

# Konfigurieren und Bereitstellen eines sicheren Client NAM-Profiles über ISE 3.3 unter Windows

## Inhalt

---

[Einleitung](#)

[Hintergrundinformationen](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfiguration](#)

[Netzwerkdiagramm](#)

[Datenfluss](#)

[Switch konfigurieren](#)

[Secure Client-Paket herunterladen](#)

[ISE-Konfiguration](#)

[Schritt 1: Paket auf ISE hochladen](#)

[Schritt 2: Erstellen eines NAM-Profiles mit dem Profil-Editor-Tool](#)

[Schritt 3: NAM-Profil auf die ISE hochladen](#)

[Schritt 4: Erstellen eines Statusprofils](#)

[Schritt 5: Agent-Konfiguration erstellen](#)

[Schritt 6: Client-Bereitstellungsrichtlinie](#)

[Schritt 7. Statusrichtlinie](#)

[Schritt 8: Netzwerkgerät hinzufügen](#)

[Schritt 9. Autorisierungsprofil](#)

[Schritt 10. Zulässige Protokolle](#)

[Schritt 11. Active Directory](#)

[Schritt 12: Richtlinien](#)

[Überprüfung](#)

[Schritt 1: Secure Client Posture/NAM-Modul von ISE herunterladen und installieren](#)

[Schritt 2: EAP-FAST](#)

[Schritt 3: Statusüberprüfung](#)

[Fehlerbehebung](#)

[Schritt 1: NAM-Profil](#)

[Schritt 2: Erweiterte NAM-Protokollierung](#)

[Schritt 3. Debuggen auf Switch](#)

[Schritt 4: Debuggen auf der ISE](#)

[Zugehörige Informationen](#)

---

## Einleitung

In diesem Dokument wird die Bereitstellung des Cisco Secure Client Network Access Manager (NAM)-Profils über die Identity Services Engine (ISE) beschrieben.

## Hintergrundinformationen

Die EAP-FAST-Authentifizierung erfolgt in zwei Phasen. In der ersten Phase verwendet EAP-FAST einen TLS-Handshake, um Schlüsselaustausch mithilfe von TLV-Objekten (Type-Length-Values) bereitzustellen und zu authentifizieren und so einen geschützten Tunnel einzurichten. Diese TLV-Objekte werden verwendet, um authentifizierungsbezogene Daten zwischen dem Client und dem Server zu übertragen. Sobald der Tunnel eingerichtet ist, beginnt die zweite Phase mit der weiteren Kommunikation zwischen dem Client und dem ISE-Knoten, um die erforderlichen Authentifizierungs- und Autorisierungsrichtlinien festzulegen.

Das NAM-Konfigurationsprofil dient zur Verwendung von EAP-FAST als Authentifizierungsmethode und ist für vom Administrator definierte Netzwerke verfügbar. Darüber hinaus können im NAM-Konfigurationsprofil sowohl die Verbindungstypen für Computer als auch für Benutzer konfiguriert werden.

Das Windows-Gerät des Unternehmens erhält vollständigen Unternehmenszugriff über den NAM mit Statusprüfung.

Das persönliche Windows-Gerät erhält über dieselbe NAM-Konfiguration Zugriff auf ein beschränktes Netzwerk.

Dieses Dokument enthält Anweisungen zur Bereitstellung des Cisco Secure Client Network Access Manager (NAM)-Profils über das Identity Services Engine (ISE) Posture Portal mithilfe der Webbereitstellung sowie der Statusprüfung.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Identity Services Engine (ISE)
- AnyConnect NAM und Profile Editor
- Statusrichtlinie
- Cisco Catalyst-Konfiguration für 802.1x-Services

### Verwendete Komponenten

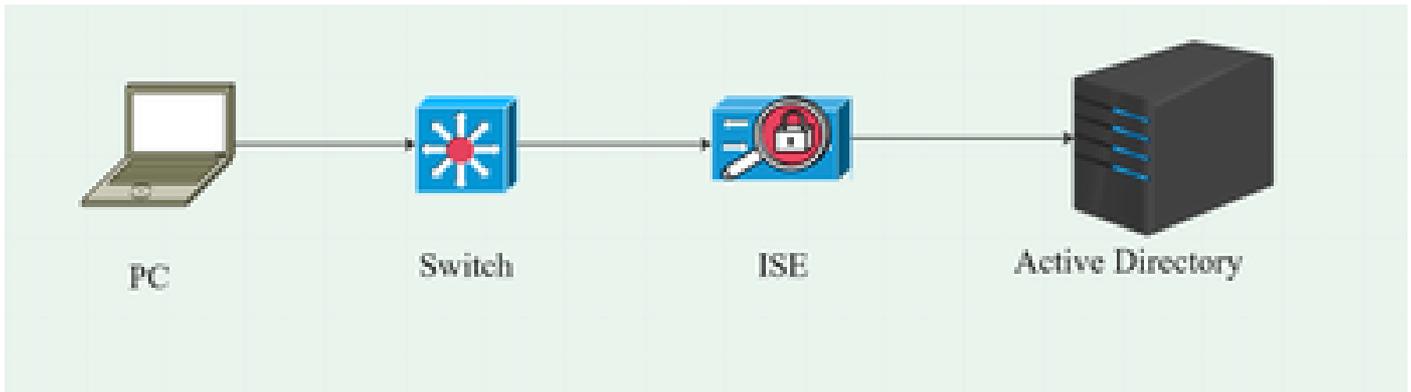
Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco ISE, Version 3.3 und höher
- Windows 10 mit Cisco Secure Mobility Client 5.1.4.74 und höher
- Cisco Catalyst Switch der Serie 9200 mit Software Cisco IOS® XE 17.6.5 und höher
- Active Directory 2016

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

## Konfiguration

### Netzwerkdiagramm



### Datenfluss

Wenn ein PC eine Verbindung mit dem Netzwerk herstellt, stellt die ISE die Autorisierungsrichtlinie für die Umleitung zum Posture Portal bereit.

Der HTTP-Datenverkehr auf dem PC wird zur ISE-Client-Bereitstellungsseite umgeleitet, auf der die NSA-Anwendung von der ISE heruntergeladen wird.

Die NSA installiert dann die Secure Client-Agent-Module auf dem PC.

Nach Abschluss der Agenteninstallation lädt der Agent das auf der ISE konfigurierte Statusprofil und NAM-Profil herunter.

Die Installation des NAM-Moduls löst einen Neustart auf dem PC aus.

Nach dem Neustart führt das NAM-Modul basierend auf dem NAM-Profil eine EAP-FAST-Authentifizierung durch.

Anschließend wird der Status-Scan ausgelöst, und die Konformität wird anhand der ISE-Statusrichtlinie überprüft.

### Switch konfigurieren

Konfigurieren Sie den Access Switch für die 802.1x-Authentifizierung und -Umleitung.

```
aaa neues Modell

aaa authentication dot1x Standardgruppenradius
Standardgruppenradius des AAA-Autorisierungsnetzwerks
aaa accounting dot1x Standard-Start-Stopp-Gruppenradius
aaa server radius dynamic-author
client 10.127.197.53 server-key Qwerty123
```

Authentifizierungstyp any

aaa, Sitzungs-ID gemeinsam

ip radius source-interface Vlan1000

radius-server-Attribut 6 bei Anmeldung

radius-server-Attribut 8 include-in-access-req

radius-server-Attribut 25 access-request include

radius-server-Attribut 31 Mac-Format ietf Großbuchstaben

Radius-Server RAD1

address ipv4 <ISE-Server-IP> auth-port 1812 acct-port 1813

key <geheimer Schlüssel>

dot1x System-Authentifizierungssteuerung

Konfigurieren Sie die Umleitungszugriffskontrollliste für den Benutzer, der zum ISE-Client-Bereitstellungsportal umgeleitet werden soll.

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

Aktivieren Sie die Geräteverfolgung und die HTTP-Umleitung auf dem Switch.

```
Device Tracking Policy <Device Tracking Policy Name>
Nachverfolgung aktivieren
interface <Schnittstellenname>
Device-Tracking Attach-Policy <Name der Device-Tracking-Policy>

ip http server
ip http secure-server
```

## Secure Client-Paket herunterladen

Laden Sie den Profil-Editor, Secure Client-Fenster und das Compliance-Modul herunter, um Dateien manuell über [software.cisco.com](https://software.cisco.com) bereitzustellen.

Geben Sie in der Suchleiste des Produktnamens "Secure Client 5" ein.

Downloads Startseite > Sicherheit > Endpunktsicherheit > Sicherer Client (einschließlich AnyConnect) > Sicherer 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-Konfiguration

### Schritt 1: Paket auf ISE hochladen

Zum Hochladen des Secure Client und des Compliance-Moduls können Sie über die ISE Pakete bereitstellen. Rufen Sie dazu Workcenter > Status > Client-Bereitstellung > Ressourcen > Hinzufügen > Agent-Ressourcen von lokaler Festplatte auf.

The screenshot shows the 'Agent Resources From Local Disk' configuration page in the ISE Client Provisioning interface. The 'Category' dropdown is set to 'Cisco Provided Packages'. A 'Choose File' button is highlighted, showing the file 'cisco-secure-...deploy-k9.pkg'. Below, a table shows 'Agent Uploaded Resources' with one entry: 'CiscoSecureClientDesktopWindows 5.1...'. A 'Submit' button is highlighted at the bottom left.

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

The screenshot shows the 'Resources' page in the ISE Client Provisioning interface. A table lists various resources, with two entries highlighted in red: 'CiscoSecureClientComplianceModuleWindows 4.3.4164...' and 'CiscoSecureClientDesktopWindows 5.1.4.074'.

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

## Schritt 2: Erstellen eines NAM-Profiles mit dem Profil-Editor-Tool

Weitere Informationen zum Konfigurieren eines NAM-Profiles finden Sie in diesem Handbuch [Konfigurieren des sicheren Client-NAM-Profiles](#) .

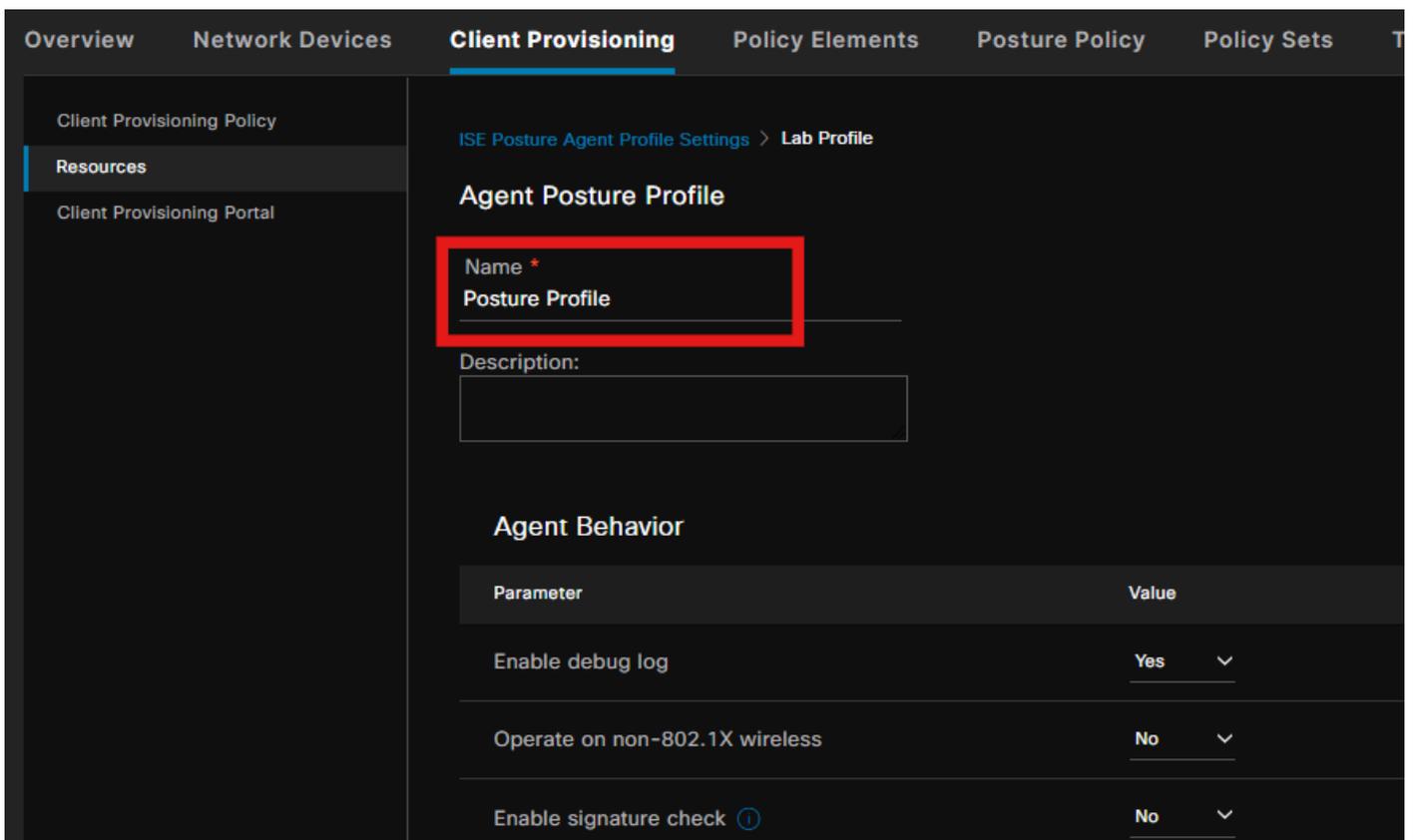
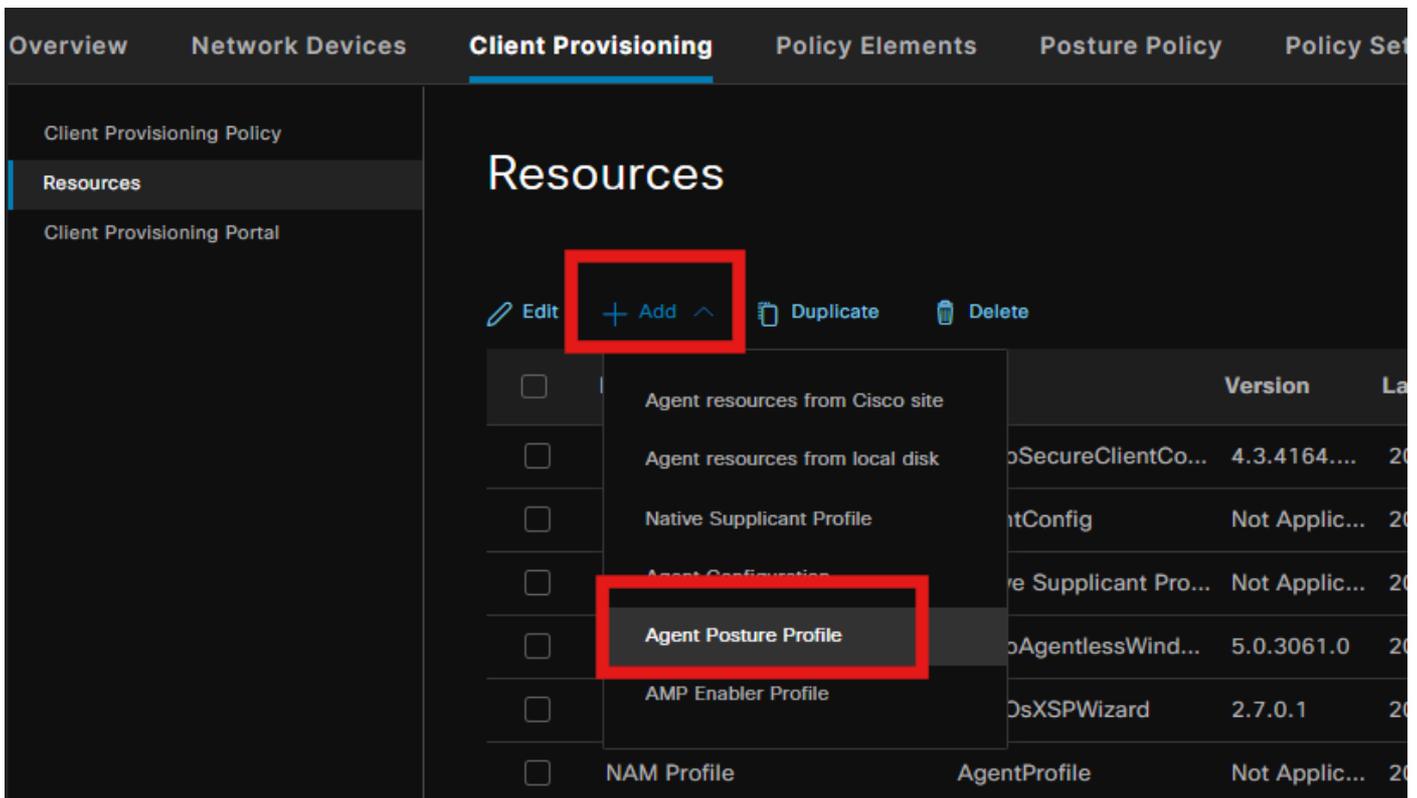
## Schritt 3: NAM-Profil auf die ISE hochladen

Um das NAM-Profil "Configuration.xml" auf die ISE als Agent-Profil hochzuladen, navigieren Sie zu Client Provisioning > Resources > Agent Resources From Local Disk (Client-Bereitstellung > Ressourcen > Agent-Ressourcen von lokaler Festplatte).

The screenshot shows the Cisco ISE Client Provisioning interface. The navigation menu includes Overview, Network Devices, Client Provisioning (selected), Policy Elements, Posture Policy, Policy Sets, Troubleshoot, Reports, and Settings. The left sidebar shows Client Provisioning Policy, Resources (selected), and Client Provisioning Portal. The main content area is titled 'Agent Resources From Local Disk' and contains the following fields:

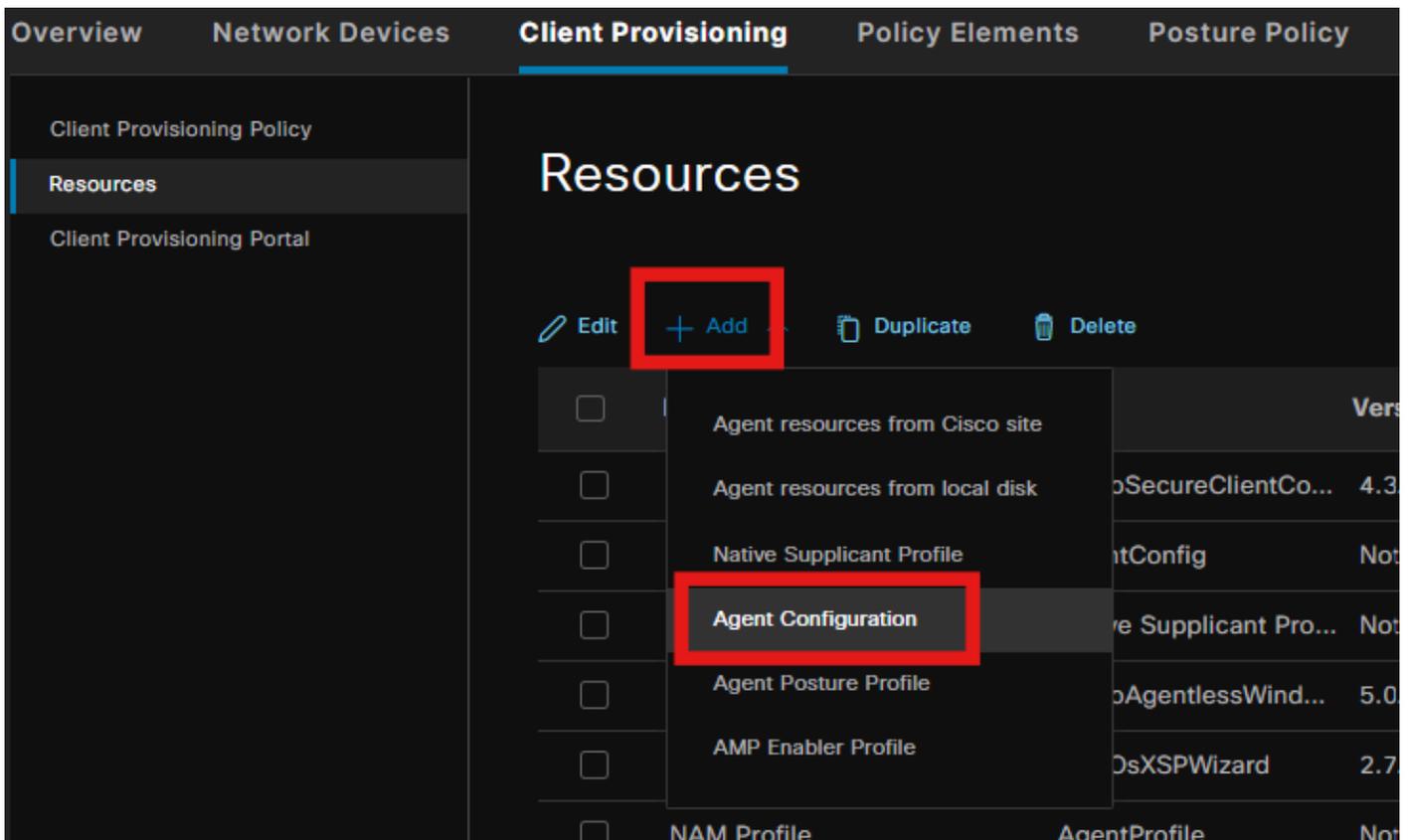
- Category: Customer Created Packa (dropdown menu)
- Type: Agent Profile (dropdown menu)
- \* Name: New Profile (text input)
- Description: (empty text input)
- Choose File: configuration.xml (file selection button)
- Submit (button)
- Cancel (button)

## Schritt 4: Erstellen eines Statusprofils



Vergessen Sie nicht, im Abschnitt "Posture Protocol" (Statusprotokoll) \* hinzuzufügen, damit der Agent eine Verbindung zu allen Servern herstellen kann.

Schritt 5: Agent-Konfiguration erstellen



Wählen Sie das hochgeladene Paket des sicheren Client- und Compliance-Moduls und unter "Module" die ISE Posture-, NAM- und DART-Module aus.

Overview

Network Devices

**Client Provisioning**

Policy Elements

Posture Policy

Policy Sets

Client Provisioning Policy

**Resources**

Client Provisioning Portal

Agent Configuration &gt; 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

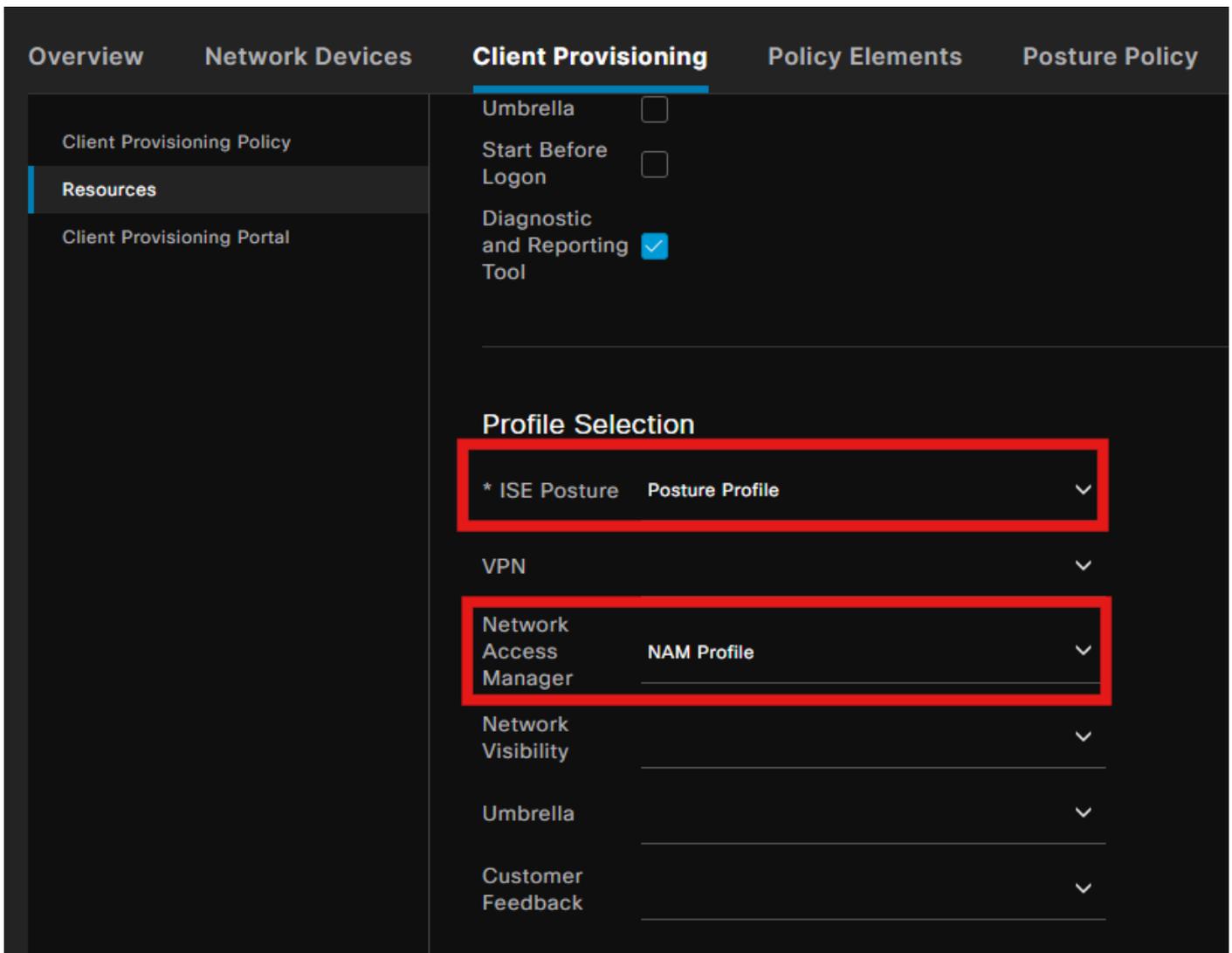
Zero Trust Access

Network Access Manager

Secure Firewall Posture

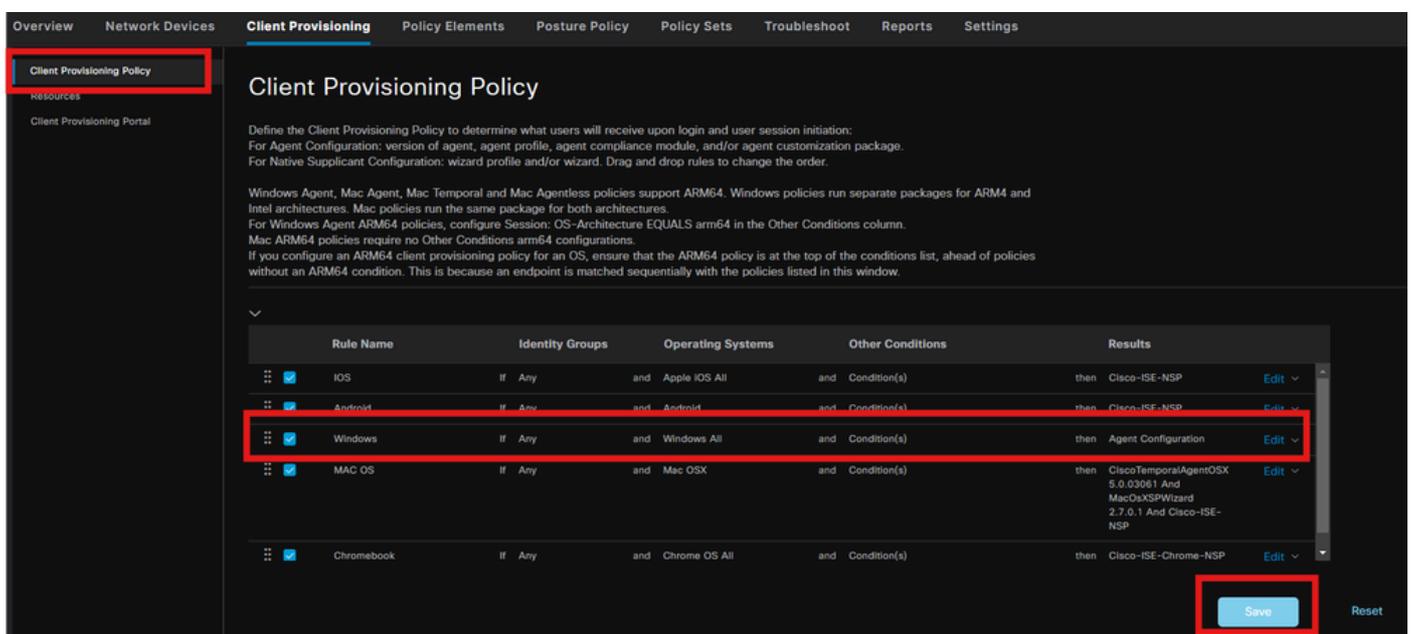
Network Visibility

Wählen Sie unter "Profile" (Profil) die Option Posture (Status) und NAM Profile (NAM-Profil) aus, und klicken Sie auf Submit (Senden).



## Schritt 6: Client-Bereitstellungsrichtlinie

Erstellen Sie eine Client-Bereitstellungsrichtlinie für das Windows-Betriebssystem, und wählen Sie die im vorherigen Schritt erstellte Agentenkonfiguration aus.



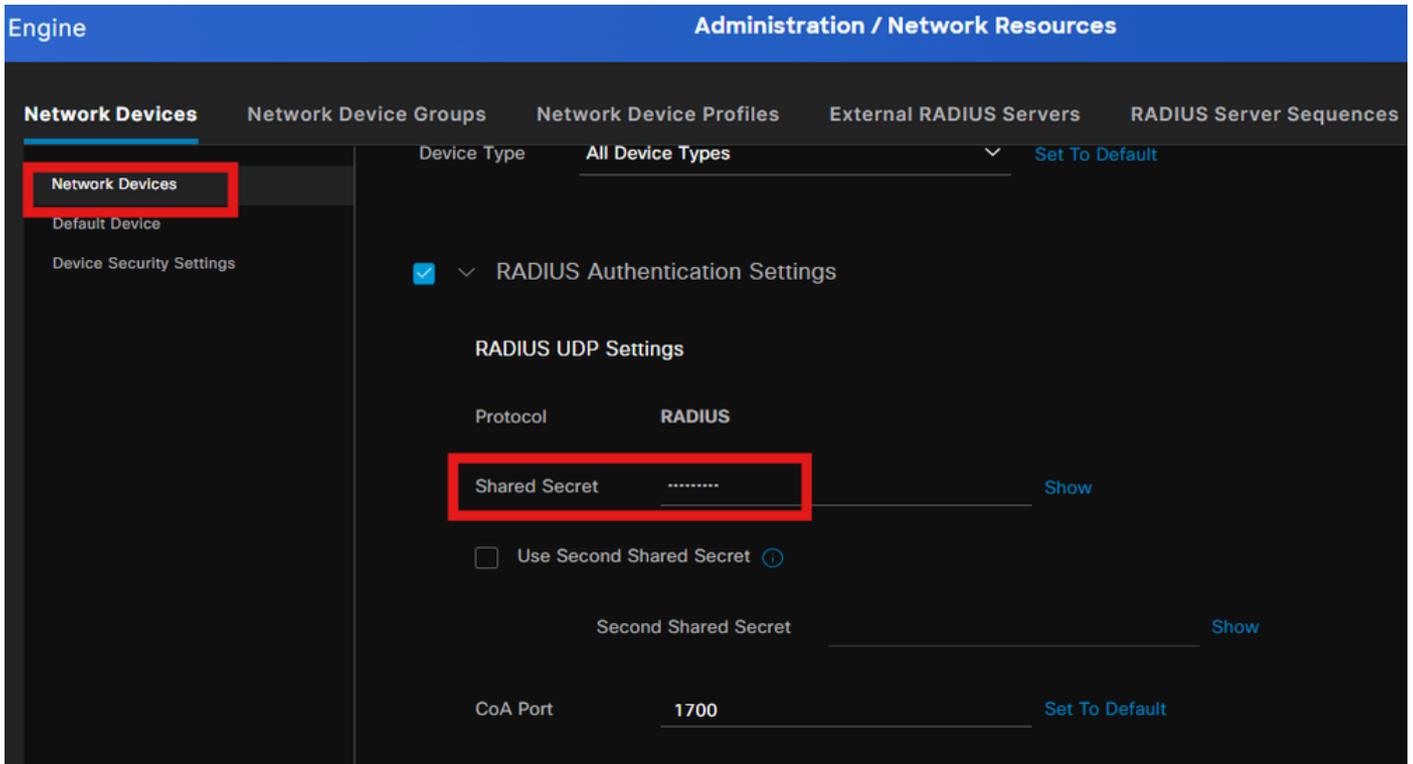
## Schritt 7. Statusrichtlinie

Informationen zum Erstellen der Statusrichtlinie und der Bedingungen finden Sie in diesem [ISE-Bereitstellungsleitfaden](#) .

## Schritt 8: Netzwerkgerät hinzufügen

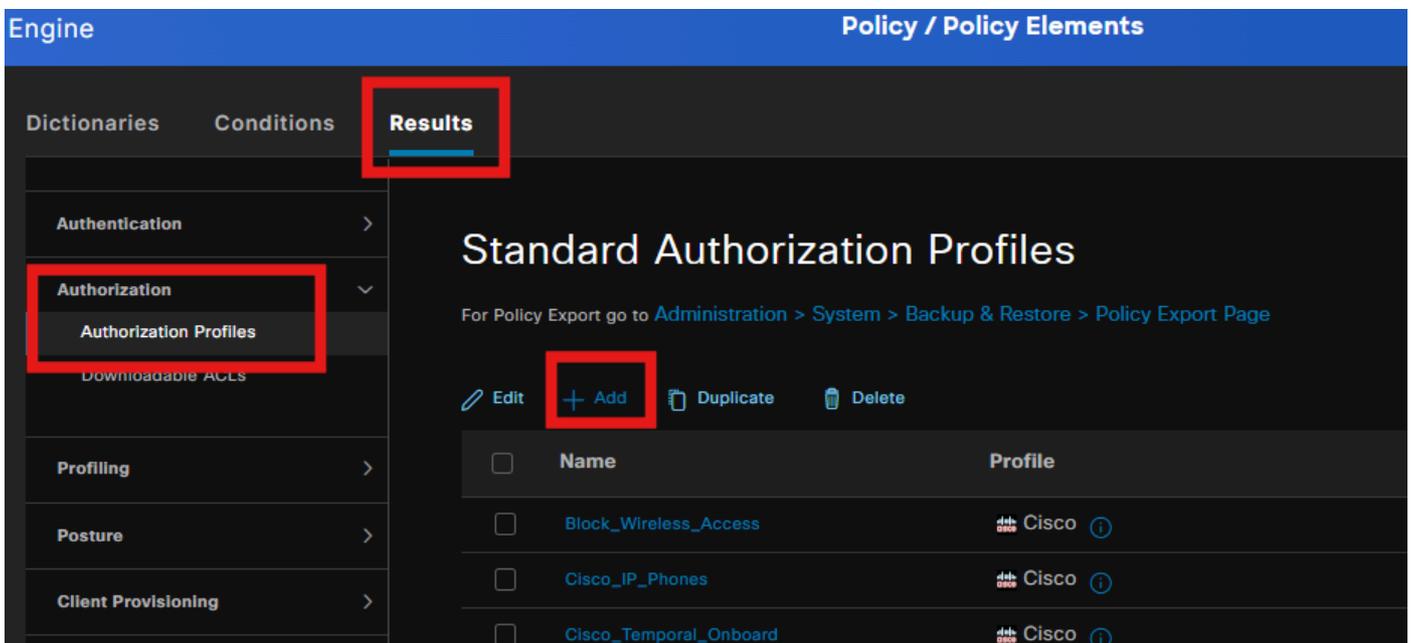
Um die IP-Adresse des Switches und den gemeinsamen geheimen Schlüssel für den Radius hinzuzufügen, navigieren Sie zu Administration > Network Resources (Administration > Netzwerkressourcen).

The screenshot displays the Cisco ISE Administration console interface. The top navigation bar is blue and contains the text "Engine" on the left and "Administration / Network Resources" on the right. Below this, a dark grey navigation menu lists 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 rectangular box. The main content area shows the configuration for a specific network device named "aaa". The breadcrumb "Network Devices List > aaa" is visible. The configuration fields include: "Name" (aaa), "Description" (empty), "IP Address" (10.197.213.22 / 32), "Device Profile" (Cisco), and "Model Name" (empty). The "IP Address" field is highlighted with a red rectangular box. A gear icon is present next to the IP address field, indicating configuration options.

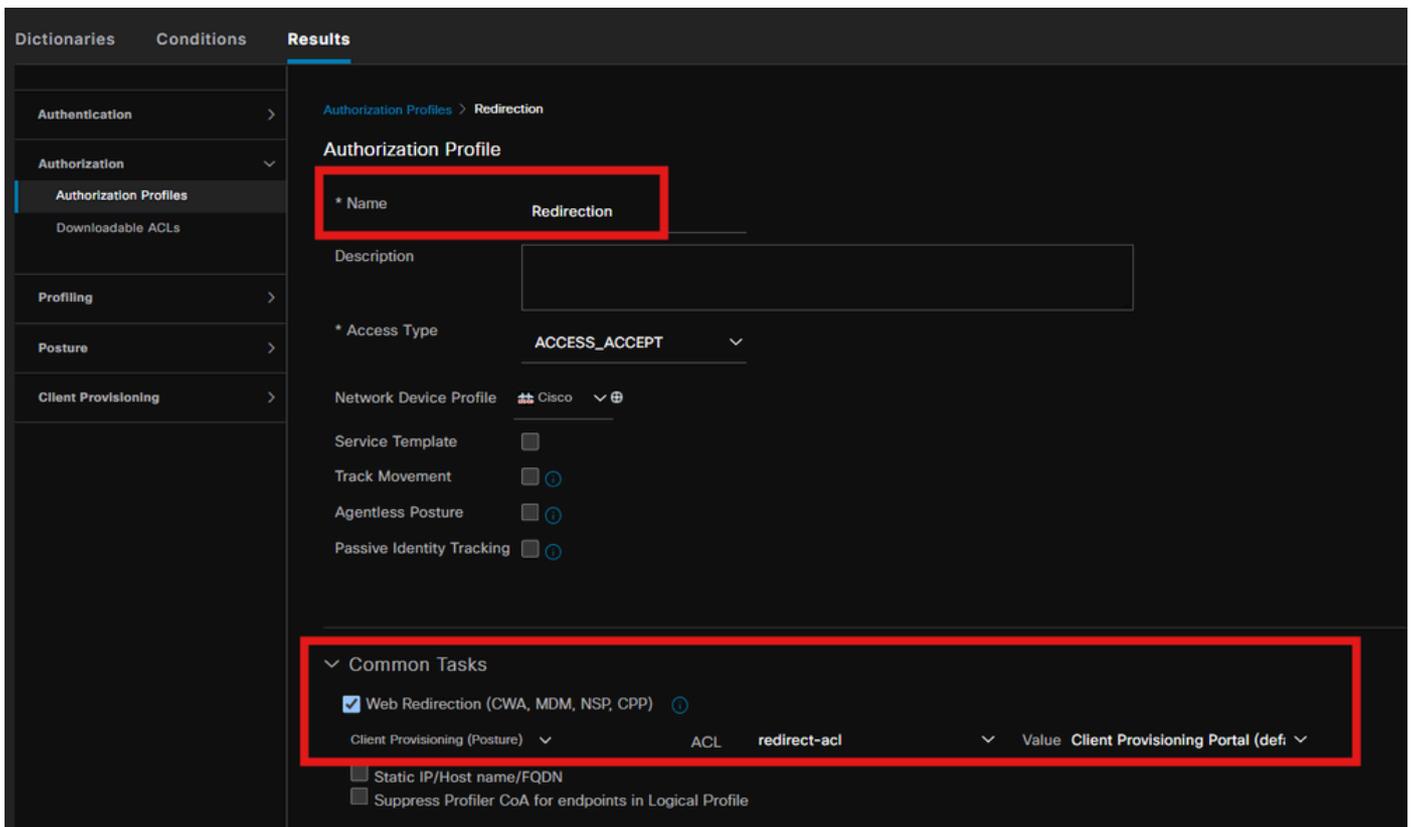


## Schritt 9. Autorisierungsprofil

Um ein Posture-Umleitungsprofil zu erstellen, navigieren Sie zu Policy > Policy Elements > Results.

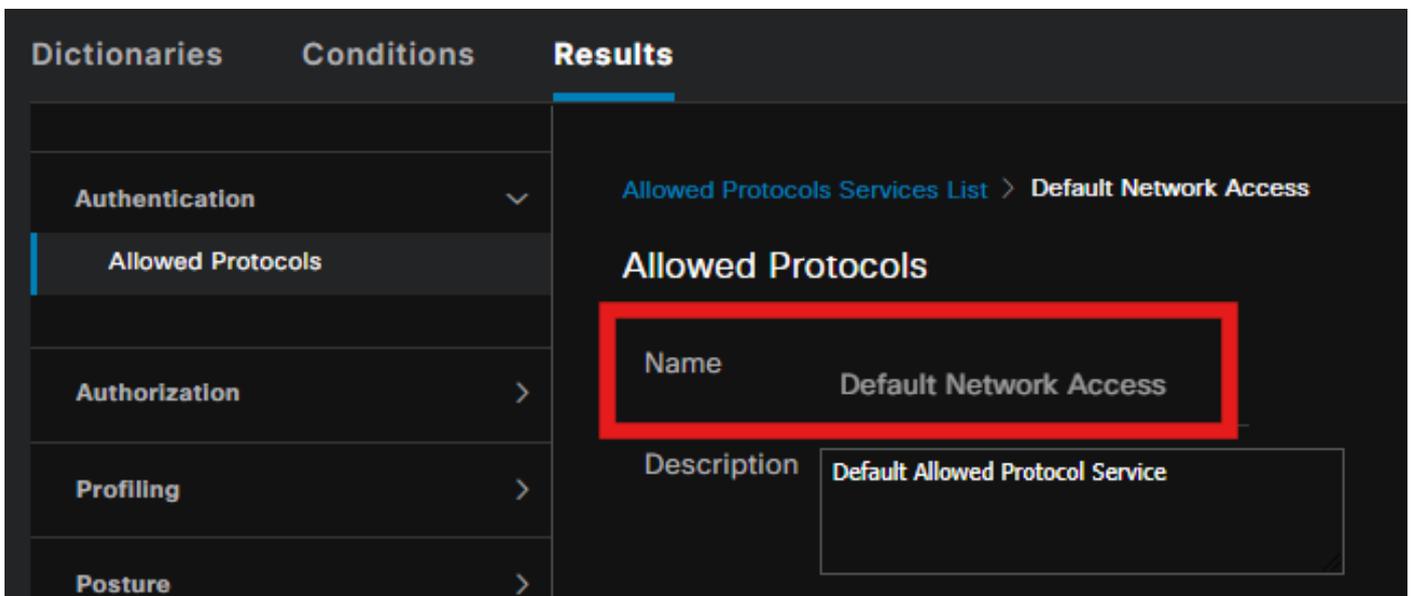


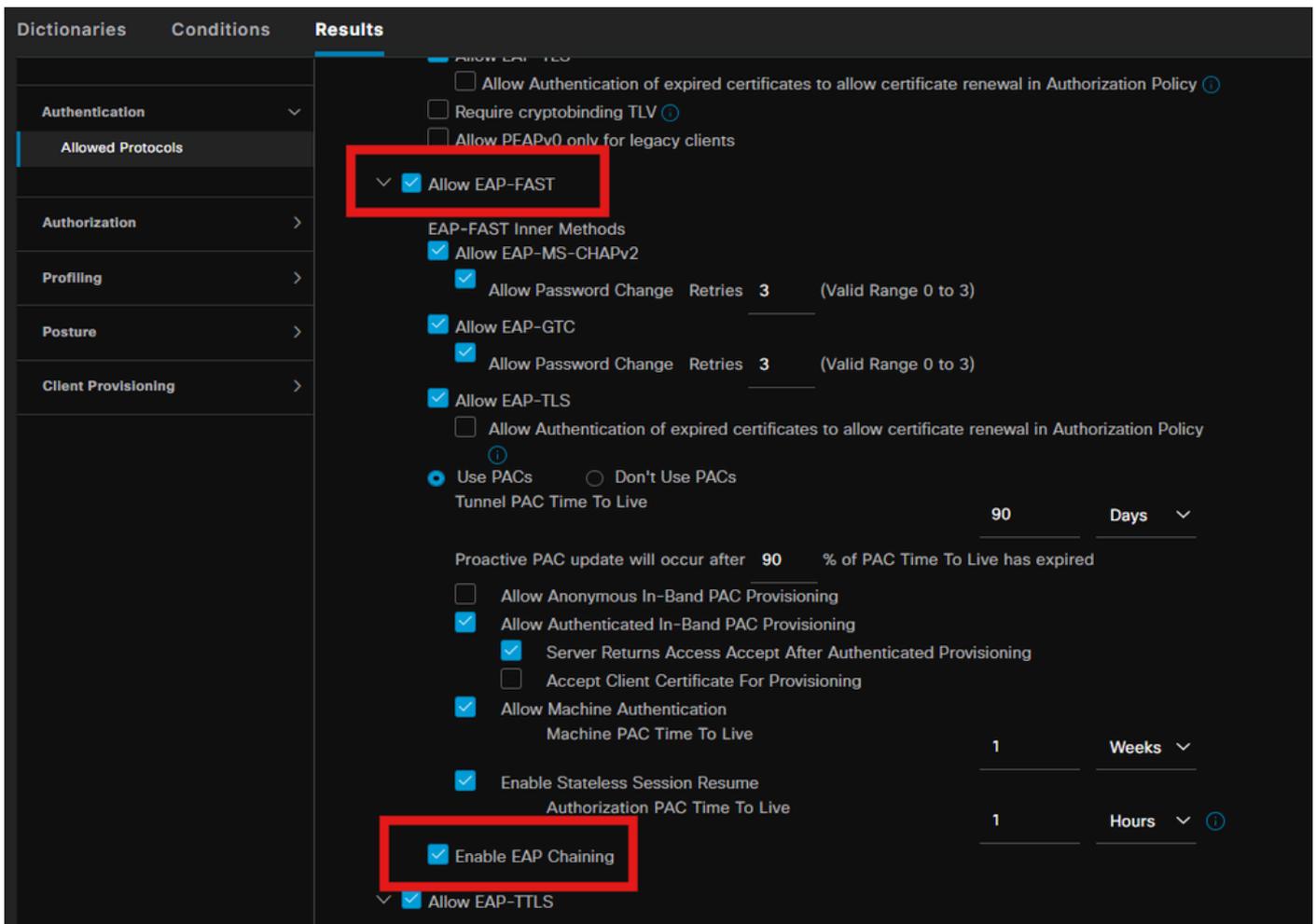
Wählen Sie unter Command Task das Client-Bereitstellungsportal mit Umleitungs-ACL aus.



## Schritt 10. Zulässige Protokolle

Navigieren Sie zu Policy > Policy elements > Results > Authentication > Allowed Protocols, und wählen Sie die EAP Chaining-Einstellungen aus.

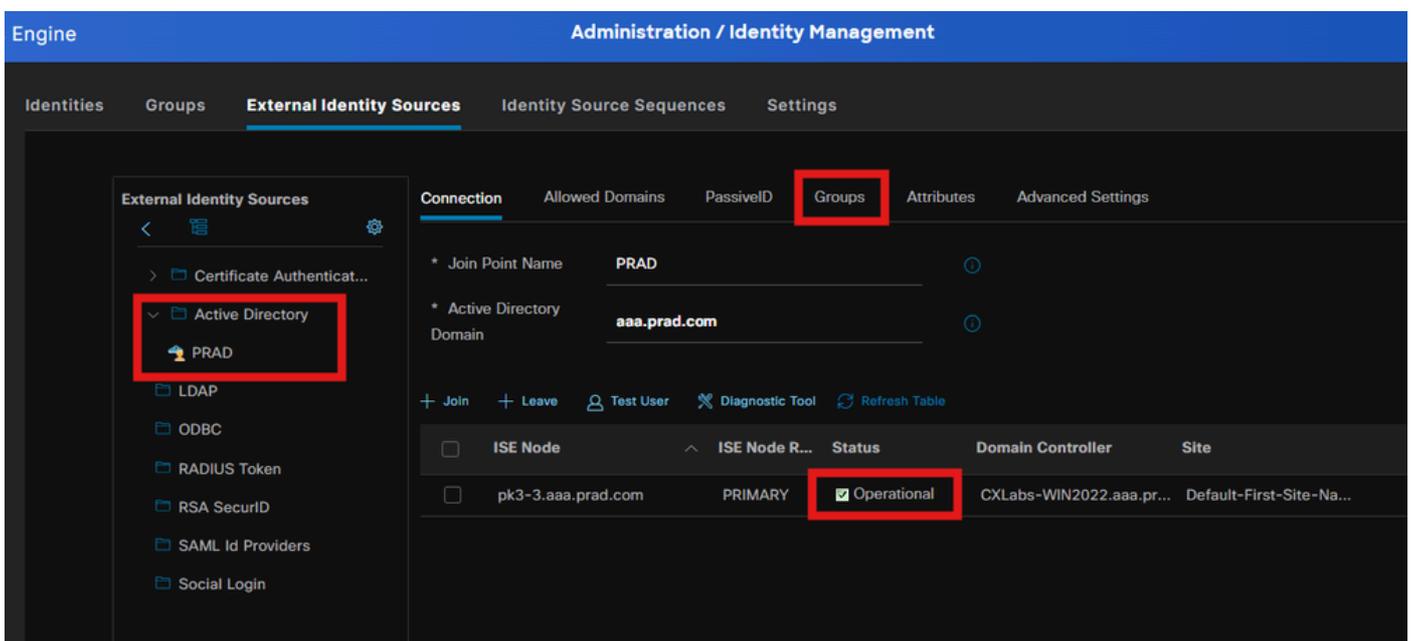




## Schritt 11. Active Directory

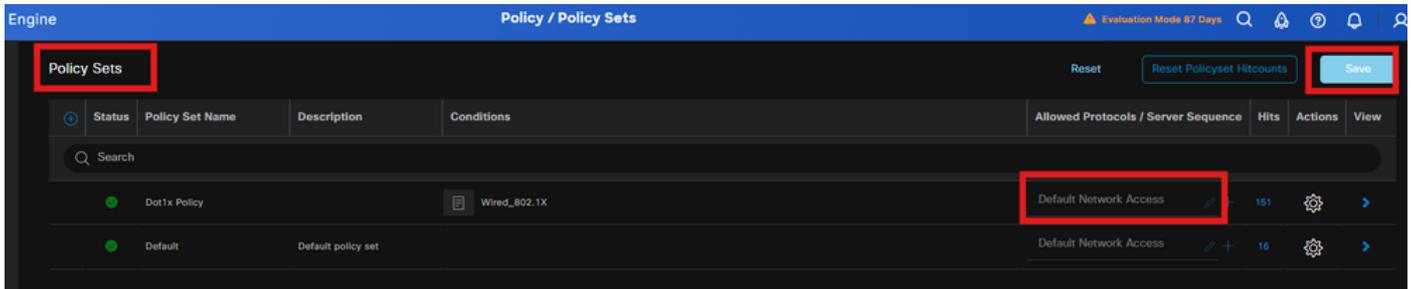
Überprüfen, ob ISE mit der Active Directory-Domäne verknüpft ist, und die Domänengruppen werden ausgewählt, wenn dies für die Autorisierungsbedingungen erforderlich ist.

Administration > Identity Management > External Identity Sources > Active Directory

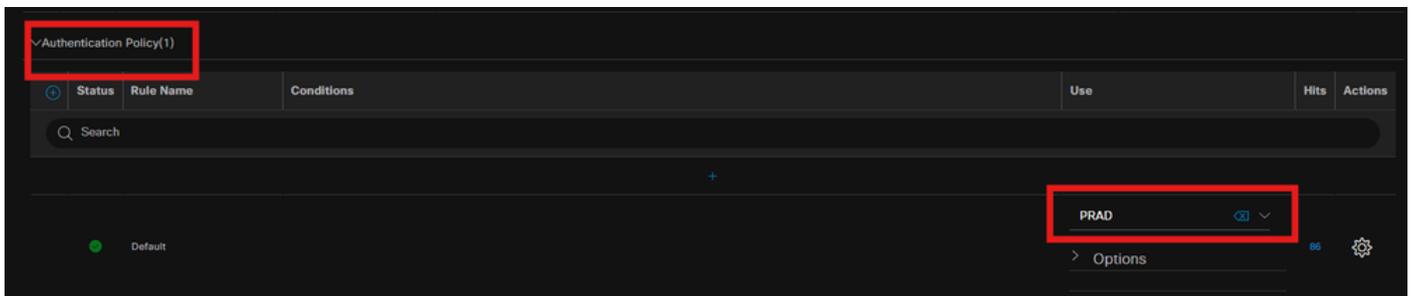


## Schritt 12: Richtlinien

Erstellen Sie eine auf der ISE festgelegte Richtlinie zur Authentifizierung der dot1x-Anforderung. Navigieren Sie zu Policy > Policy Sets (Richtlinie > Richtlinienansätze).



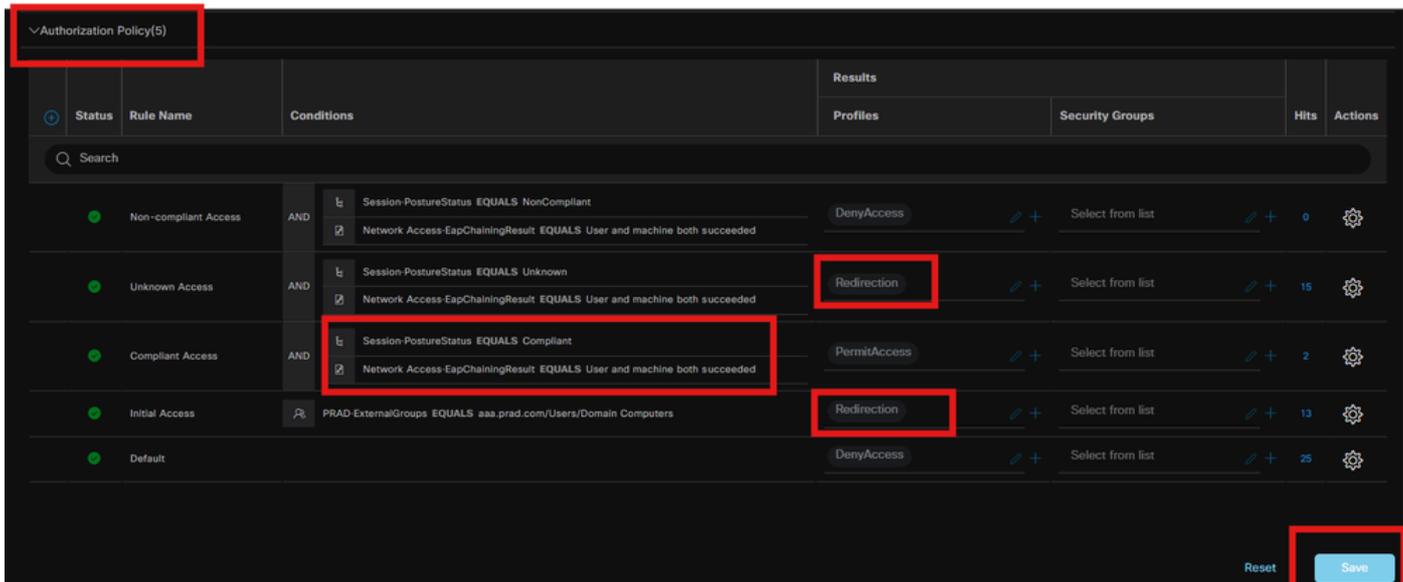
Wählen Sie das Active Directory als Identitätsquelle für die Authentifizierungsrichtlinie aus.



Konfigurieren Sie unterschiedliche Autorisierungsregeln basierend auf dem Status "Unbekannt", "nicht konform" und "konform".

In diesem Anwendungsfall.

- Erstzugriff: Umleitung zum ISE Client Provisioning Portal zur Installation des Secure Client Agent und des NAM-Profiles
- Unbekannter Zugriff: Zugriff auf das Client-Bereitstellungsportal zur umleitungsbasierten Stuserkennung
- Compliance-Zugriff: vollständiger Netzwerkzugriff
- Nicht konform: Zugriff verweigern



## Überprüfung

Schritt 1: Secure Client Posture/NAM-Modul von ISE herunterladen und installieren

Wählen Sie den Endpunkt aus, der mit Punkt1x authentifiziert wurde, und treffen Sie die Autorisierungsregel "Initial Access". Navigieren Sie zu 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

Geben Sie auf Switch die Umleitungs-URL und die ACL an, die für den Endpunkt angewendet werden sollen.

```
Switch#show authentication session interface te1/0/24 details
Schnittstelle: TenGigabitEthernet1/0/24
IIF-ID: 0x19262768
MAC-Adresse: x4x6.xxxx.xxxx
IPv6-Adresse: Unbekannt
IPv4-Adresse: <client-IP>
Benutzername: host/DESKTOP-xxxxxx.aaa.prad.com
Status: Autorisiert
Domäne: DATEN
Oper-Host-Modus: Single-Host
Ober Kontrollverzeichnis: beide
Sitzungs-Timeout: k. A.
Allgemeine Sitzungs-ID: 16D5C50A0000002CF067366B
Kontositzungs-ID: 0x0000001f
```

Griff: 0x7a000017

Aktuelle Richtlinie: POLICY\_TE1/0/24

Lokale Richtlinien:

Servicevorlage: DEFAULT\_LINKSEC\_POLICY\_SHOULD\_SECURE (Priorität 150)

Sicherheitsrichtlinien: sollten

Sicherheitsstatus: Verbindung ungesichert

Serverrichtlinien:

URL-Umleitungszugriffskontrollliste: redirect-acl

URL-Umleitung:

<https://ise33.aaa.prad.com:8443/portal/gateway?sessionId=16D5C50A0000002CF067366A&portal=ee397180-4995-8aa2-9fb282645a8f&action=cpp&token=518f857900a37f9afc6d2da8b6fe3bc2>

ACS ACL: xACSACLx-IP-PERMIT\_ALL\_IPV4\_TRAFFIC-57f6b0d3

Methodenstatusliste:

Methodenstatus

dot1x Authentifizierung erfolgreich

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

Network Layer Address Link Layer Address Interface vlan prlvl age state Restzeit

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

Überprüfen Sie auf dem Endgerät den an ISE Posture Posture Posture umgeleiteten Datenverkehr, und klicken Sie auf Start, um den Network Setup Assistant auf den Endgerät herunterzuladen.

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

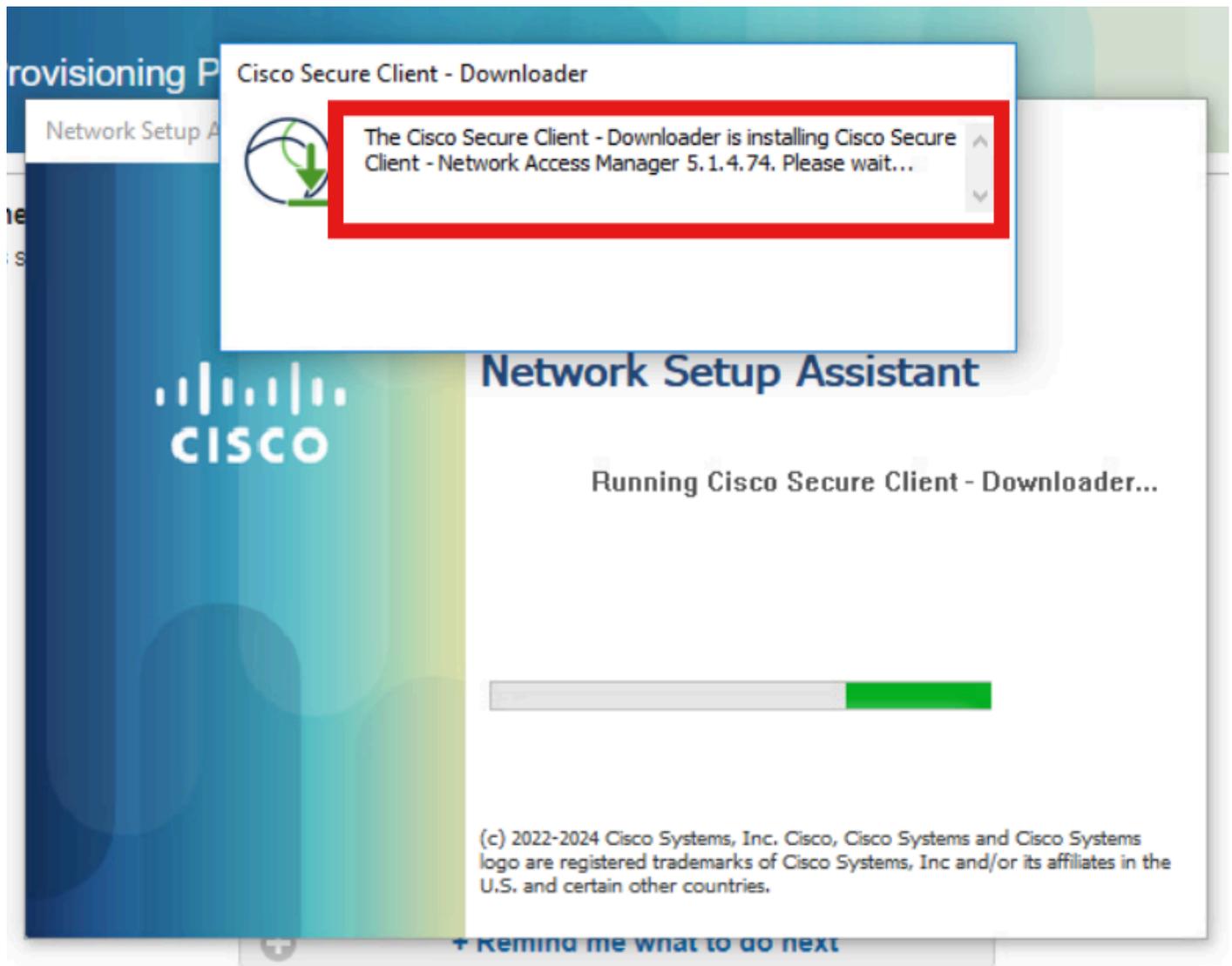
The screenshot shows the Cisco Client Provisioning Portal interface. At the top left, the 'SCO' logo and 'Client Provisioning Portal' text are visible. Below this, a 'Device Security Check' section states: 'Your computer requires security software to be installed before you can connect to the network.' A central message box titled 'Unable to detect Posture Agent' contains the following text: '+ 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.', and 'You have 4 minutes to install and for the compliance check to complete'. At the bottom of this message box is a '+ Remind me what to do next' button. In the top right corner, a 'Recent download history' window is open, showing a single entry: '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'. A 'Full download history' link is also present.

Klicken Sie auf Ausführen, um die NSA-Anwendung zu installieren.

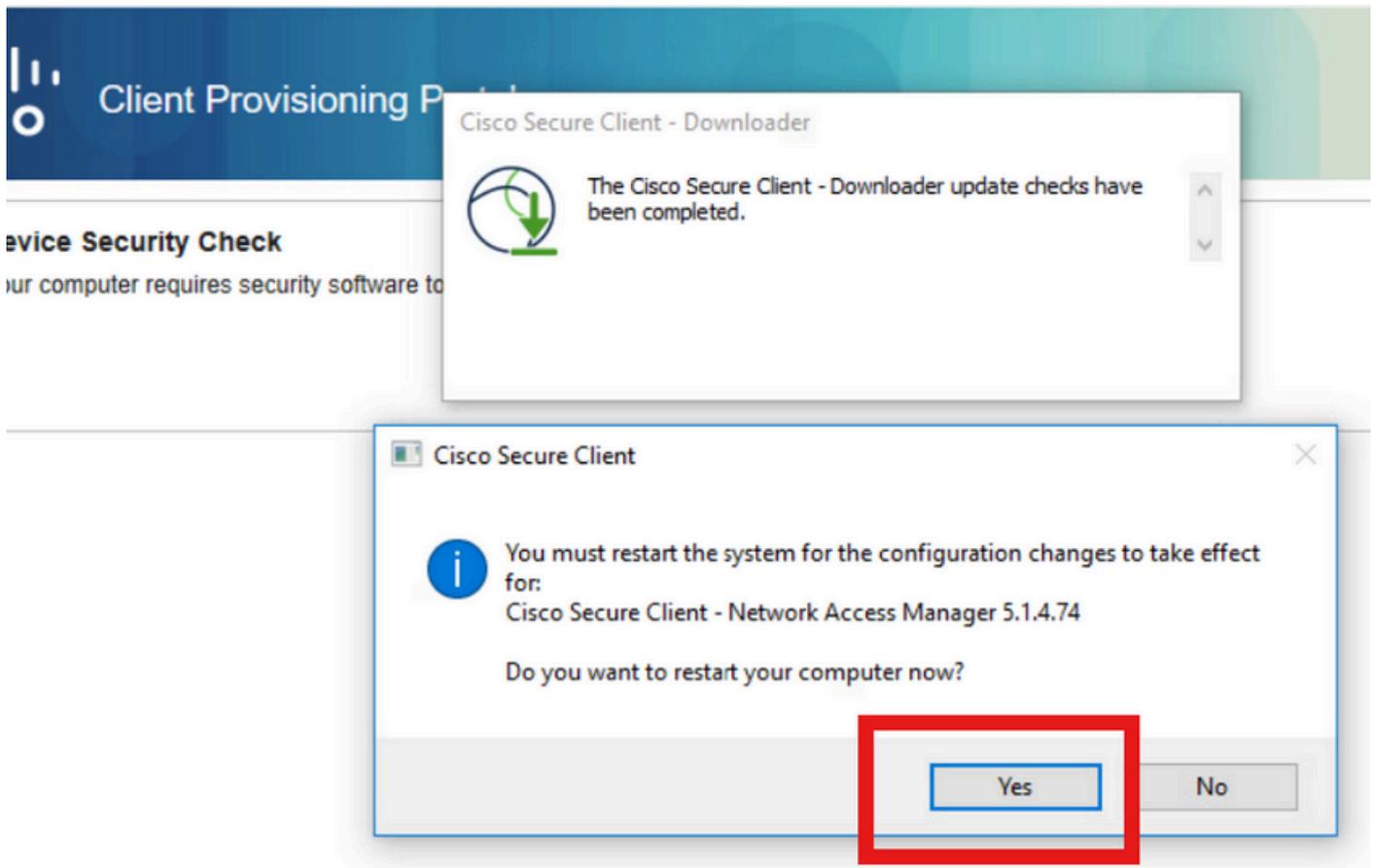
The screenshot shows a Windows SmartScreen warning dialog box overlaid on the Cisco Client Provisioning Portal. The dialog box has a blue background and white text. The title bar reads 'SmartScreen can't be reached right now'. The main text says: 'Check your Internet connection. Windows Defender SmartScreen is unreachable and can't help you decide if this app is ok to run.' Below this, it lists 'Publisher: Cisco Systems, Inc.' and 'App: cisco-secure-client-ise-network-assistant-win-5.1.4.74\_pk3-...'. At the bottom right, there are two buttons: 'Run' and 'Don't Run'. The 'Run' button is highlighted with a red dashed border.

Jetzt ruft die NSA den Download des Secure Client Agent von der ISE auf und installiert das

Posture-Modul, das NAM-Modul und die NAM Profile-configuration.xml.



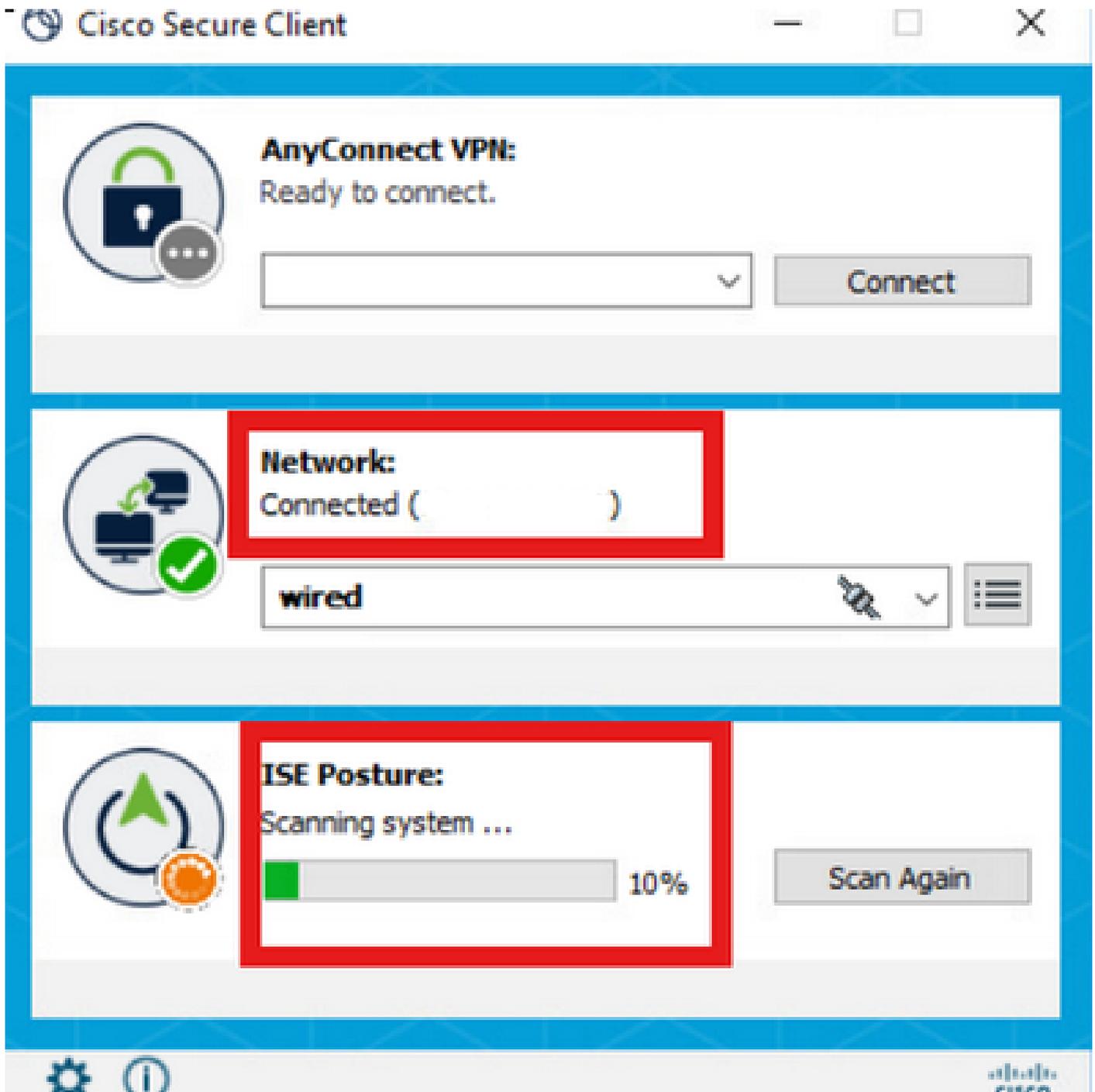
Nach der NAM-Installation wird eine Aufforderung zum Neustart ausgelöst. Klicken Sie auf Ja.



## Schritt 2: EAP-FAST

Nach dem Neustart des PCs und der Anmeldung des Benutzers authentifiziert das NAM Benutzer und Computer über EAP-FAST.

Wenn sich das Endgerät korrekt authentifiziert, zeigt NAM an, dass eine Verbindung besteht, und das Statusmodul löst den Status-Scan aus.



Bei ISE-Live-Protokollen gilt für den Endpunkt jetzt die Regel für unbekanntes Zugriff.

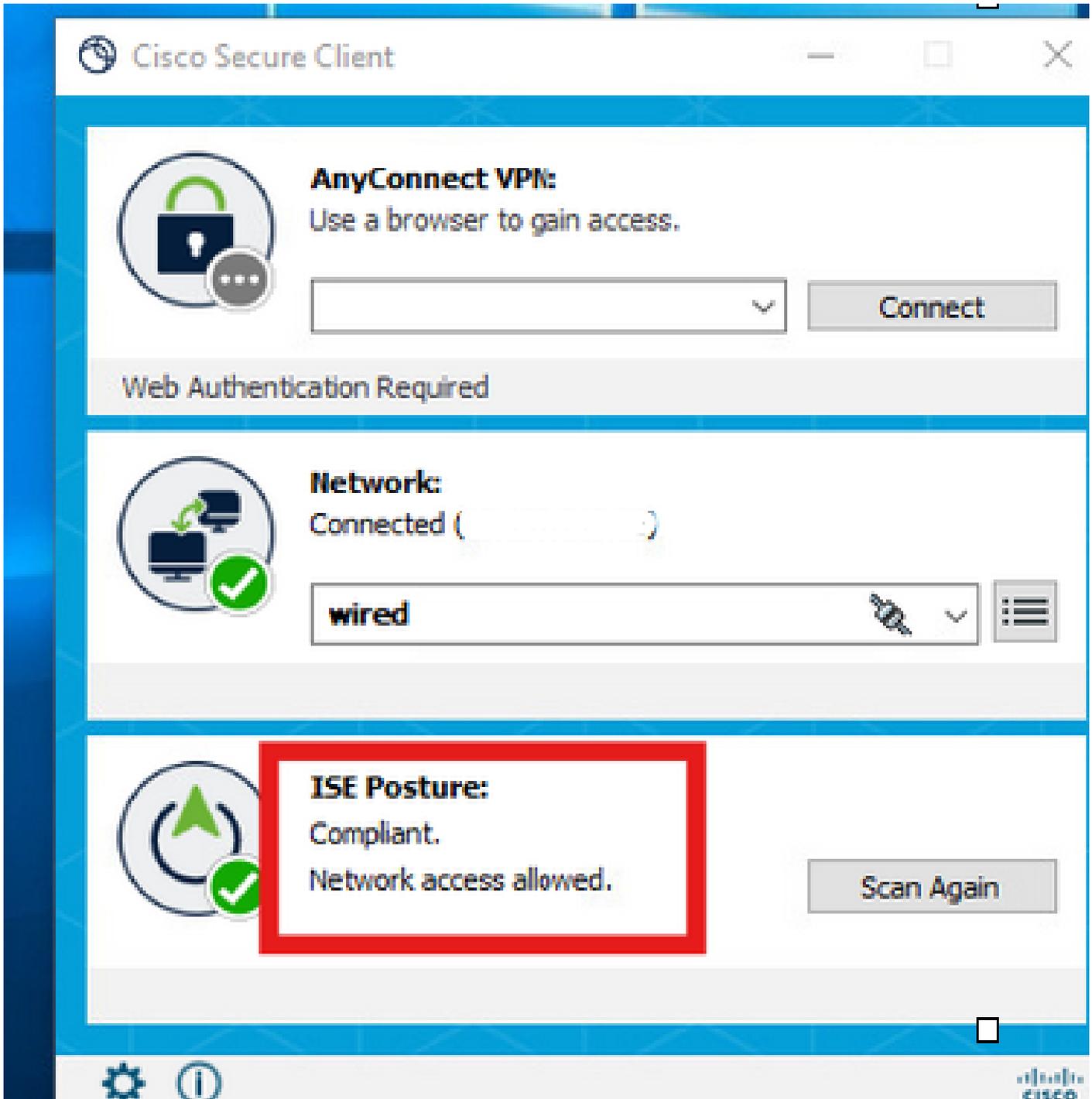
Jul 27, 2024 12:29:06...			user1_host/DESKTOP-QSC...	Dot1x Policy >> Default	<b>Dot1x Policy &gt;&gt; Unknown Access</b>	Redirection	Pending
Jul 27, 2024 12:28:48...			host/DESKTOP-QSCE4P3	Dot1x Policy >> Default	Dot1x Policy >> Initial Access	Redirection	Pending

Das Authentifizierungsprotokoll basiert nun auf der NAM-Profilkonfiguration auf EAP-FAST, und das EAP-Chaining-Ergebnis lautet "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	
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

### Schritt 3: Statusüberprüfung

Das Secure Client Posture-Modul löst den Status-Scan aus und wird entsprechend der ISE-Statusrichtlinie als "Complaint" (Beschwerde) markiert.



Die CoA wird nach dem Status-Scan ausgelöst, und der Endpunkt erreicht jetzt die Beschwerdeinformationsrichtlinie.

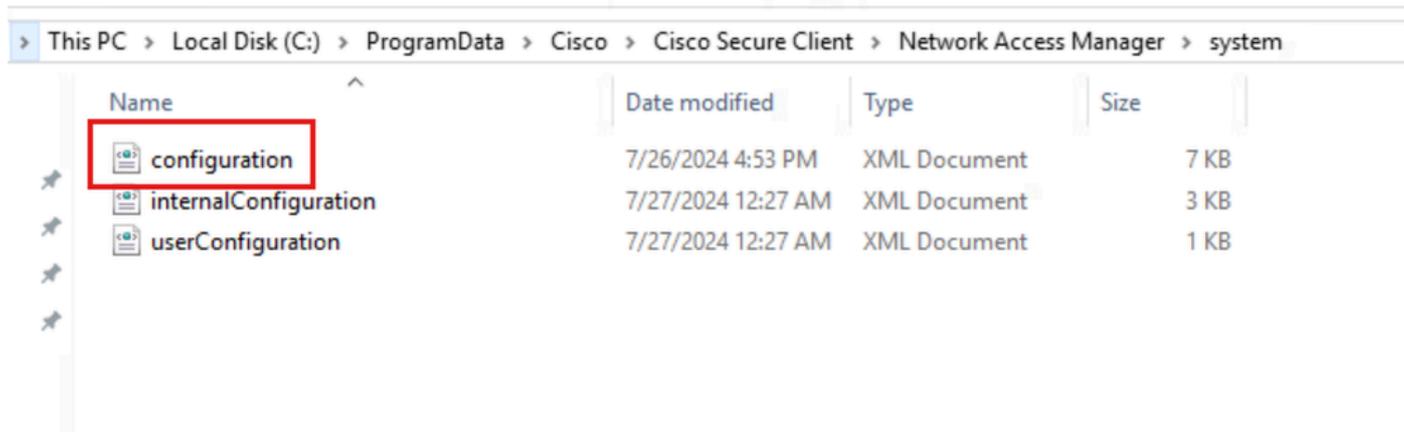
Time	Status	Details	Endpoint ID	Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture Status
Jul 27, 2024 12:29:32...			B4:96:91:F9:56:8B	user1_host/DESKTOP-QSC...	Dot1x Policy >> Default	Dot1x Policy >> Compliant Access	PermitAccess	Compliant
Jul 27, 2024 12:29:32...			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

Fehlerbehebung

## Schritt 1: NAM-Profil

Vergewissern Sie sich, dass die Datei NAM Profile configuration.xml nach der Installation des NAM-Moduls in diesem Pfad auf dem PC vorhanden ist.

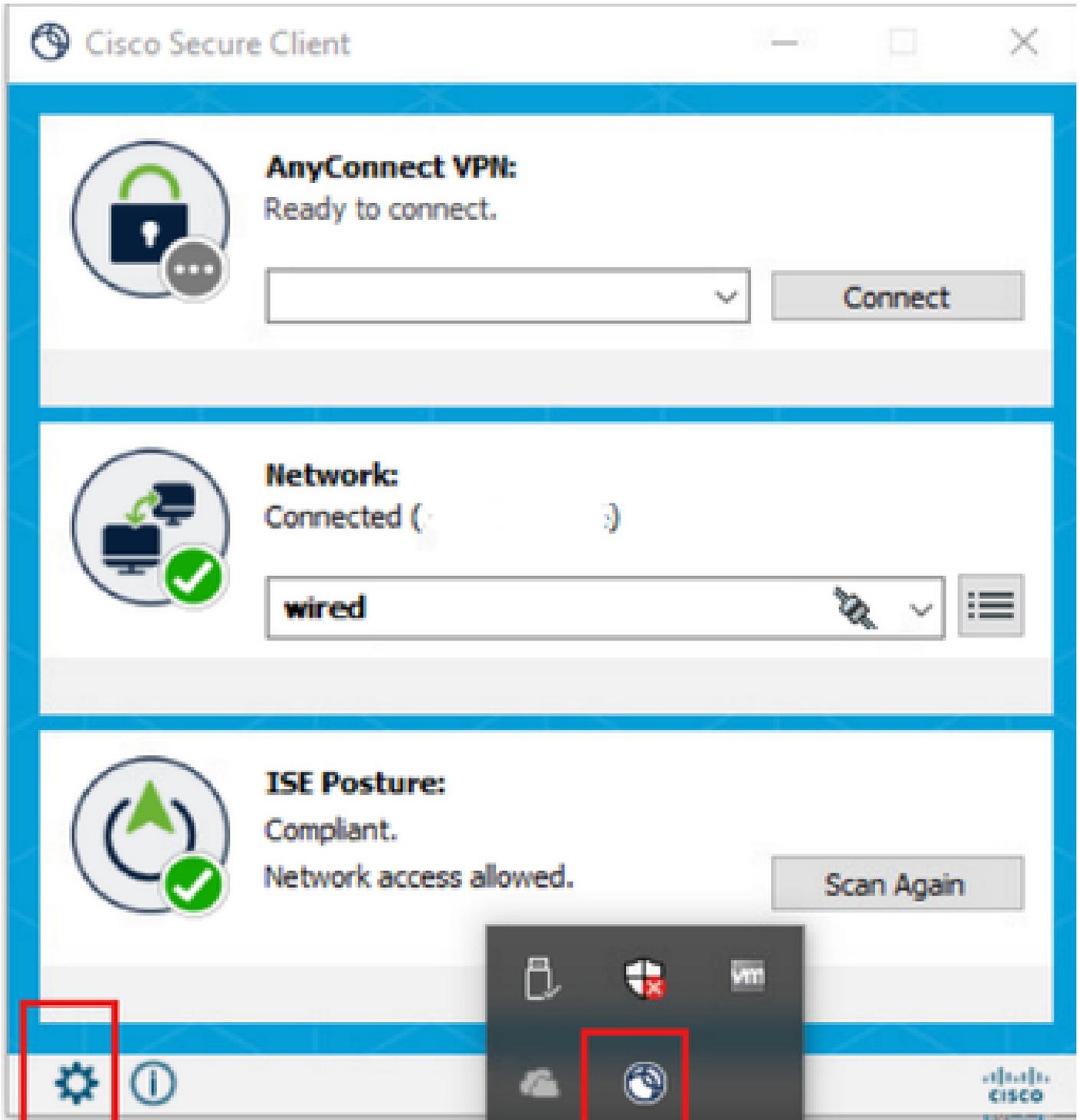
C:\ProgramData\Cisco\Cisco Secure Client\Network Access Manager\system



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

## Schritt 2: Erweiterte NAM-Protokollierung

Klicken Sie in der Taskleiste auf das Symbol für den sicheren Client, und wählen Sie das Symbol "Einstellungen" aus.



Navigieren Sie zur Registerkarte Netzwerk > Protokolleinstellungen. Aktivieren Sie das Kontrollkästchen "Erweiterte Protokollierung aktivieren".

Legen Sie die Größe der Paketerfassungsdatei auf 100 MB fest.

Klicken Sie nach der Reproduktion des Problems auf Diagnostics (Diagnose), um das DART-Paket auf dem Endgerät zu erstellen.



The screenshot shows the Cisco Secure Client interface. On the left, a navigation pane has 'Network' highlighted. The main content area is titled 'Network Access Manager' and has tabs for 'Configuration', 'Log Settings', 'Statistics', and 'Message History'. The 'Log Settings' tab is active, showing a section for 'Use extended logging to collect additional information about product operations.' This section contains several settings: 'Enable Extended Logging' is checked, 'IHV' is set to 'Off', 'Filter Driver' is set to 'Off', 'Credential Provider' is unchecked, 'Packet Capture' is checked, and 'Maximum Packet Capture File Size (MB)' is set to 100. At the bottom left of the interface, there is a 'Diagnostics' button.

Im Abschnitt Nachrichtenverlauf werden die Details zu jedem Schritt angezeigt, den NAM durchgeführt hat.

### Schritt 3: Debuggen auf Switch

Aktivieren Sie diese Fehlerbehebungen auf dem Switch, um dot1x und den Umleitungsfluss zu beheben.

```
debug ip http all
```

debuggen von IP-HTTP-Transaktionen

```
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 debugging
```

```
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
```

So zeigen Sie die Protokolle an

```
show logging
```

```
show logging prozess smd intern
```

## Schritt 4: Debuggen auf der ISE

Sammeln Sie das ISE-Supportpaket mit den folgenden Attributen, die auf Debugebene festgelegt werden sollen:

- Körperhaltung
- Portal
- Bereitstellung
- Laufzeit-AAA
- NSF
- NSF-Sitzung
- Schweizer
- Client-Webanwendung

## Zugehörige Informationen

[Konfigurieren von Secure Client NAM](#)

[ISE-Bereitstellungsleitfaden mit Vorschriften für Status](#)

[Fehlerbehebung bei Dot1x auf Catalyst Switches der Serie 9000](#)

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.