Configurazione e distribuzione di Secure Client NAM Profile con ISE 3.3 su Windows

Sommario

Introduzione

In questo documento viene descritto come distribuire il profilo Cisco Secure Client Network Access Manager (NAM) tramite Identity Services Engine (ISE).

Premesse

L'autenticazione EAP-FAST si svolge in due fasi. Nella prima fase, EAP-FAST utilizza un handshake TLS per fornire e autenticare gli scambi di chiavi utilizzando oggetti TLV (Type-Length-Values) per stabilire un tunnel protetto. Questi oggetti TLV vengono utilizzati per trasmettere i dati relativi all'autenticazione tra il client e il server. Una volta stabilito il tunnel, la seconda fase inizia con il client e il nodo ISE impegnati in ulteriori conversazioni per stabilire i criteri di autenticazione e autorizzazione richiesti.

Il profilo di configurazione NAM è impostato per utilizzare EAP-FAST come metodo di autenticazione ed è disponibile per le reti definite dall'amministratore.
Inoltre, è possibile configurare sia il tipo di connessione utente che il tipo di connessione computer all'interno del profilo di configurazione NAM.
Il dispositivo Windows aziendale ottiene l'accesso aziendale completo utilizzando il controllo NAM con postura.
Il dispositivo Windows personale può accedere a una rete con restrizioni utilizzando la stessa configurazione NAM.

In questo documento vengono fornite istruzioni per la distribuzione del profilo Cisco Secure Client Network Access Manager (NAM) tramite il portale delle posture di Identity Services Engine (ISE) tramite la distribuzione Web, insieme al controllo di conformità delle posture.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Identity Services Engine (ISE)
- AnyConnect NAM ed Editor di profili
- Criteri di postura
- Configurazione Cisco Catalyst per servizi 802.1x

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

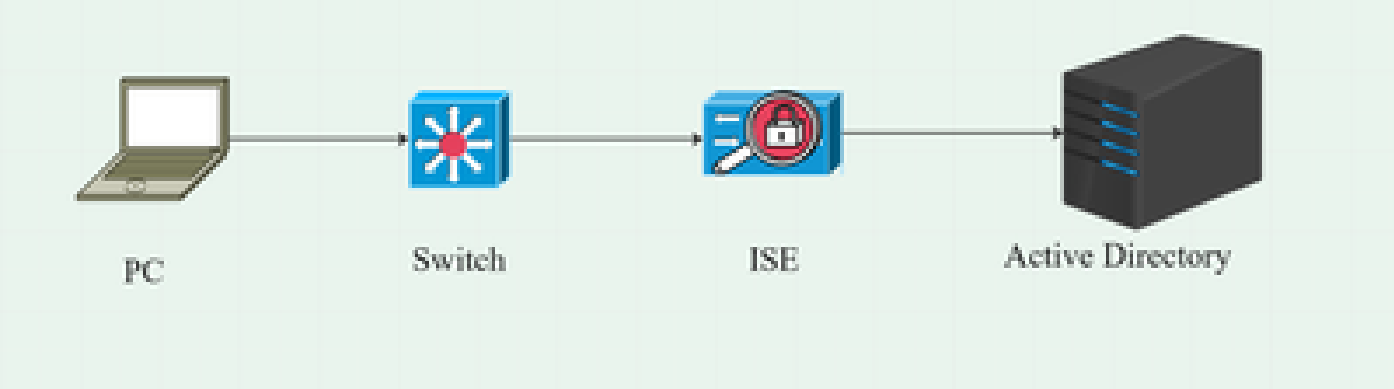
- Cisco ISE versione 3.3 e successive
- Windows 10 con Cisco Secure Mobility Client 5.1.4.74 e versioni successive
- Switch Cisco Catalyst 9200 con software Cisco IOS® XE 17.6.5 e versioni successive
- Active Directory 2016

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico

ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete



Flusso di dati

Quando un PC si connette alla rete, ISE fornisce la policy di autorizzazione per il reindirizzamento al portale delle posture.
Il traffico http sul PC viene reindirizzato alla pagina ISE Client Provisioning, dove l'applicazione NSA viene scaricata da ISE.
L'NSA installa quindi i moduli dell'agente Secure Client sul PC.
Al termine dell'installazione dell'agente, l'agente scarica il profilo Posture e il profilo NAM configurati su ISE.
L'installazione del modulo NAM attiva un riavvio del PC.
Dopo il riavvio, il modulo NAM esegue l'autenticazione EAP-FAST in base al profilo NAM.
La scansione della postura viene quindi attivata e la conformità viene verificata in base alla policy ISE Posture.

Configura switch

Configurare lo switch di accesso per l'autenticazione e il reindirizzamento dot1x.

```
aaa new-model

raggio gruppo predefinito dot1x autenticazione aaa
raggio gruppo predefinito rete di autorizzazione aaa
raggio predefinito del gruppo start-stop aaa accounting dot1x
autore dinamico radius server aaa
client 10.127.197.53 chiave server Qwerty123
auth-type any
```

```
id sessione aaa comune
ip radius source-interface Vlan1000
attributo radius-server 6 on-for-login-auth
radius-server attributo 8 include-in-access-req
attributo radius-server 25 access-request include
attributo radius-server 31 mac format ietf maiuscolo
server RADIUS RAD1
address ipv4 <ISE server IP> auth-port 1812 acct-port 1813
key <chiave segreta>

dot1x system-auth-control
```

Configurare l'ACL di reindirizzamento per il reindirizzamento dell'utente al portale di provisioning del client ISE.

```
acl di reindirizzamento esteso ip access-list
10 nega udp a qualsiasi dominio eq
20 deny tcp any eq domain
30 deny udp any eq bootpc any eq bootps
40 deny ip any host <IP server ISE>
50 Permetti tcp any eq www
60 permettere tcp qualsiasi eq 443
```

Abilitare il rilevamento dei dispositivi e il reindirizzamento http sullo switch.

```
criteri di rilevamento dispositivi <nome criteri di rilevamento dispositivi>
 attivazione tracciamento
interface <nome interfaccia>
 device-tracking attach-policy <nome criterio di rilevamento dispositivi>

server http ip
ip http secure-server
```

Scarica il pacchetto client sicuro

Scaricare l'Editor di profili, le finestre Secure Client e i file Web Compliance Module manualmente da software.cisco.com

Nella barra di ricerca del nome del prodotto, digitare Secure Client 5.

Download Home > Sicurezza > Sicurezza degli endpoint > Secure Client (incluso AnyConnect) > Secure Client 5 > Software Client VPN AnyConnect

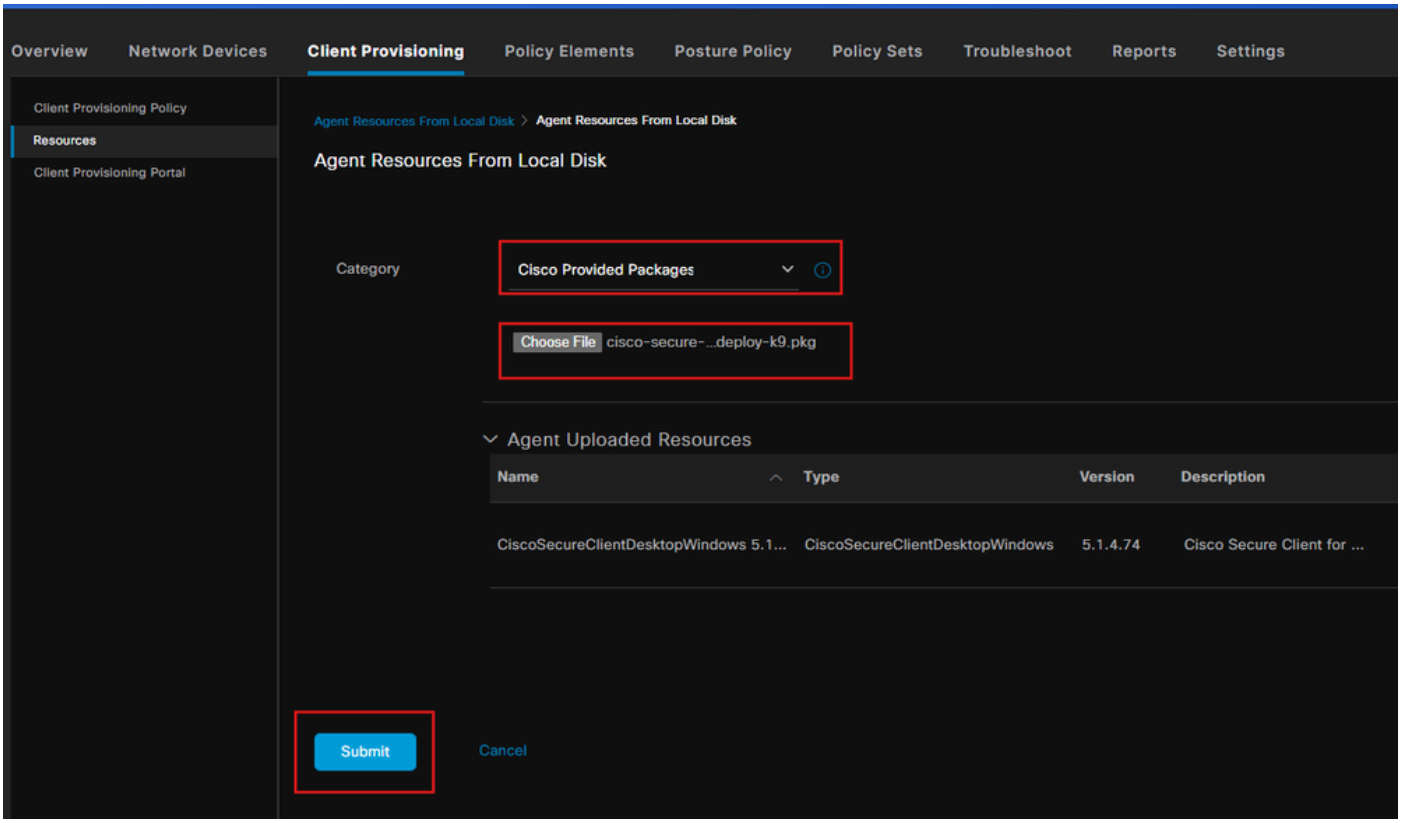
- cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg

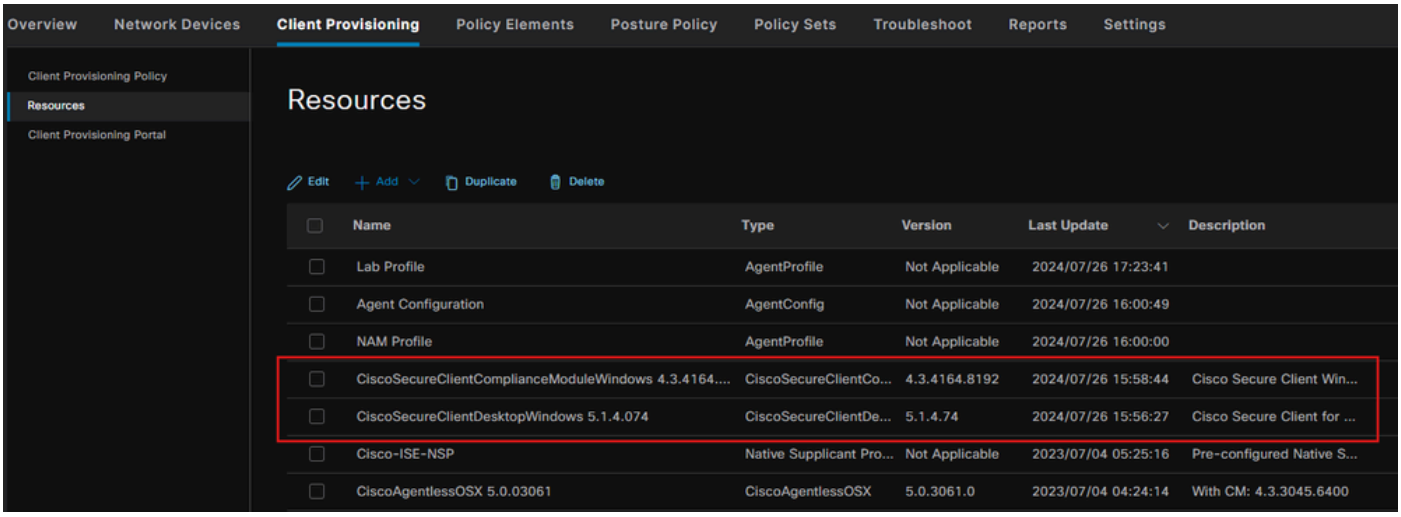
- cisco-secure-client-win-4.3.4164.8192-isecompliance-webdeploy-k9.pkg
- tools-cisco-secure-client-win-5.1.4.74-profileeditor-k9.msi

Configurazione di ISE

Passaggio 1. Carica il pacchetto su ISE

Per caricare i pacchetti Web Secure Client and Compliance Module su ISE, selezionare Workcenter > Postura > Client Provisioning > Risorse > Aggiungi > Risorse agente dal disco locale.



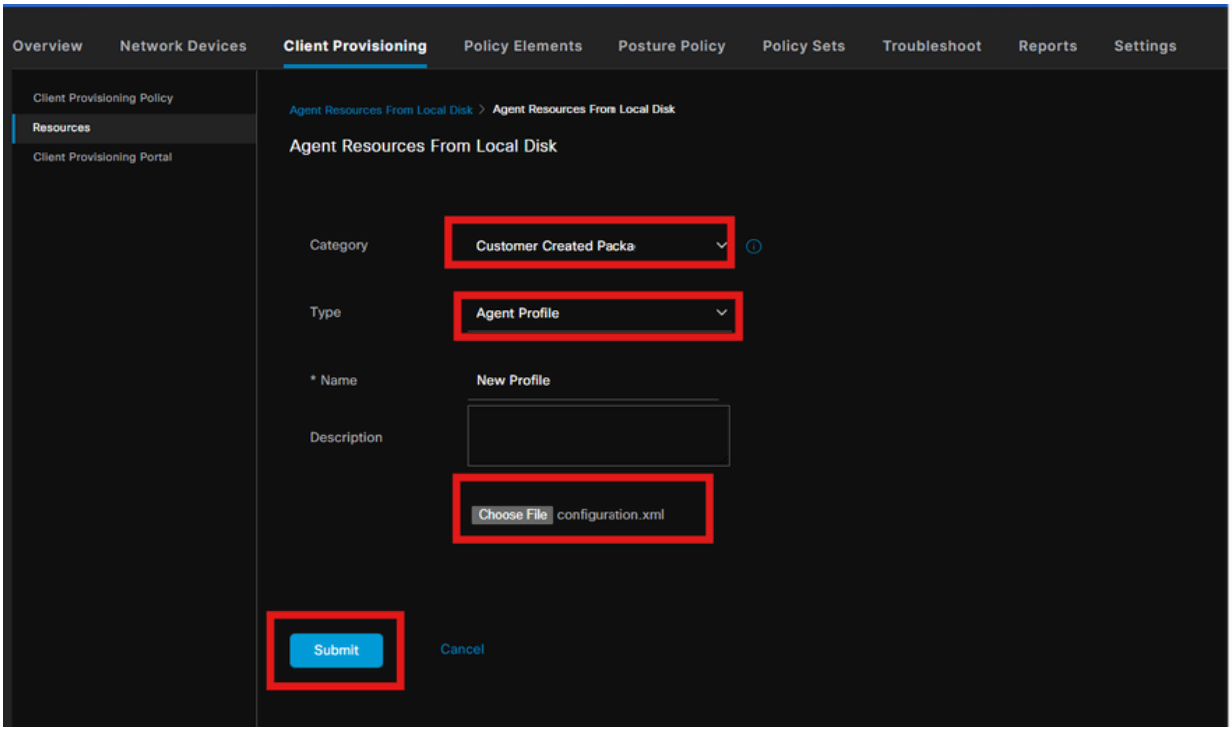


Passaggio 2. Creazione di un profilo NAM dall'editor profili

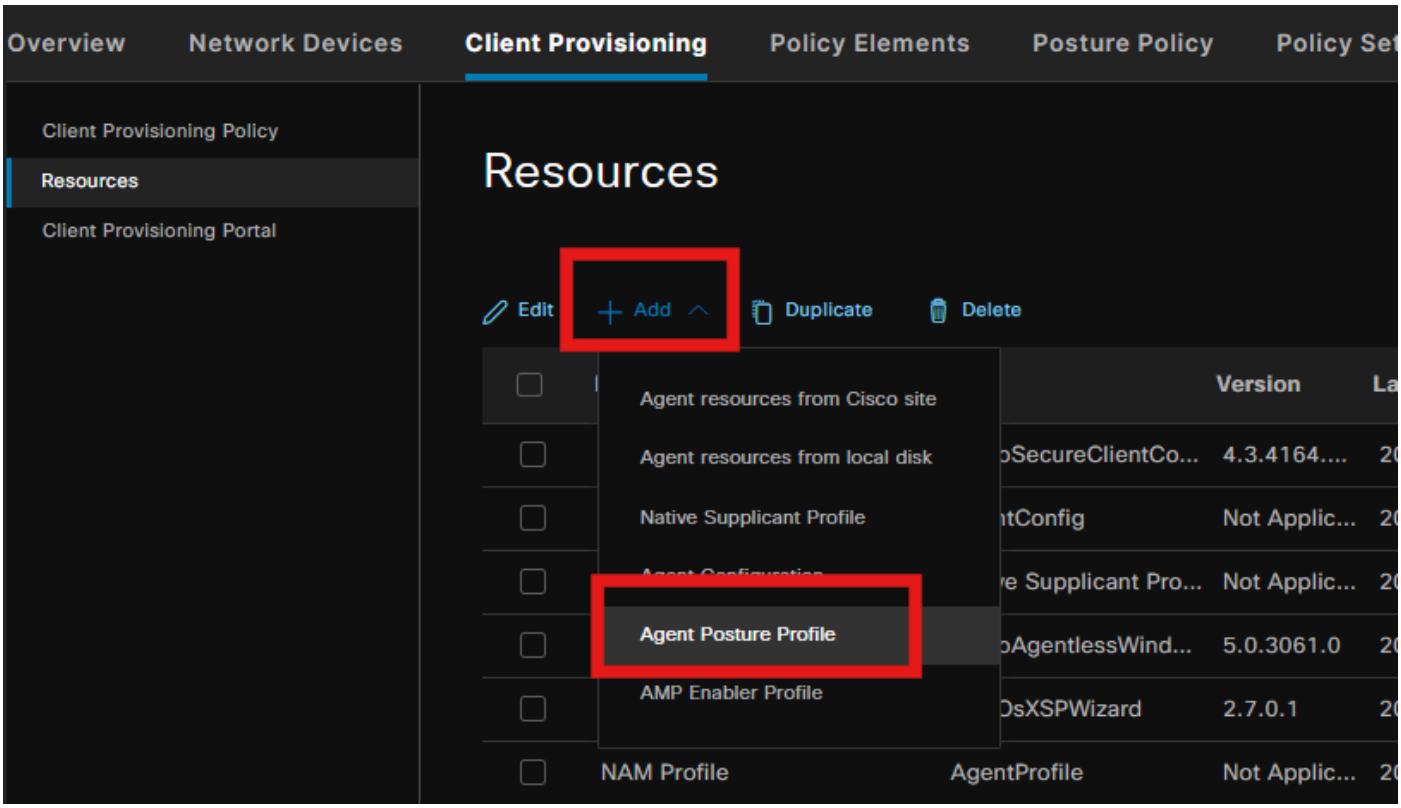
Per informazioni su come configurare un profilo NAM, consultare la presente guida Configurazione del profilo NAM Secure Client.

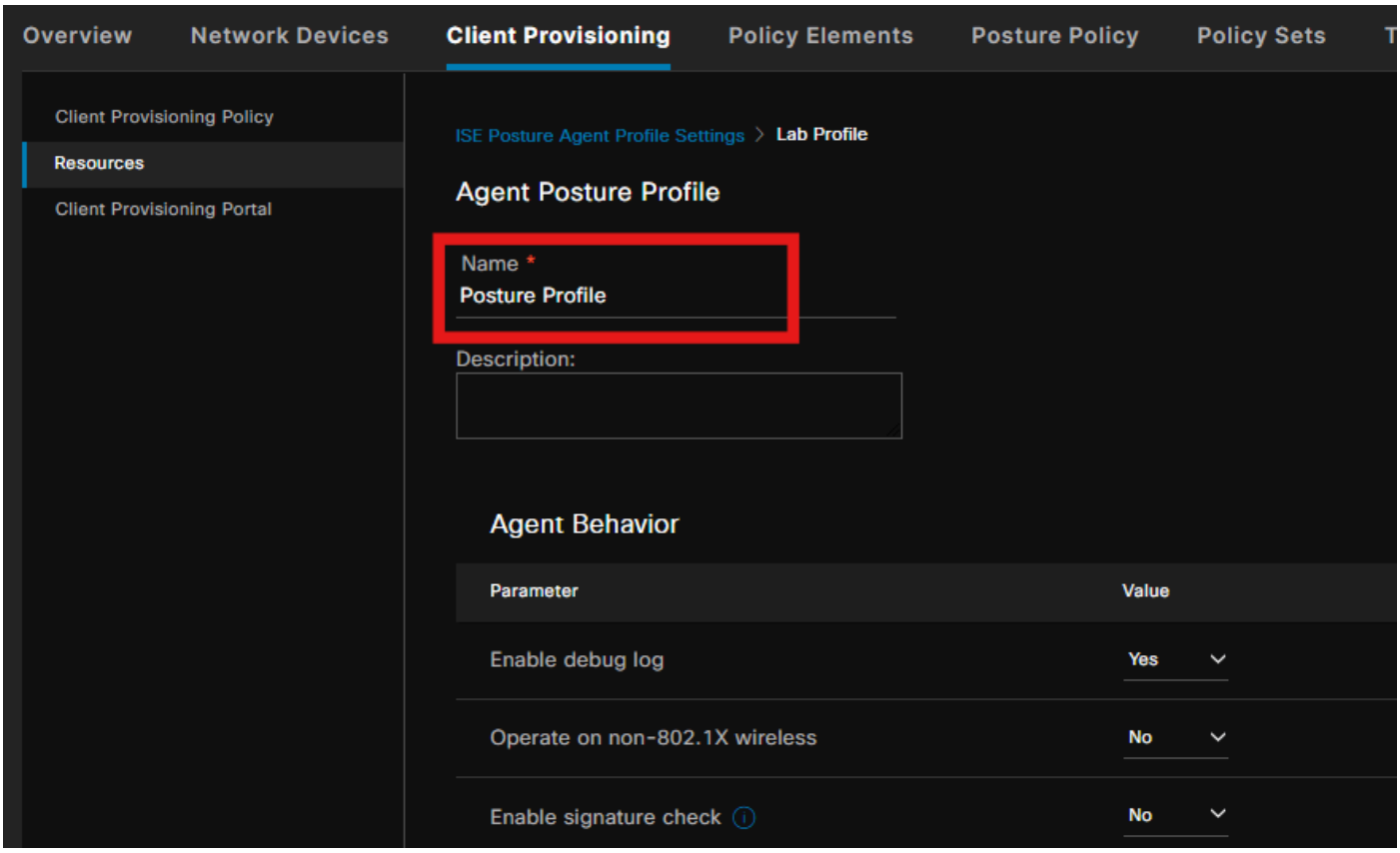
Passaggio 3. Caricare il profilo NAM su ISE

Per caricare il profilo NAM "Configuration.xml" su ISE come profilo agente, selezionare Client Provisioning > Risorse > Risorse agente dal disco locale.



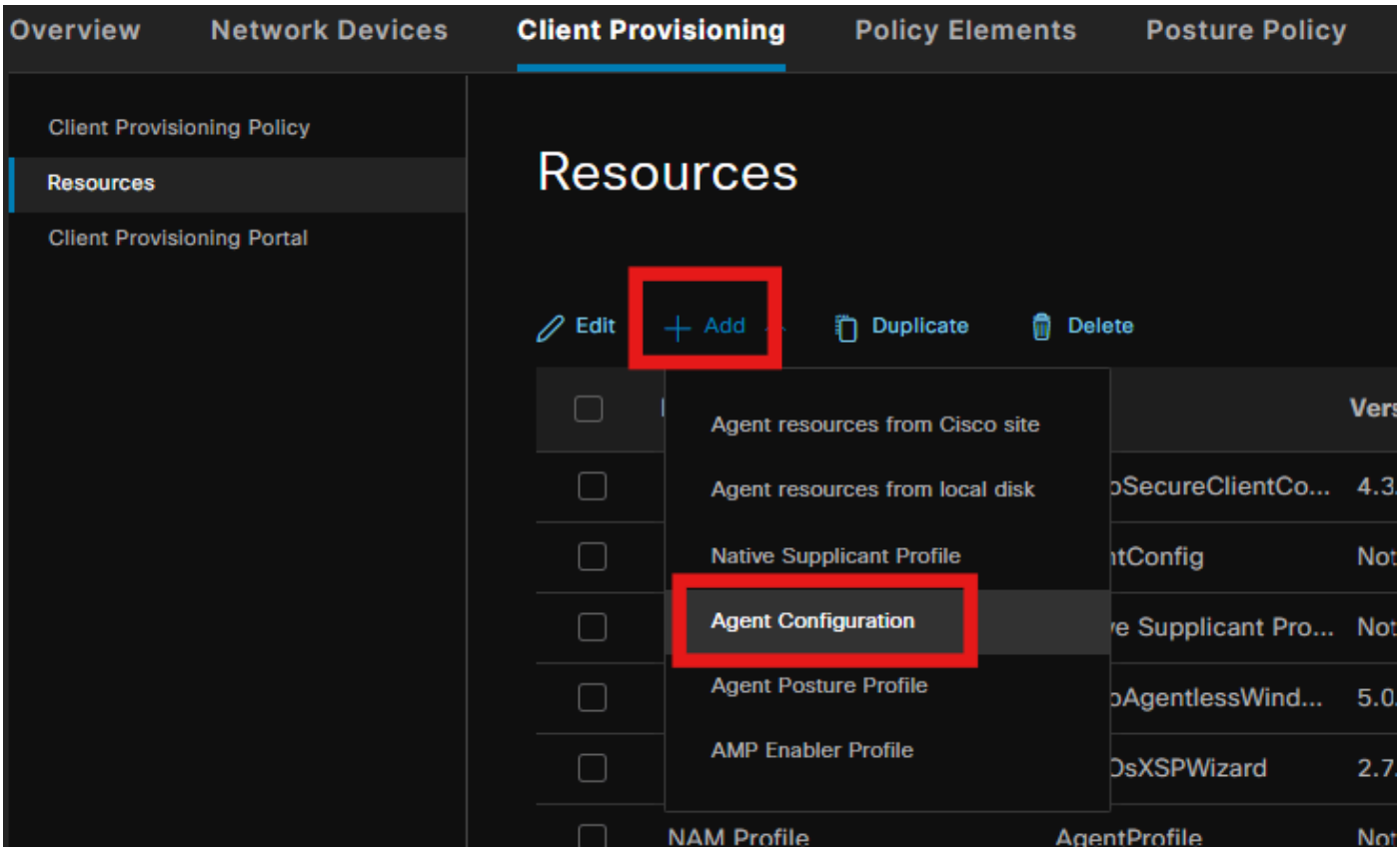
Passaggio 4. Crea un profilo di postura



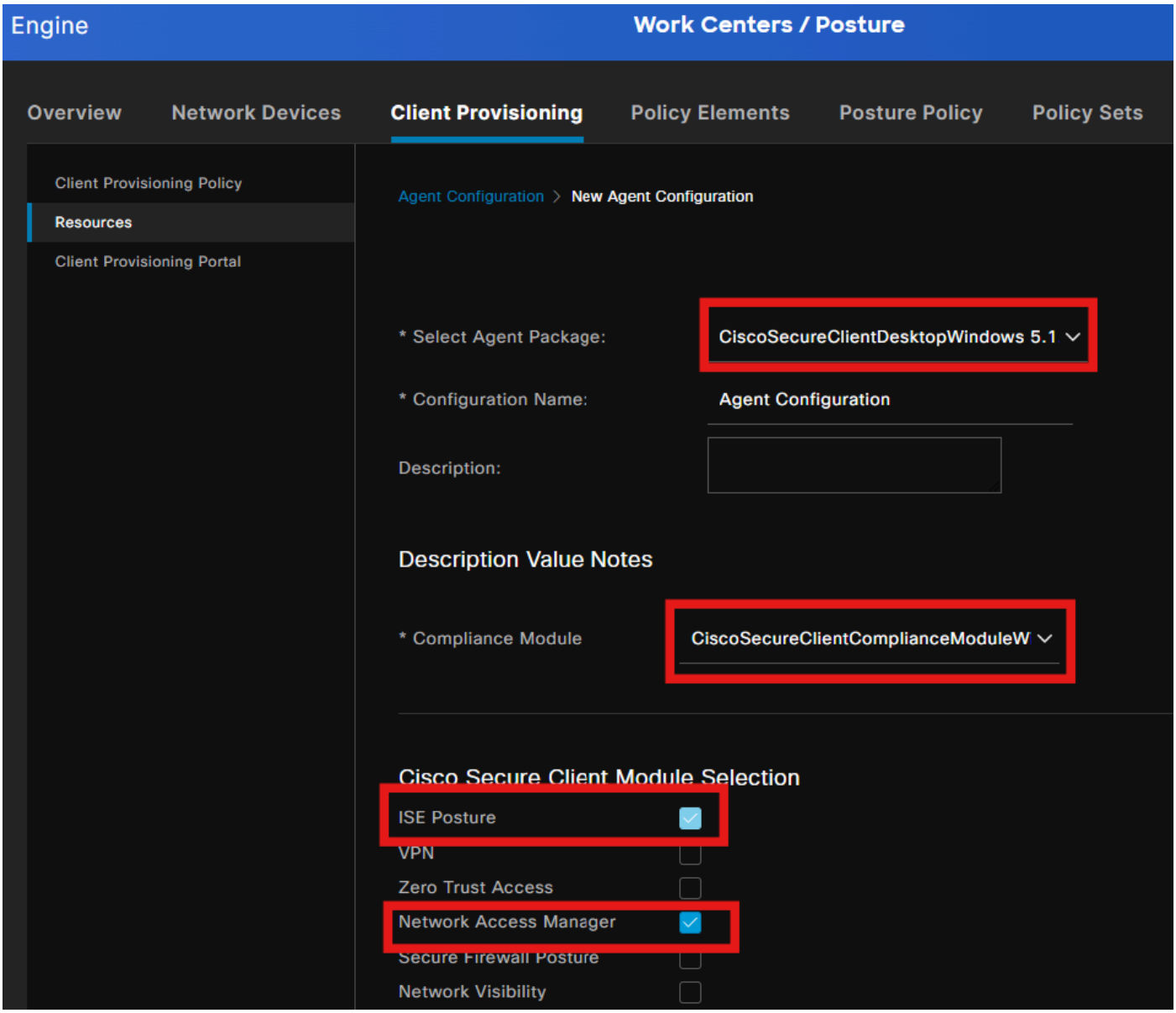


Dalla sezione Posture Protocol, non dimenticare di aggiungere * per consentire all'agente di connettersi a tutti i server.

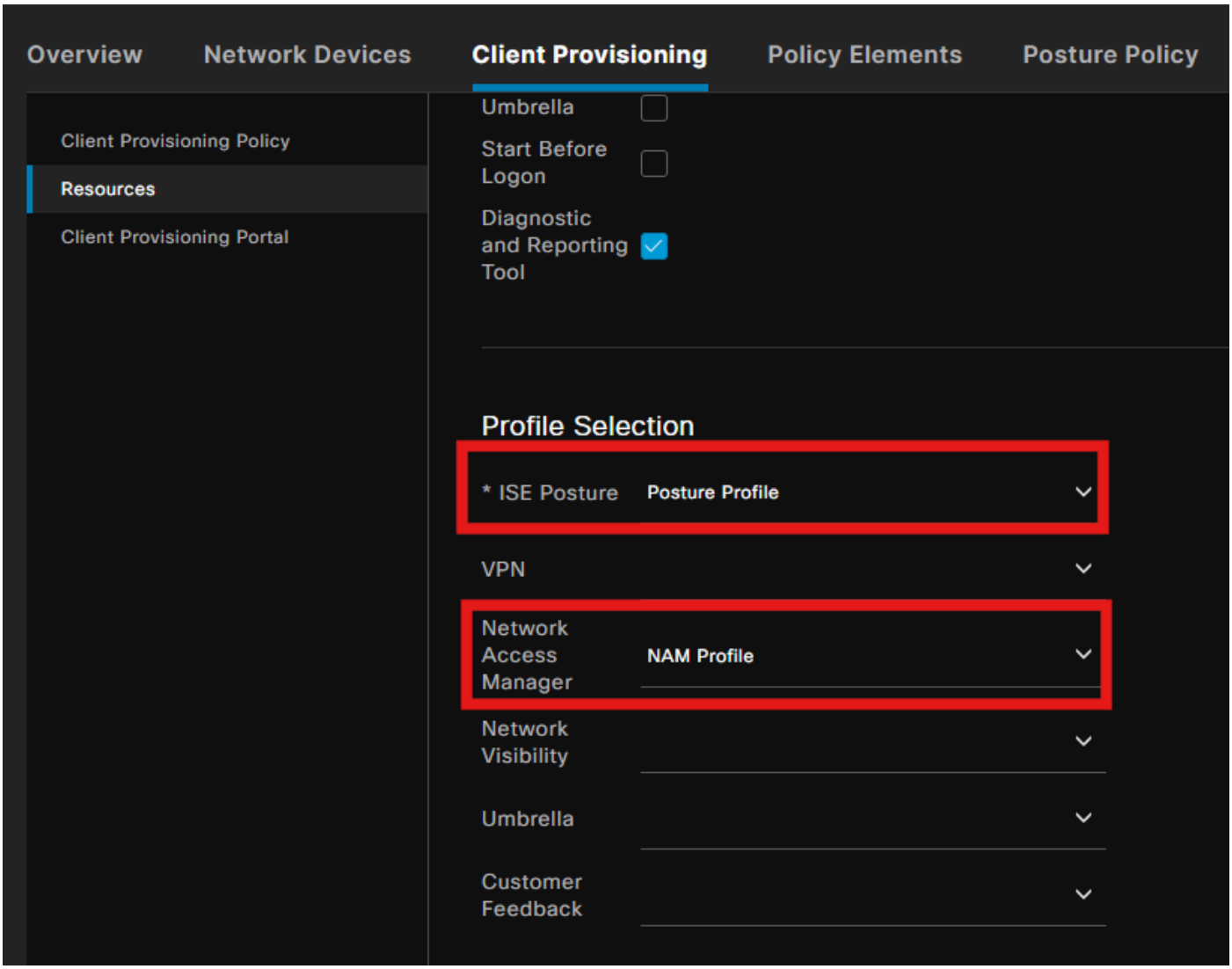
Passaggio 5. Crea configurazione agente



Selezionare il pacchetto client sicuro e modulo di conformità caricato e, sotto la selezione del modulo, selezionare i moduli ISE Posture, NAM e DART

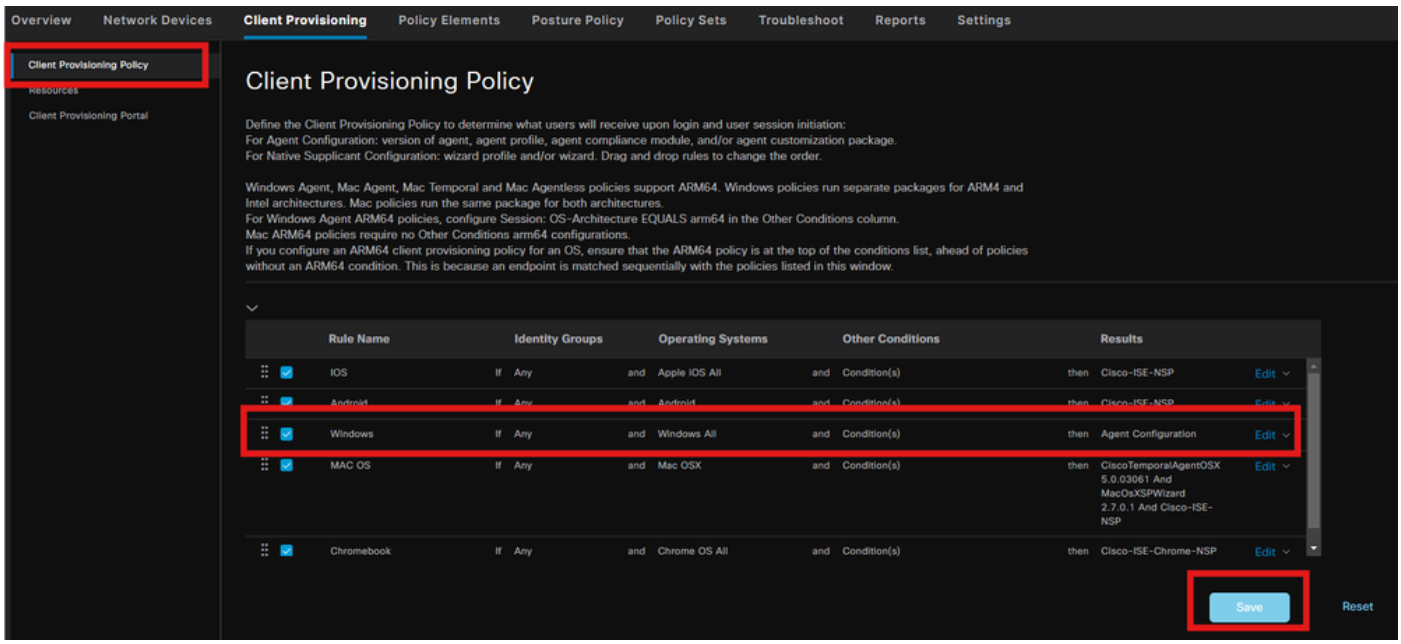


In Profilo (Profile), selezionate il profilo Postura (Posture) e NAM (NAM), quindi fate clic su Sottometti (Submit).



Passaggio 6. Criterio di provisioning client

Creare un criterio di provisioning client per il sistema operativo Windows e selezionare la configurazione agente creata nel passaggio precedente.

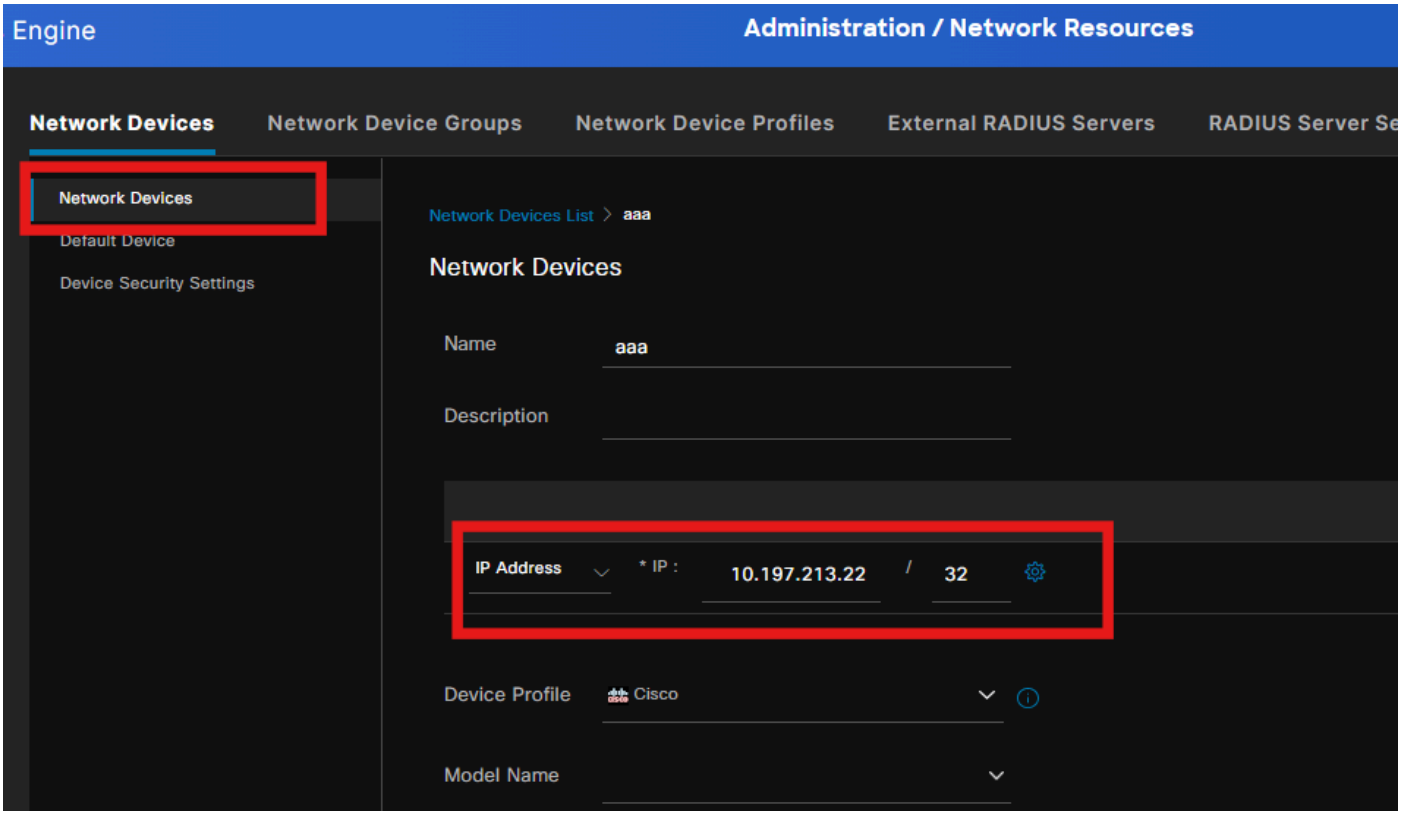


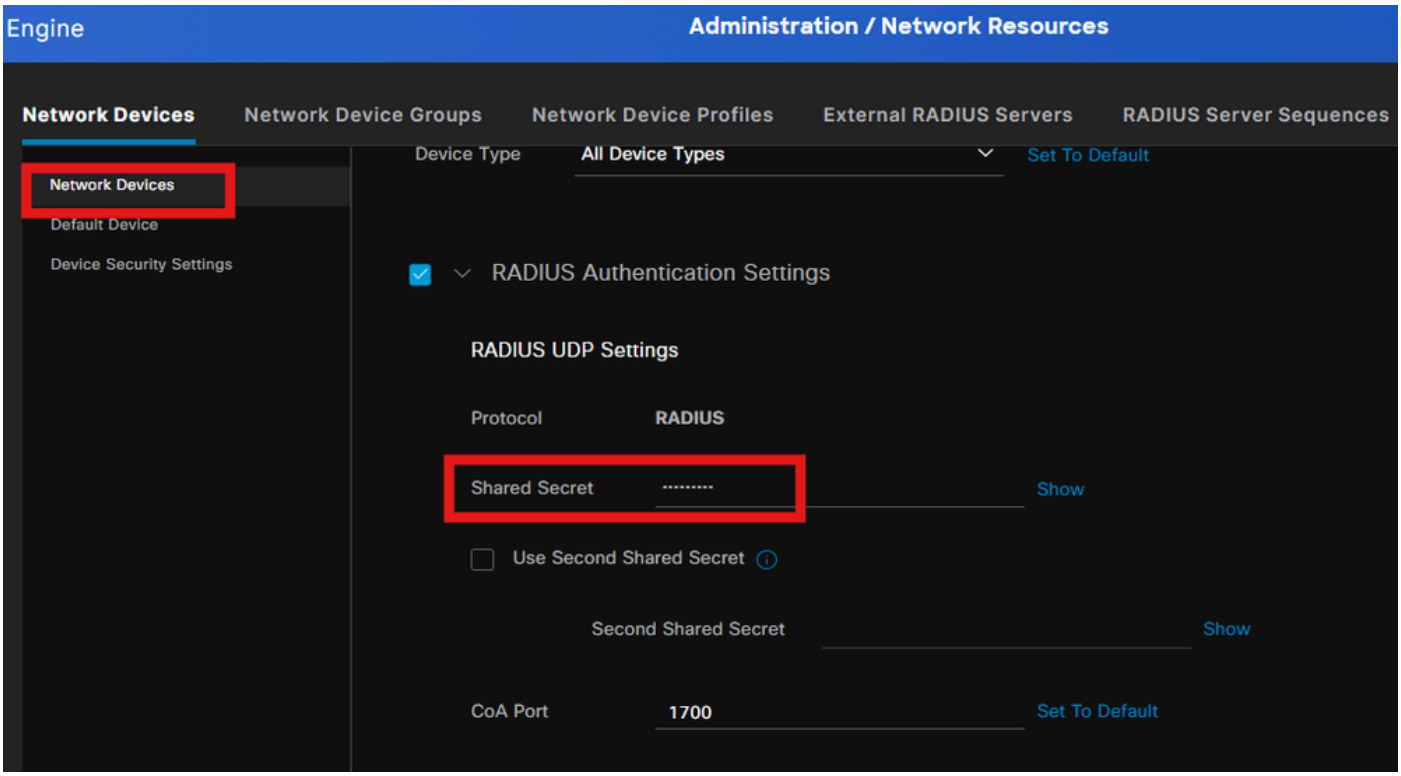
Passaggio 7. Criteri di postura

Per informazioni su come creare le condizioni e i criteri di postura, consultare questa guida [ISE Posture Prescriptive Deployment Guide](#) .

Passaggio 8. Aggiungi dispositivo di rete

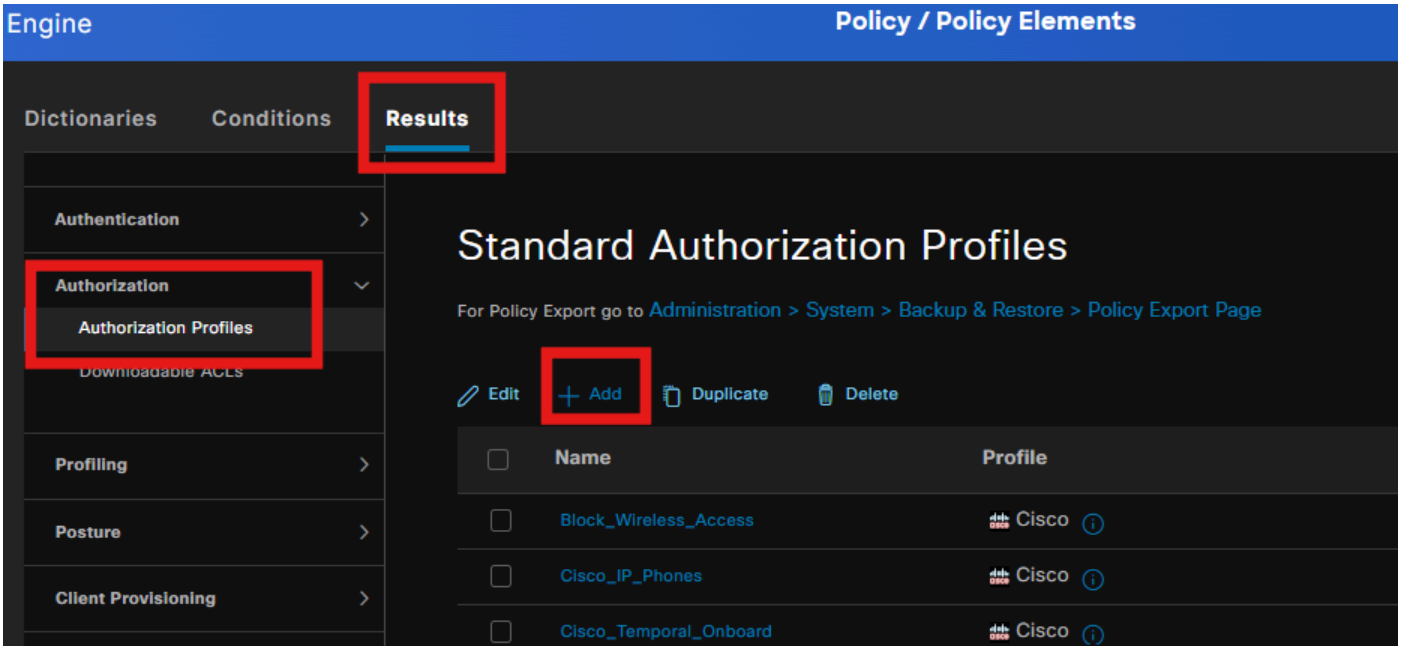
Per aggiungere l'indirizzo IP dello switch e la chiave segreta condivisa Radius, selezionare Amministrazione > Risorse di rete.



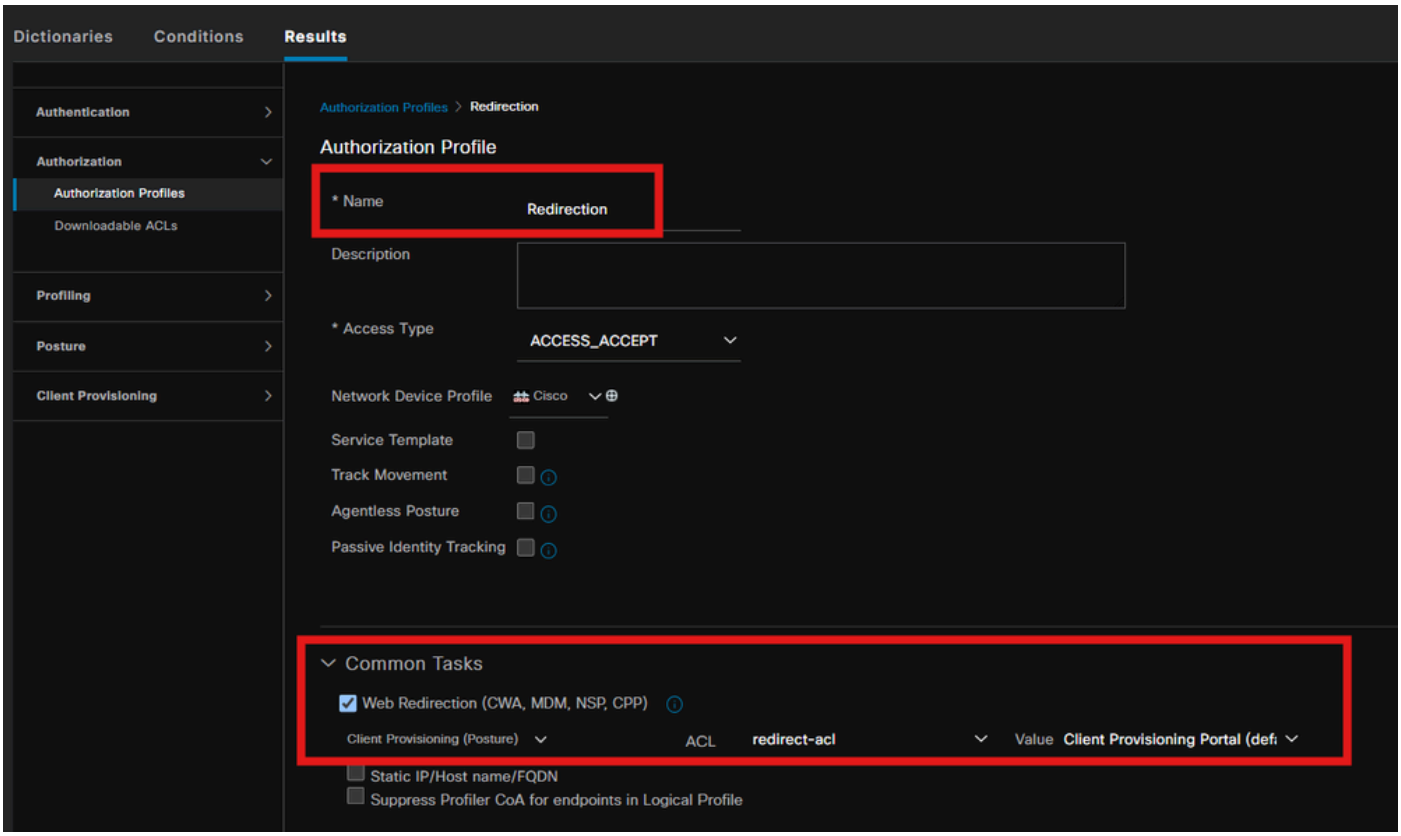


Passaggio 9. Profilo di autorizzazione

Per creare un profilo di reindirizzamento delle posture, selezionare Criteri > Elementi criterio > Risultati.

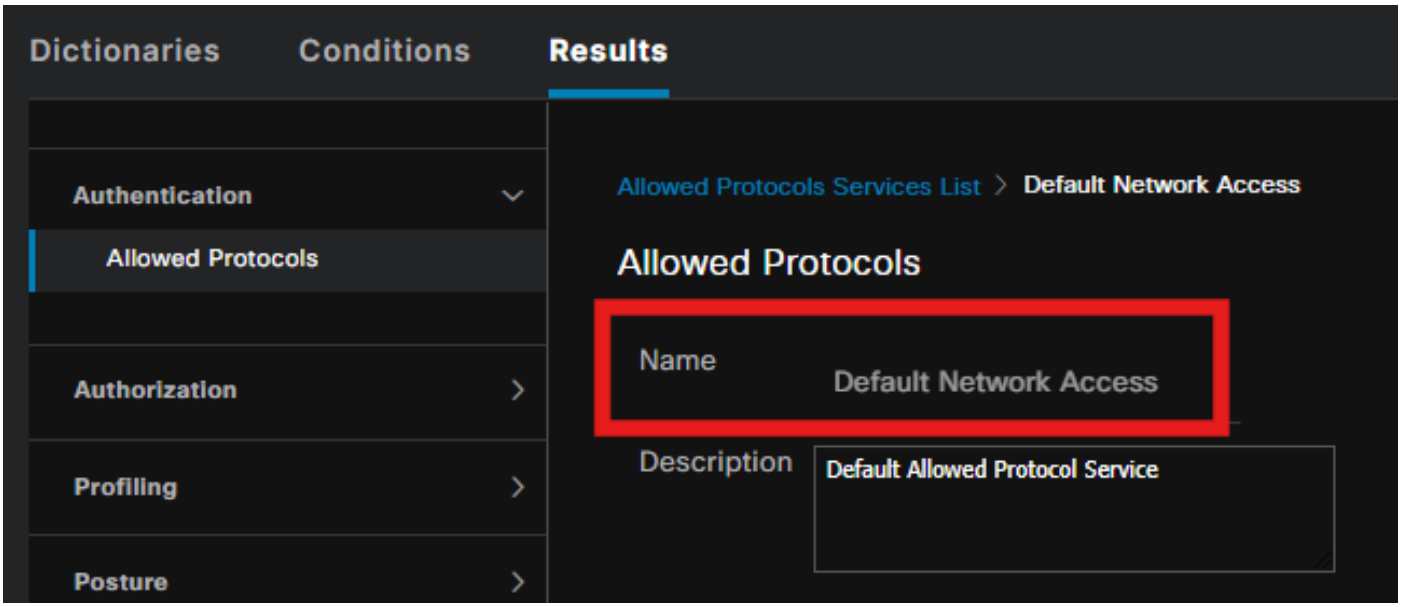


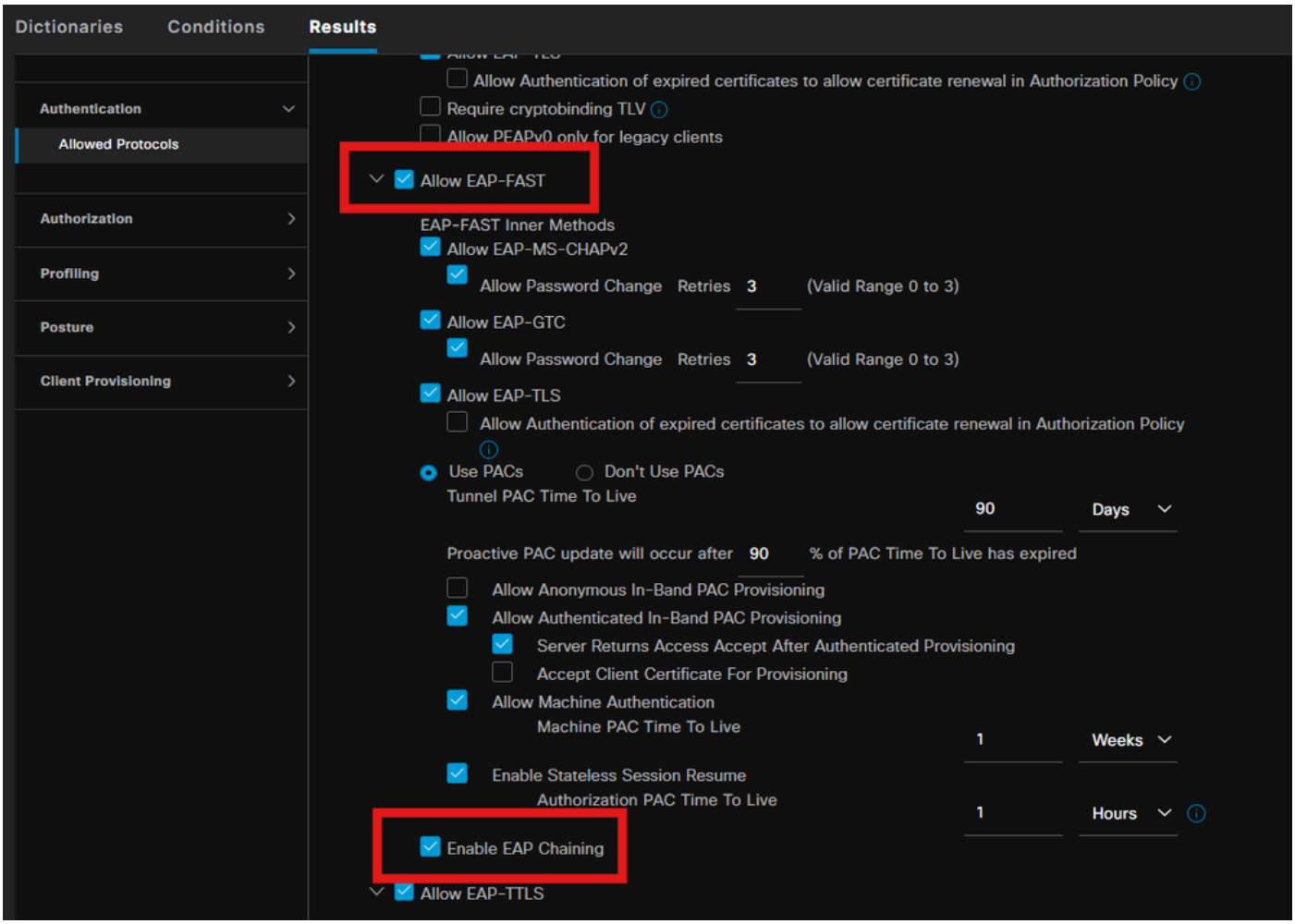
In Attività comando selezionare il portale di provisioning client con ACL di reindirizzamento.



Passaggio 10. Protocolli consentiti

Passare a Criterio > Elementi criterio > Risultati > Autenticazione > Protocolli consentiti, Selezionare le impostazioni di Concatenamento EAP,

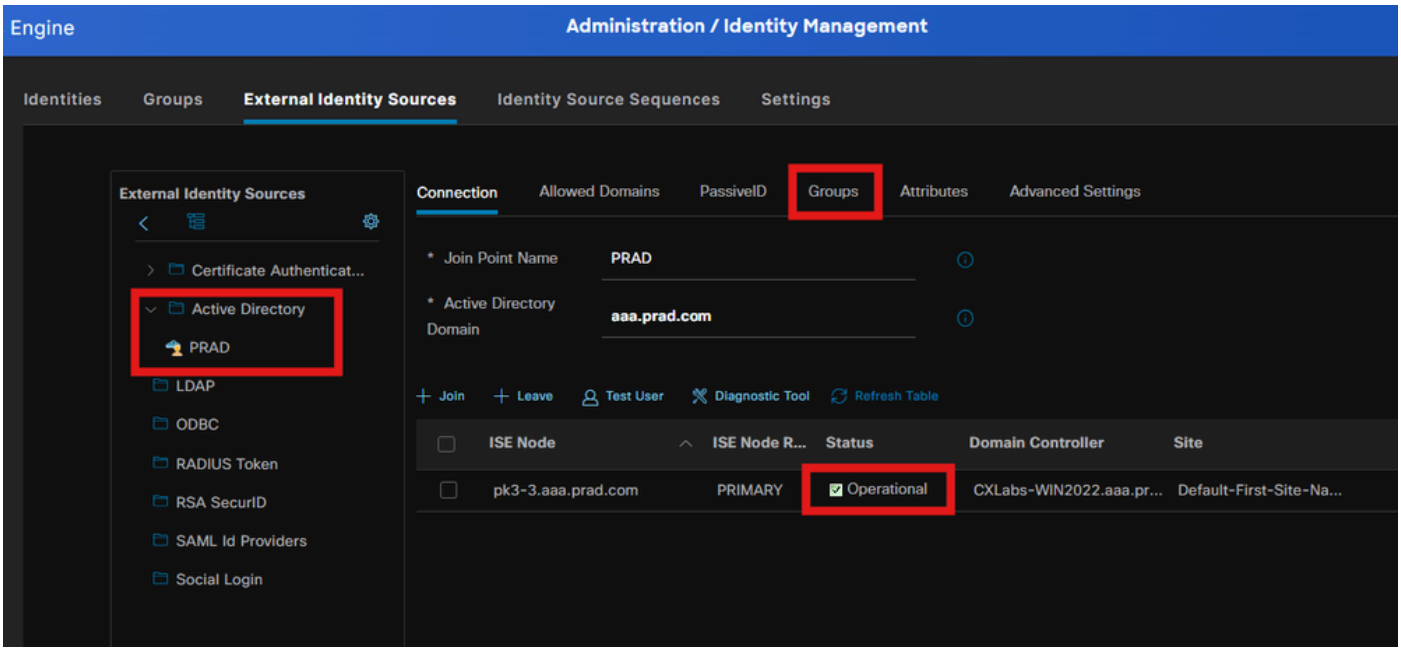




Passaggio 11. Active Directory

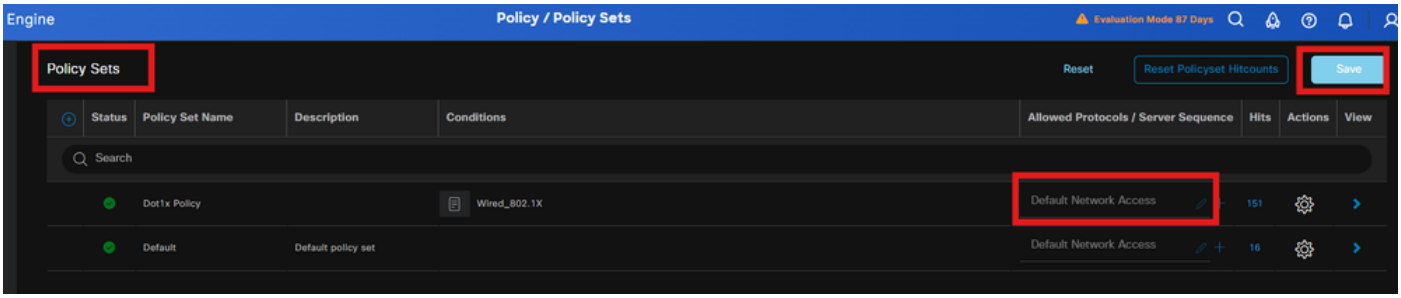
Verificare che ISE sia stato aggiunto al dominio Active Directory e che i gruppi di dominio siano selezionati se necessario per le condizioni di autorizzazione.

Amministrazione > Gestione delle identità > Origini identità esterne > Active Directory

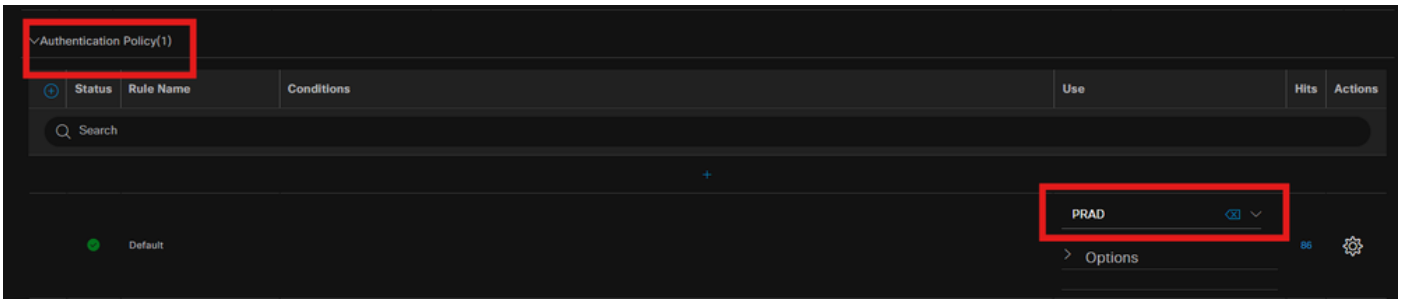


Passaggio 12. Set di criteri

Creare un set di criteri in ISE per autenticare la richiesta dot1x. Passare a Criterio > Set di criteri.



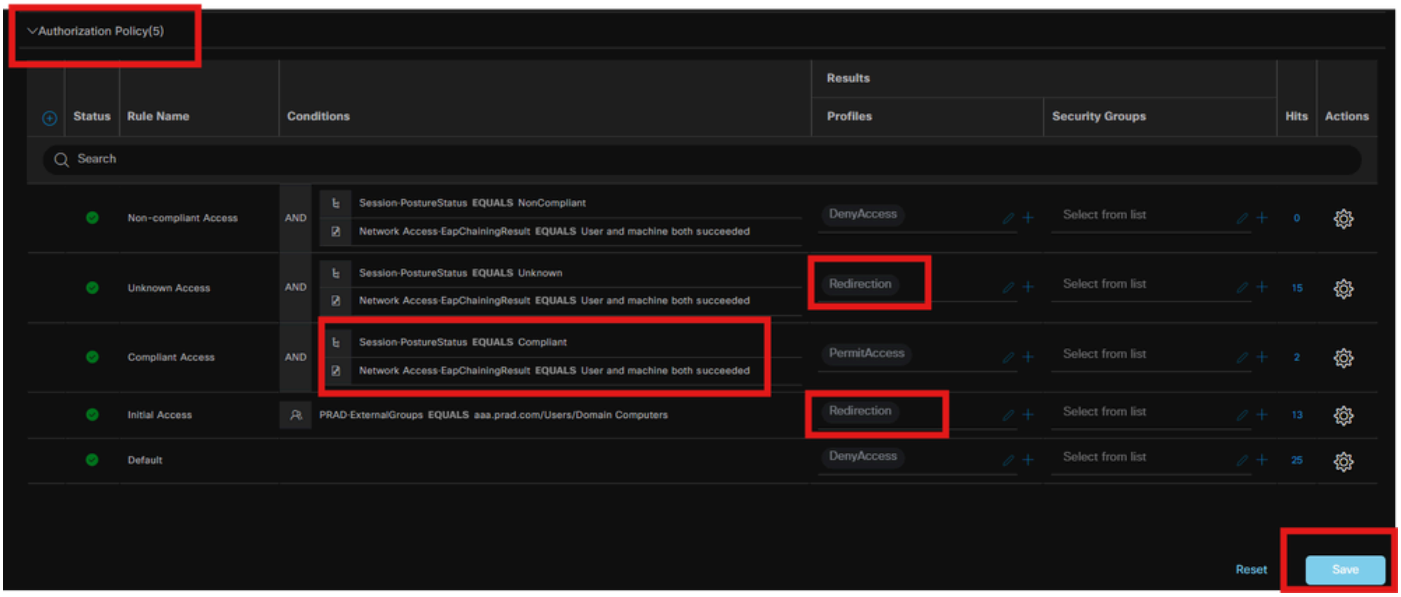
Selezionare Active Directory come origine identità per i criteri di autenticazione.



Configurare diverse regole di autorizzazione in base allo stato di postura sconosciuto, non conforme e conforme.

In questo scenario.

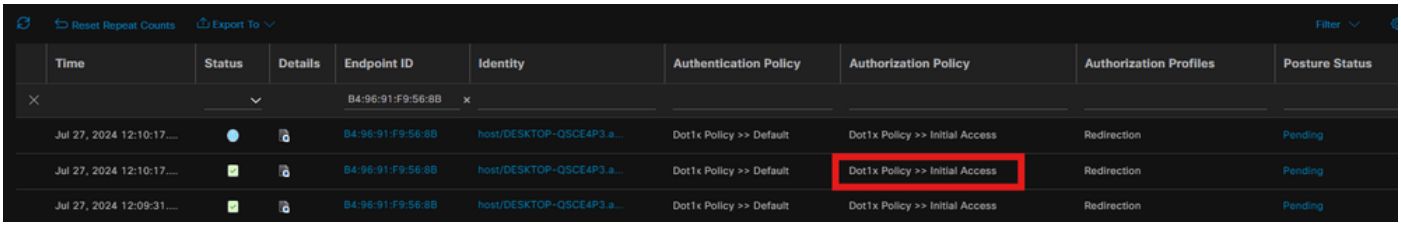
- Accesso iniziale : Reindirizzamento al portale di provisioning dei client ISE per installare Secure client agent e NAM Profile
- Accesso sconosciuto: accesso al portale di provisioning client per l'individuazione della postura basata sul reindirizzamento
- Accesso conforme: accesso completo alla rete
- Non conforme: nega accesso



Verifica

Passaggio 1. Scaricare e installare il modulo Secure Client Posture/NAM da ISE

Selezionare l'endpoint autenticato tramite dot1x, premendo "Initial Access" Authorization rule.
Passare a Operazioni > Raggio > Live Log



Su Switch, specificare l'URL di reindirizzamento e l'ACL da applicare all'endpoint.

```
Switch#show authentication session interface te1/0/24 - Dettagli
Interfaccia: TenGigabit Ethernet1/0/24
IIF-ID: 0x19262768
Indirizzo MAC: x4x6.xxxx.xxxx
Indirizzo IPv6: sconosciuto
Indirizzo IPv4: <IP-client>
Nome utente: host/DESKTOP-xxxxxx.aaa.prad.com
Stato: autorizzato
Dominio: DATA
Modalità host operativo: host singolo
Direzione controllo operazioni: entrambi
Timeout sessione: N/D
ID sessione comune: 16D5C50A000002CF067366B
ID sessione account: 0x0000001f
Handle: 0x7a000017
```

Criterio corrente: POLICY_Te1/0/24

Criteri locali:
Modello di servizio: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priorità 150)
Criterio di protezione: deve essere protetto
Stato protezione: collegamento non protetto

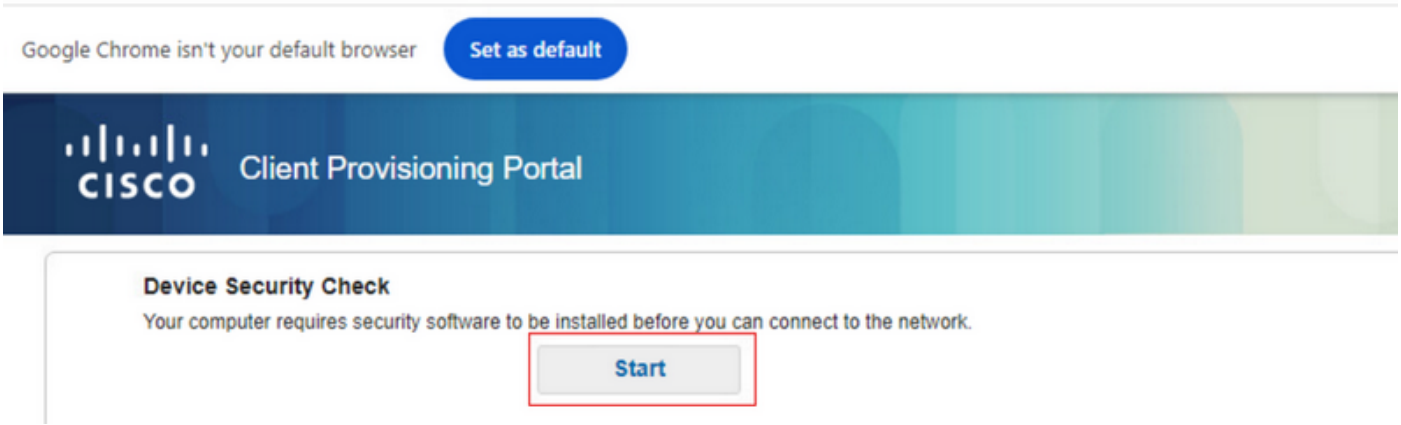
Criteri server:
ACL di reindirizzamento dell'URL: redirect-acl
Reindirizzamento URL:
https://ise33.aaa.prad.com:8443/portal/gateway?sessionId=16D5C50A0000002CF067366A&portal=ee39
7180-4995-8aa2-9fb282645a8f&action=cpp&token=518f857900a37f9afc6d2da8b6fe3bc2
ACS ACL: xACSACLx-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3

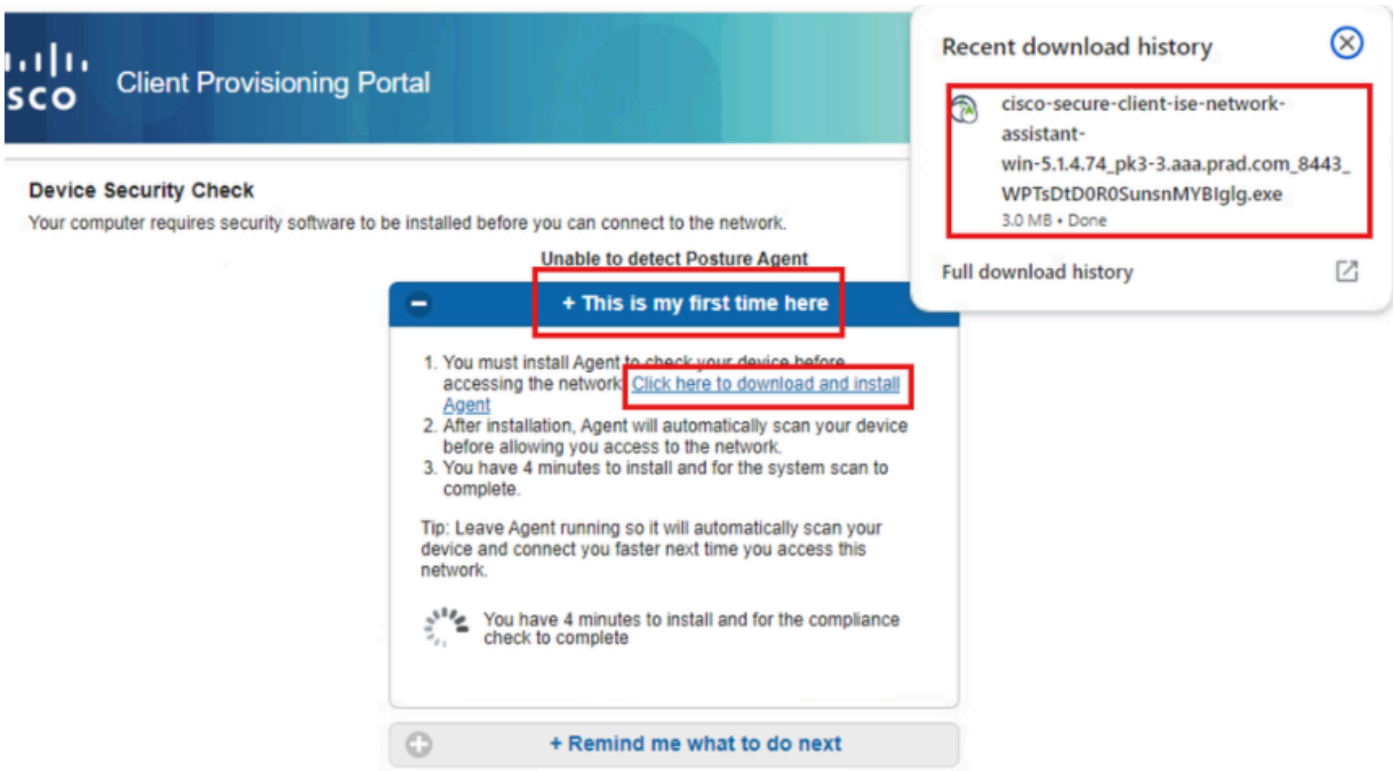
Elenco stato metodo:
Stato metodo
Autenticazione dot1x riuscita

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

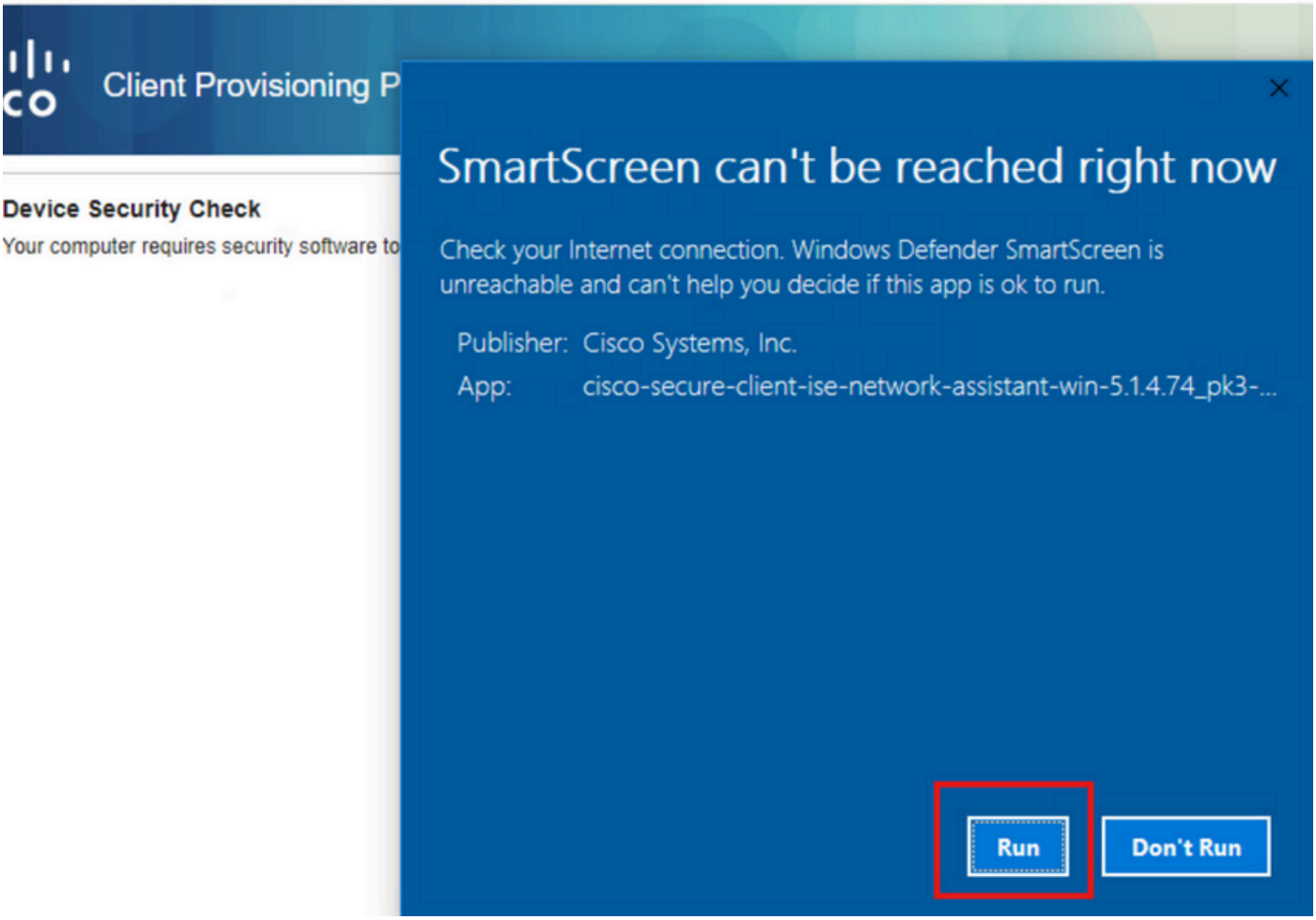
Livello rete Indirizzo Collegamento Livello indirizzo Interfaccia vlan livello livello livello di durata Tempo rim
ARP X.X.X.X b496.91f9.568b Te1/0/24 1000 005 4mn RAGGIUNGIBILE 39 s try 0

Sull'endpoint, verificare il traffico reindirizzato a ISE Posture Posture e fare clic su Start per scaricare l'Assistente installazione di rete sull'endpoint.



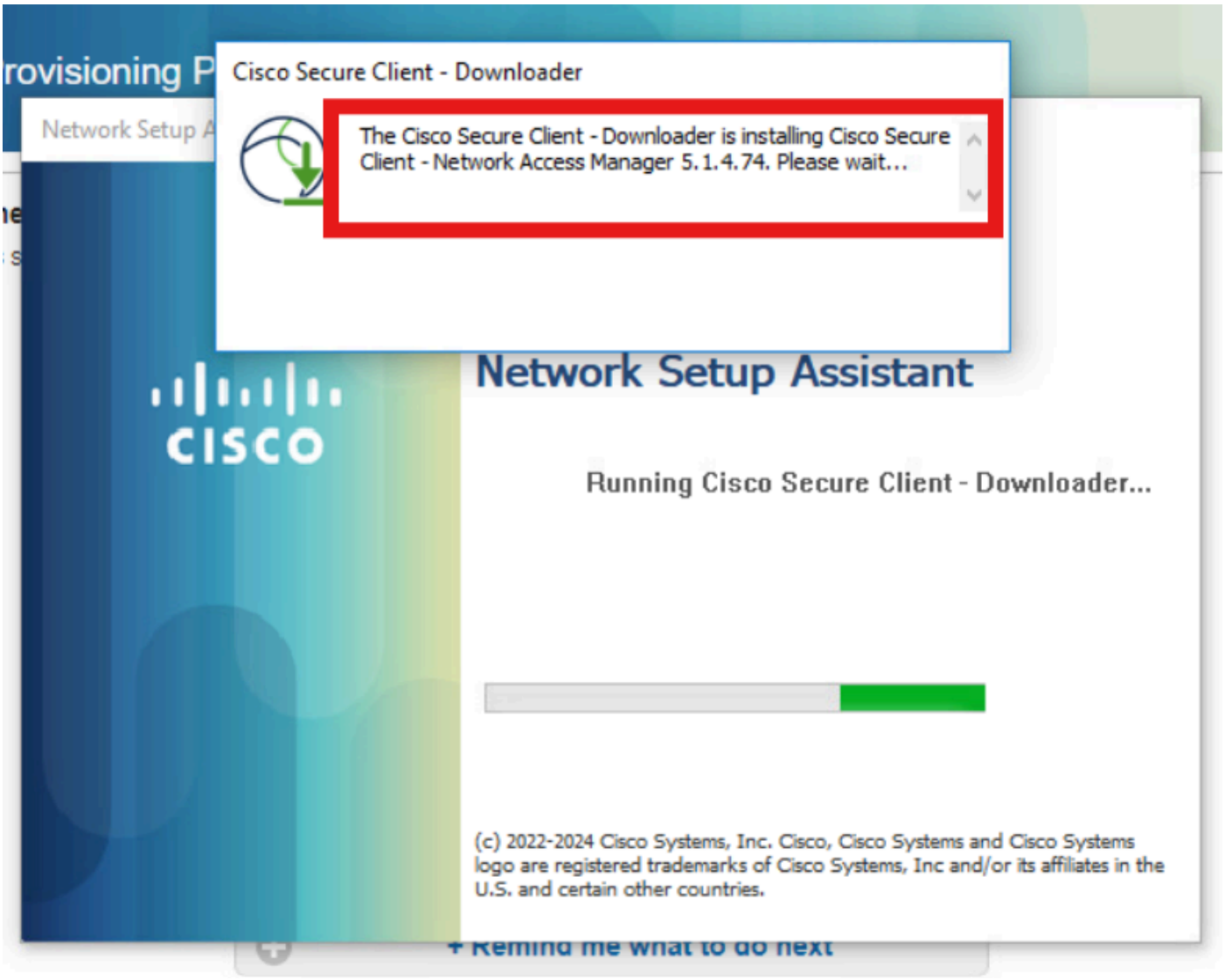


Fare clic su Esegui per installare l'applicazione NSA.

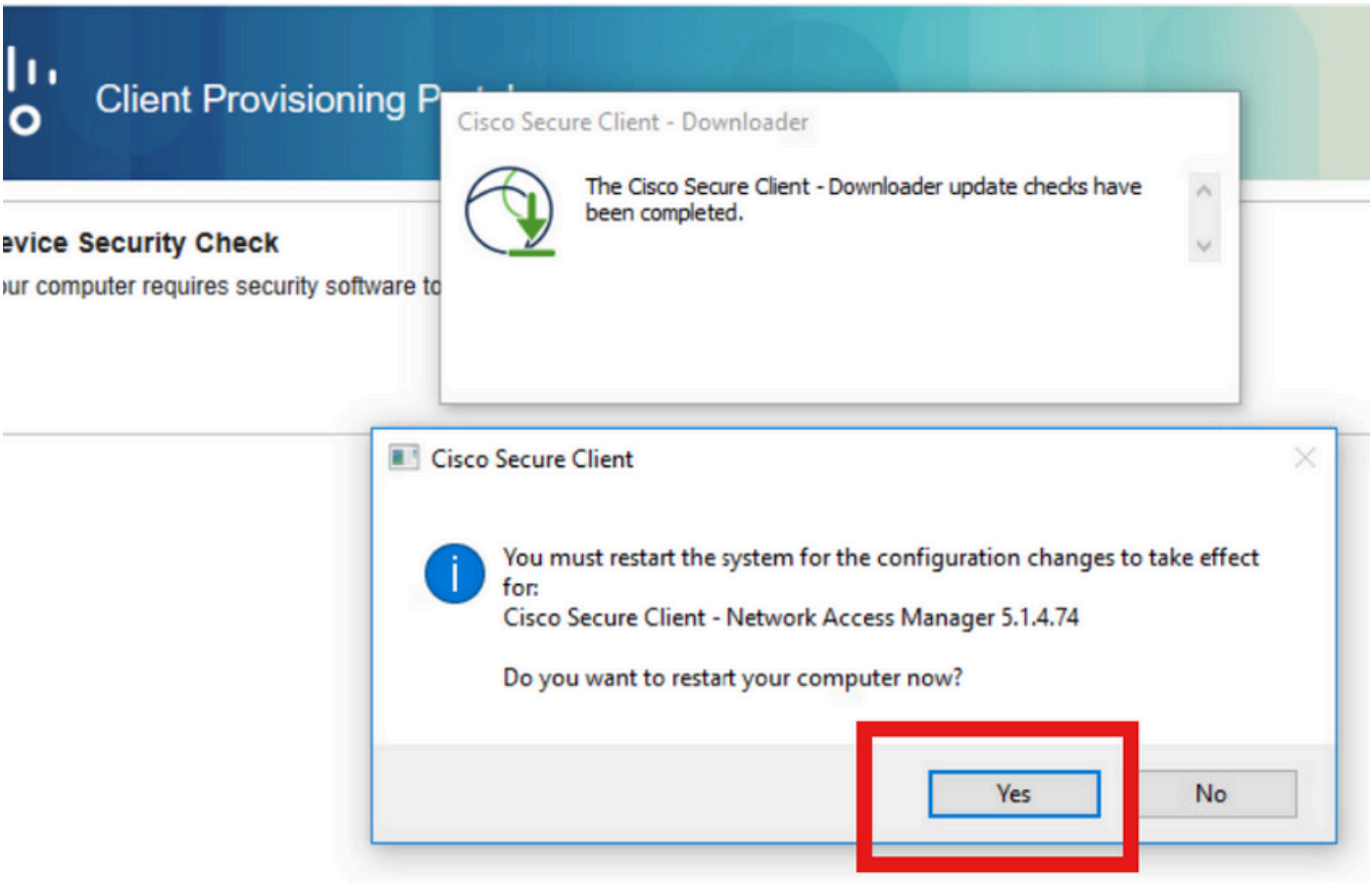


A questo punto, l'NSA richiama il download di Secure Client Agent da ISE e installa Posture, il

modulo NAM e il file di configurazione del profilo NAM.xml .



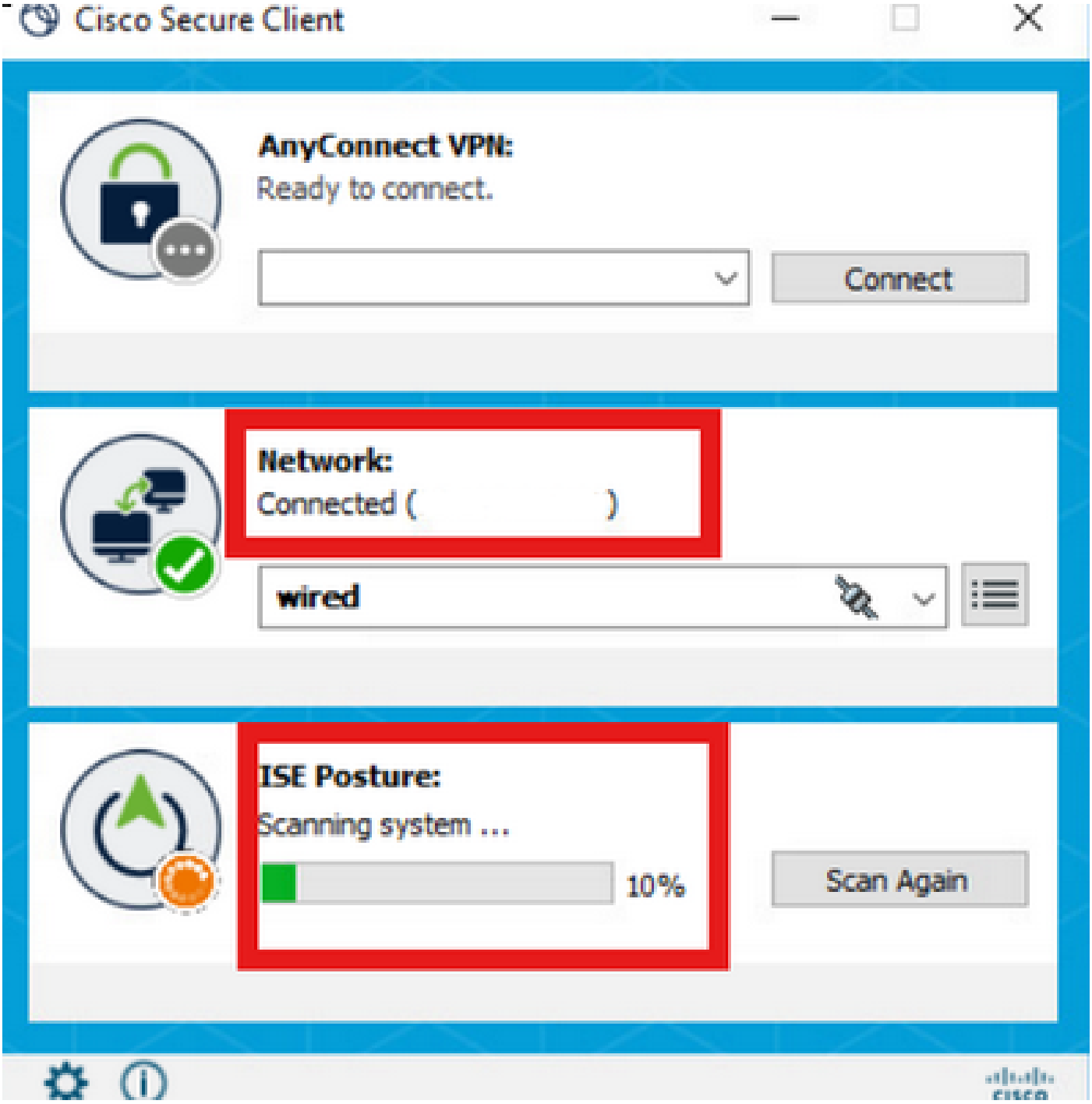
Prompt di riavvio attivato dopo l'installazione di NAM. Fare clic su Sì.



Passaggio 2. EAP-FAST

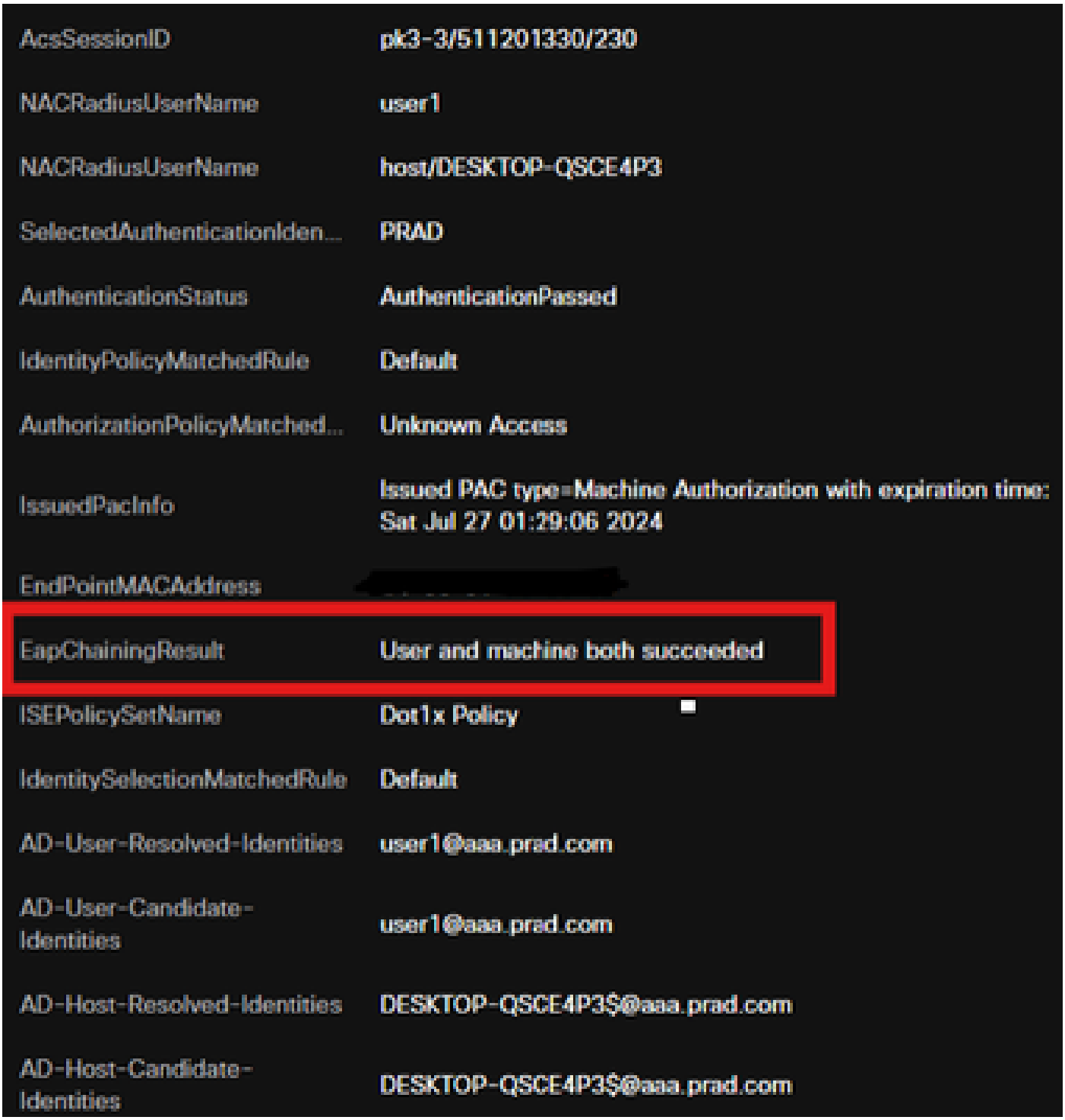
Dopo il riavvio del PC e l'accesso dell'utente, NAM autentica sia l'utente che il computer tramite EAP-FAST.

Se l'endpoint viene autenticato correttamente, NAM indica che è connesso e il modulo Posture attiva la scansione della postura.



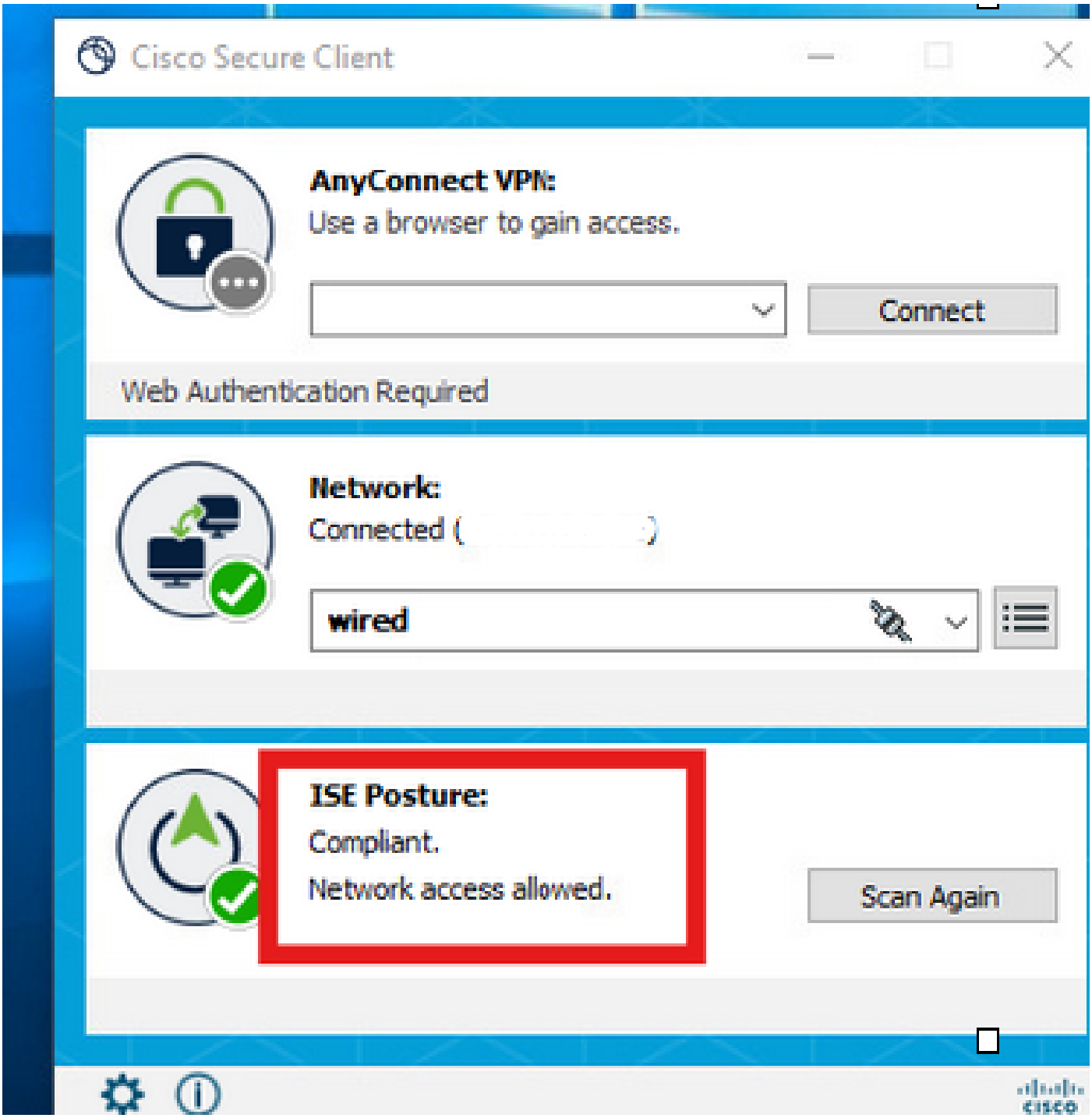
Sui log ISE Live, l'endpoint sta violando la regola di accesso sconosciuto.

Ora il protocollo di autenticazione è EAP-FAST basato sulla configurazione del profilo NAM e il risultato del concatenamento EAP è "Successo".

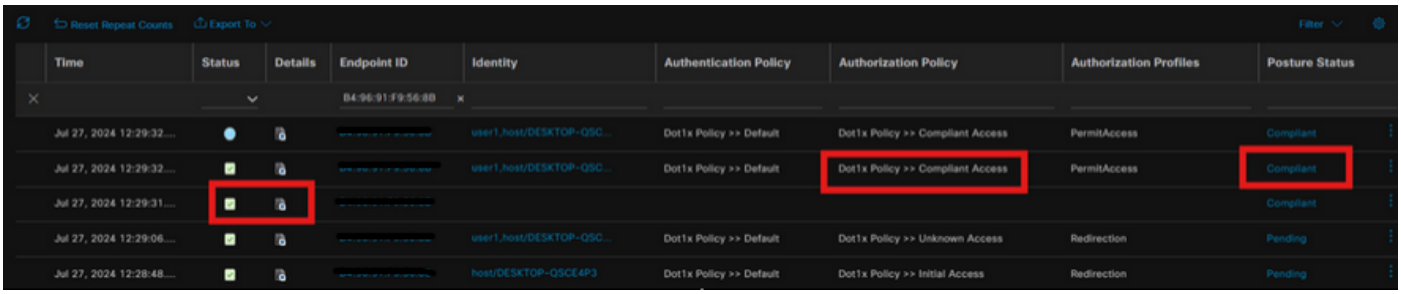


Passaggio 3. Analisi postura

Il modulo Secure Client Posture attiva la scansione delle posture ed è contrassegnato come un reclamo basato sulla policy ISE Posture.



Il CoA viene attivato dopo l'analisi delle posture e ora l'endpoint raggiunge la policy di accesso al reclamo.

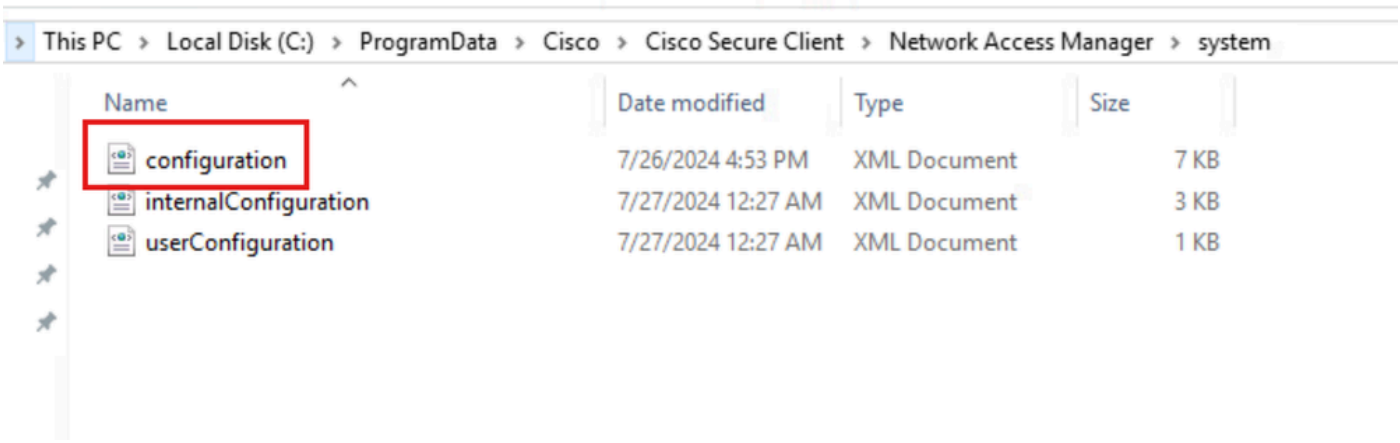


Risoluzione dei problemi

Passaggio 1. Profilo NAM

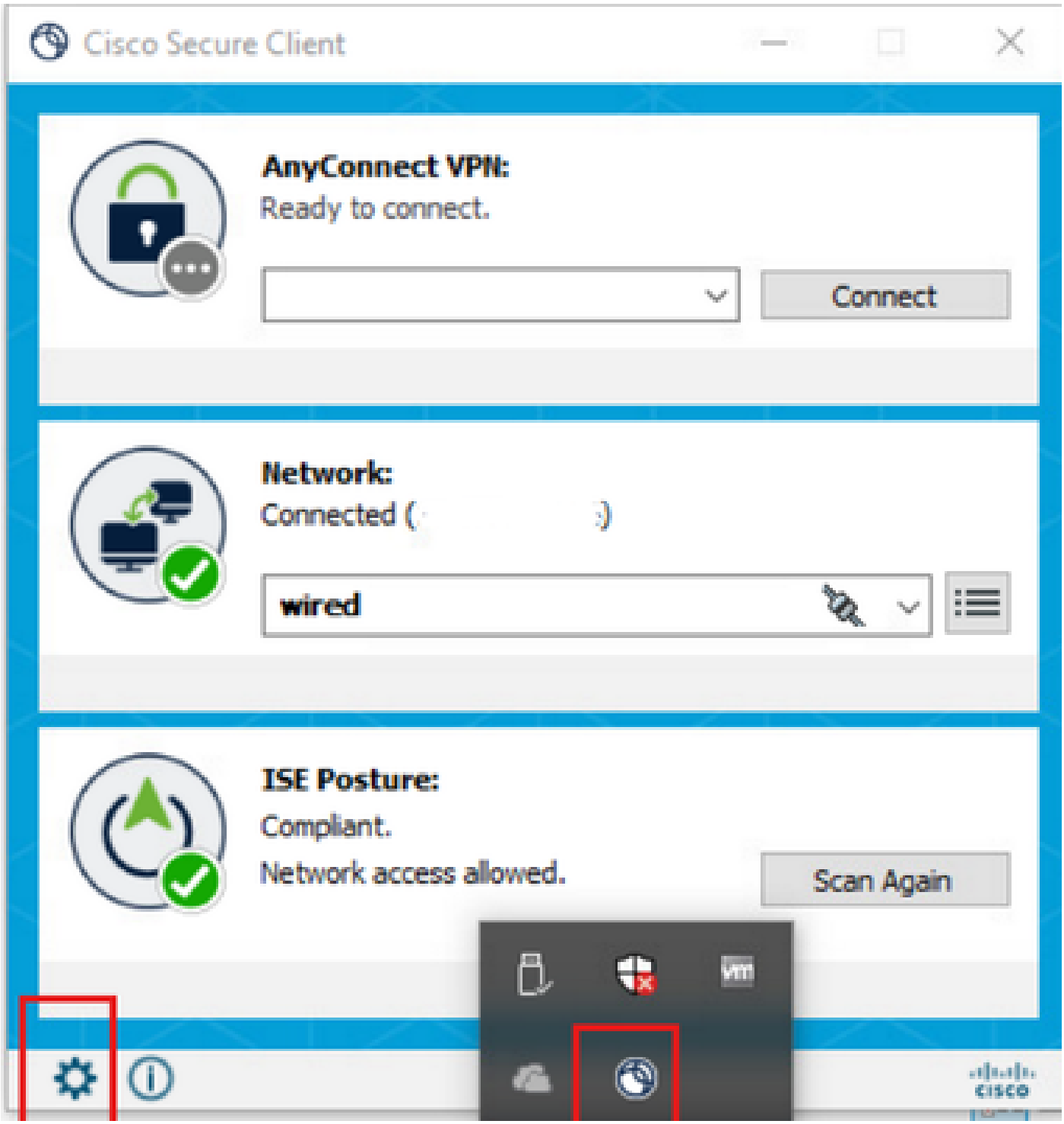
Verificare che il file configuration.xml del profilo NAM sia presente in questo percorso sul PC dopo l'installazione del modulo NAM.

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



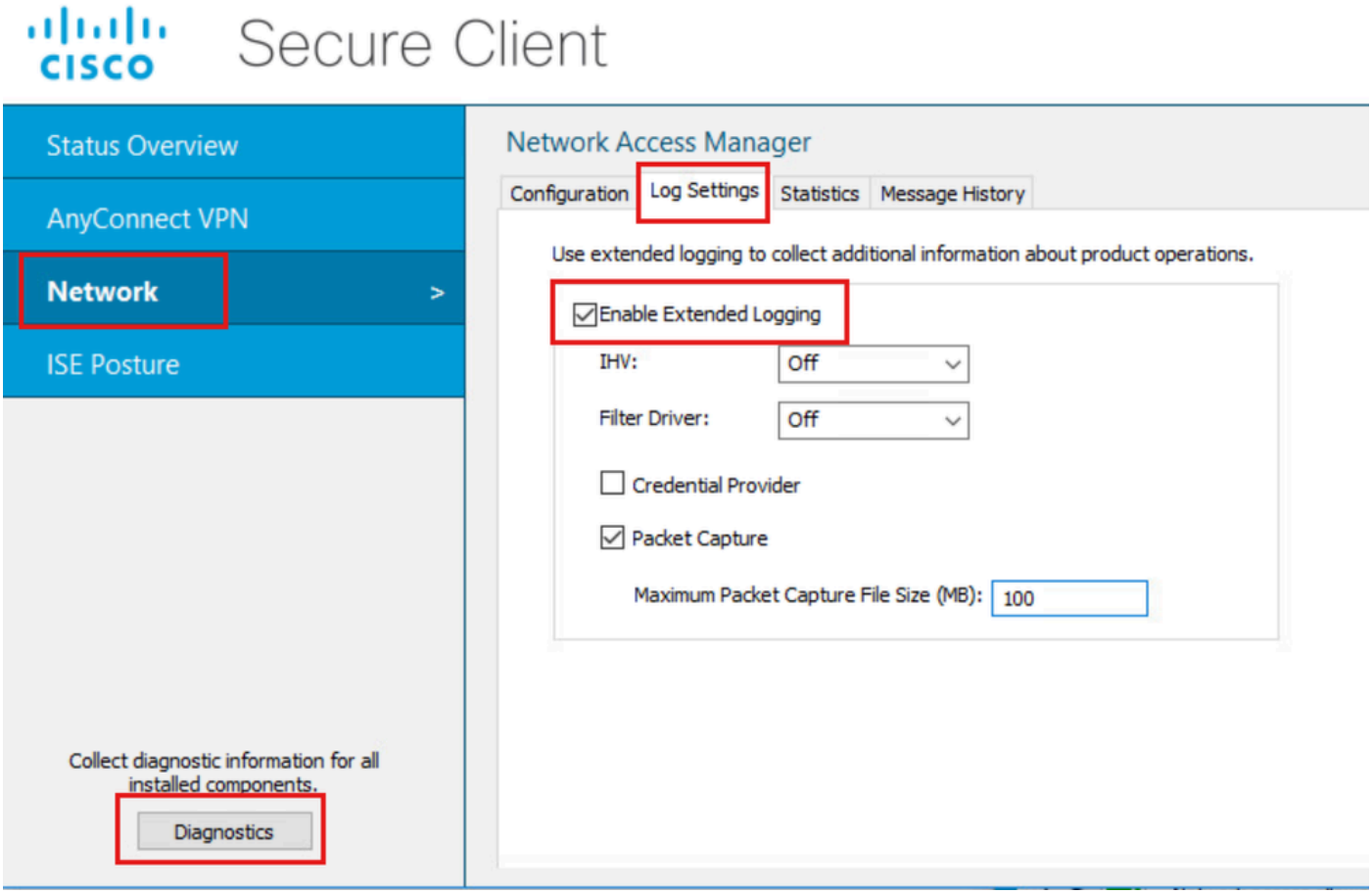
Passaggio 2. Registrazione estesa NAM

Fare clic sull'icona Secure Client nella barra delle applicazioni e selezionare l'icona "settings" (Impostazioni).



Passare alla scheda Rete > Impostazioni registro. Selezionare la casella di controllo Abilita registrazione estesa.
Impostare la dimensione del file di acquisizione del pacchetto su 100 MB.

Dopo aver riprodotto il problema, fare clic su Diagnostics (Diagnostica) per creare il pacchetto DART sull'endpoint.



Nella sezione Cronologia messaggi vengono visualizzati i dettagli di ogni passaggio eseguito da NAM.

Passaggio 3. Debug sullo switch

Abilitare questi debug sullo switch per la risoluzione dei problemi relativi al dot1x e al flusso di reindirizzamento.

debug ip http all

transazioni http ip di debug

url http ip di debug

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

set platform software trace smd switch attivo 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

Per visualizzare i registri

show logging (visualizza registri)

mostra processo di registrazione smd interno

Passaggio 4. Debug su ISE

Raccogliere il bundle di supporto ISE con questi attributi da impostare al livello di debug:

- postura
- portale
- provisioning
- runtime-AAA
- nsf
- sessione nsf
- svizzero
- client-webapp

Informazioni correlate

Configurazione di Secure Client NAM

Guida all'implementazione prescrittiva di ISE Posture

Risoluzione dei problemi relativi al dot1x sugli switch Catalyst serie 9000

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).