

Configuración de Secure Client NAM Profile en Windows mediante ISE

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configuración](#)

[Diagrama de la red](#)

[Flujo de datos](#)

[Configurar switch](#)

[Descargue el paquete Secure Client](#)

[Configuración de ISE](#)

[Paso 1. Cargue el paquete en ISE](#)

[Paso 2. Crear un perfil NAM desde la herramienta Profile Editor](#)

[Paso 3. Cargue el perfil de NAM en ISE](#)

[Paso 4. Crear un perfil de postura](#)

[Paso 5. Crear configuración de agente](#)

[Paso 6. Política de aprovisionamiento de clientes](#)

[Paso 7. Política de estado](#)

[Paso 8. Agregar dispositivo de red](#)

[Paso 9. Perfil de autorización](#)

[Paso 10. Protocolos permitidos](#)

[Paso 11. Active Directory](#)

[Paso 12. Conjuntos de políticas](#)

[Validación](#)

[Paso 1. Descargue e instale el módulo Secure Client Posture/NAM desde ISE](#)

[Paso 2. EAP-FAST](#)

[Paso 3. Análisis de estado](#)

[Troubleshoot](#)

[Paso 1. Perfil de NAM](#)

[Paso 2. Registro extendido NAM](#)

[Paso 3. Depuraciones en el switch](#)

[Paso 4. Depuraciones en ISE](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo implementar el perfil de Cisco Secure Client Network Access Manager (NAM) a través de Identity Services Engine (ISE).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Identity Services Engine (ISE)
- AnyConnect NAM y Profile Editor
- Política de estado
- Configuración de Cisco Catalyst para servicios 802.1x

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco ISE, versión 3.3 y posteriores
- Windows 10 con Cisco Secure Mobility Client 5.1.4.74 y versiones posteriores
- Switch Cisco Catalyst 9200 con software Cisco IOS® XE 17.6.5 y versiones posteriores
- Active Directory 2016

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

La autenticación EAP-FAST se produce en dos fases. En la primera fase, EAP-FAST emplea un protocolo de enlace TLS para proporcionar y autenticar intercambios de claves mediante objetos Type-Length-Values (TLV) para establecer un túnel protegido. Estos objetos TLV se utilizan para transmitir datos relacionados con la autenticación entre el cliente y el servidor. Una vez establecido el túnel, la segunda fase comienza con el cliente y el nodo ISE participando en más conversaciones para establecer las políticas de autenticación y autorización necesarias.

El perfil de configuración de NAM está configurado para utilizar EAP-FAST como método de autenticación y está disponible para redes definidas administrativamente.

Además, se pueden configurar los tipos de conexión de equipo y usuario dentro del perfil de configuración de NAM.

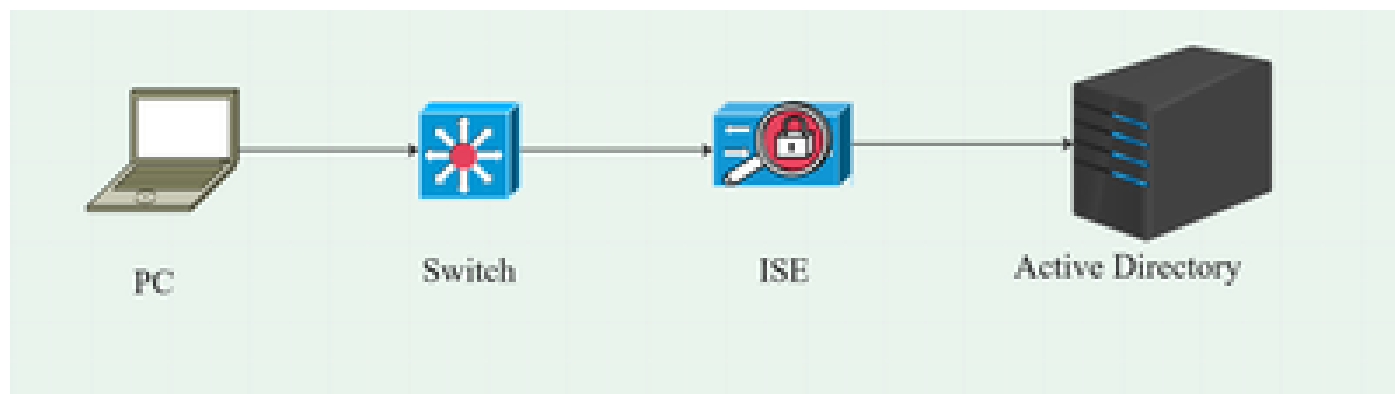
El dispositivo Windows corporativo obtiene acceso corporativo completo mediante la comprobación NAM con estado.

El dispositivo personal de Windows obtiene acceso a una red restringida con la misma configuración de NAM.

Este documento proporciona instrucciones para implementar el perfil de Cisco Secure Client Network Access Manager (NAM) a través del portal de estado de Identity Services Engine (ISE) mediante la implementación web, junto con la comprobación de cumplimiento de estado.

Configuración

Diagrama de la red



Flujo de datos

Cuando un PC se conecta a la red, ISE proporciona la política de autorización para la redirección al portal de estado.

El tráfico http del PC se redirige a la página de aprovisionamiento de clientes de ISE, donde la aplicación NSA se descarga desde ISE.

A continuación, la NSA instala los módulos del agente Secure Client en el PC.

Una vez finalizada la instalación del agente, éste descarga el perfil de estado y el perfil NAM configurados en ISE.

La instalación del módulo NAM desencadena un reinicio en el PC.

Después del reinicio, el módulo NAM realiza la autenticación EAP-FAST basada en el perfil NAM.

A continuación, se activa el análisis de estado y se comprueba el cumplimiento según la política de estado de ISE.

Configurar switch

Configure el switch de acceso para la autenticación y redirección dot1x.

```
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
client 10.127.197.53 server-key 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 Server RAD1
address ipv4 <IP del servidor ISE> auth-port 1812 acct-port 1813
key <secret-key>

dot1x system-auth-control
```

Configure la ACL de redirección para que el usuario sea redirigido al portal de aprovisionamiento de clientes de ISE.

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

Habilite el seguimiento de dispositivos y la redirección http en el switch.

```
device-tracking policy <device tracking policy name>
tracking enable
interface <interface name>
device-tracking attach-policy <device tracking policy name>

ip http server
ip http secure-server
```

Descargue el paquete Secure Client

Descargue los archivos webdeploy del Editor de perfiles, las ventanas de Secure Client y el Módulo de cumplimiento manualmente desde software.cisco.com

En la barra de búsqueda del nombre del producto, escriba Secure Client 5.

Inicio > Seguridad > Seguridad de terminales > Secure Client (incluido AnyConnect) > Secure Client 5 > AnyConnect VPN Client Software

- cisco-secure-client-win-5.1.x-webdeploy-k9.pkg

- cisco-secure-client-win-4.3.x-isecomcompliance-webdeploy-k9.pkg
- tools-cisco-secure-client-win-5.1.x-profile-editor-k9.msi

Configuración de ISE

Paso 1. Cargue el paquete en ISE

Para cargar los paquetes de implementación web de Secure Client and Compliance Module en ISE, navegue hasta Workcenter > Estado > Aprovisionamiento del cliente > Recursos > Agregar > Recursos del agente desde el disco local.

The screenshot shows the 'Client Provisioning' tab in the ISE Workcenter. Under 'Agent Resources From Local Disk', the 'Category' is set to 'Cisco Provided Packages'. A file named 'cisco-secure-...deploy-k9.pkg' is selected. The 'Submit' button is highlighted.

The screenshot shows the 'Resources' table in the ISE Workcenter. The table lists various resources, including 'CiscoSecureClientComplianceModuleWindows 4.3.4164....' and 'CiscoSecureClientDesktopWindows 5.1.4.074', which are highlighted.

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

Paso 2. Crear un perfil NAM desde la herramienta Profile Editor

Para obtener información sobre cómo configurar un perfil NAM, consulte esta guía [Configuración de Secure Client NAM para Dot1x con Windows e ISE 3.2](#)

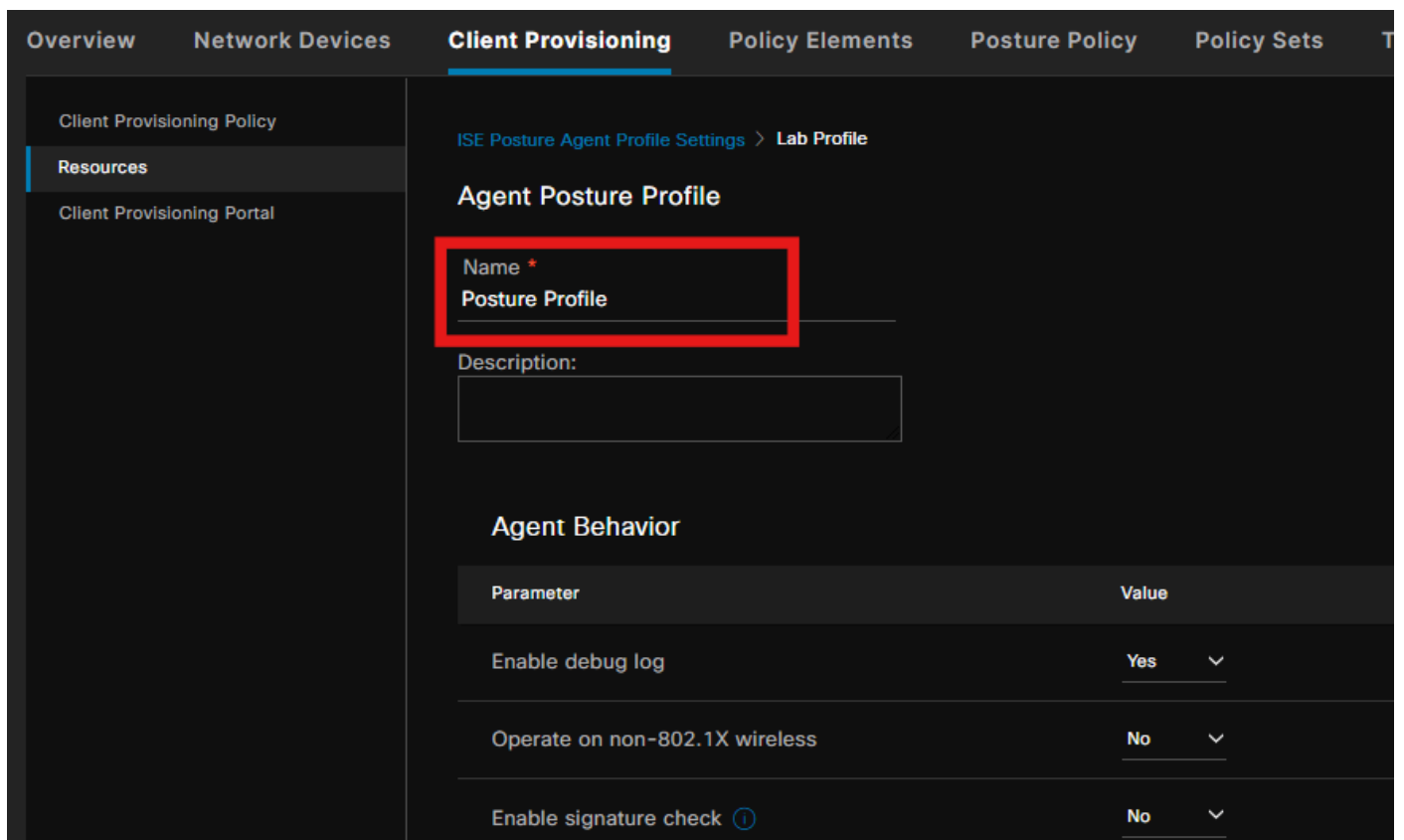
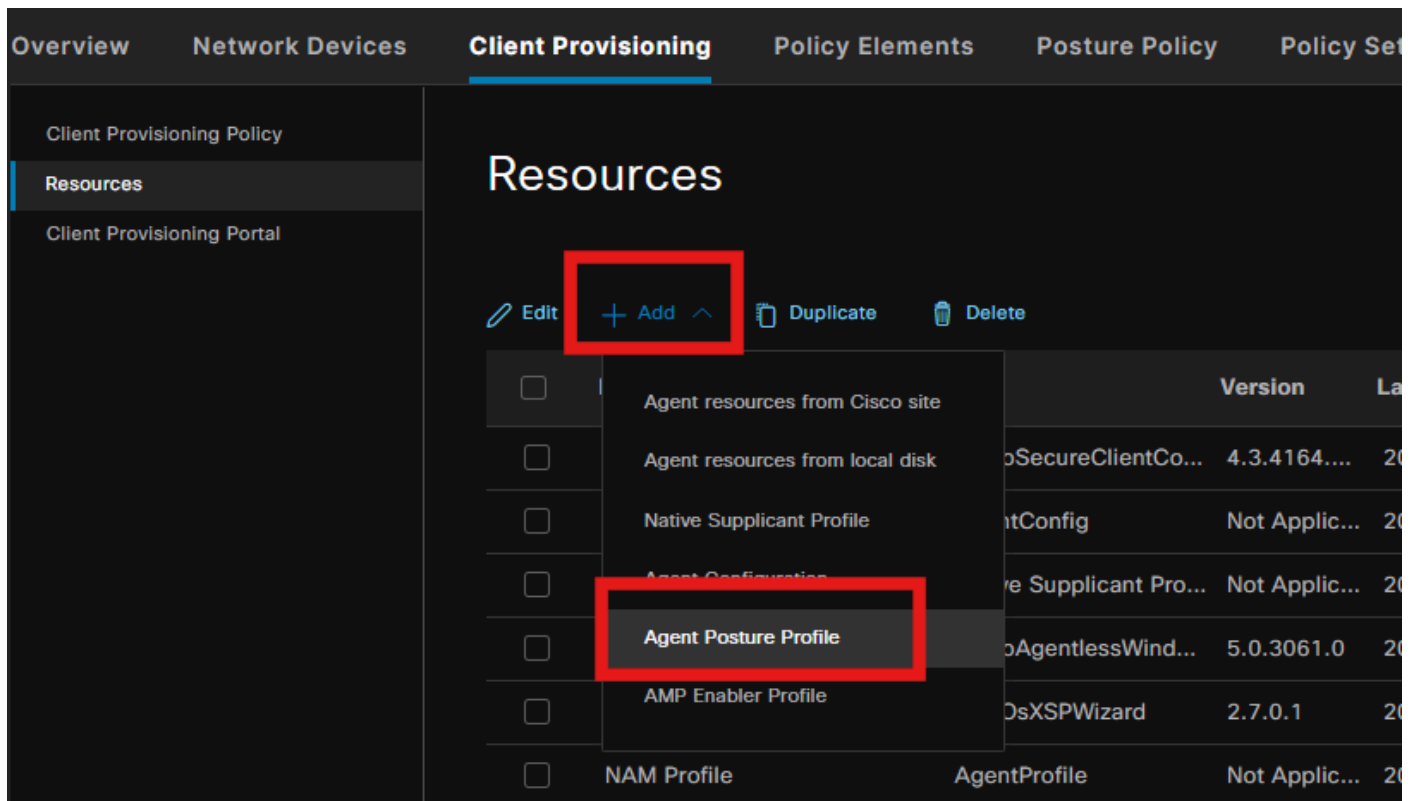
Paso 3. Cargue el perfil de NAM en ISE

Para cargar el archivo Configuration.xml del perfil de NAM en ISE como el perfil de agente, navegue hasta Aprovisionamiento de cliente > Recursos > Recursos de agente desde disco local.

The screenshot shows the ISE Client Provisioning interface. The left sidebar contains 'Client Provisioning Policy', 'Resources', and 'Client Provisioning Portal'. The main area is titled 'Agent Resources From Local Disk' and contains the following fields:

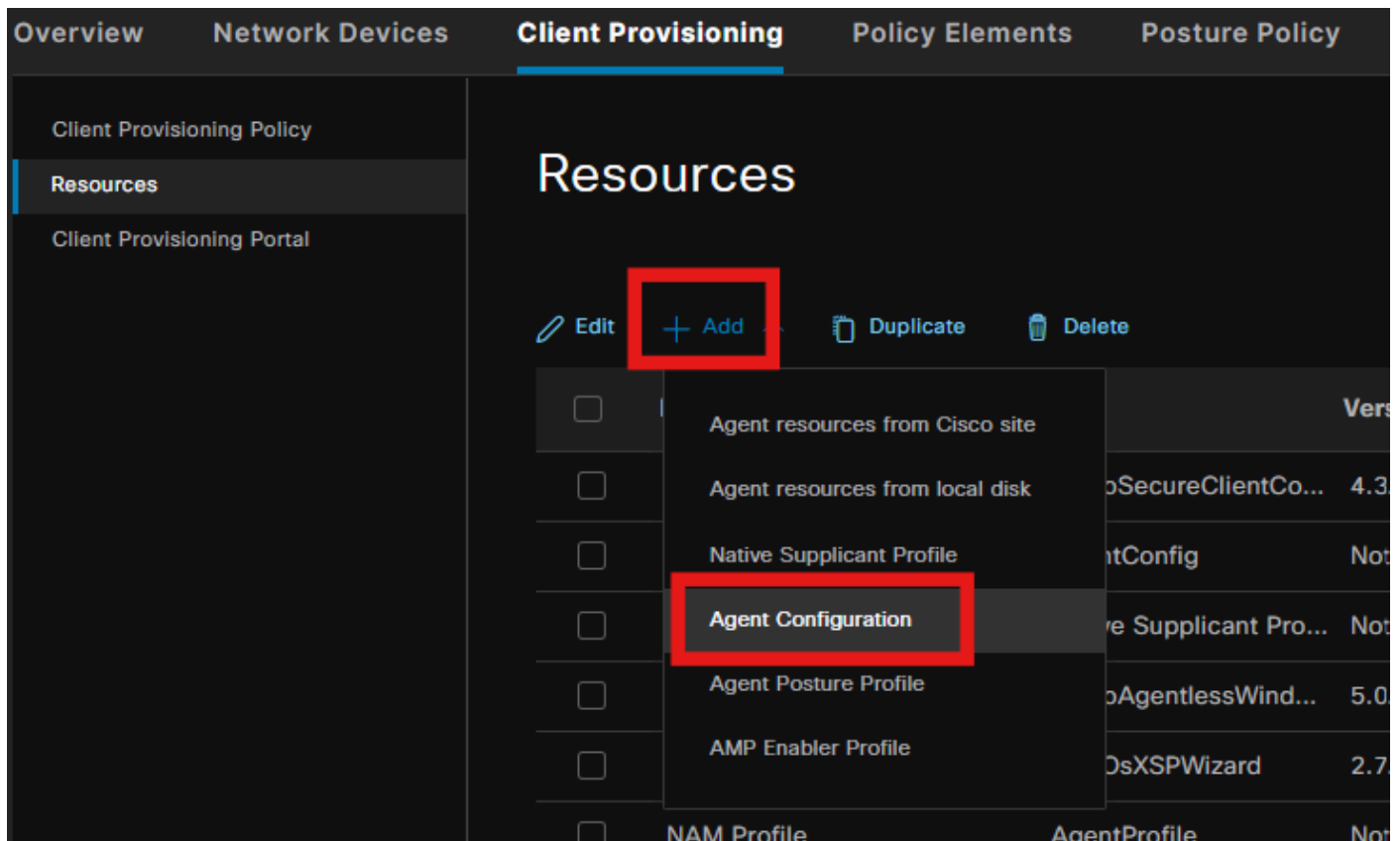
- Category:** A dropdown menu set to 'Customer Created Packs'.
- Type:** A dropdown menu set to 'Agent Profile'.
- * Name:** A text field containing 'New Profile'.
- Description:** A text area.
- Choose File:** A button to upload a file, with 'configuration.xml' listed below it.
- Submit:** A blue button at the bottom left, highlighted with a red box.
- Cancel:** A blue link at the bottom right.

Paso 4. Crear un perfil de postura



Desde la sección Protocolo de postura, no olvide agregar * para permitir que el agente se conecte a todos los servidores.

Paso 5. Crear configuración de agente



Seleccione el paquete de módulo de cumplimiento y cliente seguro cargado y, en la selección de Módulo, seleccione los módulos ISE Posture, NAM y DART.

Engine

Work Centers / Posture

Overview

Network Devices

Client Provisioning

Policy Elements

Posture Policy

Policy Sets

Client Provisioning Policy

Resources

Client Provisioning Portal

Agent Configuration > New Agent Configuration

* 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

☒

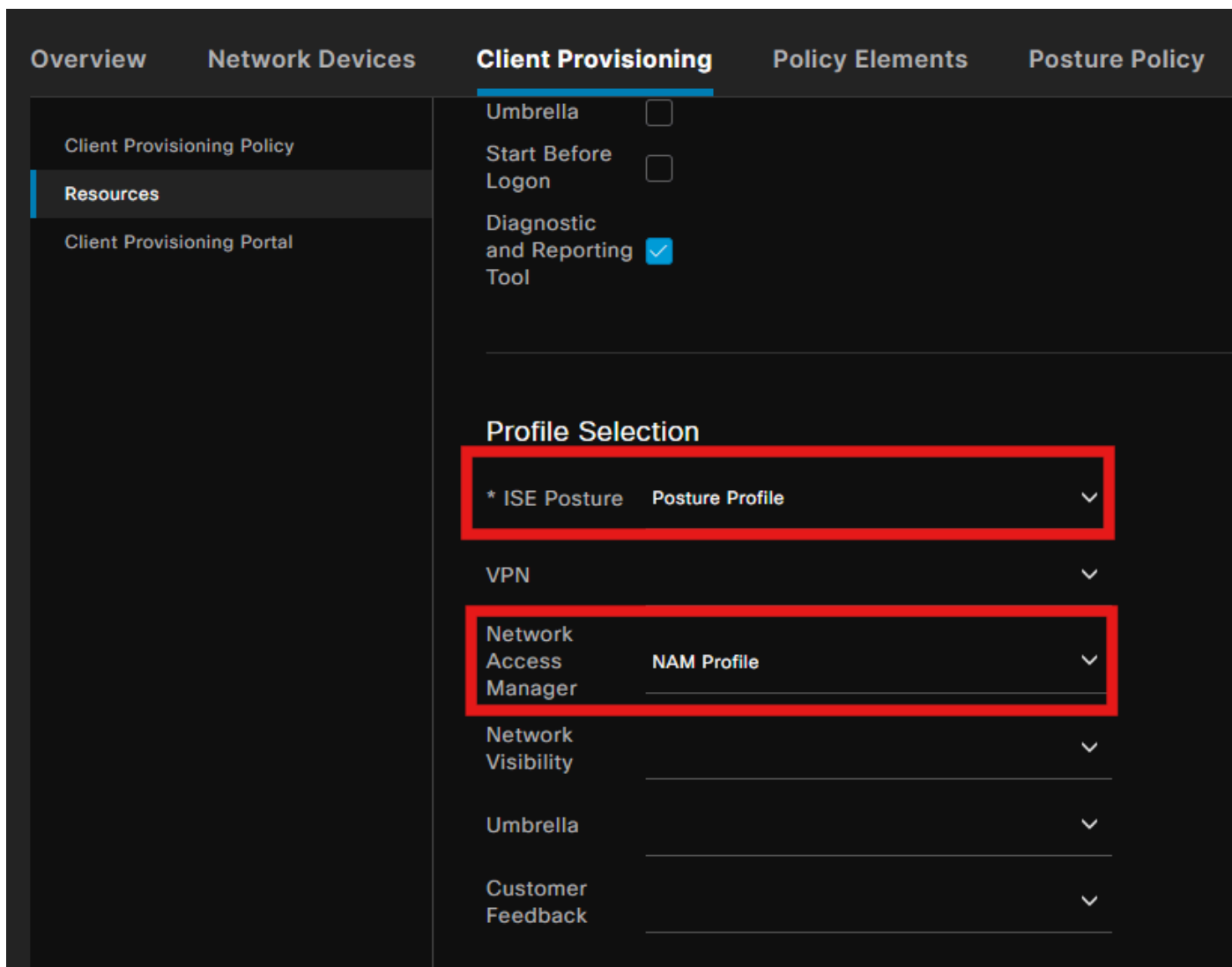
Secure Firewall Posture

☐

Network Visibility

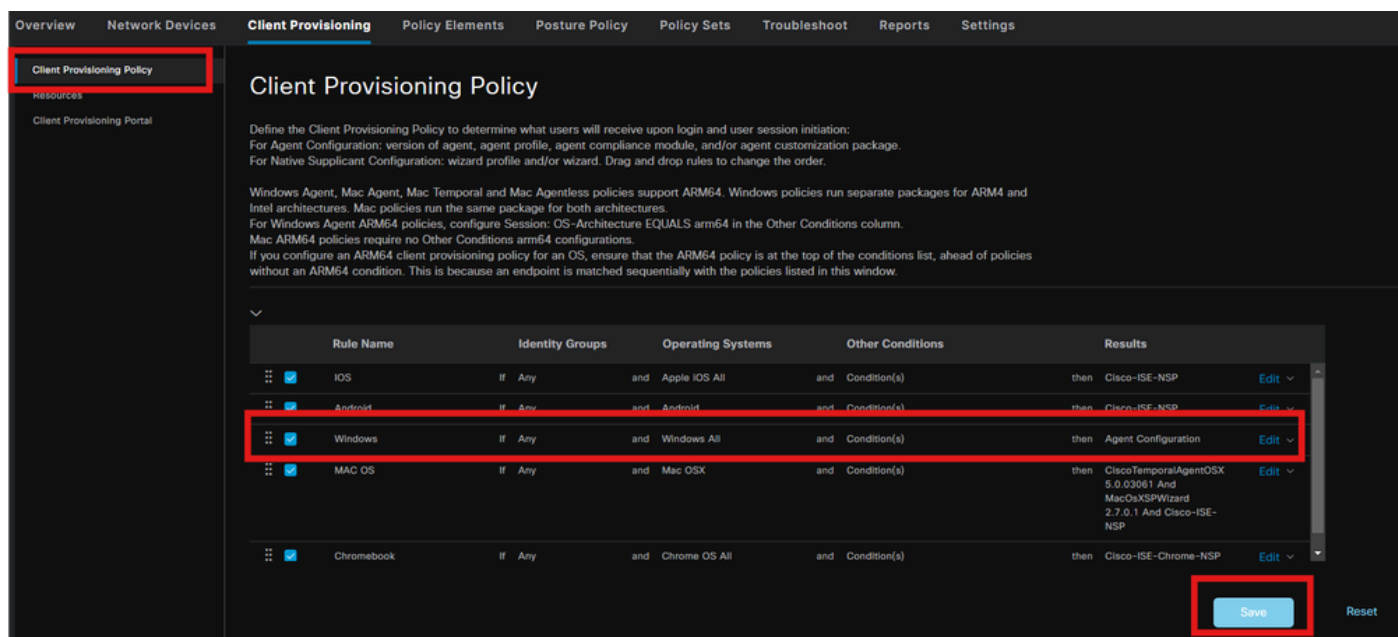
☐

En Profile select, elija el Posture y el NAM Profile y haga clic en Submit.



Paso 6. Política de aprovisionamiento de clientes

Cree una directiva de aprovisionamiento de cliente para el sistema operativo Windows y seleccione la configuración de agente creada en el paso anterior.



Paso 7. Política de estado

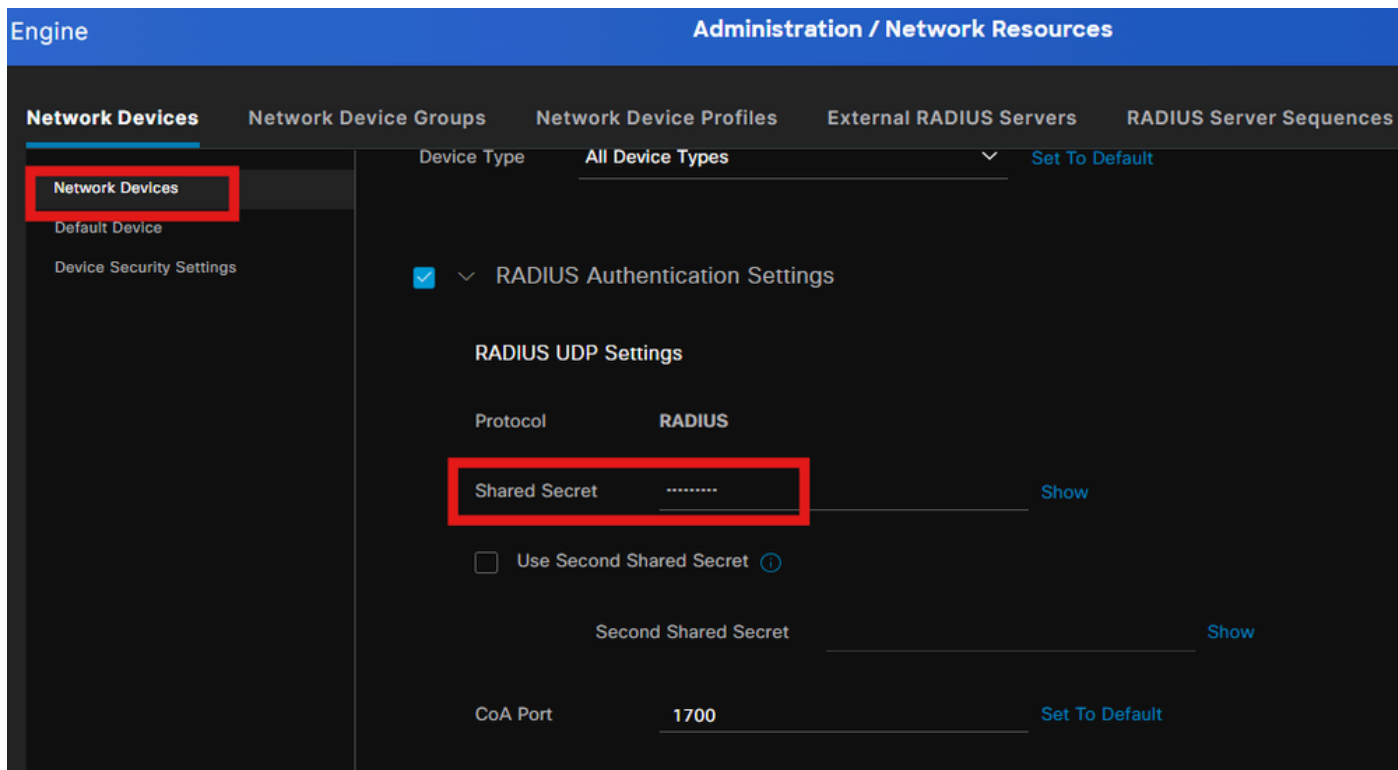
Para obtener información sobre cómo crear la política de estado y las condiciones, consulte esta guía [ISE Posture Prescriptive Deployment Guide](#).

Paso 8. Agregar dispositivo de red

Para agregar la dirección IP del switch y la clave secreta compartida RADIUS, navegue hasta Administration > Network Resources.

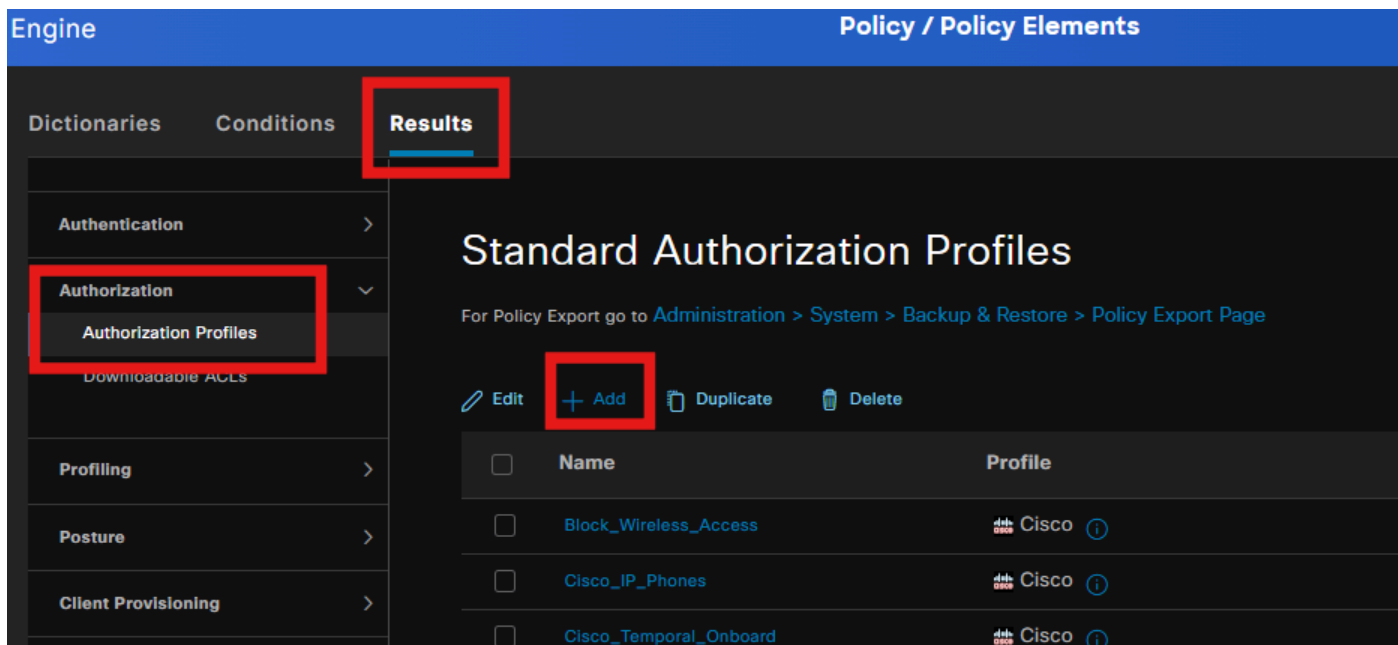
The screenshot displays the Cisco ISE Administration console interface. The top navigation bar shows 'Engine' and 'Administration / Network Resources'. The left sidebar contains the 'Network Devices' menu, which is highlighted with a red box. The main content area is titled 'Network Devices' and shows the configuration for a device named 'aaa'. The 'IP Address' field is highlighted with a red box, showing the value '10.197.213.22 / 32'. Other fields visible include 'Name' (aaa), 'Description', 'Device Profile' (Cisco), and 'Model Name'.

Field	Value
Name	aaa
Description	
IP Address	10.197.213.22 / 32
Device Profile	Cisco
Model Name	



Paso 9. Perfil de autorización

Para crear un perfil de redirección de postura, navegue hasta Política > Elementos de política > Resultados.



En Tareas comunes, seleccione el Portal de aprovisionamiento de clientes con ACL de redirección.

Dictionaryes Conditions **Results**

Authentication >

Authorization >

Authorization Profiles

Downloadable ACLs

Profiling >

Posture >

Client Provisioning >

Authorization Profiles > Redirection

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

Paso 10. Protocolos permitidos

Vaya a Policy > Policy elements > Results > Authentication > Allowed Protocols, seleccione la configuración de EAP Chaining.

Dictionaryes Conditions **Results**

Authentication >

Allowed Protocols

Authorization >

Profiling >

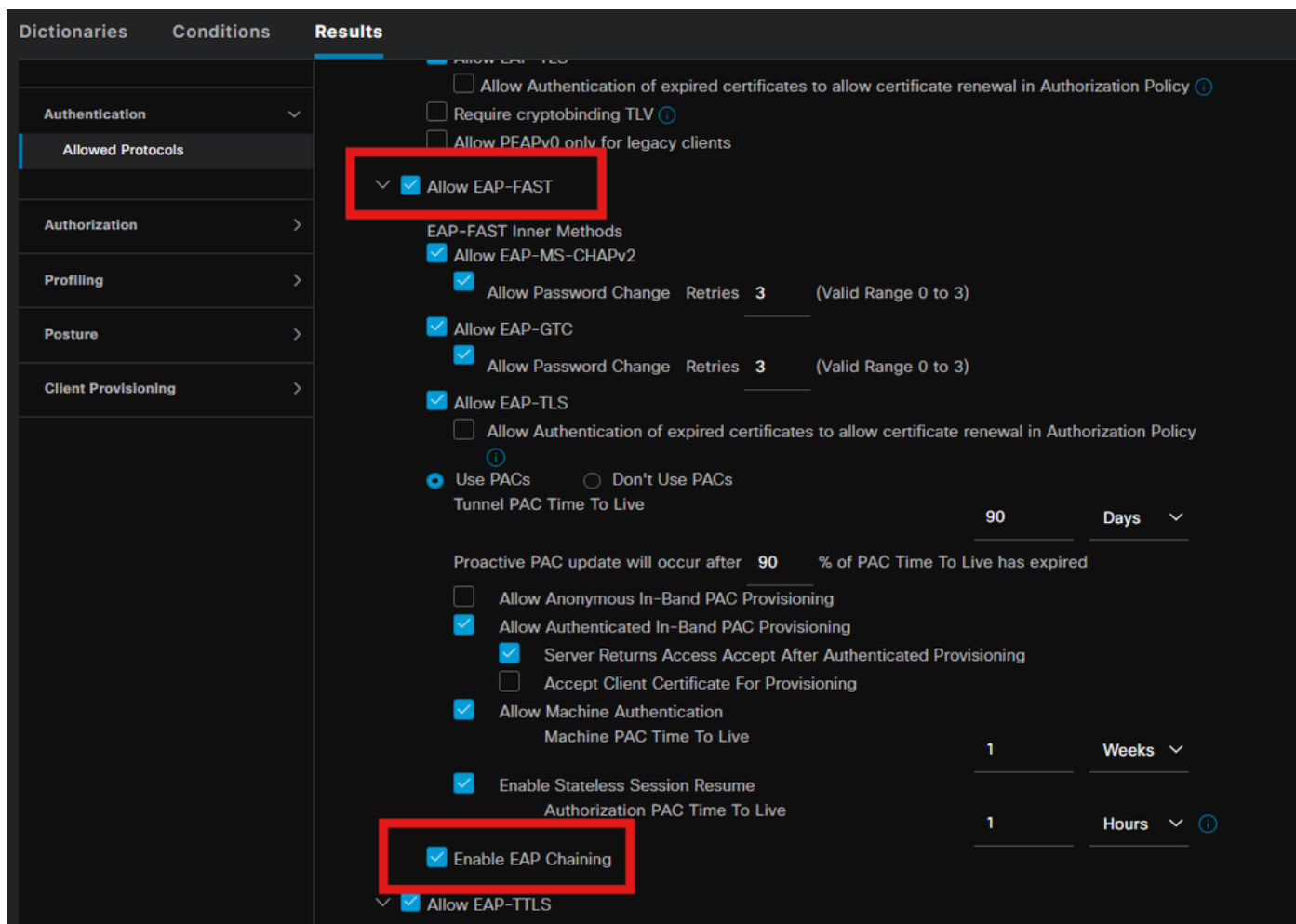
Posture >

Allowed Protocols Services List > **Default Network Access**

Allowed Protocols

Name **Default Network Access**

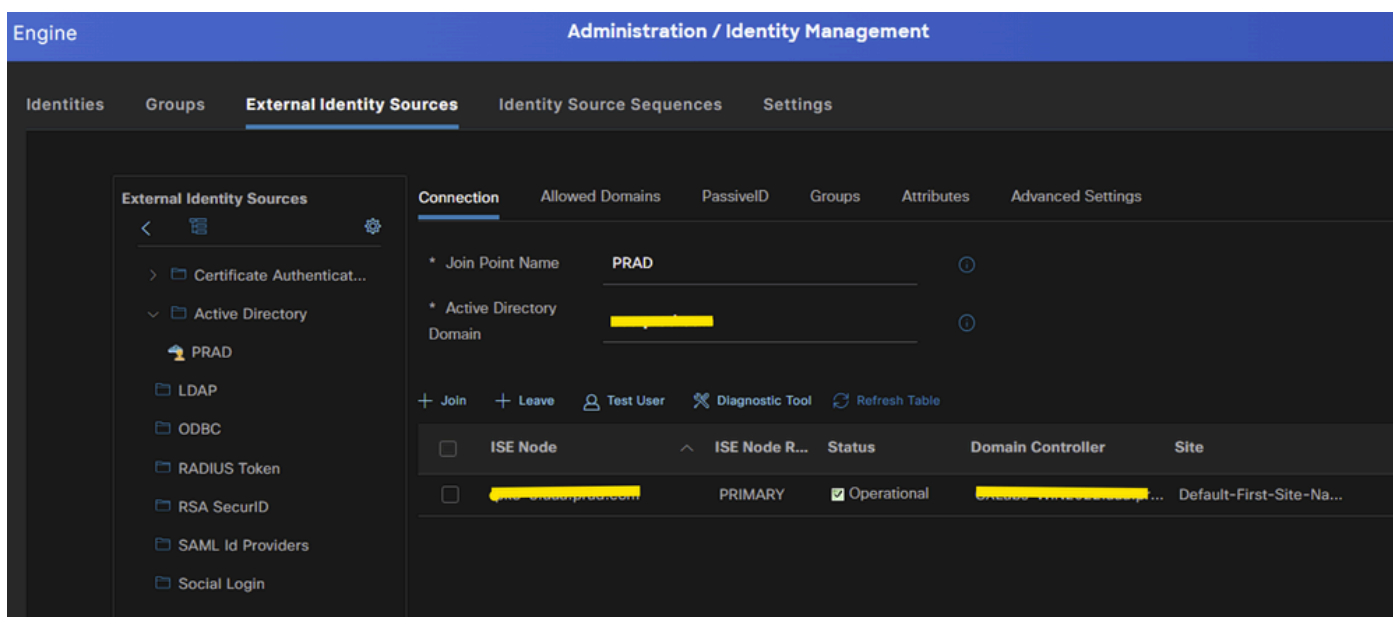
Description **Default Allowed Protocol Service**



Paso 11. Active Directory

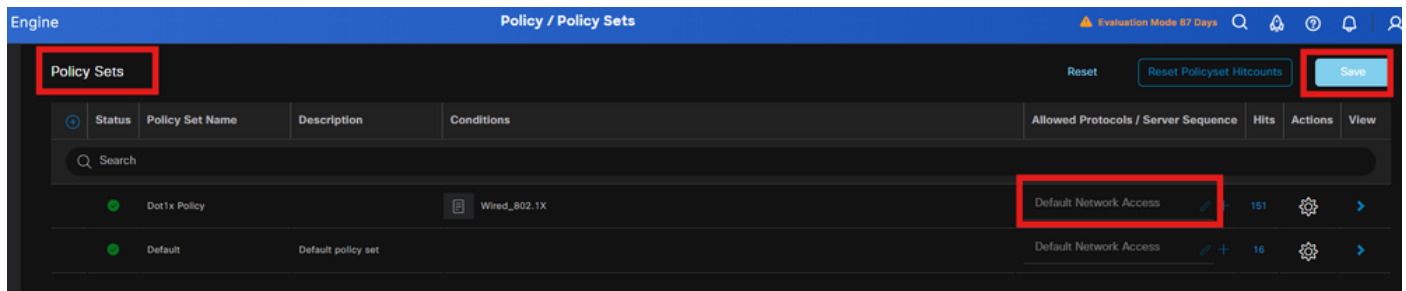
Validar ISE se une con el dominio de directorio activo y se seleccionan los grupos de dominio, si es necesario para las condiciones de autorización.

Administration > Identity Management > External Identity Sources > Active Directory

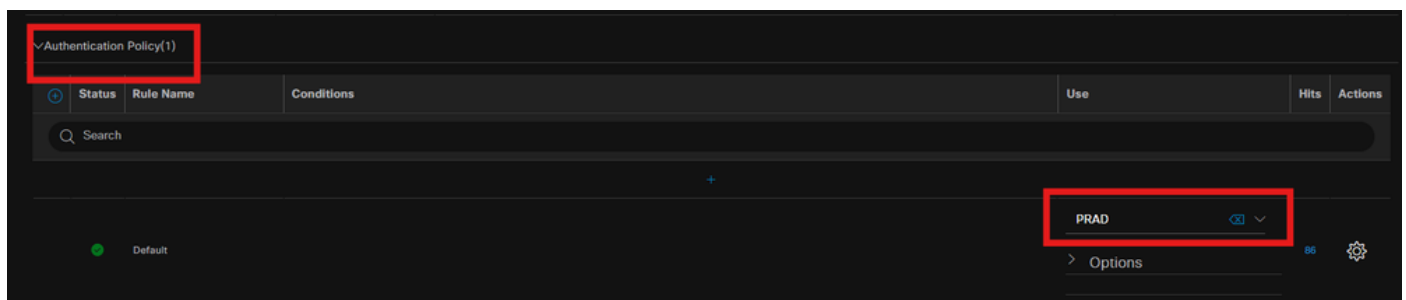


Paso 12. Conjuntos de políticas

Cree un conjunto de políticas en ISE para autenticar la solicitud dot1x. Vaya a Política > Conjuntos de políticas.



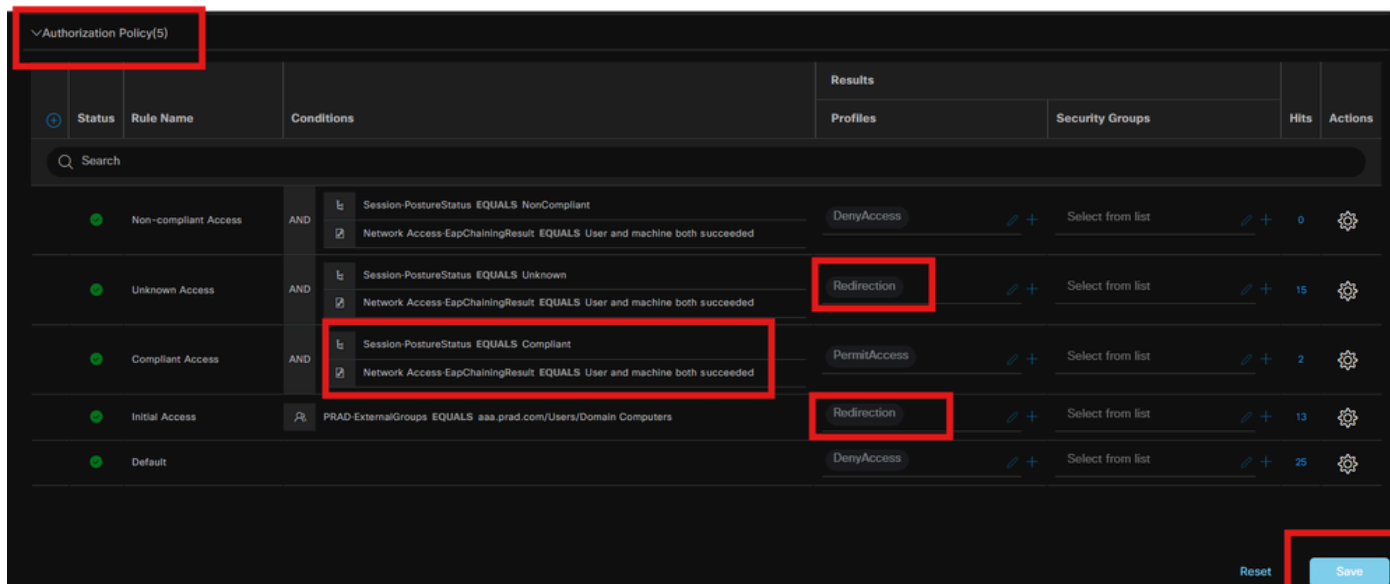
Seleccione el directorio activo como origen de identidad para la política de autenticación.



Configure diferentes reglas de autorización basadas en el estado desconocido, no conforme y conforme.

En este caso práctico.

- Acceso inicial: Redirección a ISE Client Provisioning Portal para instalar Secure client agent y NAM Profile.
- Acceso desconocido: Acceso al portal de aprovisionamiento de clientes para la detección de estado basada en redirección.
- Acceso conforme: Acceso completo a la red.
- No conforme: Denegar acceso.



Validación

Paso 1. Descargue e instale el módulo Secure Client Posture/NAM desde ISE

Seleccione el punto final autenticado a través de dot1x, pulsando la regla Initial Access Authorization . Vaya a Operaciones > Radio > Registros en directo.

Time	Status	Details	Endpoint ID	Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture Status
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

En Switch, especifique la URL de redirección y la ACL que se aplicarán al punto final.

```
Switch#show authentication session interface te1/0/24 details
```

Interfaz: Diez GigabitEthernet1/0/24

IIF-ID: 0x19262768

Dirección MAC: x4x6.xxxx.xxxx

Dirección IPv6: Desconocido

Dirección IPv4: <client-IP>

Nombre de usuario: host/DESKTOP-xxxxxxx.xxx

Estado: Autorizado

Dominio: DATOS

Modo de host Oper: de host único

Oper control dir: ambas

Tiempo de espera de sesión: N/A

ID de sesión común: 16D5C50A0000002CF067366B

ID de sesión de cuenta: 0x0000001f

Manejar: 0x7a000017

Política actual: POLICY_Te1/0/24

Políticas locales:

Plantilla de servicio: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (prioridad 150)

Política de seguridad: Debe asegurar

Estado de seguridad: Enlace no seguro

Políticas de servidor:

ACL de redirección de URL: redirect-acl

Redirección de URL:

<https://ise33.xxxx:8443/portal/gateway?sessionId=16D5C50A0000002CF067366A&portal=ee39fd08-7180-4995-8aa2-9fb282645a8f&action=cpp&token=518f857900a37f9afc6d2da8b6fe3bc2>

ACL de ACS: xACSACLx-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3

Lista de estados de método:

Estado del método

dot1x Auténtica Correcta

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

Network Layer Address	Link Layer Address	Interface	vlan	prlvl	age	state	Tiempo restante
ARP X.X.X.X	b496.91f9.568b	Te1/0/24	1000	0005	4mn	ALCANZABLE	39 s try 0

En el terminal, verifique el tráfico redirigido a la condición de ISE y haga clic en Start para descargar Network Setup Assistant en el terminal.

Google Chrome isn't your default browser

Set as default

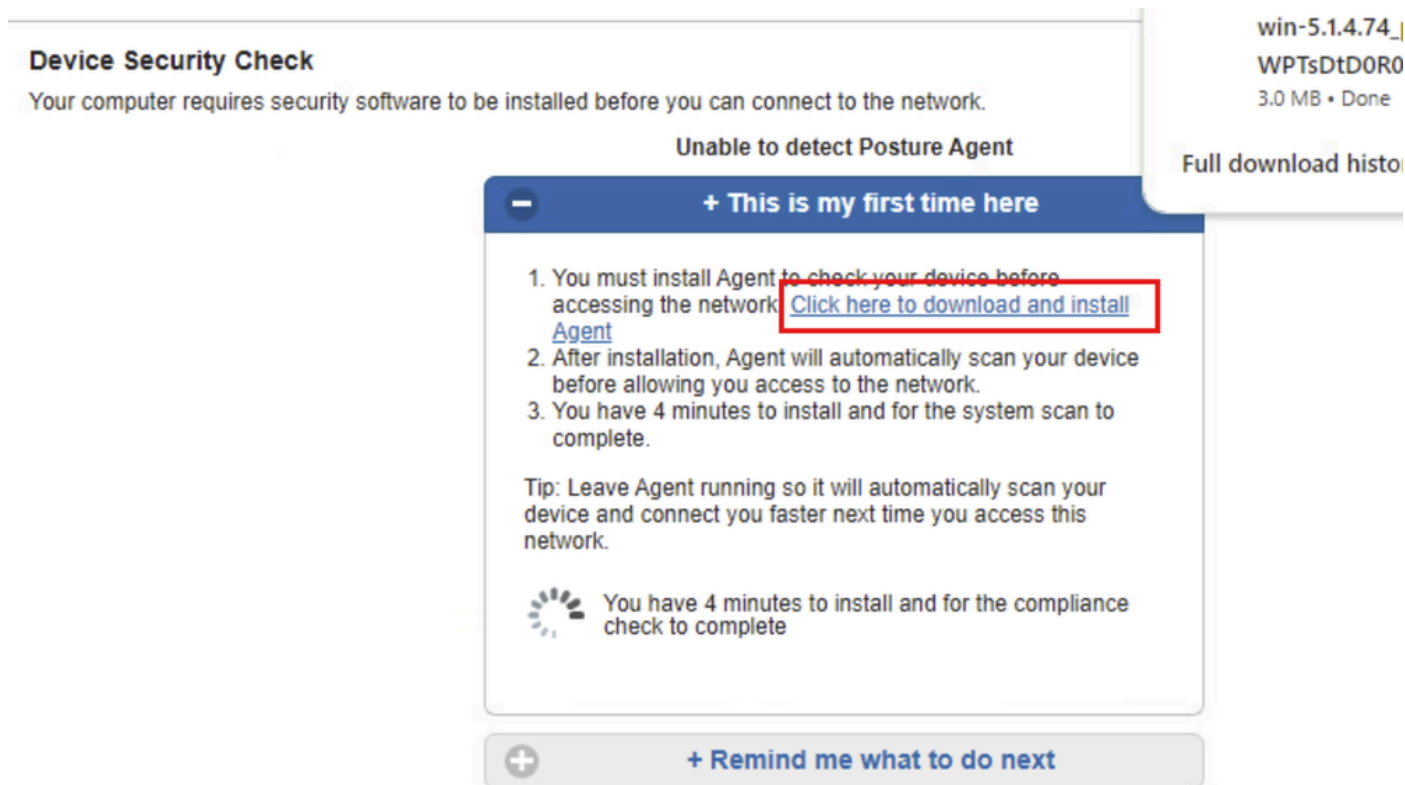


Client Provisioning Portal

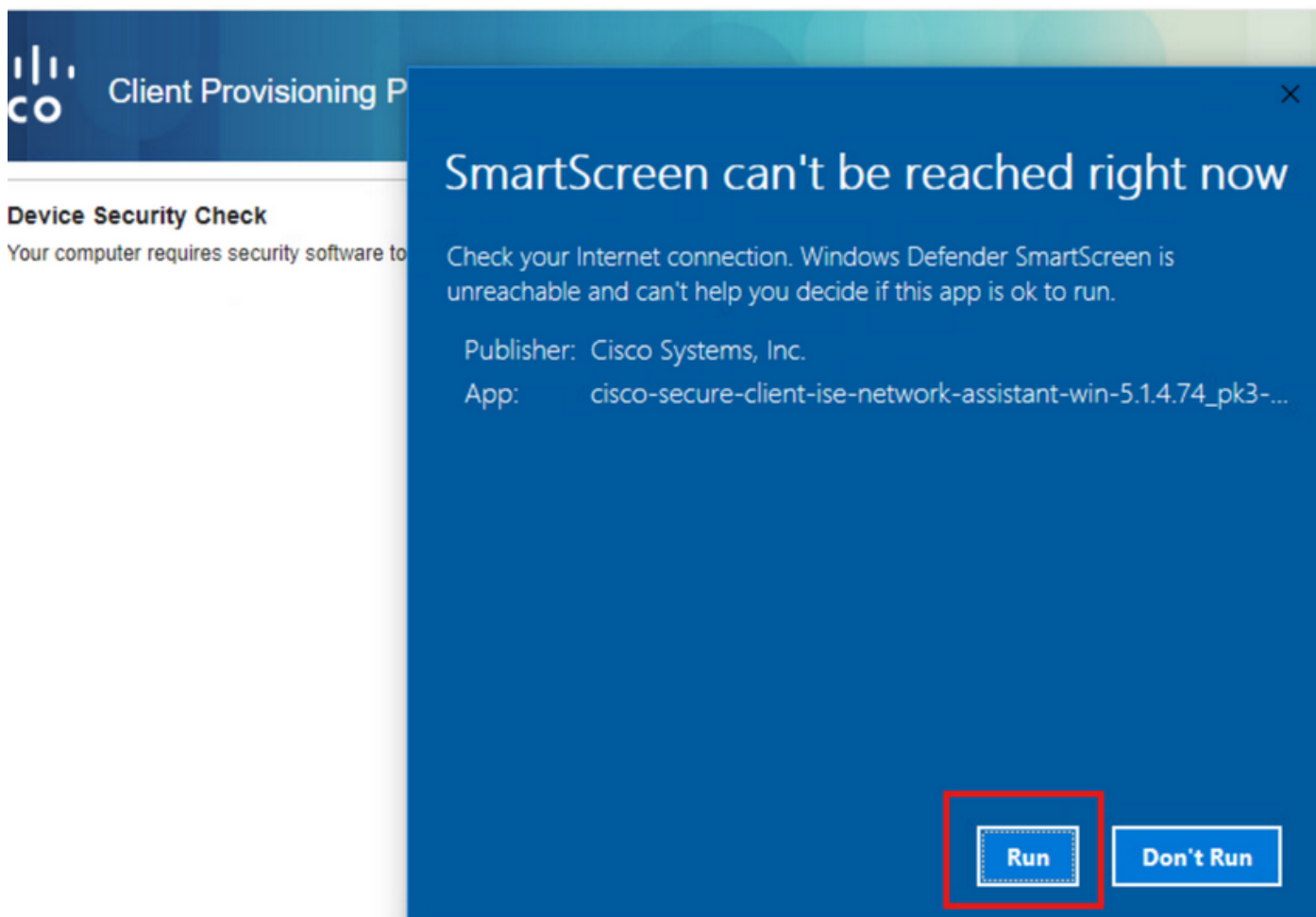
Device Security Check

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

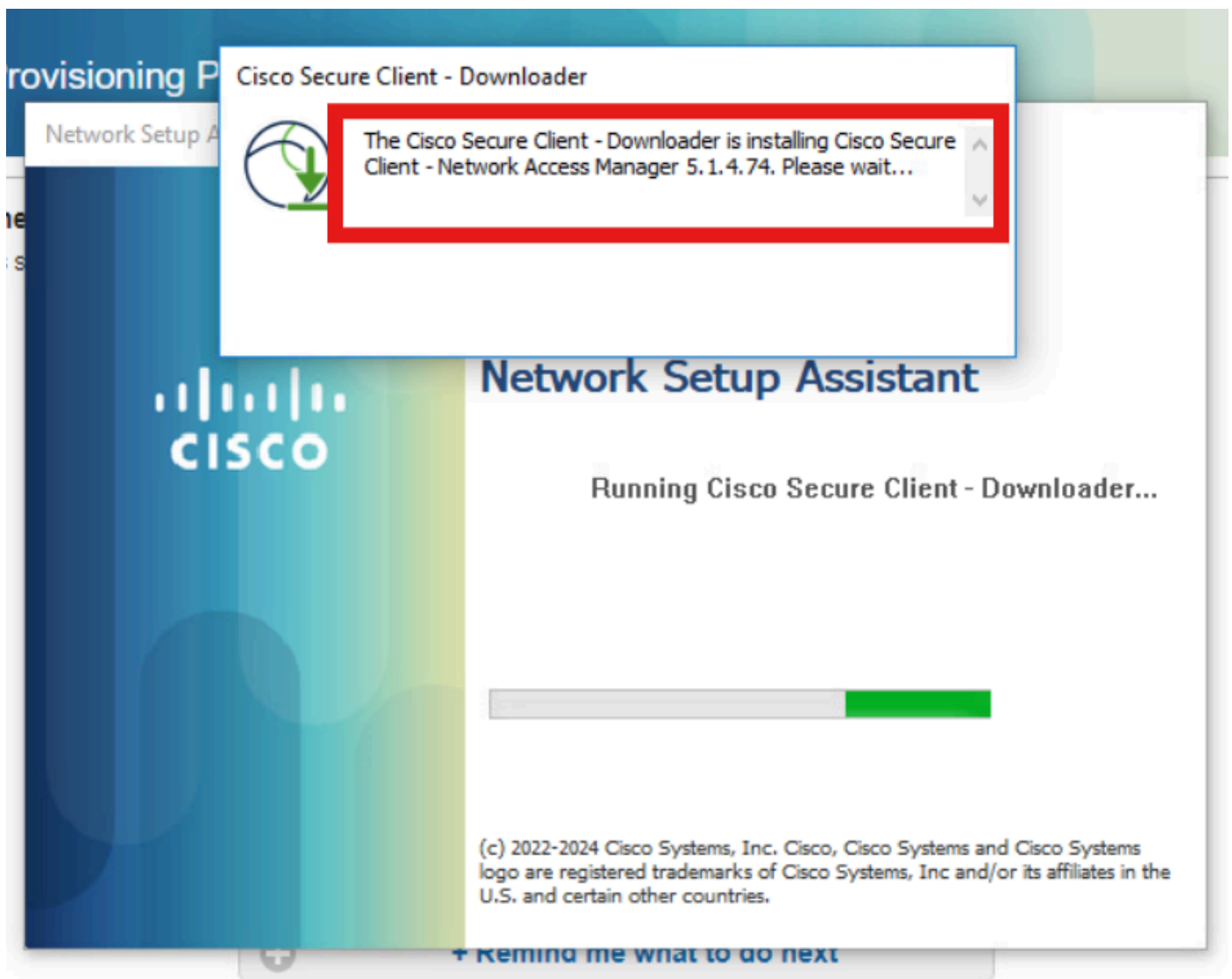
Start



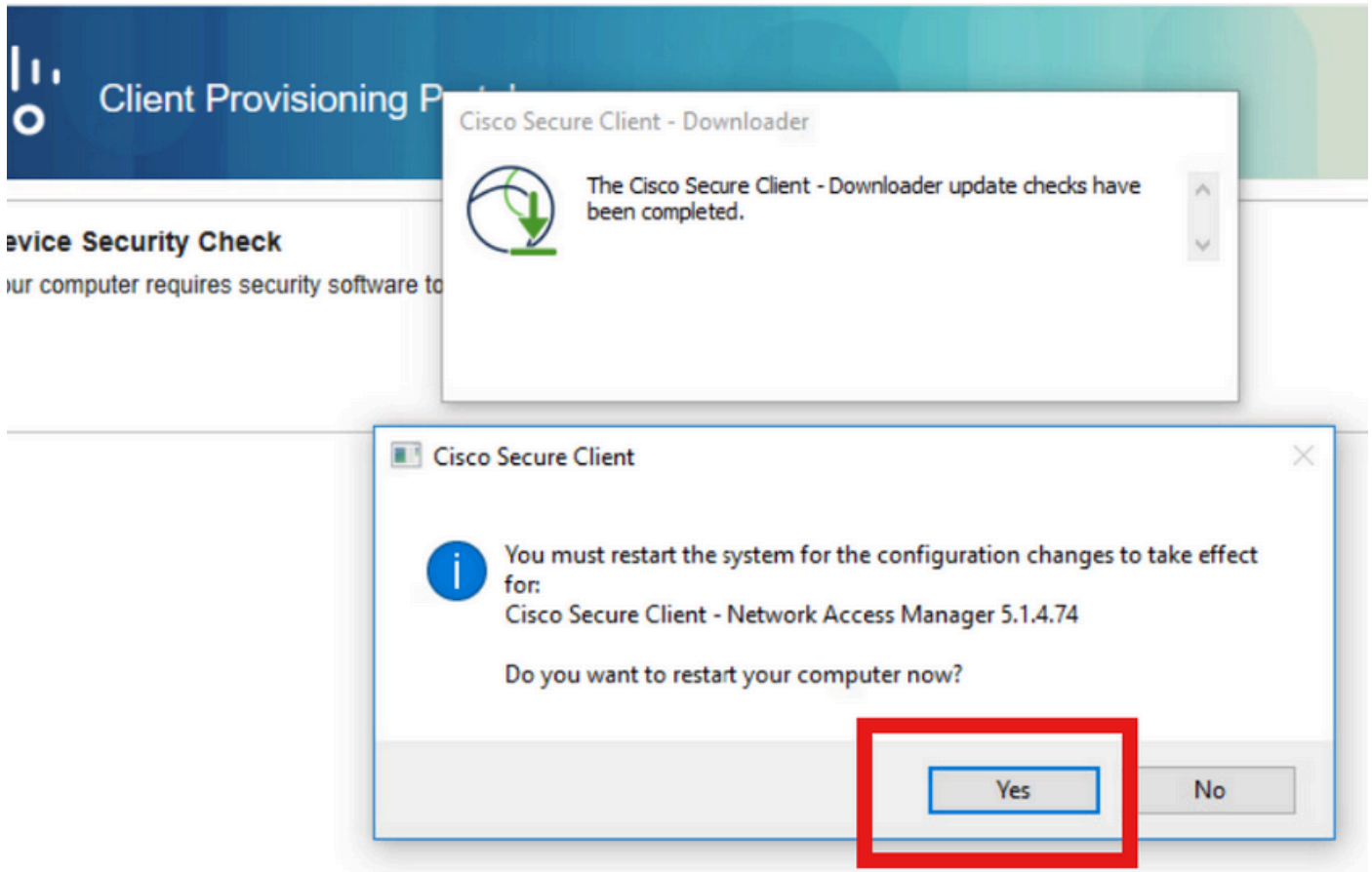
Haga clic en Run para instalar la aplicación NSA.



Ahora, la NSA invoca la descarga de Secure Client Agent desde ISE e instala la condición, el módulo NAM y el archivo configuration.xml del perfil NAM.



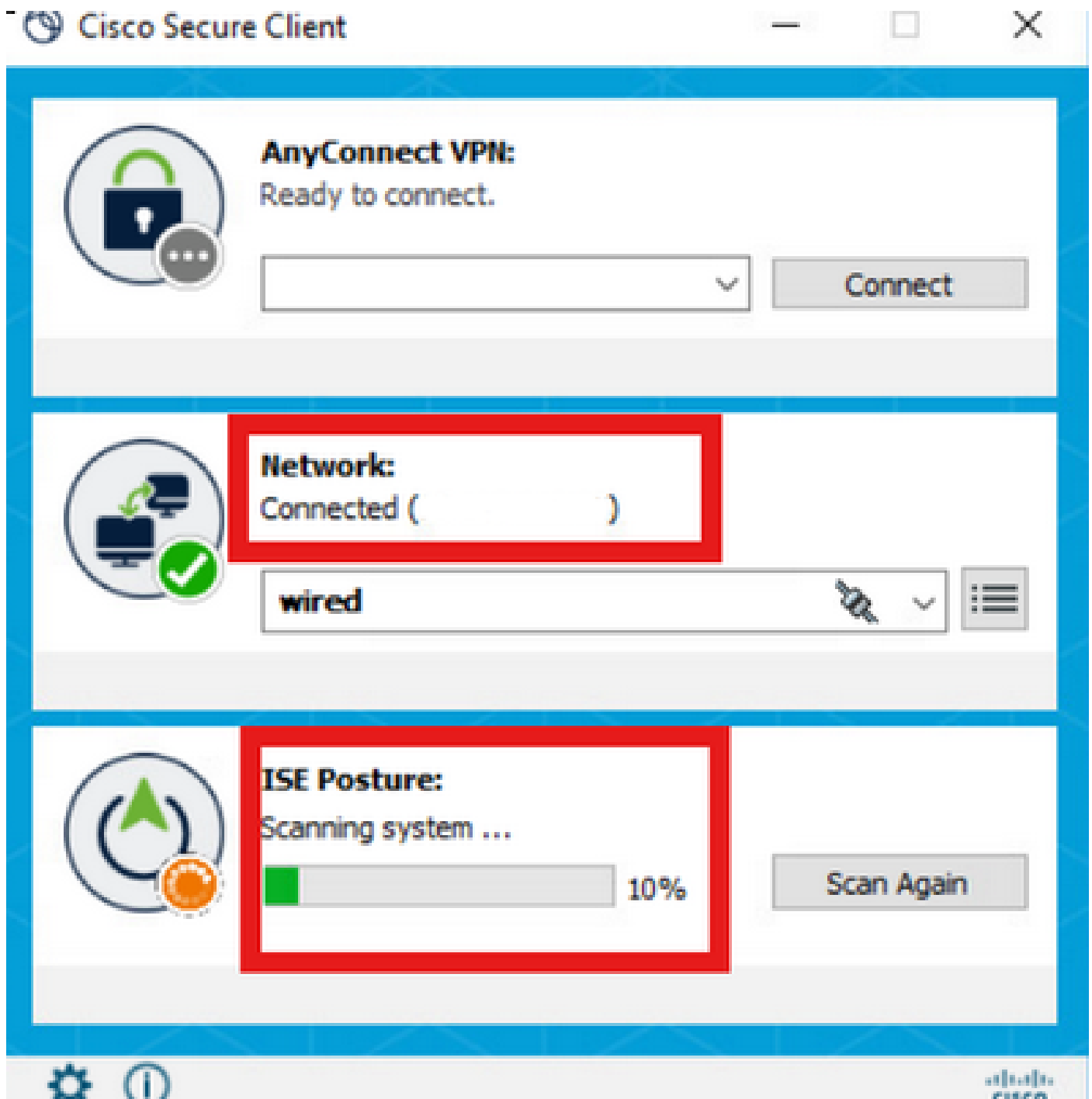
Mensaje de reinicio que se activa tras la instalación de NAM. Haga clic en Sí



Paso 2. EAP-FAST

Una vez que el equipo se reinició y el usuario inició sesión, el NAM autentica tanto al usuario como al equipo a través de EAP-FAST.

Si el terminal se autentica correctamente, NAM muestra que está conectado y el módulo de postura activa el análisis de posición.



En ISE Live Logs, el terminal está alcanzando ahora la regla de acceso desconocido.

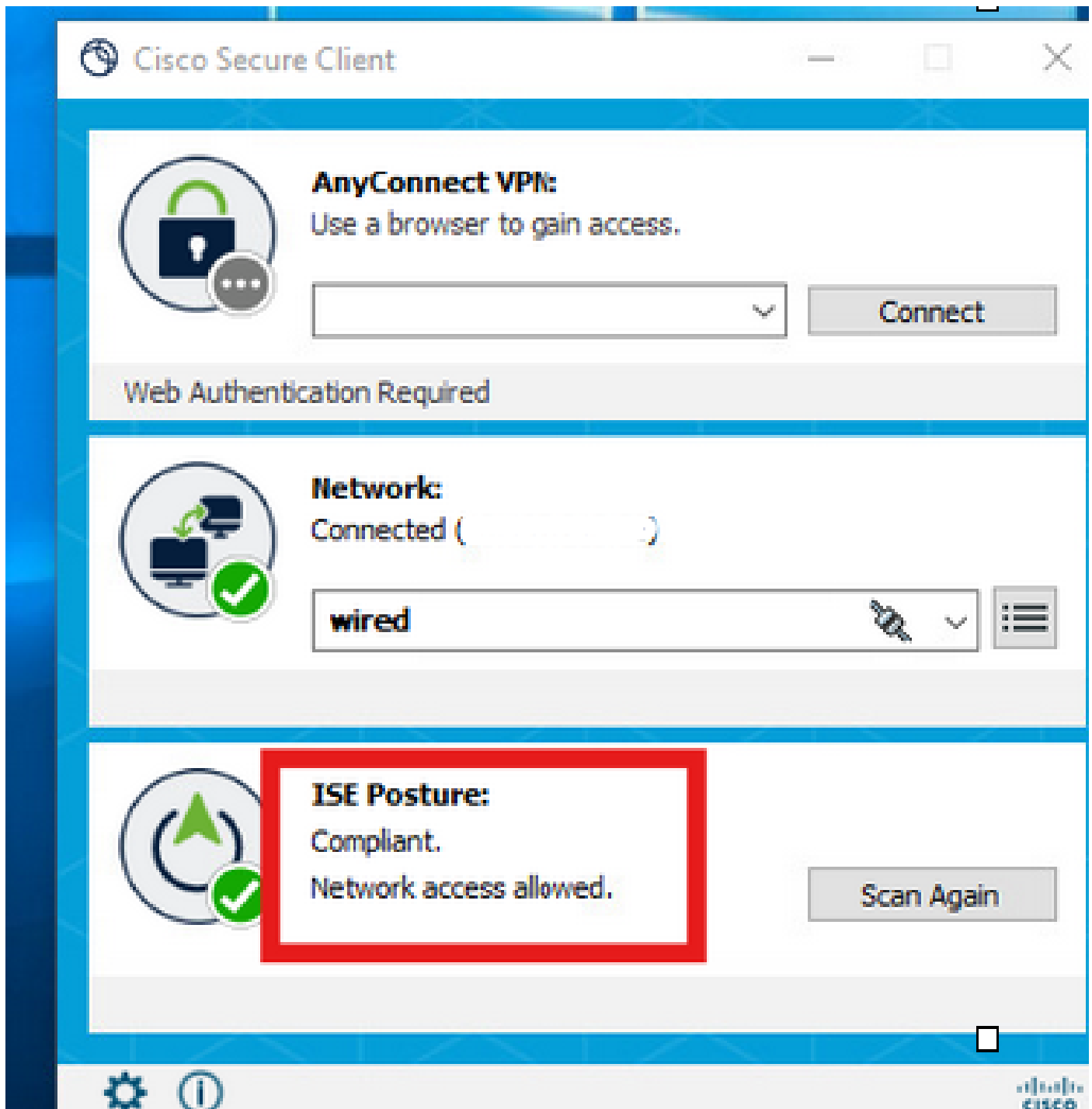
Jul 27, 2024 12:29:06...			user1.host/DESKTOP-QSC...	Dot1x Policy >> Default	Dot1x Policy >> Unknown Access	Redirection	Pending
Jul 27, 2024 12:28:48...			host/DESKTOP-QSCE4P3	Dot1x Policy >> Default	Dot1x Policy >> Initial Access	Redirection	Pending

Ahora el protocolo de autenticación es EAP-FAST basado en la configuración del perfil NAM y el resultado de EAP-Chaining es correcto.

AuthenticationStatus	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatched...	Unknown Access
IssuedPacInfo	Issued PAC type=Machine Authorization with expiration time: Sat Jul 27 01:29:06 2024
EndPointMACAddress	B4-96-91-F9-56-8B
EapChainingResult	User and machine both succeeded
ISEPolicySetName	Dot1x Policy
IdentitySelectionMatchedRule	Default

Paso 3. Análisis de estado

El módulo de estado de cliente seguro activa el análisis de estado y se marca como queja según la política de estado de ISE.



El CoA se activa después del análisis de posición y ahora el terminal llega a la política de acceso de quejas.

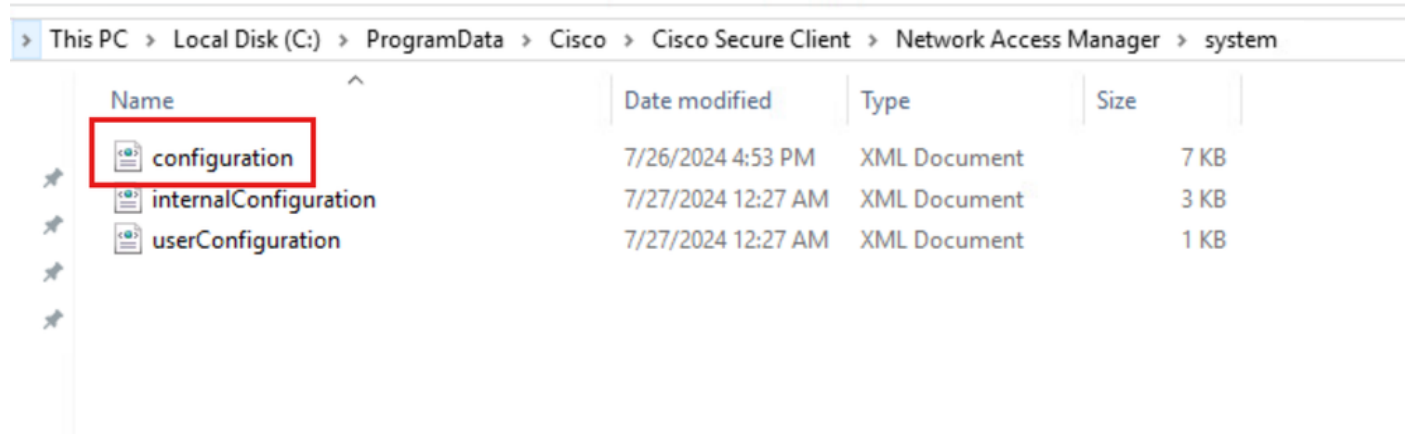
Time	Status	Details	Endpoint ID	Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture Status
Jul 27, 2024 12:29:32...			B4:96:91:F9:56:8B	user1_host/DESKTOP-QSC...	Dot1x Policy >> Default	Dot1x Policy >> Compliant Access	PermitAccess	Compliant
Jul 27, 2024 12:29:32...			B4:96:91:F9:56:8B	user1_host/DESKTOP-QSC...	Dot1x Policy >> Default	Dot1x Policy >> Compliant Access	PermitAccess	Compliant
Jul 27, 2024 12:29:31...			B4:96:91:F9:56:8B	user1_host/DESKTOP-QSC...	Dot1x Policy >> Default	Dot1x Policy >> Unknown Access	Redirection	Pending
Jul 27, 2024 12:29:06...			B4:96:91:F9:56:8B	user1_host/DESKTOP-QSC...	Dot1x Policy >> Default	Dot1x Policy >> Initial Access	Redirection	Pending
Jul 27, 2024 12:28:48...			B4:96:91:F9:56:8B	host/DESKTOP-QSCE4P3	Dot1x Policy >> Default	Dot1x Policy >> Initial Access	Redirection	Pending

Troubleshoot

Paso 1. Perfil de NAM

Verifique que el archivo configuration.xml del perfil NAM esté presente en esta trayectoria en la PC después de la instalación del módulo NAM.

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

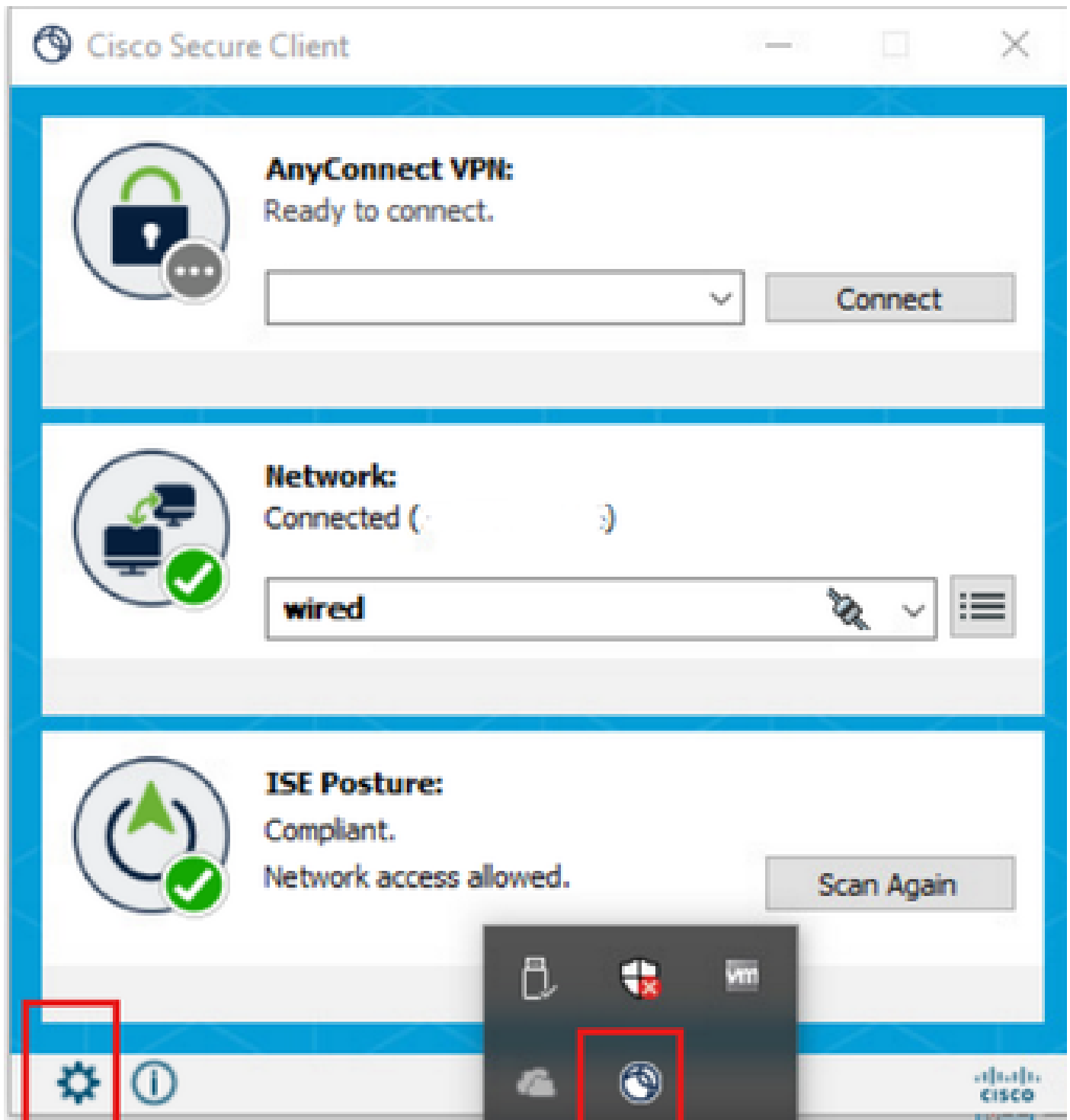


The screenshot shows a Windows File Explorer window with the address bar displaying the path: This PC > Local Disk (C:) > ProgramData > Cisco > Cisco Secure Client > Network Access Manager > system. The main pane shows a list of files with columns for Name, Date modified, Type, and Size. The file 'configuration' is highlighted with a red box.

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

Paso 2. Registro extendido NAM

Haga clic en el icono Secure Client de la barra de tareas y seleccione el icono settings.



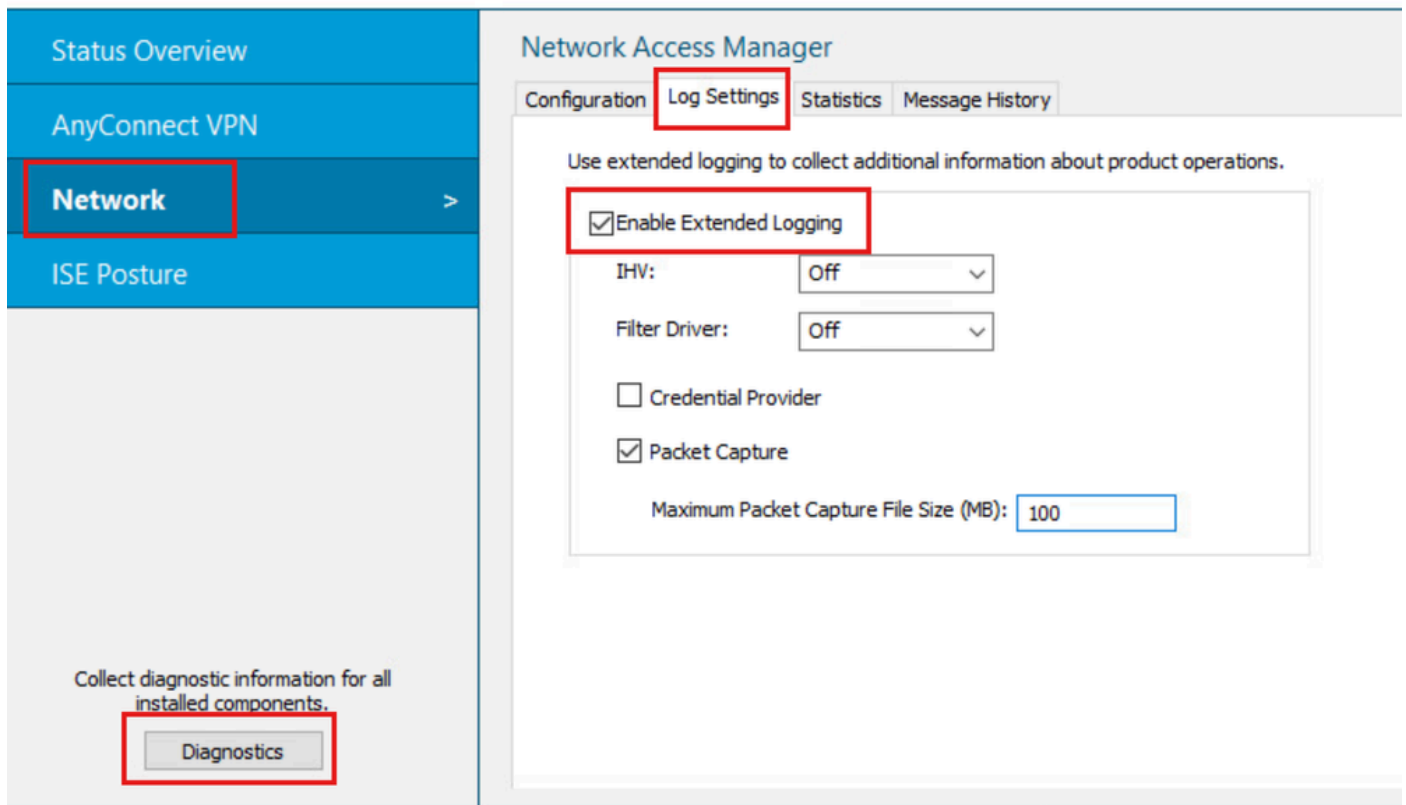
Vaya a la pestaña Red > Configuración de registro. Marque la casilla de verificación Enable Extended Logging.

Establezca el tamaño del archivo de captura de paquetes en 100 MB.

Después de reproducir el problema, haga clic en Diagnostics para crear el paquete DART en el terminal.



Secure Client



La sección Historial de Mensajes muestra los detalles de cada paso que NAM realizó.

Paso 3. Depuraciones en el switch

Habilite estos debugs en el switch para resolver problemas de dot1x y flujo de redirección.

```
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
```

Para ver los registros

show logging

show logging process smd internal

Paso 4. Depuraciones en ISE

Recopile el paquete de soporte de ISE con estos atributos que se establecerán en el nivel de depuración:

- postura
- portal
- aprovisionamiento
- Runtime-AAA
- nsf
- nsf-session
- suizo
- client-webapp

Información Relacionada

[Configuración de Secure Client NAM para Dot1x con Windows e ISE 3.2](#)

[Guía de implementación prescriptiva de estado de ISE](#)

[Resolución de problemas Dot1x en Cisco IOS® XE Catalyst 9000 Series Switches](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).