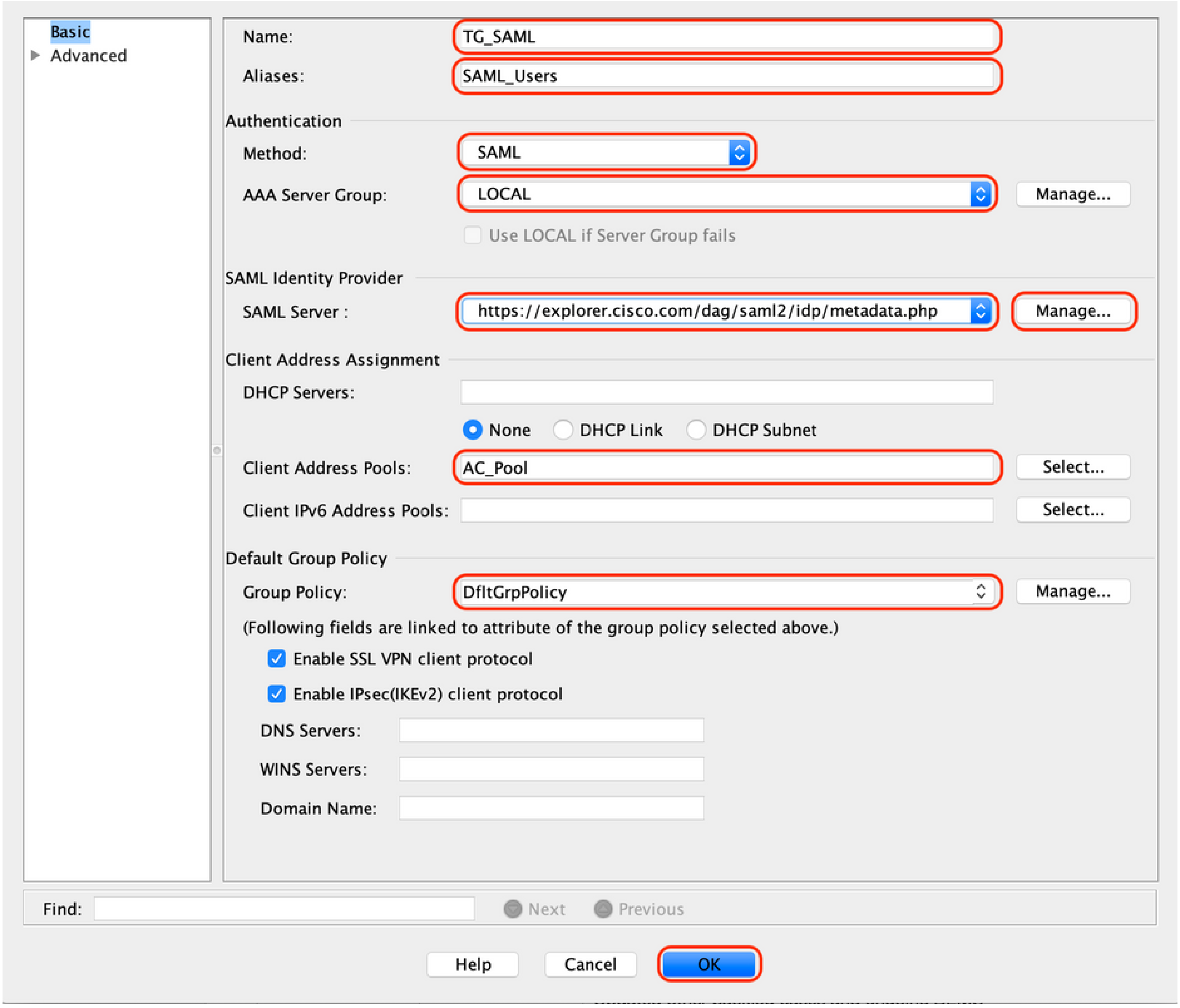
Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the ma from certificate to connection profile here.

Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGr...	☑	☑		AAA(LOCAL)	DfltGrpPolicy
DefaultWEBV...	☑	☑		AAA(LOCAL)	DfltGrpPolicy
TG_SAML	☑	☑	SAML_Users	Saml	DfltGrpPolicy

□ Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, th connection profile that matches the certificate map will be used.

C.配置以下與連線配置檔案相關的詳細資訊：

名稱	TG_SAML
別名	SAML_Users
方法	SAML
AAA伺服器組	本地
客戶端地址池	AC_Pool
組策略	DfltGrpPolicy



Name: TG_SAML

Aliases: SAML_Users

Authentication

Method: SAML

AAA Server Group: LOCAL

□ Use LOCAL if Server Group fails

SAML Identity Provider

SAML Server : https://explorer.cisco.com/dag/saml2/idp/metadata.php

Client Address Assignment

DHCP Servers:

● None ○ DHCP Link ○ DHCP Subnet

Client Address Pools: AC_Pool

Client IPv6 Address Pools:

Default Group Policy

Group Policy: DfltGrpPolicy

(Following fields are linked to attribute of the group policy selected above.)

☑ Enable SSL VPN client protocol

☑ Enable IPsec(IKEv2) client protocol

DNS Servers:

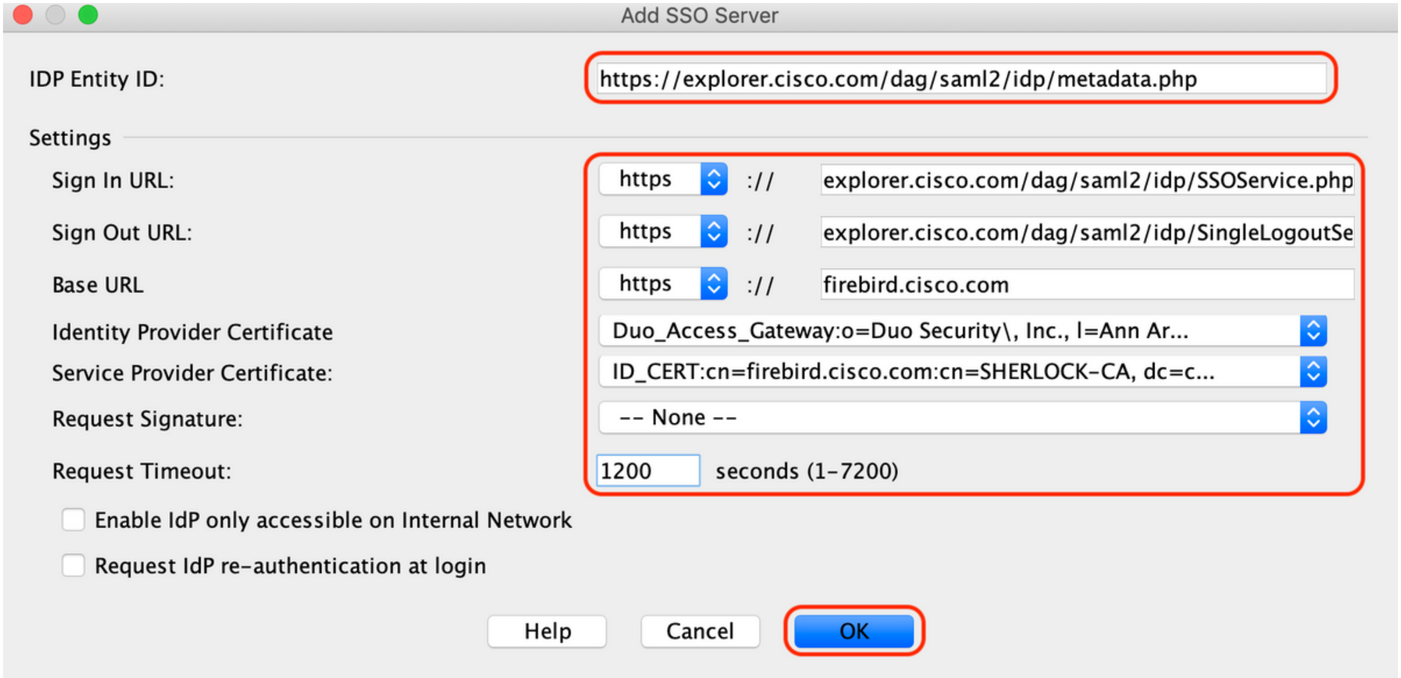
WINS Servers:

Domain Name:

D.在同一頁面上，配置SAML身份提供程式詳細資訊，如下所示：

IDP實體標識	https://explorer.cisco.com/dag/saml2/idp/metadata.php
登入URL	https://explorer.cisco.com/dag/saml2/idp/SSOService.php
註銷URL	https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explorer.cisc
基本URL	https://firebird.cisco.com

E.按一下「管理>新增」



Add SSO Server

IDP Entity ID: https://explorer.cisco.com/dag/saml2/idp/metadata.php

Settings

Sign In URL: https :// explorer.cisco.com/dag/saml2/idp/SSOService.php

Sign Out URL: https :// explorer.cisco.com/dag/saml2/idp/SingleLogoutSe

Base URL: https :// firebird.cisco.com

Identity Provider Certificate: Duo_Access_Gateway:o=Duo Security\, Inc., l=Ann Ar...

Service Provider Certificate: ID_CERT:cn=firebird.cisco.com:cn=SHERLOCK-CA, dc=c...

Request Signature: -- None --

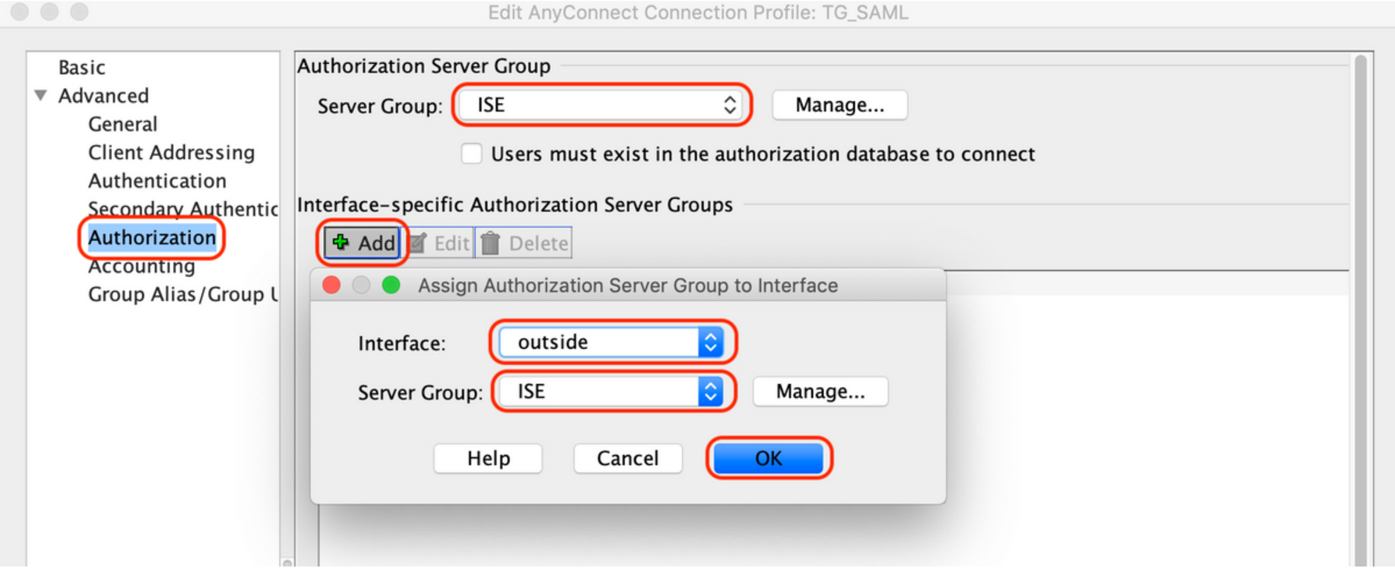
Request Timeout: 1200 seconds (1-7200)

□ Enable IdP only accessible on Internal Network

□ Request IdP re-authentication at login

F.在連線配置檔案的「高級」部分下，定義用於授權的AAA伺服器

導航至「Advanced > Authorization」，然後按一下「Add」



Edit AnyConnect Connection Profile: TG_SAML

Authorization Server Group

Server Group: ISE

□ Users must exist in the authorization database to connect

Interface-specific Authorization Server Groups

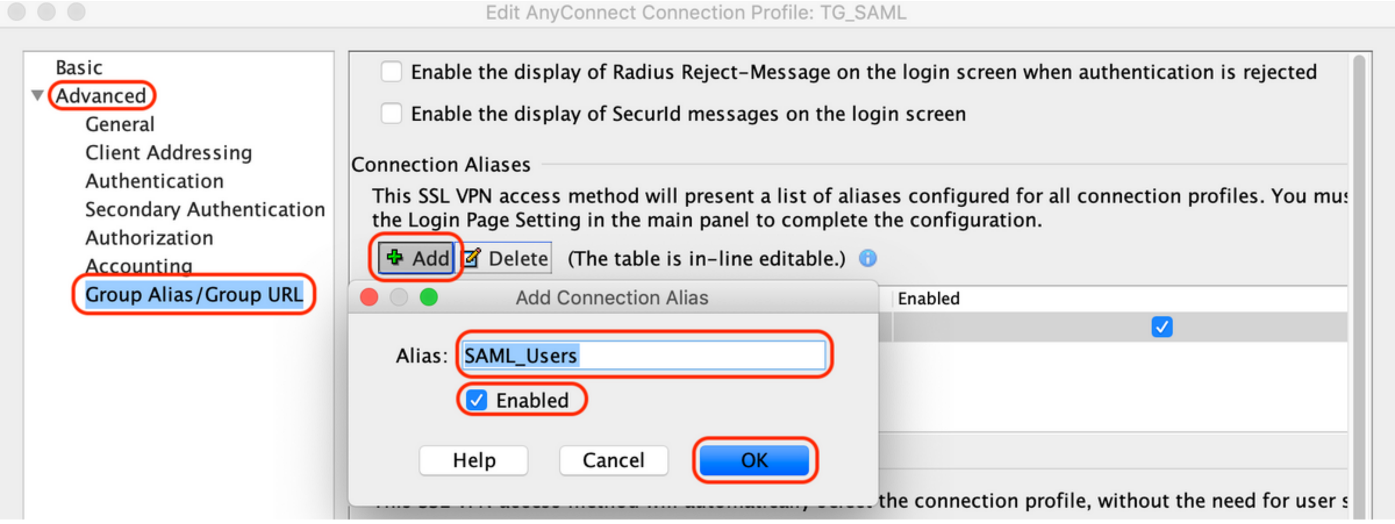
Assign Authorization Server Group to Interface

Interface: outside

Server Group: ISE

G.在「組別名」下，定義連線別名

導航到「Advanced > Group Alias/Group URL」，然後按一下「Add」



□ Enable the display of Radius Reject-Message on the login screen when authentication is rejected

□ Enable the display of SecurId messages on the login screen

Connection Aliases

This SSL VPN access method will present a list of aliases configured for all connection profiles. You mus
the Login Page Setting in the main panel to complete the configuration.

(The table is in-line editable.)

Enabled
☑

Alias: SAML_Users

☑ Enabled

the connection profile, without the need for user s

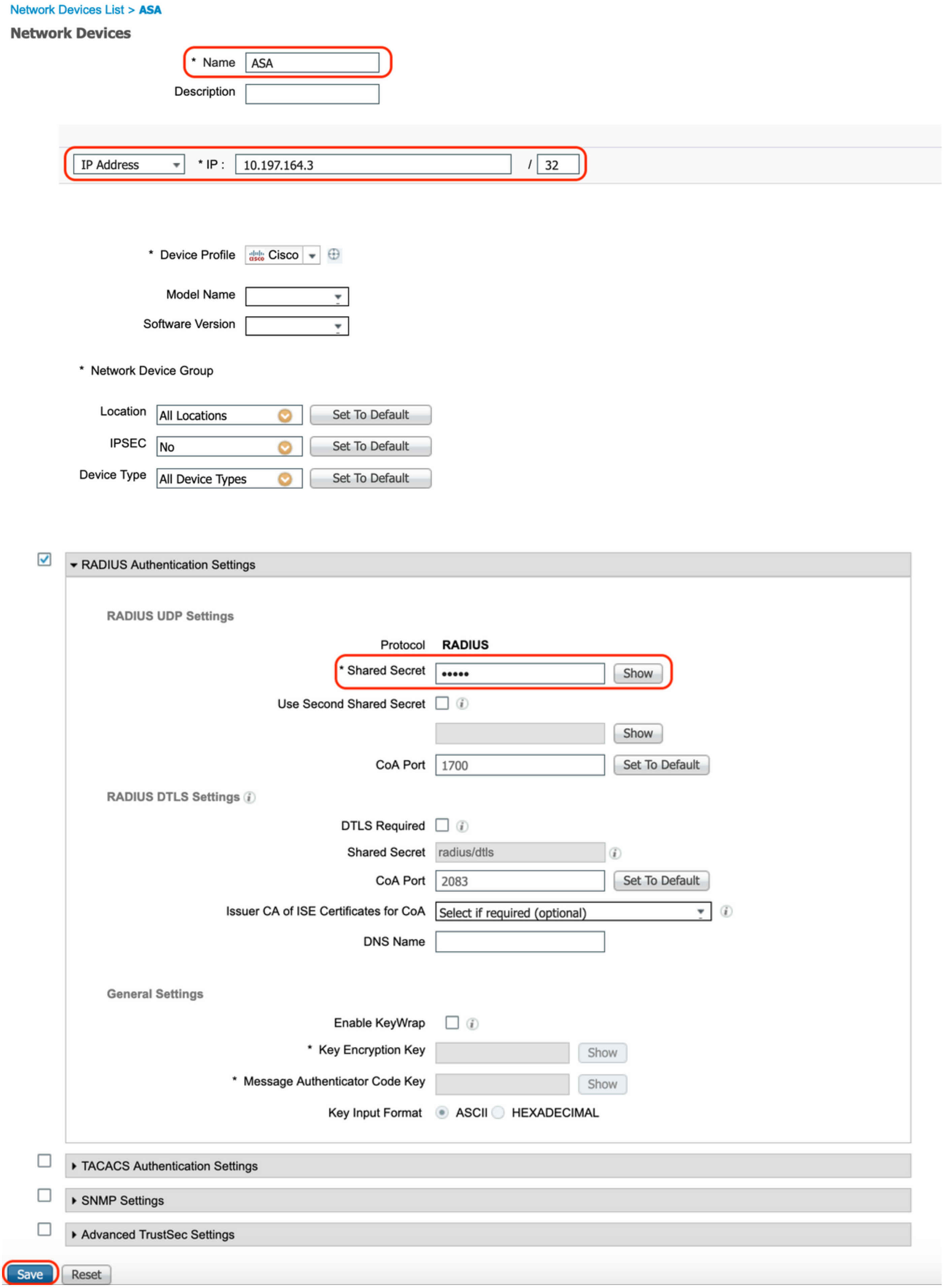
H.這樣ASA配置即完成，與命令列介面(CLI)上的如下所示相同

```
!
hostname firebird
domain-name cisco.com
!
!
name 10.197.164.7 explorer.cisco.com
name 10.197.164.3 firebird.cisco.com
!
!--------------------Client pool configuration--------------------
!
ip local pool AC_Pool 10.197.164.6-explorer.cisco.com mask 255.255.255.0
!
!--------------------Redirect Access-list-------------------------
!
access-list redirect extended deny udp any any eq domain
access-list redirect extended deny ip any host 10.197.243.116
access-list redirect extended deny icmp any any
access-list redirect extended permit ip any any
access-list redirect extended permit tcp any any eq www
!
!--------------------AAA server configuration---------------------
!
aaa-server ISE protocol radius
 authorize-only
 interim-accounting-update periodic 1
 dynamic-authorization
aaa-server ISE (outside) host 10.106.44.77
 key *****
!
!-----Configure Trustpoint for Duo Access Gateway Certificate-----
!
crypto ca trustpoint Duo_Access_Gateway
 enrollment terminal
 crl configure
!
!-------Configure Trustpoint for ASA Identity Certificate---------
!
crypto ca trustpoint ID_CERT
 enrollment terminal
 fqdn firebird.cisco.com
 subject-name CN=firebird.cisco.com
 ip-address 10.197.164.3
 keypair ID_RSA_KEYS
 no ca-check
 crl configure
!
!------Enable AnyConnect and configuring SAML authentication------
!
webvpn
 enable outside
 hsts
  enable
  max-age 31536000
  include-sub-domains
  no preload
 anyconnect image disk0:/anyconnect-win-4.8.03052-webdeploy-k9.pkg 1
 anyconnect enable
 saml idp https://explorer.cisco.com/dag/saml2/idp/metadata.php
  url sign-in https://explorer.cisco.com/dag/saml2/idp/SSOService.php
  url sign-out https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explor
  base-url https://firebird.cisco.com
  trustpoint idp Duo_Access_Gateway
  trustpoint sp ID_CERT
  no signature
  no force re-authentication
  timeout assertion 1200
 tunnel-group-list enable
 cache
  disable
 error-recovery disable
!
!--------------------Group Policy configuration--------------------
!
group-policy DfltGrpPolicy attributes
 vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless
!
!----------Tunnel-Group (Connection Profile) Configuraiton----------
!
tunnel-group TG_SAML type remote-access
tunnel-group TG_SAML general-attributes
 address-pool AC_Pool
 authorization-server-group ISE
 accounting-server-group ISE
tunnel-group TG_SAML webvpn-attributes
 authentication saml
 group-alias SAML_Users enable
 saml identity-provider https://explorer.cisco.com/dag/saml2/idp/metadata.php
!
```

-ISE 組態

1.新增Cisco ASA作為網路裝置

在「Administration > Network Resources > Network Devices」下，按一下「Add」。
配置網路裝置的名稱、關聯的IP地址，並在「Radius身份驗證設定」下配置「共用金鑰」並按一下「儲存」



Network Devices List > **ASA**

Network Devices

* Name: ASA

Description:

IP Address ▾ * IP : 10.197.164.3 / 32

* Device Profile: Cisco ▾

Model Name: ▾

Software Version: ▾

* Network Device Group

Location: All Locations — Set To Default

IPSEC: No — Set To Default

Device Type: All Device Types — Set To Default

☑ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: **RADIUS**

* Shared Secret: ••••• — Show

Use Second Shared Secret ☐

Show

CoA Port: 1700 — Set To Default

RADIUS DTLS Settings

DTLS Required ☐

Shared Secret: radius/dtls

CoA Port: 2083 — Set To Default

Issuer CA of ISE Certificates for CoA: Select if required (optional) ▾

DNS Name:

General Settings

Enable KeyWrap ☐

* Key Encryption Key: — Show

* Message Authenticator Code Key: — Show

Key Input Format: ● ASCII ○ HEXADECIMAL

☐ TACACS Authentication Settings

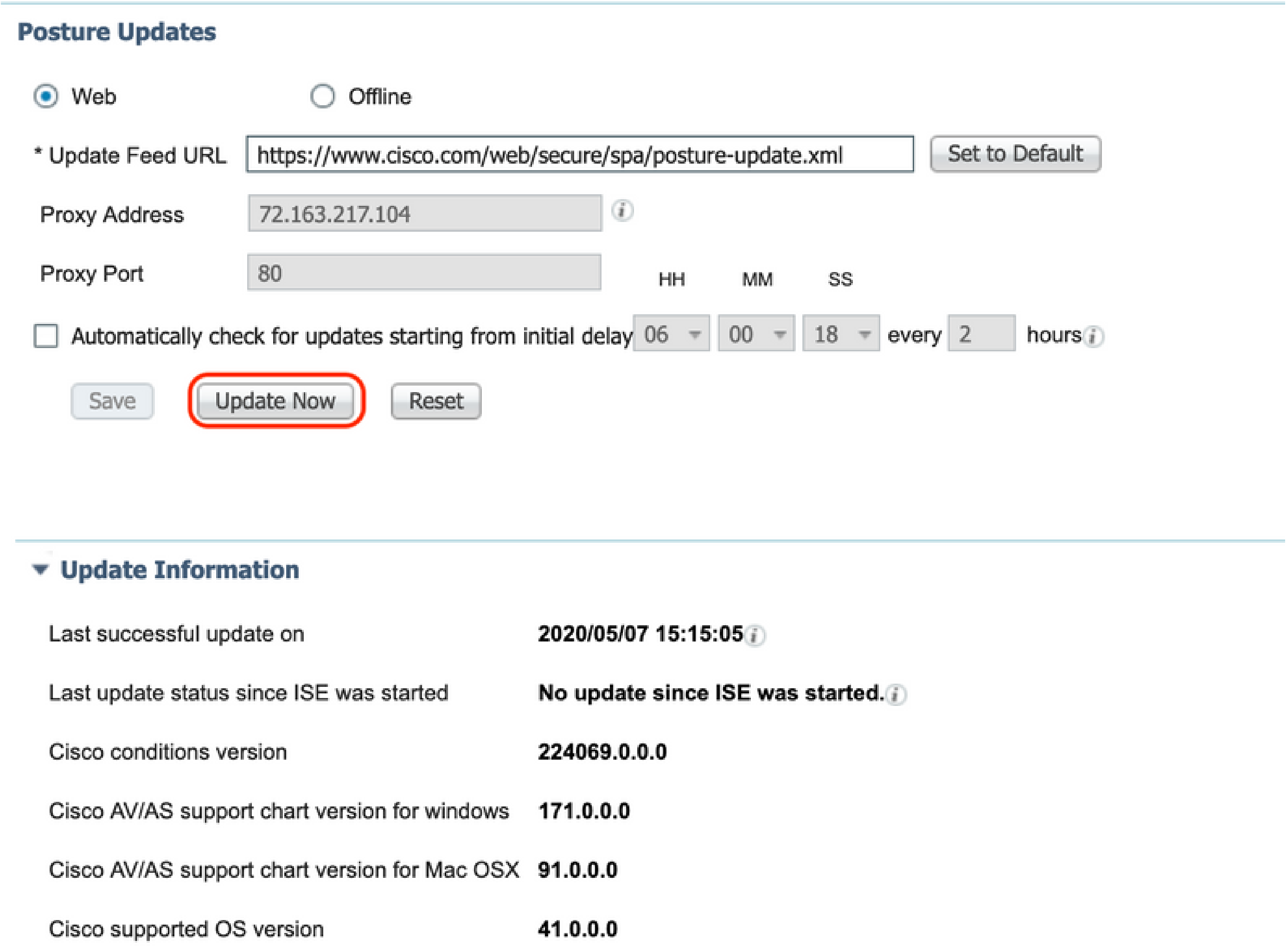
☐ SNMP Settings

☐ Advanced TrustSec Settings

Save Reset

2.安裝最新的狀態更新

導航到「Administration > System > Settings > Posture > Updates」，然後按一下「Update Now」



Posture Updates

● Web　　○ Offline

* Update Feed URL: https://www.cisco.com/web/secure/spa/posture-update.xml [Set to Default]

Proxy Address: 72.163.217.104

Proxy Port: 80

□ Automatically check for updates starting from initial delay HH 06 MM 00 SS 18 every 2 hours

[Save] [Update Now] [Reset]

Update Information

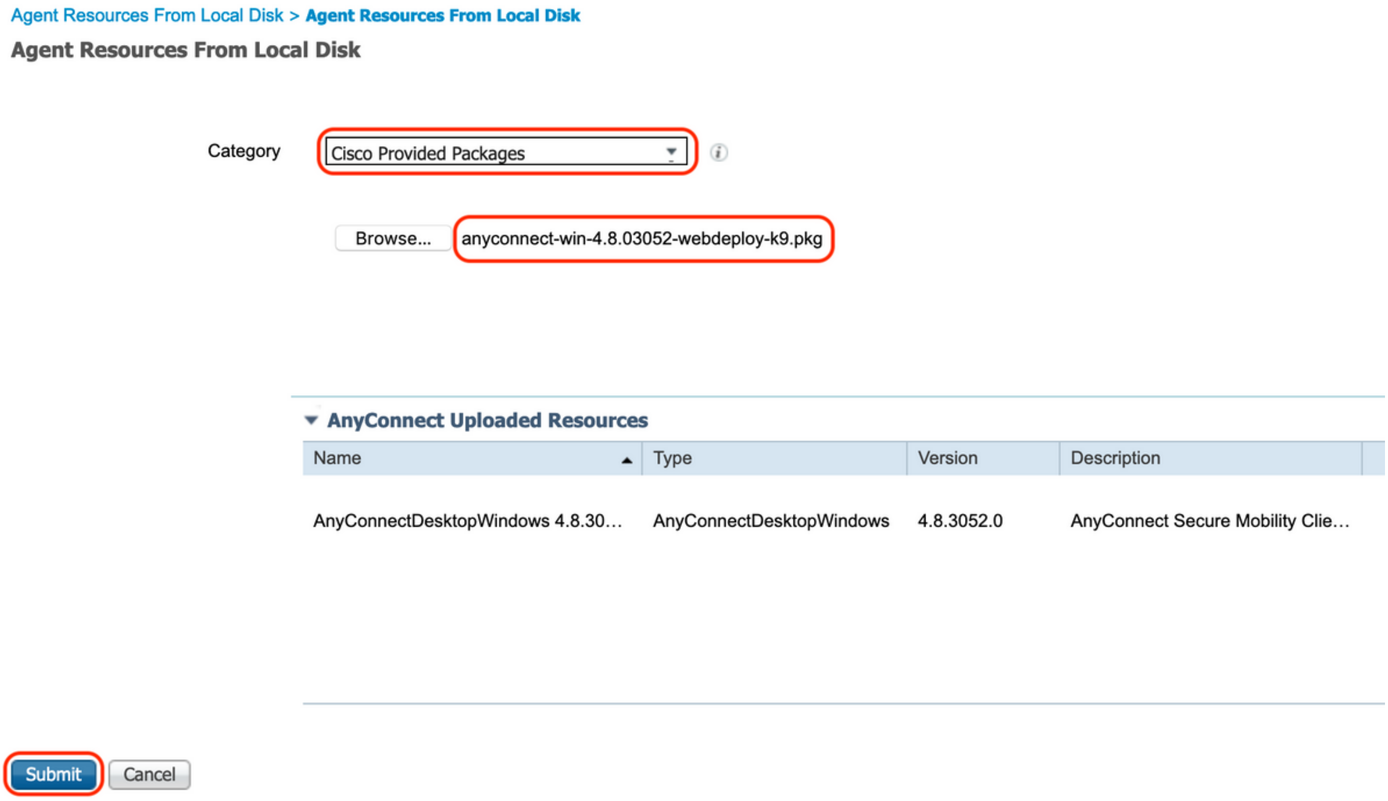
Last successful update on	2020/05/07 15:15:05
Last update status since ISE was started	No update since ISE was started.
Cisco conditions version	224069.0.0.0
Cisco AV/AS support chart version for windows	171.0.0.0
Cisco AV/AS support chart version for Mac OSX	91.0.0.0
Cisco supported OS version	41.0.0.0

3.在ISE上上傳合規性模組和AnyConnect頭端部署包

導航至「Policy > Policy Elements > Results > Client Provisioning > Resources」。點選「新增」，然後根據檔案是從本地工作站還是思科站點回遷來選擇「從本地磁碟獲取代理資源」或「從思科站點獲取代理資源」。

在這種情況下，要從本地工作站的「類別」下上傳檔案，請選擇「思科提供的包」，按一下「瀏覽」並選擇所需的包，然後按一下「提交」。

本文檔使用「anyconnect-win-4.3.1012.6145-isecompliance-webdeploy-k9.pkg」作為合規性模組，使用「anyconnect-win-4.8.03052-webdeploy-k9.pkg」作為AnyConnect頭端部署包。



Agent Resources From Local Disk > **Agent Resources From Local Disk**

Agent Resources From Local Disk

Category: Cisco Provided Packages

Browse... anyconnect-win-4.8.03052-webdeploy-k9.pkg

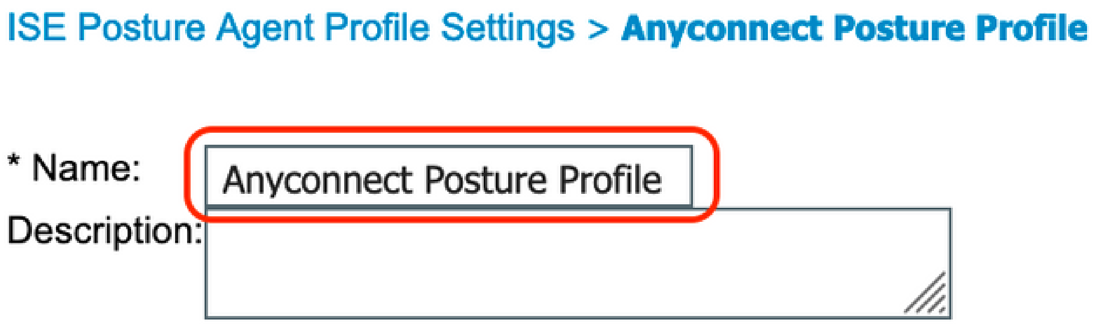
AnyConnect Uploaded Resources

Name	Type	Version	Description
AnyConnectDesktopWindows 4.8.30…	AnyConnectDesktopWindows	4.8.3052.0	AnyConnect Secure Mobility Clie…

4.建立AnyConnect終端安全評估配置檔案

A.導航到「策略>策略元素>結果>客戶端調配>資源」。點選「新增」並選擇「AnyConnect狀態配置檔案」

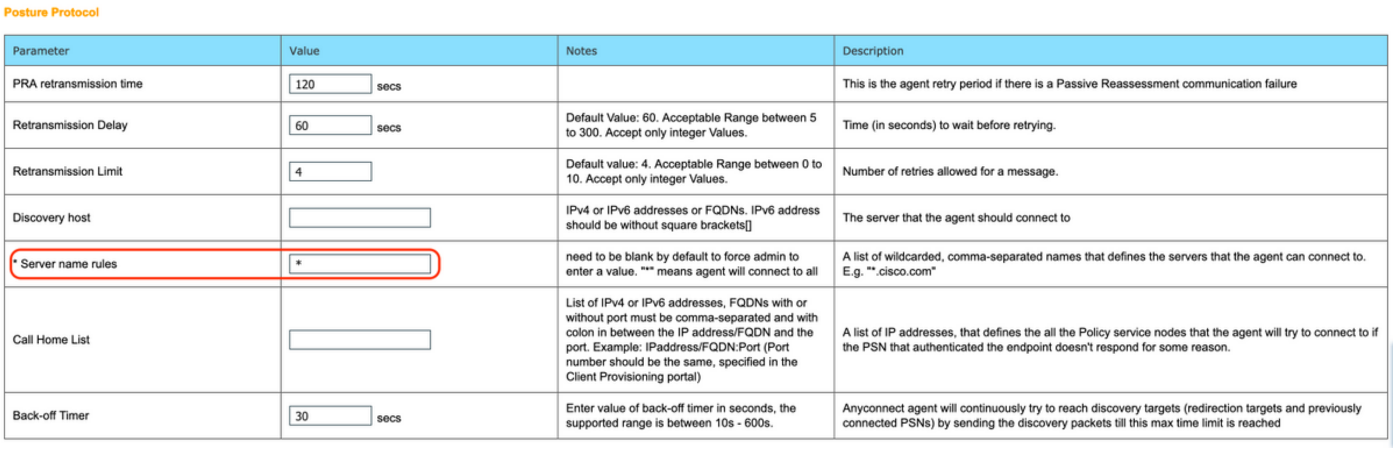
B.輸入Anyconnect狀態配置檔案的名稱，並在「伺服器名稱」規則下將伺服器名稱配置為「*」，然後按一下「儲存」



ISE Posture Agent Profile Settings > **Anyconnect Posture Profile**

* Name: Anyconnect Posture Profile

Description:



Posture Protocol

Parameter	Value	Notes	Description
PRA retransmission time	120 secs		This is the agent retry period if there is a Passive Reassessment communication failure
Retransmission Delay	60 secs	Default Value: 60. Acceptable Range between 5 to 300. Accept only integer Values.	Time (in seconds) to wait before retrying.
Retransmission Limit	4	Default value: 4. Acceptable Range between 0 to 10. Accept only integer Values.	Number of retries allowed for a message.
Discovery host		IPv4 or IPv6 addresses or FQDNs. IPv6 address should be without square brackets[]	The server that the agent should connect to
* Server name rules	*	need to be blank by default to force admin to enter a value. "*" means agent will connect to all	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. "*.cisco.com"
Call Home List		List of IPv4 or IPv6 addresses, FQDNs with or without port must be comma-separated and with colon in between the IP address/FQDN and the port. Example: IPaddress/FQDN:Port (Port number should be the same, specified in the Client Provisioning portal)	A list of IP addresses, that defines the all the Policy service nodes that the agent will try to connect to if the PSN that authenticated the endpoint doesn't respond for some reason.
Back-off Timer	30 secs	Enter value of back-off timer in seconds, the supported range is between 10s - 600s.	Anyconnect agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this max time limit is reached

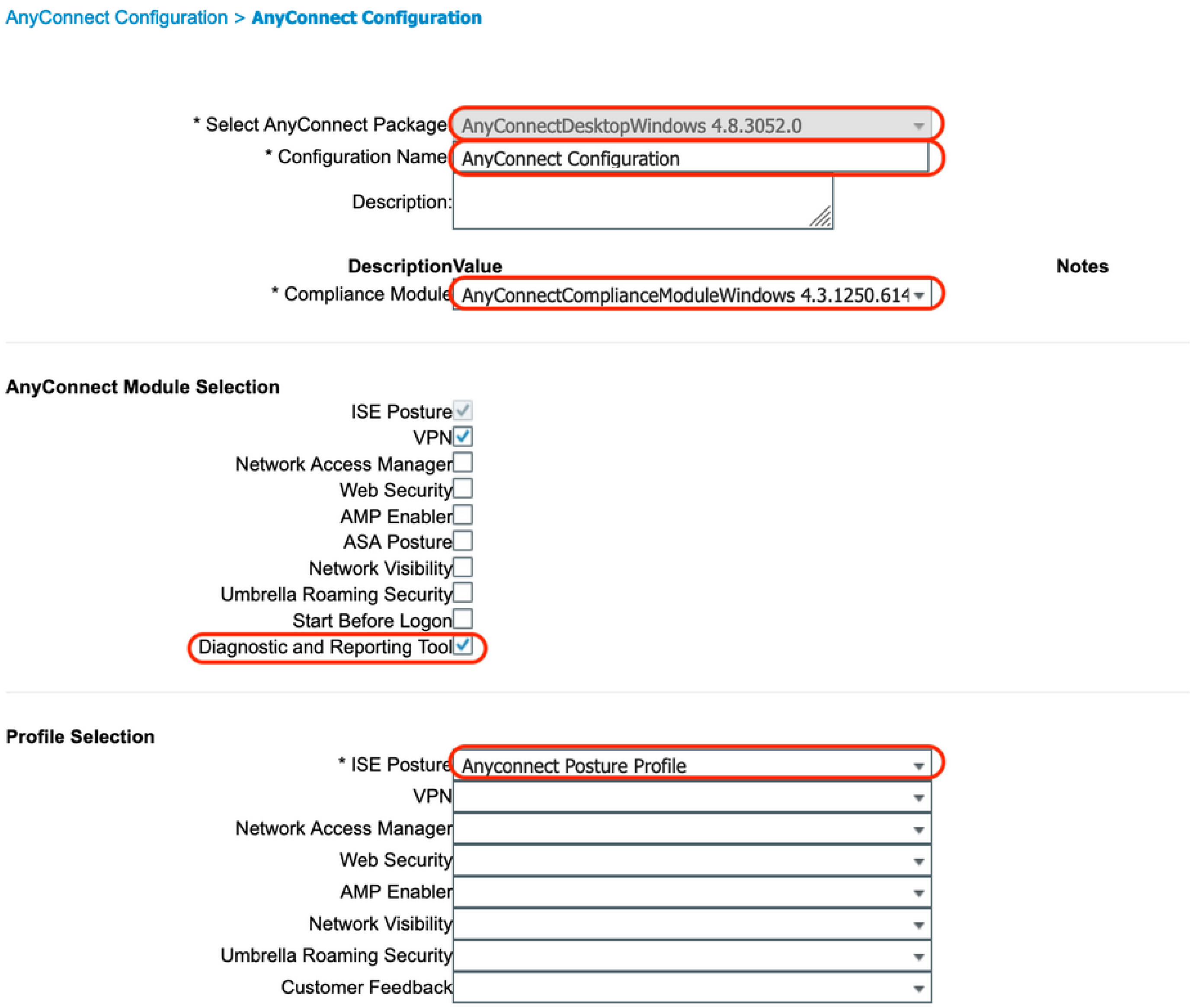
5.建立Anyconnect配置

A.導航到「策略>策略元素>結果>客戶端調配>資源」。按一下「新增」並選擇「AnyConnect配置」

B.選擇AnyConnect包，輸入配置名稱，選擇所需的合規性模組

C.在「AnyConnect模組選擇」下，選中「診斷和報告工具」

D.在「Profile Selection」下，選擇Posture Profile並按一下「Save」



AnyConnect Configuration > **AnyConnect Configuration**

* Select AnyConnect Package: AnyConnectDesktopWindows 4.8.3052.0

* Configuration Name: AnyConnect Configuration

Description:

DescriptionValue		Notes
* Compliance Module	AnyConnectComplianceModuleWindows 4.3.1250.614	

AnyConnect Module Selection

- ISE Posture ☑
- VPN ☑
- Network Access Manager □
- Web Security □
- AMP Enabler □
- ASA Posture □
- Network Visibility □
- Umbrella Roaming Security □
- Start Before Logon □
- Diagnostic and Reporting Tool ☑

Profile Selection

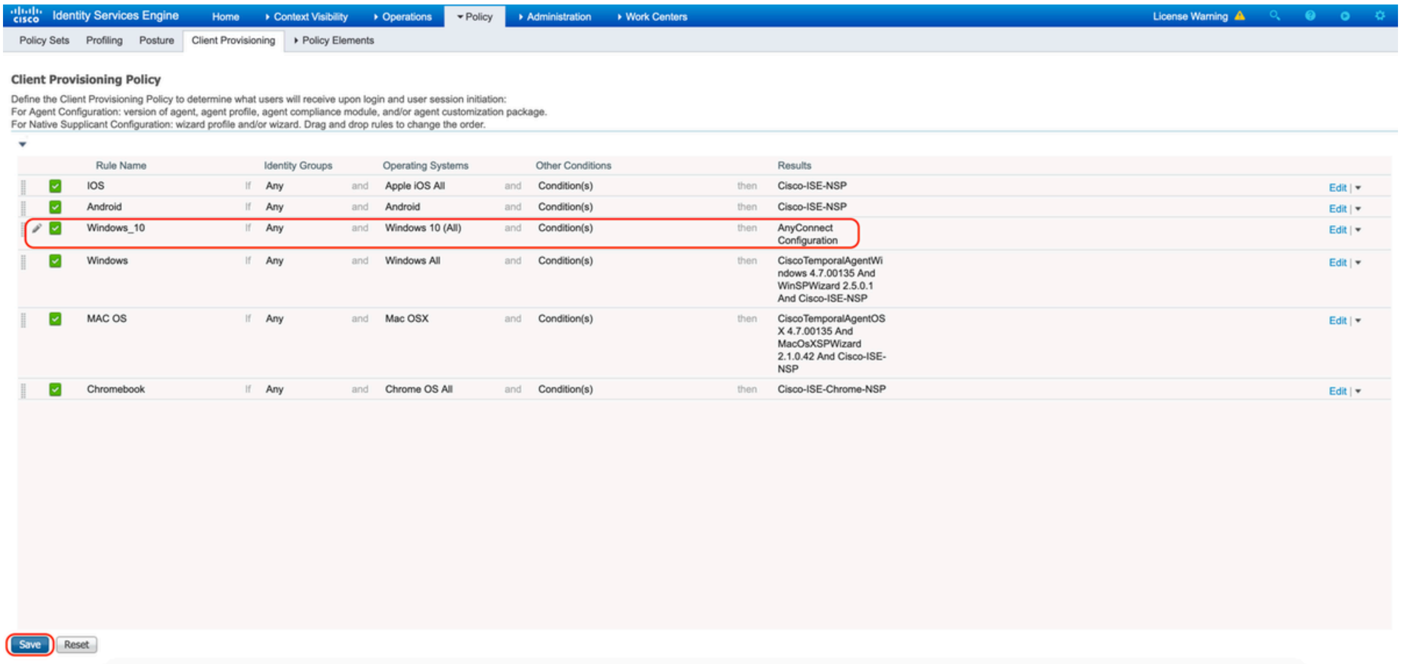
* ISE Posture	Anyconnect Posture Profile
VPN	
Network Access Manager	
Web Security	
AMP Enabler	
Network Visibility	
Umbrella Roaming Security	
Customer Feedback	

6.建立客戶端調配策略

A.導航至「策略>客戶端調配」

B.按一下「編輯」，然後選擇「在上方插入規則」

C.輸入規則名稱，選擇所需的作業系統，然後在「結果」（在「代理」>「代理配置」中）下，選擇在步驟5中建立的「AnyConnect配置」，然後按一下「儲存」



Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

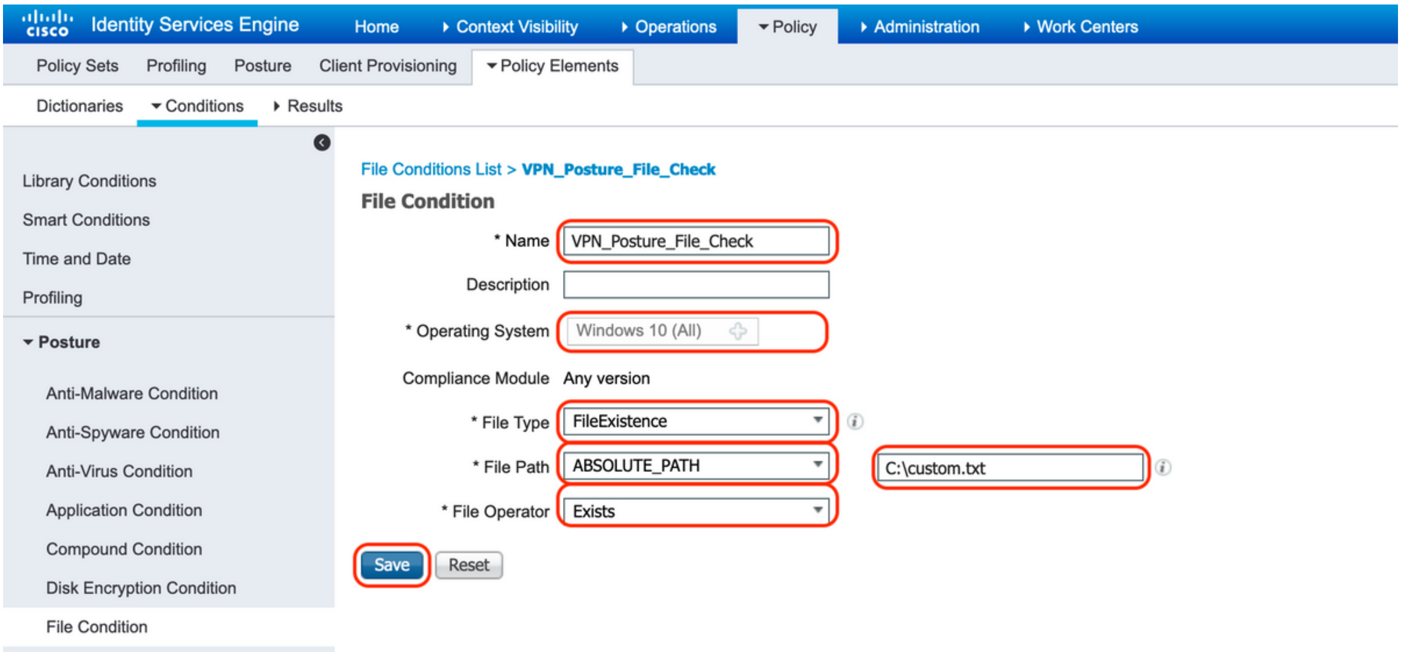
	Rule Name		Identity Groups		Operating Systems		Other Conditions		Results	
☑	IOS	If	Any	and	Apple iOS All	and	Condition(s)	then	Cisco-ISE-NSP	Edit | ▾
☑	Android	If	Any	and	Android	and	Condition(s)	then	Cisco-ISE-NSP	Edit | ▾
☑	Windows_10	If	Any	and	Windows 10 (All)	and	Condition(s)	then	AnyConnect Configuration	Edit | ▾
☑	Windows	If	Any	and	Windows All	and	Condition(s)	then	CiscoTemporalAgentWindows 4.7.00135 And WinSPWizard 2.5.0.1 And Cisco-ISE-NSP	Edit | ▾
☑	MAC OS	If	Any	and	Mac OSX	and	Condition(s)	then	CiscoTemporalAgentOSX 4.7.00135 And MacOsXSPWizard 2.1.0.42 And Cisco-ISE-NSP	Edit | ▾
☑	Chromebook	If	Any	and	Chrome OS All	and	Condition(s)	then	Cisco-ISE-Chrome-NSP	Edit | ▾

7.建立狀態條件

A.導航到「策略>策略元素>條件>狀態>檔案條件」

B.按一下「新增」並將條件名稱「VPN_Posture_File_Check」、所需的作業系統配置為「Windows 10(All)」、檔案型別配置為「FileExistence」、檔案路徑配置為「ABSOLUTE_PATH」、完整路徑和檔名配置為「C:\custom.txt」，選擇檔案運算子配置為「Exists」

C.此示例使用C:drive下名為「custom.txt」的檔案作為檔案條件



File Conditions List > **VPN_Posture_File_Check**

File Condition

* Name	VPN_Posture_File_Check
Description	
* Operating System	Windows 10 (All)
Compliance Module	Any version
* File Type	FileExistence
* File Path	ABSOLUTE_PATH C:\custom.txt
* File Operator	Exists

8.建立狀態修正操作

導航到「Policy > Policy Elements > Results > Posture > Remediation Actions」以建立對應的「File Remediation Action」。本文檔使用「僅消息文本」作為下一步中配置的補救操作。

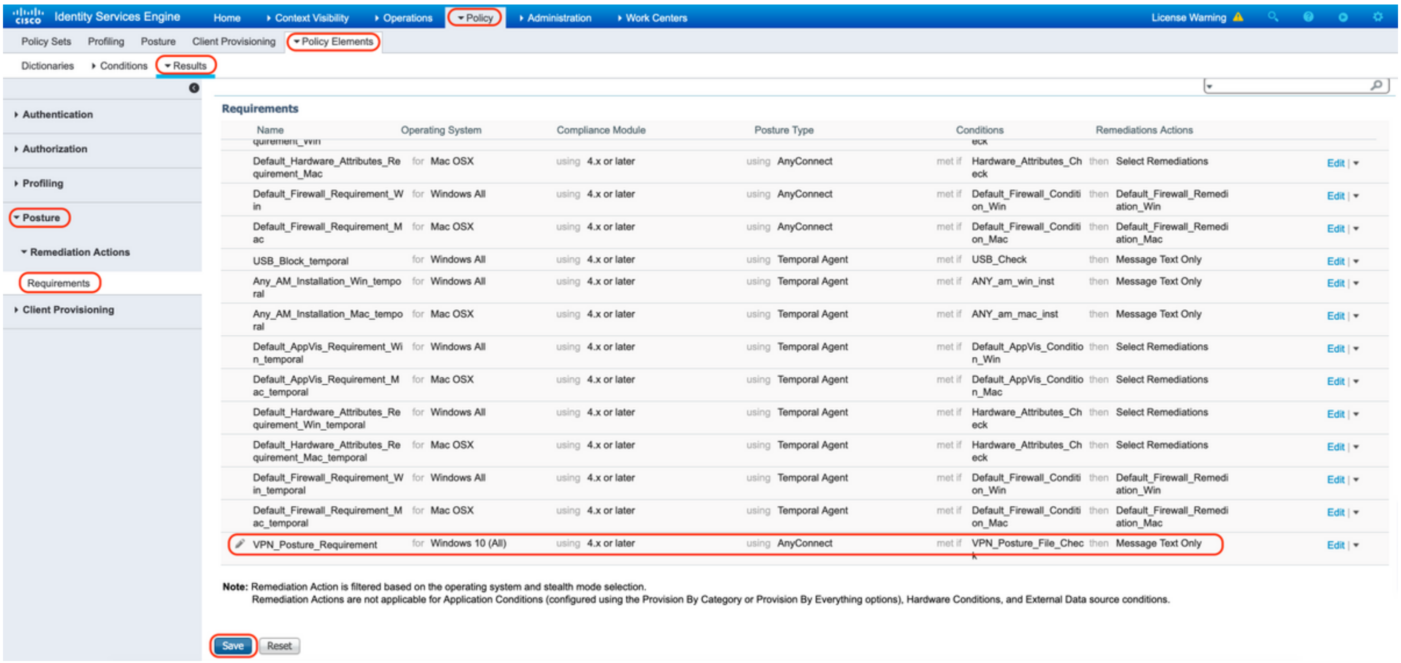
9.建立狀態要求規則

A.導航到「策略>策略元素>結果>狀態>要求」

B.按一下「編輯」，然後選擇「插入新要求」

C.將條件名稱「VPN_Posture_Requirement」、所需作業系統配置為「Windows 10(All)」、合規性模組配置為「4.x或更高版本」、安全狀態型別配置為「Anyconnect」

D.條件為「VPN_Posture_File_Check」（在步驟7中建立），在「Remediations Actions」下，選擇「Action」為「Message Text Only」，然後為代理使用者輸入自定義消息



Requirements

Name	Operating System	Compliance Module	Posture Type	Conditions	Remediations Actions	
quirement_Win				eck		
Default_Hardware_Attributes_Requirement_Mac	for Mac OSX	using 4.x or later	using AnyConnect	met if Hardware_Attributes_Check	then Select Remediations	Edit | ▾
Default_Firewall_Requirement_Win	for Windows All	using 4.x or later	using AnyConnect	met if Default_Firewall_Condition_Win	then Default_Firewall_Remediation_Win	Edit | ▾
Default_Firewall_Requirement_Mac	for Mac OSX	using 4.x or later	using AnyConnect	met if Default_Firewall_Condition_Mac	then Default_Firewall_Remediation_Mac	Edit | ▾
USB_Block_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if USB_Check	then Message Text Only	Edit | ▾
Any_AM_Installation_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if ANY_am_win_inst	then Message Text Only	Edit | ▾
Any_AM_Installation_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if ANY_am_mac_inst	then Message Text Only	Edit | ▾
Default_AppVis_Requirement_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if Default_AppVis_Condition_Win	then Select Remediations	Edit | ▾
Default_AppVis_Requirement_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if Default_AppVis_Condition_Mac	then Select Remediations	Edit | ▾
Default_Hardware_Attributes_Requirement_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if Hardware_Attributes_Check	then Select Remediations	Edit | ▾
Default_Hardware_Attributes_Requirement_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if Hardware_Attributes_Check	then Select Remediations	Edit | ▾
Default_Firewall_Requirement_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if Default_Firewall_Condition_Win	then Default_Firewall_Remediation_Win	Edit | ▾
Default_Firewall_Requirement_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if Default_Firewall_Condition_Mac	then Default_Firewall_Remediation_Mac	Edit | ▾
VPN_Posture_Requirement	for Windows 10 (All)	using 4.x or later	using AnyConnect	met if VPN_Posture_File_Check	then Message Text Only	Edit | ▾

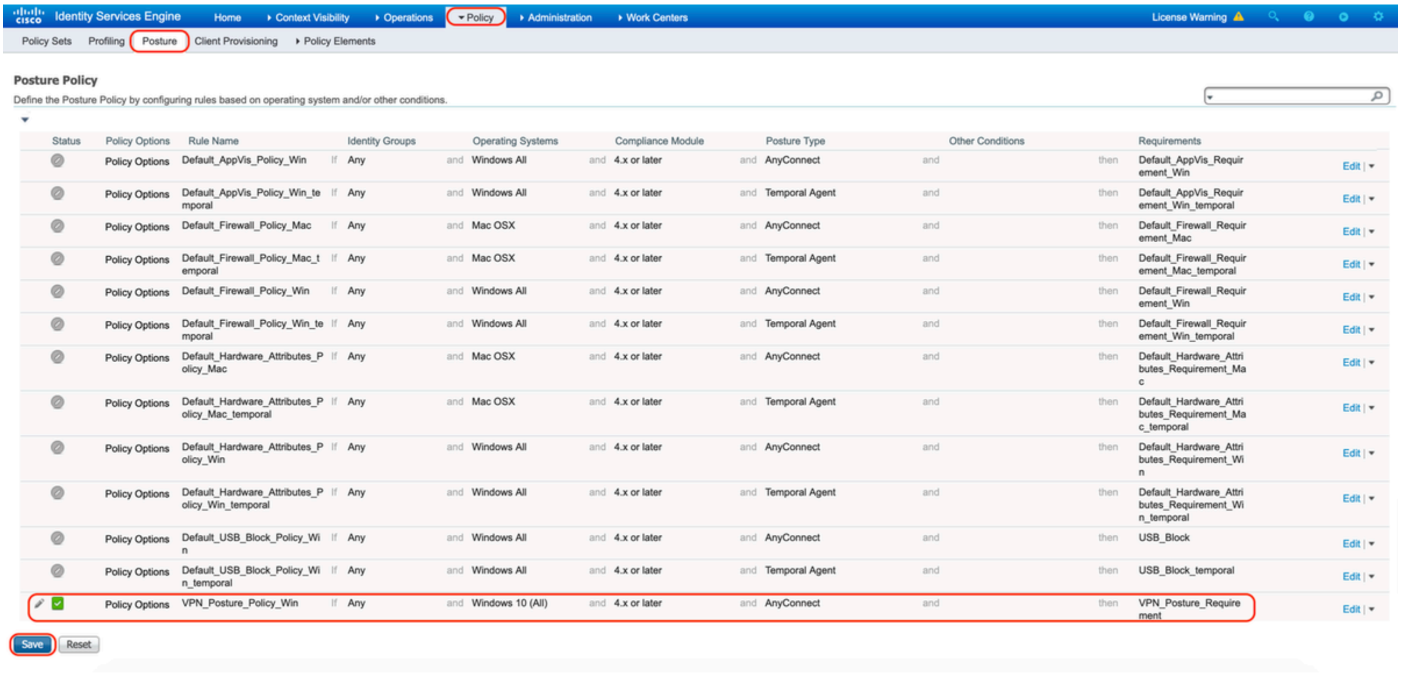
Note: Remediation Action is filtered based on the operating system and stealth mode selection.
Remediation Actions are not applicable for Application Conditions (configured using the Provision By Category or Provision By Everything options), Hardware Conditions, and External Data source conditions.

Save Reset

10.建立狀態策略

A.導航至「策略>狀態」

B.將規則名稱配置為「VPN_Posture_Policy_Win」，將所需的作業系統配置為「Windows 10(All)」，將合規性模組配置為「4.x或更高版本」，將狀態型別配置為「Anyconnect」，將要求配置為「VPN_Posture_Requirement」（如步驟9中所配置）



Posture Policy

Define the Posture Policy by configuring rules based on operating system and/or other conditions.

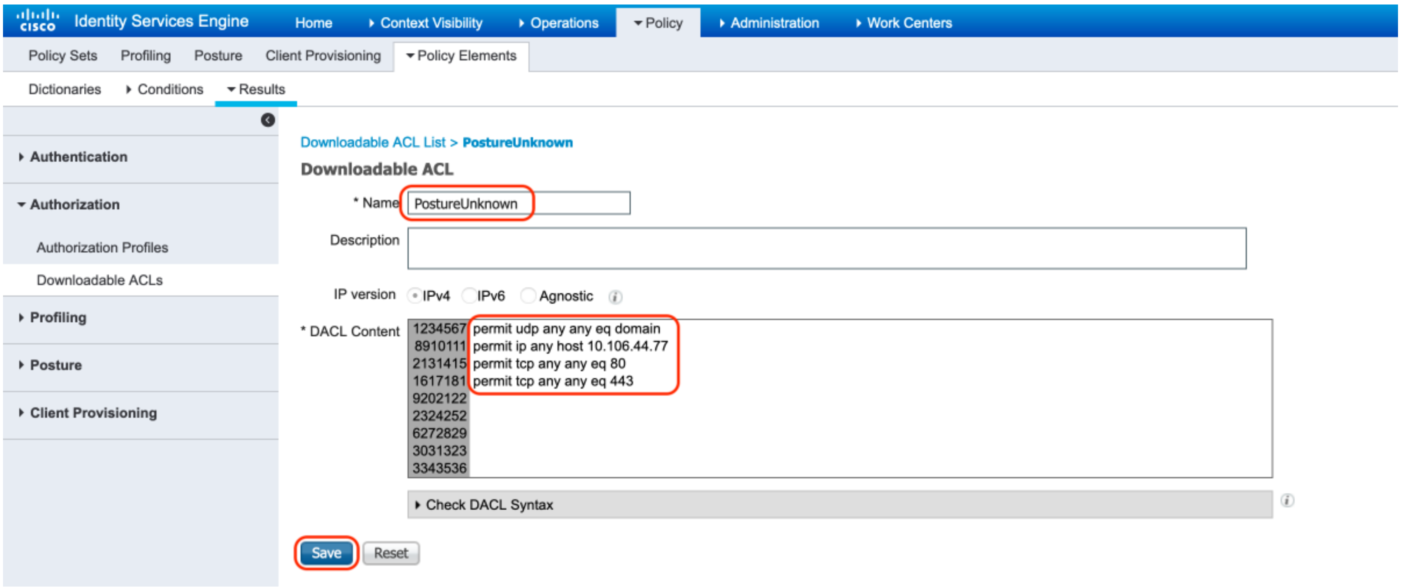
Status	Policy Options	Rule Name	Identity Groups	Operating Systems	Compliance Module	Posture Type	Other Conditions	Requirements	
⊘	Policy Options	Default_AppVis_Policy_Win	If Any	and Windows All	and 4.x or later	and AnyConnect	and	then Default_AppVis_Requirement_Win	Edit | ▾
⊘	Policy Options	Default_AppVis_Policy_Win_temporal	If Any	and Windows All	and 4.x or later	and Temporal Agent	and	then Default_AppVis_Requirement_Win_temporal	Edit | ▾
⊘	Policy Options	Default_Firewall_Policy_Mac	If Any	and Mac OSX	and 4.x or later	and AnyConnect	and	then Default_Firewall_Requirement_Mac	Edit | ▾
⊘	Policy Options	Default_Firewall_Policy_Mac_temporal	If Any	and Mac OSX	and 4.x or later	and Temporal Agent	and	then Default_Firewall_Requirement_Mac_temporal	Edit | ▾
⊘	Policy Options	Default_Firewall_Policy_Win	If Any	and Windows All	and 4.x or later	and AnyConnect	and	then Default_Firewall_Requirement_Win	Edit | ▾
⊘	Policy Options	Default_Firewall_Policy_Win_temporal	If Any	and Windows All	and 4.x or later	and Temporal Agent	and	then Default_Firewall_Requirement_Win_temporal	Edit | ▾
⊘	Policy Options	Default_Hardware_Attributes_Policy_Mac	If Any	and Mac OSX	and 4.x or later	and AnyConnect	and	then Default_Hardware_Attributes_Requirement_Mac	Edit | ▾
⊘	Policy Options	Default_Hardware_Attributes_Policy_Mac_temporal	If Any	and Mac OSX	and 4.x or later	and Temporal Agent	and	then Default_Hardware_Attributes_Requirement_Mac_temporal	Edit | ▾
⊘	Policy Options	Default_Hardware_Attributes_Policy_Win	If Any	and Windows All	and 4.x or later	and AnyConnect	and	then Default_Hardware_Attributes_Requirement_Win	Edit | ▾
⊘	Policy Options	Default_Hardware_Attributes_Policy_Win_temporal	If Any	and Windows All	and 4.x or later	and Temporal Agent	and	then Default_Hardware_Attributes_Requirement_Win_temporal	Edit | ▾
⊘	Policy Options	Default_USB_Block_Policy_Win	If Any	and Windows All	and 4.x or later	and AnyConnect	and	then USB_Block	Edit | ▾
⊘	Policy Options	Default_USB_Block_Policy_Win_temporal	If Any	and Windows All	and 4.x or later	and Temporal Agent	and	then USB_Block_temporal	Edit | ▾
✎ ☑	Policy Options	VPN_Posture_Policy_Win	If Any	and Windows 10 (All)	and 4.x or later	and AnyConnect	and	then VPN_Posture_Requirement	Edit | ▾

11.建立動態ACL(DACL)

導航到「Policy > Policy Elements > Results > Authorization > Downloadable ACL」，然後為不同的狀態建立DACL。

本檔案使用以下DACL。

A.狀態未知：允許到DNS、PSN和HTTP的流量和HTTPS流量



Downloadable ACL List > **PostureUnknown**

Downloadable ACL

* Name: PostureUnknown

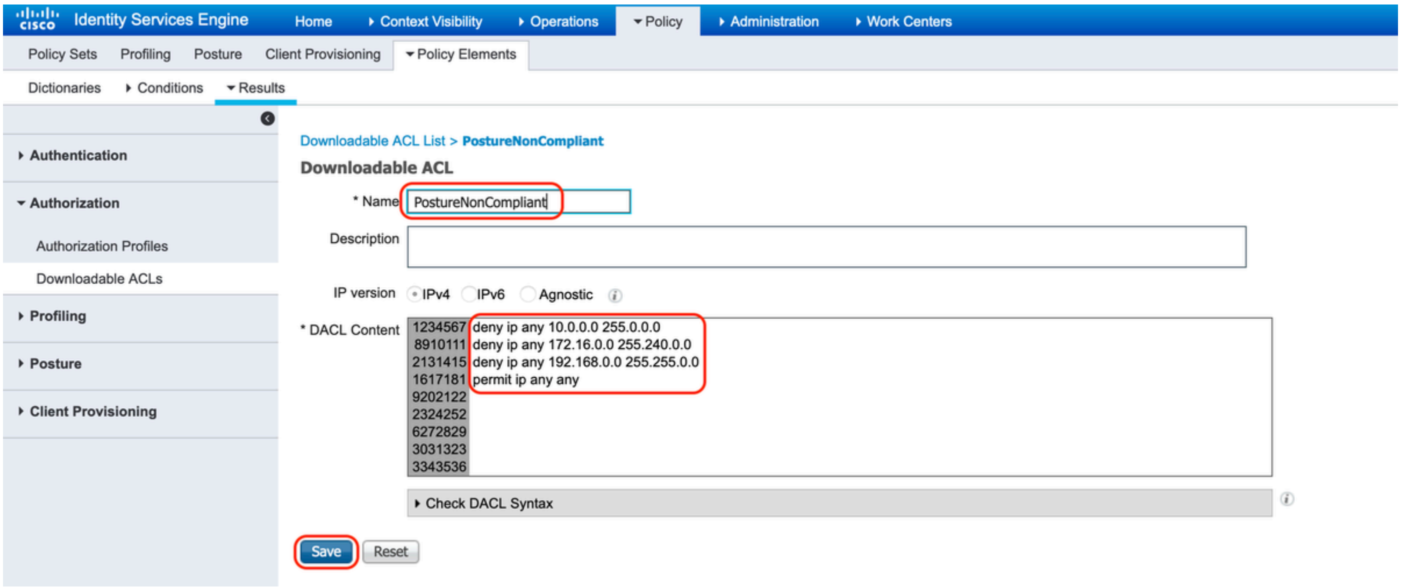
Description:

IP version: ● IPv4 ○ IPv6 ○ Agnostic

* DACL Content:

```
permit udp any any eq domain
permit ip any host 10.106.44.77
permit tcp any any eq 80
permit tcp any any eq 443
```

B.狀態不符合：拒絕訪問專用子網並僅允許網際網路流量



Downloadable ACL

* Name: PostureNonCompliant

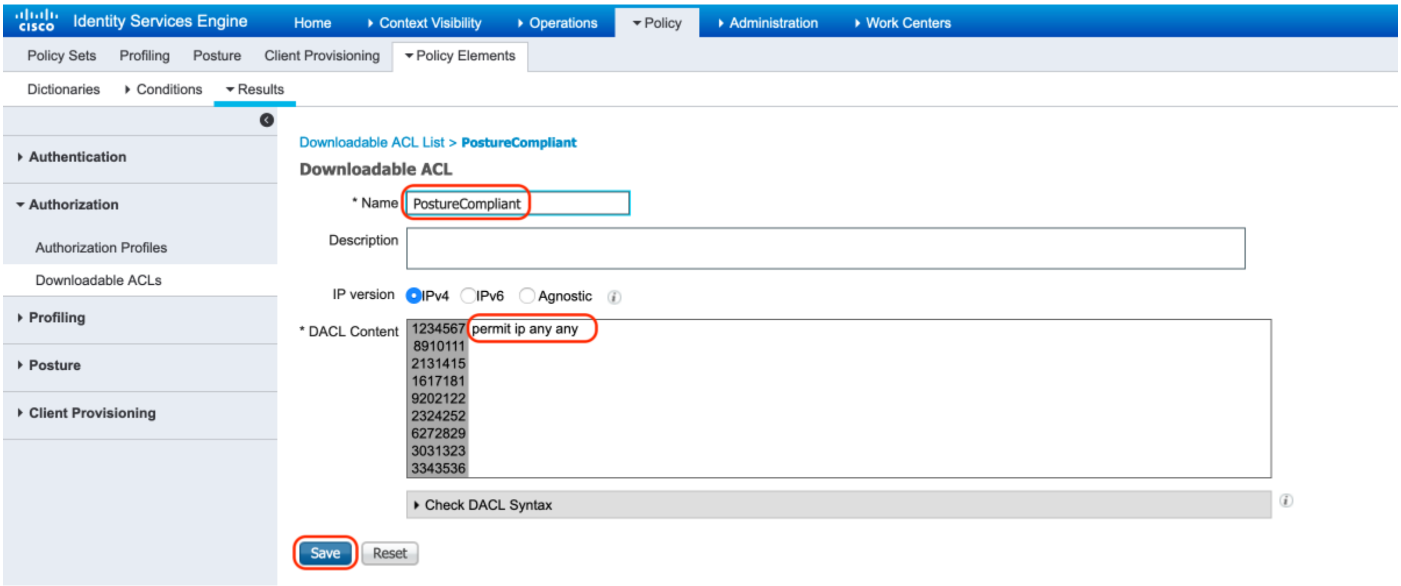
Description:

IP version: ● IPv4 ○ IPv6 ○ Agnostic

* DACL Content:

```
deny ip any 10.0.0.0 255.0.0.0
deny ip any 172.16.0.0 255.240.0.0
deny ip any 192.168.0.0 255.255.0.0
permit ip any any
```

C.符合安全評估標準：允許符合安全評估標準的終端使用者的所有流量



Downloadable ACL

* Name: PostureCompliant

Description:

IP version: ● IPv4 ○ IPv6 ○ Agnostic

* DACL Content:

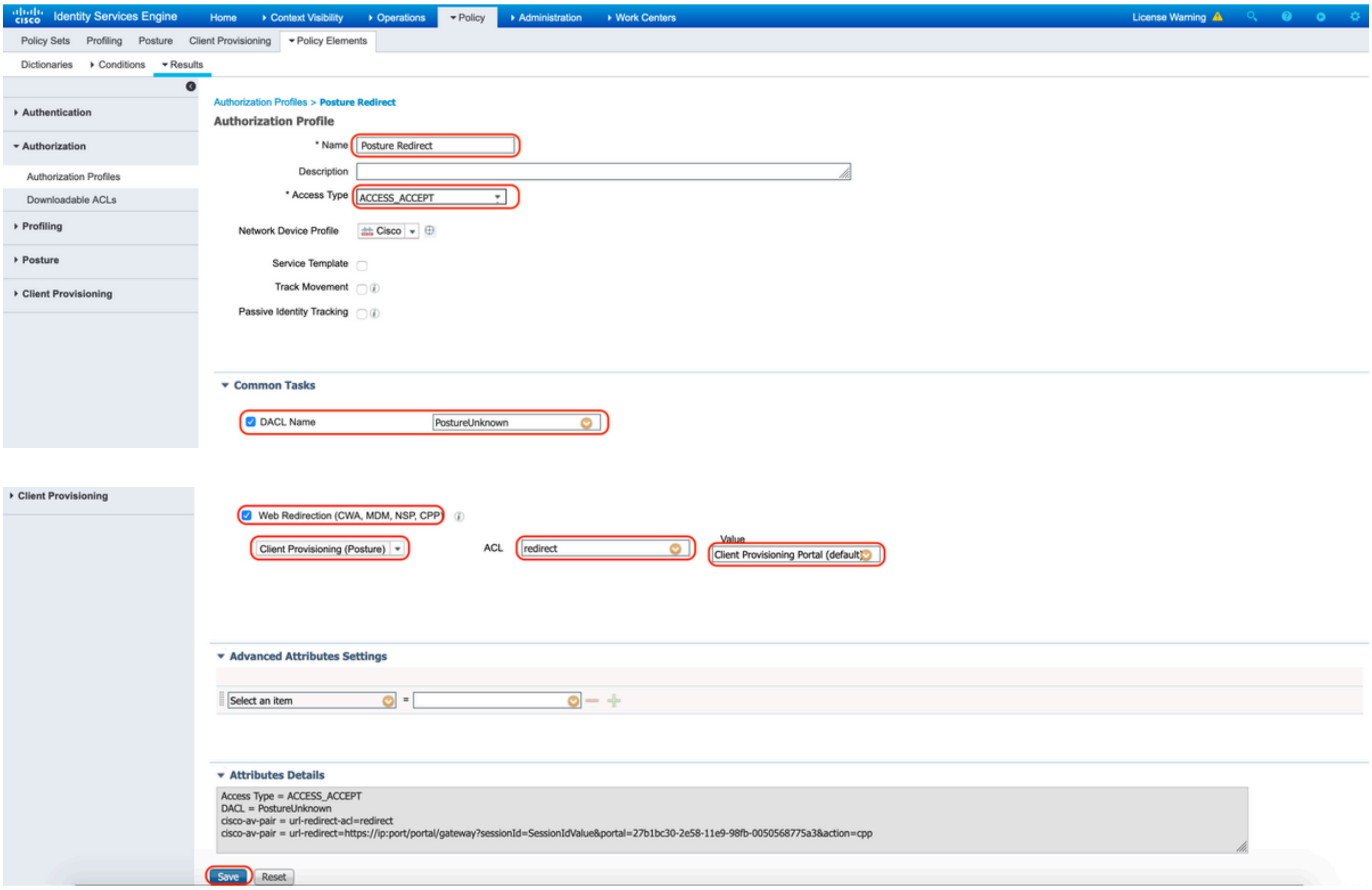
```
permit ip any any
```

12.建立授權配置檔案

導航至「Policy > Policy Elements > Results > Authorization > Authorization Profiles」。

A.未知狀態的授權配置檔案

選擇DACL「PostureUnknown」，檢查Web重定向，選擇Client Provisioning(Posture)，配置Redirect ACL名稱「redirect」（要在ASA上配置），然後選擇客戶端調配門戶（預設）



Authorization Profiles > Posture Redirect

Authorization Profile

* Name: Posture Redirect

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template: □

Track Movement: □

Passive Identity Tracking: □

Common Tasks

☑ DACL Name: PostureUnknown

☑ Web Redirection (CWA, MDM, NSP, CPP)

Client Provisioning (Posture) ACL: redirect Value: Client Provisioning Portal (default)

Advanced Attributes Settings

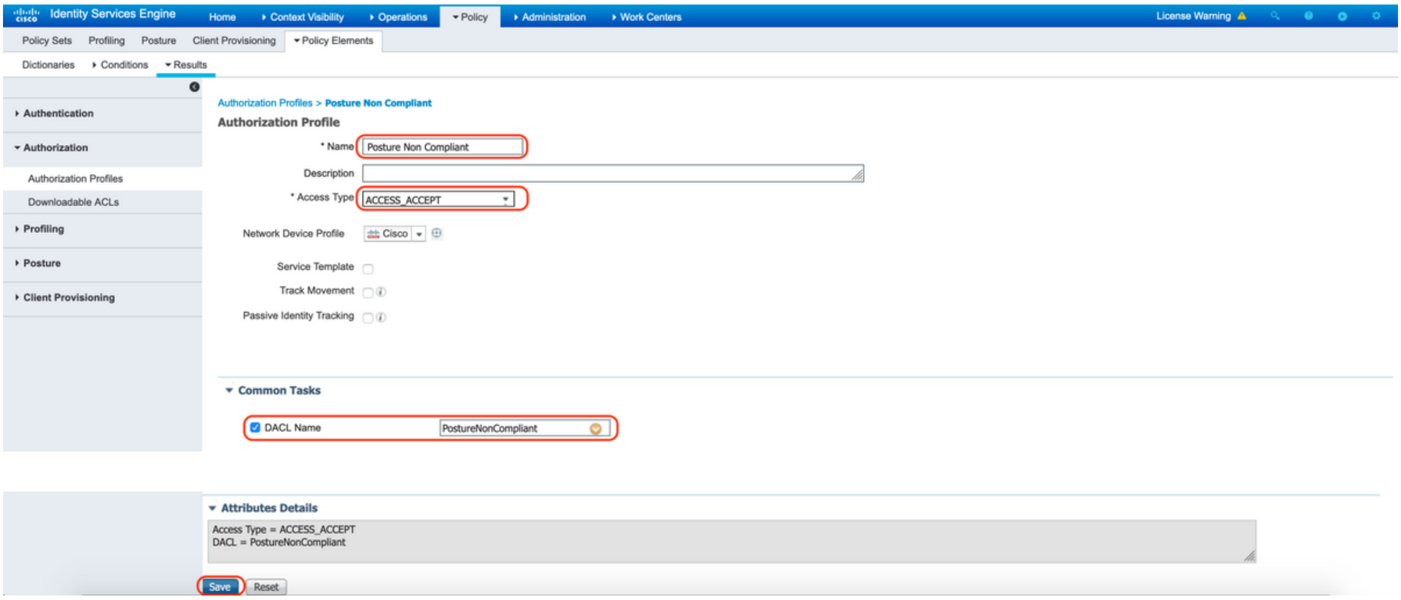
Select an item =

Attributes Details

```
Access Type = ACCESS_ACCEPT
DACL = PostureUnknown
cisco-av-pair = url-redirect-acl=redirect
cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=27b1bc30-2e58-11e9-98fb-0050568775a3&action=cpp
```

B.不符合安全狀態的授權配置檔案

選擇DACL「PostureNonCompliant」以限制對網路的訪問



Authorization Profiles > Posture Non Compliant

Authorization Profile

* Name: Posture Non Compliant

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template: □

Track Movement: □

Passive Identity Tracking: □

Common Tasks

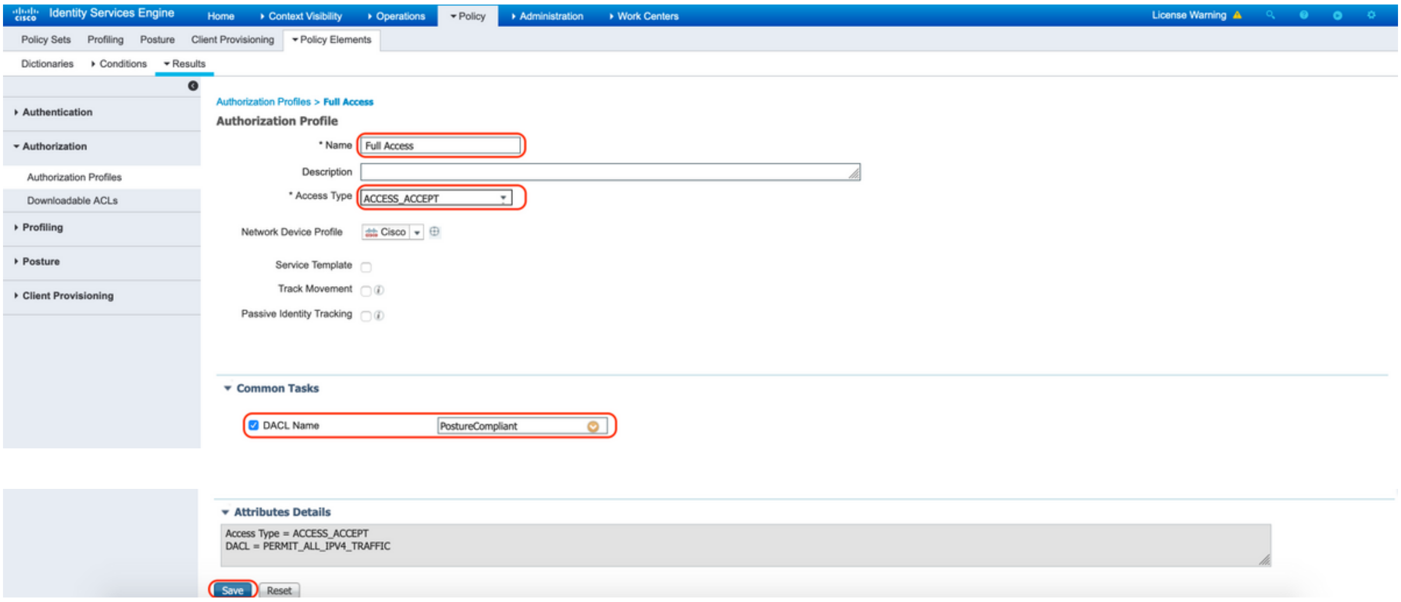
☑ DACL Name: PostureNonCompliant

Attributes Details

```
Access Type = ACCESS_ACCEPT
DACL = PostureNonCompliant
```

C.符合安全狀態的授權配置檔案

選擇DACL「PostureCompliant」以允許完全訪問網路



Authorization Profiles > Full Access

Authorization Profile

- * Name: Full Access
- Description:
- * Access Type: ACCESS_ACCEPT
- Network Device Profile: Cisco
- Service Template: □
- Track Movement: □
- Passive Identity Tracking: □

Common Tasks

☑ DACL Name: PostureCompliant

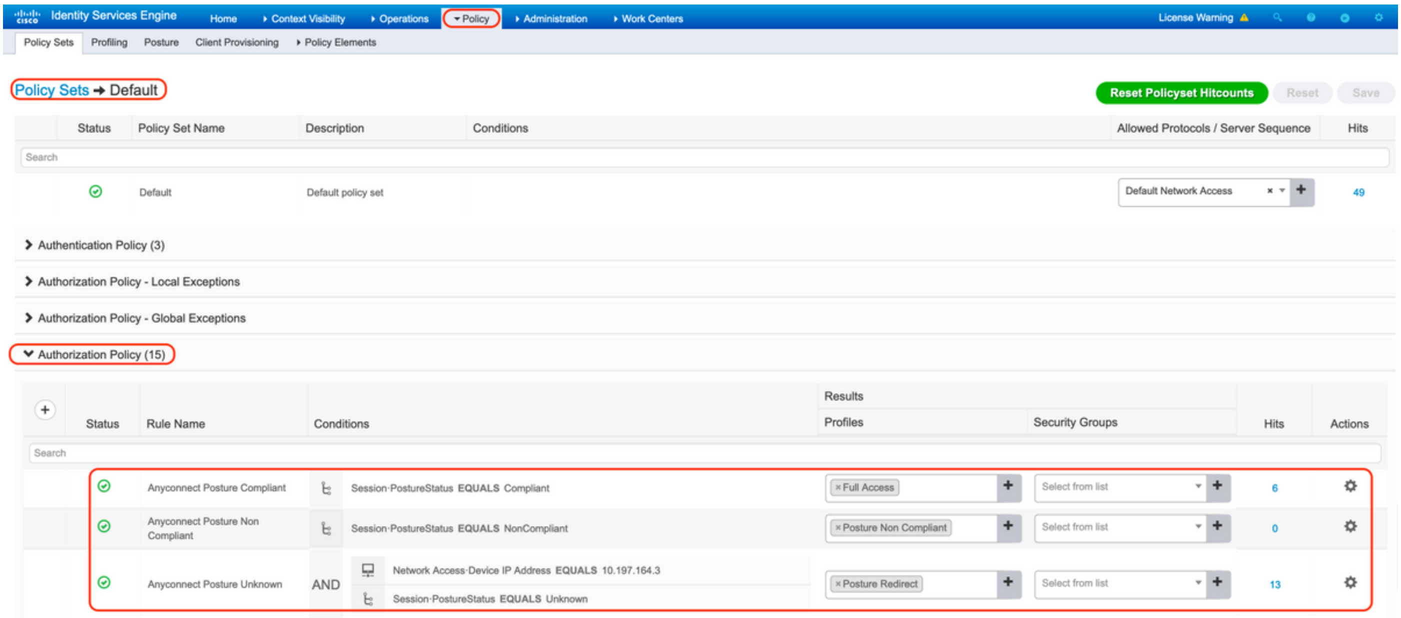
Attributes Details

```
Access Type = ACCESS_ACCEPT
DACL = PERMIT_ALL_IPV4_TRAFFIC
```

12.配置授權策略

使用在上一步中配置的授權配置檔案為安全評估合規性、安全評估不合規性和安全評估未知配置3個授權策略。

常見條件「會話：狀態狀態」用於確定每個策略的結果



Policy Sets → Default

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	49

- Authentication Policy (3)
- Authorization Policy - Local Exceptions
- Authorization Policy - Global Exceptions
- Authorization Policy (15)

Status	Rule Name	Conditions	Results: Profiles	Results: Security Groups	Hits	Actions
✓	Anyconnect Posture Compliant	Session·PostureStatus EQUALS Compliant	Full Access	Select from list	6	⚙
✓	Anyconnect Posture Non Compliant	Session·PostureStatus EQUALS NonCompliant	Posture Non Compliant	Select from list	0	⚙
✓	Anyconnect Posture Unknown	AND Network Access·Device IP Address EQUALS 10.197.164.3 Session·PostureStatus EQUALS Unknown	Posture Redirect	Select from list	13	⚙

驗證

使用本節內容，確認您的組態是否正常運作。

要驗證使用者是否成功通過身份驗證，請在ASA上運行以下命令。

<#root>

```
firebird(config)#

show vpn-sess detail anyconnect



Session Type: AnyConnect Detailed

Username     : _585b5291f01484dfd16f394be7031d456d314e3e62
Index        : 125
Assigned IP  : explorer.cisco.com     Public IP    : 10.197.243.143
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES-GCM-256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA384
Bytes Tx     : 16404                  Bytes Rx     : 381
Pkts Tx      : 16                     Pkts Rx      : 6
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : DfltGrpPolicy                Tunnel Group :

TG_SAML

Login Time   : 07:05:45 UTC Sun Jun 14 2020
Duration     : 0h:00m:16s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 0ac5a4030007d0005ee5cc49
Security Grp : none

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
  Tunnel ID    : 125.1
  Public IP    : 10.197.243.143
  Encryption   : none                   Hashing      : none
  TCP Src Port : 57244                  TCP Dst Port : 443
  Auth Mode    : SAML
  Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
  Client OS    : win
  Client OS Ver: 10.0.15063
  Client Type  : AnyConnect
  Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.8.03052
  Bytes Tx     : 7973                   Bytes Rx     : 0
  Pkts Tx      : 6                      Pkts Rx      : 0
  Pkts Tx Drop : 0                      Pkts Rx Drop : 0

SSL-Tunnel:
  Tunnel ID    : 125.2
  Assigned IP  : explorer.cisco.com     Public IP    : 10.197.243.143
  Encryption   : AES-GCM-256            Hashing      : SHA384
  Ciphersuite  : ECDHE-RSA-AES256-GCM-SHA384
  Encapsulation: TLSv1.2                TCP Src Port : 57248
  TCP Dst Port : 443                    Auth Mode    : SAML
  Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
  Client OS    : Windows
  Client Type  : SSL VPN Client
  Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.8.03052
  Bytes Tx     : 7973                   Bytes Rx     : 0
  Pkts Tx      : 6                      Pkts Rx      : 0
  Pkts Tx Drop : 0                      Pkts Rx Drop : 0
  Filter Name  : #ACSACL#-IP-PostureUnknown-5ee45b05

DTLS-Tunnel:
  Tunnel ID    : 125.3
  Assigned IP  : explorer.cisco.com     Public IP    : 10.197.243.143
  Encryption   : AES-GCM-256            Hashing      : SHA384
  Ciphersuite  : ECDHE-ECDSA-AES256-GCM-SHA384
  Encapsulation: DTLSv1.2               UDP Src Port : 49175
  UDP Dst Port : 443                    Auth Mode    : SAML
  Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
  Client OS    : Windows
  Client Type  : DTLS VPN Client
  Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.8.03052
  Bytes Tx     : 458                    Bytes Rx     : 381
  Pkts Tx      : 4                      Pkts Rx      : 6
  Pkts Tx Drop : 0                      Pkts Rx Drop : 0
  Filter Name  :
```

```
#ACSACL#-IP-PostureUnknown-5ee45b05
```

```
ISE Posture:
  Redirect URL : https://ise261.pusaxena.local:8443/portal/gateway?sessionId=0ac5a4030007d0005ee5cc49&po
  Redirect ACL : redirect
```

狀態評估完成後，使用者訪問將更改為完全訪問，如欄位「Filter Name」中推送的DACL中所示

<#root>

```
firebird(config)#
```

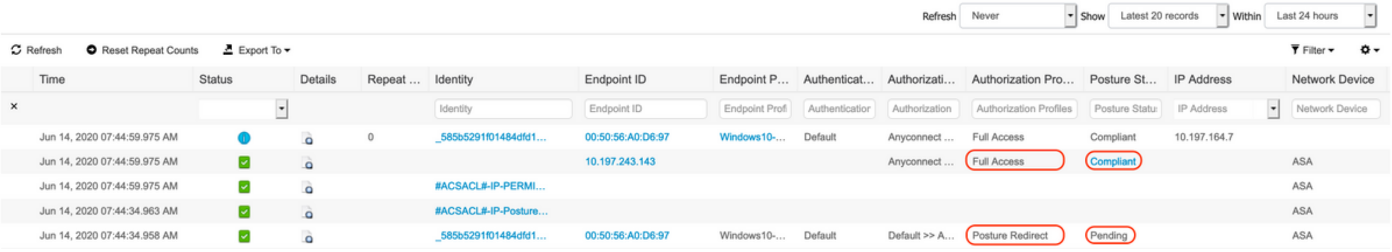
```
show vpn-sess detail anyconnect
```

```
Session Type: AnyConnect Detailed

Username     : _585b5291f01484dfd16f394be7031d456d314e3e62
Index        : 125
Assigned IP  : explorer.cisco.com     Public IP    : 10.197.243.143
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES-GCM-256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA384
Bytes Tx     : 16404                  Bytes Rx     : 381
Pkts Tx      : 16                     Pkts Rx      : 6
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
```

```
Group Policy : DfltGrpPolicy                Tunnel Group :

TG_SAML

Login Time   : 07:05:45 UTC Sun Jun 14 2020
Duration     : 0h:00m:36s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                     VLAN         : none
Audt Sess ID : 0ac5a4030007d0005ee5cc49
Security Grp : none

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
  Tunnel ID    : 125.1
  Public IP    : 10.197.243.143
  Encryption   : none                   Hashing      : none
  TCP Src Port : 57244                  TCP Dst Port : 443
  Auth Mode    : SAML
  Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
  Client OS    : win
  Client OS Ver: 10.0.15063
  Client Type  : AnyConnect
  Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.8.03052
  Bytes Tx     : 7973                   Bytes Rx     : 0
  Pkts Tx      : 6                      Pkts Rx      : 0
  Pkts Tx Drop : 0                      Pkts Rx Drop : 0

SSL-Tunnel:
  Tunnel ID    : 125.2
  Assigned IP  : explorer.cisco.com     Public IP    : 10.197.243.143
  Encryption   : AES-GCM-256            Hashing      : SHA384
  Ciphersuite  : ECDHE-RSA-AES256-GCM-SHA384
  Encapsulation: TLSv1.2                TCP Src Port : 57248
  TCP Dst Port : 443                    Auth Mode    : SAML
  Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
  Client OS    : Windows
  Client Type  : SSL VPN Client
  Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.8.03052
  Bytes Tx     : 7973                   Bytes Rx     : 0
  Pkts Tx      : 6                      Pkts Rx      : 0
  Pkts Tx Drop : 0                      Pkts Rx Drop : 0
  Filter Name  : #ACSACL#-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3

DTLS-Tunnel:
  Tunnel ID    : 125.3
  Assigned IP  : explorer.cisco.com     Public IP    : 10.197.243.143
  Encryption   : AES-GCM-256            Hashing      : SHA384
  Ciphersuite  : ECDHE-ECDSA-AES256-GCM-SHA384
  Encapsulation: DTLSv1.2               UDP Src Port : 49175
  UDP Dst Port : 443                    Auth Mode    : SAML
  Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
  Client OS    : Windows
  Client Type  : DTLS VPN Client
  Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.8.03052
  Bytes Tx     : 458                    Bytes Rx     : 381
  Pkts Tx      : 4                      Pkts Rx      : 6
  Pkts Tx Drop : 0                      Pkts Rx Drop : 0
  Filter Name  :

#ACSACL#-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3
```

要驗證是否在ISE上成功執行授權，請導航至「操作> RADIUS >即時日誌」

本節顯示與授權使用者相關的資訊，如身份、授權配置檔案、授權策略和狀態資訊。



Refresh: Never　Show: Latest 20 records　Within: Last 24 hours

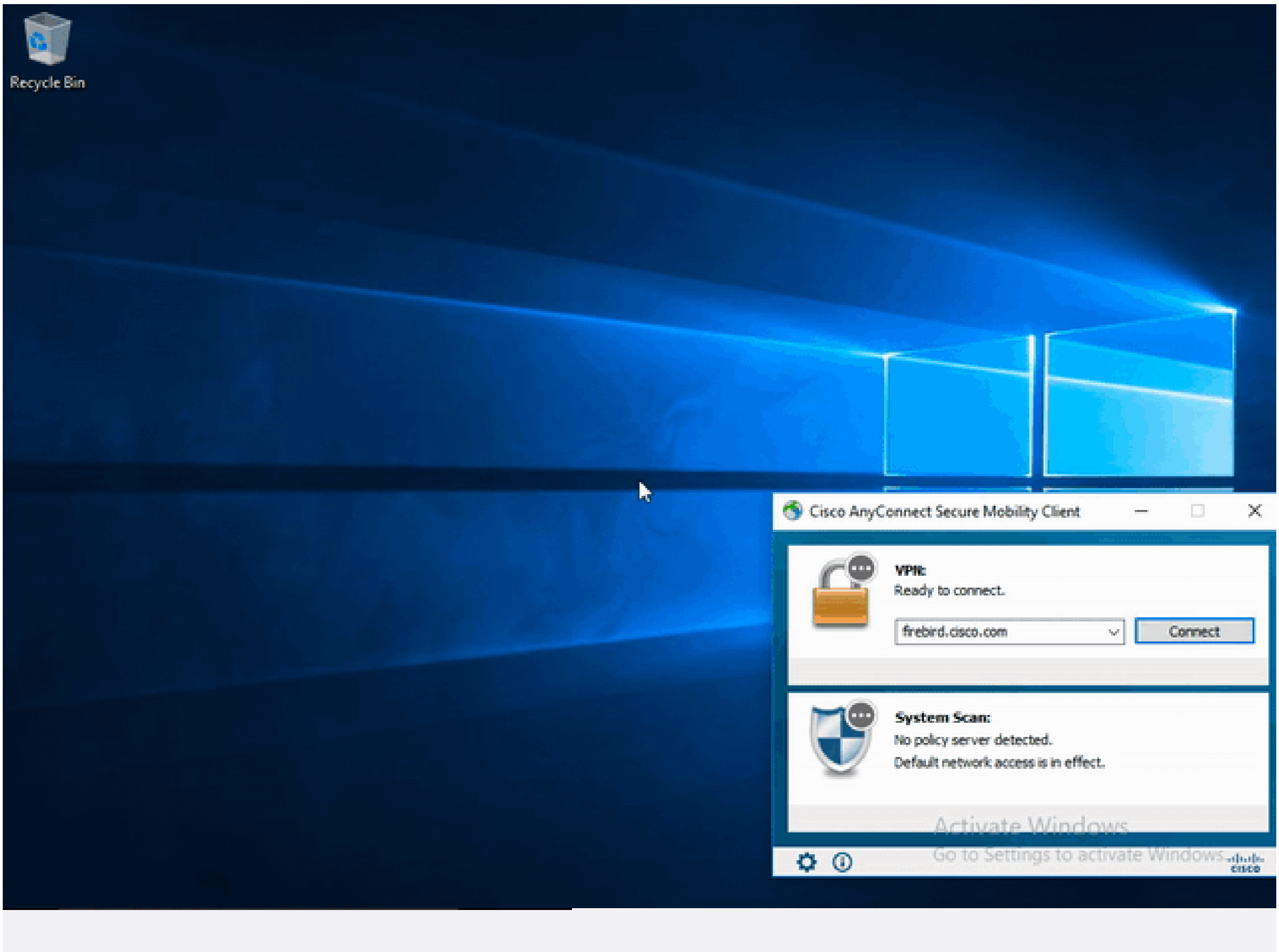
Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorization Pro...	Posture St...	IP Address	Network Device
Jun 14, 2020 07:44:59.975 AM	●	🔍	0	_585b5291f01484dfd1...	00:50:56:A0:D6:97	Windows10-...	Default	Anyconnect ...	Full Access	Compliant	10.197.164.7	
Jun 14, 2020 07:44:59.975 AM	✓	🔍			10.197.243.143			Anyconnect ...	Full Access	Compliant		ASA
Jun 14, 2020 07:44:59.975 AM	✓	🔍		#ACSACL#-IP-PERMI...								ASA
Jun 14, 2020 07:44:34.963 AM	✓	🔍		#ACSACL#-IP-Posture...								ASA
Jun 14, 2020 07:44:34.958 AM	✓	🔍		_585b5291f01484dfd1...	00:50:56:A0:D6:97	Windows10-...	Default	Default >> A...	Posture Redirect	Pending		ASA

注意：有關ISE上的其他狀態驗證，請參閱以下文檔：
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215236-ise-posture-over-anyconnect-remote-acces.html#anc7

要驗證Duo Admin Portal的身份驗證狀態，請按一下顯示身份驗證日誌的管理面板左側的「報告」。
更多詳細資訊：https://duo.com/docs/administration#reports

要檢視Duo Access Gateway的調試日誌記錄，請使用以下連結：
https://help.duo.com/s/article/1623?language=en_US

使用者體驗



Recycle Bin
Cisco AnyConnect Secure Mobility Client
VPN:
Ready to connect.
firebird.cisco.com
Connect
System Scan:
No policy server detected.
Default network access is in effect.
Activate Windows
Go to Settings to activate Windows.

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

附註：使用 debug 指令之前，請先參閱有關 Debug 指令的重要資訊。

注意：在ASA上，您可以設定各種調試級別；預設情況下，使用級別1。如果更改調試級別，調試的詳細程度可能會增加。請謹慎執行此操作，尤其是在生產環境中。

大多數SAML故障排除都會涉及配置錯誤，通過檢查SAML配置或運行調試可以發現該錯誤。

「debug webvpn saml 255」可用於排除大多數問題，但在此調試不提供有用資訊的情況下，可以運行其他調試：

```
debug webvpn 255
debug webvpn anyconnect 255
debug webvpn session 255
debug webvpn request 255
```

要排除ASA上的身份驗證和授權問題，請使用以下debug命令：

```
debug radius all
debug aaa authentication
debug aaa authorization To troubleshoot Posture related issues on ISE, set the following attributes to 
```

```
posture (ise-psc.log)
portal (guest.log)
provisioning (ise-psc.log)
runtime-AAA (prrt-server.log)
nsf (ise-psc.log)
nsf-session (ise-psc.log)
swiss (ise-psc.log)
```

注意：有關詳細狀態流程和AnyConnect和ISE故障排除，請參閱以下連結：
ISE終端安全評估樣式比較，用於前期和後期2.2

解釋Duo Access Gateway調試日誌並對其進行故障排除
https://help.duo.com/s/article/5016?language=en_US

相關資訊

https://www.youtube.com/watch?v=W6bE2GTU0Is&
https://duo.com/docs/cisco#asa-ssl-vpn-using-saml
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215236-ise-posture-over-anyconnect-remote-acces.html#anc0

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。