在Windows上通过ISE 3.3配置和部署安全客户端NAM配置文件

目录

简介

背景信息

先决条件

- 要求
- 使用的组件

配置

- 网络图
- 数据流
- 配置交换机
- 下载安全客户端软件包

ISE 配置

- 步骤1:在ISE上上传包
- 第二步：从配置文件编辑器工具创建NAM配置文件
- 第三步：在ISE上上传NAM配置文件
- 第四步：创建安全评估配置文件
- 第五步：创建代理配置
- 第六步：客户端调配策略
- 步骤 7.安全评估策略
- 步骤 8添加网络设备
- 步骤 9授权配置文件
- 步骤 10允许的协议
- 步骤 11Active Directory
- 步骤 12策略集

验证

- 步骤1:从ISE下载并安装安全客户端状态/NAM模块
- 第二步：EAP-FAST
- 第三步：状态扫描

故障排除

- 步骤1:NAM配置文件
- 第二步：NAM扩展日志记录
- 第3步：在交换机上进行调试
- 第四步：ISE上的调试

相关信息

简介

本文档介绍如何通过身份服务引擎(ISE)部署思科安全客户端网络访问管理器(NAM)配置文件。

背景信息

EAP-FAST身份验证分两个阶段进行。在第一阶段，EAP-FAST使用TLS握手来提供密钥交换并验证使用类型长度值(TLV)对象建立受保护的隧道。这些TLV对象用于在客户端和服务器之间传输身份验证相关数据。隧道建立后，第二阶段从客户端和ISE节点进行进一步对话以建立所需的身份验证和授权策略开始。

NAM配置配置文件设置为使用EAP-FAST作为身份验证方法，并且可用于管理定义的网络。
此外，可在NAM配置配置文件中配置计算机和用户连接类型。
企业Windows设备使用具有状态检查的NAM获得完整的企业访问权限。
个人Windows设备使用相同的NAM配置获得对受限网络的访问权限。

本文档提供有关使用网络部署通过身份服务引擎(ISE)终端安全评估门户部署思科安全客户端网络访问管理器(NAM)配置文件的说明以及终端安全评估合规性检查。

先决条件

要求

Cisco 建议您了解以下主题：

- 身份服务引擎 (ISE)
- AnyConnect NAM和配置文件编辑器
- 安全评估策略
- 适用于802.1x服务的Cisco Catalyst配置

使用的组件

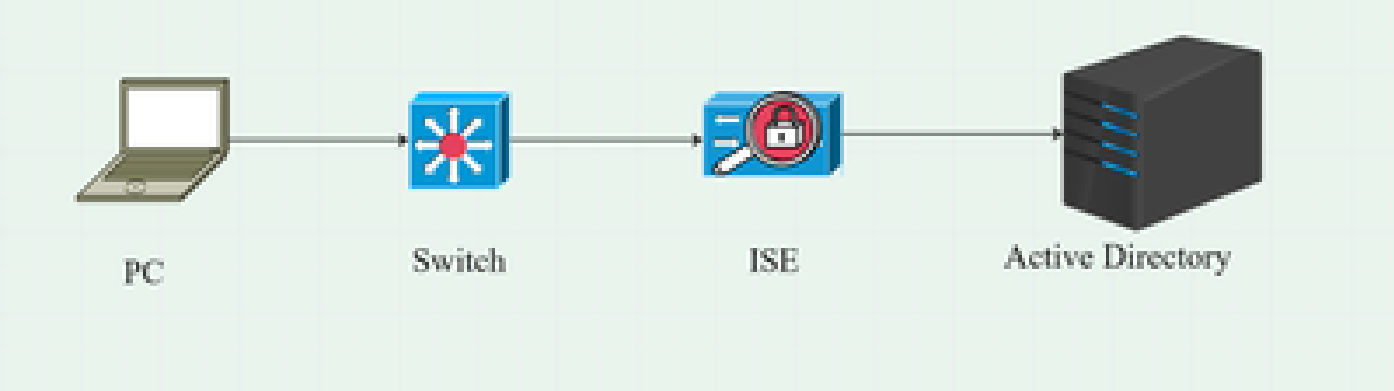
本文档中的信息基于以下软件和硬件版本：

- 思科ISE版本3.3及更高版本
- Windows 10及Cisco安全移动客户端5.1.4.74及更高版本
- 装有软件Cisco IOS® XE 17.6.5及更高版本的Cisco Catalyst 9200交换机
- Active Directory 2016

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

网络图



数据流

当PC连接到网络时，ISE提供重定向到终端安全评估门户的授权策略。
PC上的http流量被重定向到ISE客户端调配页面，在该页面中从ISE下载NSA应用。
然后，NSA在PC上安装安全客户端代理模块。
代理安装完成后，代理下载ISE上配置的状态配置文件和NAM配置文件。
安装NAM模块会触发PC上的重新启动。
重新启动后，NAM模块根据NAM配置文件执行EAP-FAST身份验证。
然后根据ISE终端安全评估策略触发终端安全评估扫描并检查合规性。

配置交换机

配置接入交换机的dot1x身份验证和重定向。

```
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服务器RAD1
address ipv4 <ISE server IP> auth-port 1812 acct-port 1813
key <secret-key>

dot1x system-auth-control
```

为要重定向到ISE客户端调配门户的用户配置重定向ACL。

```
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
```

在交换机上启用设备跟踪和http重定向。

```
device-tracking policy <设备跟踪策略名称>
 tracking enable
interface <interface name>
 device-tracking attach-policy <设备跟踪策略名称>

ip http server
ip http secure-server
```

下载安全客户端软件包

从software.cisco.com手动下载配置文件编辑器、安全客户端窗口和合规性模块webdeploy文件

在产品名称搜索栏中，键入Secure Client 5。

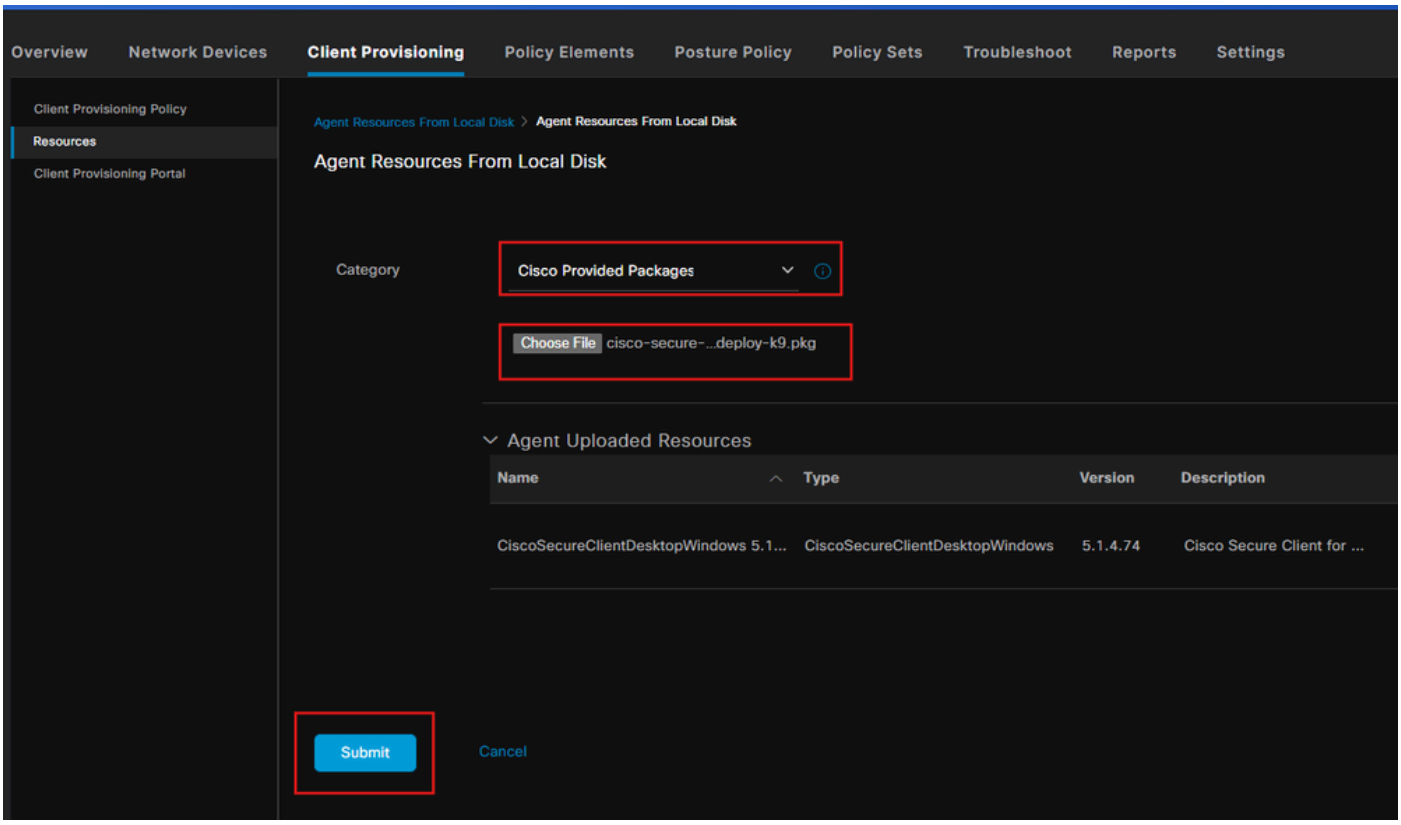
Downloads Home > Security > Endpoint Security > Secure Client (including AnyConnect) > Secure Client 5 > AnyConnect VPN Client Software

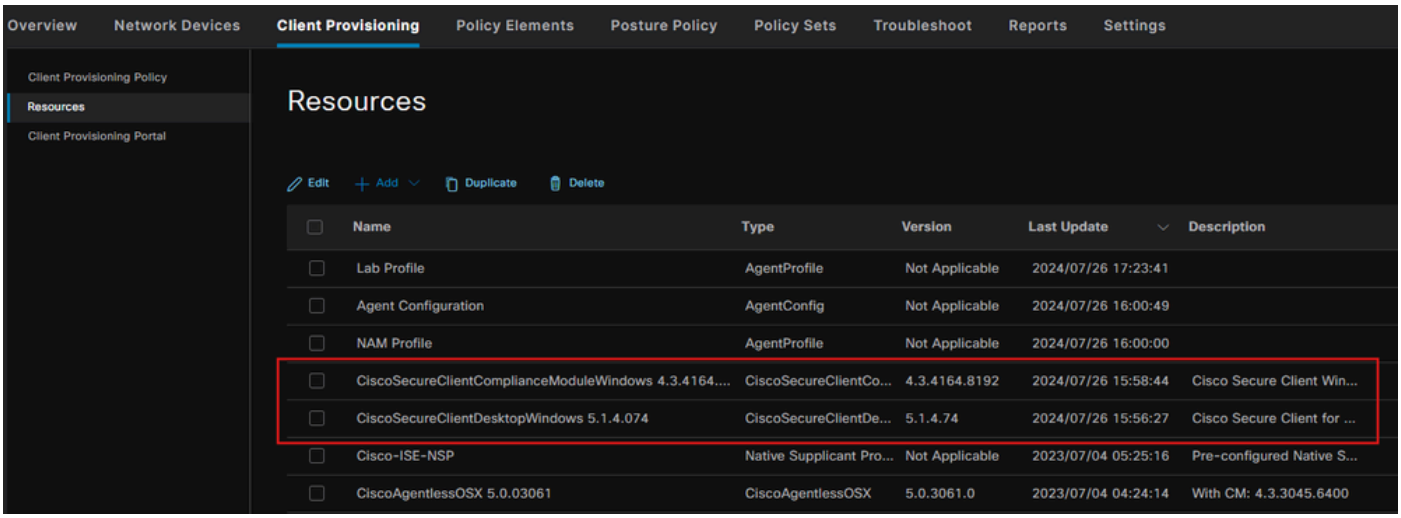
- cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg
- cisco-secure-client-win-4.3.4164.8192-isecompliance-webdeploy-k9.pkg
- tools-cisco-secure-client-win-5.1.4.74-profileeditor-k9.msi

ISE 配置

步骤1:在ISE上上传包

要在ISE上上传安全客户端和合规性模块webdeploy包，请导航到Workcenter > Posture > Client Provisioning > Resources > Add > Agent Resources from Local Disk。



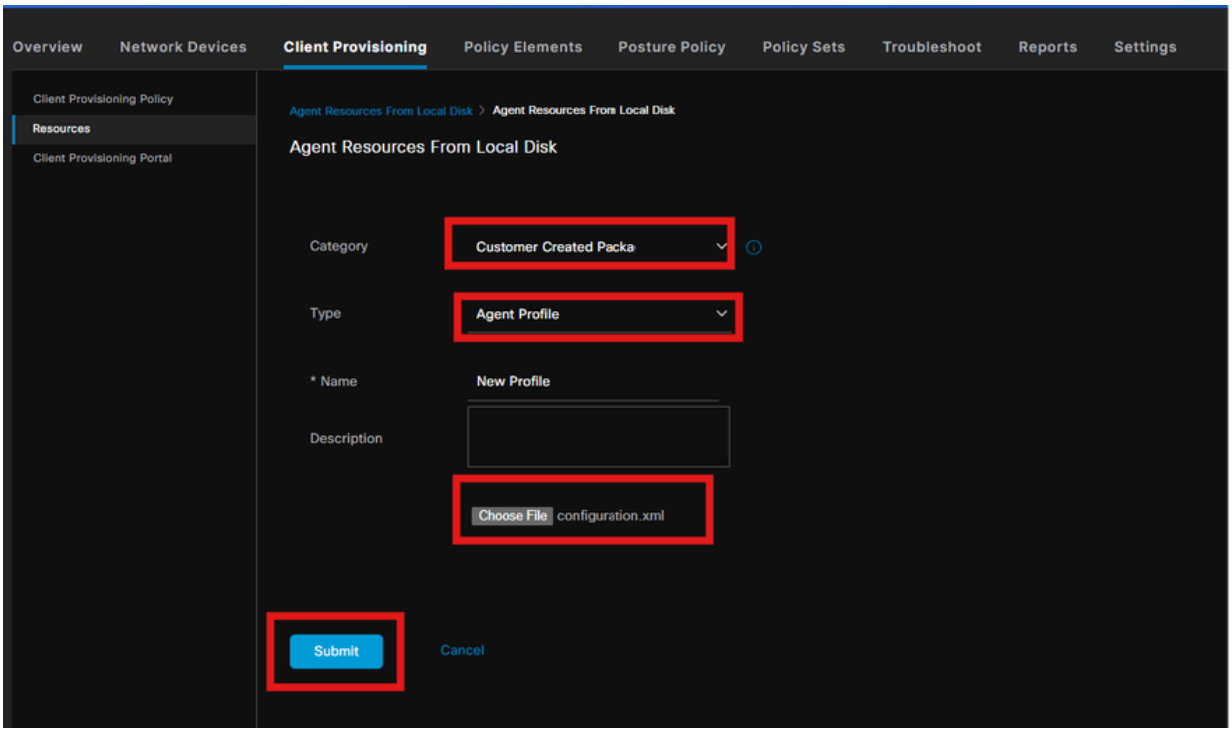


第二步：从配置文件编辑器工具创建NAM配置文件

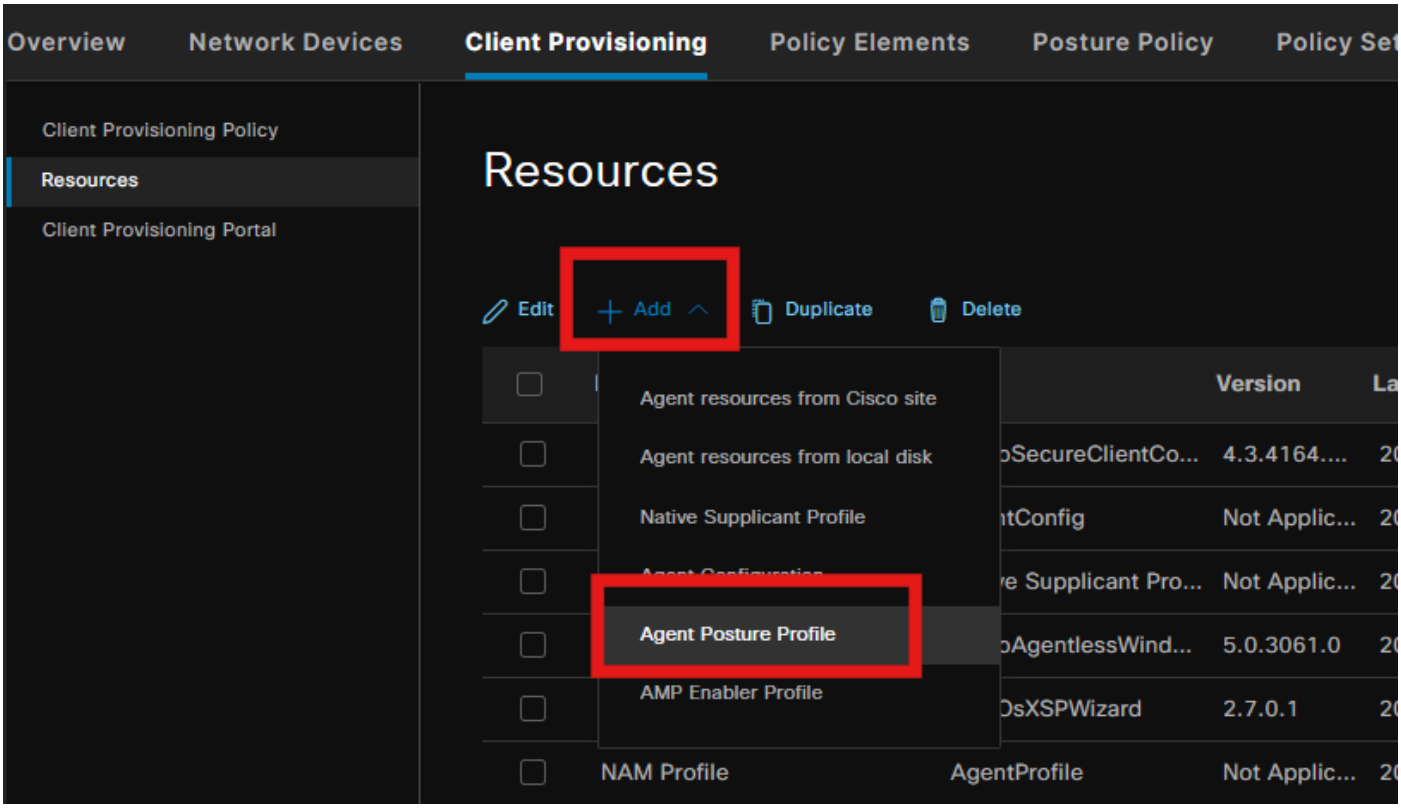
有关如何配置NAM配置文件的信息，请参阅本指南配置安全客户端NAM配置文件。

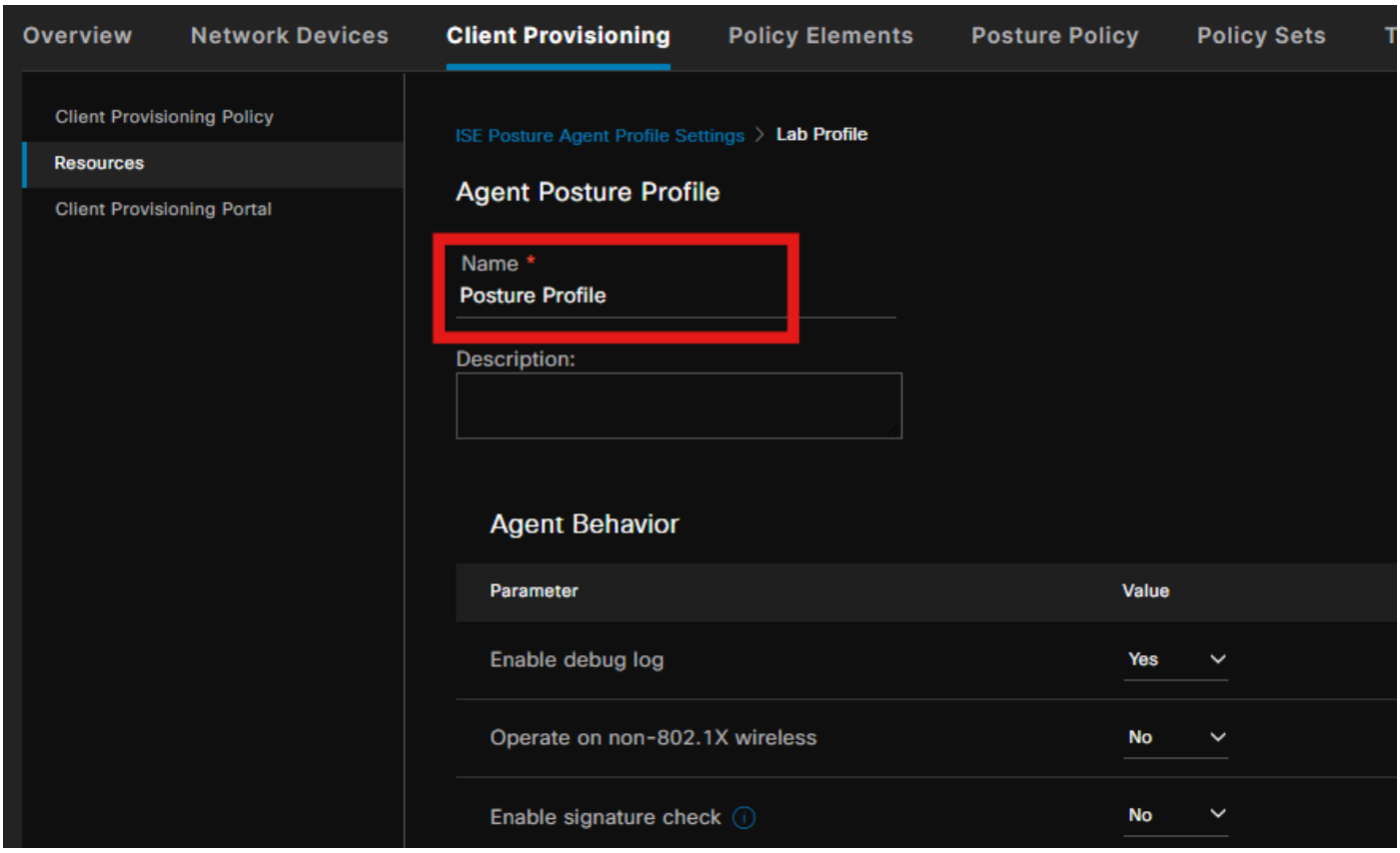
第三步：在ISE上上传NAM配置文件

要将NAM配置文件“Configuration.xml”作为代理配置文件上传到ISE上，请导航到客户端调配>资源>来自本地磁盘的代理资源。



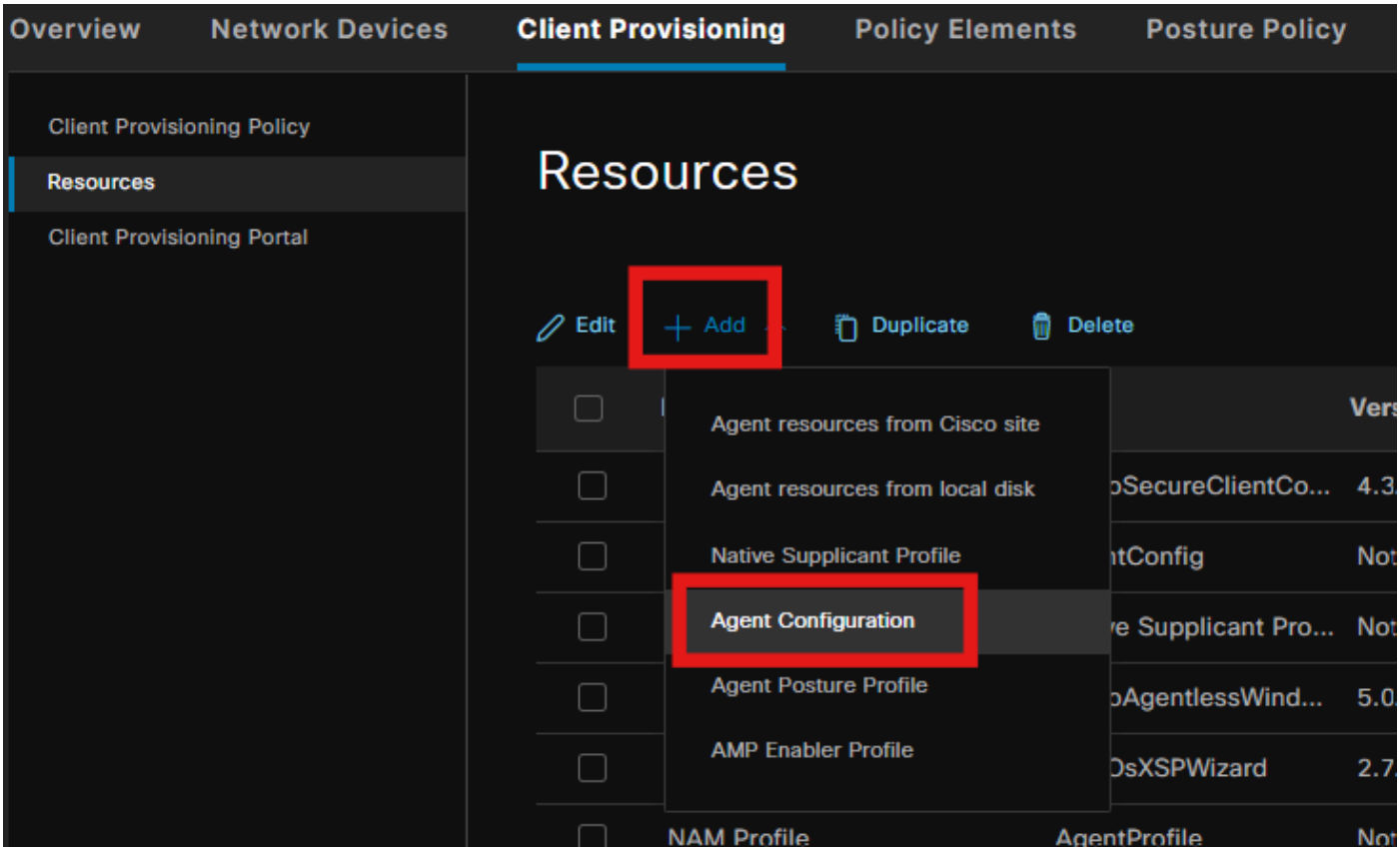
第四步：创建安全评估配置文件



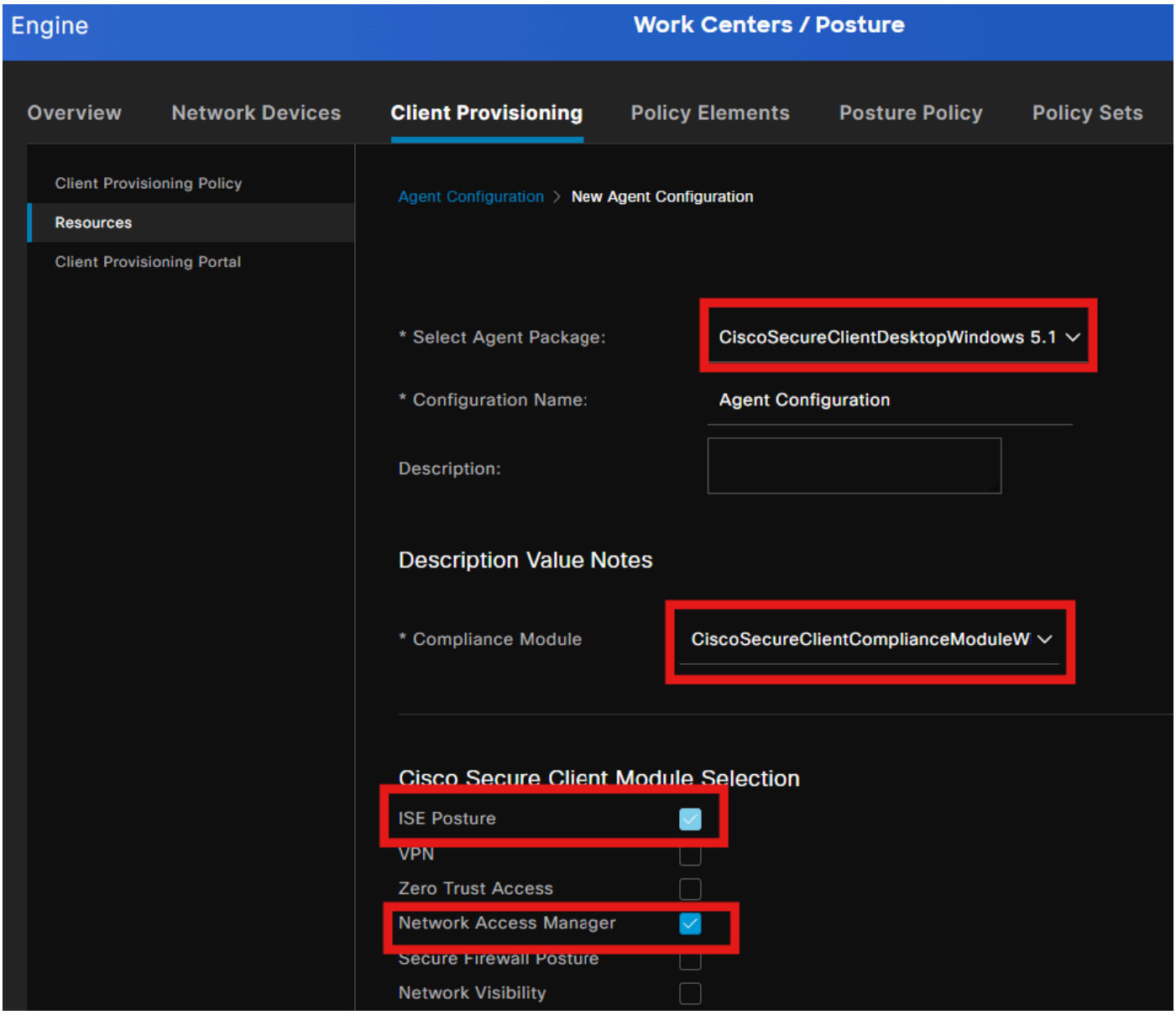


在Posture Protocol部分，不要忘记添加*以允许代理连接到所有服务器。

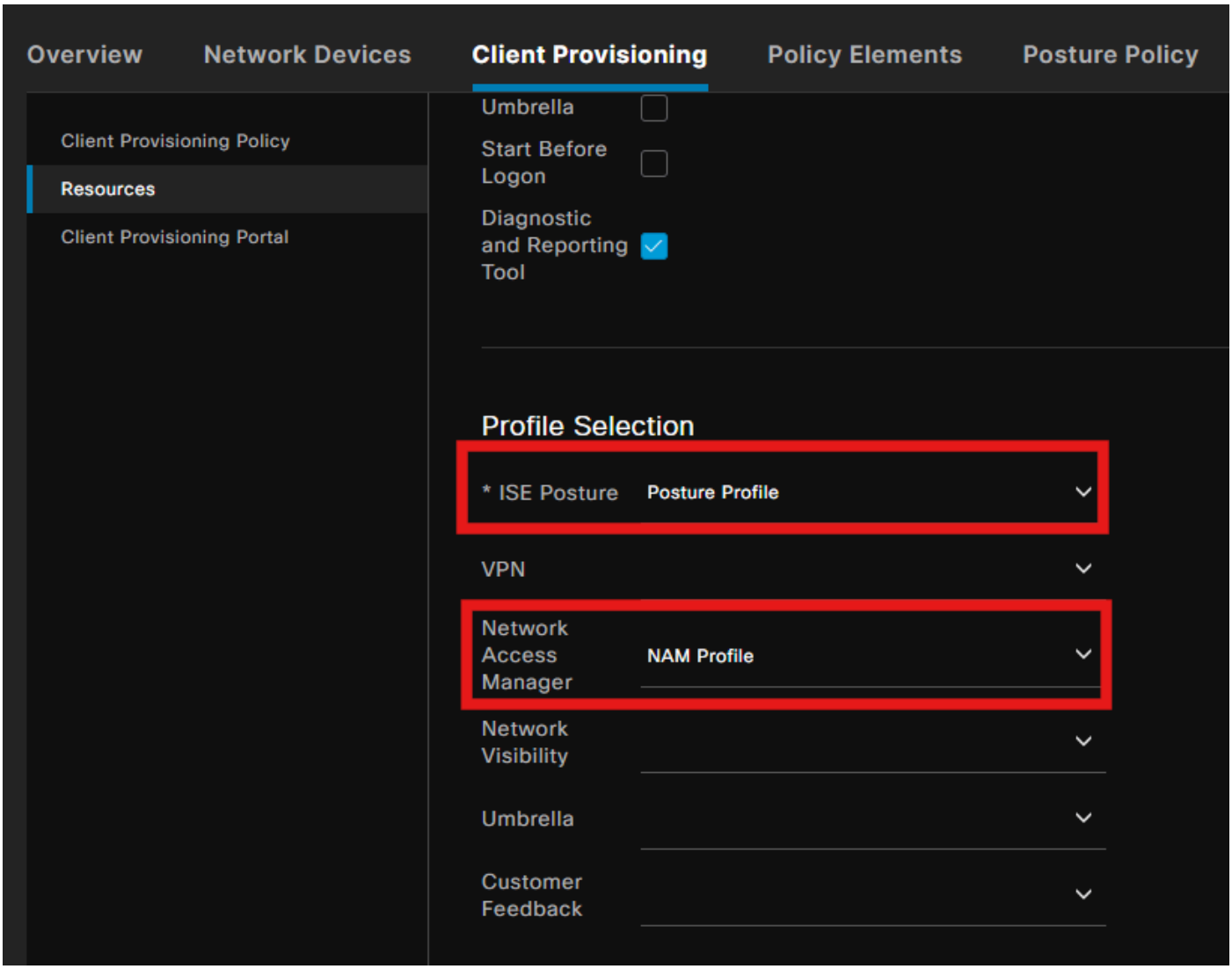
第五步：创建代理配置



选择上传的安全客户端和合规性模块包，然后在Module selection下选择ISE Posture、NAM和DART模块

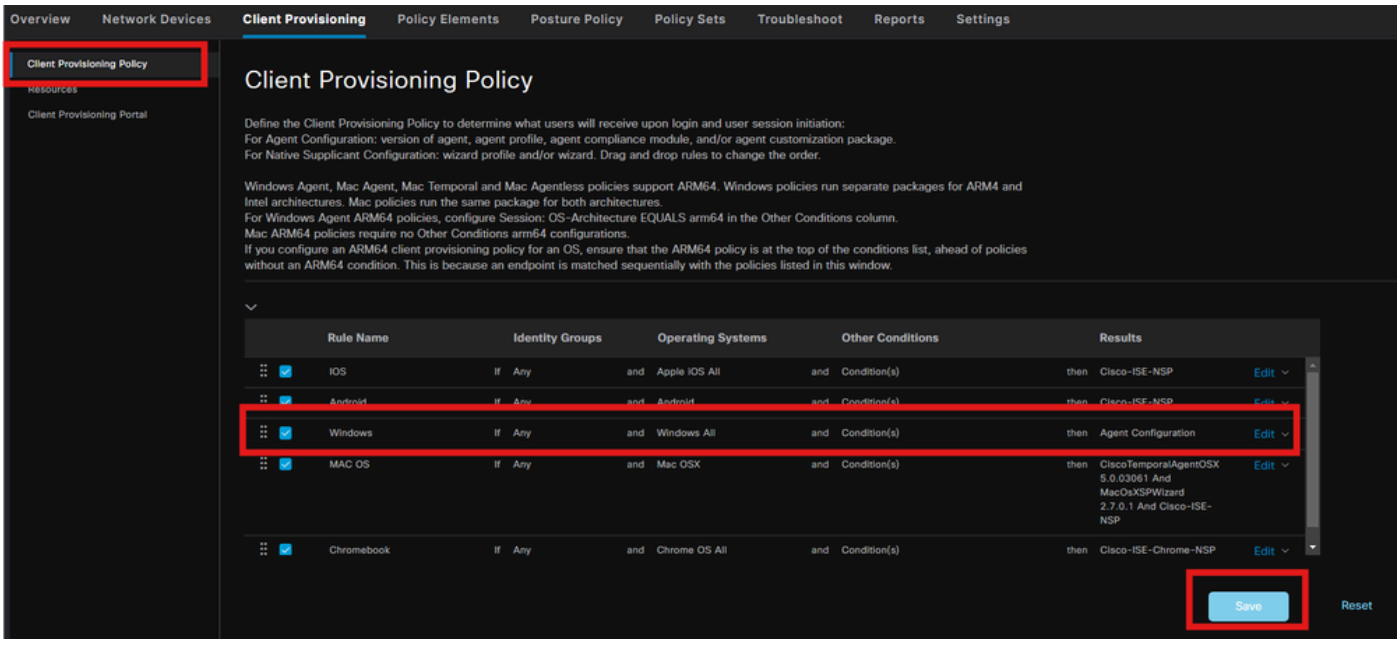


在Profile下，选择Posture和NAM配置文件，并单击Submit。



第六步：客户端调配策略

为Windows操作系统创建客户端调配策略，并选择上一步中创建的代理配置。

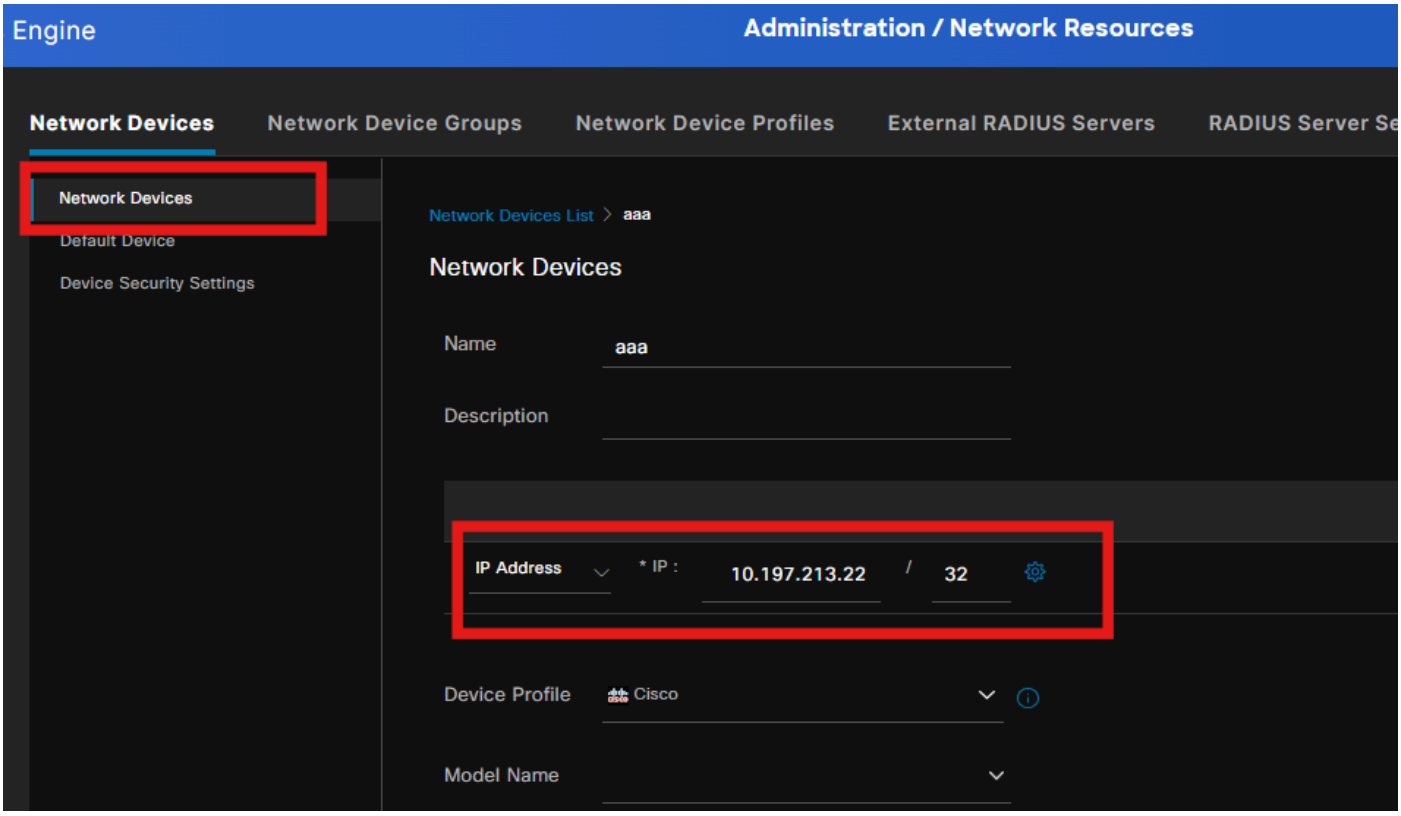


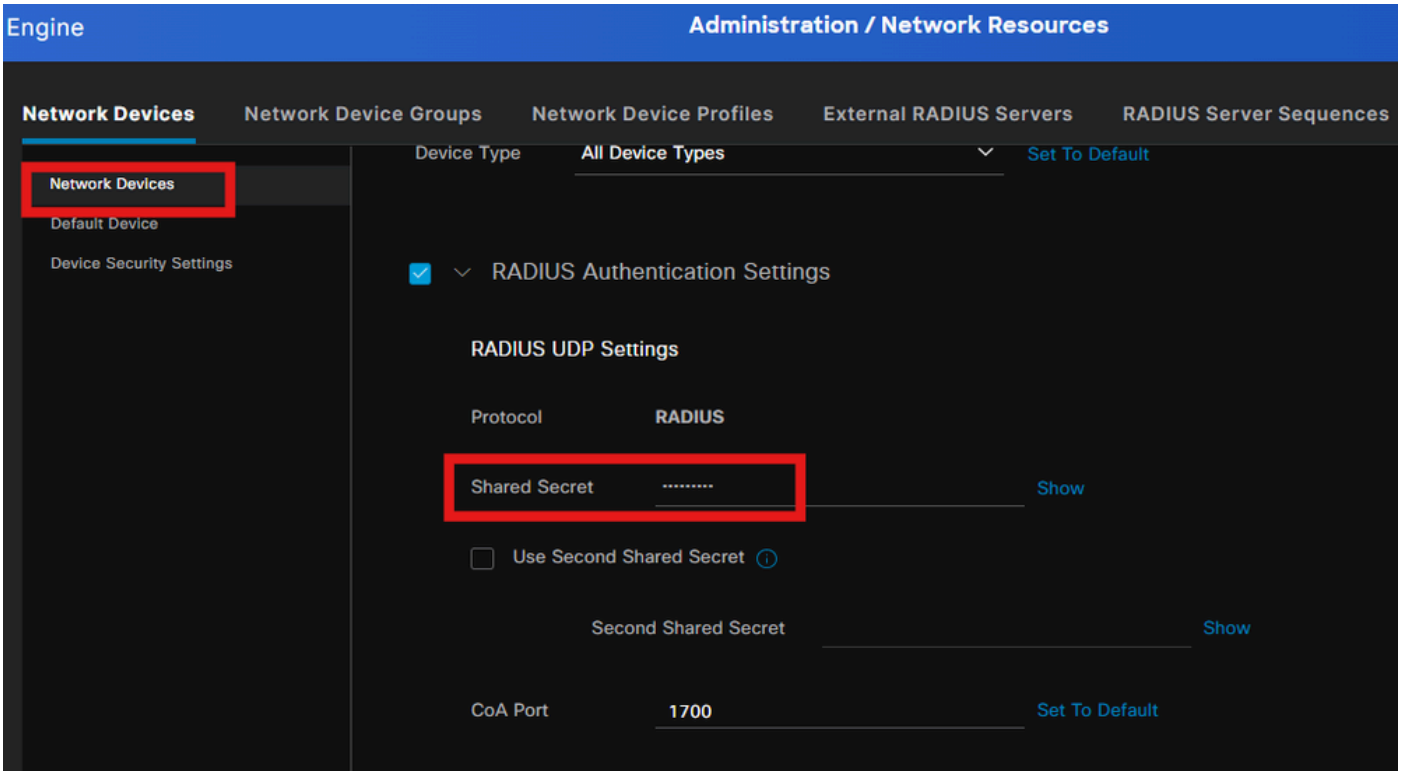
步骤 7.安全评估策略

有关如何创建终端安全评估策略和条件的信息，请参阅本指南ISE终端安全评估规范部署指南。

步骤 8添加网络设备

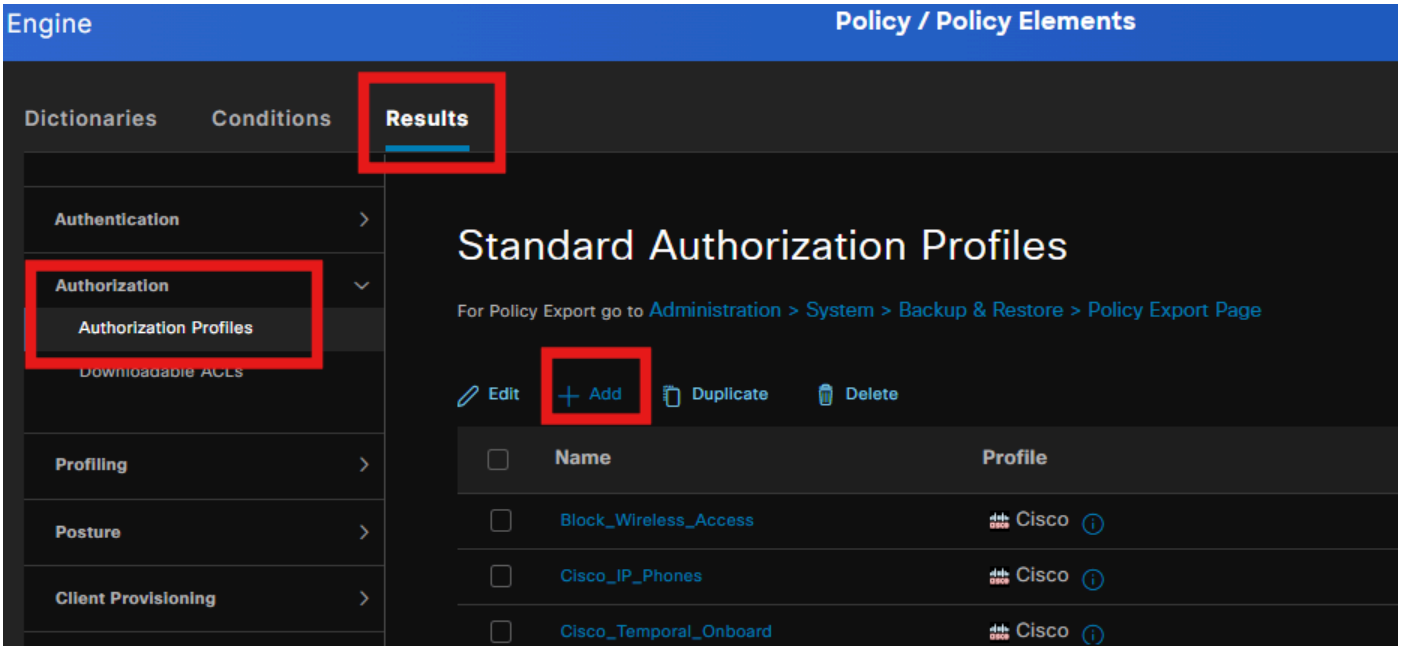
要添加交换机IP地址和RADIUS共享密钥，请导航到Administration > Network Resources。



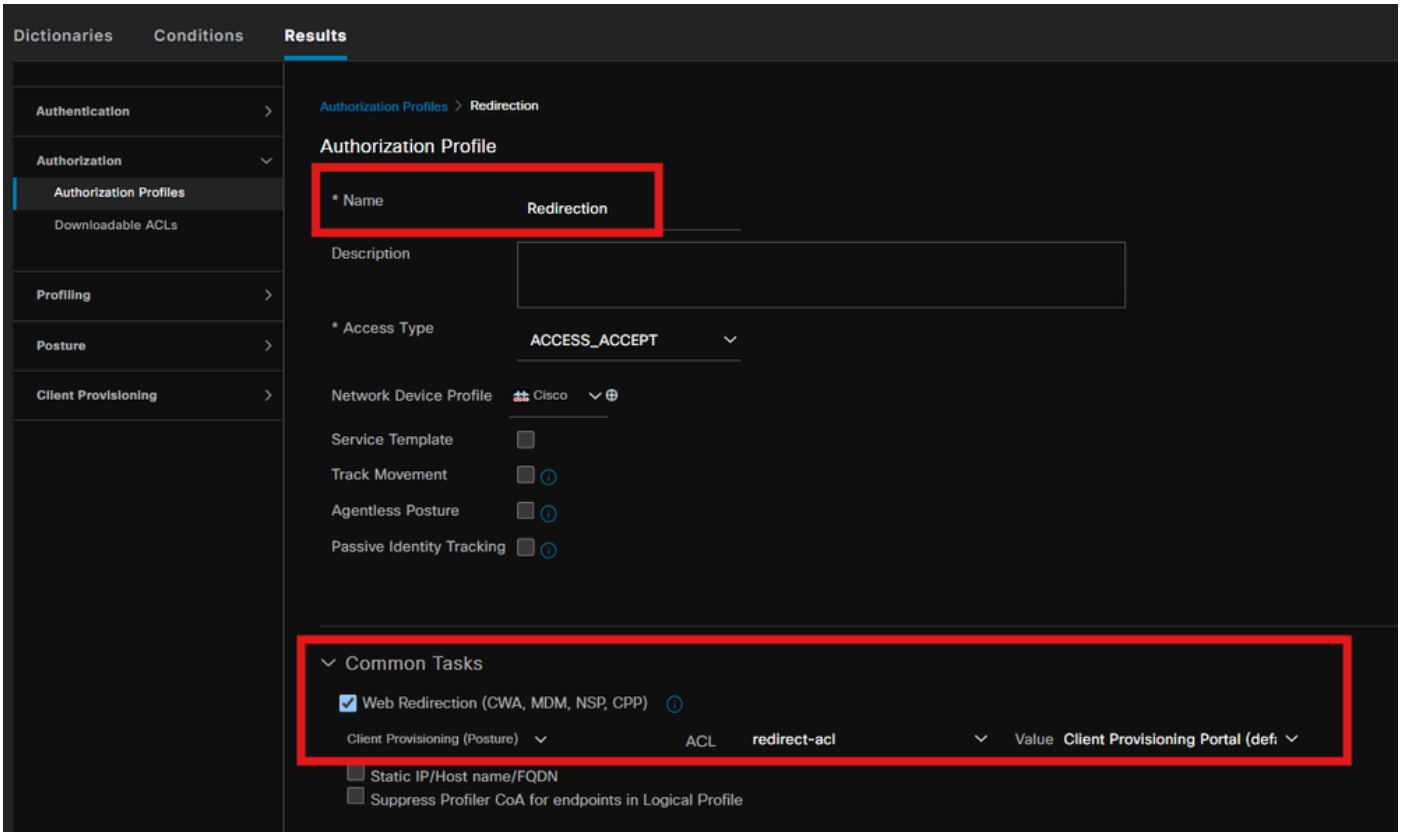


步骤 9授权配置文件

要创建状态重定向配置文件，请导航到Policy > Policy Elements > Results。

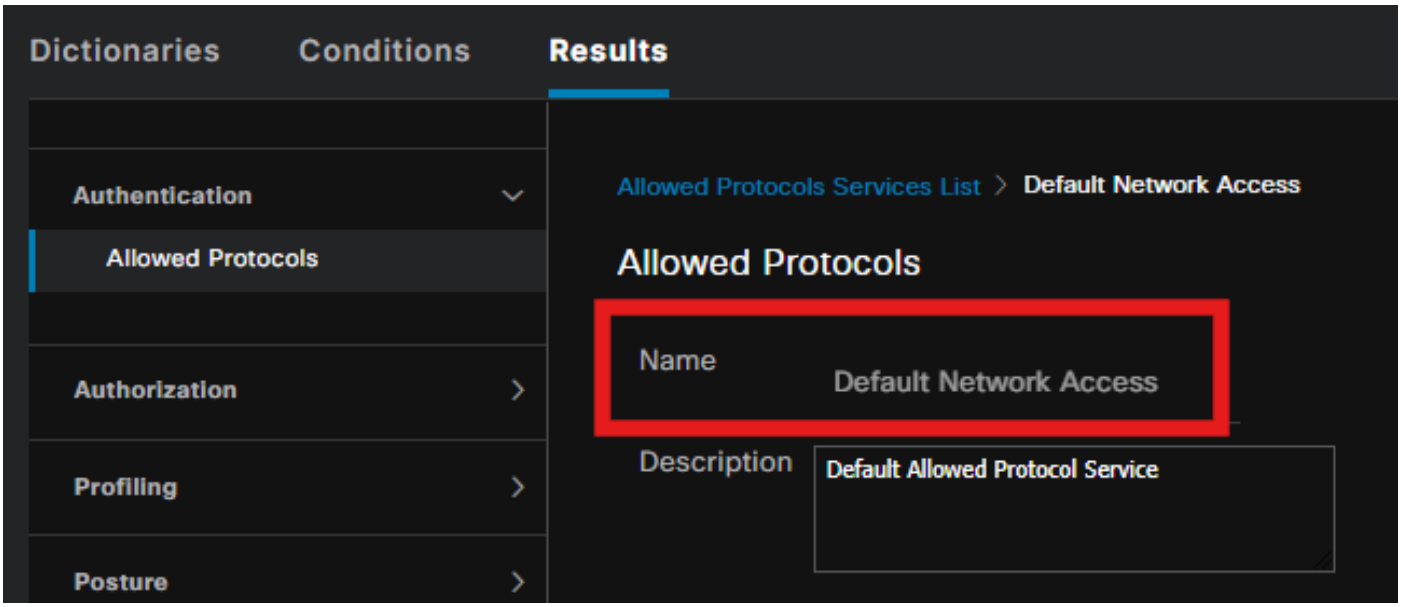


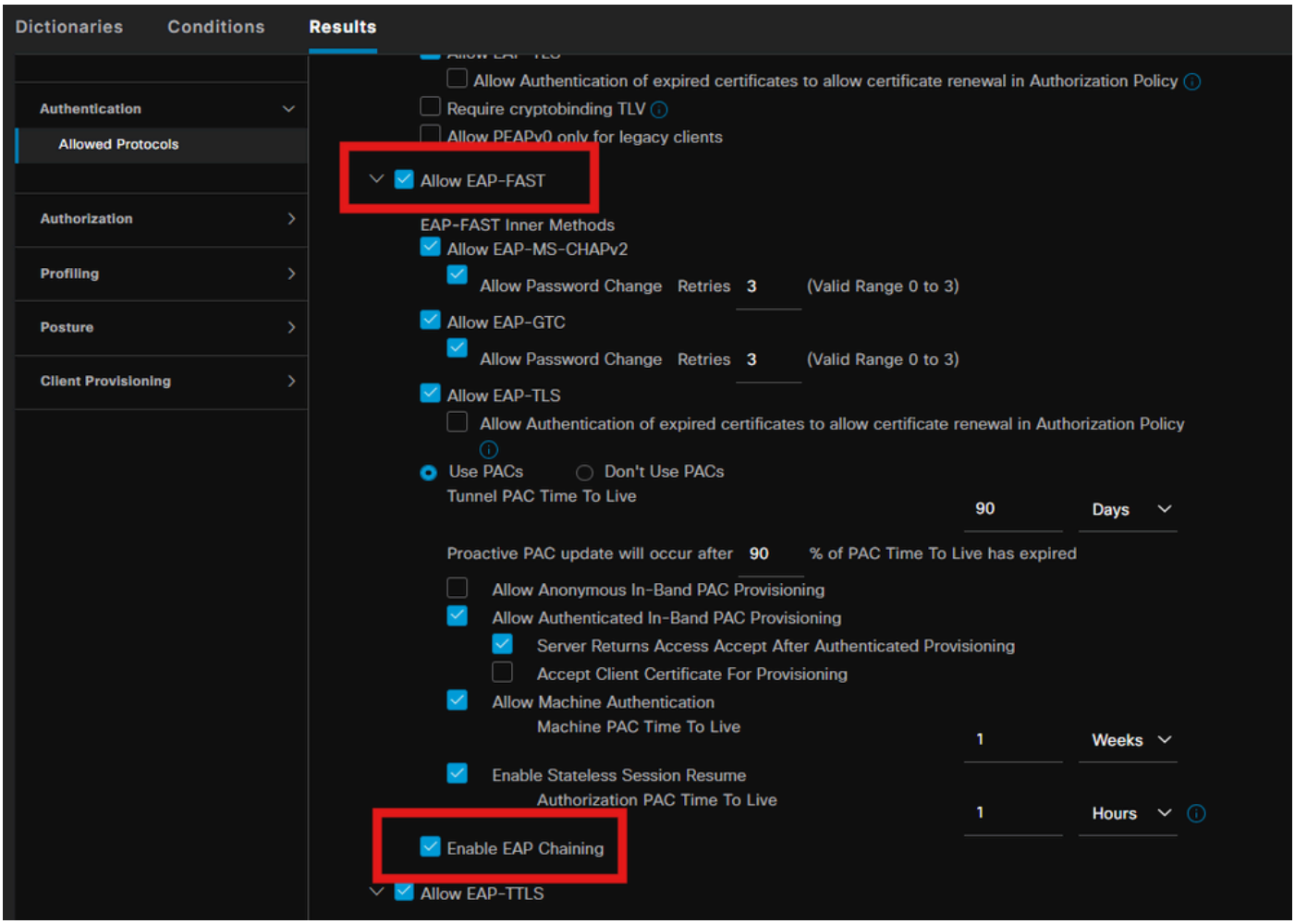
在command task下，选择client Provisioning Portal with redirect ACL。



步骤 10允许的协议

导航到策略>策略元素>结果>身份验证>允许的协议，选择EAP链接设置，

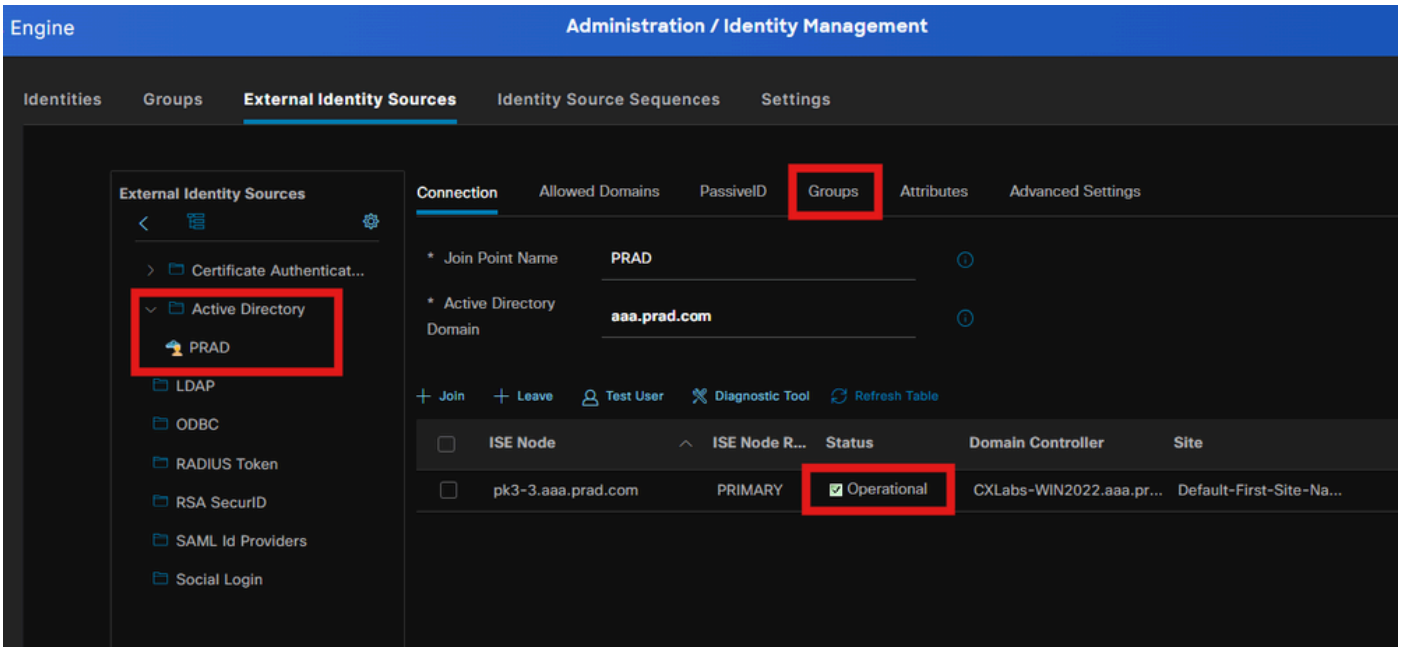




步骤 11Active Directory

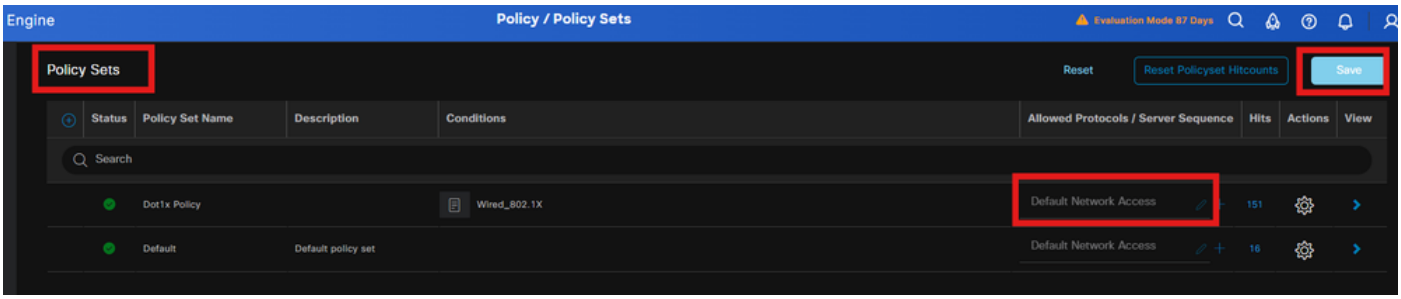
验证ISE已加入Active directory域，并且如果授权条件需要，会选择域组。

管理>身份管理>外部身份源> Active Directory

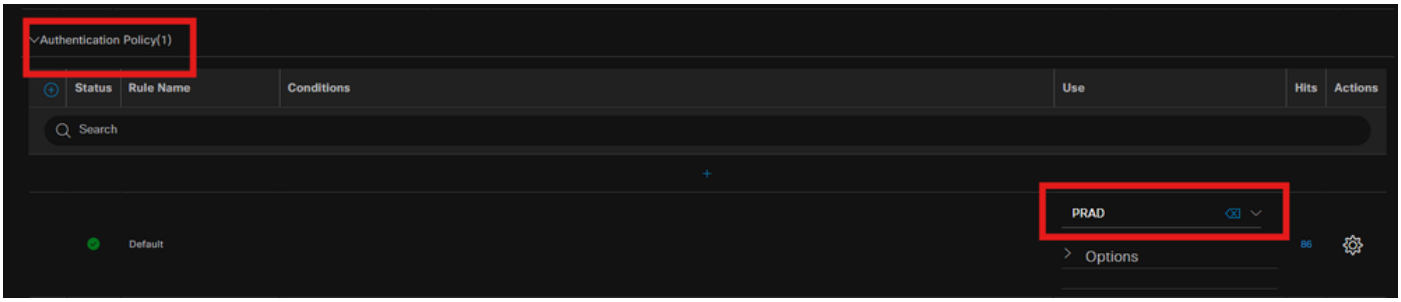


步骤 12策略集

在ISE上创建策略集，对dot1x请求进行身份验证。导航到策略>策略集。



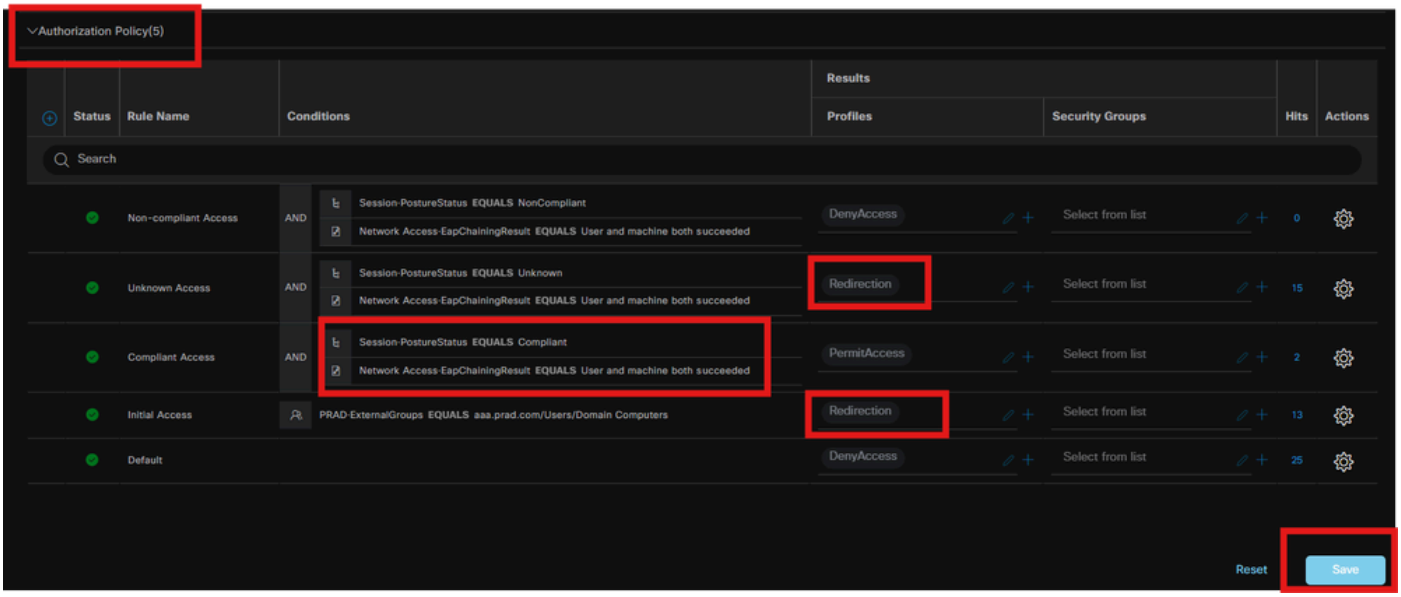
选择Active directory作为身份验证策略的身份源。



根据状态未知、不合规和合规配置不同的授权规则。

在此使用案例中。

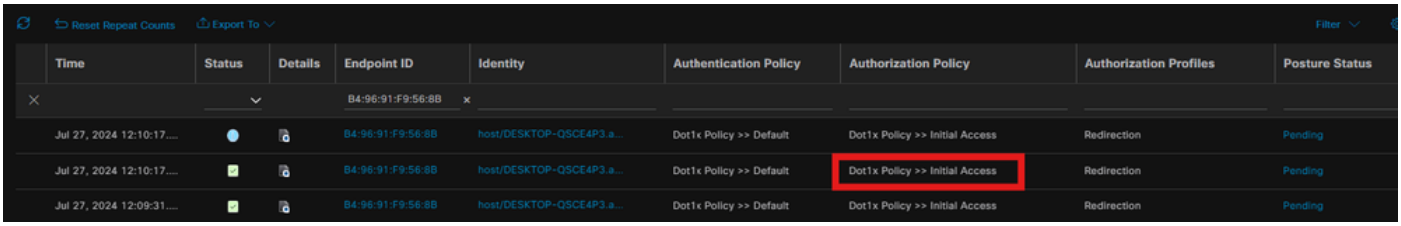
- 初始访问：重定向至ISE客户端调配门户以安装安全客户端代理和NAM配置文件
- 未知访问：访问客户端调配门户以进行基于重定向的状态发现
- 合规访问：完全网络访问
- 不合规：拒绝访问



验证

步骤1:从ISE下载并安装安全客户端状态/NAM模块

选择通过dot1x身份验证的终端，点击“初始访问”授权规则。导航到操作> Radius >实时日志



在交换机上，指定应用于终端的重定向URL和ACL。

```
Switch#show authentication session interface te1/0/24 details
接口：TenGigabitEthernet1/0/24
IIF-ID：0x19262768
MAC地址：x4x6.xxxx.xxxx
IPv6地址：未知
IPv4地址：<client-IP>
用户名：host/DESKTOP-xxxxxx.aaa.prad.com
状态：已授权
域：数据
操作主机模式：单主机
操作控制目录：两者
会话超时：不适用
通用会话ID：16D5C50A0000002CF067366B
计费会话ID：0x0000001f
句柄：0x7a000017
当前策略：POLICY_Te1/0/24
```

本地策略：
服务模板：DEFAULT_LINKSEC_POLICY_SHOULD_SECURE（优先级150）
安全策略：应确保
安全状态：链路不安全

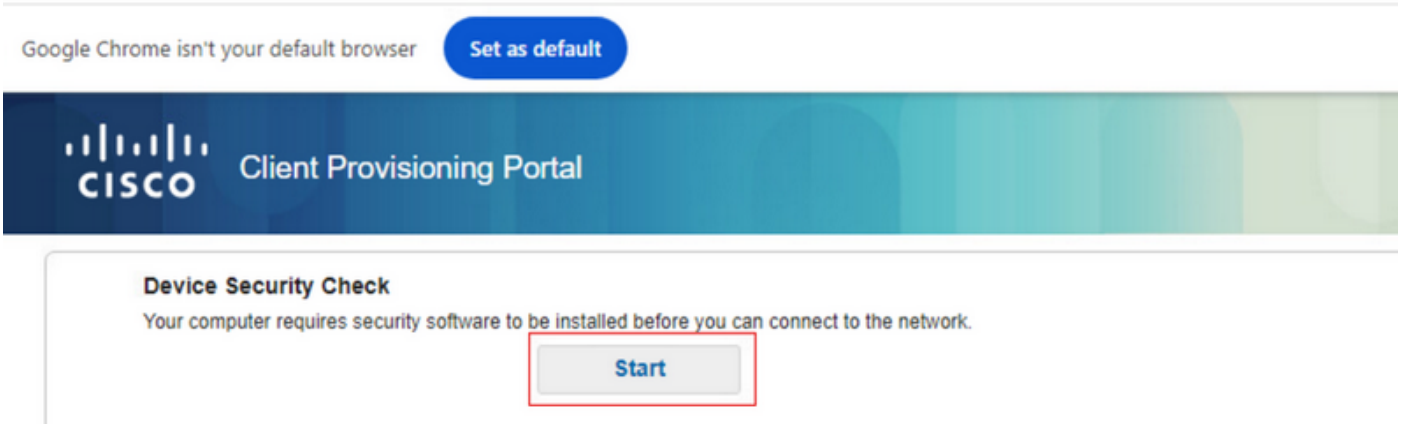
服务器策略：
URL重定向ACL：redirect-acl
URL重定向
：https://ise33.aaa.prad.com:8443/portal/gateway?sessionId=16D5C50A0000002CF067366A&portal=ee
7180-4995-8aa2-9fb282645a8f&action=cpp&token=518f857900a37f9afc6d2da8b6fe3bc2
ACS ACL：xACSACLx-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3

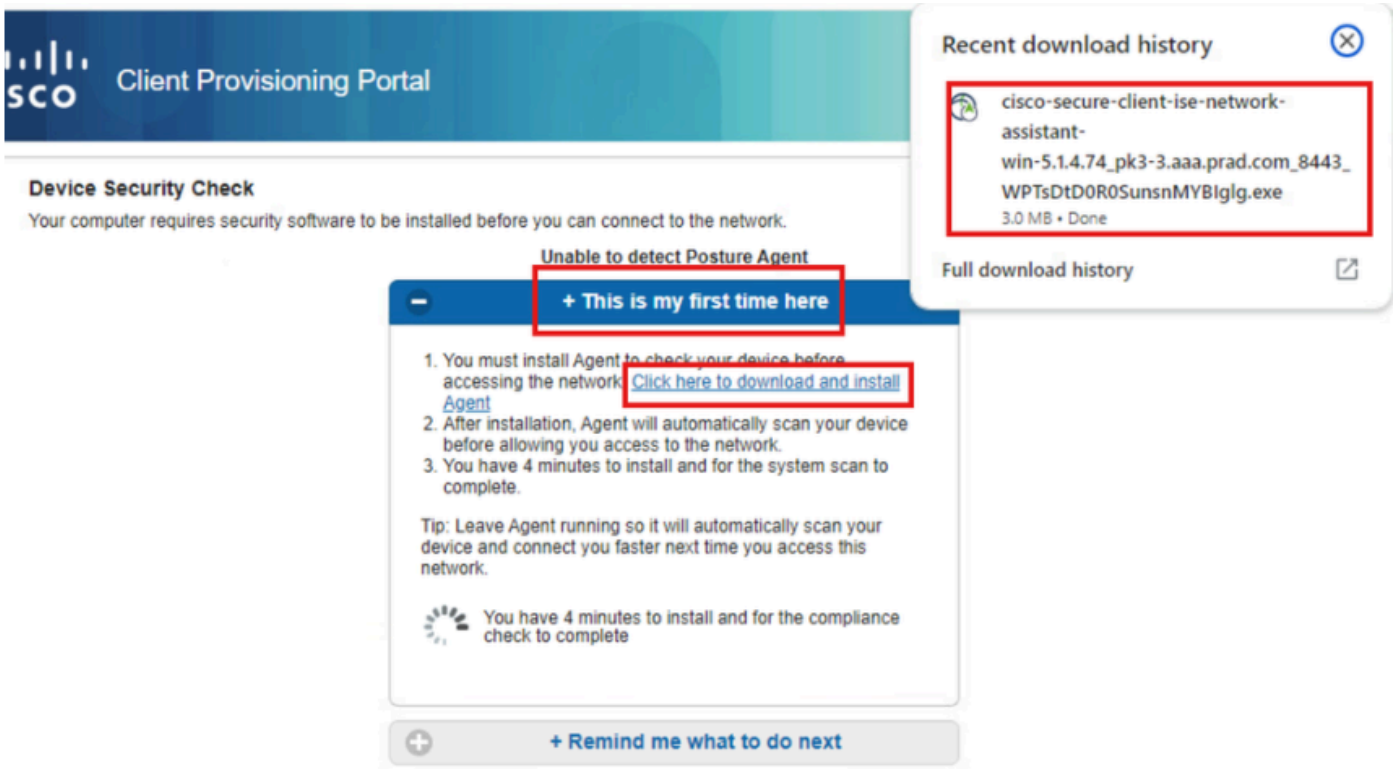
方法状态列表：
方法状态
dot1x身份验证成功

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

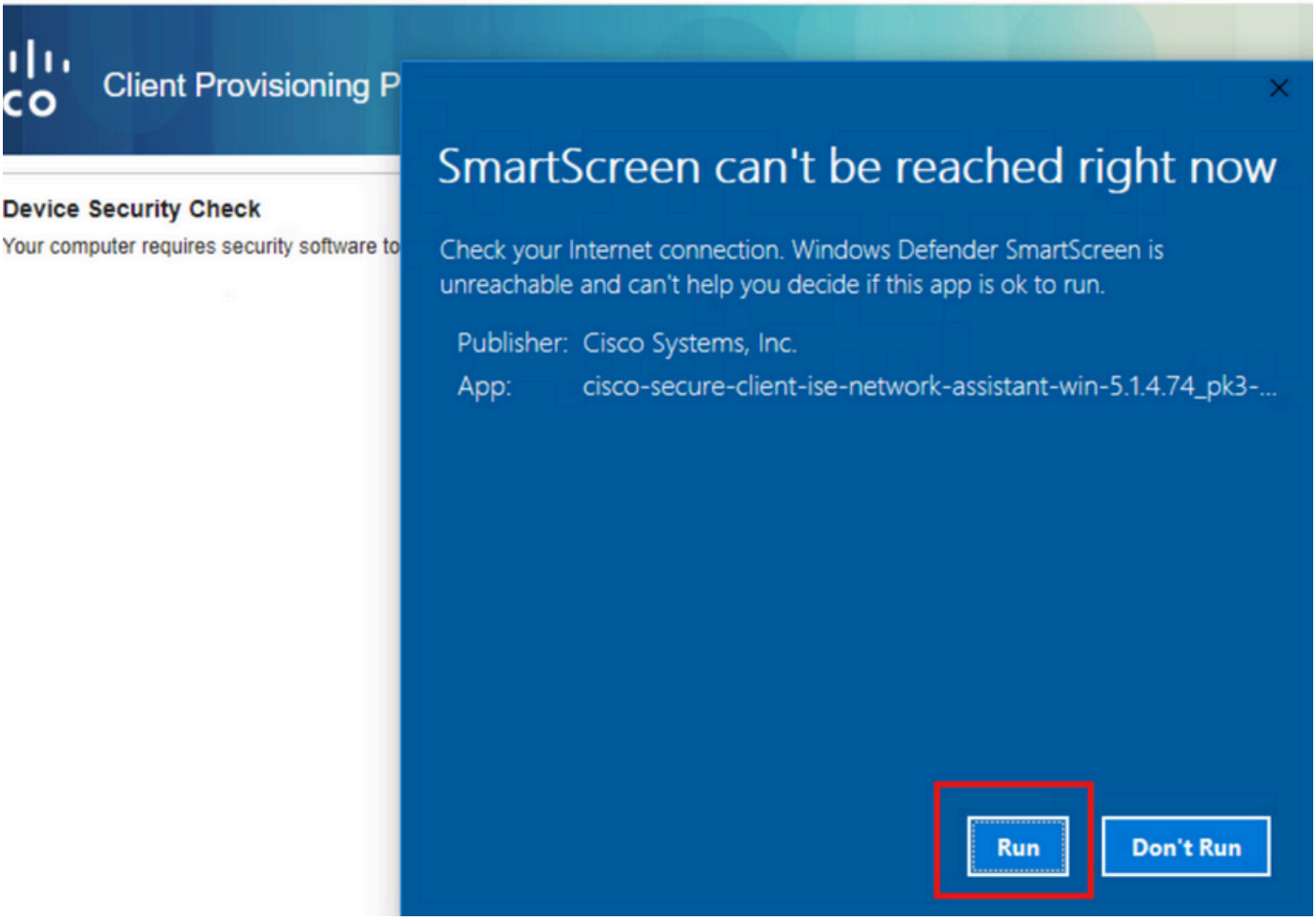
网络层地址链路层地址接口VLAN端口老化状态剩余时间
ARP X.X.X.X b496.91f9.568b Te1/0/24 1000 0005 4mn可访问39秒尝试0

在终端上，验证重定向到ISE终端安全评估的数据流，并单击Start以下载终端上的网络设置助手。



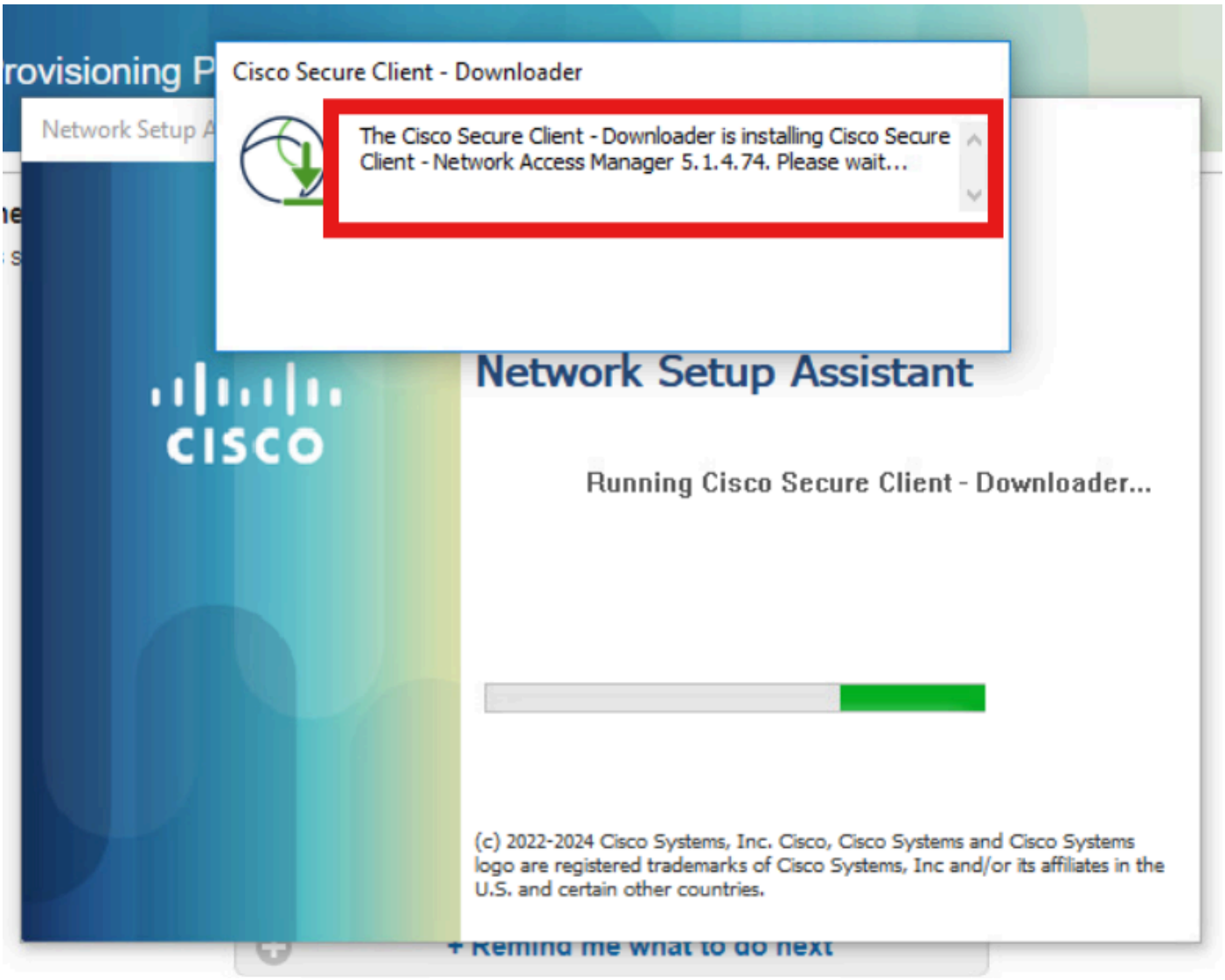


单击Run以安装NSA应用程序。

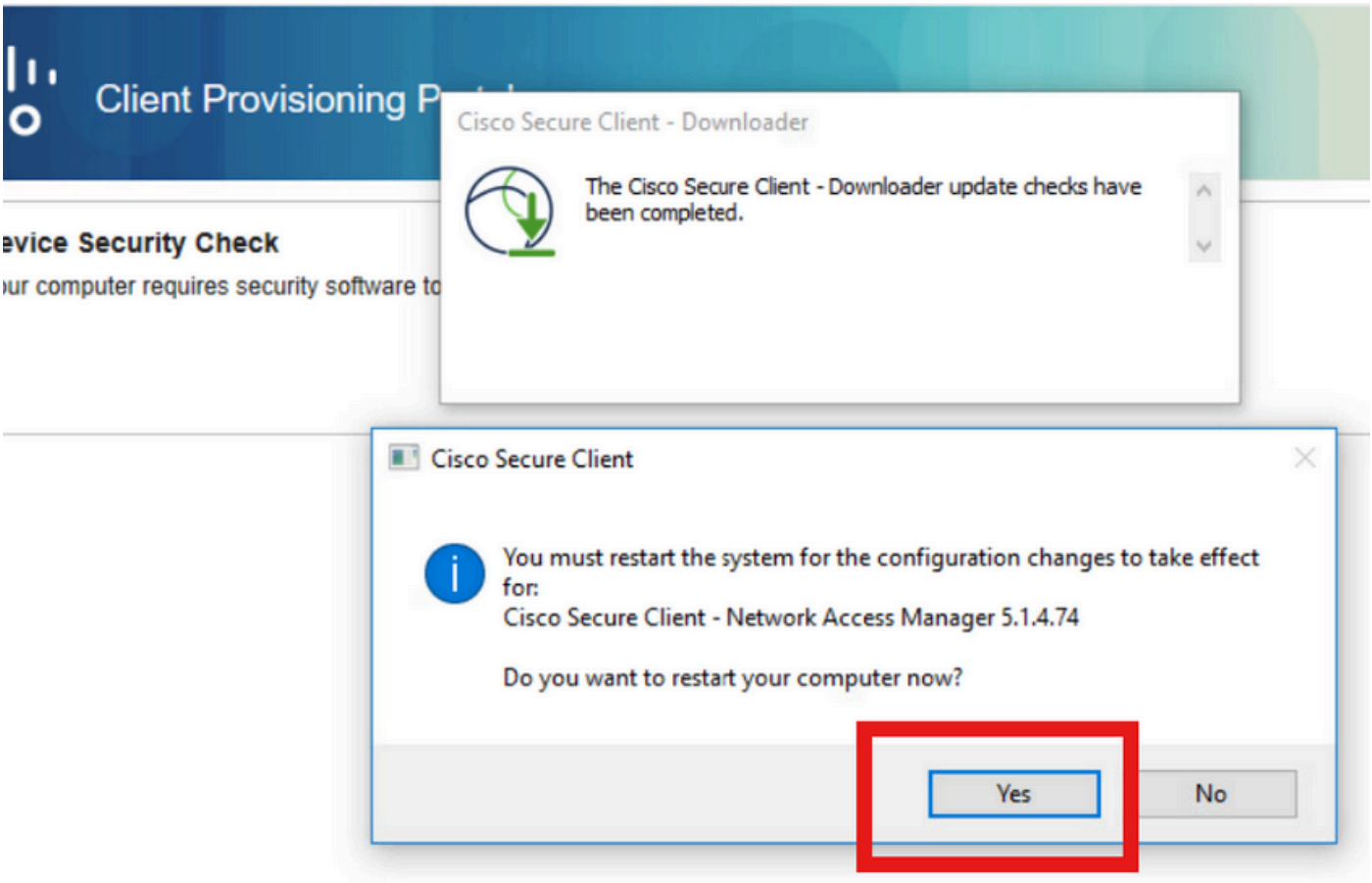


现在，NSA从ISE调用安全客户端代理下载并安装终端安全评估、NAM模块和NAM配置文件

configuration.xml。



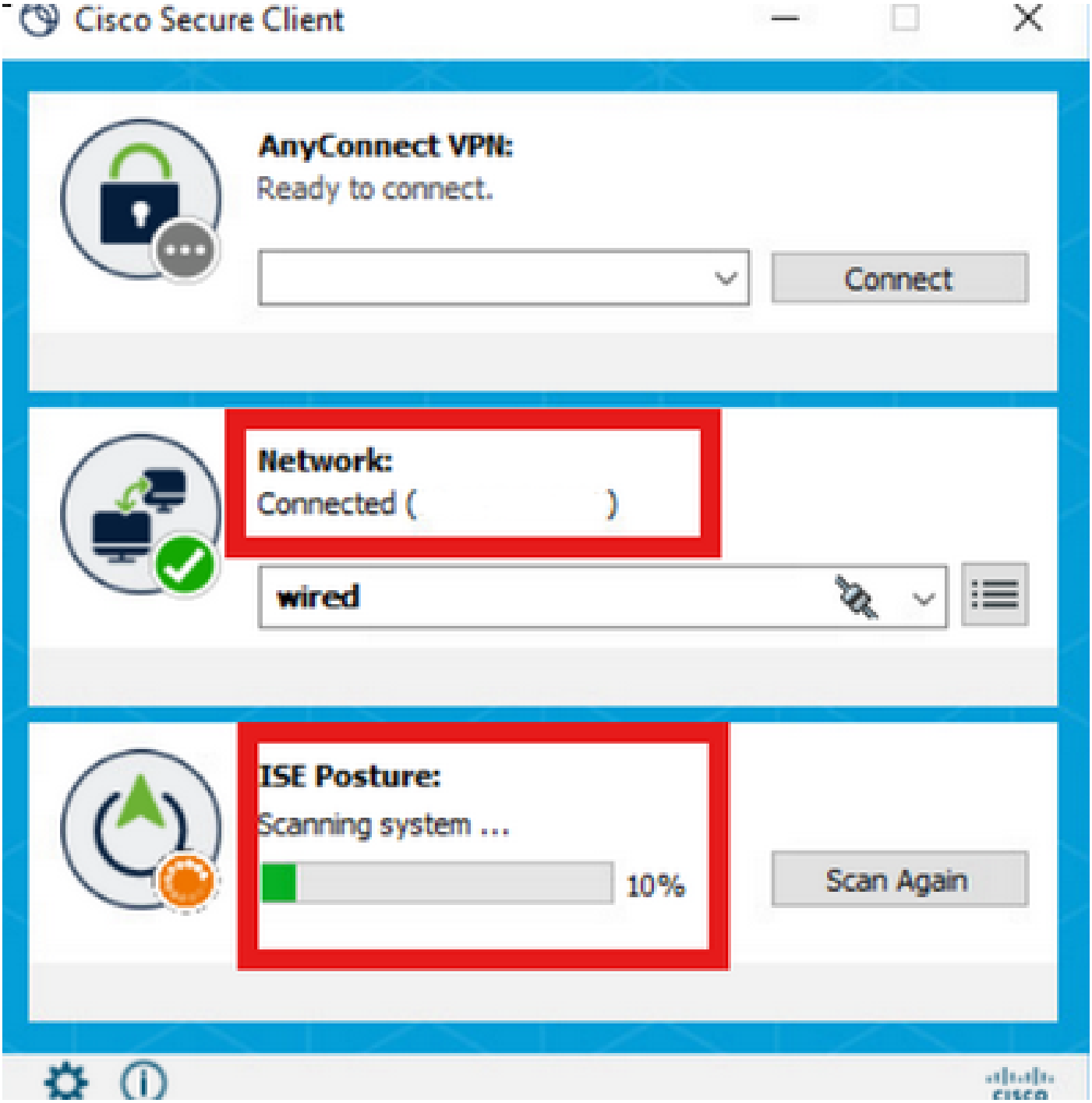
安装NAM后触发重新启动提示。单击 Yes。



第二步：EAP-FAST

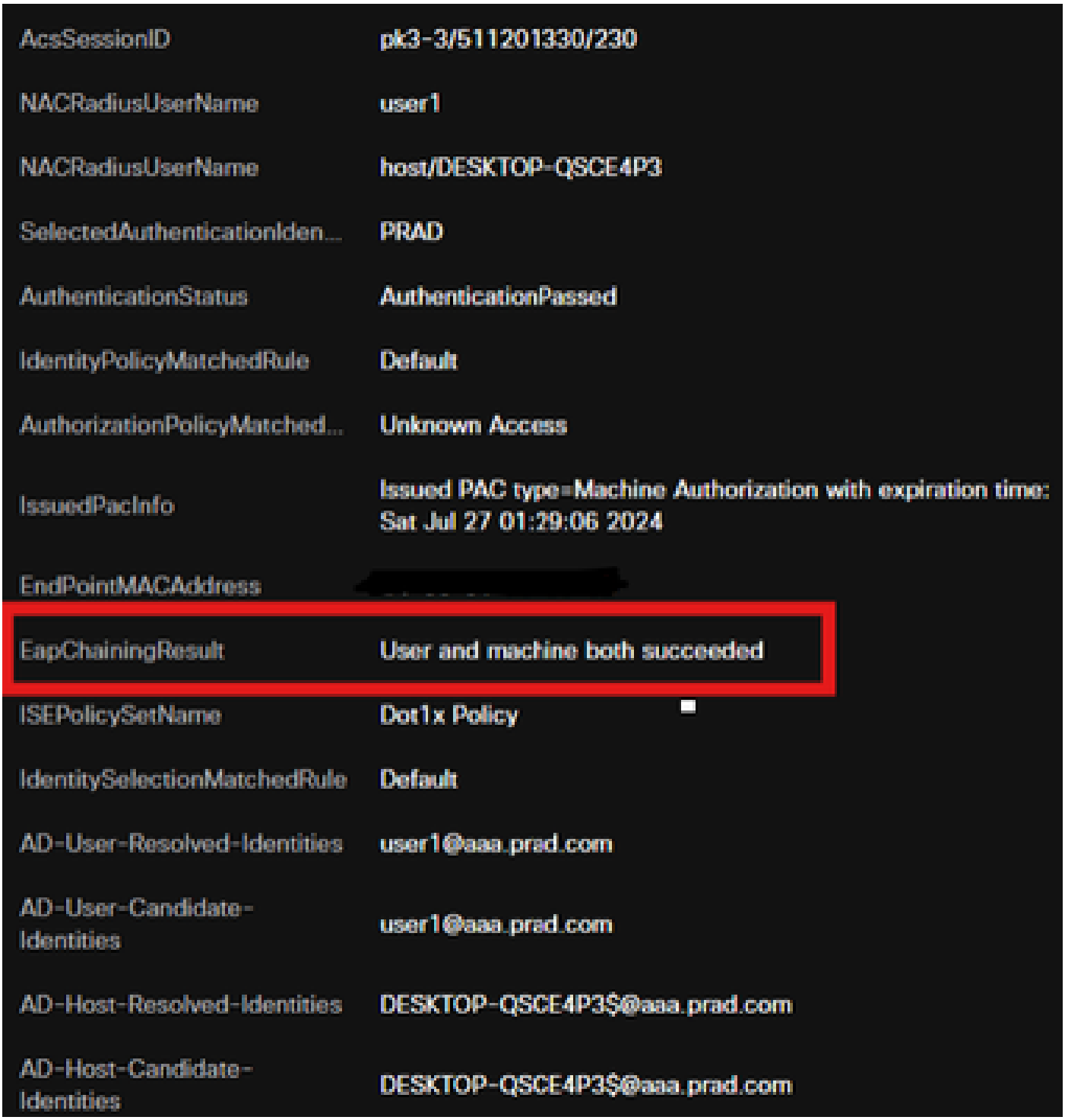
PC重新启动且用户登录后，NAM将通过EAP-FAST对用户和计算机进行身份验证。

如果终端身份验证正确，NAM显示其已连接，并且状态模块触发状态扫描。



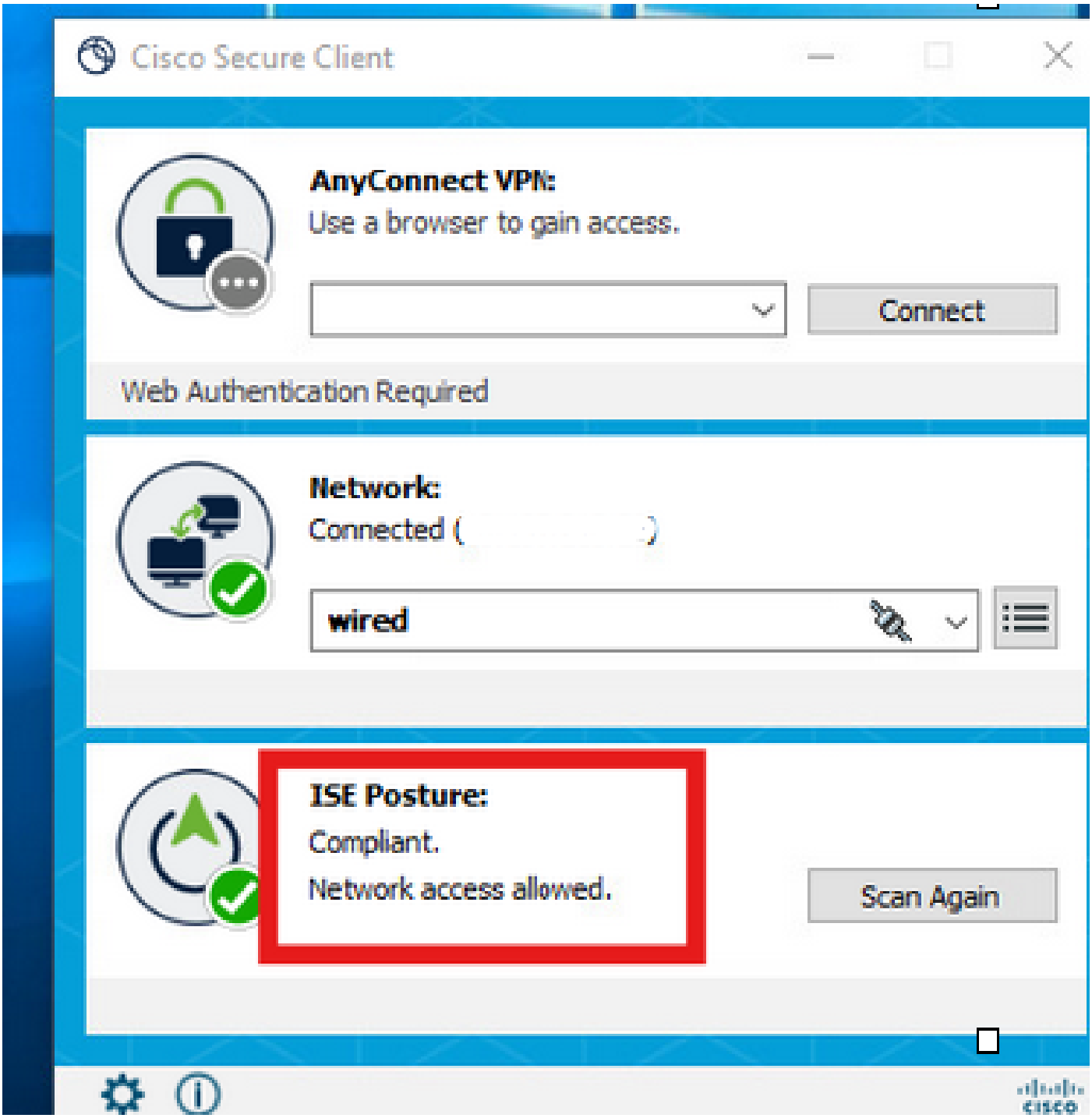
在ISE实时日志中，终端现在触发未知访问规则。

现在，身份验证协议基于NAM配置文件配置为EAP-FAST，EAP-Chaining结果为“成功”。

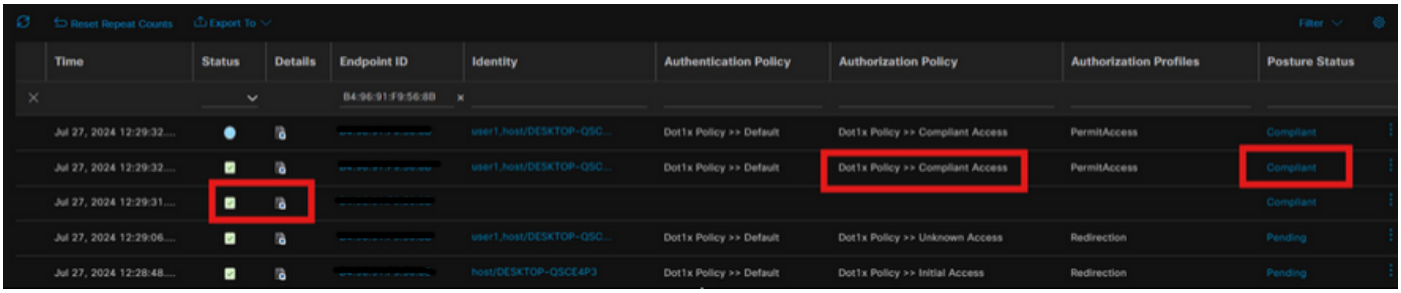


第三步：状态扫描

安全客户端安全评估模块触发安全评估扫描并根据ISE安全评估策略标记为投诉。



CoA在终端安全评估扫描后触发，现在终端达到投诉访问策略。

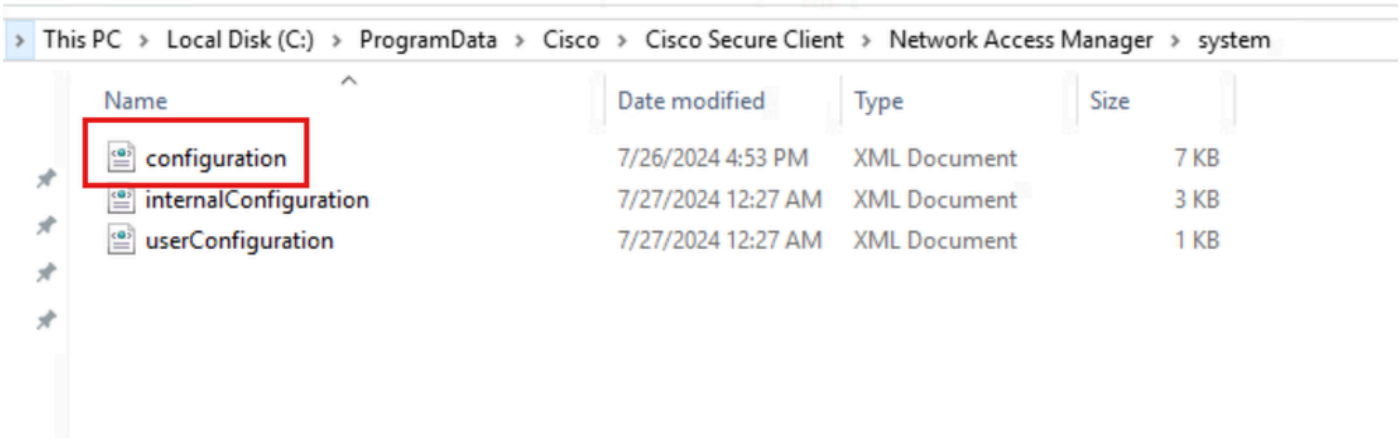


故障排除

步骤1:NAM配置文件

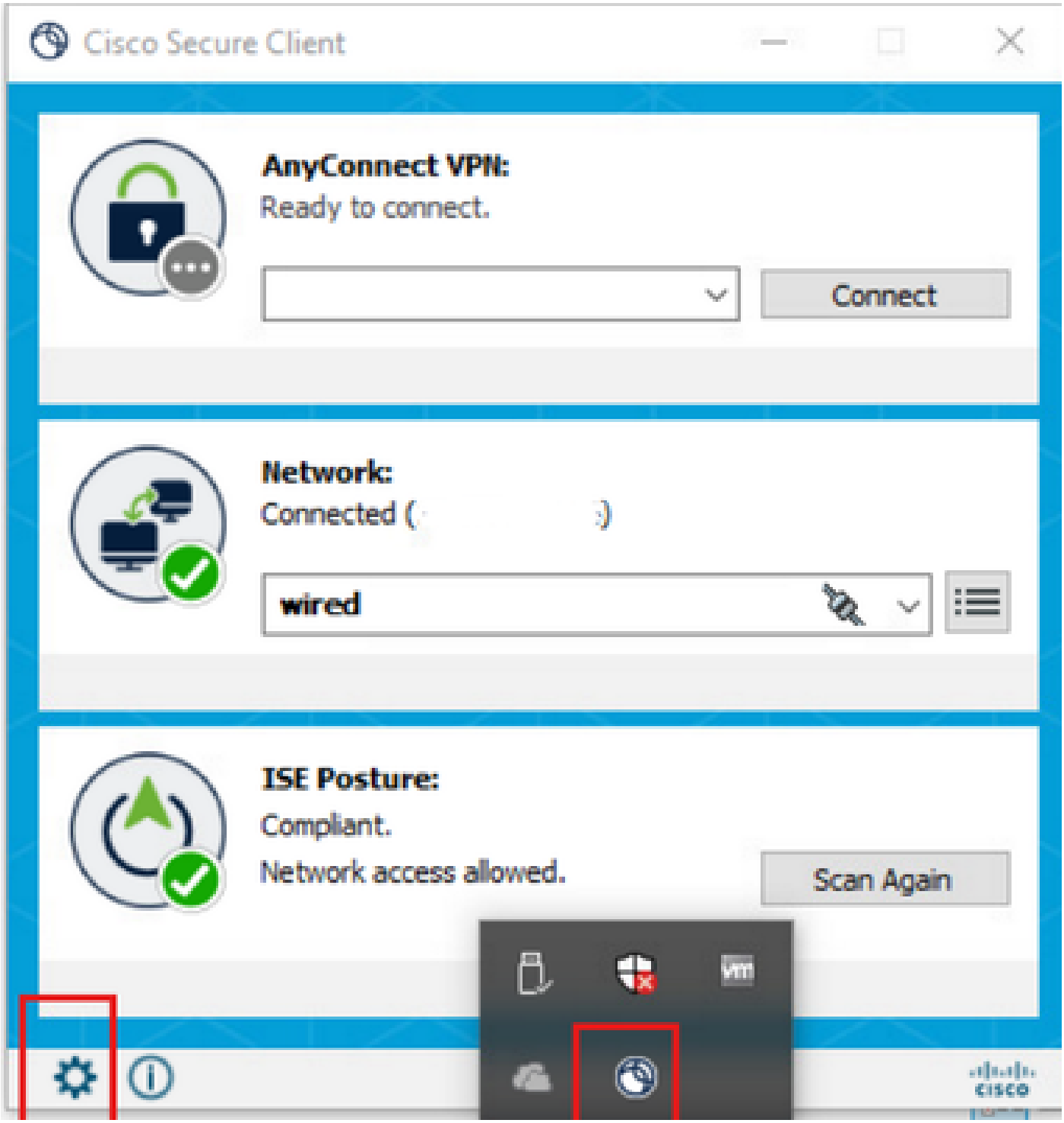
安装NAM模块后，在PC上的此路径中验证NAM配置文件configuration.xml是否存在。

C:\ProgramData\Cisco\Cisco安全客户端\网络访问管理器\system



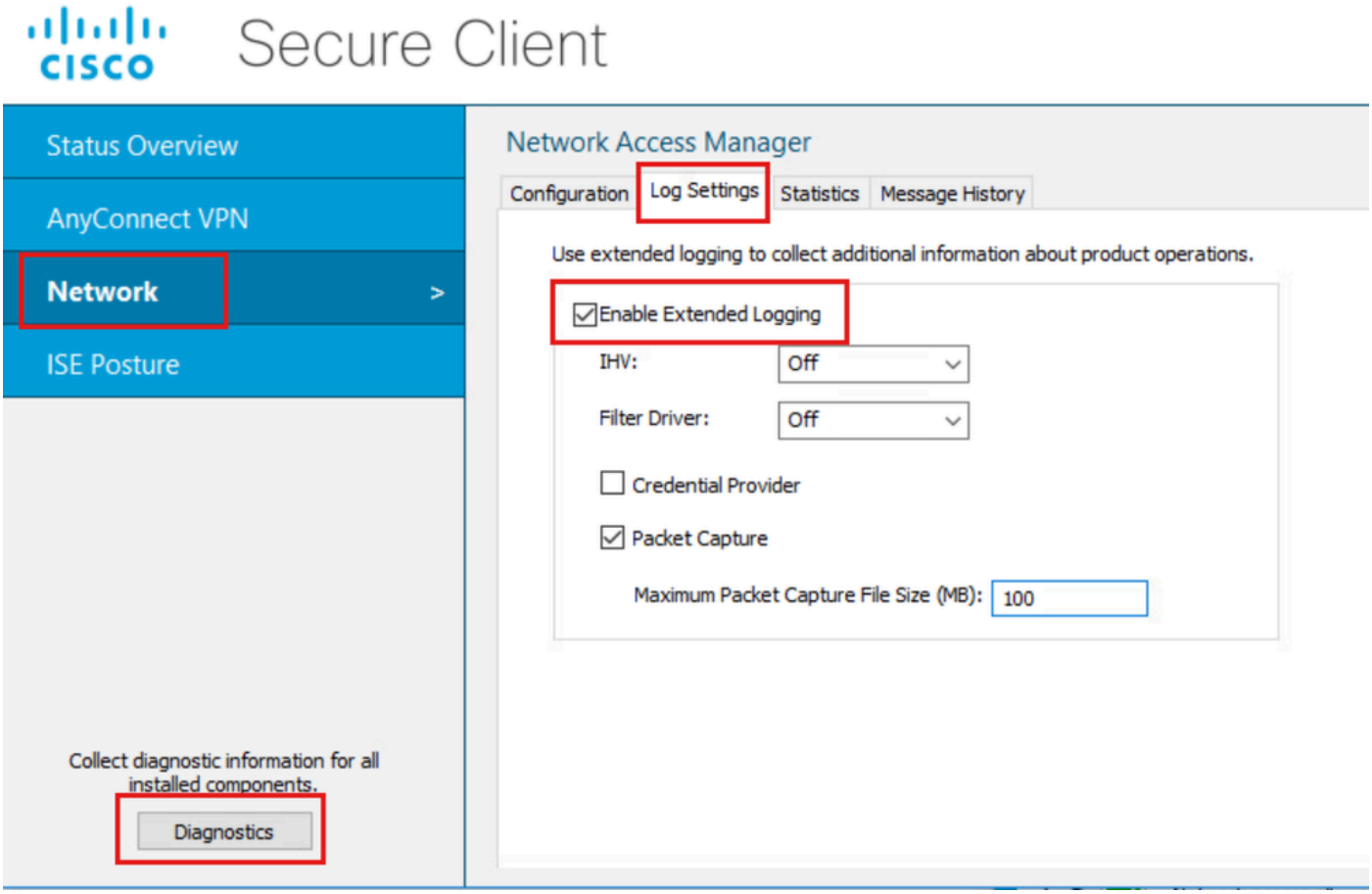
第二步：NAM扩展日志记录

从任务栏中单击“安全客户端”图标，然后选择“设置”图标。



导航到网络>日志设置选项卡。选中Enable Extended Logging复选框。
将数据包捕获文件大小设置为100 MB。

重现问题后，单击Diagnostics在终端上创建DART套件。



消息历史记录部分显示NAM执行的每个步骤的详细信息。

第三步： 交换机上的调试

在交换机上启用这些调试，以排除dot1x和重定向流故障。

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

查看日志

show logging

show logging process smd internal

第四步：ISE上的调试

收集具有以下属性的ISE支持捆绑包，在调试级别进行设置：

- 状态
- 门户
- 调配
- 运行时AAA
- nsf
- NSF会话
- 瑞士
- 客户端Web应用

相关信息

配置安全客户端NAM

ISE终端安全评估规范部署指南

Catalyst 9000系列交换机上的Dot1x故障排除

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。