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

Inhalt

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

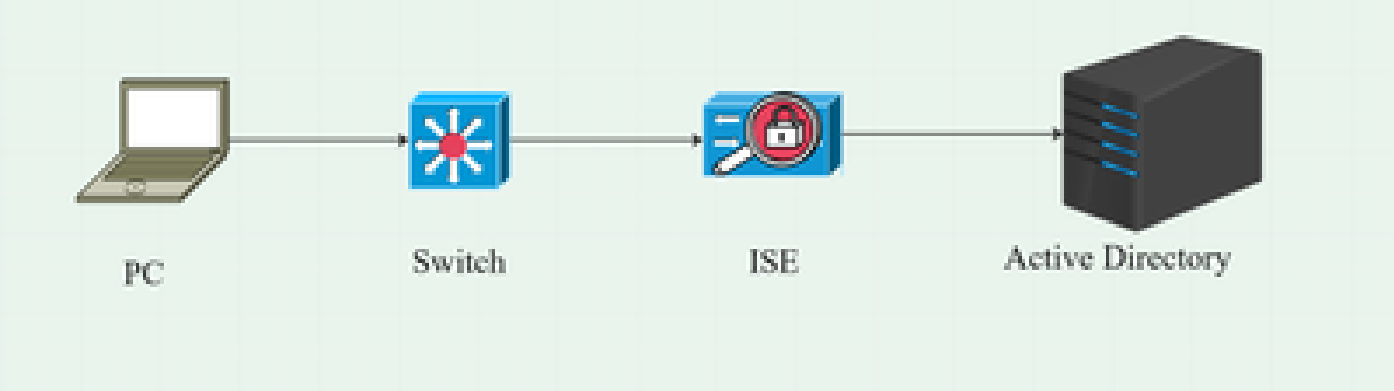
Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- 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 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 bereitzustellen.

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

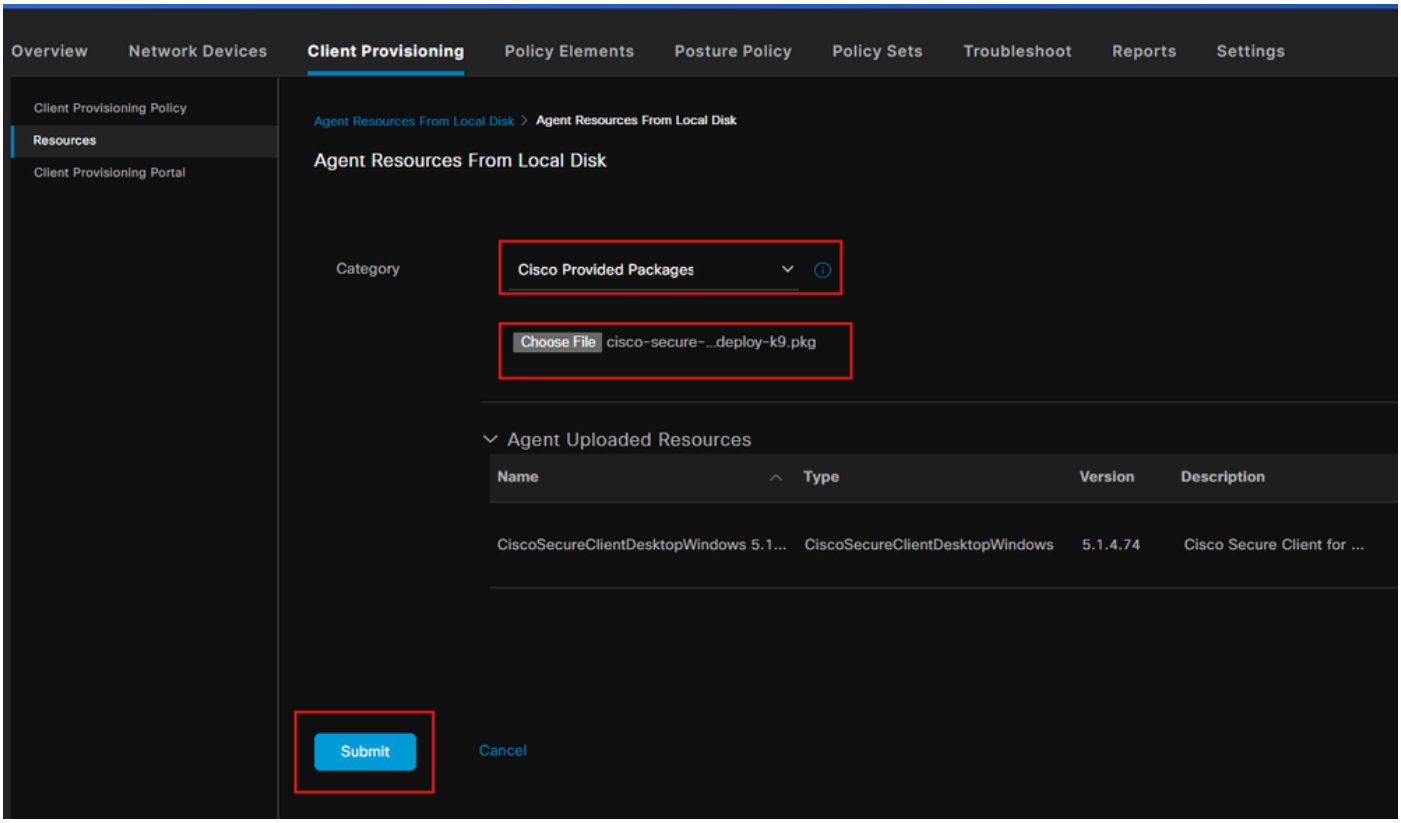
Downloads Startseite > Sicherheit > Endpunktsicherheit > Sicherer Client (einschließlich AnyConnect) > Sicherer Client 5 > AnyConnect VPN Client-Software

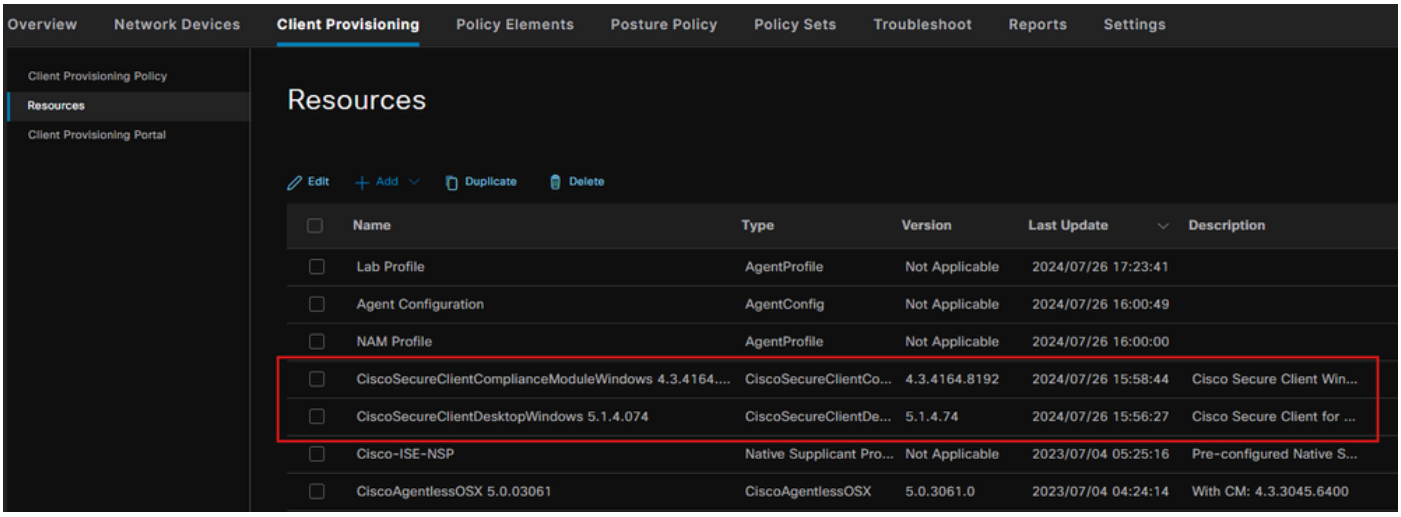
- cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg
- cisco-secure-client-win-4.3.4164.8192-isecompliance-webdeploy-k9.pkg
- tools-cisco-secure-client-win-5.1.4.74-profileeditor-k9.msi

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.



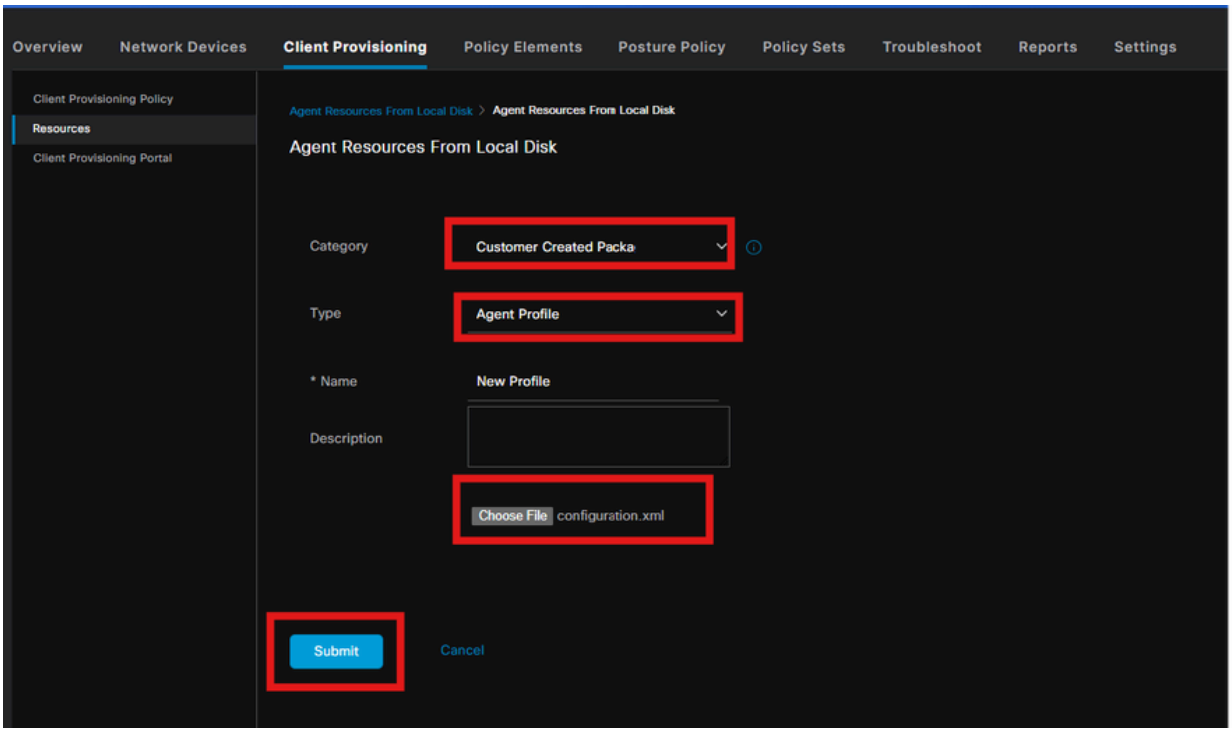


Schritt 2: Erstellen eines NAM-Profils mit dem Profil-Editor-Tool

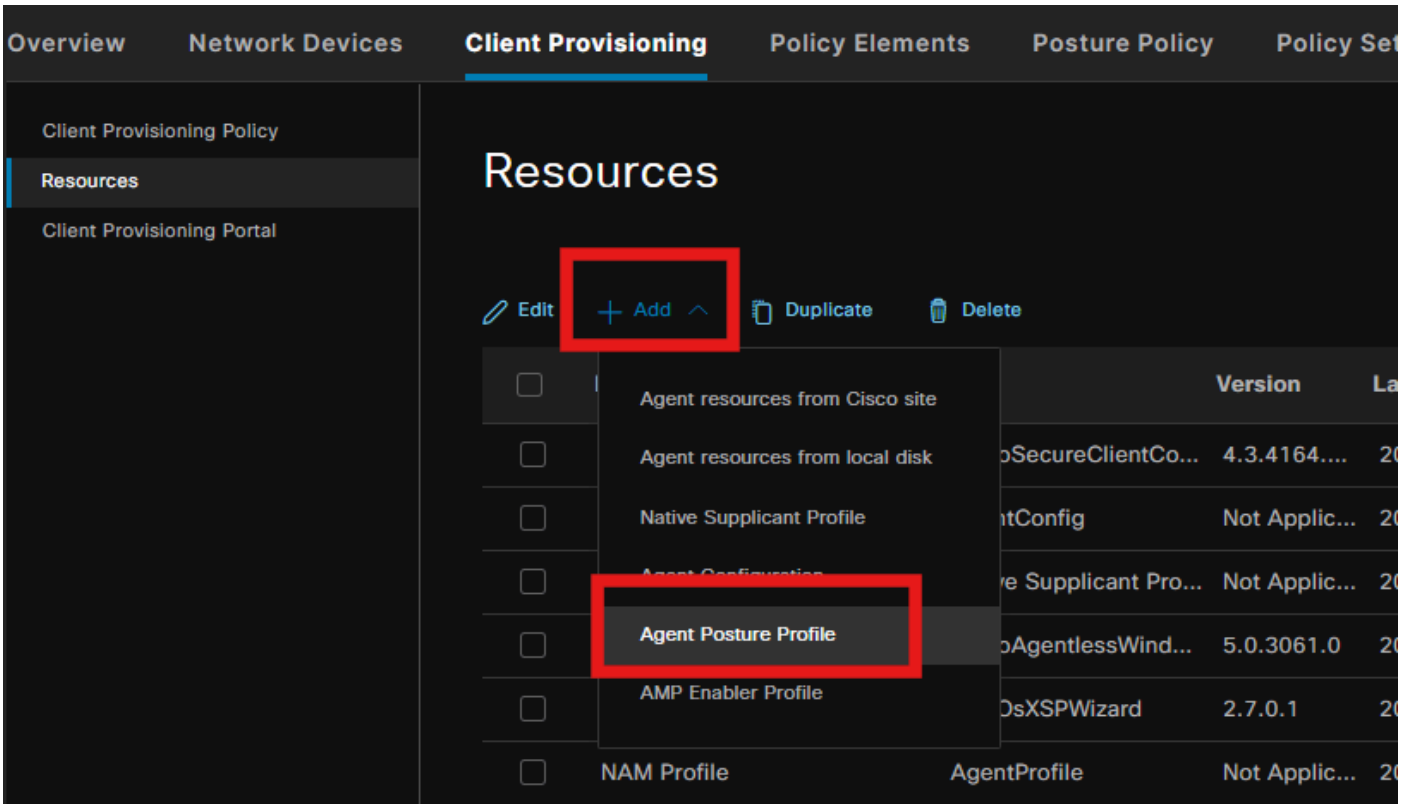
Weitere Informationen zum Konfigurieren eines NAM-Profils finden Sie in diesem Handbuch [Konfigurieren des sicheren Client-NAM-Profils](#) .

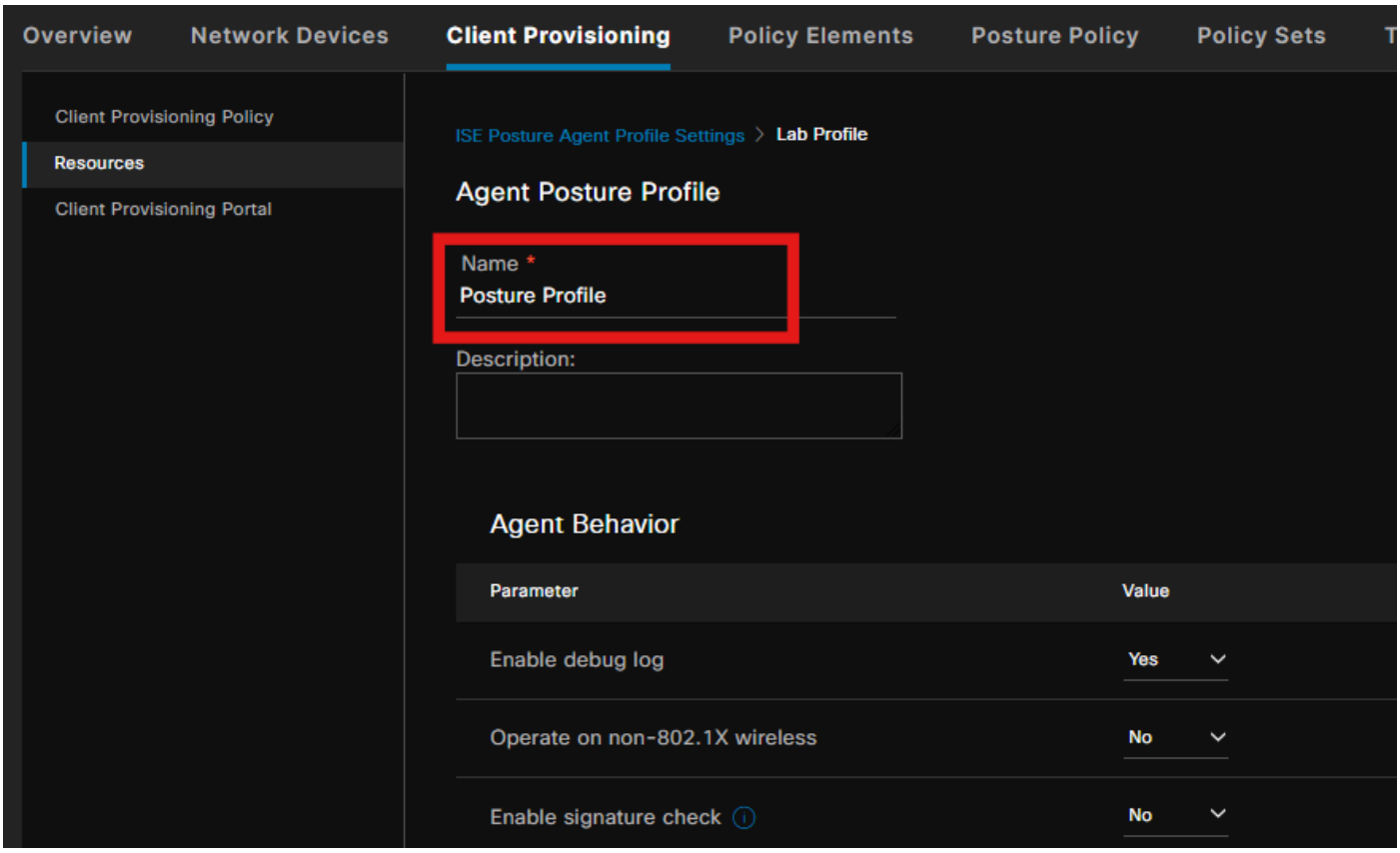
Schritt 3: NAM-Profil auf die ISE hochladen

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).



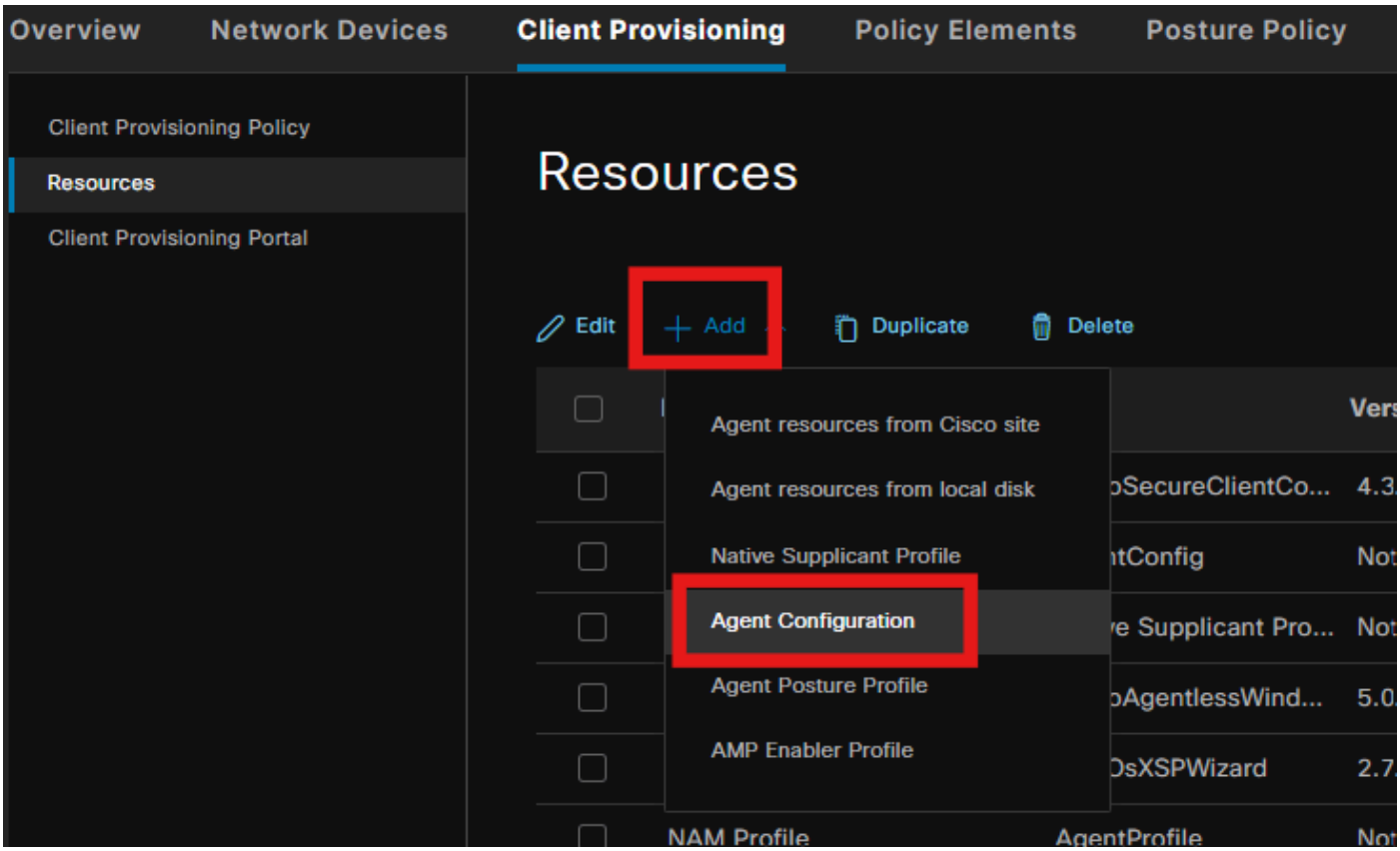
Schritt 4: Erstellen eines Statusprofils



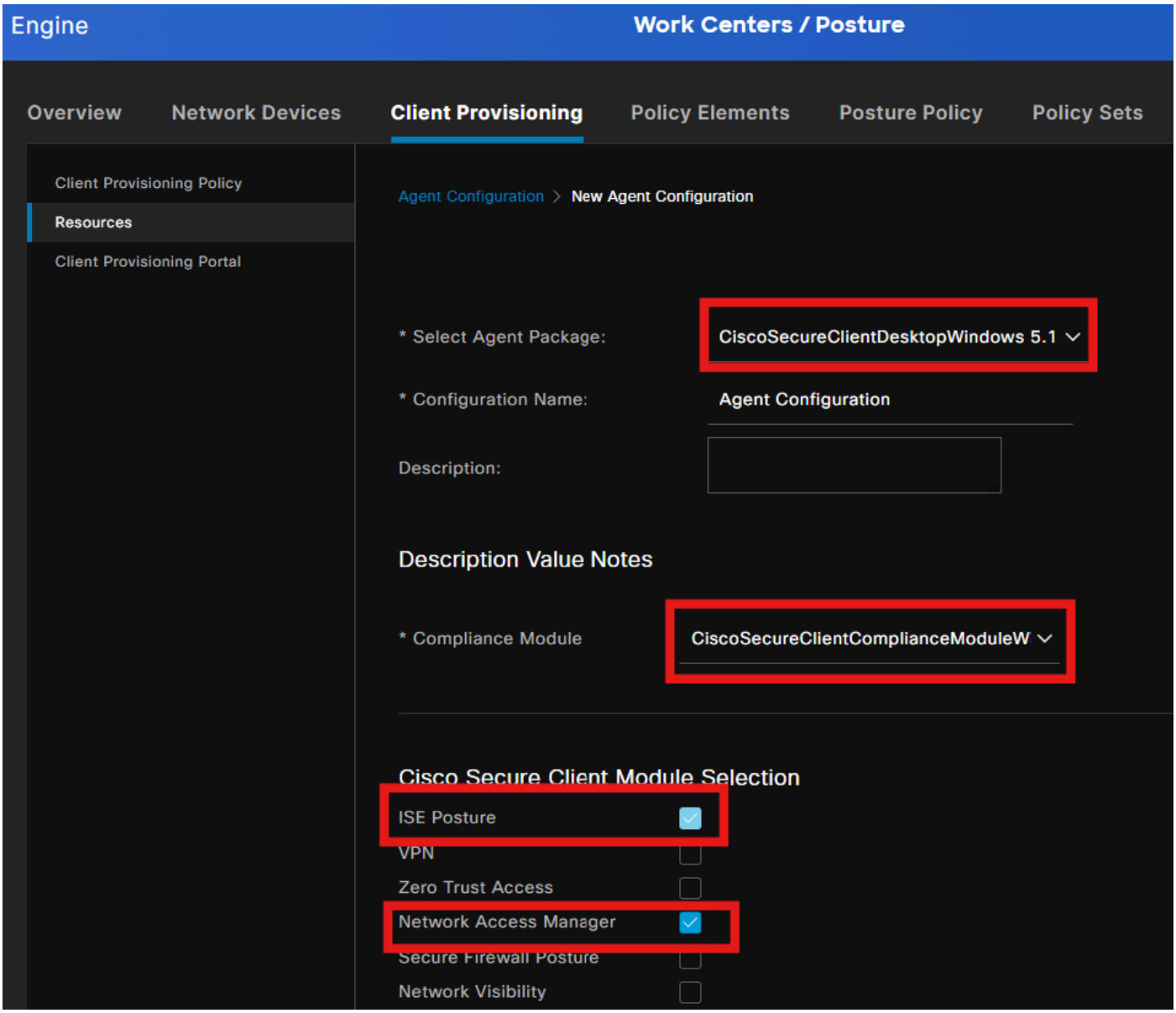


Vergessen Sie nicht, im Abschnitt "Posture Protocol" (Statusprotokoll) * hinzuzufügen, damit der Agent eine Verbindung zu allen Servern herstellen kann.

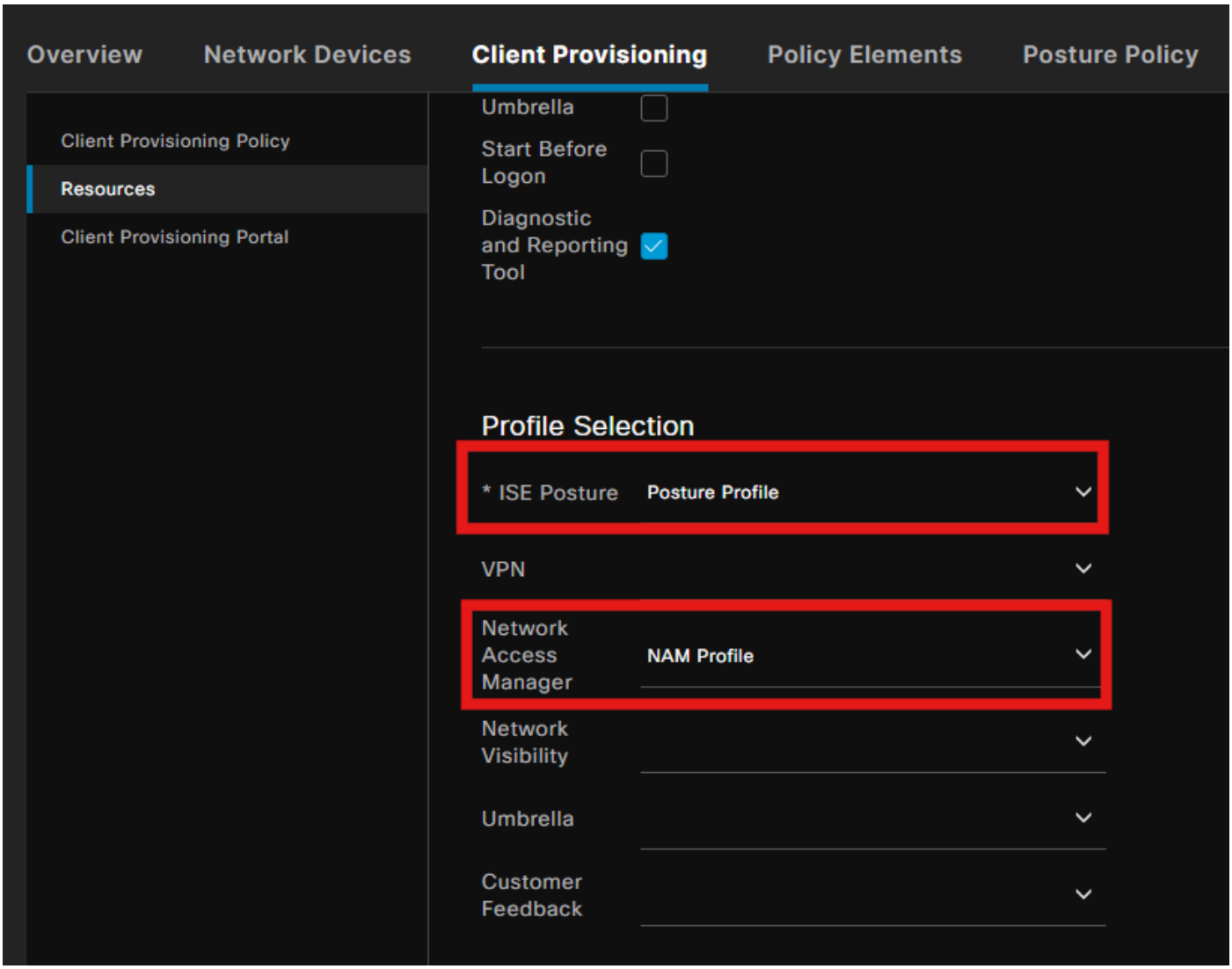
Schritt 5: Agent-Konfiguration erstellen



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

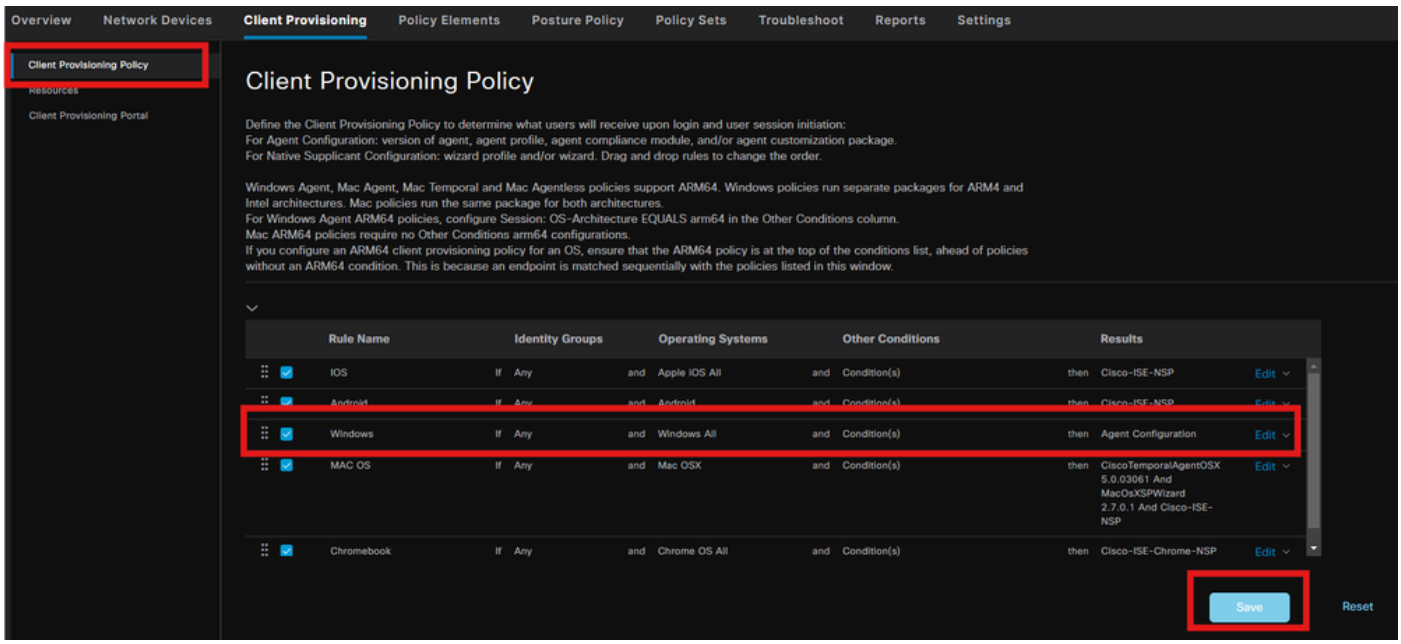


Wählen Sie unter "Profile" (Profil) die Option Posture (Status) und NAM Profile (NAM-Profil) aus, und klicken Sie auf Submit (Senden).



Schritt 6: Client-Bereitstellungsrichtlinie

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

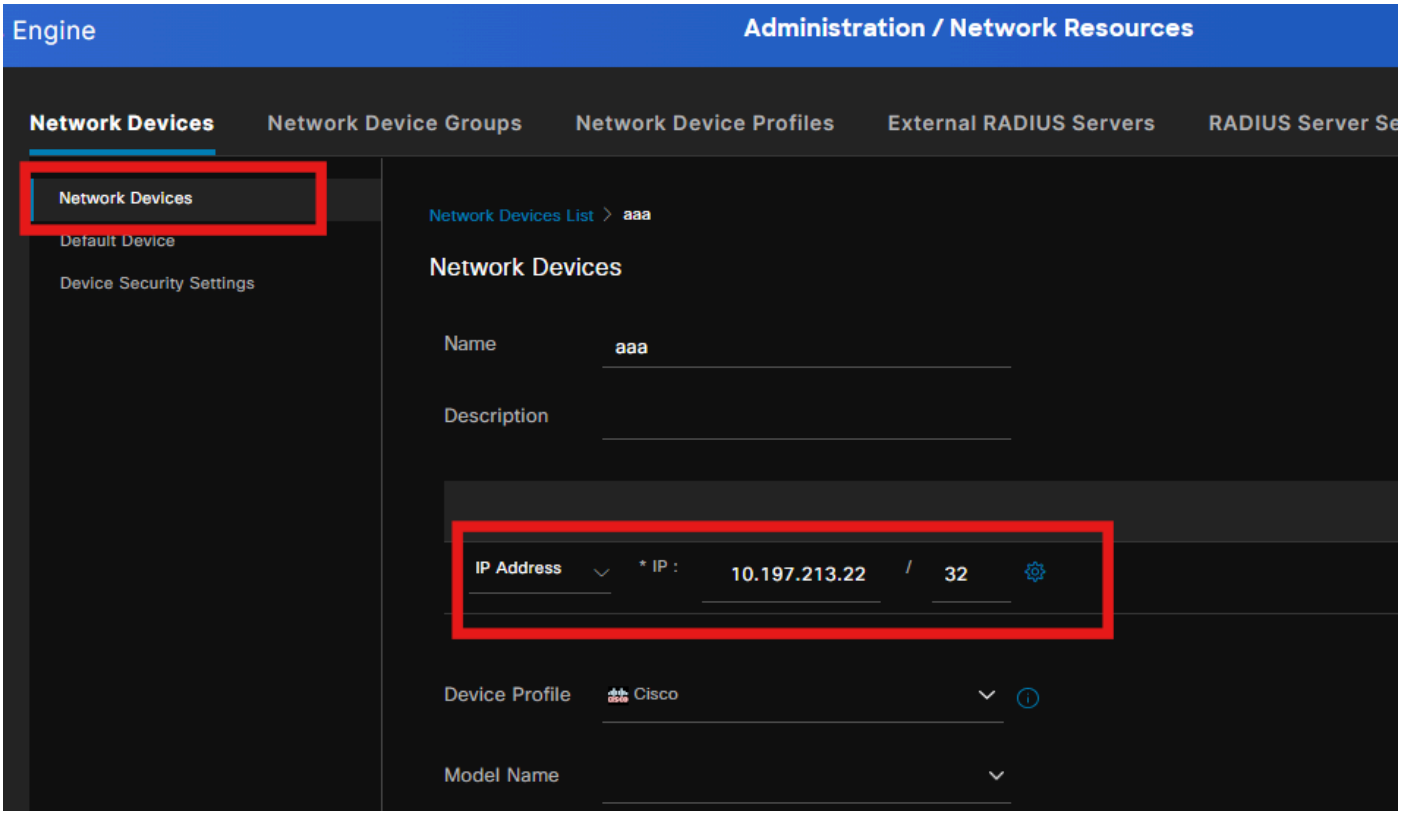


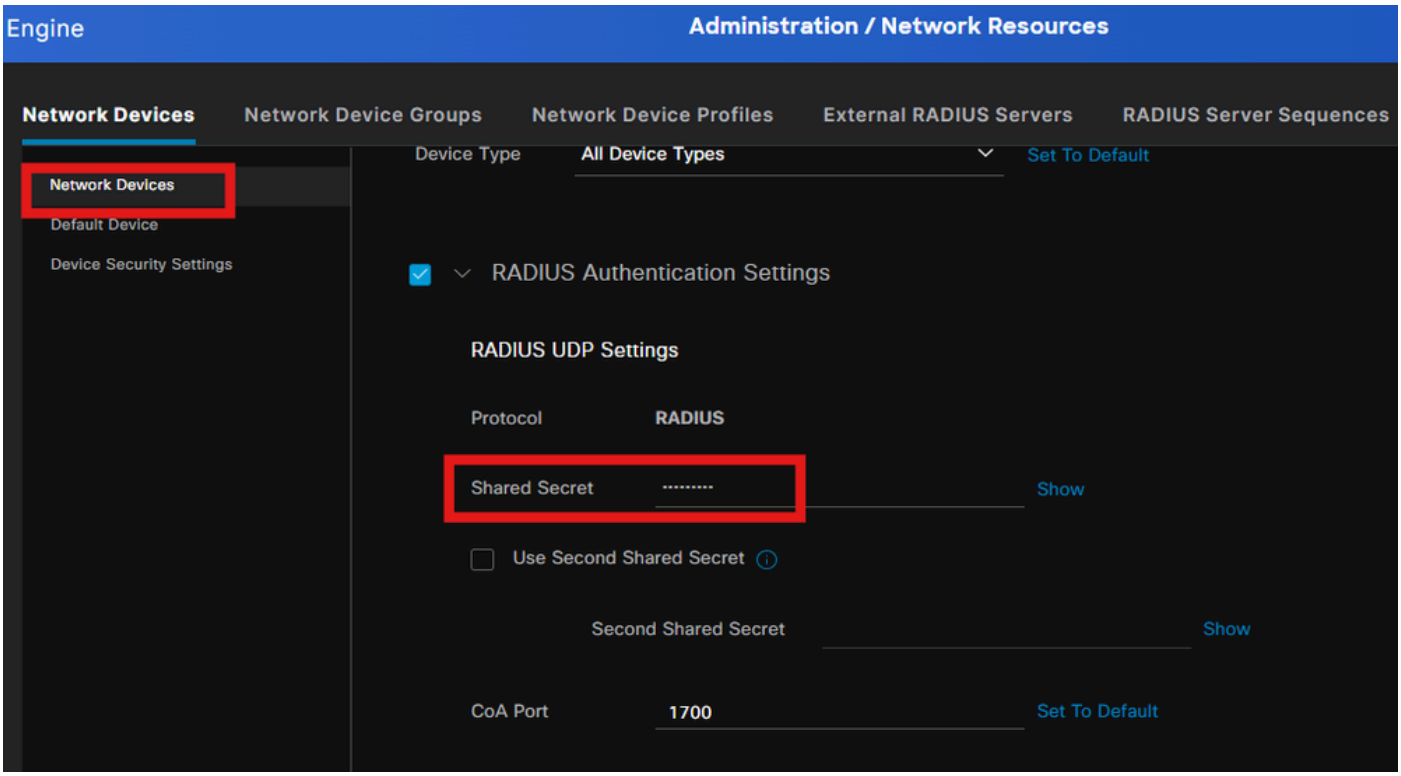
Schritt 7. Statusrichtlinie

Informationen zum Erstellen der Statusrichtlinie und der Bedingungen finden Sie in diesem ISE-Bereitstellungsleitfaden .

Schritt 8: Netzwerkgerät hinzufügen

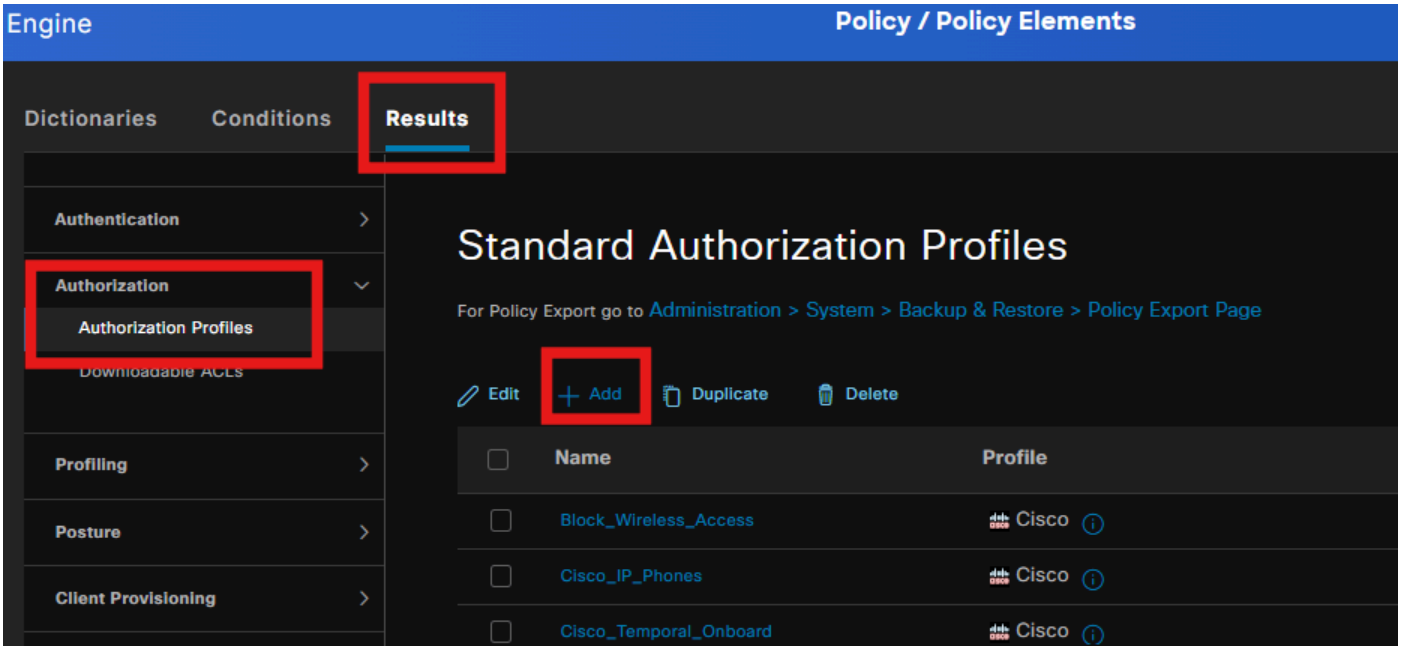
Um die IP-Adresse des Switches und den gemeinsamen geheimen Schlüssel für den Radius hinzuzufügen, navigieren Sie zu Administration > Network Resources (Administration > Netzwerkressourcen).



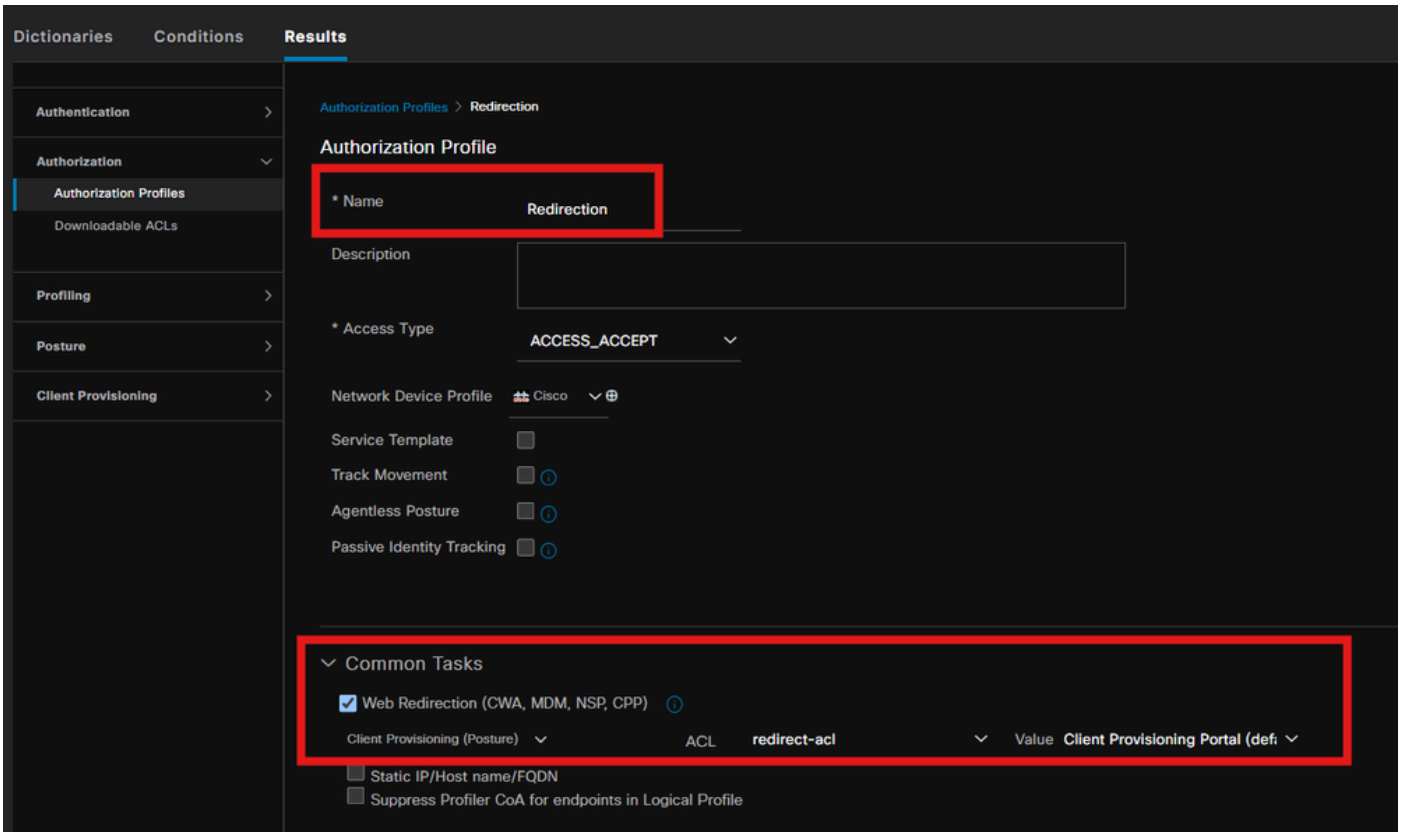


Schritt 9. Autorisierungsprofil

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

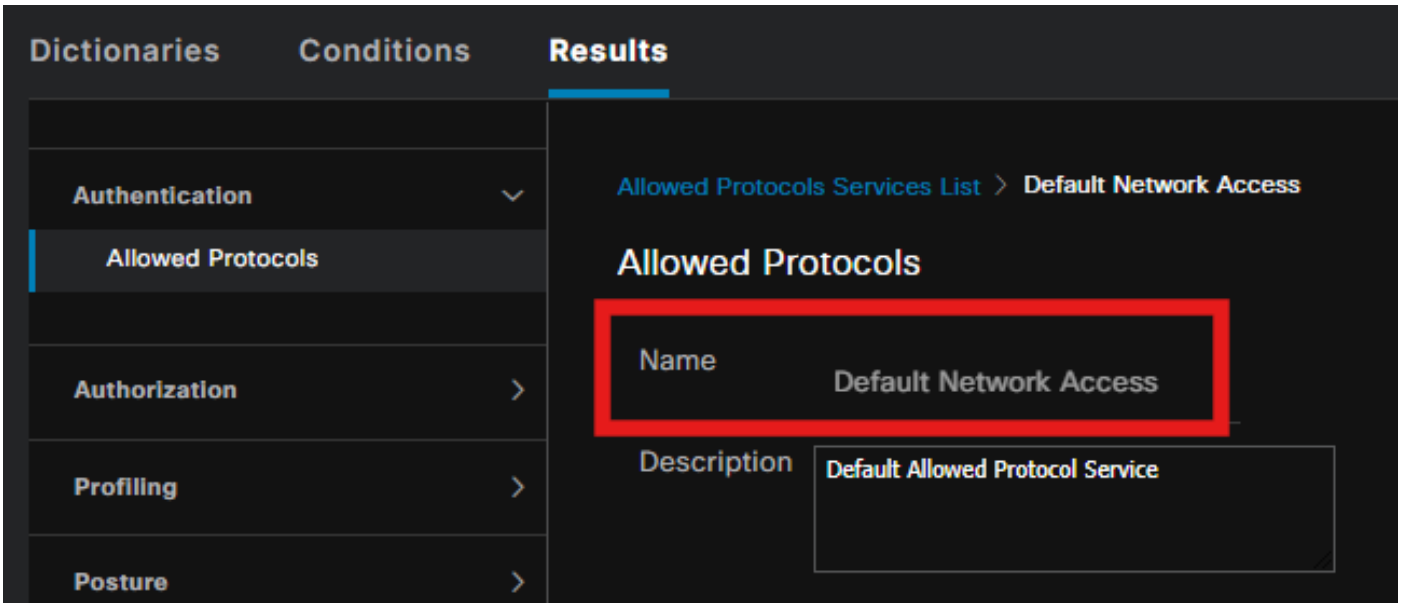


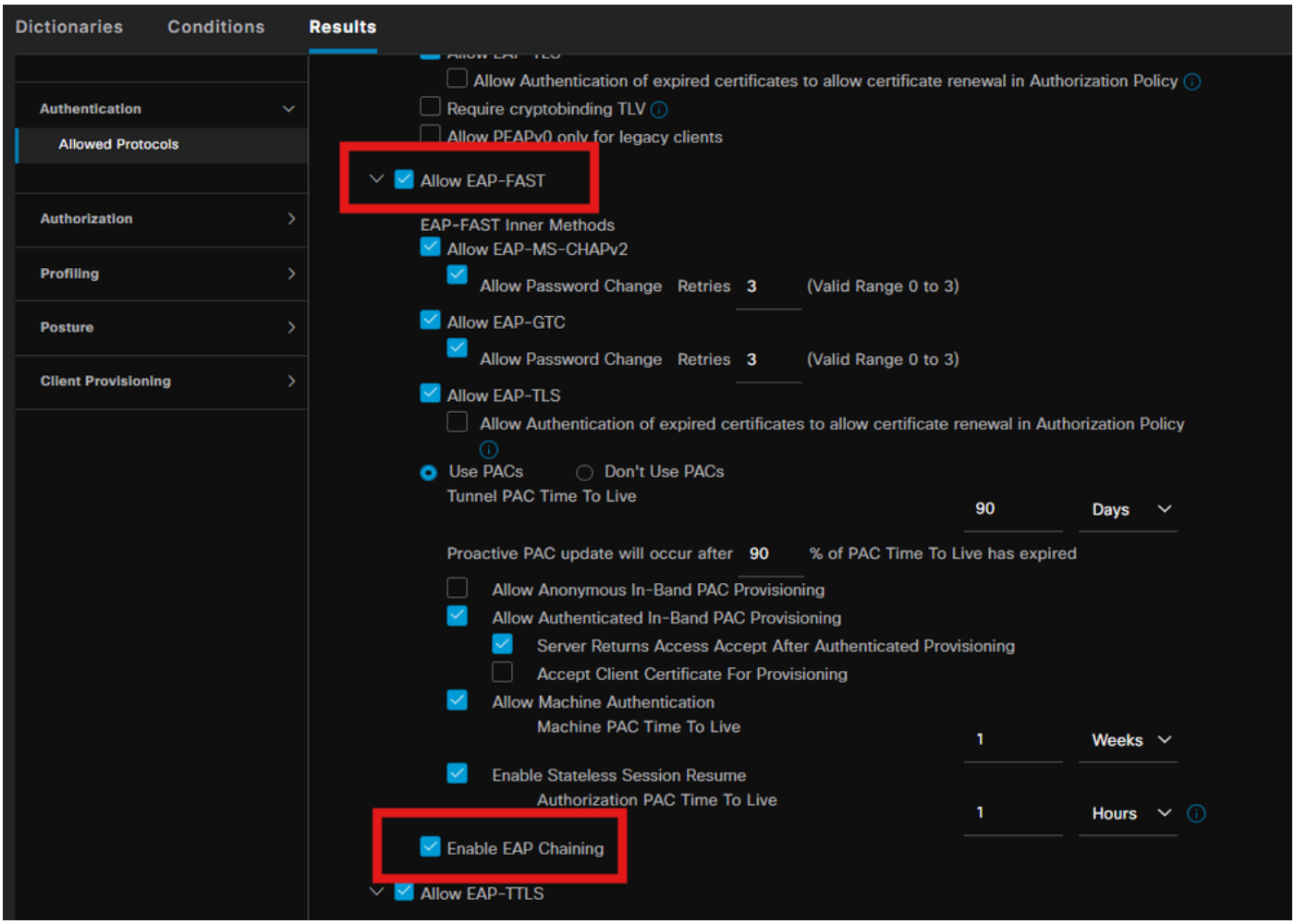
Wählen Sie unter Command Task das Client-Bereitstellungsportal mit Umleitungs-ACL aus.



Schritt 10. Zulässige Protokolle

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

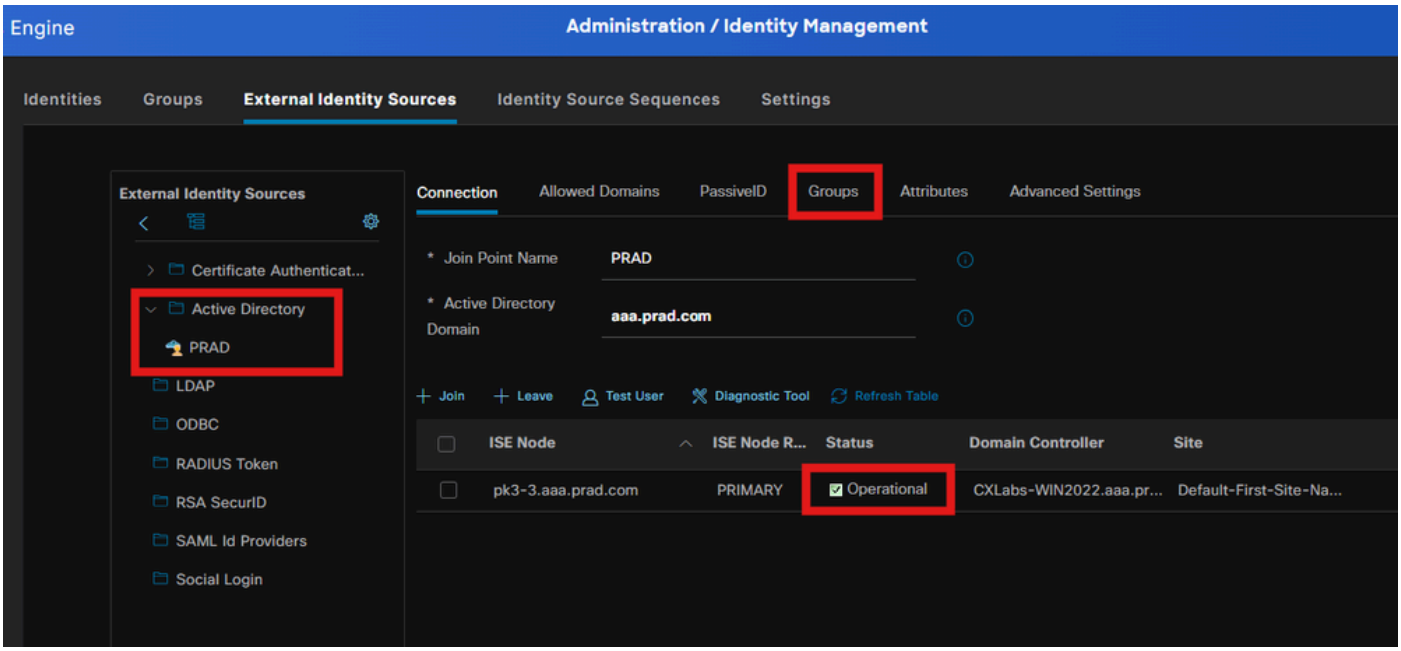




Schritt 11. Active Directory

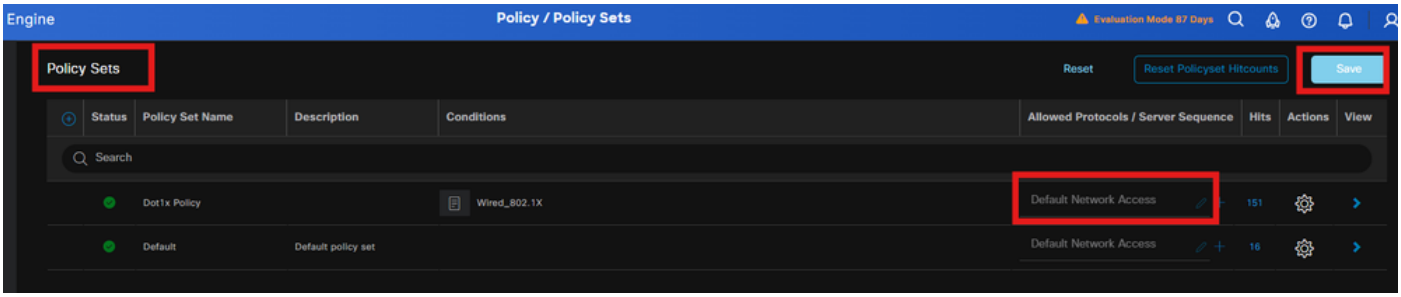
Überprüfen, ob ISE mit der Active Directory-Domäne verknüpft ist, und die Domänengruppen werden ausgewählt, wenn dies für die Autorisierungsbedingungen erforderlich ist.

Administration > Identity Management > External Identity Sources > Active Directory

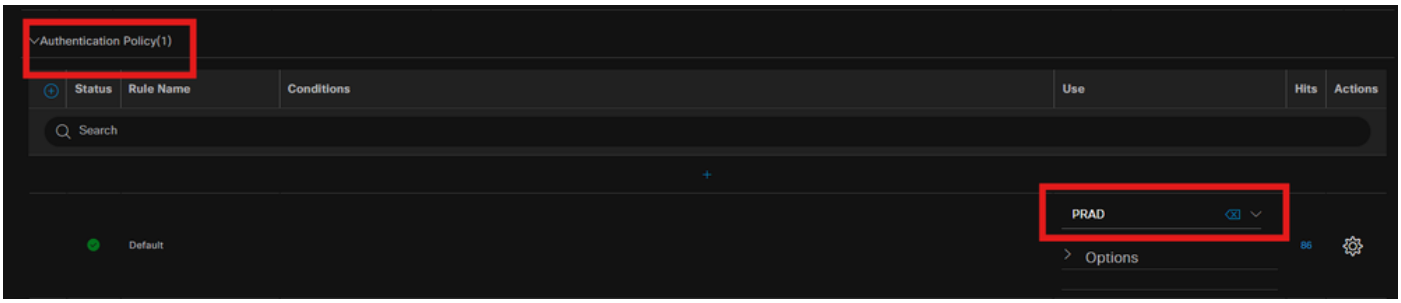


Schritt 12: Richtlinien

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



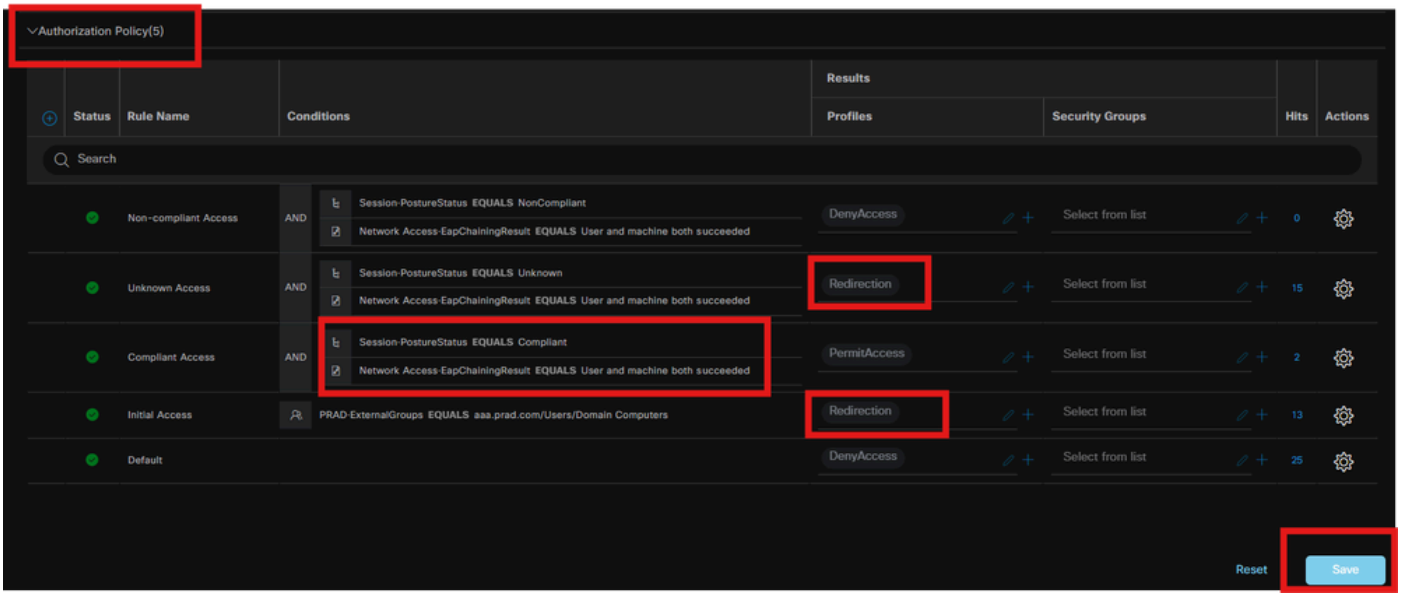
Wählen Sie das Active Directory als Identitätsquelle für die Authentifizierungsrichtlinie aus.



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

In diesem Anwendungsfall.

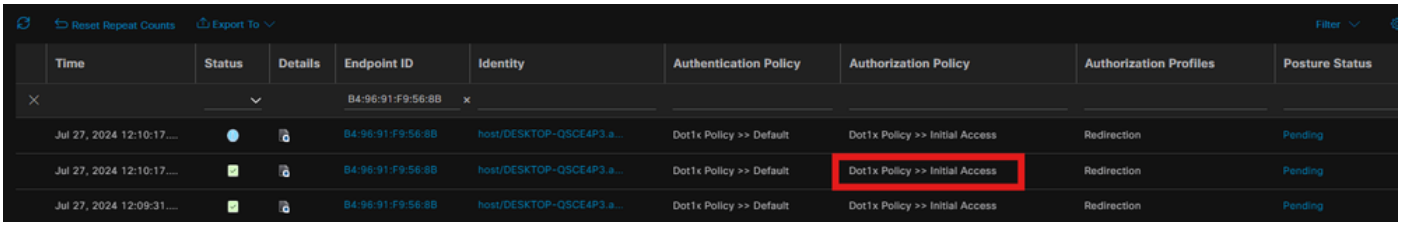
- Erstzugriff: Umleitung zum ISE Client Provisioning Portal zur Installation des Secure Client Agent und des NAM-Profils
- Unbekannter Zugriff: Zugriff auf das Client-Bereitstellungsportal zur umleitungsbasierten Statuserkennung
- Compliance-Zugriff: vollständiger Netzwerkzugriff
- Nicht konform: Zugriff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



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

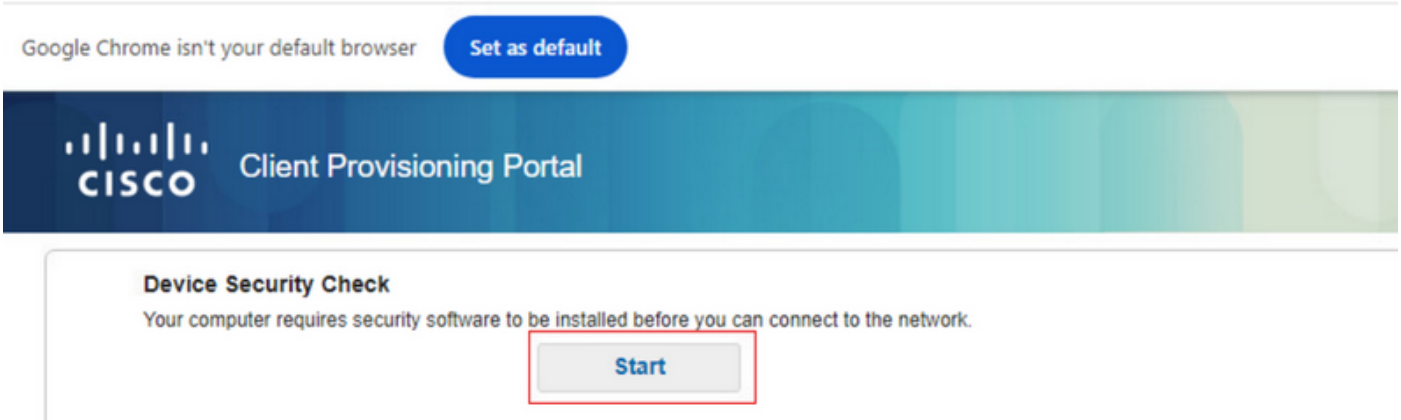
Serverrichtlinien:
URL-Umleitungszugriffskontrollliste: redirect-acl
URL-Umleitung:
https://ise33.aaa.prad.com:8443/portal/gateway?sessionId=16D5C50A0000002CF067366A&portal=ee39
7180-4995-8aa2-9fb282645a8f&action=cpp&token=518f857900a37f9afc6d2da8b6fe3bc2
ACS ACL: xACSACLx-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3

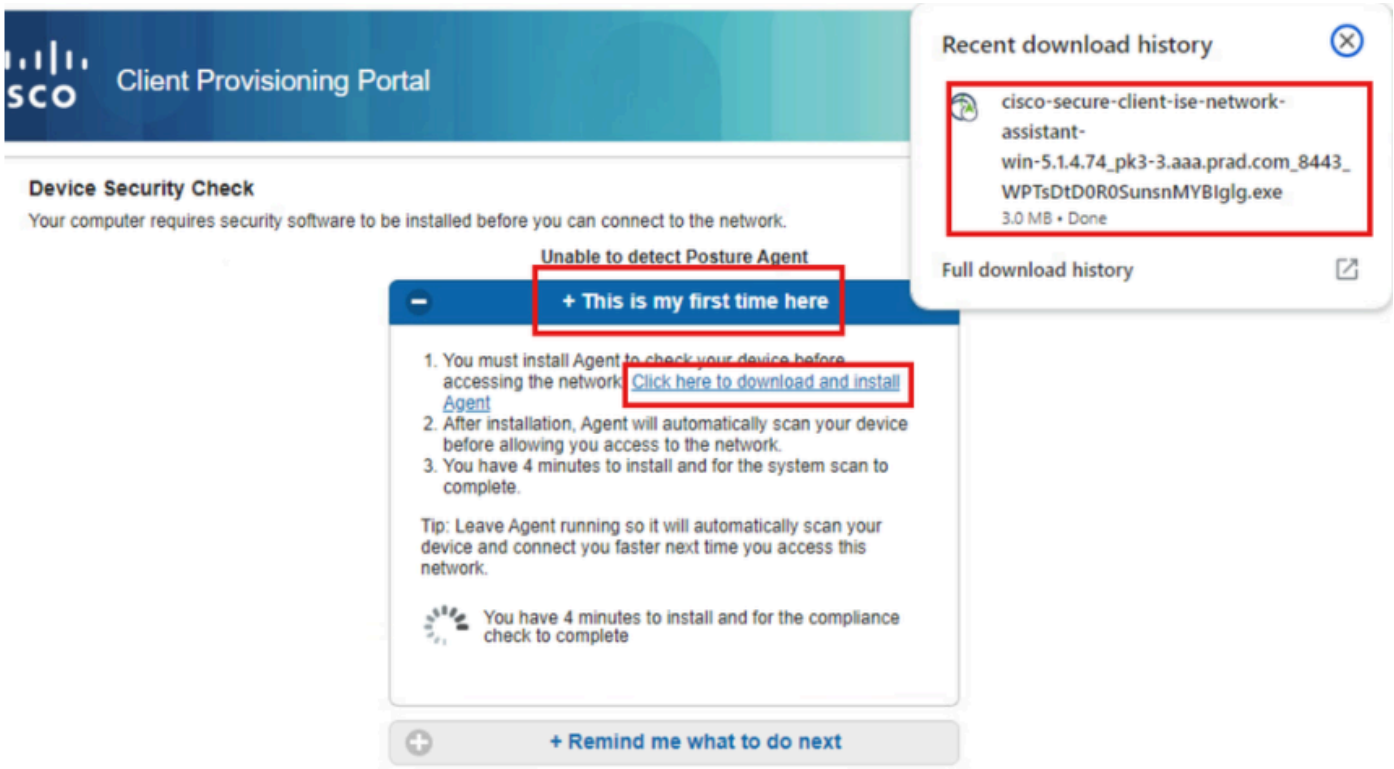
Methodenstatusliste:
Methodenstatus
dot1x Authentifizierung erfolgreich

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

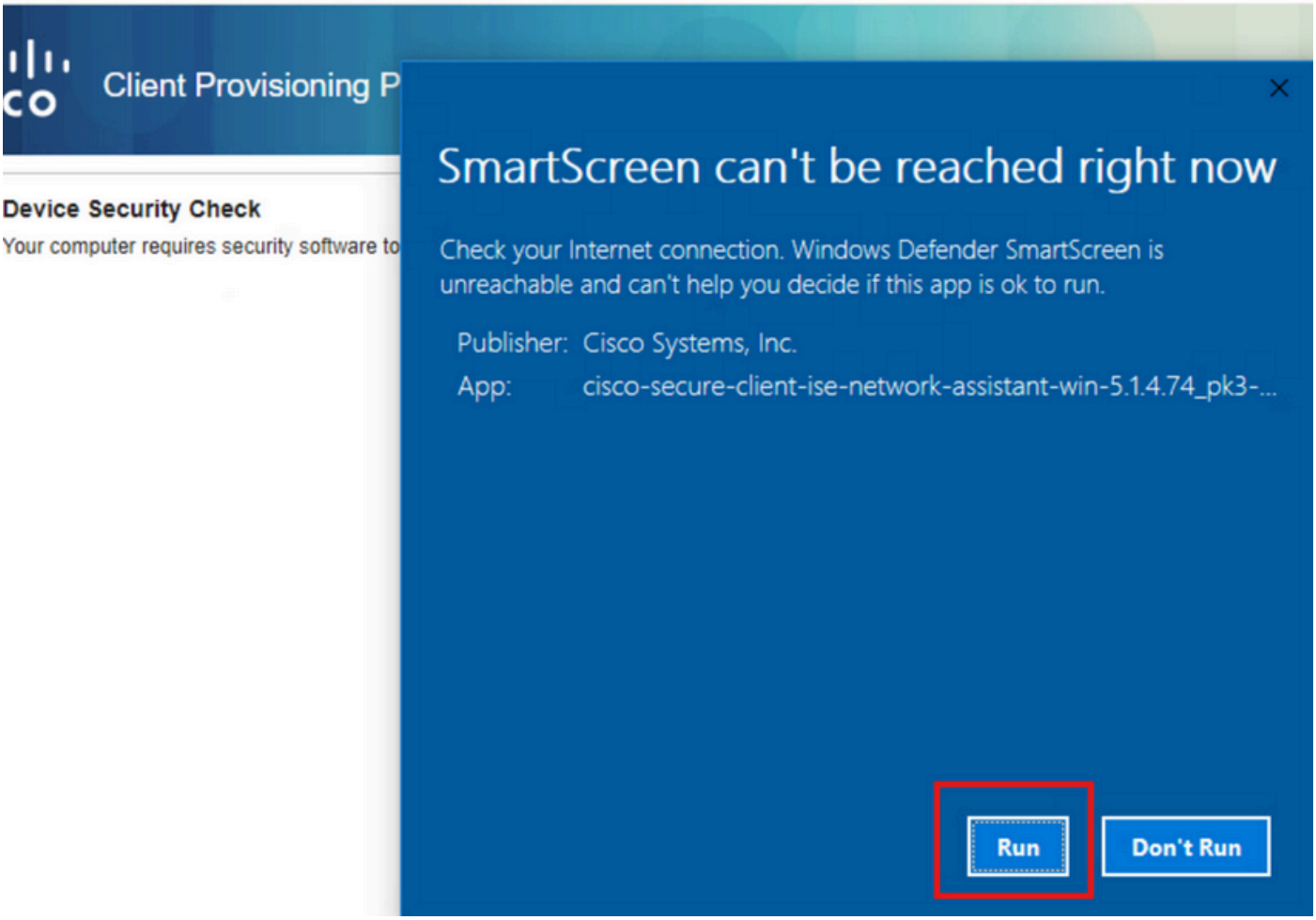
Network Layer Address Link Layer Address Interface vlan prlvl age state Restzeit
ARP X.X.X.X b496.91f9.568b Te1/0/24 1000 0005 4mn REACHABLE 39 s try 0

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.



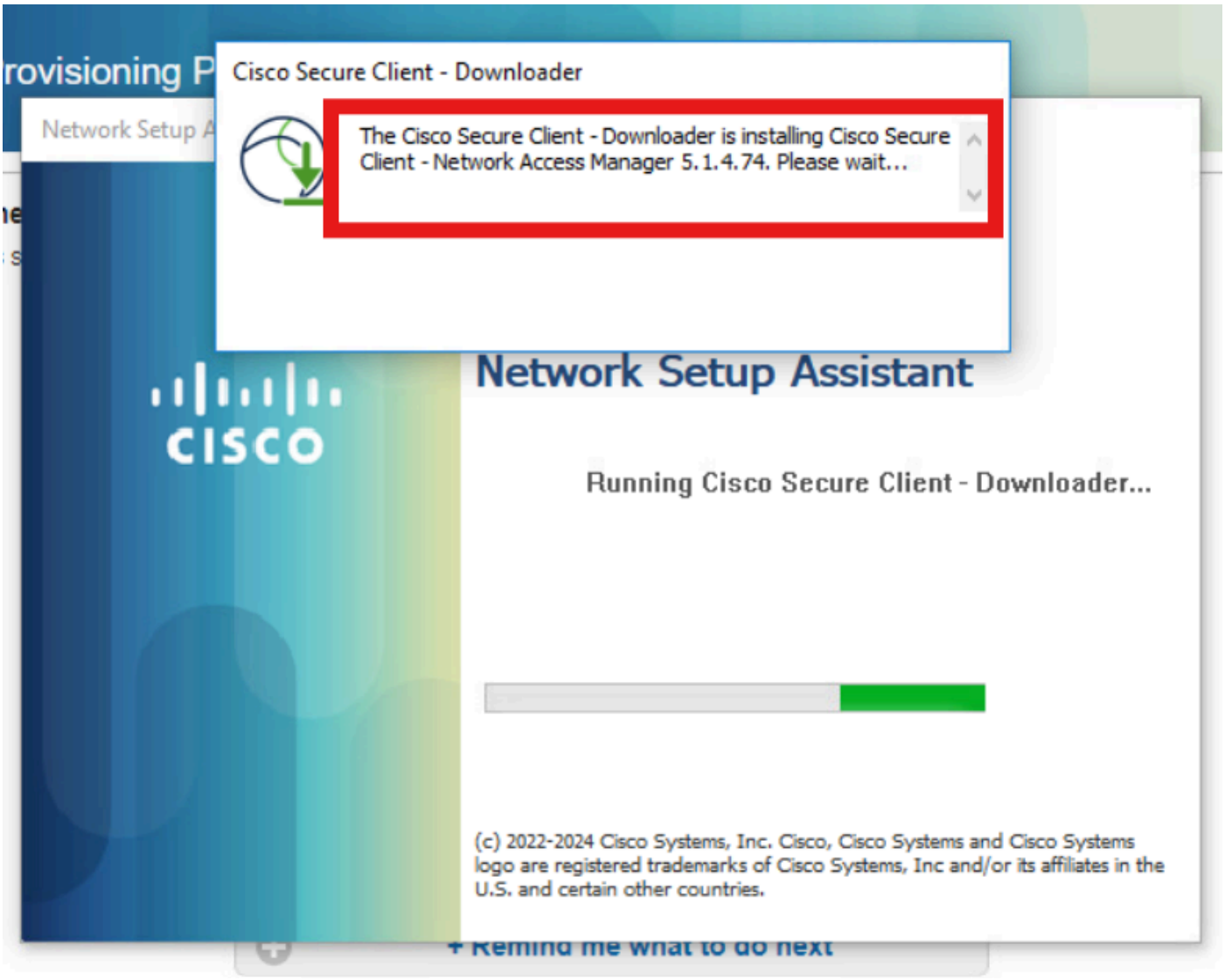


Klicken Sie auf Ausführen, um die NSA-Anwendung zu installieren.

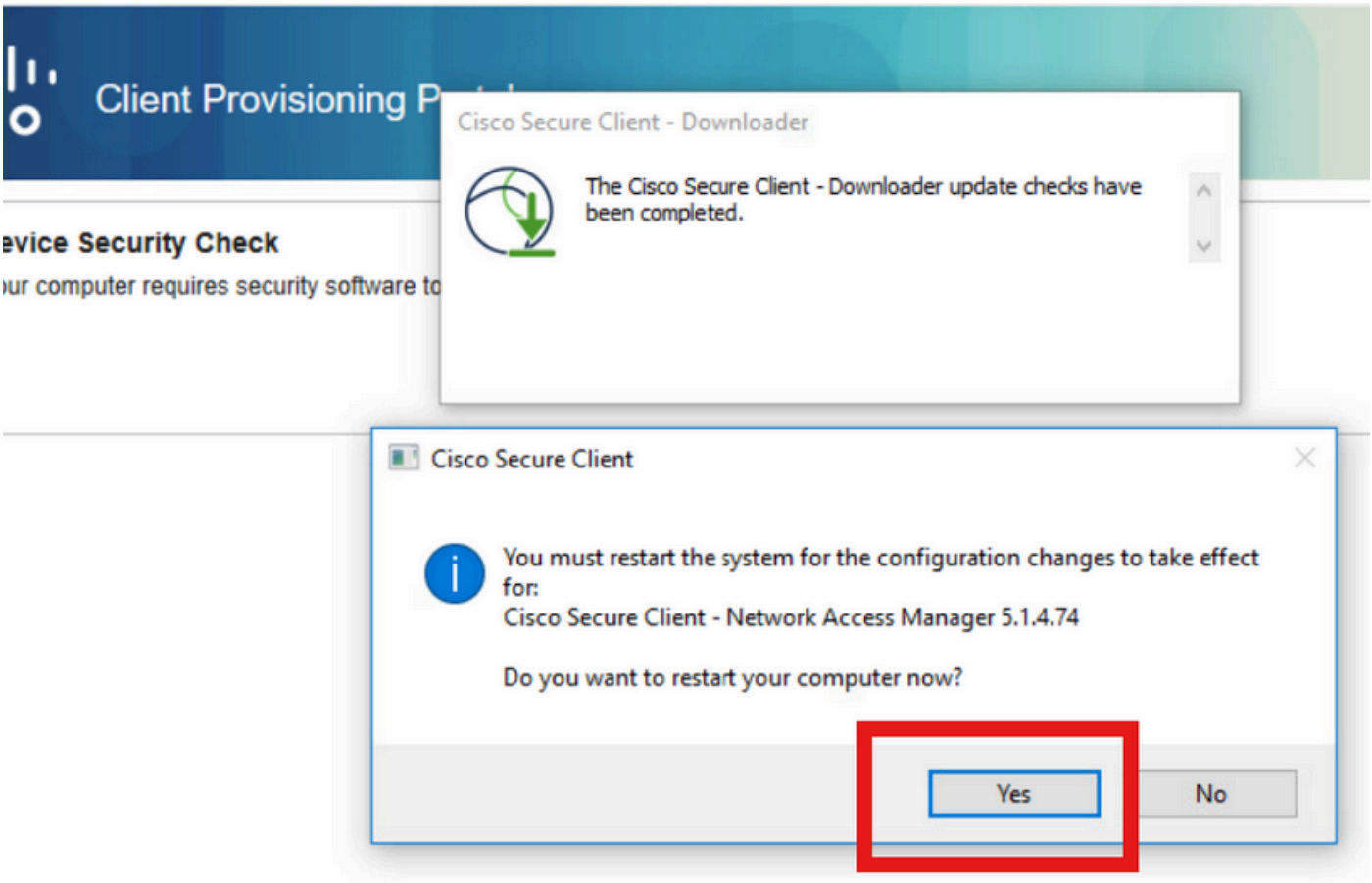


Jetzt ruft die NSA den Download des Secure Client Agent von der ISE auf und installiert das

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



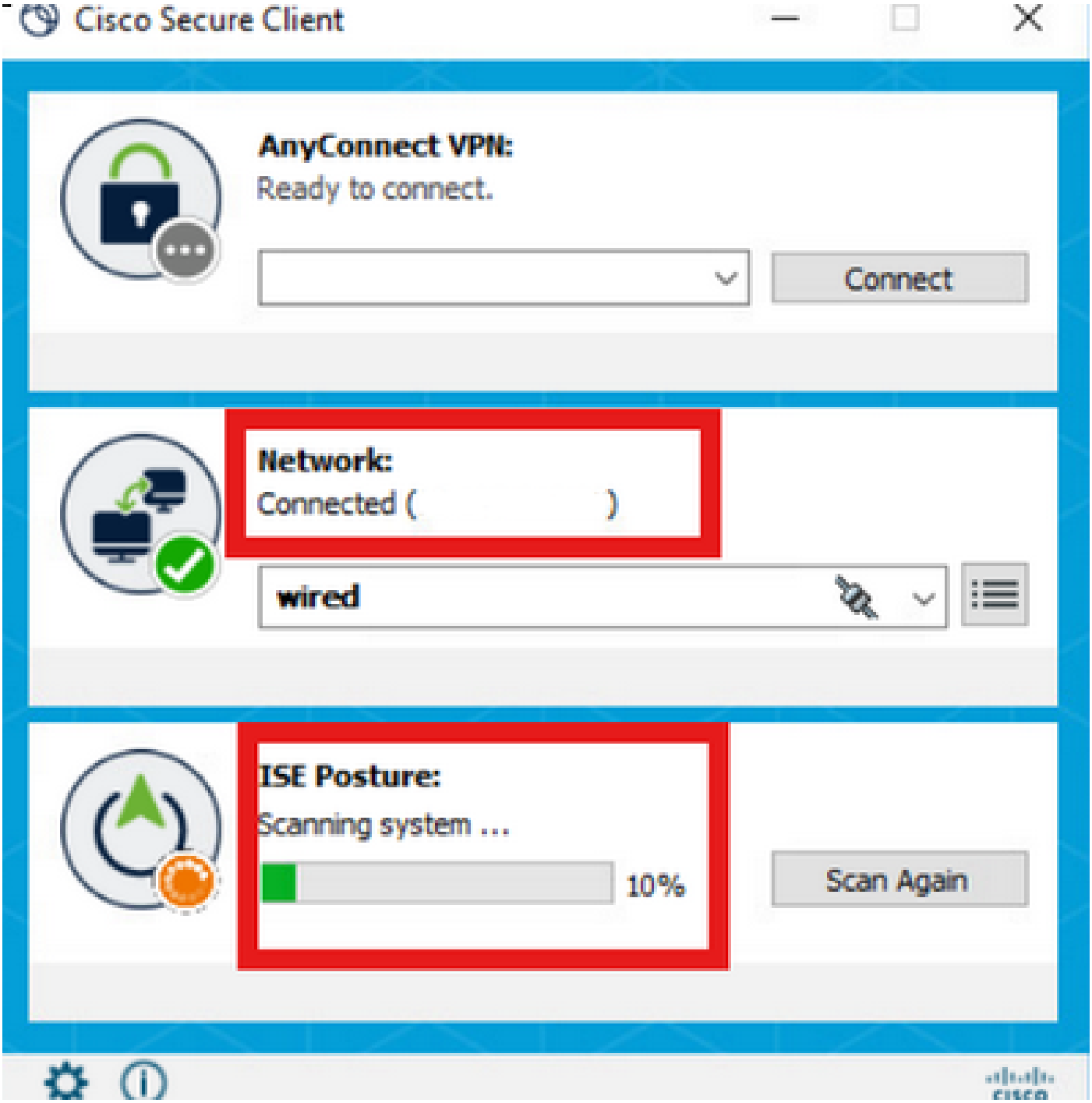
Nach der NAM-Installation wird eine Aufforderung zum Neustart ausgelöst. Klicken Sie auf Ja.



Schritt 2: EAP-FAST

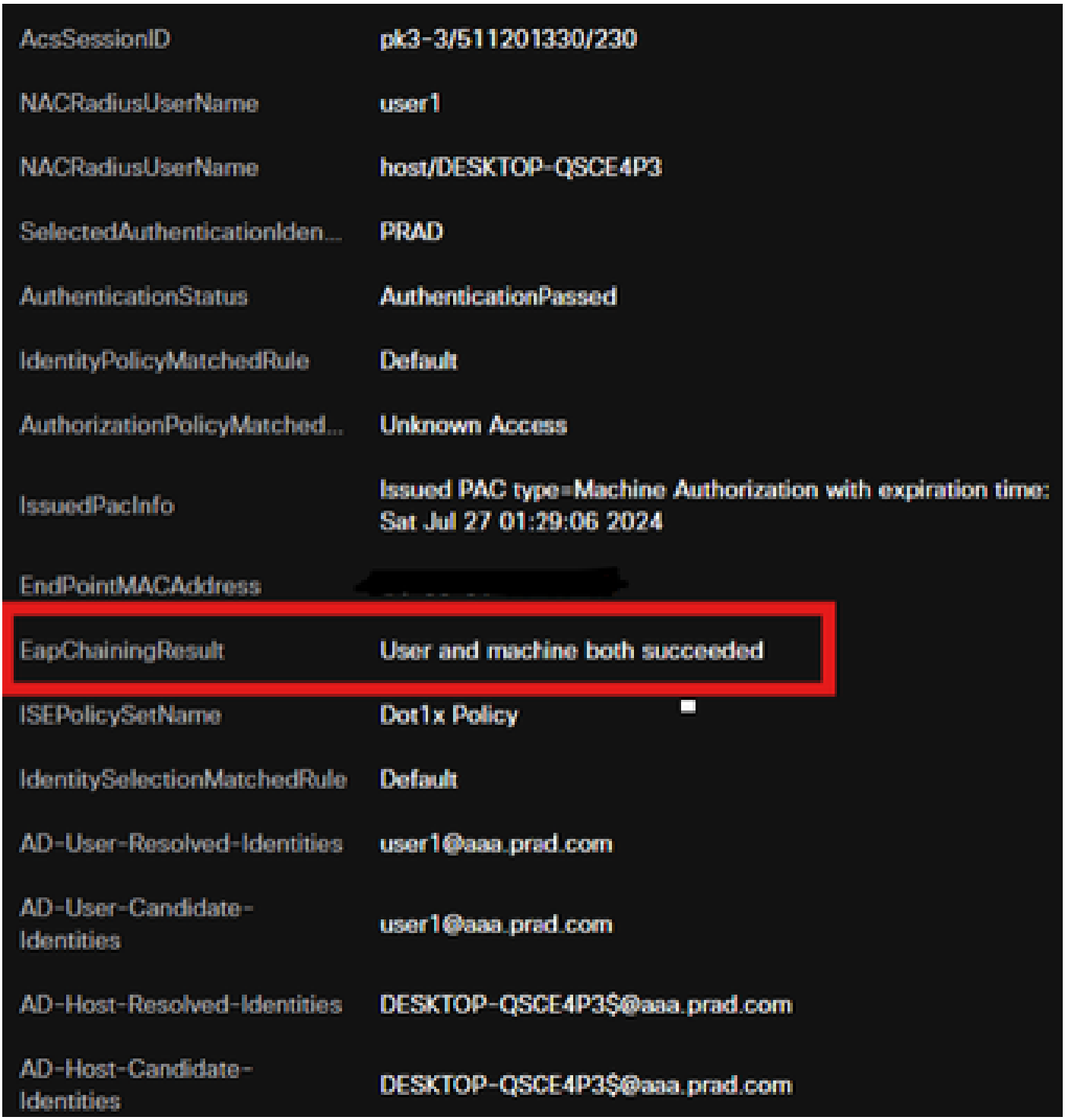
Nach dem Neustart des PCs und der Anmeldung des Benutzers authentifiziert das NAM Benutzer und Computer über EAP-FAST.

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



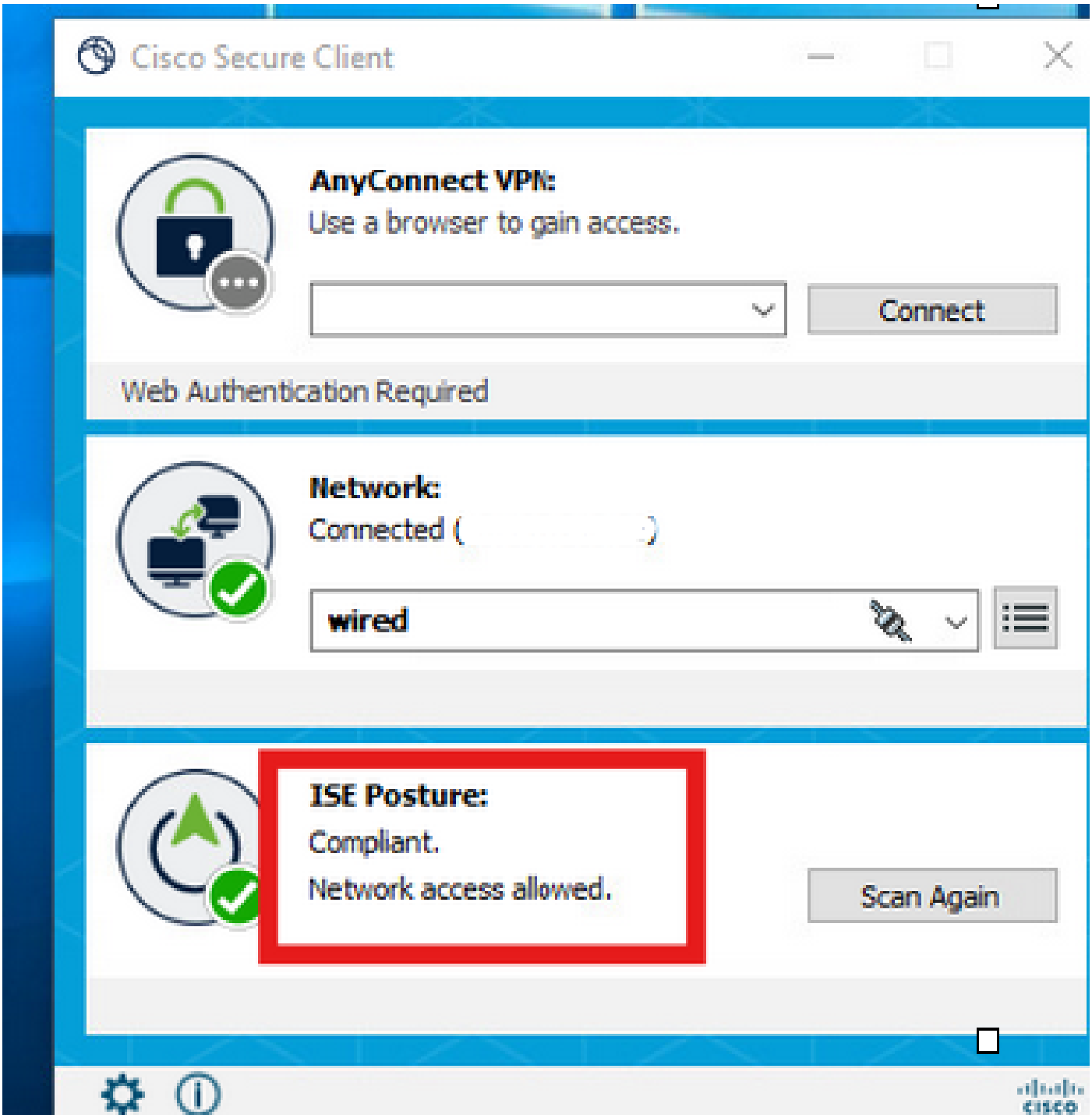
Bei ISE-Live-Protokollen gilt für den Endpunkt jetzt die Regel für unbekannten Zugriff.

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

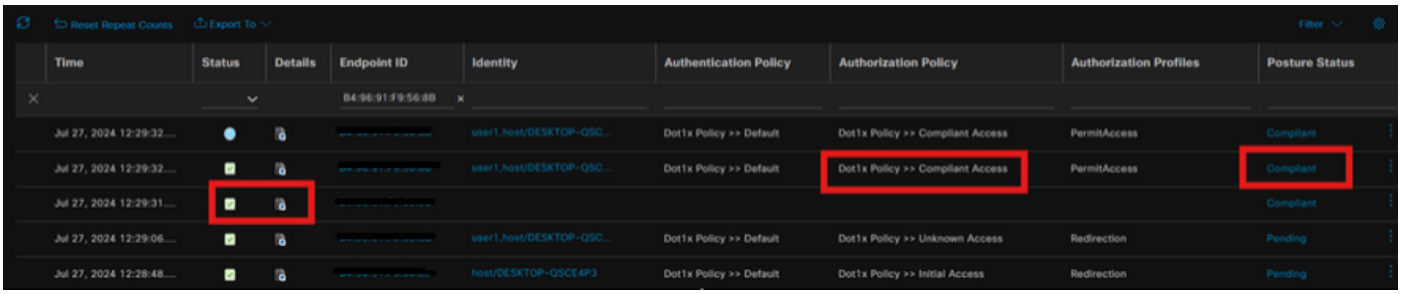


Schritt 3: Statusüberprüfung

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.

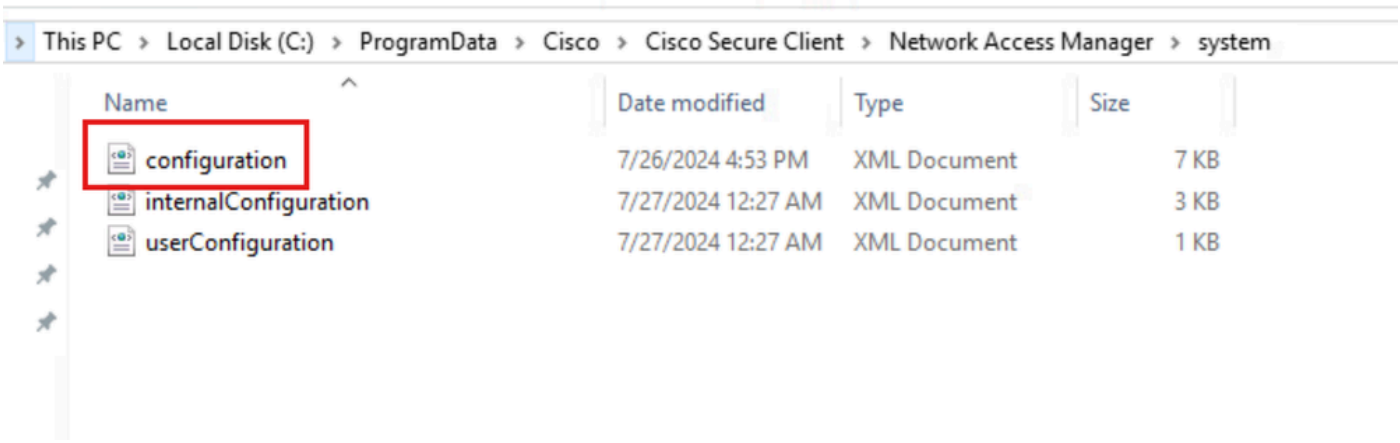


Fehlerbehebung

Schritt 1: NAM-Profil

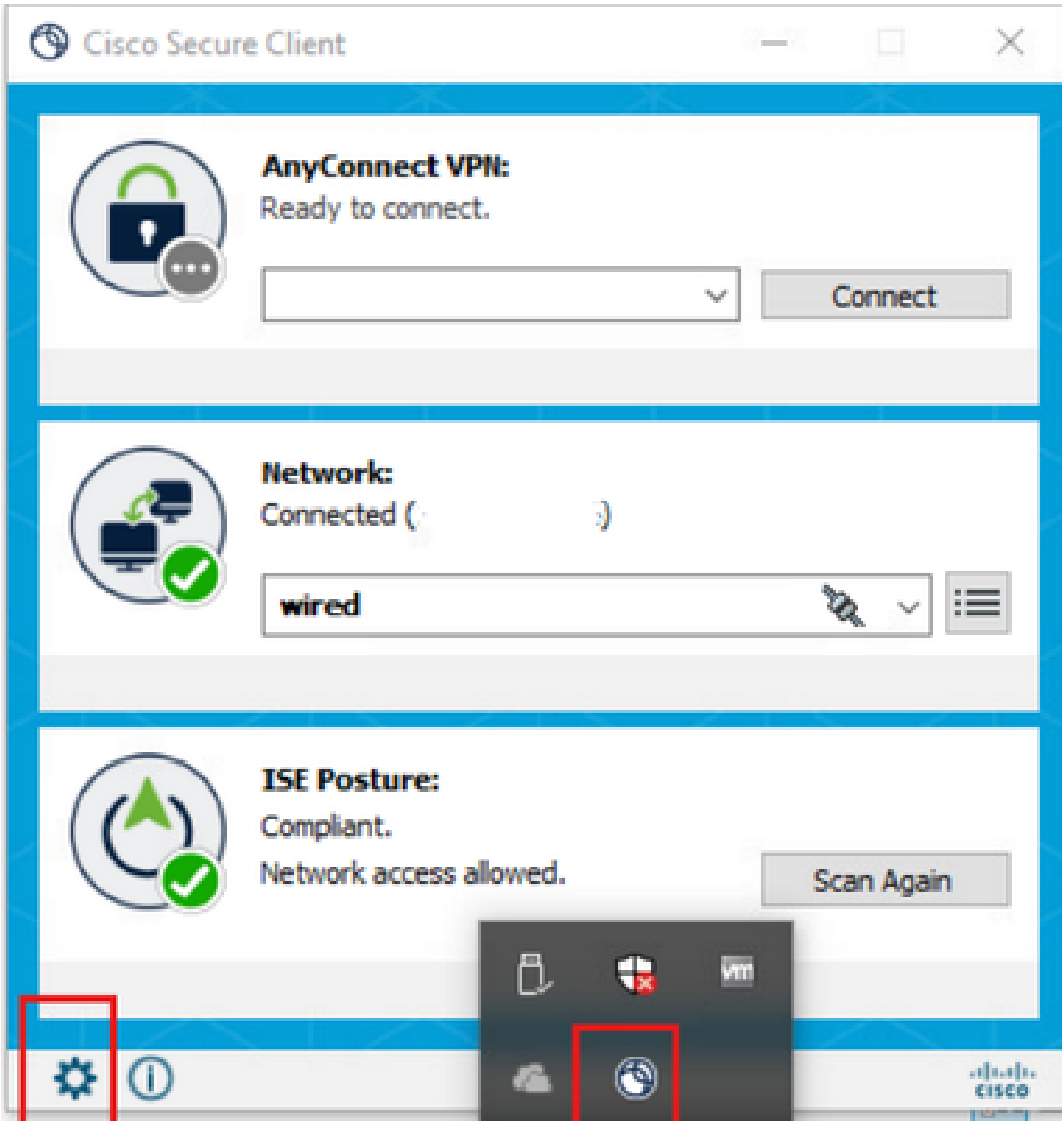
Vergewissern Sie sich, dass die Datei NAM Profile configuration.xml nach der Installation des NAM-Moduls in diesem Pfad auf dem PC vorhanden ist.

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



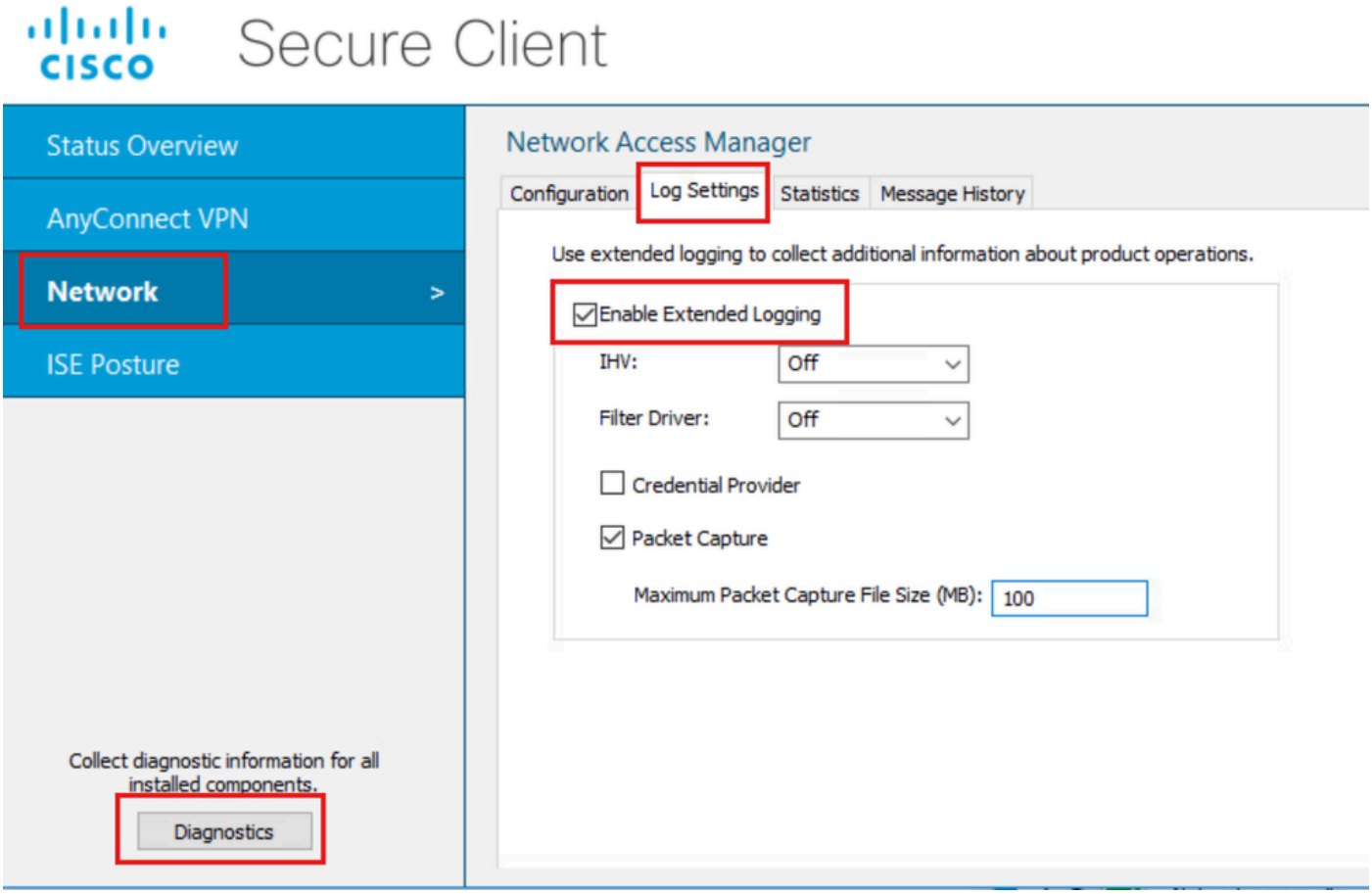
Schritt 2: Erweiterte NAM-Protokollierung

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.



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

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

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

set plattform 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.