在Windows上透過ISE 3.3配置和部署安全客戶端NAM配置檔案

目錄

簡介

背景資訊

必要條件

- 需求
- 採用元件

組態

- 網路圖表
- 資料流程
- 設定交換器
- 下載安全客戶端軟體套件

ISE 組態

- 步驟 1.在ISE上傳包
- 步驟 2.從設定檔編輯器工具建立NAM設定檔
- 步驟 3.在ISE上上傳NAM配置檔案
- 步驟 4.建立狀態配置檔案
- 步驟 5.建立代理配置
- 步驟 6.客戶端調配策略
- 步驟 7.狀態策略
- 步驟 8.增加網路裝置
- 步驟 9.授權配置檔案
- 步驟 10.允許的協定
- 步驟 11.Active Directory
- 步驟 12.策略集

驗證

- 步驟 1.從ISE下載並安裝安全客戶端狀態/NAM模組
- 步驟 2.EAP-FAST
- 步驟 3.狀態掃描

疑難排解

- 步驟 1.NAM配置檔案
- 步驟 2.NAM擴展日誌記錄
- 步驟3.在交換機上進行調試
- 步驟 4.ISE上的調試

相關資訊

簡介

本文檔介紹如何透過身份服務引擎(ISE)部署Cisco Secure Client Network Access Manager (NAM)配置檔案。

背景資訊

EAP-FAST驗證分兩個階段進行。在第一階段，EAP-FAST使用TLS握手來提供並使用型別長度值(TLV)對象驗證金鑰交換以建立受保護的隧道。這些TLV對象用於在客戶端和伺服器之間傳遞與身份驗證相關的資料。隧道建立後，第二階段從客戶端和ISE節點進行進一步通話以建立所需的身份驗證和授權策略開始。

NAM配置配置檔案設定為使用EAP-FAST作為身份驗證方法，並且可用於管理定義的網路。
此外，可以在NAM配置配置檔案中配置電腦和使用者連線型別。
企業Windows裝置使用具有狀態檢查的NAM獲得完整的企業訪問許可權。
個人Windows裝置使用相同的NAM配置訪問受限制的網路。

本文檔提供有關使用網路部署透過身份服務引擎(ISE)終端安全評估門戶部署思科安全客戶端網路訪問管理器(NAM)配置檔案的說明，以及終端安全評估合規性檢查。

必要條件

需求

思科建議您瞭解以下主題：

- 身分識別服務引擎 (ISE)
- AnyConnect NAM和配置檔案編輯器
- 狀態策略
- 適用於802.1x服務的Cisco Catalyst配置

採用元件

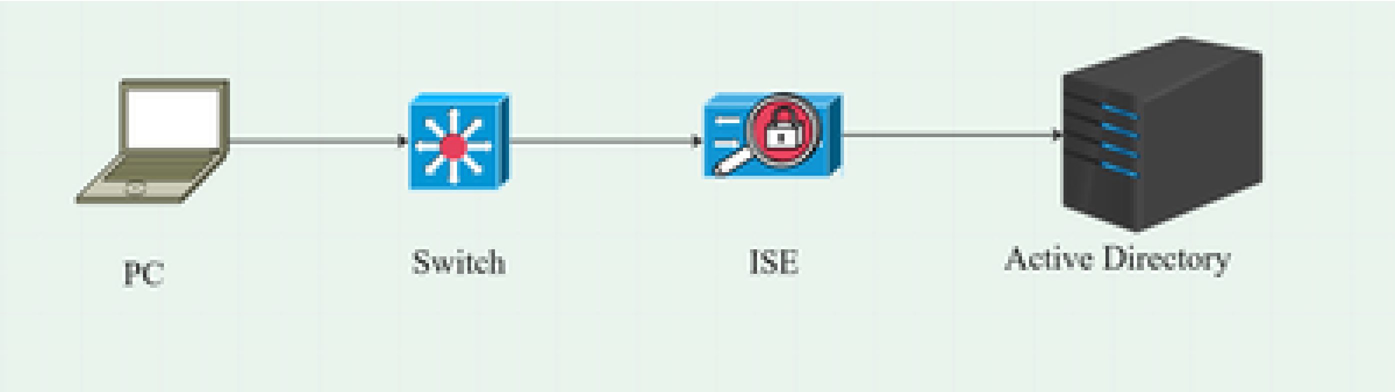
本文中的資訊係根據以下軟體和硬體版本：

- Cisco ISE版本3.3及更高版本
- Windows 10與Cisco Secure Mobility Client 5.1.4.74及更高版本
- Cisco Catalyst 9200交換機，帶軟體Cisco IOS® XE 17.6.5及更高版本
- Active Directory 2016

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

組態

網路圖表



資料流程

當PC連線到網路時，ISE提供重定向到終端安全評估門戶的授權策略。
PC上的http流量重定向到ISE客戶端調配頁面，其中從ISE下載NSA應用。
然後，NSA會在PC上安裝安全客戶端代理模組。
代理安裝完成後，代理下載在ISE上配置的狀態配置檔案和NAM配置檔案。
安裝NAM模組會觸發PC上的重新啟動。
重新啟動後，NAM模組根據NAM配置檔案執行EAP-FAST身份驗證。
然後觸發安全評估掃描，並根據ISE安全評估策略檢查合規性。

設定交換器

為dot1x身份驗證和重定向配置接入交換機。

```
aaa new-model

aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
aaa server radius dynamic-author
客戶端10.127.197.53伺服器金鑰Qwerty123
auth-type any

aaa session-id common
ip radius source-interface Vlan1000
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server attribute 31 mac format ietf upper-case
radius伺服器RAD1
address ipv4 <ISE server IP> auth-port 1812 acct-port 1813
key <secret-key>

dot1x system-auth-control
```

為要重定向到ISE客戶端調配門戶的使用者配置重定向ACL。

```
ip access-list extended redirect-acl
10 deny udp any any eq域
20 deny tcp any any eq域
30 deny udp any eq bootpc any eq bootps
40 deny ip any host <ISE伺服器IP>
50 permit tcp any any eq www
60 permit tcp any any eq 443
```

在交換機上啟用裝置跟蹤和http重定向。

```
裝置跟蹤策略<裝置跟蹤策略名稱>
 追蹤啟用
interface <interface name>
 device-tracking attach-policy <裝置跟蹤策略名稱>

ip http server
ip http secure-server
```

下載安全客戶端軟體套件

從software.cisco.com手動下載配置檔案編輯器、安全客戶端Windows和合規性模組Web部署檔案

在產品名稱搜尋欄中，鍵入Secure Client 5。

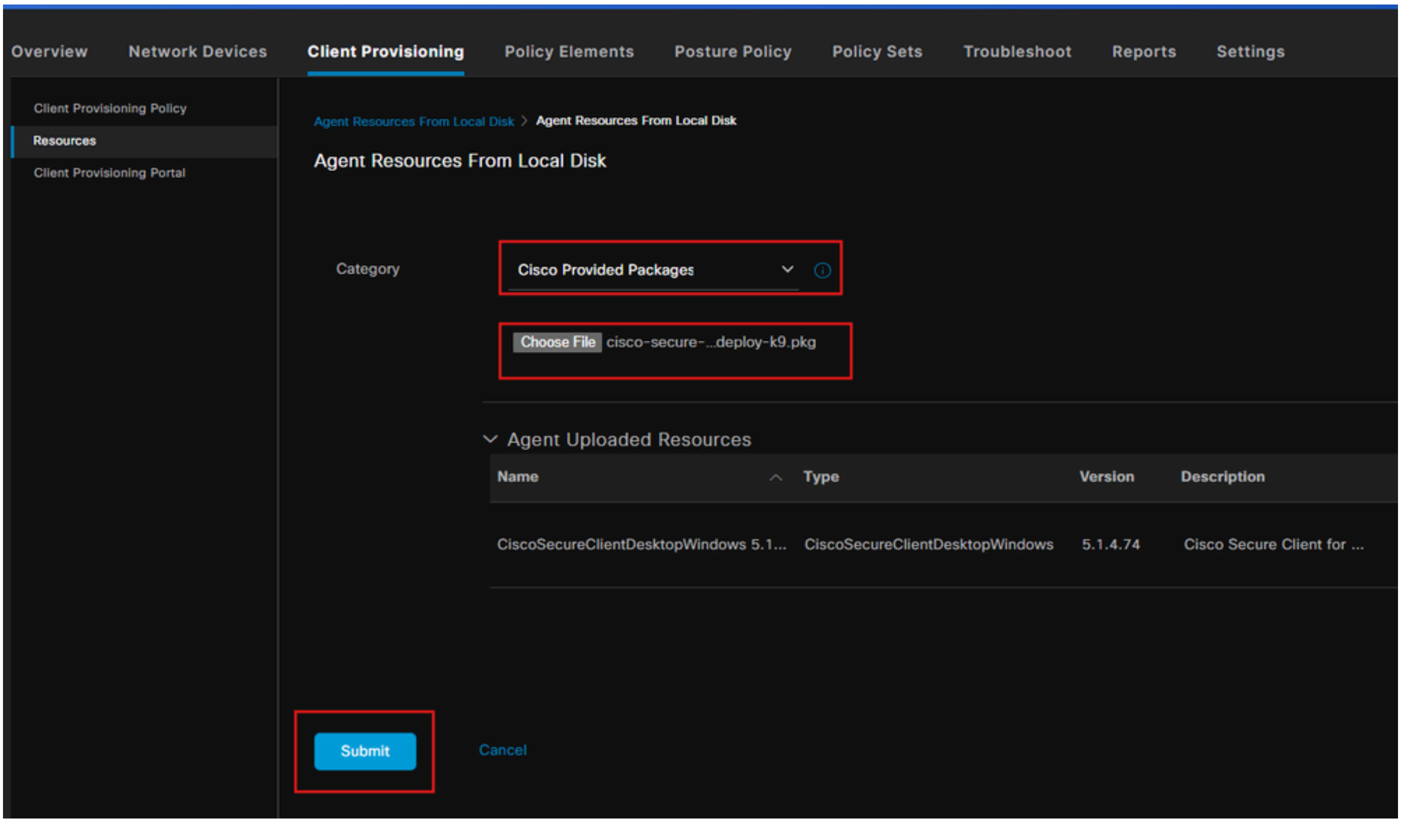
「下載首頁」(Downloads Home) >「安全」(Security) >「端點安全」(Endpoint Security) >「安全客戶端」(Secure Client)（包括AnyConnect）>「安全客戶端5」(Secure Client 5) >「AnyConnect VPN客戶端軟體」(AnyConnect VPN Client Software)

- cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg
- cisco-secure-client-win-4.3.4164.8192-isecompliance-webdeploy-k9.pkg
- tools-cisco-secure-client-win-5.1.4.74-profileeditor-k9.msi

ISE 組態

步驟 1.在ISE上傳包

要在ISE上上傳安全客戶端和合規性模組Web部署包，請導航到Workcenter > Posture > Client Provisioning > Resources > Add > Agent Resources from Local Disk。



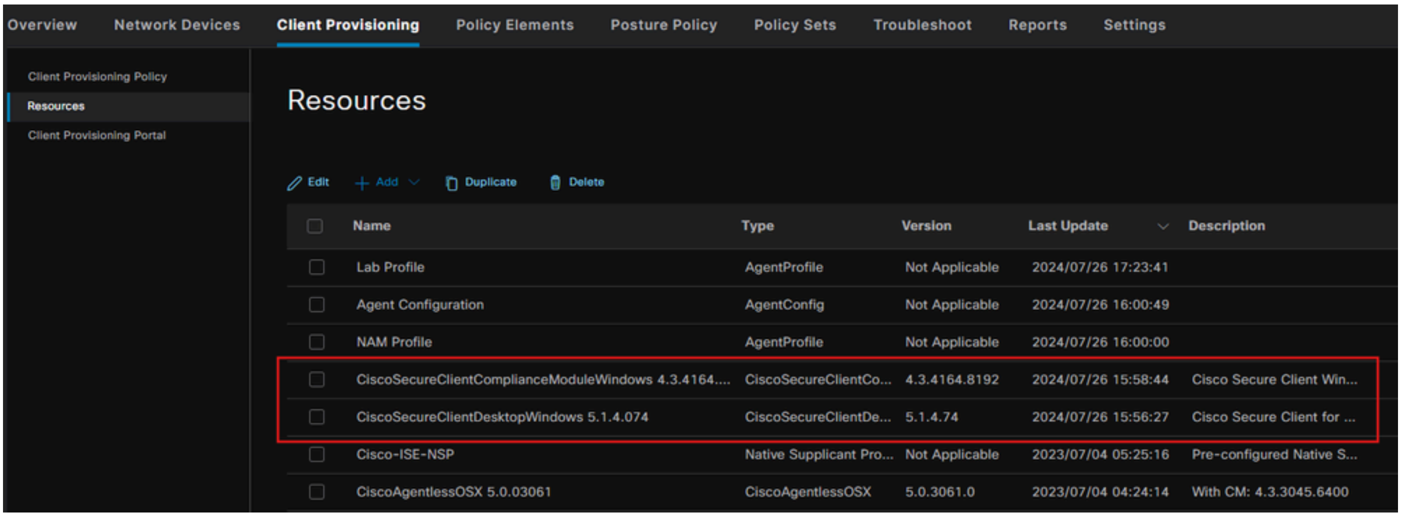
Agent Resources From Local Disk

Category: Cisco Provided Packages

Choose File cisco-secure-...deploy-k9.pkg

Agent Uploaded Resources

Name	Type	Version	Description
CiscoSecureClientDesktopWindows 5.1...	CiscoSecureClientDesktopWindows	5.1.4.74	Cisco Secure Client for ...



Resources

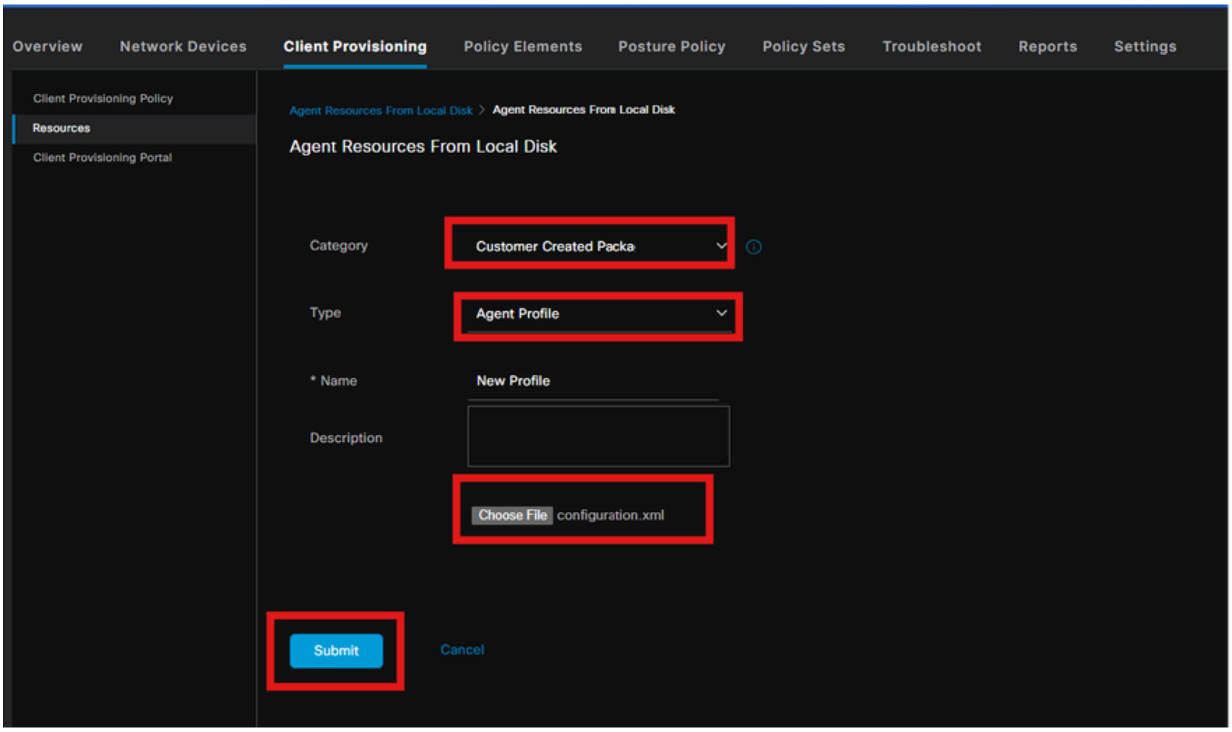
□	Name	Type	Version	Last Update	Description
□	Lab Profile	AgentProfile	Not Applicable	2024/07/26 17:23:41	
□	Agent Configuration	AgentConfig	Not Applicable	2024/07/26 16:00:49	
□	NAM Profile	AgentProfile	Not Applicable	2024/07/26 16:00:00	
□	CiscoSecureClientComplianceModuleWindows 4.3.4164....	CiscoSecureClientCo...	4.3.4164.8192	2024/07/26 15:58:44	Cisco Secure Client Win...
□	CiscoSecureClientDesktopWindows 5.1.4.074	CiscoSecureClientDe...	5.1.4.74	2024/07/26 15:56:27	Cisco Secure Client for ...
□	Cisco-ISE-NSP	Native Supplicant Pro...	Not Applicable	2023/07/04 05:25:16	Pre-configured Native S...
□	CiscoAgentlessOSX 5.0.03061	CiscoAgentlessOSX	5.0.3061.0	2023/07/04 04:24:14	With CM: 4.3.3045.6400

步驟 2.從設定檔編輯器工具建立NAM設定檔

有關如何配置NAM配置檔案的資訊，請參閱本指南配置安全客戶端NAM配置檔案。

步驟 3.在ISE上上傳NAM配置檔案

要將NAM配置檔案「Configuration.xml」作為代理配置檔案上傳到ISE上，請導航到Client Provisioning > Resources > Agent Resources From Local Disk。



Agent Resources From Local Disk

Category: Customer Created Packa

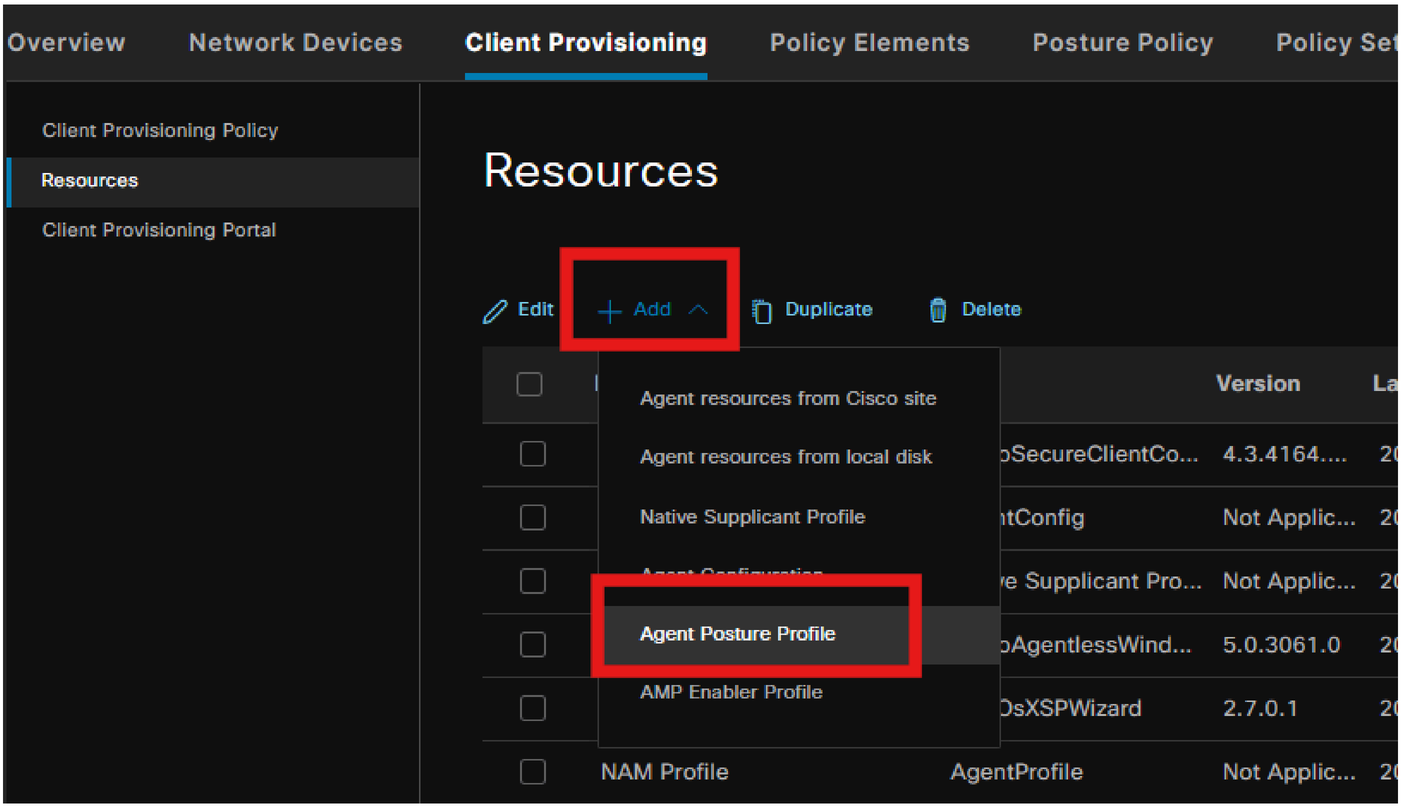
Type: Agent Profile

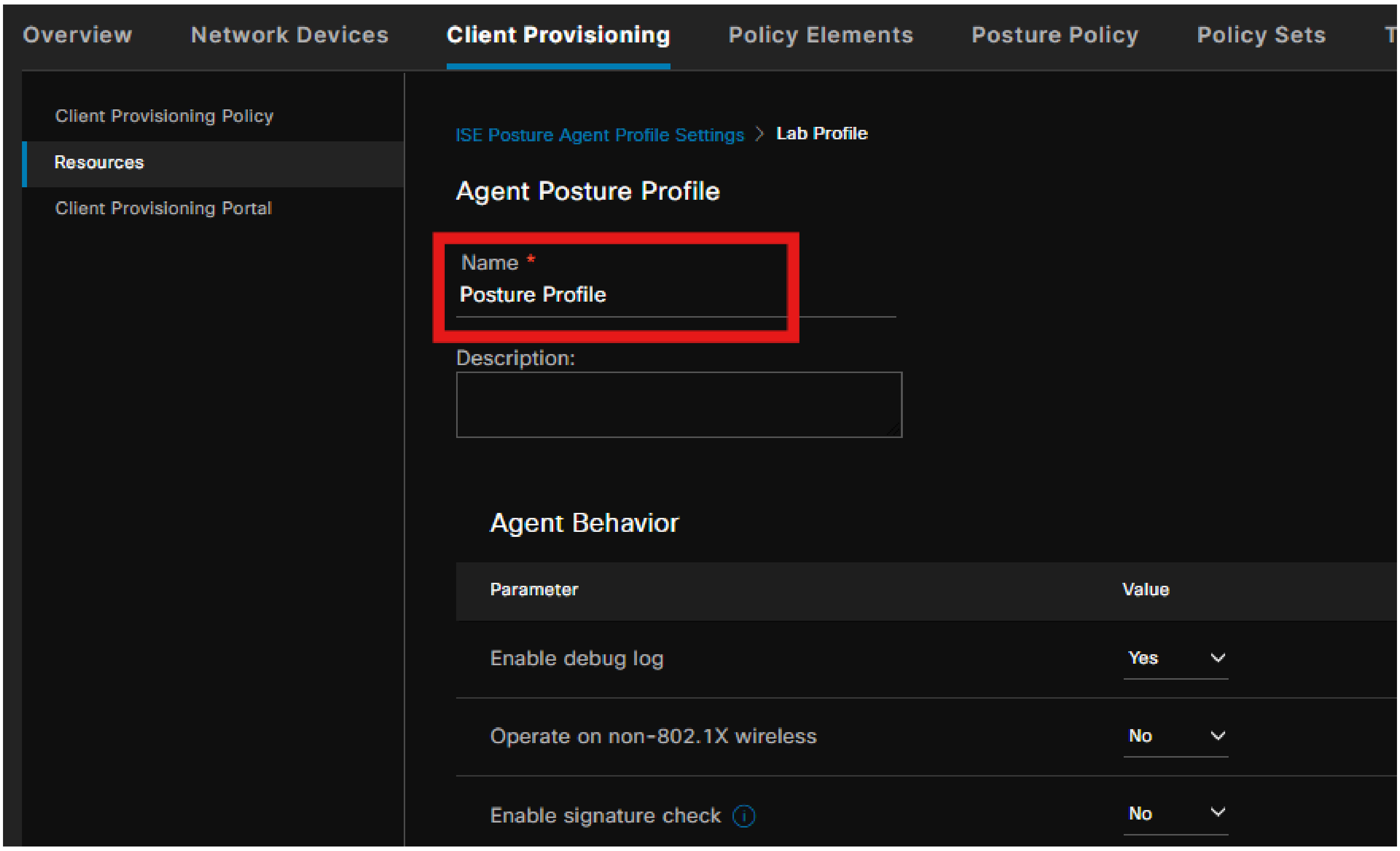
* Name: New Profile

Description:

Choose File configuration.xml

步驟 4.建立狀態配置檔案


Overview
Network Devices
Client Provisioning
Policy Elements
Posture Policy
Policy Set
Client Provisioning Policy
Resources
Client Provisioning Portal
Resources
Edit
Add
Duplicate
Delete
Agent resources from Cisco site
Agent resources from local disk
Native Supplicant Profile
Agent Configuration
Agent Posture Profile
AMP Enabler Profile
Version
La
oSecureClientCo... 4.3.4164.... 20
ntConfig Not Applic... 20
ve Supplicant Pro... Not Applic... 20
oAgentlessWind... 5.0.3061.0 20
OsXSPWizard 2.7.0.1 20
NAM Profile AgentProfile Not Applic... 20


Overview
Network Devices
Client Provisioning
Policy Elements
Posture Policy
Policy Sets
T
Client Provisioning Policy
Resources
Client Provisioning Portal
ISE Posture Agent Profile Settings > Lab Profile

Agent Posture Profile

Name * Posture Profile

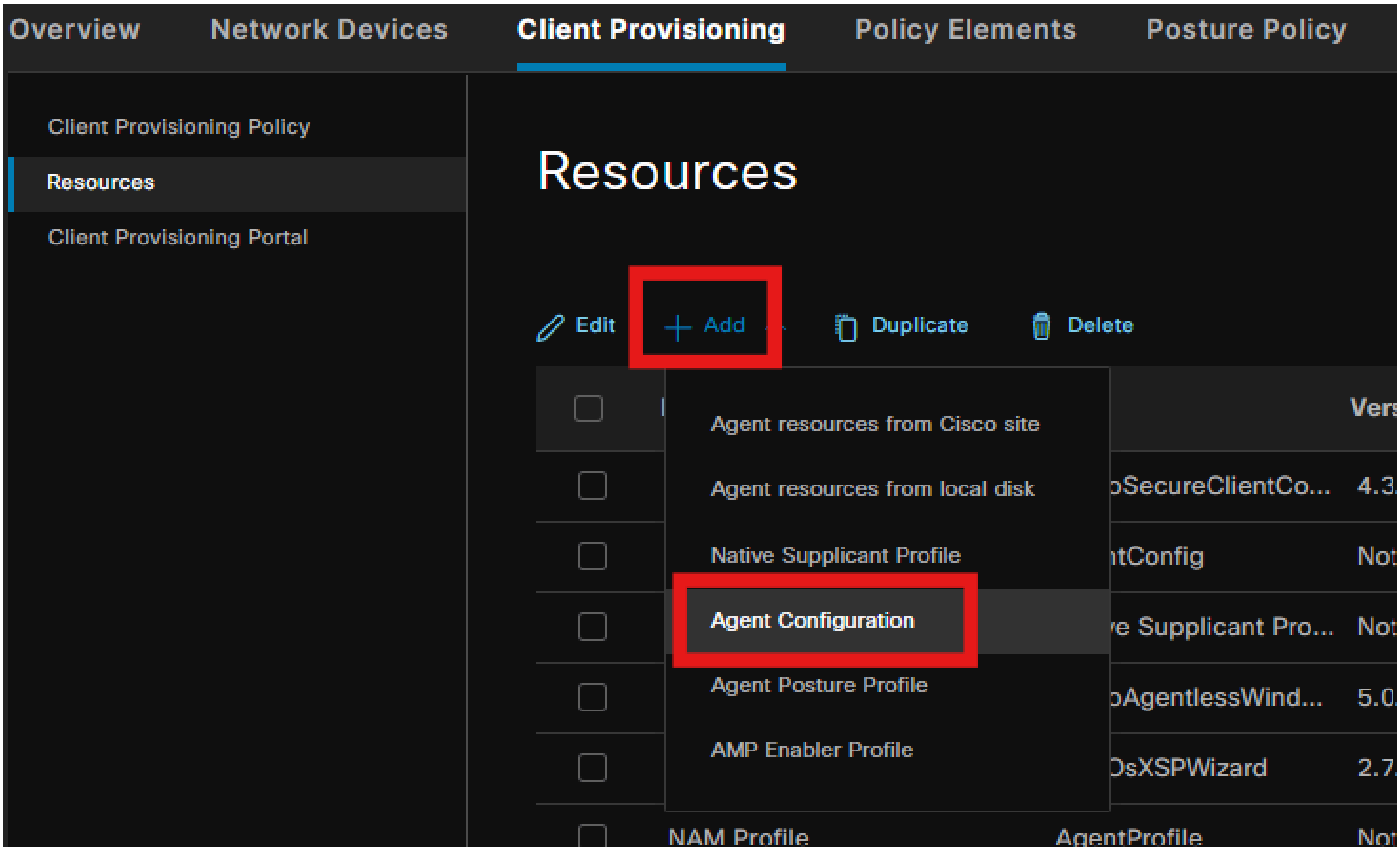
Description:

Agent Behavior

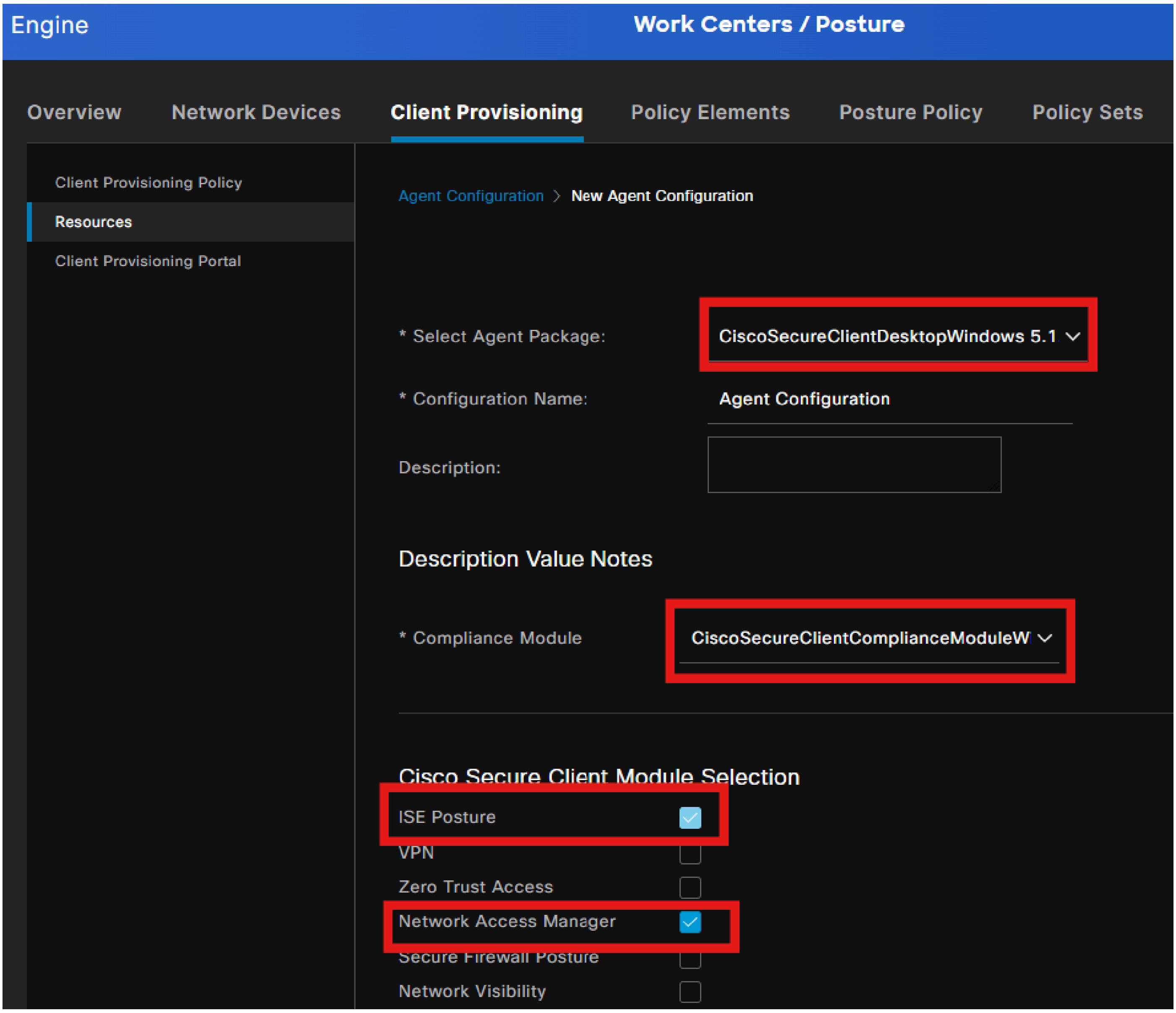
Parameter	Value
Enable debug log	Yes
Operate on non-802.1X wireless	No
Enable signature check	No

在Posture Protocol部分，不要忘記增加*以允許代理連線到所有伺服器。

步驟 5.建立代理配置



選擇上傳的安全客戶端和合規性模組包，在模組選擇下，選擇ISE終端安全評估、NAM和DART模組



* Select Agent Package: CiscoSecureClientDesktopWindows 5.1

* Configuration Name: Agent Configuration

Description:

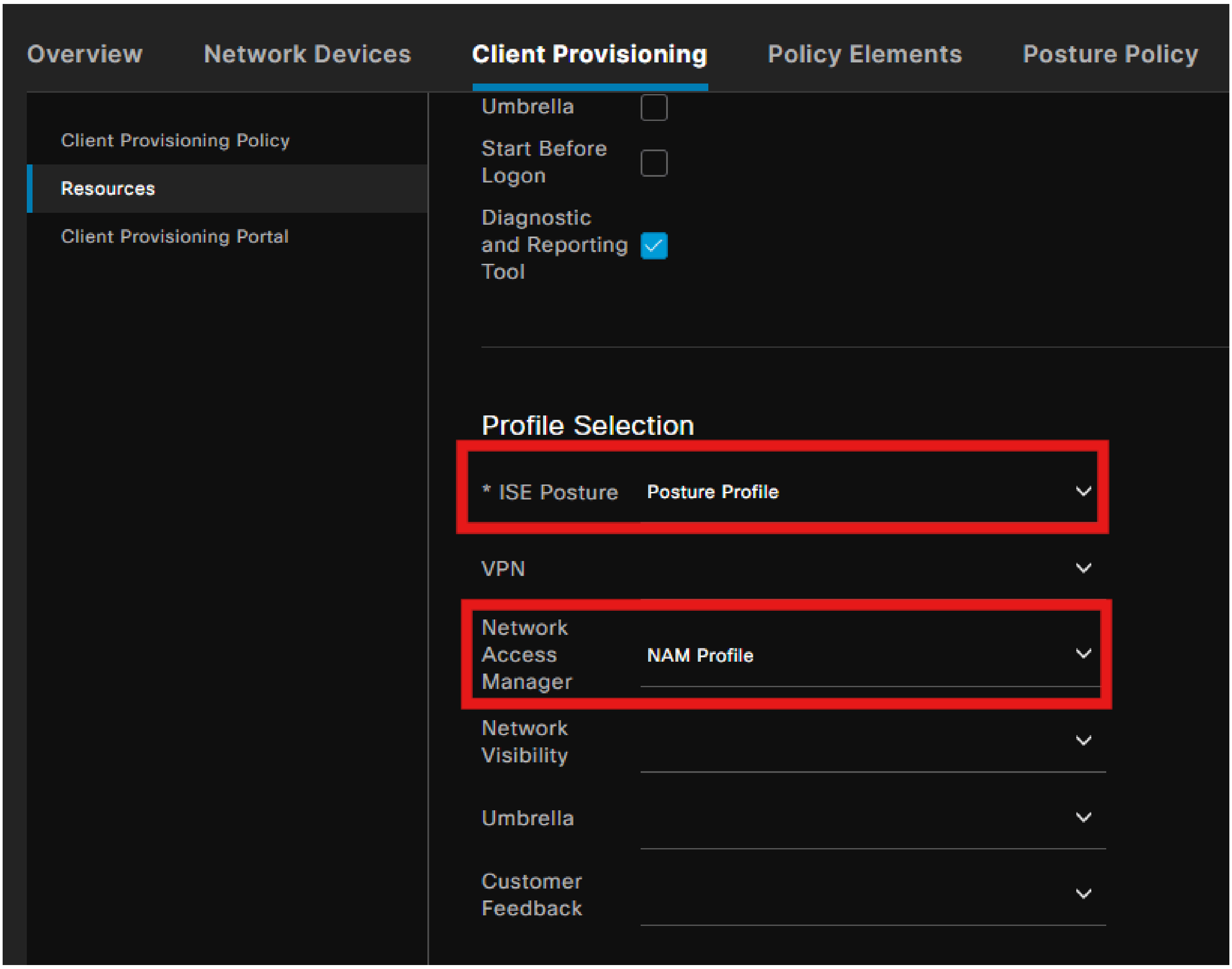
Description Value Notes

* Compliance Module CiscoSecureClientComplianceModuleW

Cisco Secure Client Module Selection

ISE Posture ☑
VPN □
Zero Trust Access □
Network Access Manager ☑
Secure Firewall Posture □
Network Visibility □

在Profile下，選擇Posture和NAM配置檔案，並按一下Submit。



Umbrella □

Start Before Logon □

Diagnostic and Reporting Tool ☑

Profile Selection

* ISE Posture: Posture Profile

VPN

Network Access Manager: NAM Profile

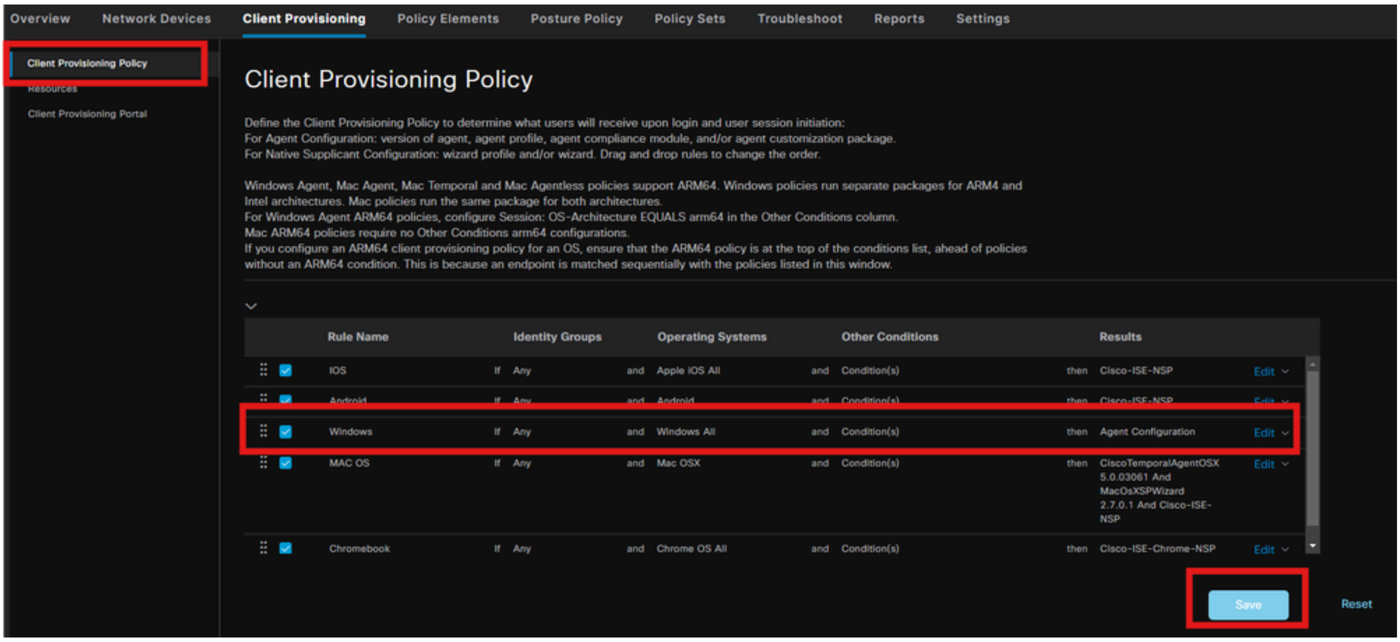
Network Visibility

Umbrella

Customer Feedback

步驟 6.客戶端調配策略

為Windows作業系統建立客戶端調配策略，並選擇上一步中建立的代理配置。



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.

Windows Agent, Mac Agent, Mac Temporal and Mac Agentless policies support ARM64. Windows policies run separate packages for ARM4 and Intel architectures. Mac policies run the same package for both architectures.
For Windows Agent ARM64 policies, configure Session: OS-Architecture EQUALS arm64 in the Other Conditions column.
Mac ARM64 policies require no Other Conditions arm64 configurations.
If you configure an ARM64 client provisioning policy for an OS, ensure that the ARM64 policy is at the top of the conditions list, ahead of policies without an ARM64 condition. This is because an endpoint is matched sequentially with the policies listed in this window.

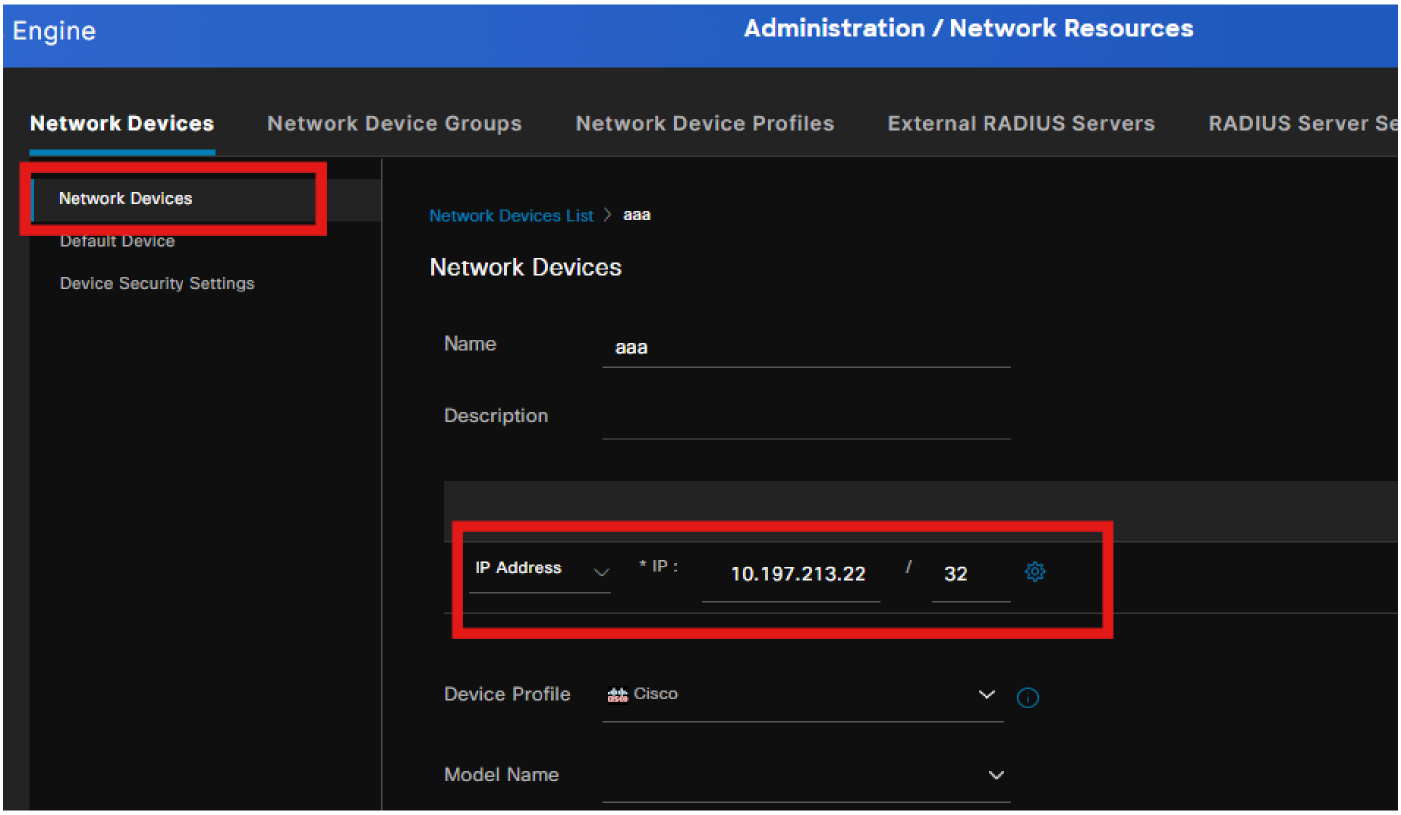
	Rule Name		Identity Groups		Operating Systems		Other Conditions		Results	
☑	IOS	If	Any	and	Apple IOS All	and	Condition(s)	then	Cisco-ISE-NSP	Edit
☑	Android	If	Any	and	Android	and	Condition(s)	then	Cisco-ISE-NSP	Edit
☑	Windows	If	Any	and	Windows All	and	Condition(s)	then	Agent Configuration	Edit
☑	MAC OS	If	Any	and	Mac OSX	and	Condition(s)	then	CiscoTemporalAgentOSX 5.0.03061 And MacOsXSPWizard 2.7.0.1 And Cisco-ISE-NSP	Edit
☑	Chromebook	If	Any	and	Chrome OS All	and	Condition(s)	then	Cisco-ISE-Chrome-NSP	Edit

步驟 7.狀態策略

有關如何建立終端安全評估策略和條件的資訊，請參閱本指南ISE終端安全評估規範部署指南。

步驟 8.增加網路裝置

要增加交換機IP地址和RADIUS共用金鑰，請導航到Administration > Network Resources。



Network Devices

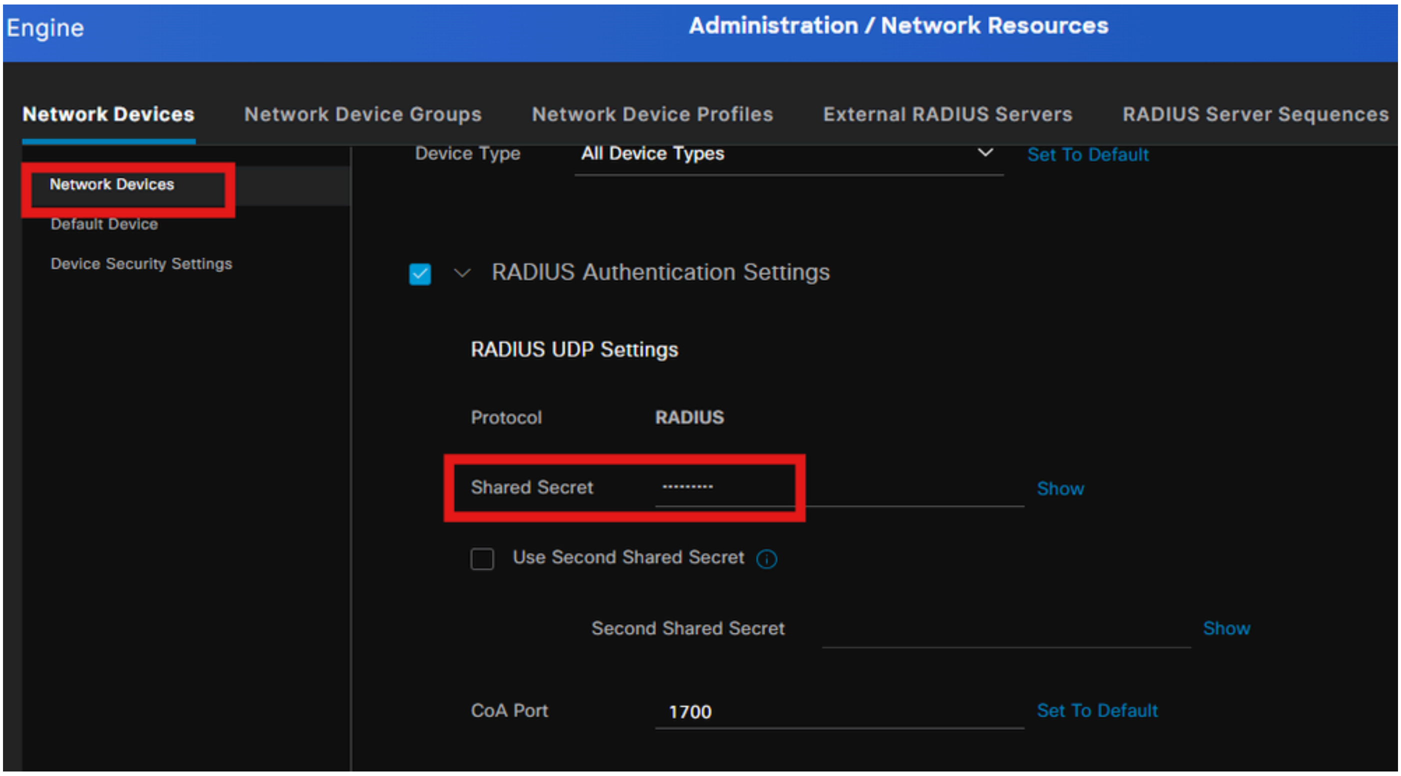
Name: aaa

Description:

IP Address * IP : 10.197.213.22 / 32

Device Profile: Cisco

Model Name:



Device Type: All Device Types

☑ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

Shared Secret: ·········

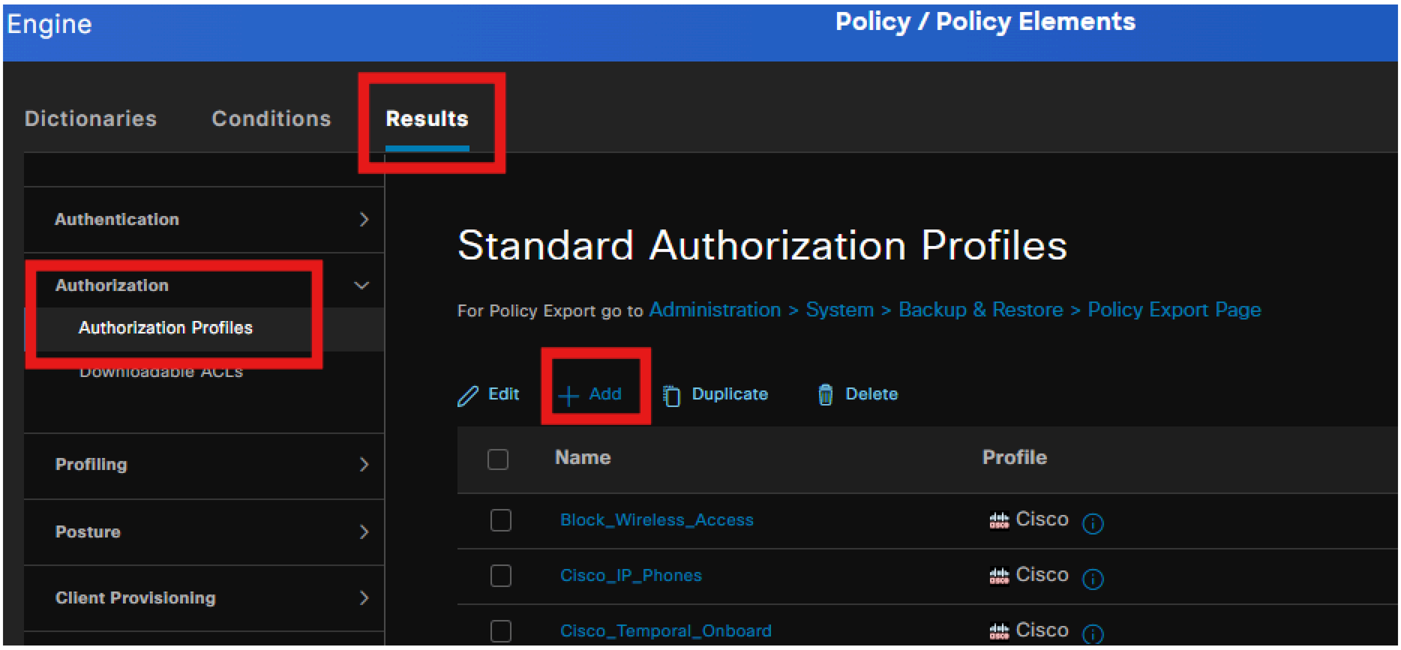
□ Use Second Shared Secret

Second Shared Secret:

CoA Port: 1700

步驟 9.授權配置檔案

要建立狀態重定向配置檔案，請導航到Policy > Policy Elements > Results。

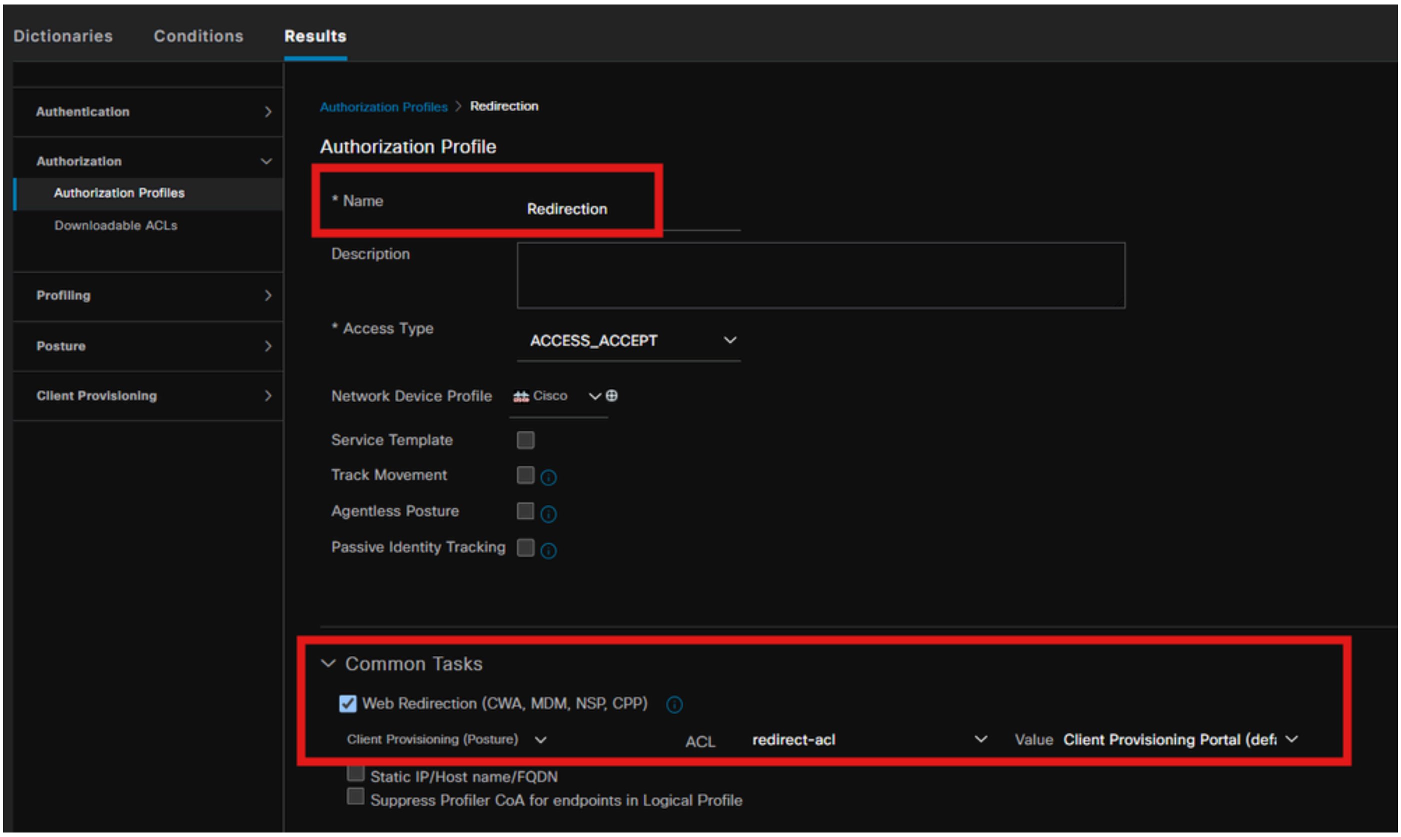


Standard Authorization Profiles

For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

□	Name	Profile
□	Block_Wireless_Access	Cisco
□	Cisco_IP_Phones	Cisco
□	Cisco_Temporal_Onboard	Cisco

在command task下，選擇具有重定向ACL的客戶端調配門戶。



Authorization Profile

* Name: Redirection

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Agentless Posture □

Passive Identity Tracking □

Common Tasks

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

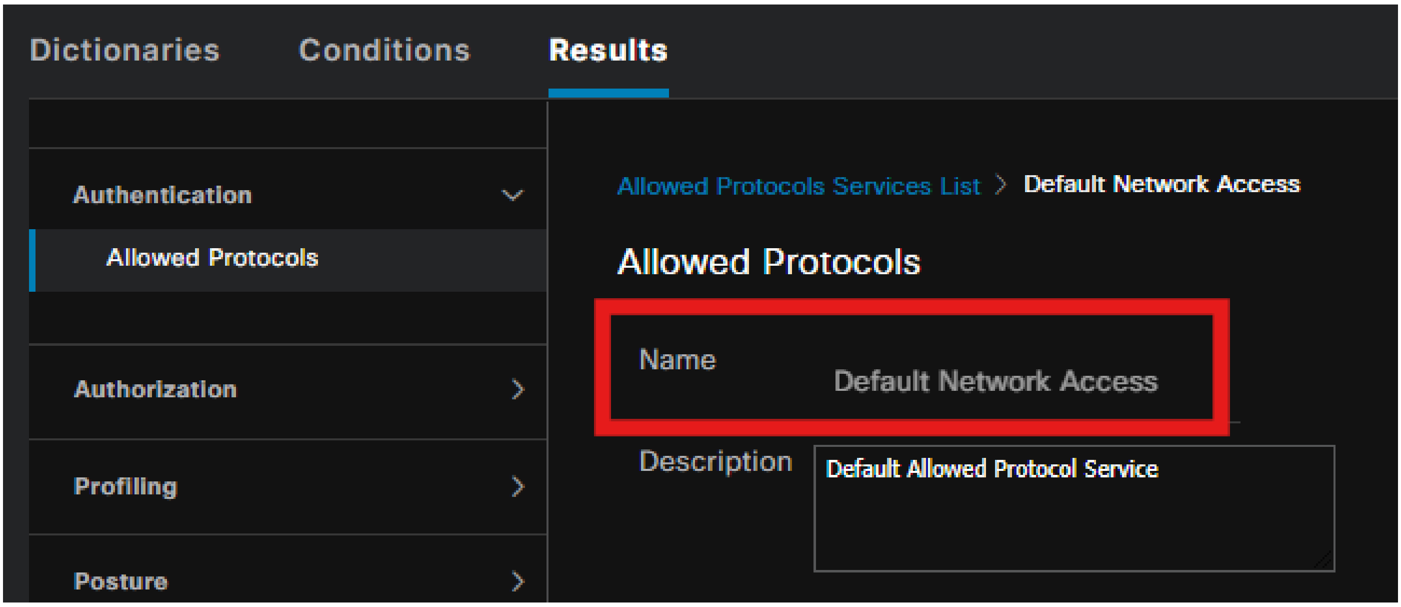
Client Provisioning (Posture) ACL redirect-acl Value Client Provisioning Portal (defi

□ Static IP/Host name/FQDN

□ Suppress Profiler CoA for endpoints in Logical Profile

步驟 10.允許的協定

導航到策略>策略元素>結果>身份驗證>允許的協定，選擇EAP連結設定，

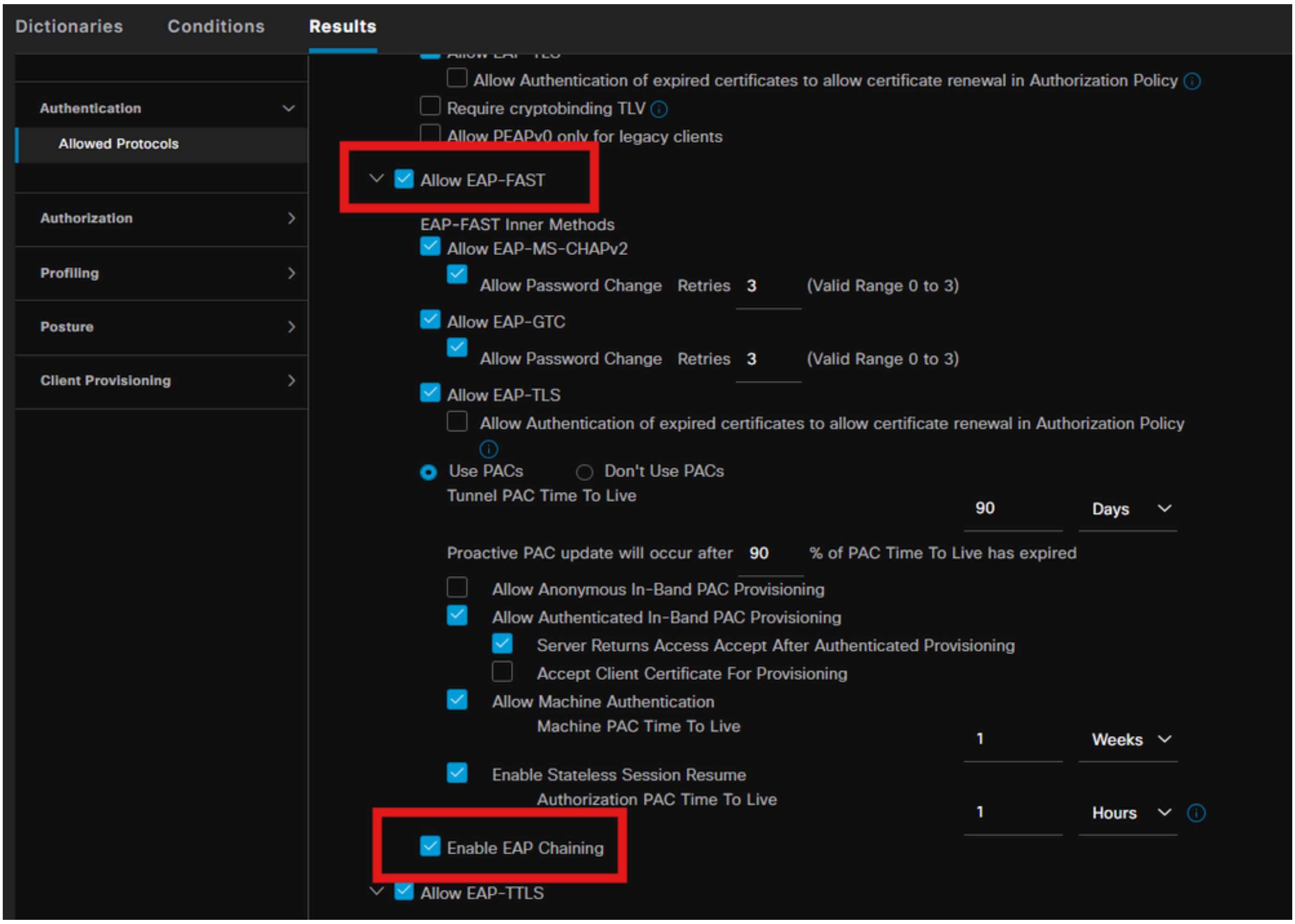


Allowed Protocols Services List > Default Network Access

Allowed Protocols

Name: Default Network Access

Description: Default Allowed Protocol Service

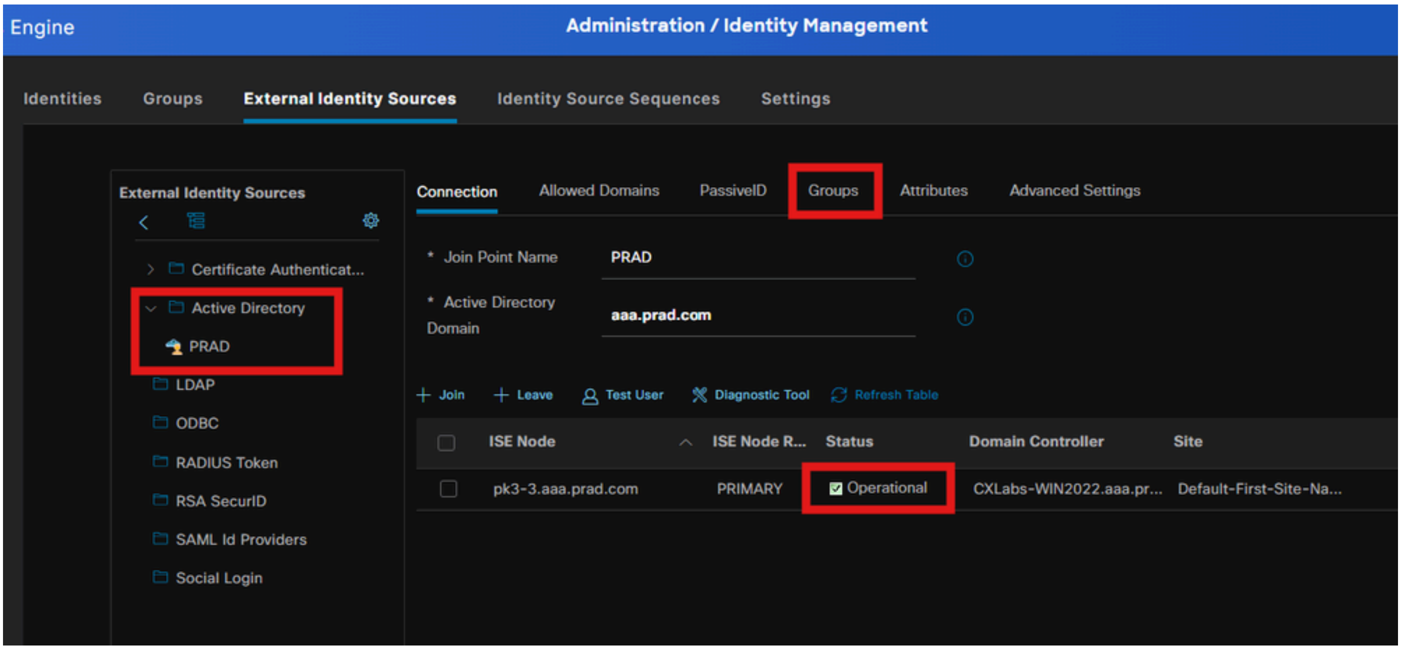


- □ Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy
- □ Require cryptobinding TLV
- □ Allow PEAPv0 only for legacy clients
- ☑ Allow EAP-FAST
  - EAP-FAST Inner Methods
  - ☑ Allow EAP-MS-CHAPv2
    - ☑ Allow Password Change Retries 3 (Valid Range 0 to 3)
  - ☑ Allow EAP-GTC
    - ☑ Allow Password Change Retries 3 (Valid Range 0 to 3)
  - ☑ Allow EAP-TLS
    - □ Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy
  - ● Use PACs ○ Don't Use PACs
    - Tunnel PAC Time To Live 90 Days
    - Proactive PAC update will occur after 90 % of PAC Time To Live has expired
    - □ Allow Anonymous In-Band PAC Provisioning
    - ☑ Allow Authenticated In-Band PAC Provisioning
      - ☑ Server Returns Access Accept After Authenticated Provisioning
      - □ Accept Client Certificate For Provisioning
    - ☑ Allow Machine Authentication
      - Machine PAC Time To Live 1 Weeks
    - ☑ Enable Stateless Session Resume
      - Authorization PAC Time To Live 1 Hours
  - ☑ Enable EAP Chaining
- ☑ Allow EAP-TTLS

步驟 11.Active Directory

驗證ISE已加入Active Directory域，並且如果授權條件需要，會選擇域組。

管理>身份管理>外部身份源> Active Directory



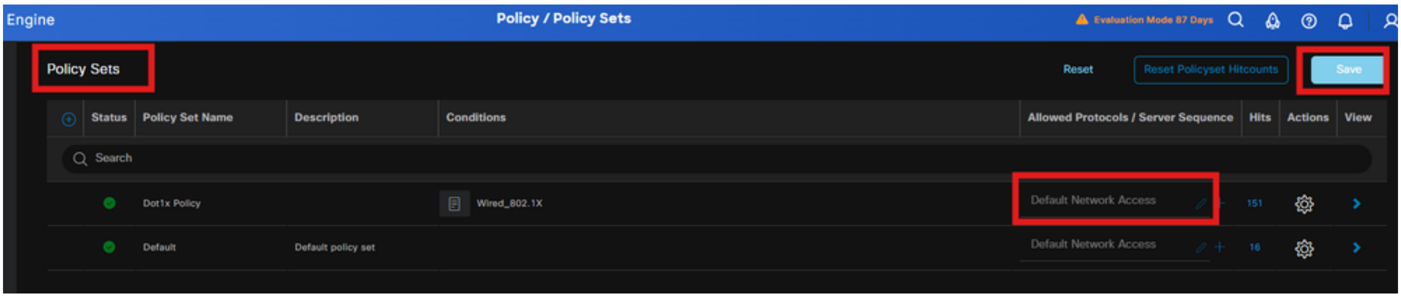
* Join Point Name: PRAD

* Active Directory Domain: aaa.prad.com

ISE Node	ISE Node R...	Status	Domain Controller	Site
pk3-3.aaa.prad.com	PRIMARY	☑ Operational	CXLabs-WIN2022.aaa.pr...	Default-First-Site-Na...

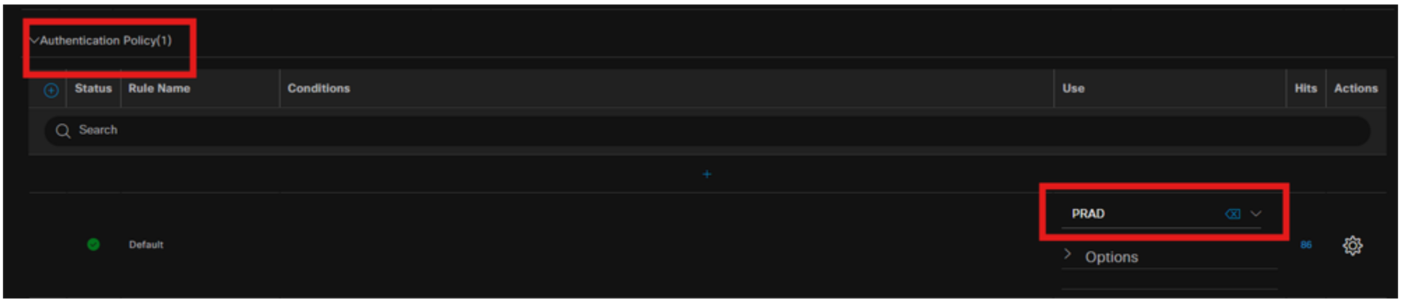
步驟 12.策略集

在ISE上建立策略集以驗證dot1x請求。導航到策略>策略集。



Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	Dot1x Policy		Wired_802.1X	Default Network Access	151	⚙	>
●	Default	Default policy set		Default Network Access	16	⚙	>

選擇Active directory作為身份驗證策略的身份源。

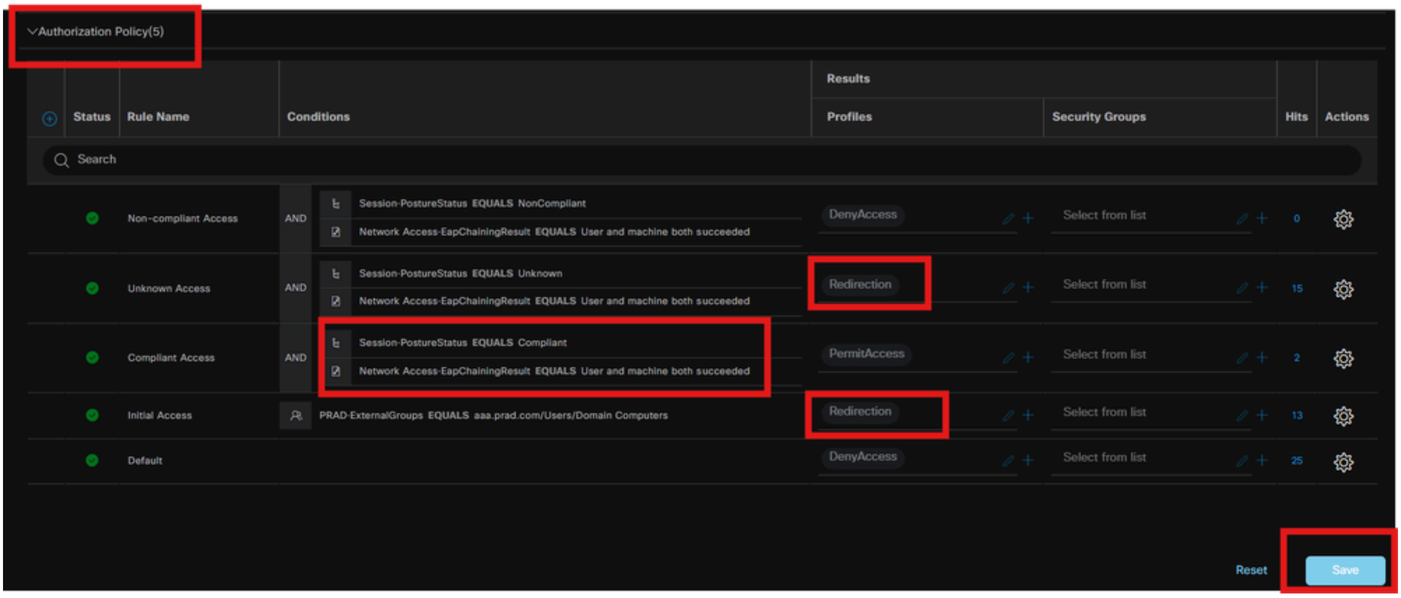


Status	Rule Name	Conditions	Use	Hits	Actions
●	Default		PRAD Options	86	⚙

根據狀態未知、不相容和相容配置不同的授權規則。

在此使用案例中。

- 初始訪問：重定向至ISE客戶端調配門戶以安裝安全客戶端代理和NAM配置檔案
- 未知訪問：訪問客戶端調配門戶以進行基於重定向的狀態發現
- 合規訪問：完全網路訪問
- 不相容：拒絕存取



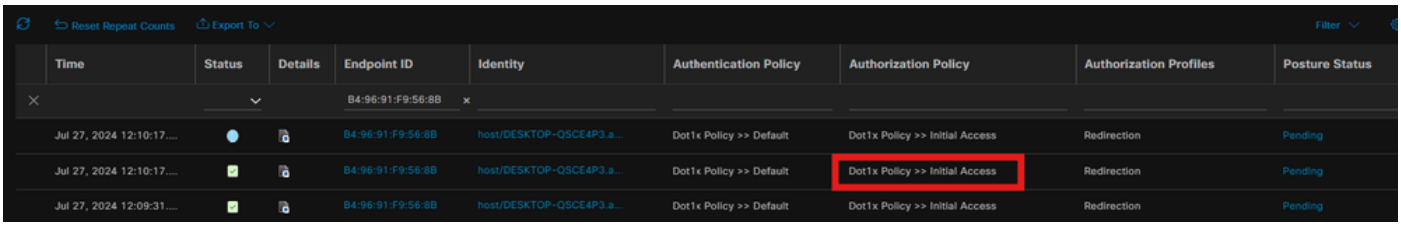
Authorization Policy(5)

Status	Rule Name	Conditions	Results		Hits	Actions
			Profiles	Security Groups		
●	Non-compliant Access	AND Session-PostureStatus EQUALS NonCompliant Network Access-EapChainingResult EQUALS User and machine both succeeded	DenyAccess	Select from list	0	⚙
●	Unknown Access	AND Session-PostureStatus EQUALS Unknown Network Access-EapChainingResult EQUALS User and machine both succeeded	Redirection	Select from list	15	⚙
●	Compliant Access	AND Session-PostureStatus EQUALS Compliant Network Access-EapChainingResult EQUALS User and machine both succeeded	PermitAccess	Select from list	2	⚙
●	Initial Access	PRAD-ExternalGroups EQUALS aaa.prad.com/Users/Domain Computers	Redirection	Select from list	13	⚙
●	Default		DenyAccess	Select from list	25	⚙

驗證

步驟 1.從ISE下載並安裝安全客戶端狀態/NAM模組

選擇透過dot1x驗證的終端，點選「初始訪問」授權規則。導航到操作> Radius >即時日誌



Time	Status	Details	Endpoint ID	Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture Status
			B4:96:91:F9:56:8B					
Jul 27, 2024 12:10:17....	●		B4:96:91:F9:56:8B	host/DESKTOP-QSCE4P3.a...	Dot1x Policy >> Default	Dot1x Policy >> Initial Access	Redirection	Pending
Jul 27, 2024 12:10:17....	☑		B4:96:91:F9:56:8B	host/DESKTOP-QSCE4P3.a...	Dot1x Policy >> Default	Dot1x Policy >> Initial Access	Redirection	Pending
Jul 27, 2024 12:09:31....	☑		B4:96:91:F9:56:8B	host/DESKTOP-QSCE4P3.a...	Dot1x Policy >> Default	Dot1x Policy >> Initial Access	Redirection	Pending

在交換機上，指定應用於終端的重定向URL和ACL。

```
Switch#show authentication session interface te1/0/24詳細資訊
介面：TenGigabitEthernet1/0/24
IIF-ID： 0x19262768
MAC地址：x4x6.xxxx.xxxx
IPv6地址：未知
IPv4地址：<client-IP>
使用者名稱：host/DESKTOP-xxxxxx.aaa.prad.com
狀態：已授權
網域：資料
Oper主機模式：單主機
Oper控制目錄：both
會話超時：不適用
通用會話ID：16D5C50A0000002CF067366B
帳戶會話ID：0x0000001f
控制代碼：0x7a000017
當前策略：POLICY_Te1/0/24
```

本地策略：
服務模板：DEFAULT_LINKSEC_POLICY_SHOULD_SECURE（優先順序150）
安全策略：應安全
安全性狀態：連結不安全

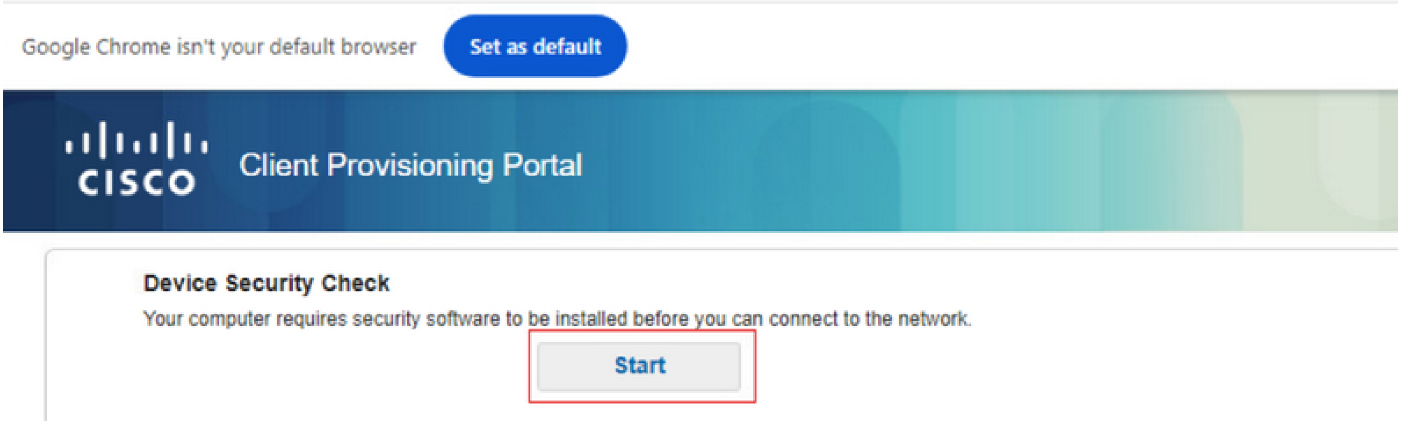
伺服器原則：
URL重定向ACL：redirect-acl
URL重定向
：https://ise33.aaa.prad.com:8443/portal/gateway?sessionId=16D5C50A0000002CF067366A&portal=ee
7180-4995-8aa2-9fb282645a8f&action=cpp&token=518f857900a37f9afc6d2da8b6fe3bc2
ACS ACL：xACSACLx-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3

方法狀態清單：
方法狀態
dot1x驗證成功

Switch#sh device-tracking database interface te1/0/24

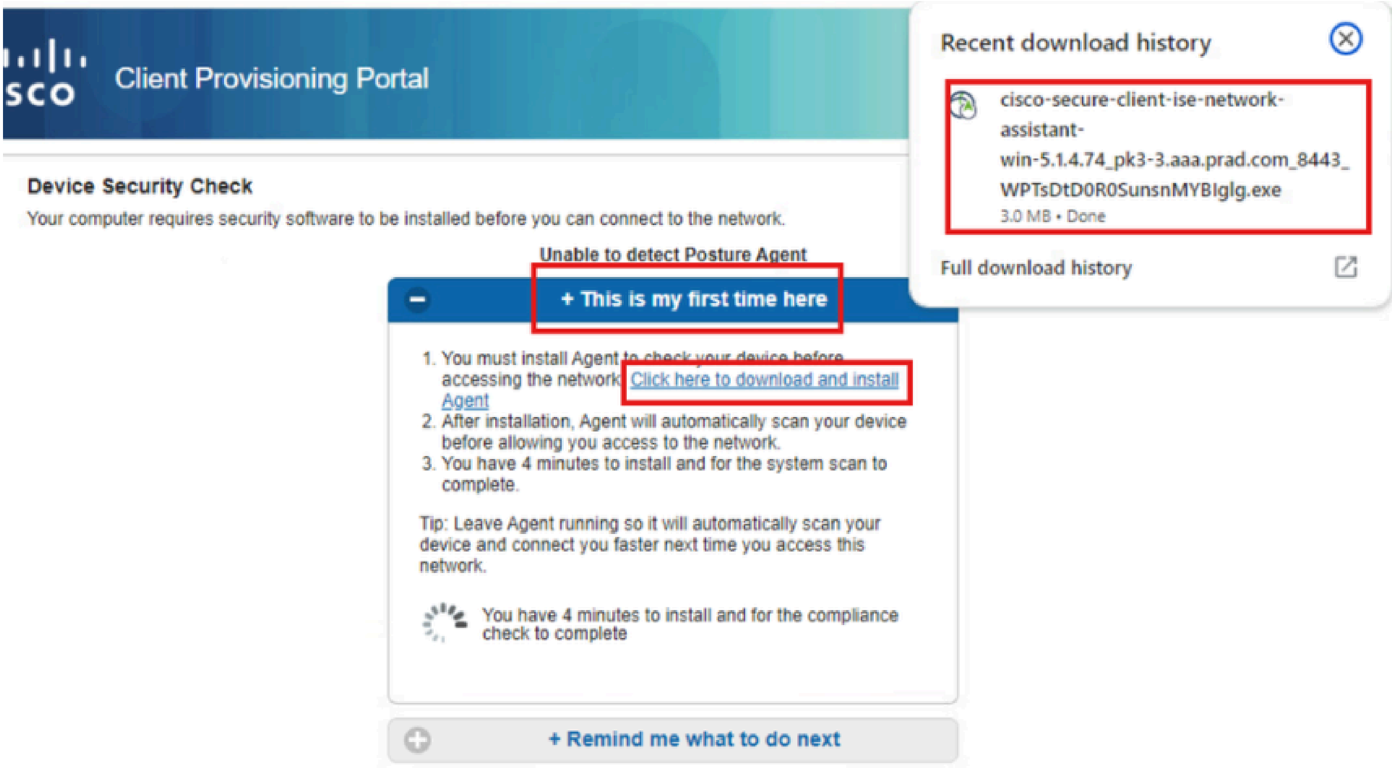
網路層地址鏈路層地址介面VLAN埠保留狀態剩餘時間
ARP X.X.X.X b496.91f9.568b Te1/0/24 1000 0005 4mn可訪問39秒，嘗試0

在終端上，驗證重定向到ISE終端安全評估的資料流，並按一下Start在終端上下載網路設定助手。


Google Chrome isn't your default browser
Set as default
cisco
Client Provisioning Portal

Device Security Check

Your computer requires security software to be installed before you can connect to the network.



Client Provisioning Portal

Device Security Check

Your computer requires security software to be installed before you can connect to the network.

Unable to detect Posture Agent

+ This is my first time here

1. You must install Agent to check your device before accessing the network. Click here to download and install Agent
2. After installation, Agent will automatically scan your device before allowing you access to the network.
3. You have 4 minutes to install and for the system scan to complete.

Tip: Leave Agent running so it will automatically scan your device and connect you faster next time you access this network.

You have 4 minutes to install and for the compliance check to complete

+ Remind me what to do next

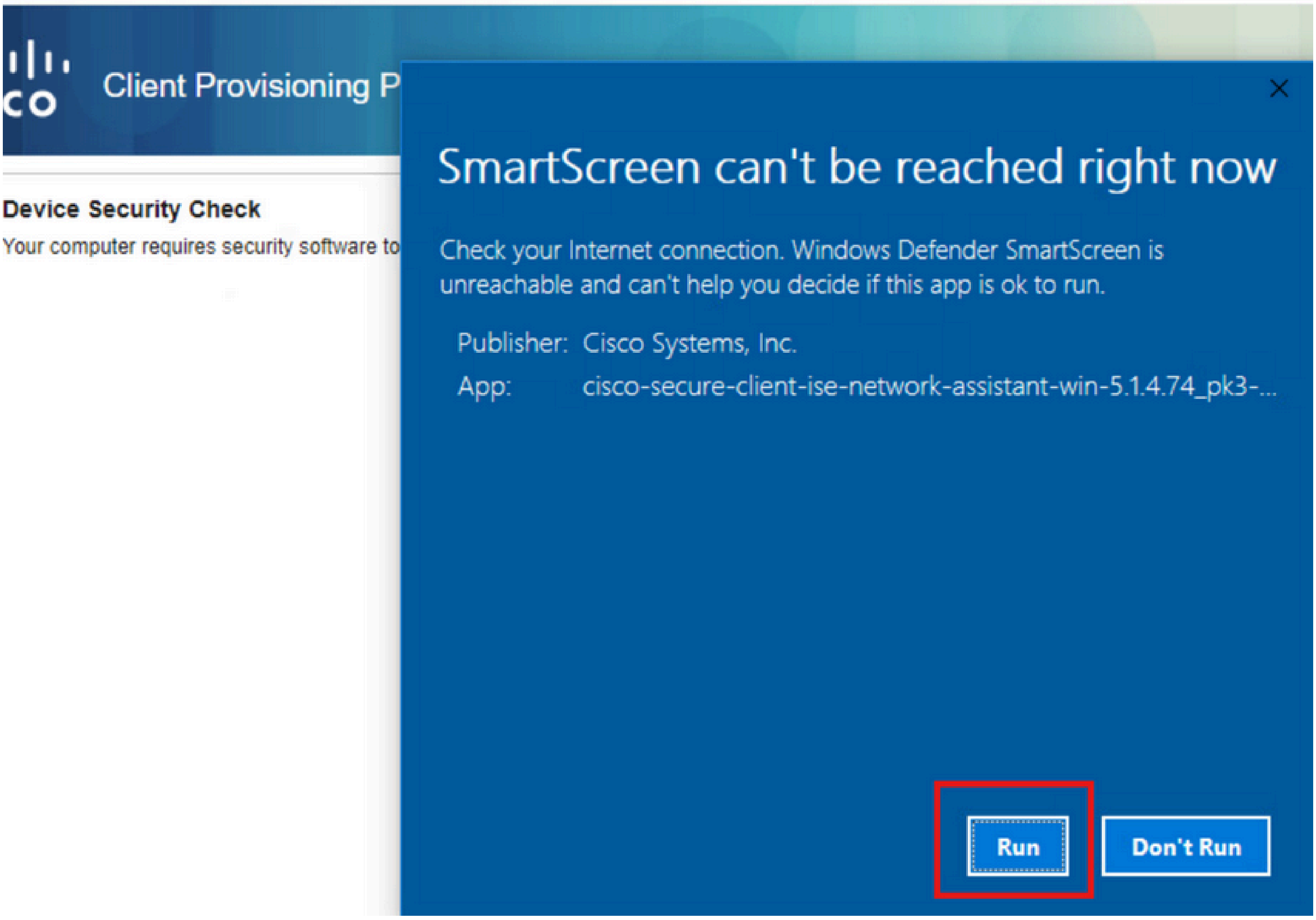
Recent download history

cisco-secure-client-ise-network-assistant-win-5.1.4.74_pk3-3.aaa.prad.com_8443_WPTsDtD0R0SunsnMYBIglg.exe

3.0 MB • Done

Full download history

按一下運行安裝NSA應用程式。



Client Provisioning P

Device Security Check

Your computer requires security software to

SmartScreen can't be reached right now

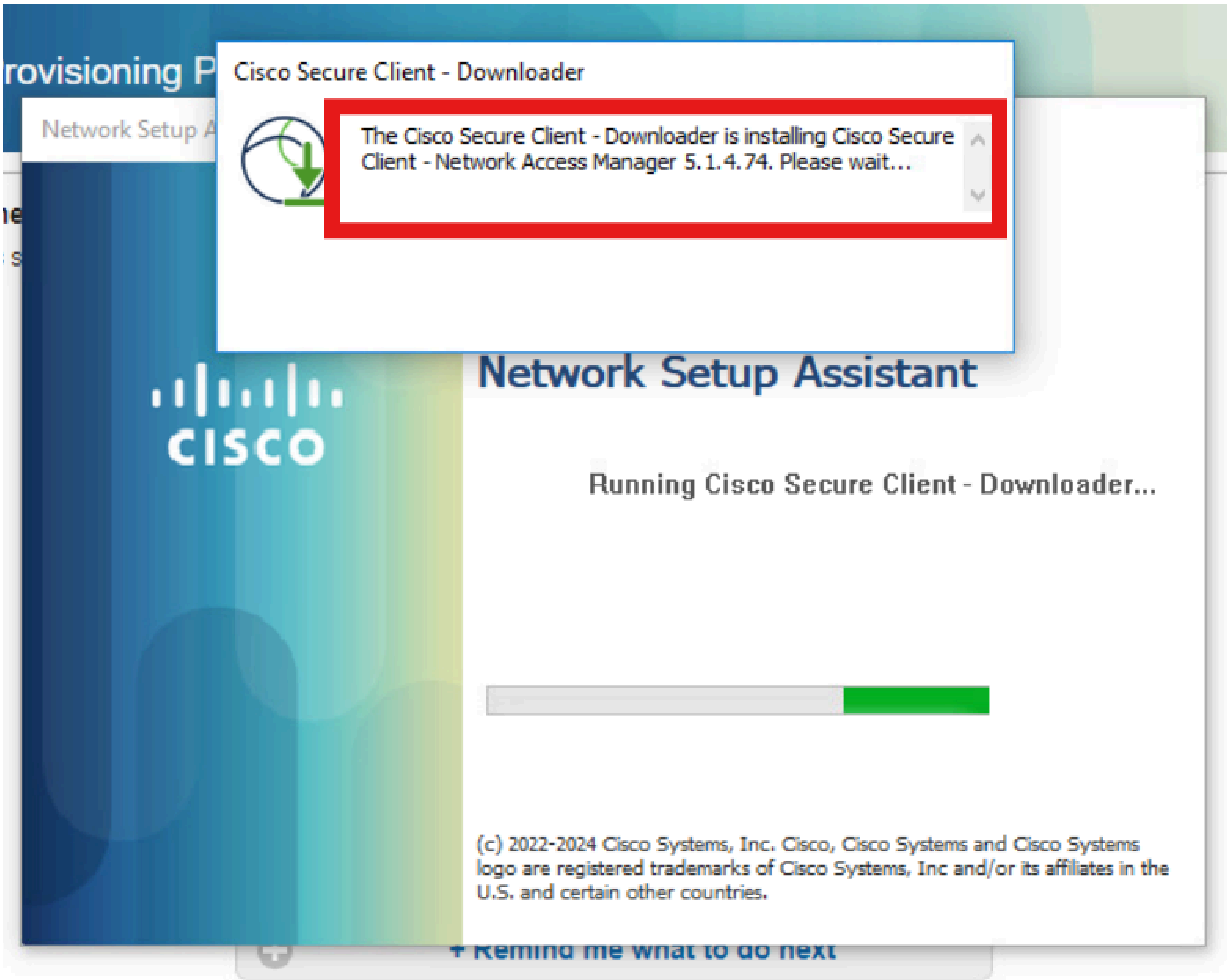
Check your Internet connection. Windows Defender SmartScreen is unreachable and can't help you decide if this app is ok to run.

Publisher: Cisco Systems, Inc.

App: cisco-secure-client-ise-network-assistant-win-5.1.4.74_pk3-...

現在，NSA會從ISE呼叫安全客戶端代理下載並安裝終端安全評估、NAM模組和NAM配置檔案

configuration.xml。



Cisco Secure Client - Downloader

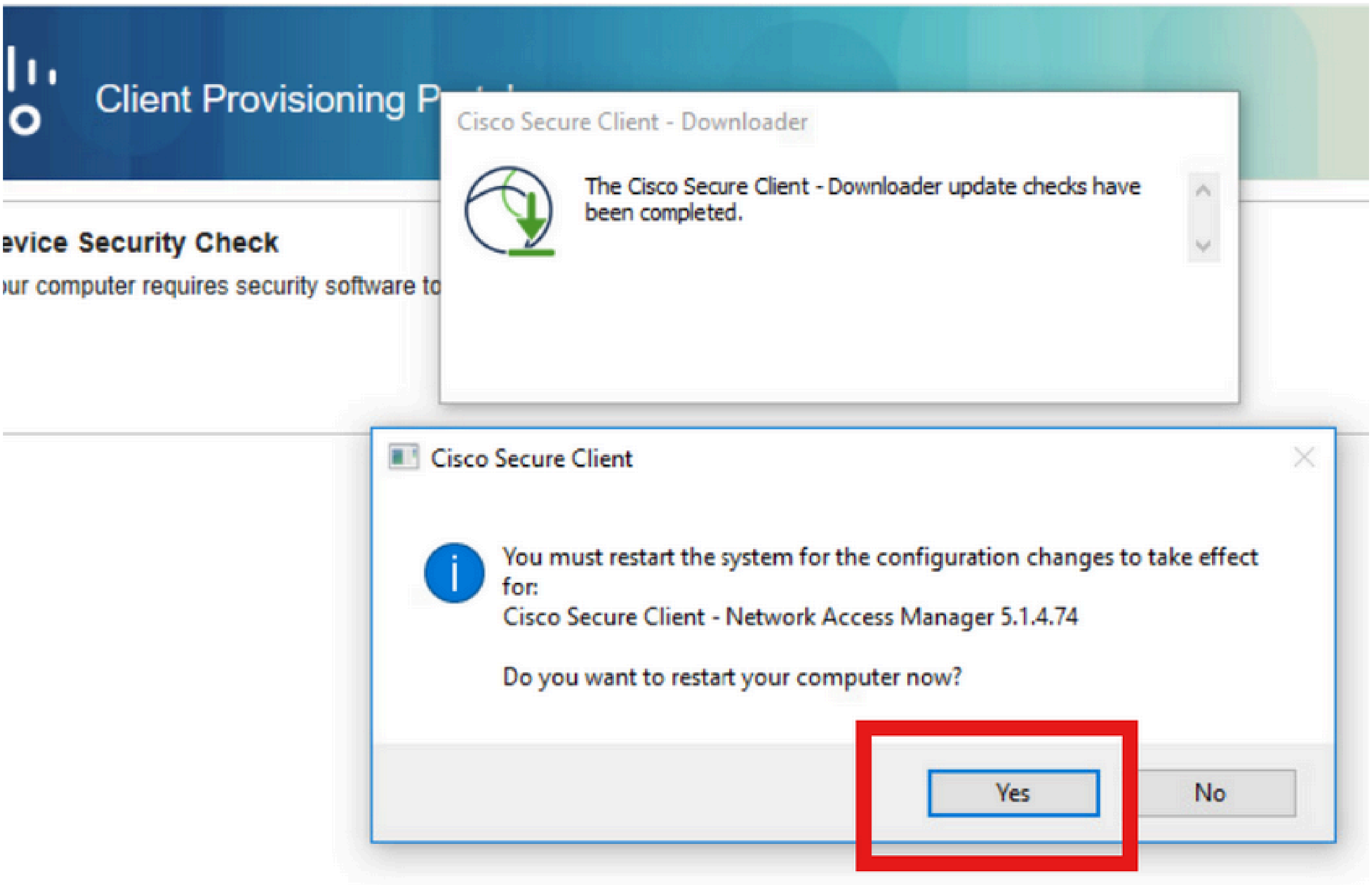
The Cisco Secure Client - Downloader is installing Cisco Secure Client - Network Access Manager 5.1.4.74. Please wait...

Network Setup Assistant

Running Cisco Secure Client - Downloader...

(c) 2022-2024 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc and/or its affiliates in the U.S. and certain other countries.

安裝NAM後觸發重新啟動提示。按一下Yes。



Client Provisioning P
evice Security Check
our computer requires security software to
Cisco Secure Client - Downloader

The Cisco Secure Client - Downloader update checks have been completed.

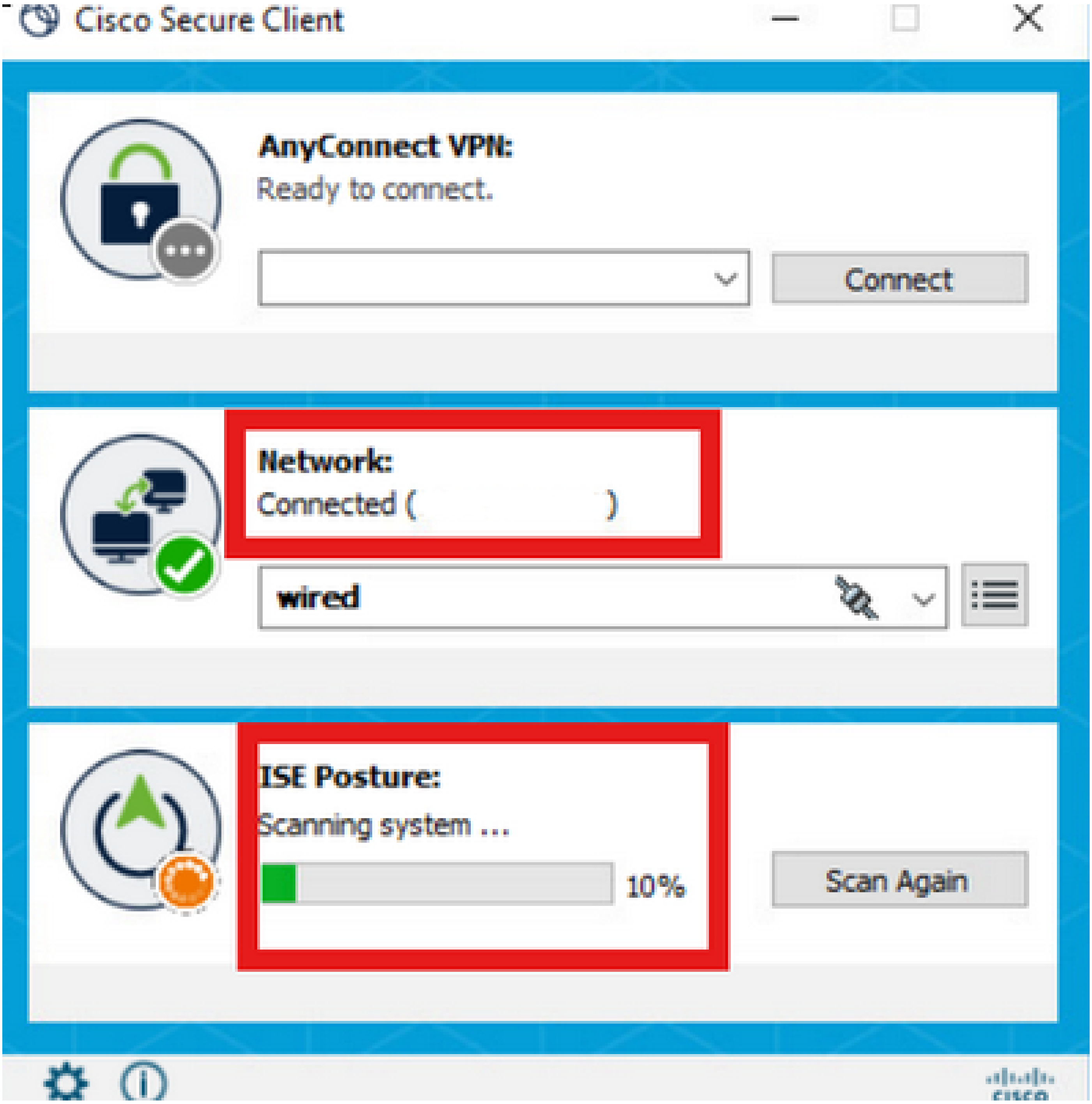
You must restart the system for the configuration changes to take effect for:
Cisco Secure Client - Network Access Manager 5.1.4.74

Do you want to restart your computer now?

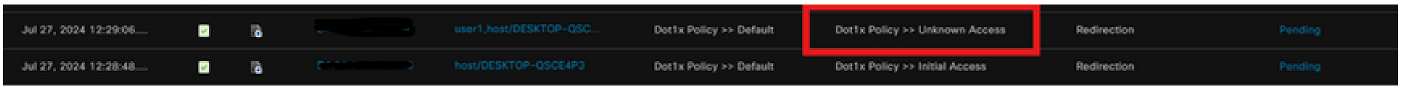
步驟 2.EAP-FAST

PC重新啟動且使用者登入後，NAM將透過EAP-FAST對使用者和電腦進行身份驗證。

如果終端身份驗證正確，NAM顯示其已連線，並且終端安全評估模組觸發終端安全評估掃描。

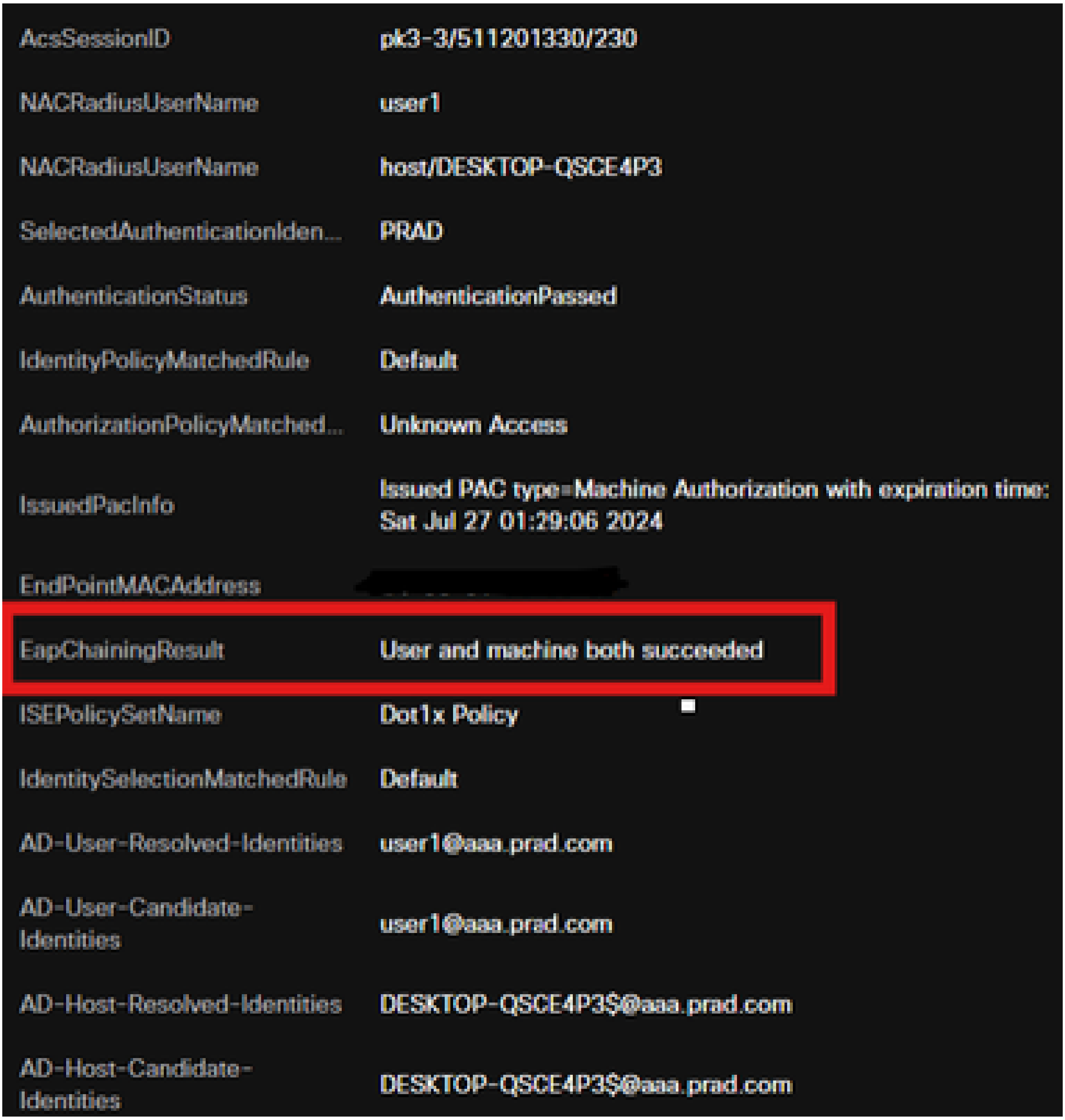


在ISE即時日誌上，終端現在觸及未知訪問規則。



Jul 27, 2024 12:29:06....	✓	🗎	[redacted]	user1,host/DESKTOP-QSC...	Dot1x Policy >> Default	Dot1x Policy >> Unknown Access	Redirection	Pending
Jul 27, 2024 12:28:48....	✓	🗎	[redacted]	host/DESKTOP-QSCE4P3	Dot1x Policy >> Default	Dot1x Policy >> Initial Access	Redirection	Pending

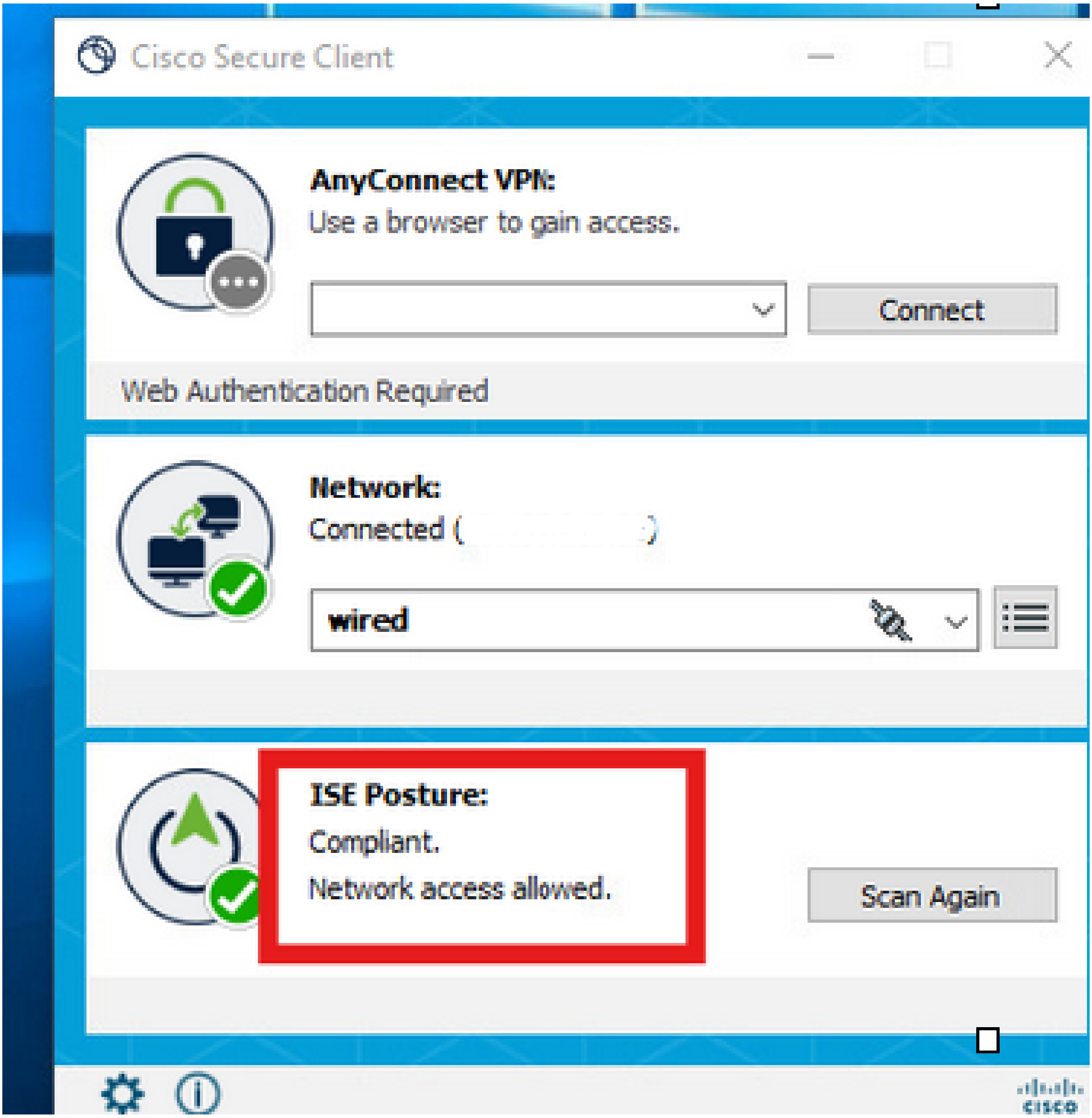
現在，根據NAM配置檔案配置，身份驗證協定為EAP-FAST，EAP-Chaining結果為「Success」。



AcsSessionID	pk3-3/511201330/230
NACRadiusUserName	user1
NACRadiusUserName	host/DESKTOP-QSCE4P3
SelectedAuthenticationIden...	PRAD
AuthenticationStatus	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatched...	Unknown Access
IssuedPacInfo	Issued PAC type=Machine Authorization with expiration time: Sat Jul 27 01:29:06 2024
EndPointMACAddress	[redacted]
EapChainingResult	User and machine both succeeded
ISEPolicySetName	Dot1x Policy
IdentitySelectionMatchedRule	Default
AD-User-Resolved-Identities	user1@aaa.prad.com
AD-User-Candidate-Identities	user1@aaa.prad.com
AD-Host-Resolved-Identities	DESKTOP-QSCE4P3$@aaa.prad.com
AD-Host-Candidate-Identities	DESKTOP-QSCE4P3$@aaa.prad.com

步驟 3.狀態掃描

安全客戶端安全評估模組觸發安全評估掃描並根據ISE安全評估策略標籤為投訴。



Cisco Secure Client

AnyConnect VPN:
Use a browser to gain access.

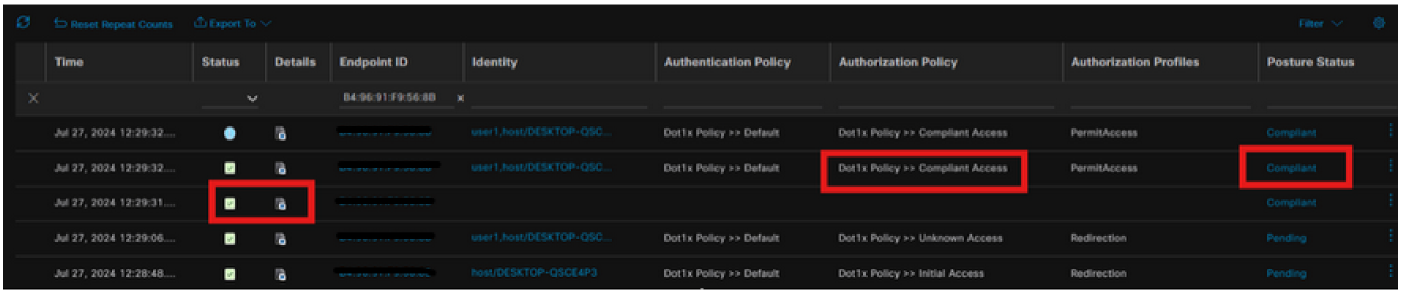
Web Authentication Required

Network:
Connected ([redacted])

wired

ISE Posture:
Compliant.
Network access allowed.

CoA在狀態掃描後觸發，現在終端觸及投訴訪問策略。



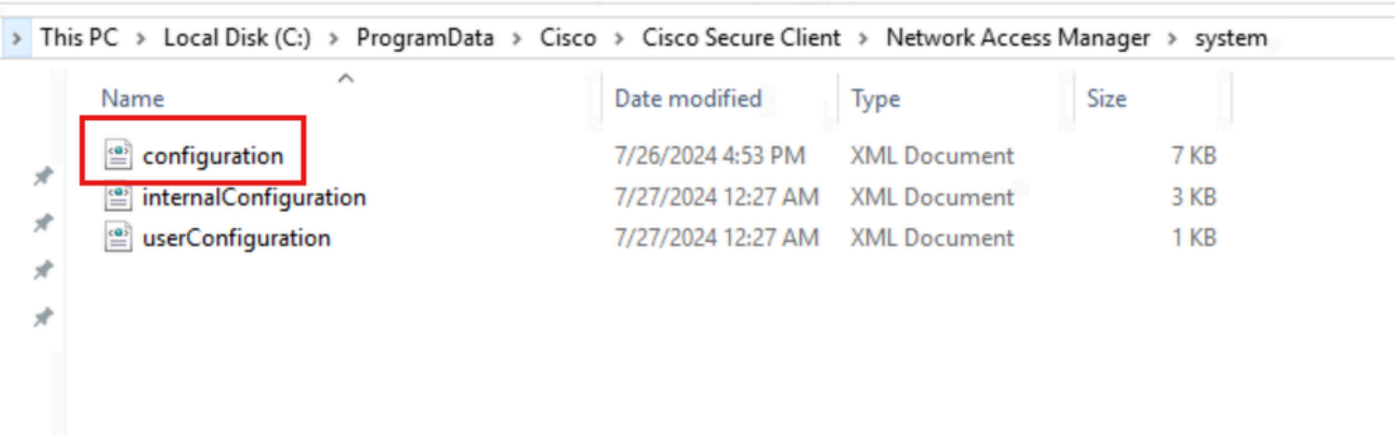
Time	Status	Details	Endpoint ID	Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture Status
			84:96:91:F9:56:8B					
Jul 27, 2024 12:29:32....	●	🗎	[redacted]	user1,host/DESKTOP-QSC...	Dot1x Policy >> Default	Dot1x Policy >> Compliant Access	PermitAccess	Compliant
Jul 27, 2024 12:29:32....	✓	🗎	[redacted]	user1,host/DESKTOP-QSC...	Dot1x Policy >> Default	Dot1x Policy >> Compliant Access	PermitAccess	Compliant
Jul 27, 2024 12:29:31....	✓	🗎	[redacted]					Compliant
Jul 27, 2024 12:29:06....	✓	🗎	[redacted]	user1,host/DESKTOP-QSC...	Dot1x Policy >> Default	Dot1x Policy >> Unknown Access	Redirection	Pending
Jul 27, 2024 12:28:48....	✓	🗎	[redacted]	host/DESKTOP-QSCE4P3	Dot1x Policy >> Default	Dot1x Policy >> Initial Access	Redirection	Pending

疑難排解

步驟 1.NAM配置檔案

安裝NAM模組後，驗證PC上的此路徑中是否存在NAM配置檔案configuration.xml。

C:\ProgramData\Cisco\Cisco Secure Client\Network Access Manager\system

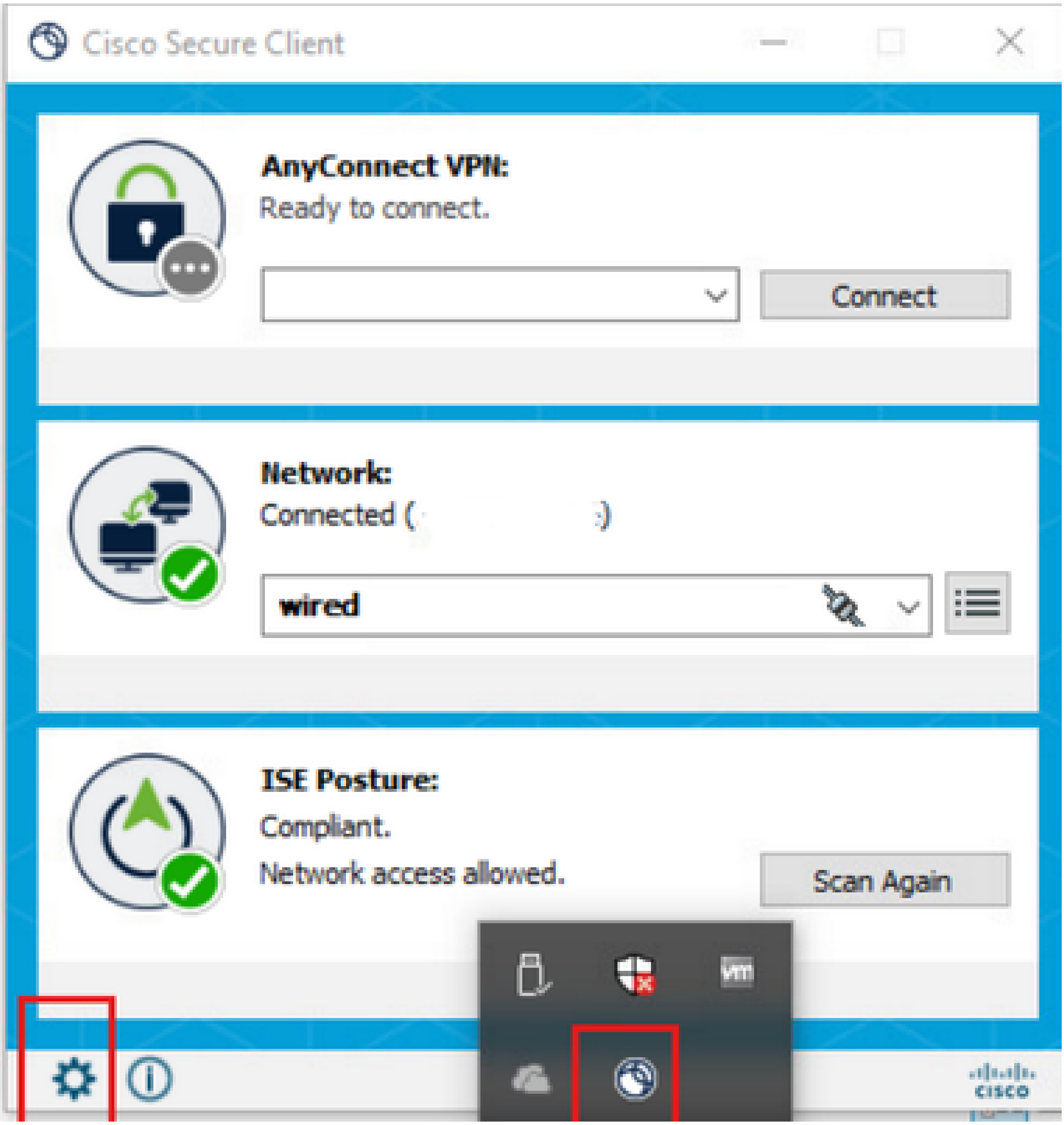


This PC › Local Disk (C:) › ProgramData › Cisco › Cisco Secure Client › Network Access Manager › system

Name	Date modified	Type	Size
configuration	7/26/2024 4:53 PM	XML Document	7 KB
internalConfiguration	7/27/2024 12:27 AM	XML Document	3 KB
userConfiguration	7/27/2024 12:27 AM	XML Document	1 KB

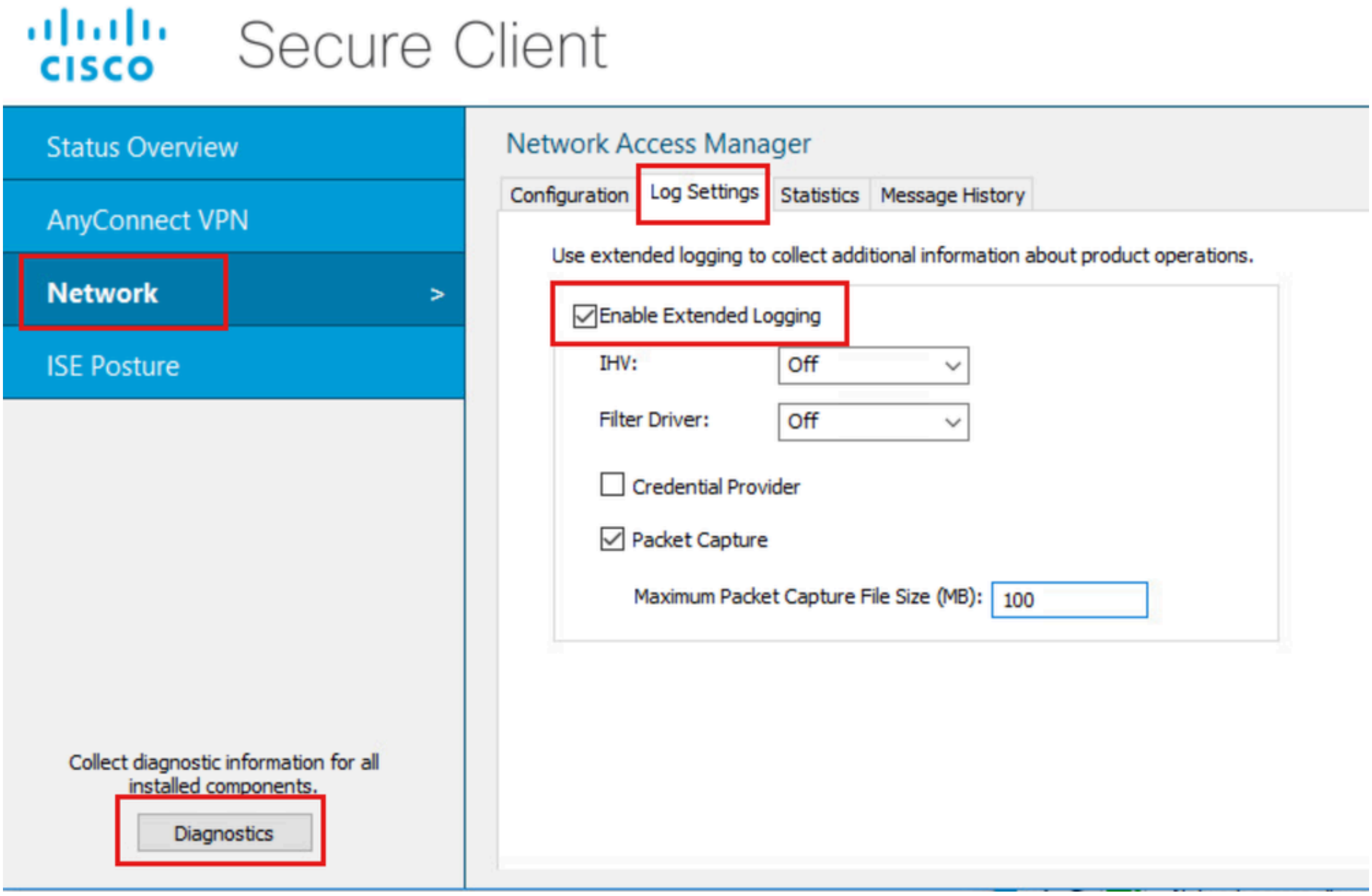
步驟 2.NAM擴展日誌記錄

按一下工作列中的「安全客戶端圖示」，然後選擇「設定」圖示。



導航到網路>日誌設定頁籤。選中Enable Extended Logging覈取方塊。
將資料包捕獲檔案大小設定為100 MB。

重現問題後，按一下Diagnostics在終端上建立DART捆綁包。



Use extended logging to collect additional information about product operations.

☑ Enable Extended Logging

IHV: Off

Filter Driver: Off

□ Credential Provider

☑ Packet Capture

Maximum Packet Capture File Size (MB): 100

Collect diagnostic information for all installed components.

Message History部分顯示了NAM執行的每個步驟的詳細資訊。

步驟 3. 交換機上的調試

在交換機上啟用這些調試，以排除dot1x和重定向流故障。

```
debug ip http all

debug ip http transactions

debug ip http url

set platform software trace smd switch active R0 aaa debug
set platform software trace smd switch active R0 dot1x-all debug
set platform software trace smd switch active R0 radius debug
set platform software trace smd switch active R0 auth-mgr-all debug
set platform software trace smd switch active R0 eap-all debug
set platform software trace smd switch active R0 epm-all debug

set platform software trace smd switch active R0 epm-redirect debug

set platform software trace smd switch active R0 webauth-aaa debug

set platform software trace smd switch active R0 webauth-httpd debug
```

若要檢視記錄

```
show logging
```

```
show logging process smd internal
```

步驟 4.ISE上的調試

收集具有以下屬性的ISE支援捆綁包，以在調試級別進行設定：

- 姿勢
- 入口網站
- 布建
- runtime-AAA
- nsf
- nsf-session
- 瑞士
- 客戶端Web應用

相關資訊

[配置安全客戶端NAM]

[ISE終端安全評估規範部署指南]

[Catalyst 9000系列交換機上的Dot1x故障排除]

關於此翻譯