

# Configure and Deploy Secure Client NAM Profile through ISE 3.3 on Windows

## Contents

---

### [Introduction](#)

### [Background Information](#)

### [Prerequisites](#)

[Requirements](#)

[Components Used](#)

### [Configuration](#)

[Network Diagram](#)

[Data Flow](#)

[Configure Switch](#)

[Download the Secure client Package](#)

### [ISE Configuration](#)

[Step 1. Upload the Package on ISE](#)

[Step 2. Create a NAM Profile from Profile editor tool](#)

[Step 3. Upload the NAM Profile on ISE](#)

[Step 4. Create a Posture Profile](#)

[Step 5. Create Agent Configuration](#)

[Step 6. Client Provisioning Policy](#)

[Step 7. Posture Policy](#)

[Step 8. Add Network device](#)

[Step 9. Authorization Profile](#)

[Step 10. Allowed Protocols](#)

[Step 11. Active Directory](#)

[Step 12. Policy sets](#)

### [Verify](#)

[Step 1. Download and Install Secure Client Posture/NAM module from ISE](#)

[Step 2. EAP-FAST](#)

[Step 3. Posture Scan](#)

### [Troubleshoot](#)

[Step 1. NAM Profile](#)

[Step 2. NAM Extended Logging](#)

[Step 3. Debugs on Switch](#)

[Step 4. Debugs on ISE](#)

### [Related Information](#)

---

## Introduction

This document describes how to deploy the Cisco Secure Client Network Access Manager (NAM) profile

through Identity Services Engine (ISE).

## Background Information

EAP-FAST authentication occurs in two phases. In the first phase, EAP-FAST employs a TLS handshake to provide and authenticate key exchanges using Type-Length-Values (TLV) objects to establish a protected tunnel. These TLV objects are used to convey authentication-related data between the client and server. Once the tunnel is established, the second phase begins with the client and ISE node engaging in further conversations to establish the required authentication and authorization policies.

The NAM configuration profile is set up to use EAP-FAST as the authentication method and is available for administratively defined networks.

In addition, both machine and user connection types can be configured within the NAM configuration profile.

The corporate Windows device gain full corporate access using the NAM with Posture check.

The personal Windows device gain access to a restricted network using the same NAM configuration.

This document provides instructions for deploying the Cisco Secure Client Network Access Manager (NAM) profile via the Identity Services Engine (ISE) Posture Portal using web deployment, along with Posture Compliance Check.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Identity Services Engine (ISE)
- AnyConnect NAM and Profile Editor
- Posture Policy
- Cisco Catalyst configuration for 802.1x services

### Components Used

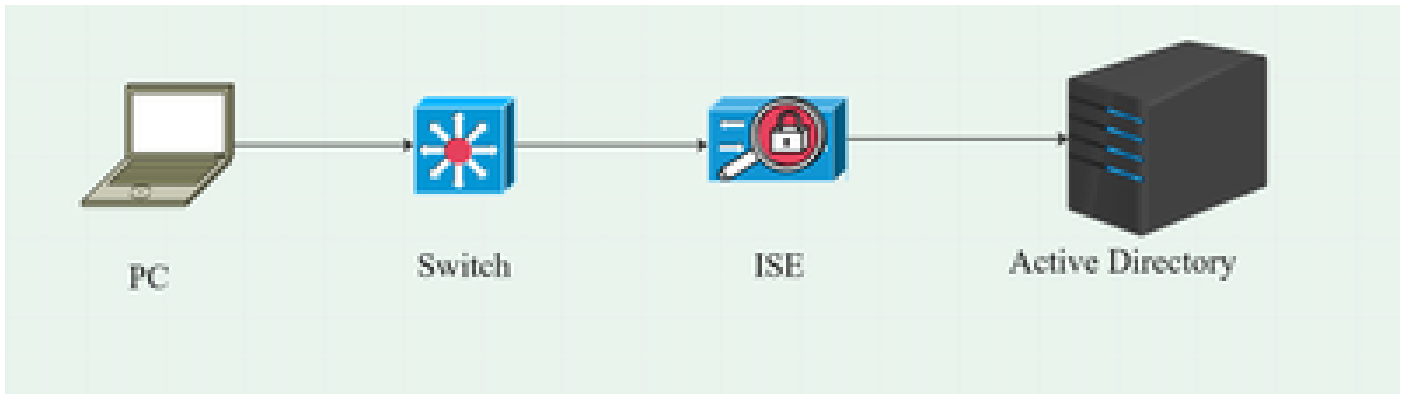
The information in this document is based on these software and hardware versions:

- Cisco ISE, Release 3.3 and later
- Windows 10 with Cisco Secure Mobility Client 5.1.4.74 and later
- Cisco Catalyst 9200 switch with software Cisco IOS® XE 17.6.5 and later
- Active Directory 2016

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

## Configuration

### Network Diagram



## Data Flow

When a PC connects to the network, the ISE provides the authorization policy for redirection to the Posture Portal.

The http traffic on the PC is redirected to the ISE Client Provisioning Page, where the NSA application is downloaded from ISE.

The NSA then installs the Secure Client agent modules on the PC.

After the agent installation is completed, the agent downloads the Posture profile and NAM profile configured on ISE.

The installation of the NAM module triggers a restart on the PC.

After the restart, NAM module performs EAP-FAST authentication based on the NAM profile.

The Posture scan is then triggered and compliance is checked based on the ISE Posture Policy.

## Configure Switch

Configure the access switch for dot1x authentication and redirection.

```

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 <ISE server IP> auth-port 1812 acct-port 1813
key <secret-key>

dot1x system-auth-control

```

Configure Redirect ACL for user to be redirected to ISE Client Provisioning Portal.

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

Enable device tracking and http redirection on the 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
```

## Download the Secure client Package

Download the Profile Editor, Secure Client windows and Compliance Module webdeploy files manually from [software.cisco.com](https://software.cisco.com)

On the product name search bar type **Secure Client 5**.

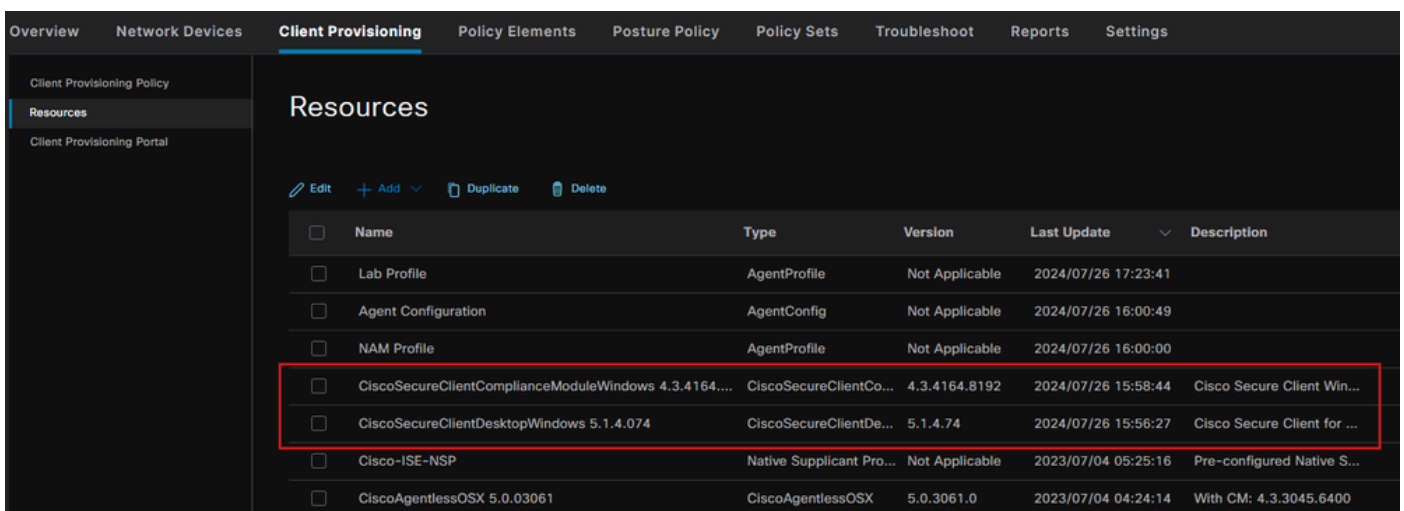
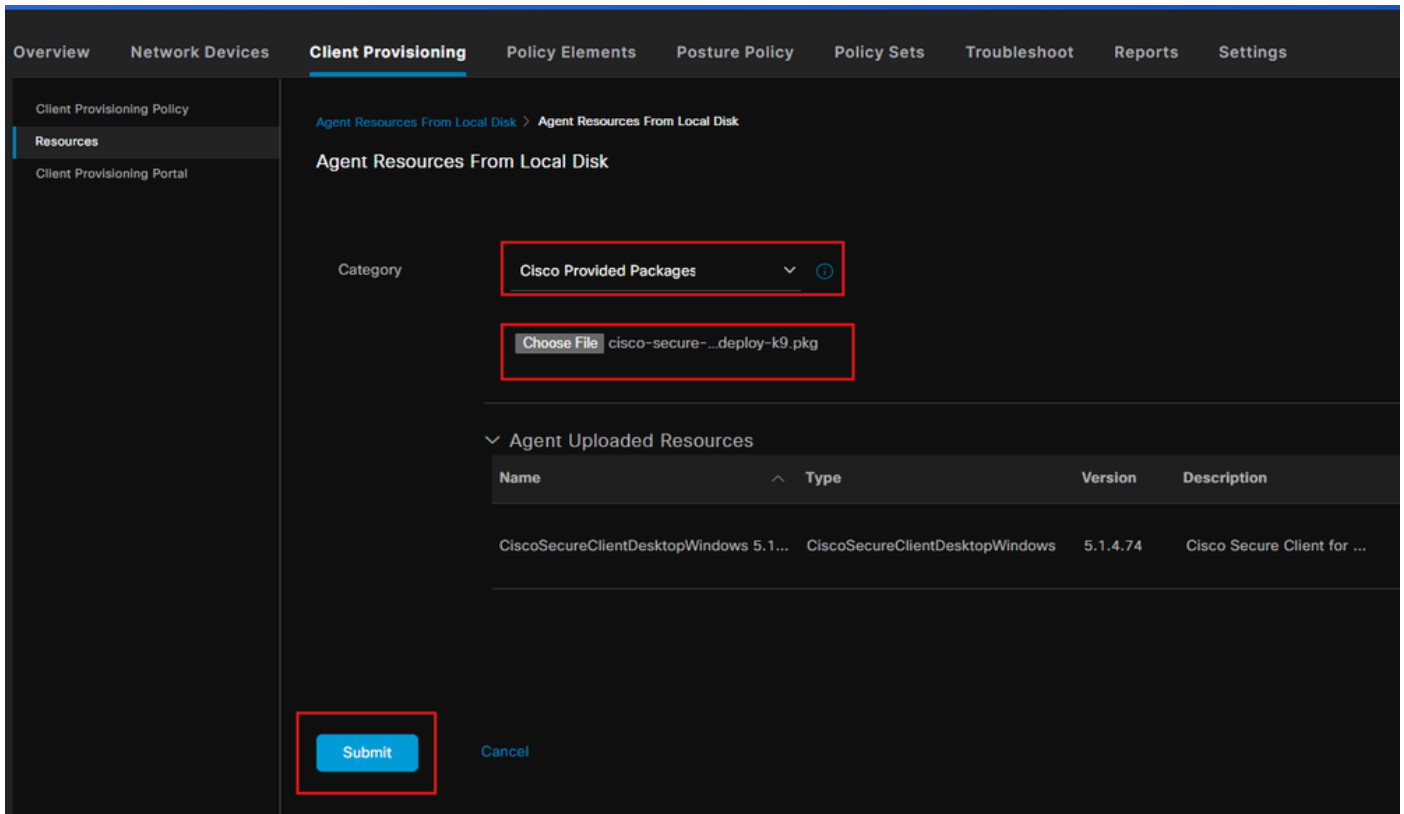
**Downloads Home > Security > Endpoint Security > Secure Client (including AnyConnect) > Secure Client 5 > AnyConnect VPN Client Software**

- 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 Configuration

### Step 1. Upload the Package on ISE

To upload the Secure Client and Compliance Module webdeploy packages on ISE, Navigate to **Workcenter > Posture > Client Provisioning > Resources > Add > Agent Resources from Local Disk**.

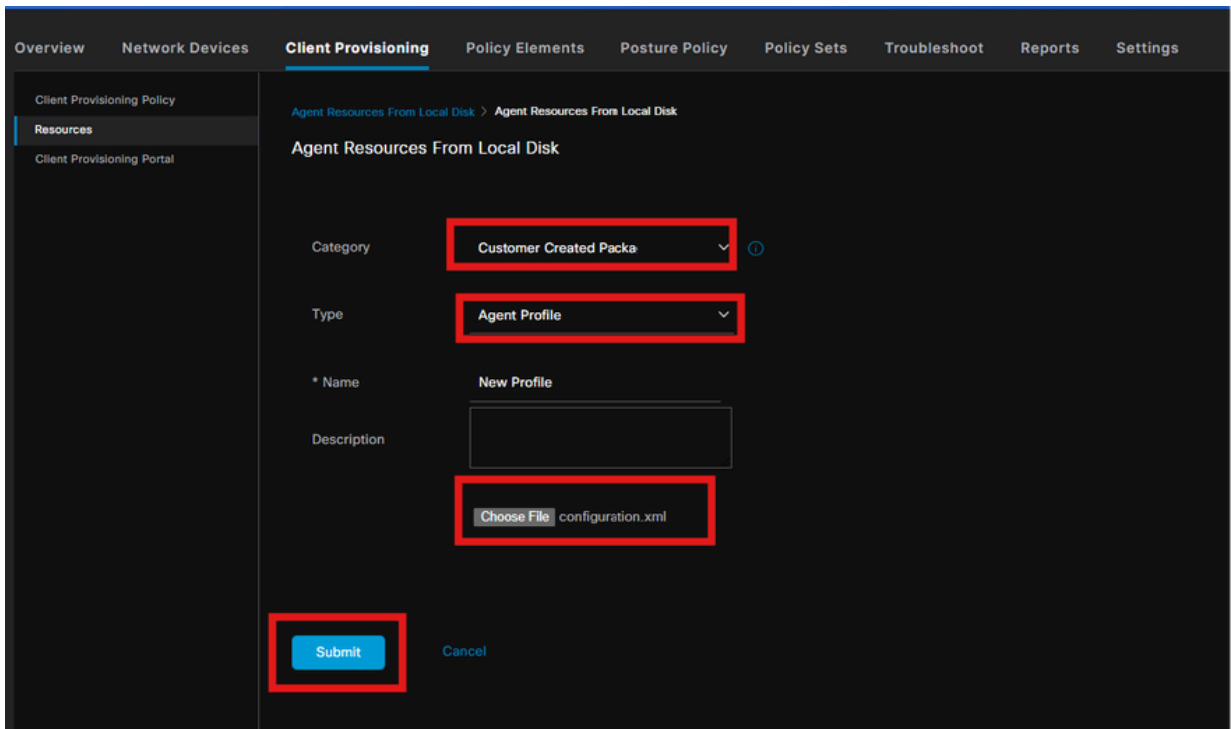


## Step 2. Create a NAM Profile from Profile editor tool

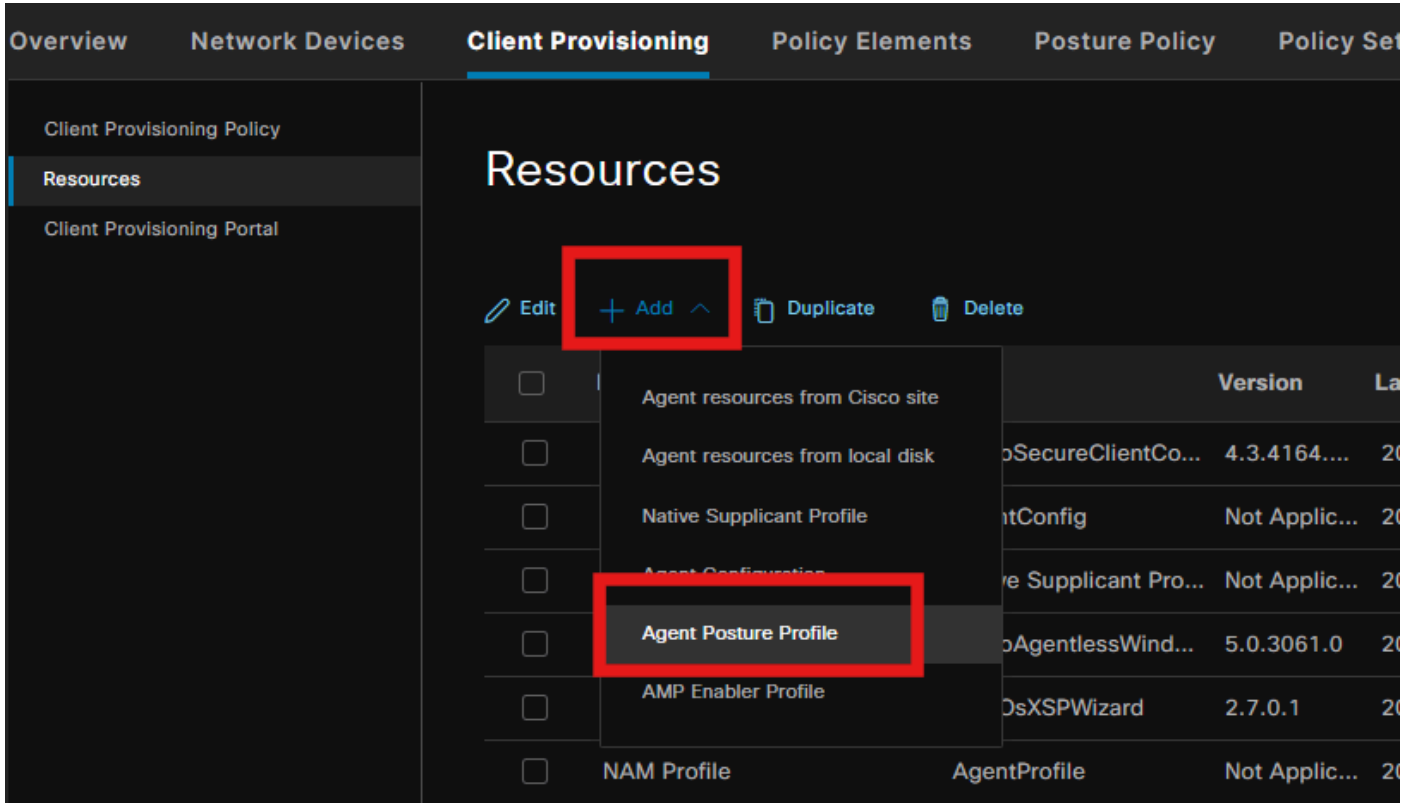
For information on how to configure a NAM profile refer this guide [Configure Secure Client NAM Profile](#) .

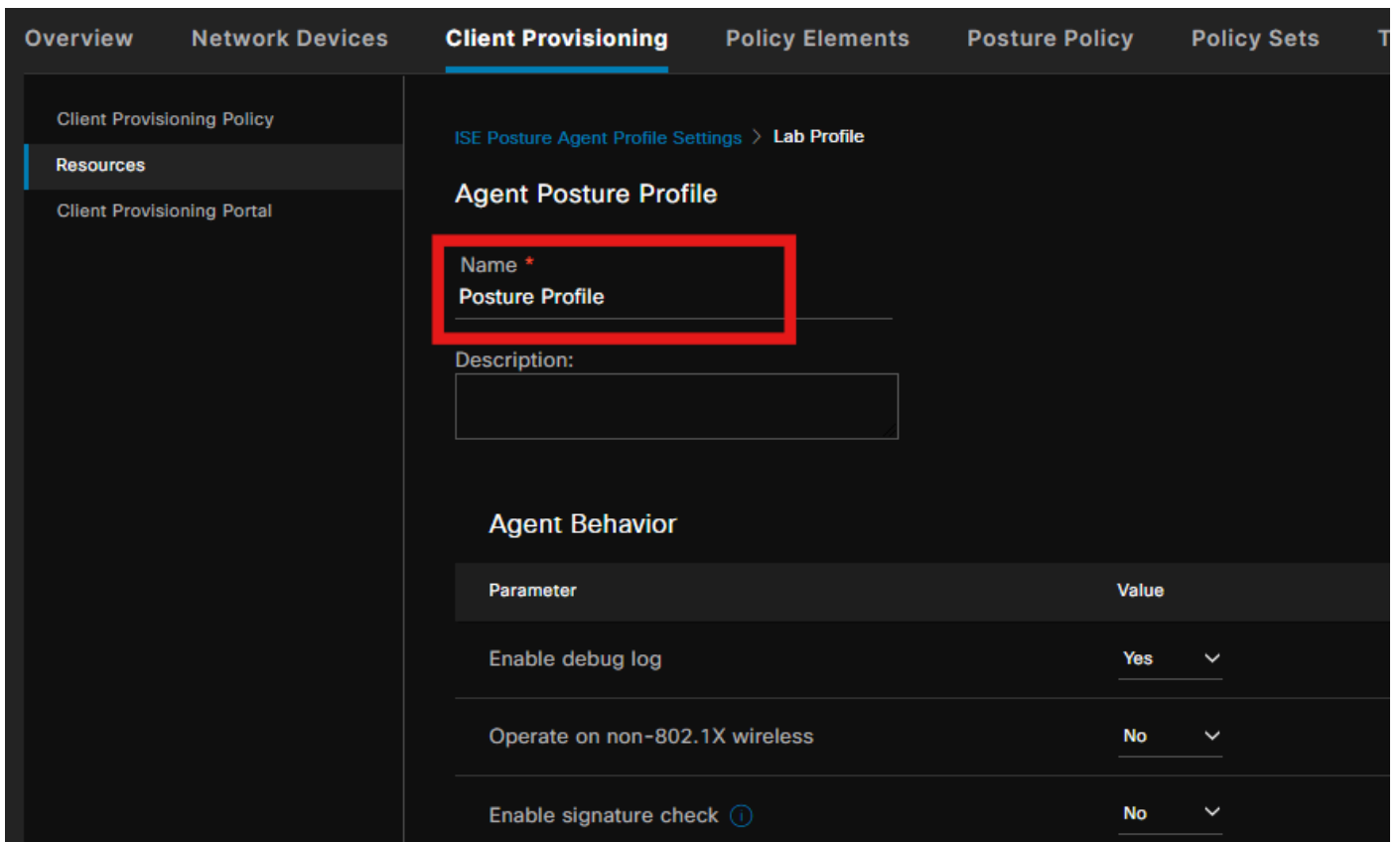
## Step 3. Upload the NAM Profile on ISE

To upload the NAM Profile "Configuration.xml" on ISE as Agent Profile, navigate to **Client Provisioning > Resources > Agent Resources From Local Disk**.



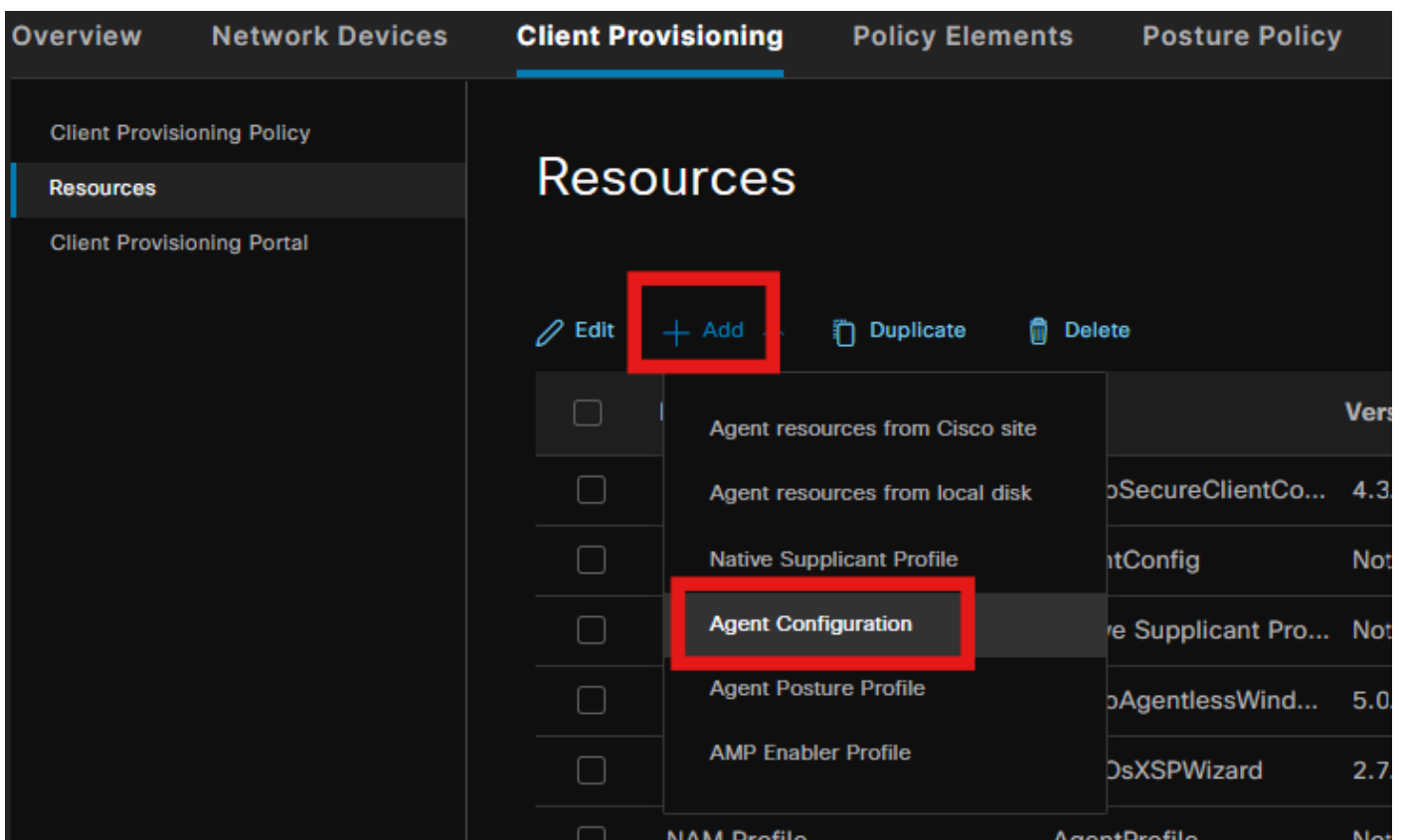
### Step 4. Create a Posture Profile





From the Posture Protocol section, do not forget to add \* in order to allow the Agent to connect to all servers.

## Step 5. Create Agent Configuration



Select the uploaded secure client and compliance module package and under the Module selection, select the ISE Posture, NAM and DART modules

The screenshot shows the Cisco ISE Client Provisioning interface. The top navigation bar includes 'Engine' and 'Work Centers / Posture'. Below this, there are tabs for 'Overview', 'Network Devices', 'Client Provisioning', 'Policy Elements', 'Posture Policy', and 'Policy Sets'. The 'Client Provisioning' tab is active, and the breadcrumb path is 'Agent Configuration > New Agent Configuration'. On the left, there is a sidebar with 'Client Provisioning Policy', 'Resources', and 'Client Provisioning Portal'. The main content area contains the following fields:

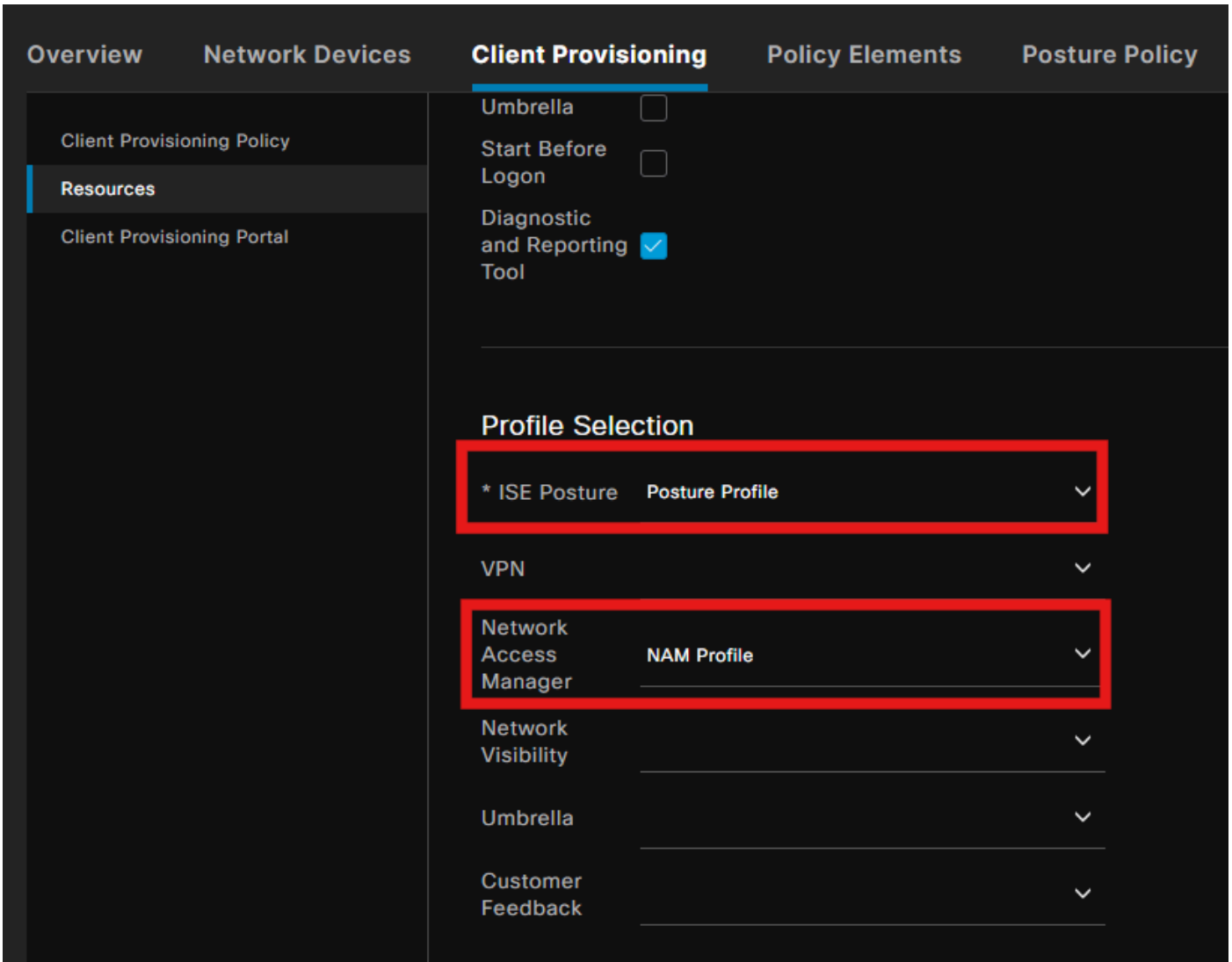
- \* Select Agent Package: CiscoSecureClientDesktopWindows 5.1 (highlighted with a red box)
- \* Configuration Name: Agent Configuration
- Description: (empty text box)
- Description Value Notes
- \* Compliance Module: CiscoSecureClientComplianceModuleW (highlighted with a red box)

Below these fields is a section titled 'Cisco Secure Client Module Selection' with the following options:

- ISE Posture  (highlighted with a red box)
- VPN
- Zero Trust Access
- Network Access Manager  (highlighted with a red box)
- Secure Firewall Posture
- Network Visibility

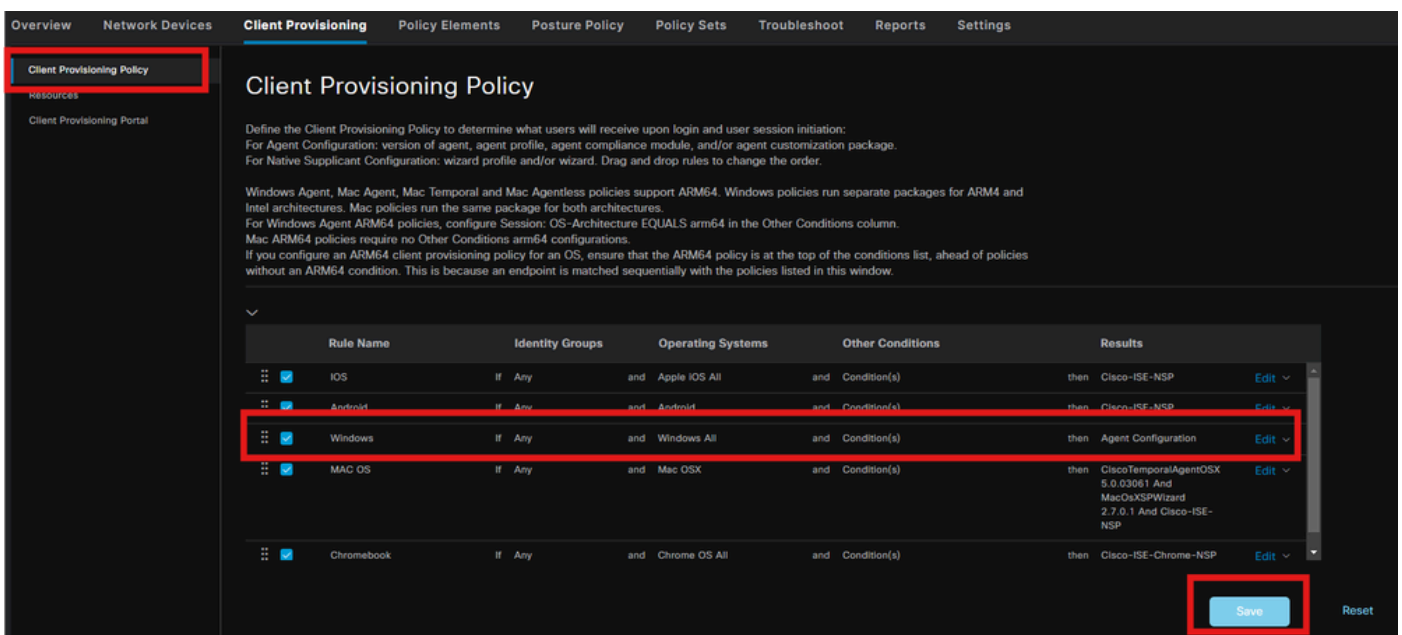
Under Profile select, choose the **Posture** and **NAM** Profile and click **Submit**.





## Step 6. Client Provisioning Policy

Create a client Provisioning Policy for Windows operating system and select the **Agent Configuration** created in the previous step.

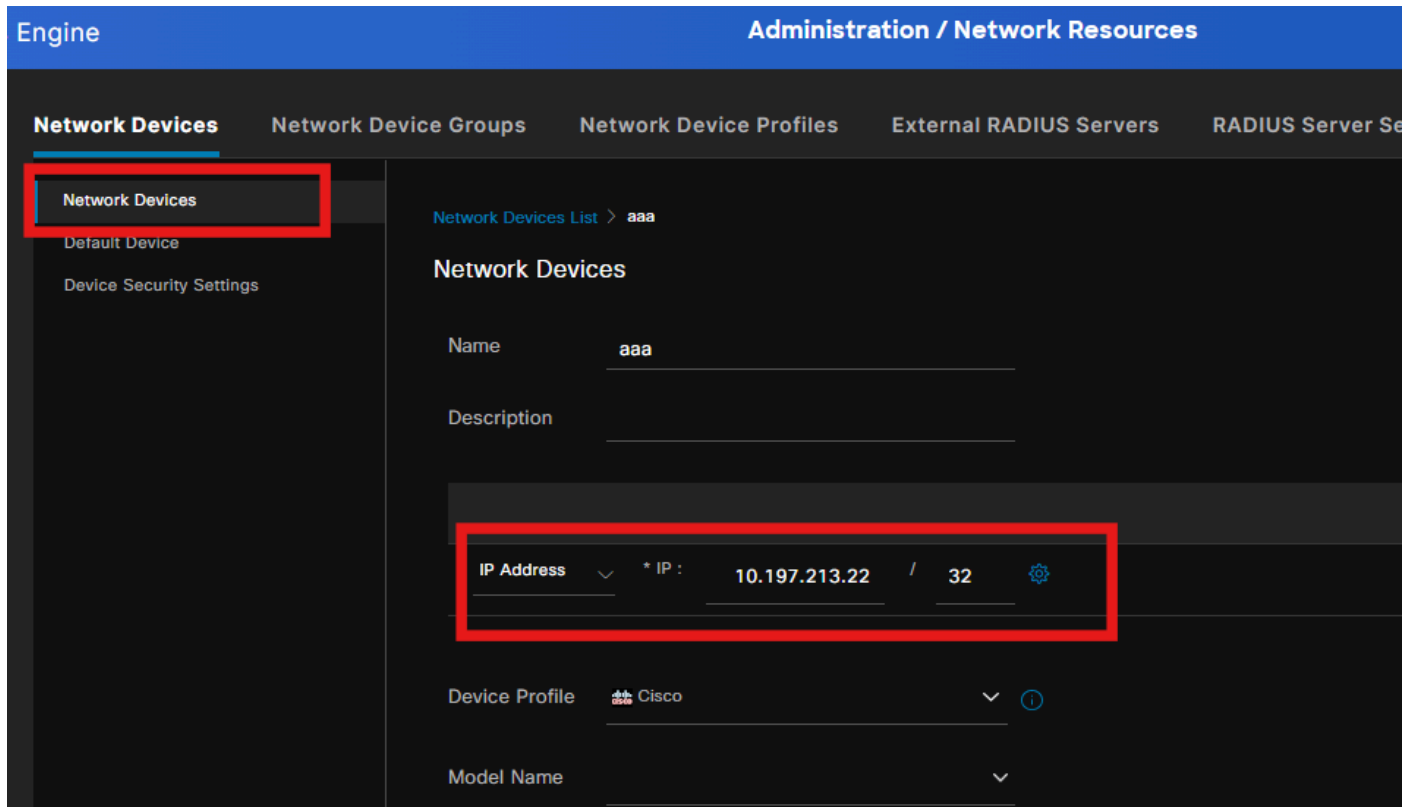


## Step 7. Posture Policy

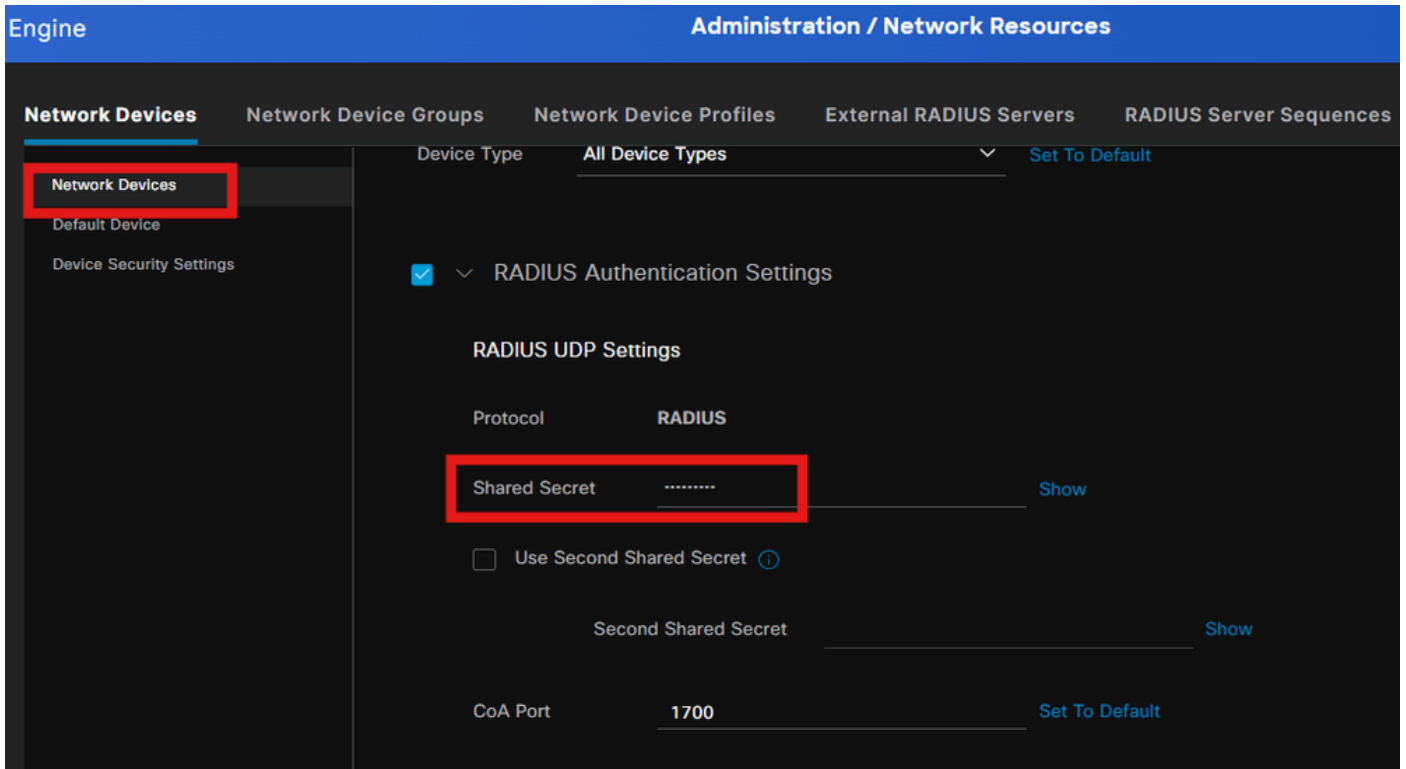
For information on how to create the Posture Policy and conditions, refer this guide [ISE Posture Prescriptive Deployment Guide](#) .

## Step 8. Add Network device

To add the switch IP address and the radius shared secret key, navigate to **Administration > Network Resources**.

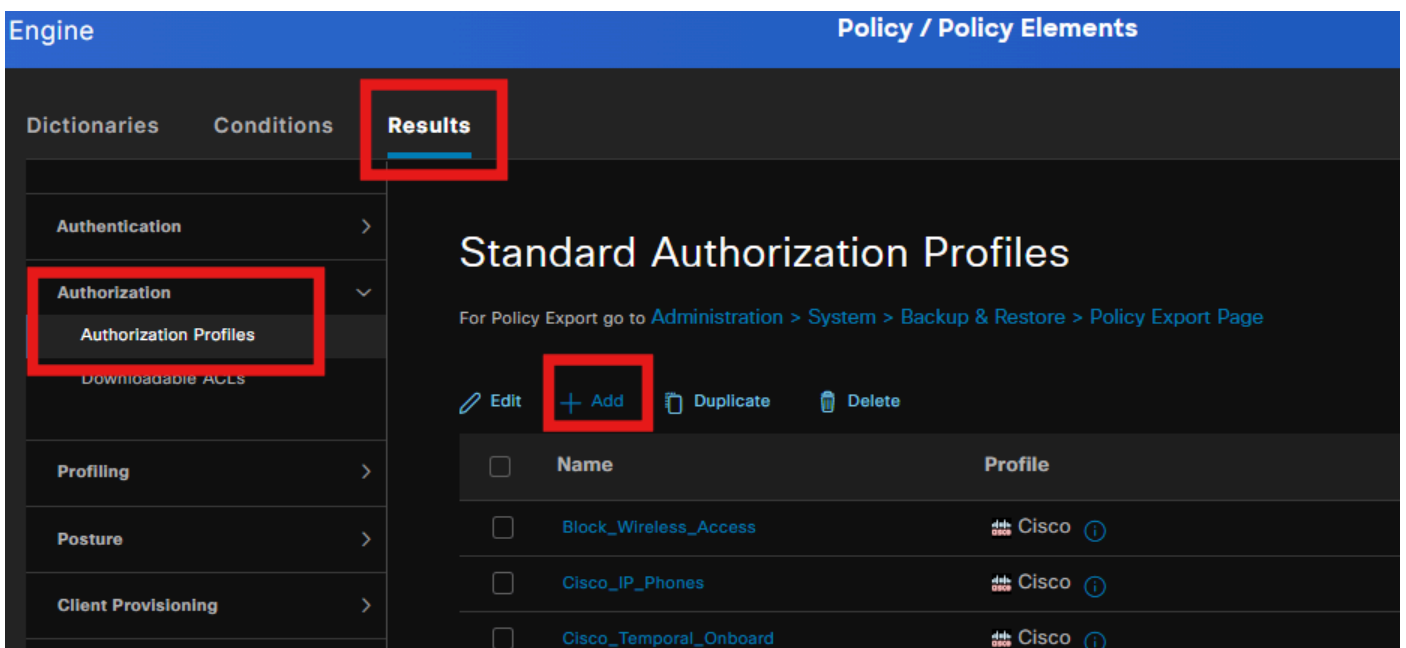


The screenshot displays the Cisco ISE Administration console interface. At the top, the breadcrumb navigation shows "Administration / Network Resources". Below this, a horizontal menu contains several options: "Network Devices", "Network Device Groups", "Network Device Profiles", "External RADIUS Servers", and "RADIUS Server Se". The "Network Devices" option is highlighted with a red box. The main content area shows the configuration for a specific network device named "aaa". The "Name" field is set to "aaa". Below it, the "Description" field is empty. A red box highlights the "IP Address" field, which is set to "10.197.213.22 / 32". Below the IP address field, the "Device Profile" is set to "Cisco" and the "Model Name" field is empty. The interface is dark-themed with white text and red highlights.

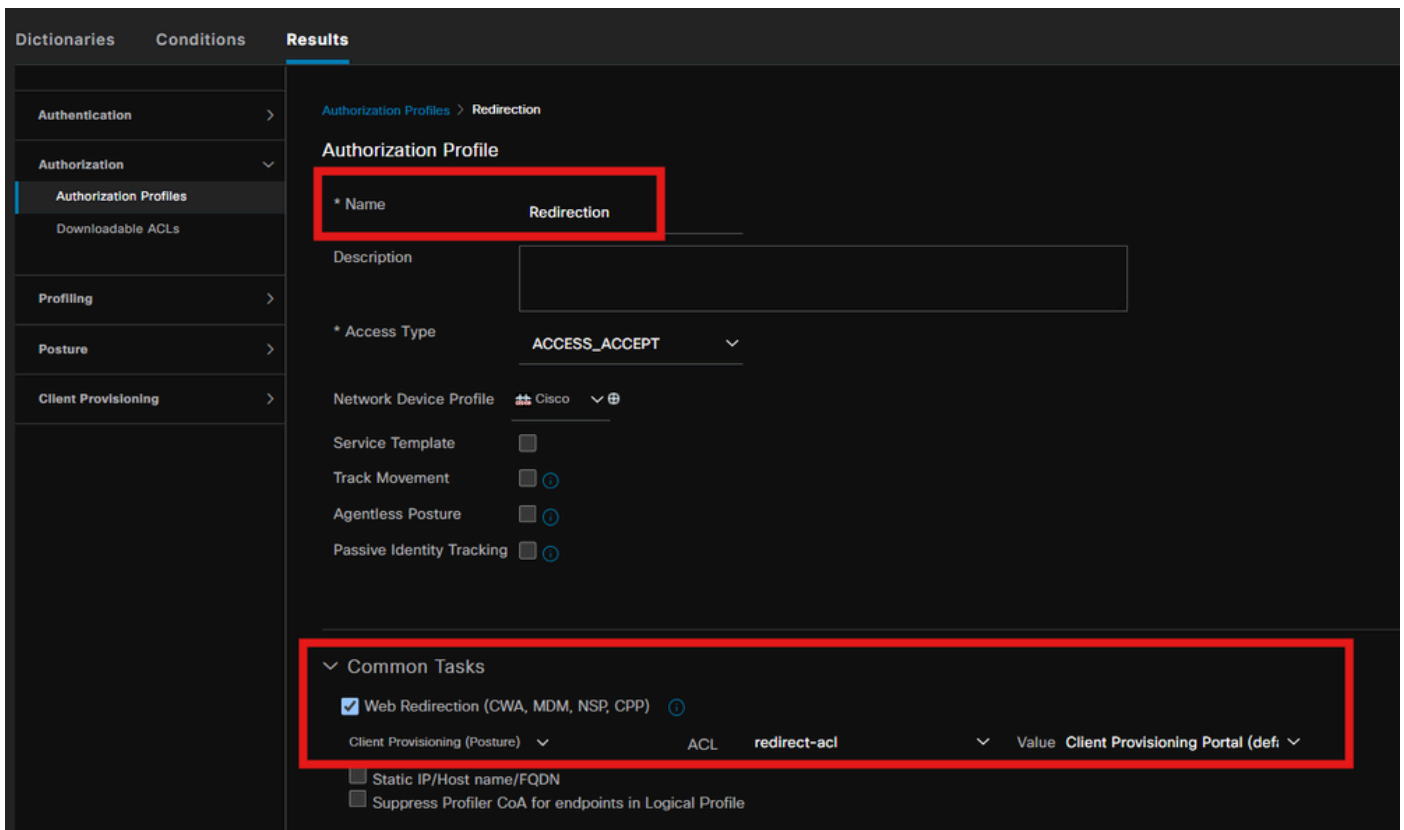


## Step 9. Authorization Profile

To create a Posture redirection profile, navigate to **Policy > Policy Elements > Results**.

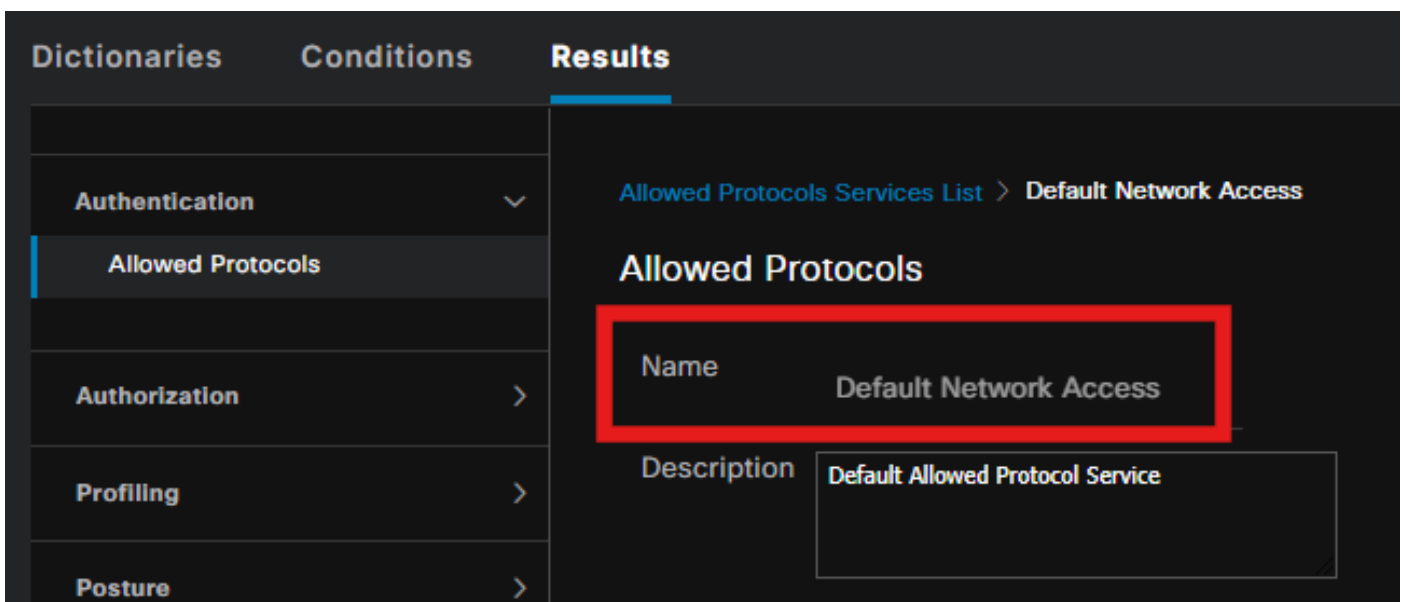


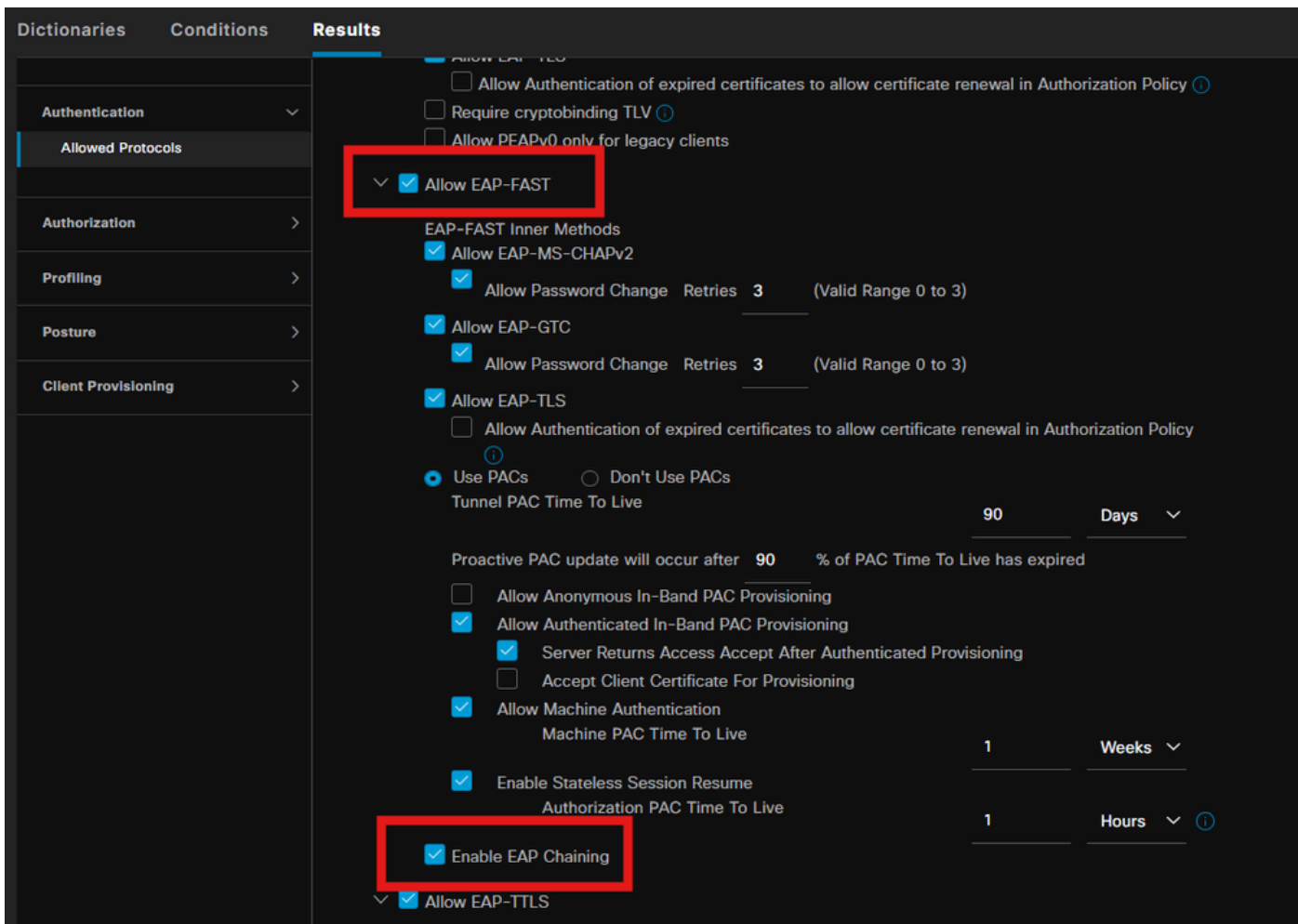
Under command task, select the client Provisioning Portal with redirect ACL.



## Step 10. Allowed Protocols

Navigate to **Policy > Policy elements > Results > Authentication > Allowed Protocols**, Select the **EAP Chaining** settings,

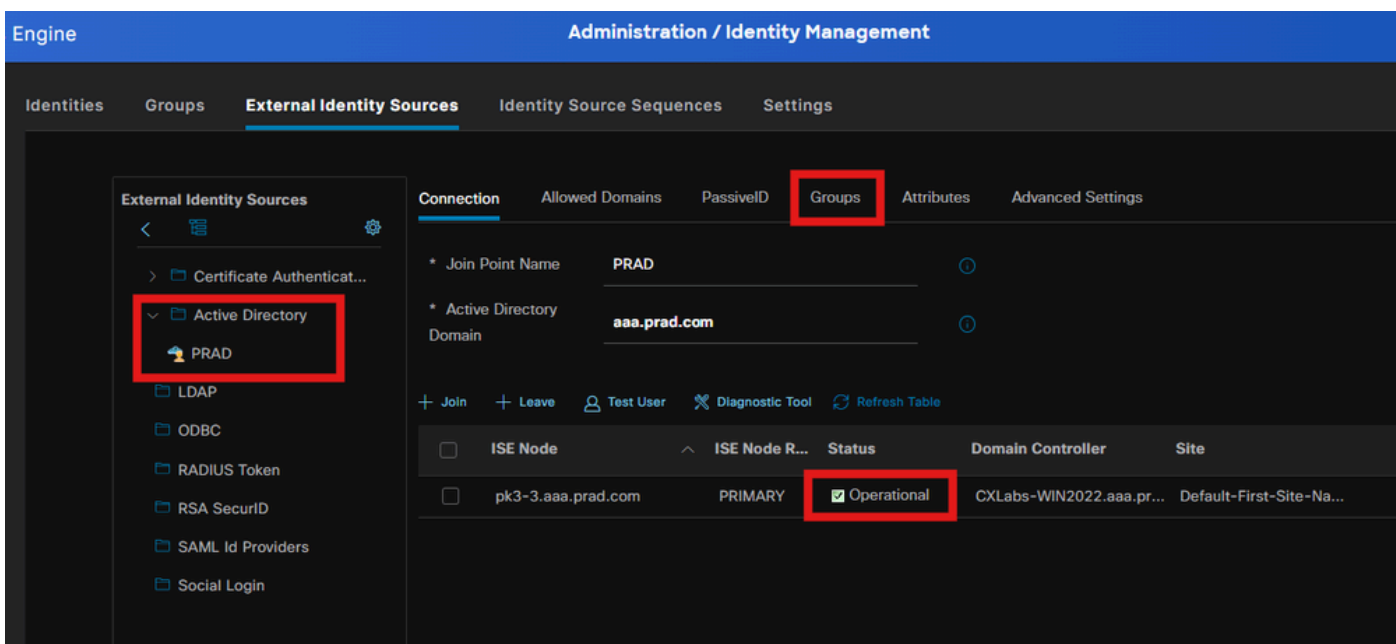




## Step 11. Active Directory

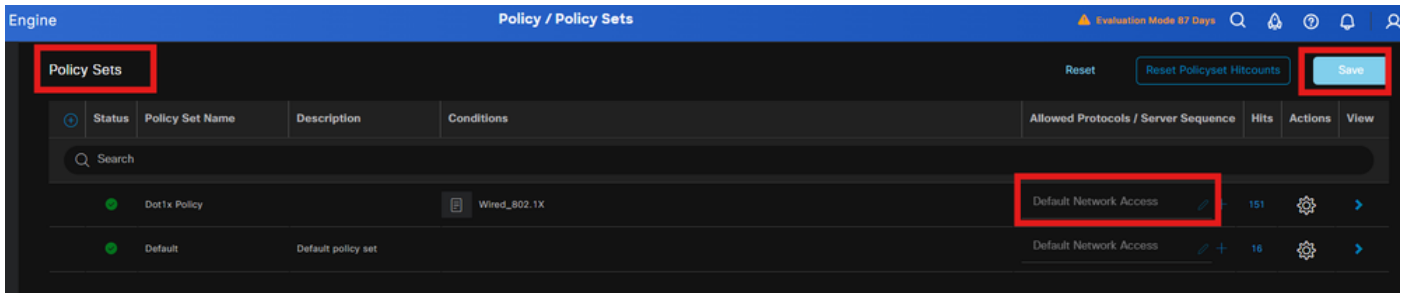
Validate ISE is joined with Active directory domain and the domain groups are selected if needed for the authorization conditions.

**Administration > Identity Management > External Identity Sources > Active Directory**

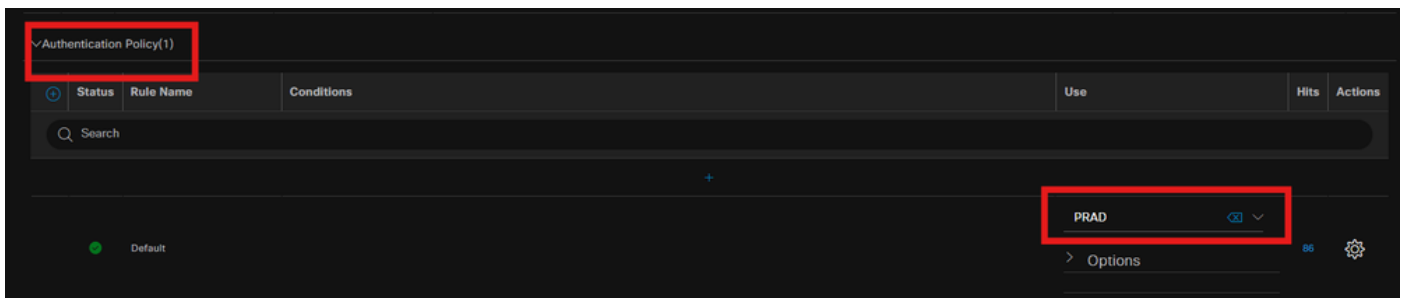


## Step 12. Policy sets

Create a Policy set on ISE to authenticate the dot1x request. Navigate to **Policy > Policy sets**.



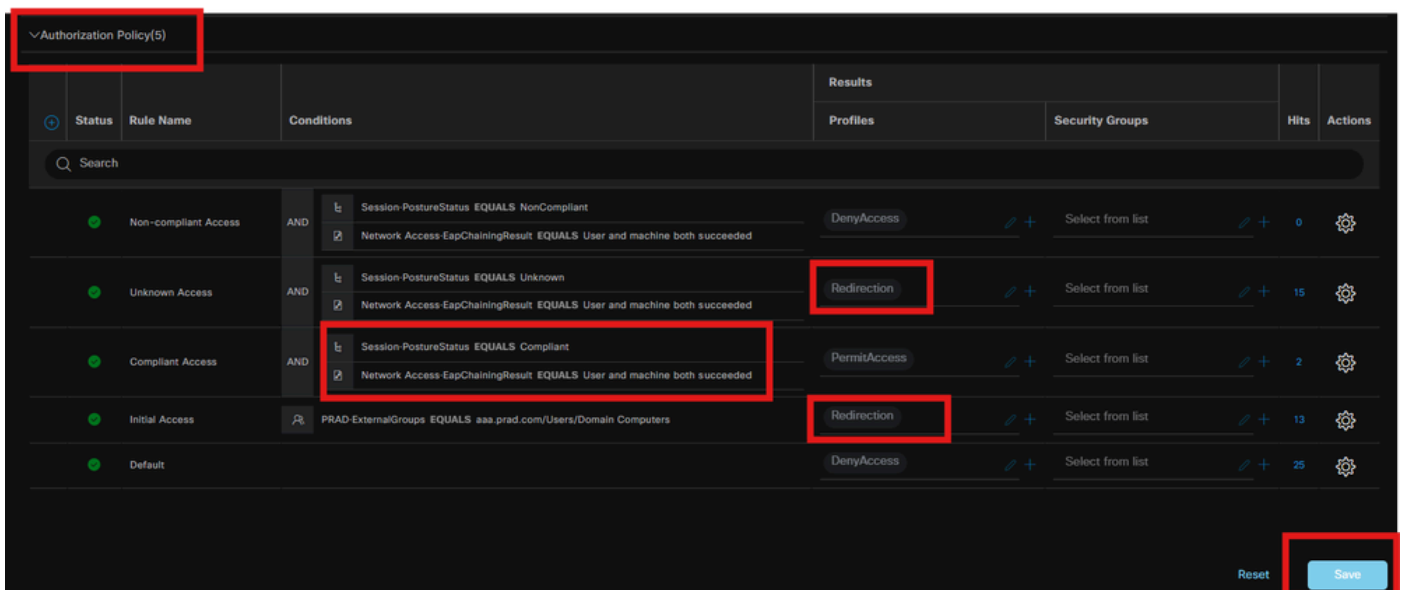
Select the Active directory as identity source for Authentication Policy.



Configure different Authorization rules based on posture status unknown, non-compliant and compliant.

In this use case.

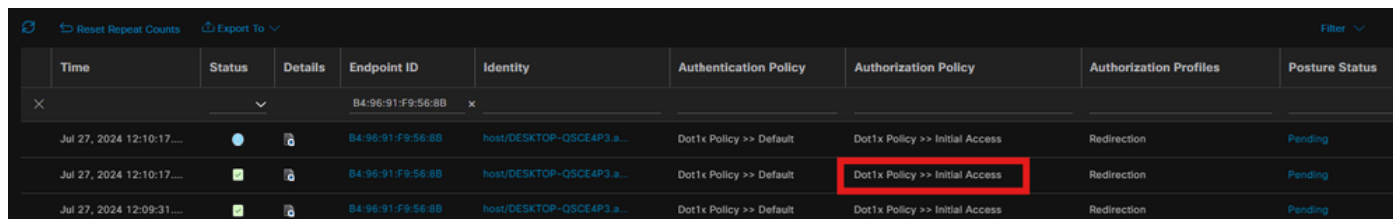
- Initial Access : Redirection to ISE Client Provisioning Portal to install Secure client agent and NAM Profile
- Unknown Access: Access to Client Provisioning Portal for redirection based Posture discovery
- Compliant Access: Full network access
- Non-Compliant: Deny Access



**Verify**

## Step 1. Download and Install Secure Client Posture/NAM module from ISE

Select the endpoint authenticated through dot1x, hitting "Initial Access" Authorization rule. Navigate to **Operations > Radius > Live Logs**



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

On Switch, specify the redirection URL and ACL getting applied for the Endpoint.

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

```
Interface: TenGigabitEthernet1/0/24
```

```
IIF-ID: 0x19262768
```

```
MAC Address: x4x6.xxxx.xxxx
```

```
IPv6 Address: Unknown
```

```
IPv4 Address: <client-IP>
```

```
User-Name: host/DESKTOP-xxxxxxx.aaa.prad.com
```

```
Status: Authorized
```

```
Domain: DATA
```

```
Oper host mode: single-host
```

```
Oper control dir: both
```

```
Session timeout: N/A
```

```
Common Session ID: 16D5C50A0000002CF067366B
```

```
Acct Session ID: 0x0000001f
```

```
Handle: 0x7a000017
```

```
Current Policy: POLICY_Te1/0/24
```

```
Local Policies:
```

```
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
```

```
Security Policy: Should Secure
```

```
Security Status: Link Unsecured
```

```
Server Policies:
```

```
URL Redirect ACL: redirect-acl
```

```
URL Redirect:
```

```
https://ise33.aaa.prad.com:8443/portal/gateway?sessionId=16D5C50A0000002CF067366A&portal=ee39fd08-7180-4995-8aa2-9fb282645a8f&action=cpp&token=518f857900a37f9afc6d2da8b6fe3bc2
```

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

```
Method status list:
```

```
Method State
```

```
dot1x Authc Success
```

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

```
Network Layer Address Link Layer Address Interface vlan prlvl age state Time left
```

```
ARP X.X.X.X b496.91f9.568b Te1/0/24 1000 0005 4mn REACHABLE 39 s try 0
```

On the Endpoint, verify the traffic redirected to ISE Posture Posture and click **Start** to download the Network Setup Assistant on the Endpoint.

The screenshot shows the Cisco Client Provisioning Portal interface. At the top, there is a notification: "Google Chrome isn't your default browser" with a "Set as default" button. Below this is the Cisco logo and the text "Client Provisioning Portal".

The main content area displays a "Device Security Check" section with the message: "Your computer requires security software to be installed before you can connect to the network." A "Start" button is highlighted with a red box.

Overlaid on the bottom right is a "Recent download history" window. It lists a download: "cisco-secure-client-ise-network-assistant-win-5.1.4.74\_pk3-3.aaa.prad.com\_8443\_WPTsDtDOR0SunsnMYB1glg.exe" with a size of "3.0 MB" and status "Done". This entry is also highlighted with a red box.

Below the download history is a "Full download history" link.

In the background, a "Unable to detect Posture Agent" dialog box is visible. It has a title bar with a red box around "+ This is my first time here". The dialog contains the following text:

Unable to detect Posture Agent

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.

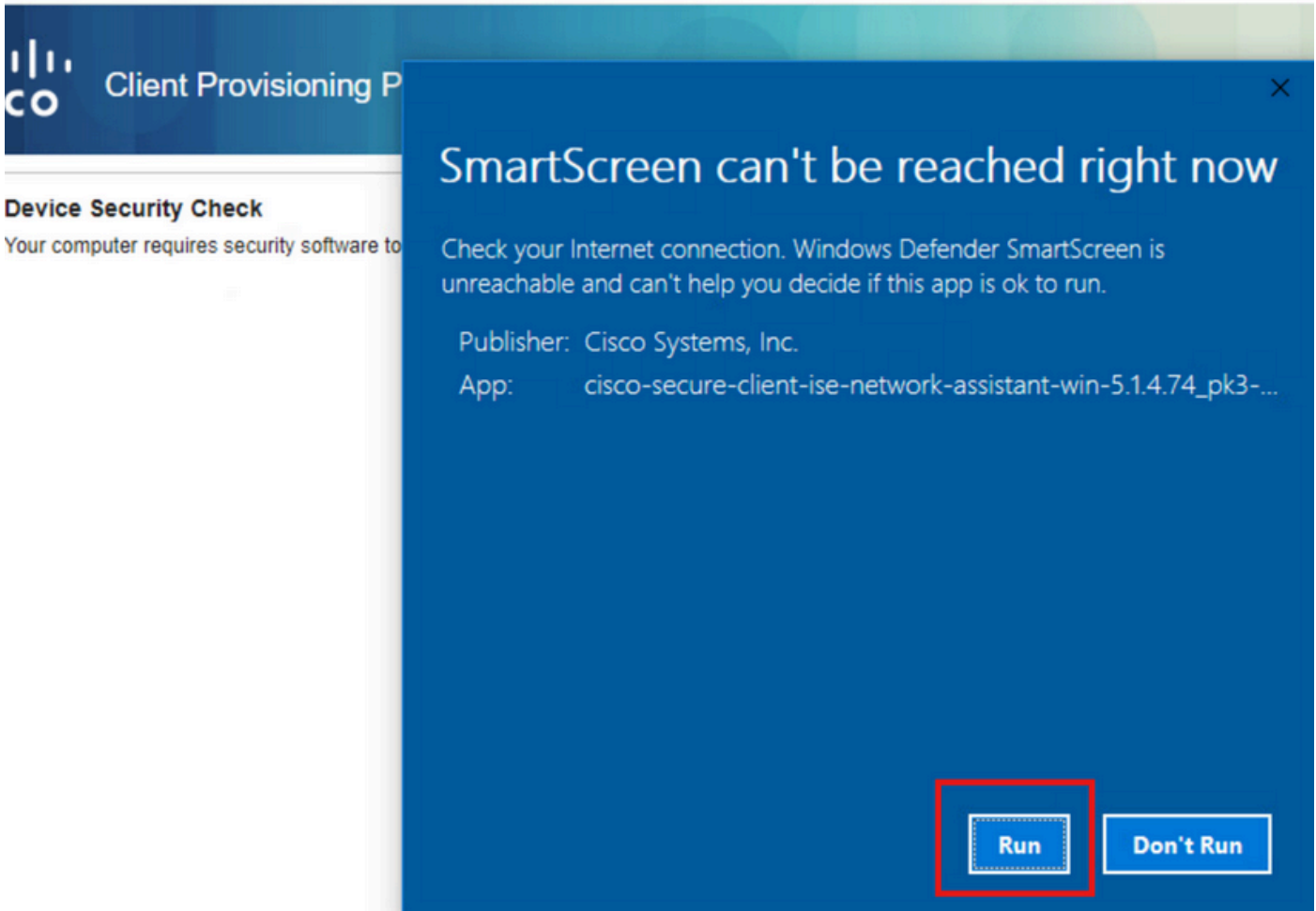
Tip: Leave Agent running so it will automatically scan your device and connect you faster next time you access this network.

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

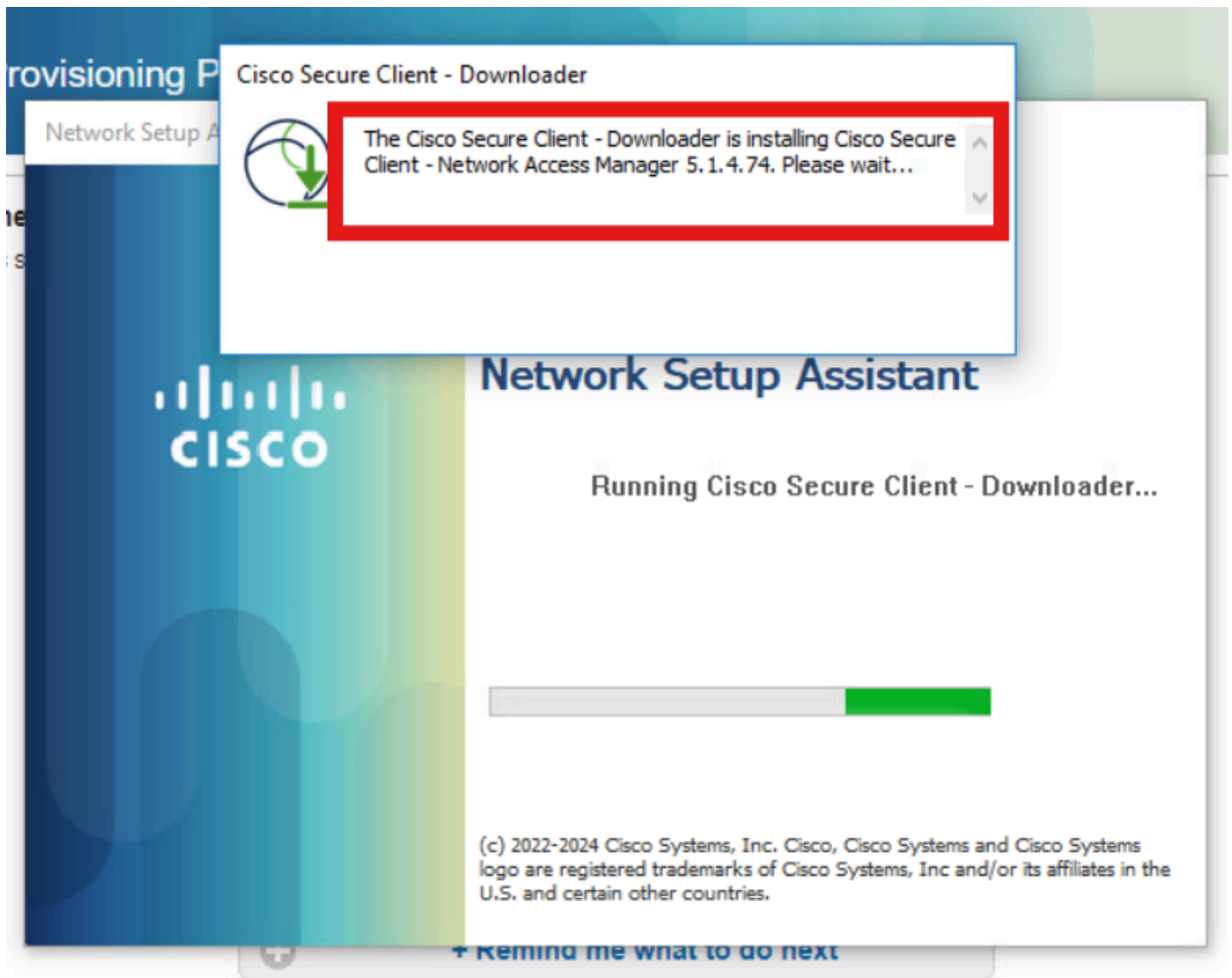
At the bottom of the dialog is a button: "+ Remind me what to do next"

Click **Run** to install the NSA application.

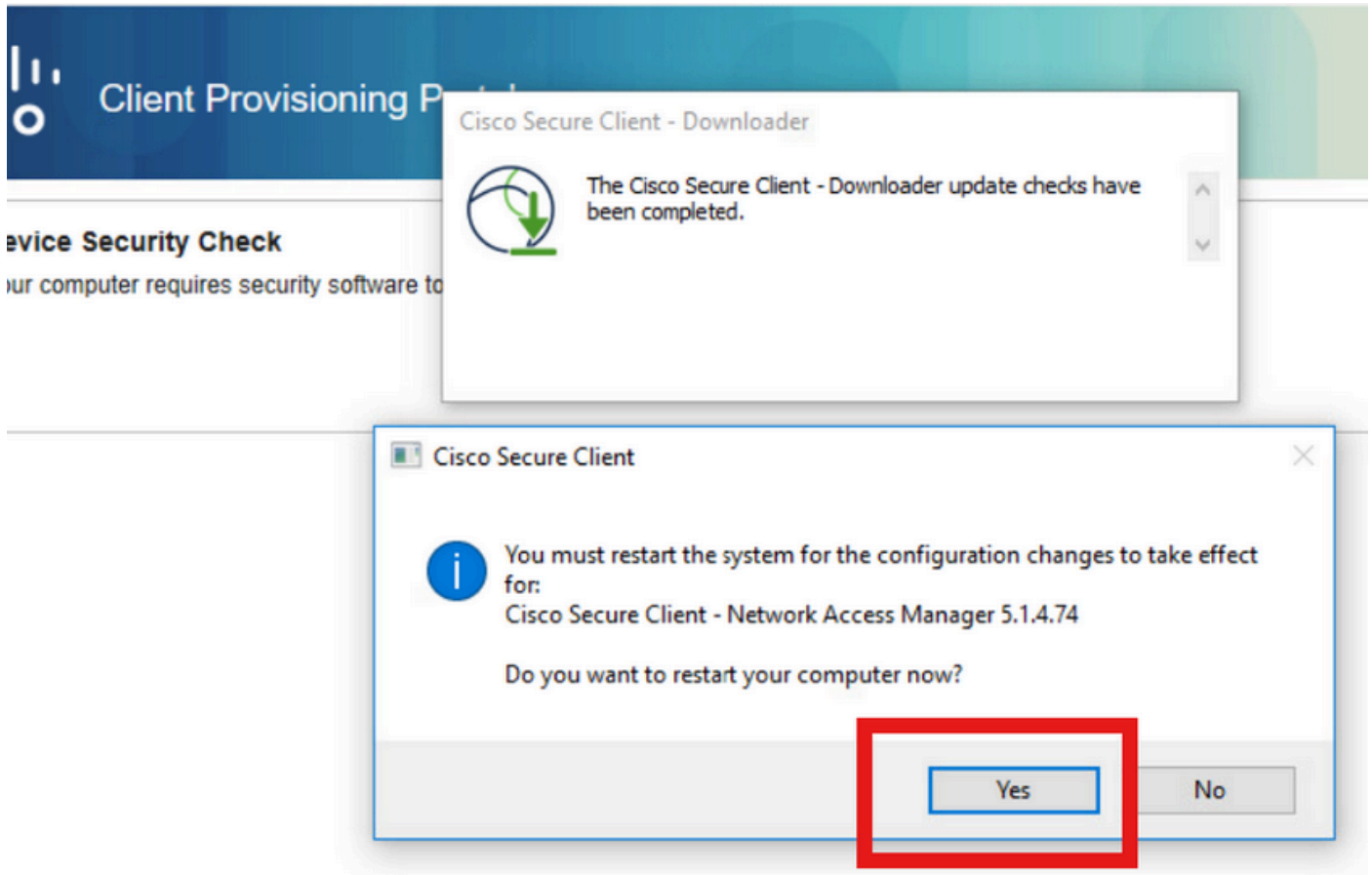




Now, the NSA invokes the Secure Client Agent download from ISE and installs the Posture, NAM module, and NAM Profile **configuration.xml** .



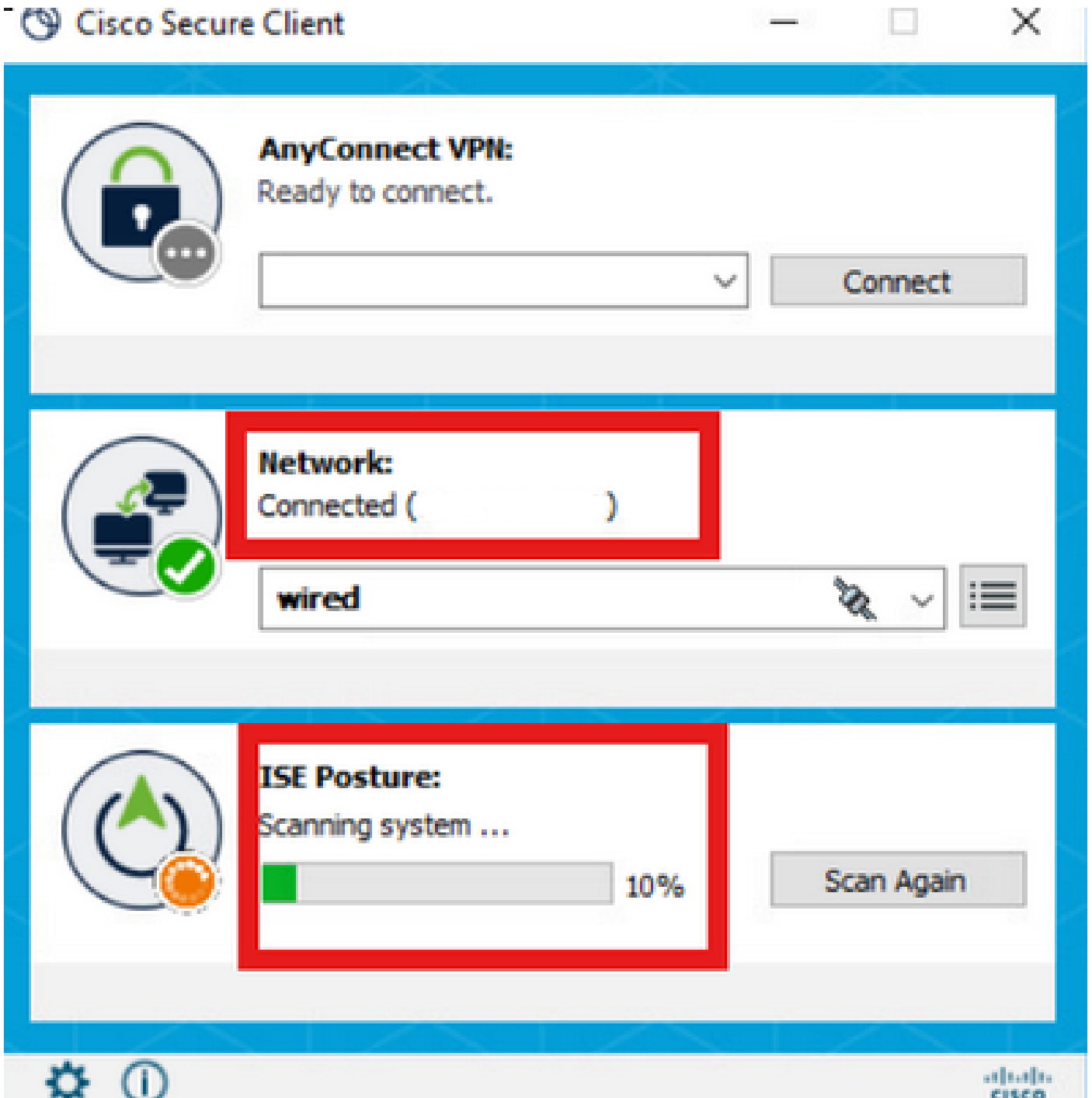
A restart prompt triggered after NAM installation. Click **Yes**.



## Step 2. EAP-FAST

Once the PC restarted and the user logged in, the NAM authenticates both user and machine through EAP-FAST.

If the endpoint authenticates correctly, NAM displays that it is connected and the Posture Module triggers the Posture Scan.



On ISE Live Logs, the Endpoint is now hitting the **Unknown Access Rule**.

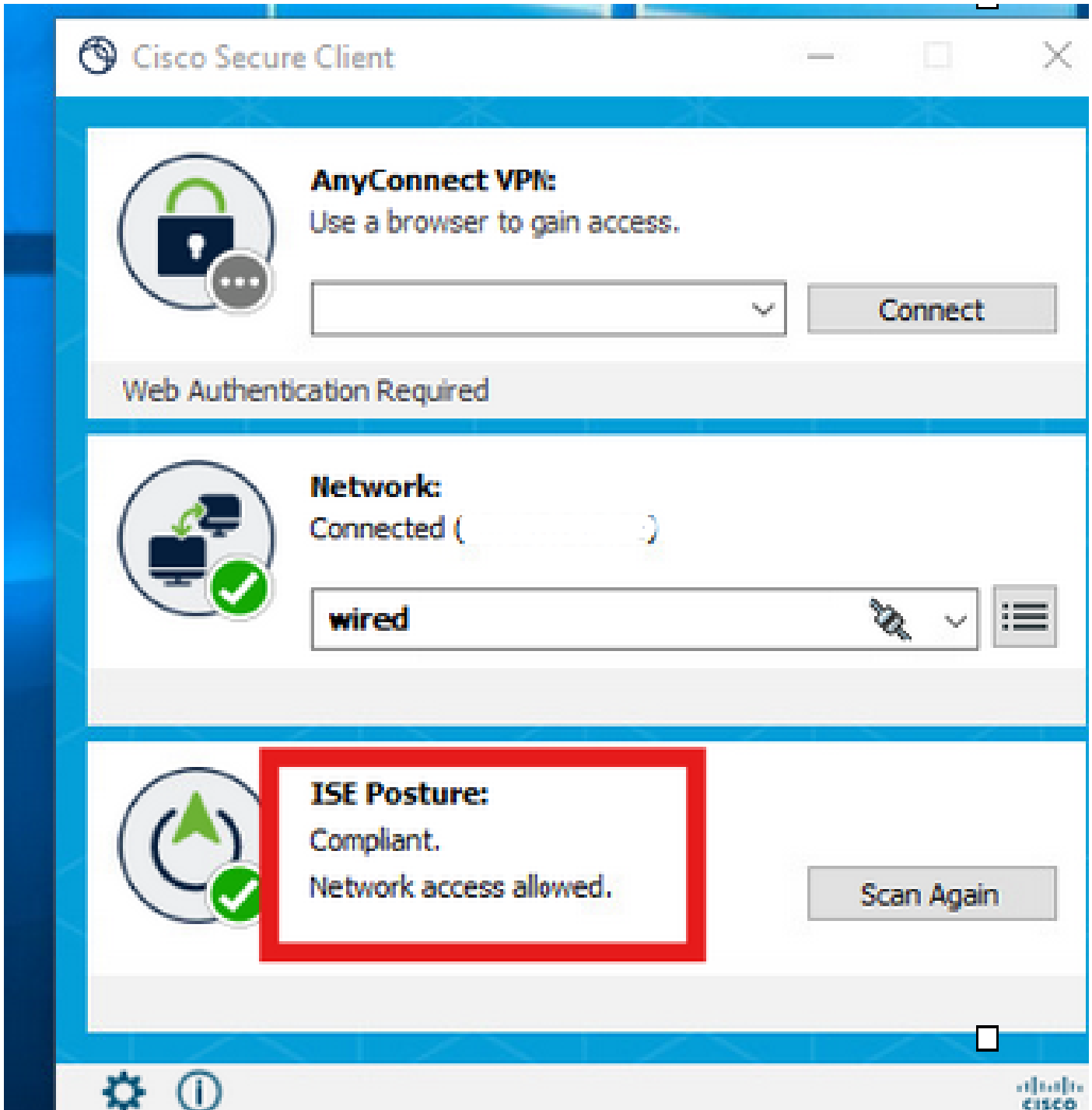
Jul 27, 2024 12:29:06...		user1_host/DESKTOP-QSC...	Dot1x Policy >> Default	<b>Dot1x Policy &gt;&gt; Unknown Access</b>	Redirection	Pending
Jul 27, 2024 12:28:48...		host/DESKTOP-QSCE4P3	Dot1x Policy >> Default	Dot1x Policy >> Initial Access	Redirection	Pending

Now the Authentication Protocol is EAP-FAST based on the NAM Profile configuration and EAP-Chaining result is "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

### Step 3. Posture Scan

The Secure Client Posture Module triggers the Posture Scan and is marked as Complaint based on the ISE Posture Policy.



The CoA is triggered after the Posture Scan and now the Endpoint hits the **Complaint Access Policy**.

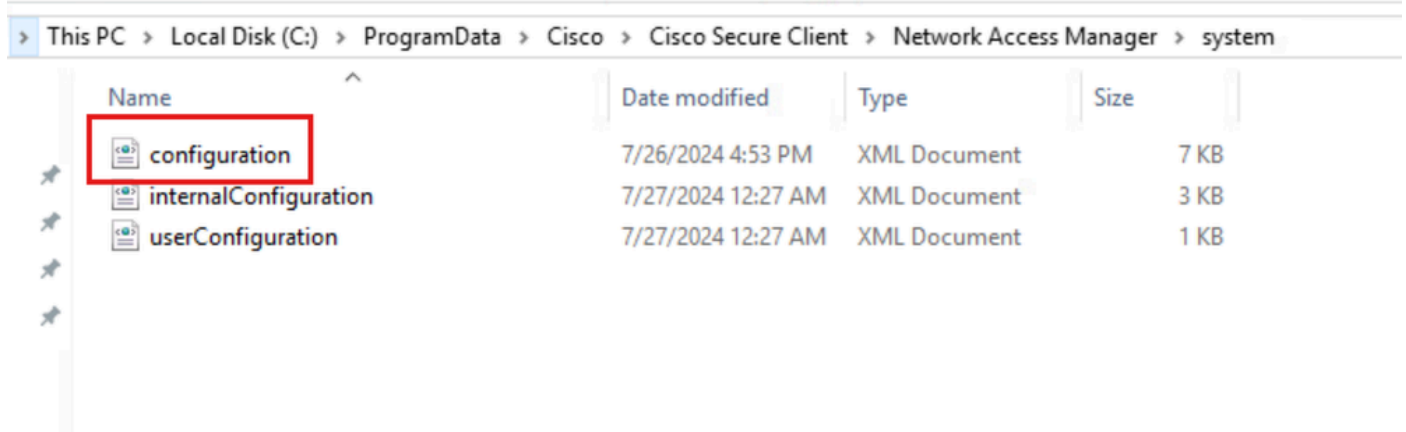
Time	Status	Details	Endpoint ID	Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture Status
Jul 27, 2024 12:29:32...			B4:96:91:F9:56:8B	user1_host/DESKTOP-QSC...	Dot1x Policy >> Default	Dot1x Policy >> Compliant Access	PermitAccess	Compliant
Jul 27, 2024 12:29:32...			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

## Troubleshoot

## Step 1. NAM Profile

Verify the NAM Profile **configuration.xml** is present in this path on the PC after the NAM module installation.

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

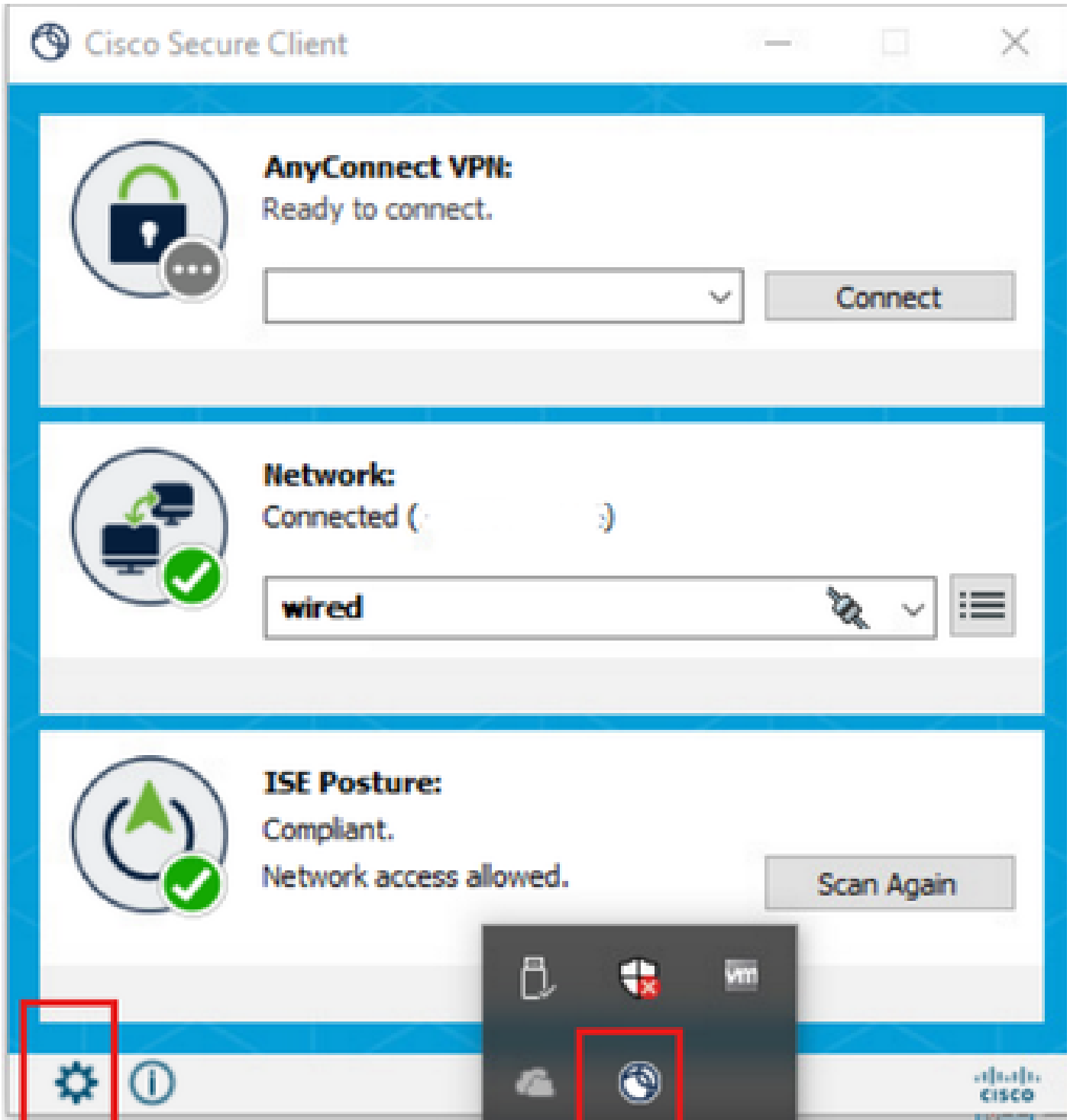


The screenshot shows a Windows File Explorer window with the address bar displaying the path: > This PC > Local Disk (C:) > ProgramData > Cisco > Cisco Secure Client > Network Access Manager > system. The main area displays a list of files with columns for Name, Date modified, Type, and Size. The 'configuration'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

## Step 2. NAM Extended Logging

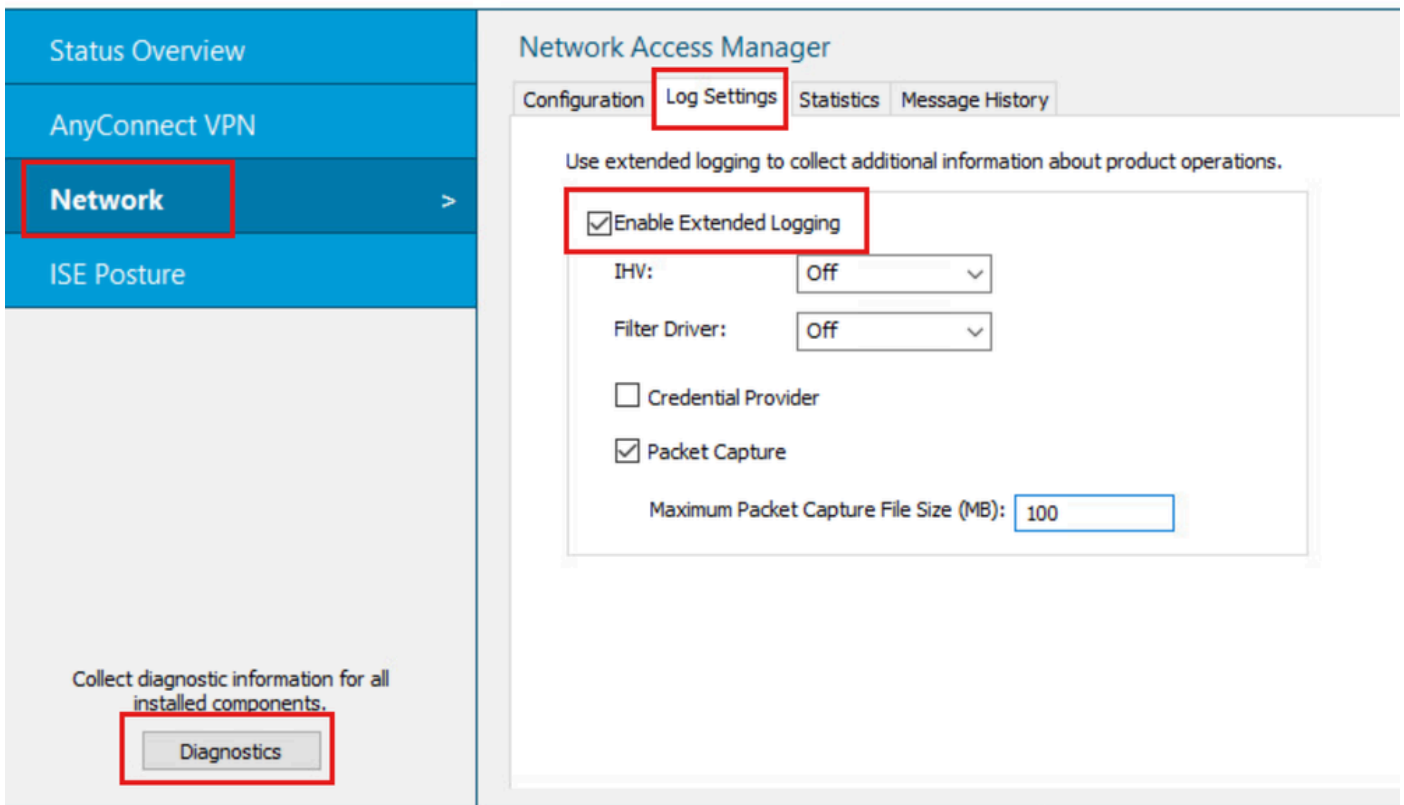
Click on the Secure Client Icon from task bar and select "settings" icon.



Navigate to the **Network > Log Settings** tab. Check the **Enable Extended Logging** checkbox. Set the Packet Capture File Size to 100 MB.

After reproducing the issue, click on **Diagnostics** to create the DART Bundle on the Endpoint.





The **Message History** section displays the details of every step that NAM performed.

### Step 3. Debugs on Switch

Enable these debugs on the switch to troubleshoot dot1x and redirection flow.

```
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
```

To view the logs

```
show logging
```

show logging process smd internal

## **Step 4. Debugs on ISE**

Collect the ISE support bundle with these attributes to be set at the debug level:

- posture
- portal
- provisioning
- runtime-AAA
- nsf
- nsf-session
- swiss
- client-webapp

## **Related Information**

[Configure Secure Client NAM](#)

[ISE Posture Prescriptive Deployment Guide](#)

[Troubleshoot Dot1x on Catalyst 9000 Series Switches](#)