使用ISE在Windows上配置安全客户端NAM配置文件

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

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上传数据包
- 步骤2.从配置文件编辑器工具创建NAM配置文件
- 步骤3.上传ISE上的NAM配置文件
- 步骤4.创建安全评估配置文件
- 步骤5.创建代理配置
- 步骤6.客户端调配策略
- 步骤7.状态策略
- 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11. Active Directory
- 步骤12.策略设置

验证

- 步骤1.从ISE下载并安装安全客户端状态/NAM模块
- 步骤2. EAP-FAST
- 步骤3.状态扫描

故障排除

- 步骤1. NAM配置文件
- 步骤2. NAM扩展日志记录
- 步骤3.在交换机上进行调试
- 步骤4.在ISE上进行调试

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。

先决条件

要求

Cisco 建议您了解以下主题：

- 状态策略
- 身份服务引擎 (ISE)
- AnyConnect NAM和配置文件编辑器
- 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：

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

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。

背景信息

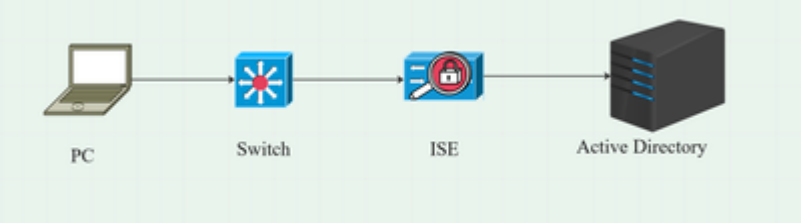
EAP-FAST身份验证分为两个阶段。在第一阶段，EAP-FAST使用TLS握手来提供使用类型长度值(TLV)对象的密钥交换并进行身份验证，以建立受保护的隧道。这些TLV对象用于在客户端和服务器之间传输身份验证相关数据。隧道建立后，第二阶段从客户端和ISE节点开始进一步对话以建立所需的身份验证和授权策略。

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，可以在NAM配置配置文件中配置计算机和用户连接类型。企业Windows设备使用带状态检查的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)配置文件以及终端安全评估合规性检查的说明。

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，代理下载终端安全评估配置文件并在ISE上配置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

配置接入交换机进行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
```

配置重定向ACL以将用户重定向到ISE客户端调配门户：

```
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
 tracking enable
interface <interface name>
 device-tracking attach-policy

ip http server
ip http secure-server
```

下载安全客户端软件包

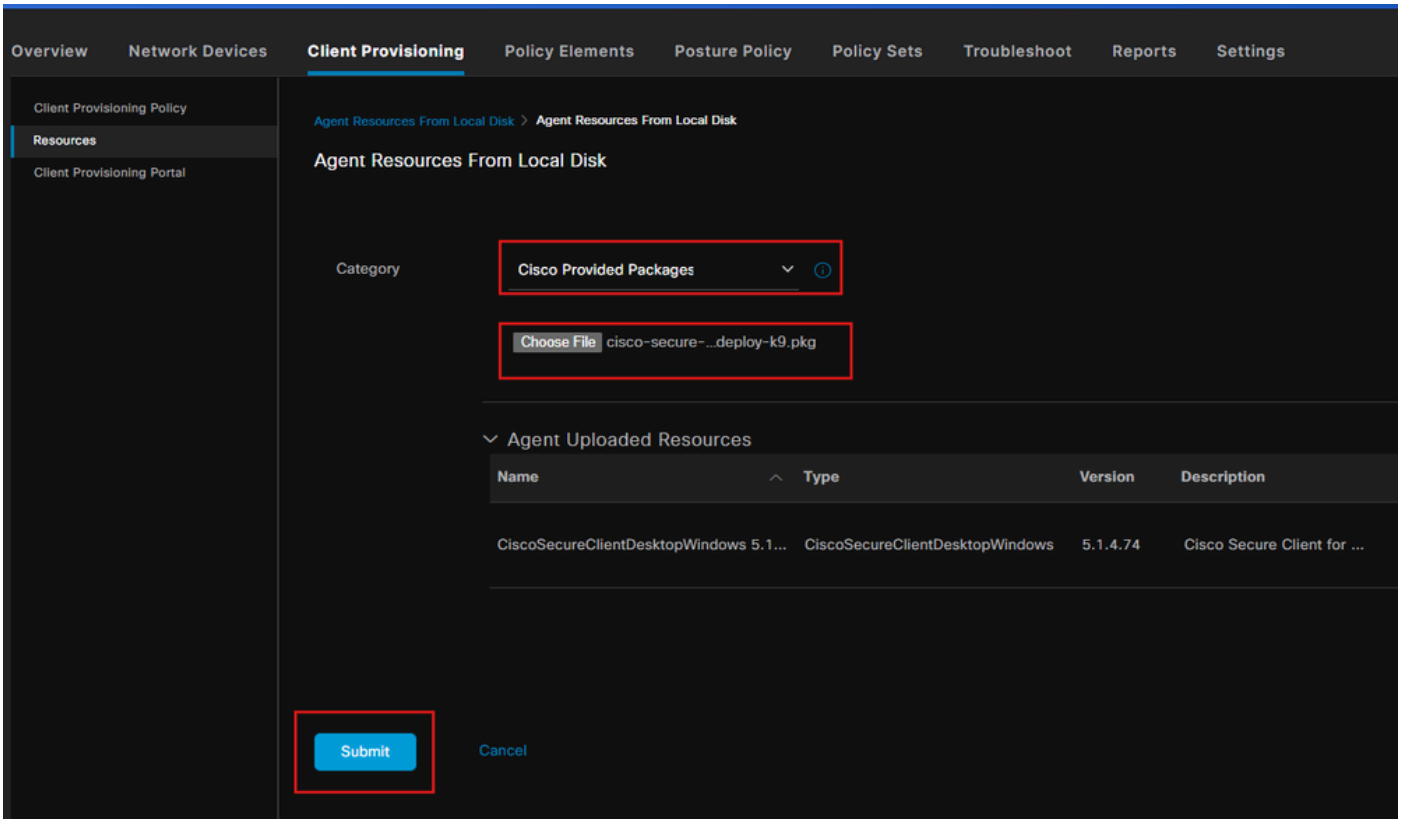
从Cisco Software Download Page手动下载配置文件编辑器、安全客户端Windows和合规性模块webdeploy文件。在产品名称搜索栏上，键入Secure Client 5。下载Home > Security > Endpoint Security > Secure Client(including AnyConnect)> Secure Client 5 > AnyConnect VPN Client Software

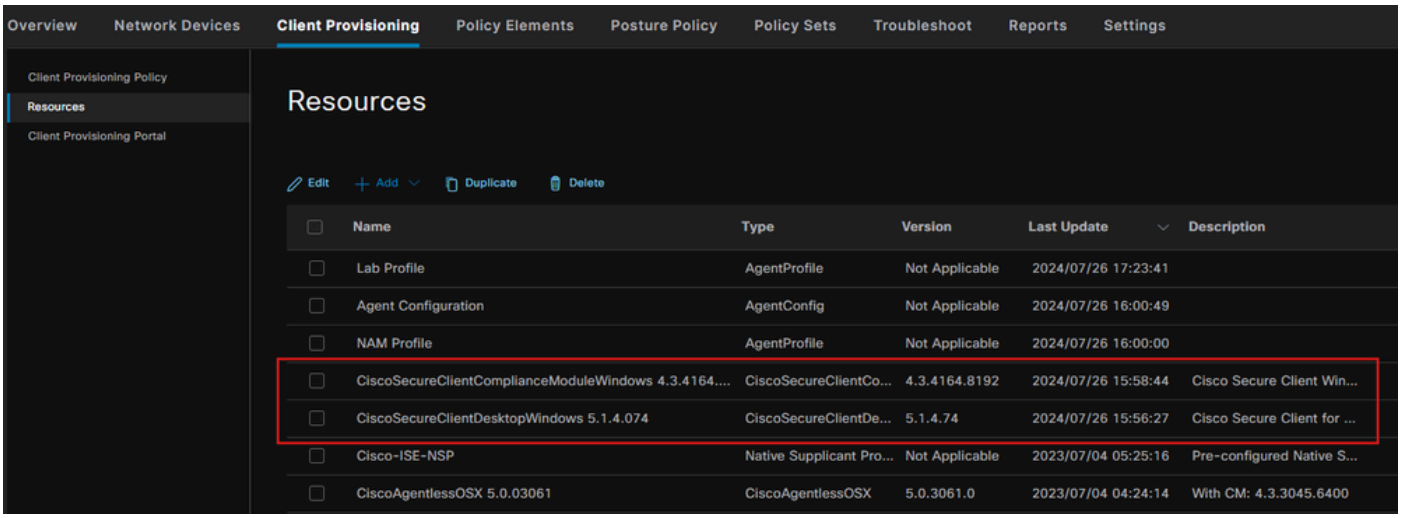
- cisco-secure-client-win-5.1.x-webdeploy-k9.pkg
- cisco-secure-client-win-4.3.x-isecompliance-webdeploy-k9.pkg
- tools-cisco-secure-client-win-5.1.x-profileeditor-k9.msi

ISE 配置

步骤1.在ISE上传数据包

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



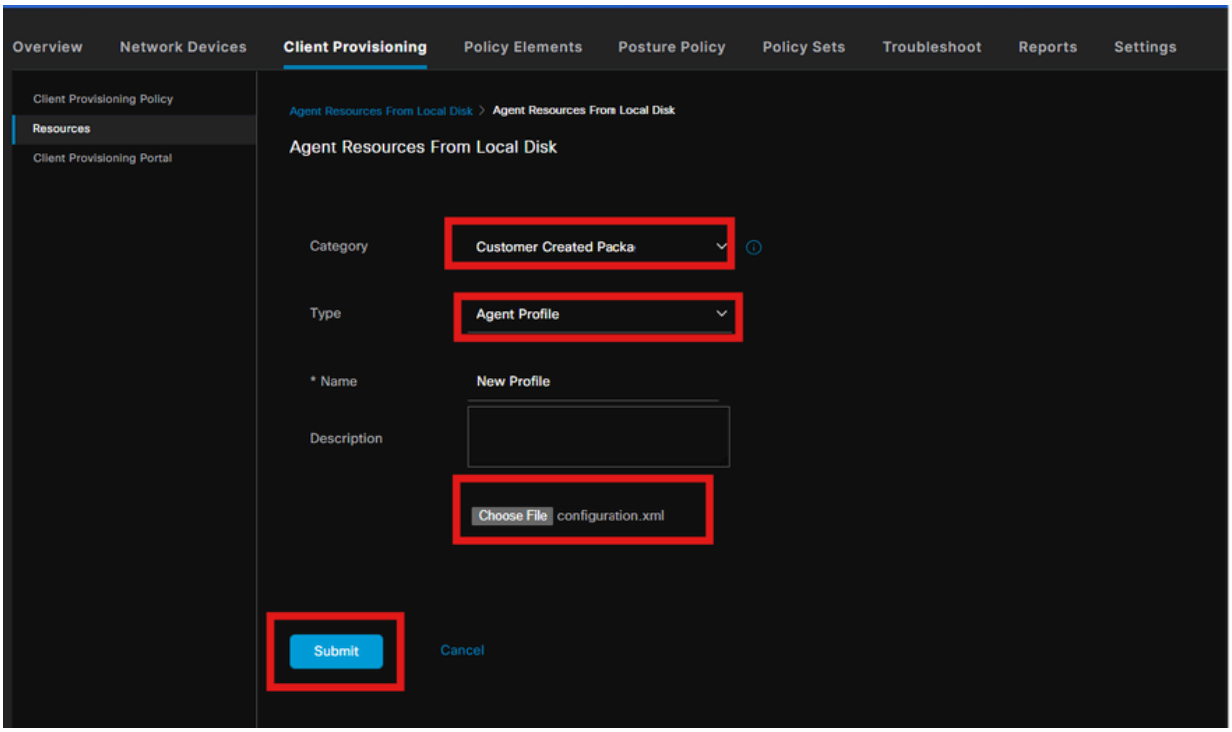


步骤2.从配置文件编辑器工具创建NAM配置文件

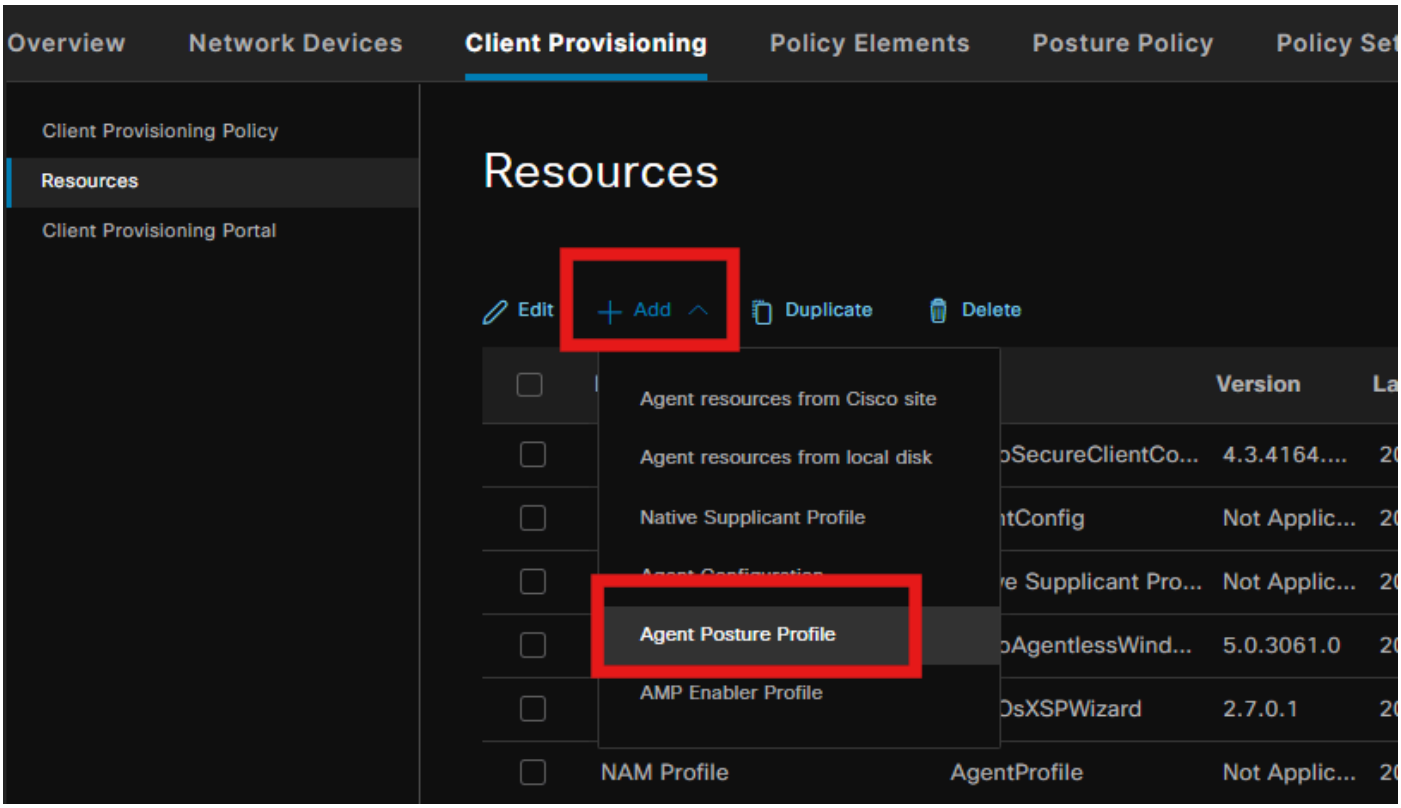
有关如何配置NAM配置文件的信息，请参阅使用Windows和ISE 3.2为Dot1x配置安全客户端NAM指南。

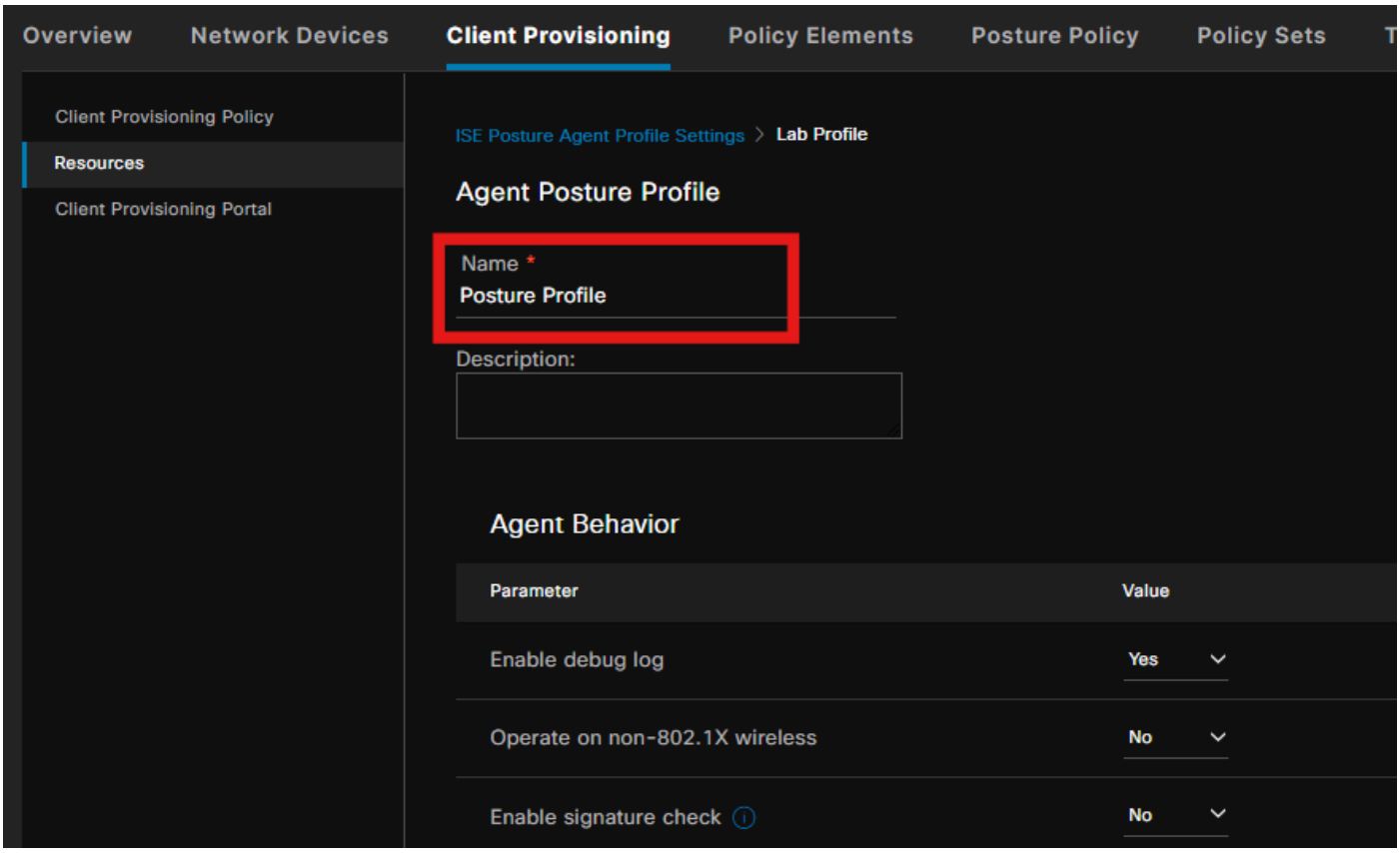
步骤3.上传ISE上的NAM配置文件

1.要上传ISE上的NAM配置文件Configuration.xml作为代理配置文件，请导航到客户端调配>资源>代理资源从本地磁盘。



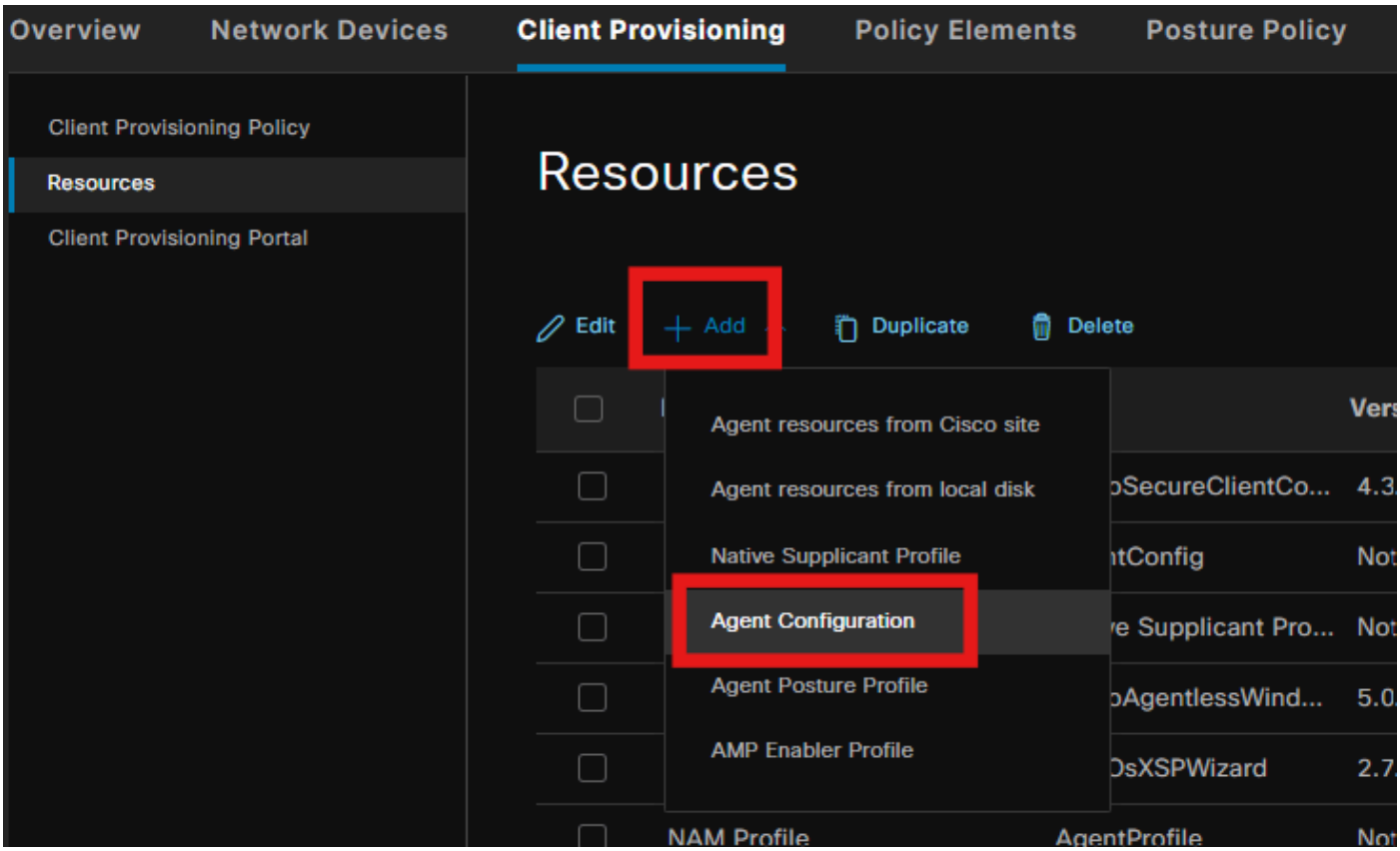
步骤4.创建安全评估配置文件


Overview
Network Devices
Client Provisioning
Policy Elements
Posture Policy
Policy Set
Client Provisioning Policy
Resources
Client Provisioning Portal
Resources
Edit
Add
Duplicate
Delete
Agent resources from Cisco site
Agent resources from local disk
Native Supplicant Profile
Agent Posture Profile
AMP Enabler Profile
Version
4.3.4164....
Not Applic...
5.0.3061.0
2.7.0.1
NAM Profile
AgentProfile
Not Applic...

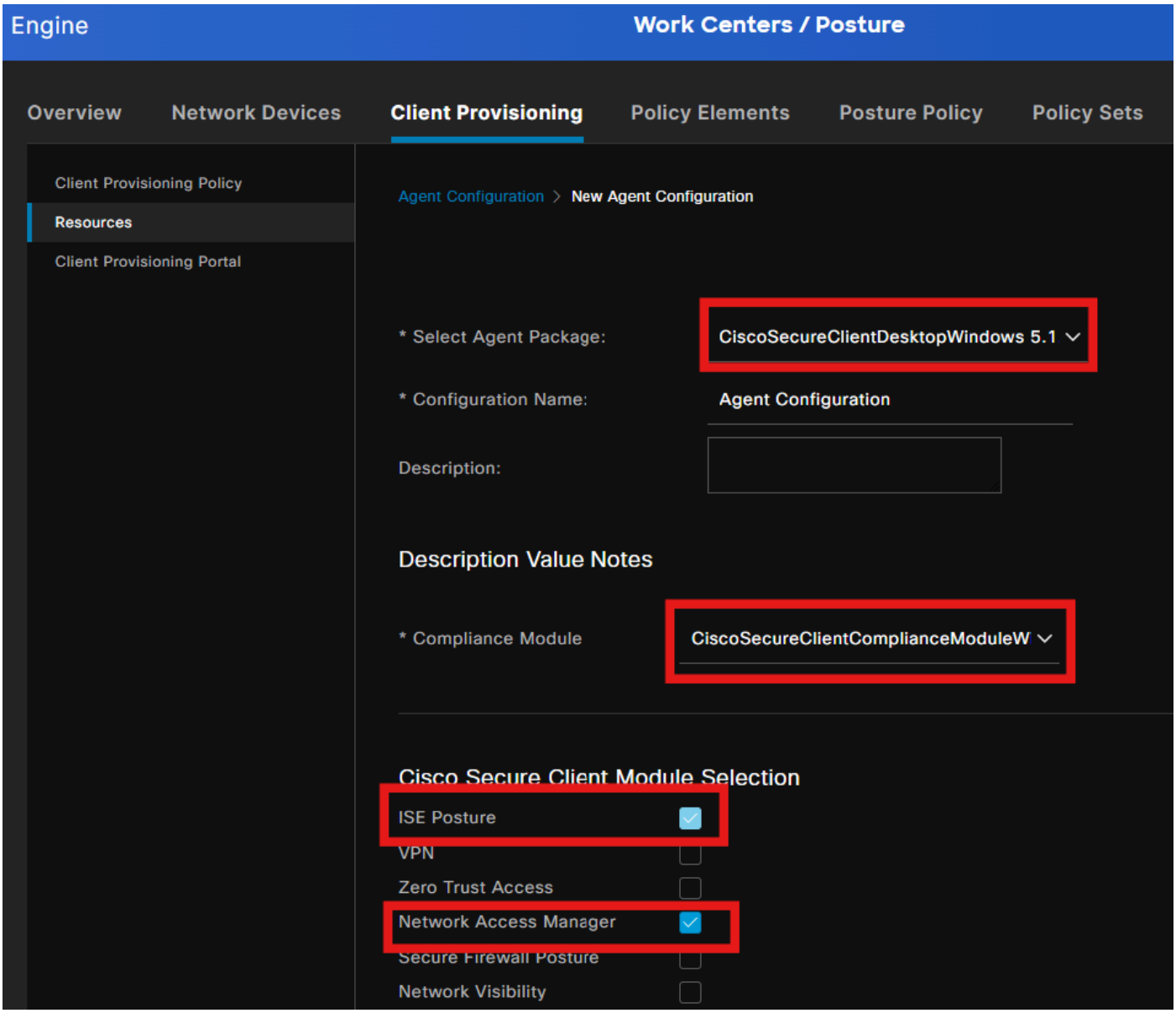


1.在Posture Protocol部分，不要忘记添加星号(*)以允许代理连接到所有服务器。

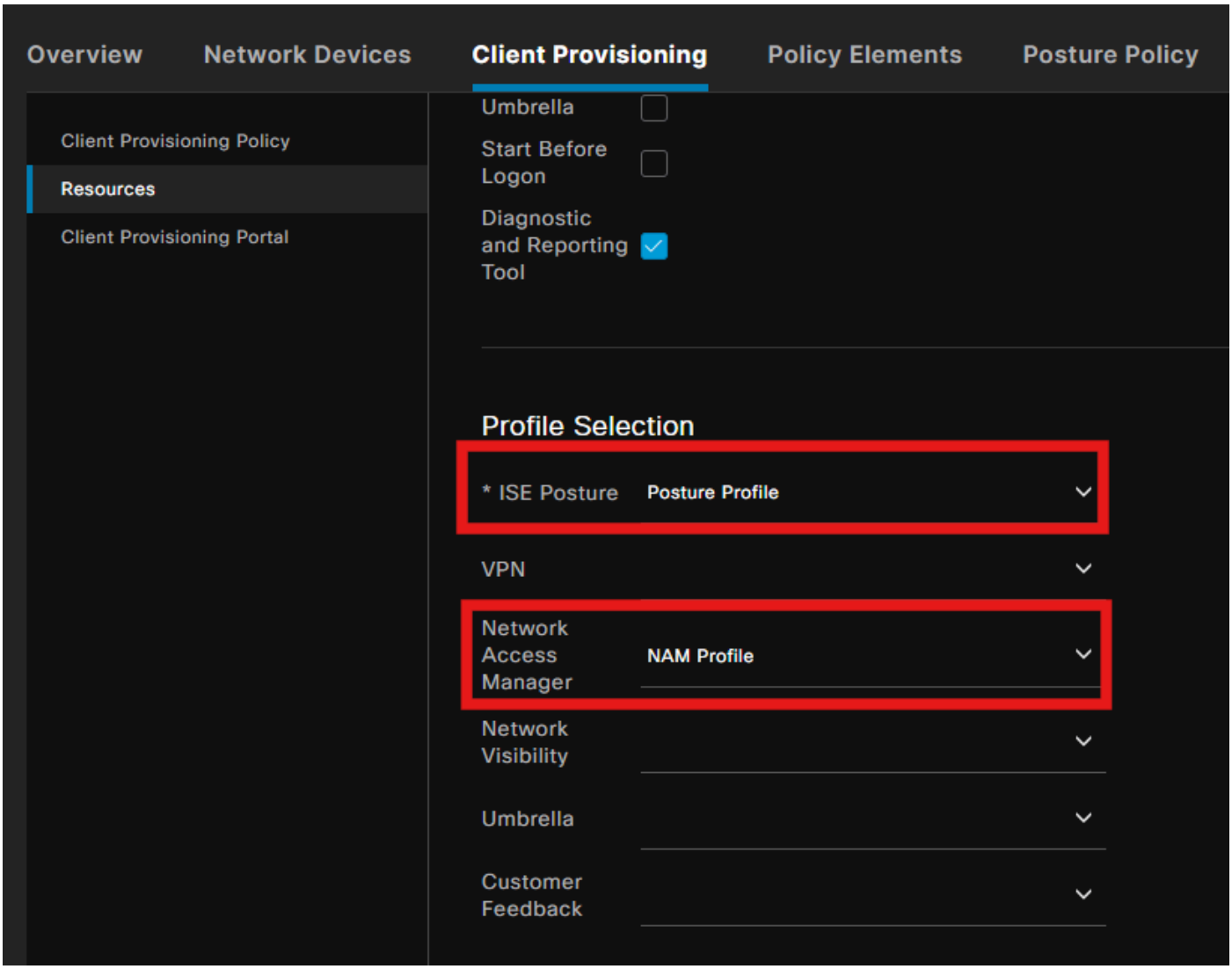
步骤5.创建代理配置



1.选择上传的安全客户端和合规性模块包，在Module选项下，选择ISE Posture、NAM和DART模块。

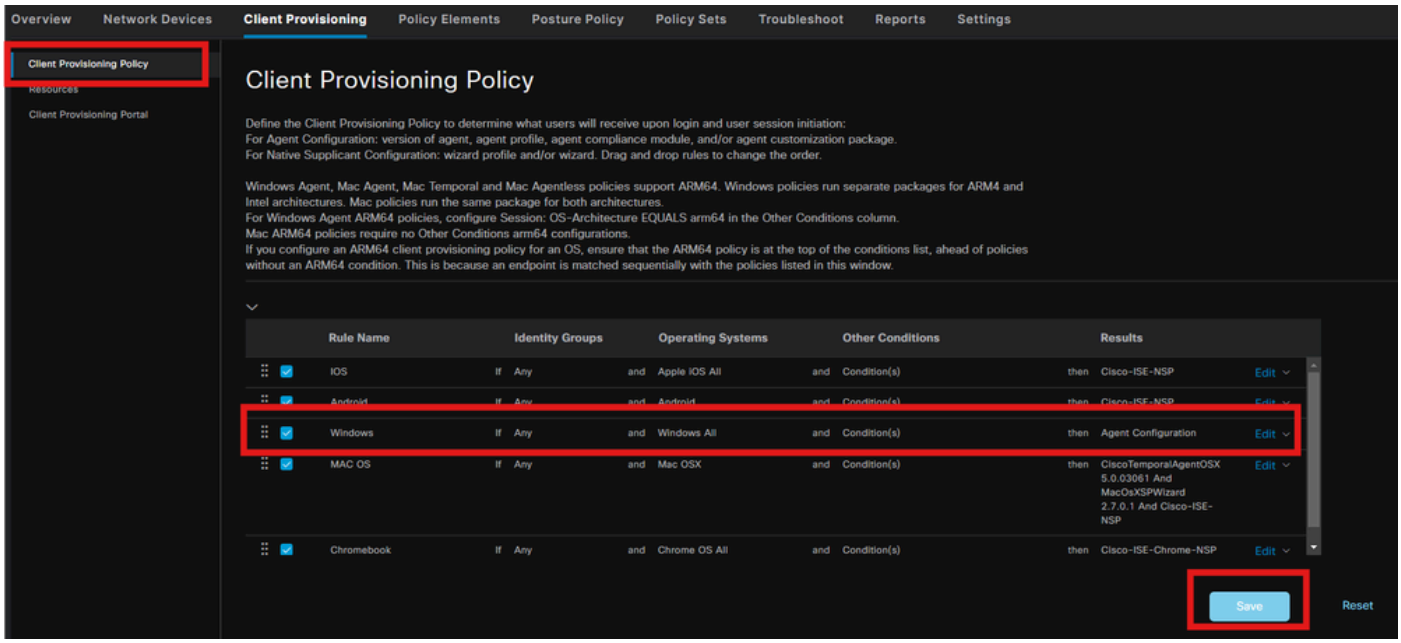


2.在配置文件选择下，选择Posture和NAM配置文件，然后单击Submit。


Overview
Network Devices
Client Provisioning
Policy Elements
Posture Policy
Client Provisioning Policy
Resources
Client Provisioning Portal
Umbrella
Start Before Logon
Diagnostic and Reporting Tool
Profile Selection
* ISE Posture
Posture Profile
VPN
Network Access Manager
NAM Profile
Network Visibility
Umbrella
Customer Feedback

步骤6.客户端调配策略

1.为Windows OS创建客户端调配策略，并选择上一步中创建的代理程序配置。

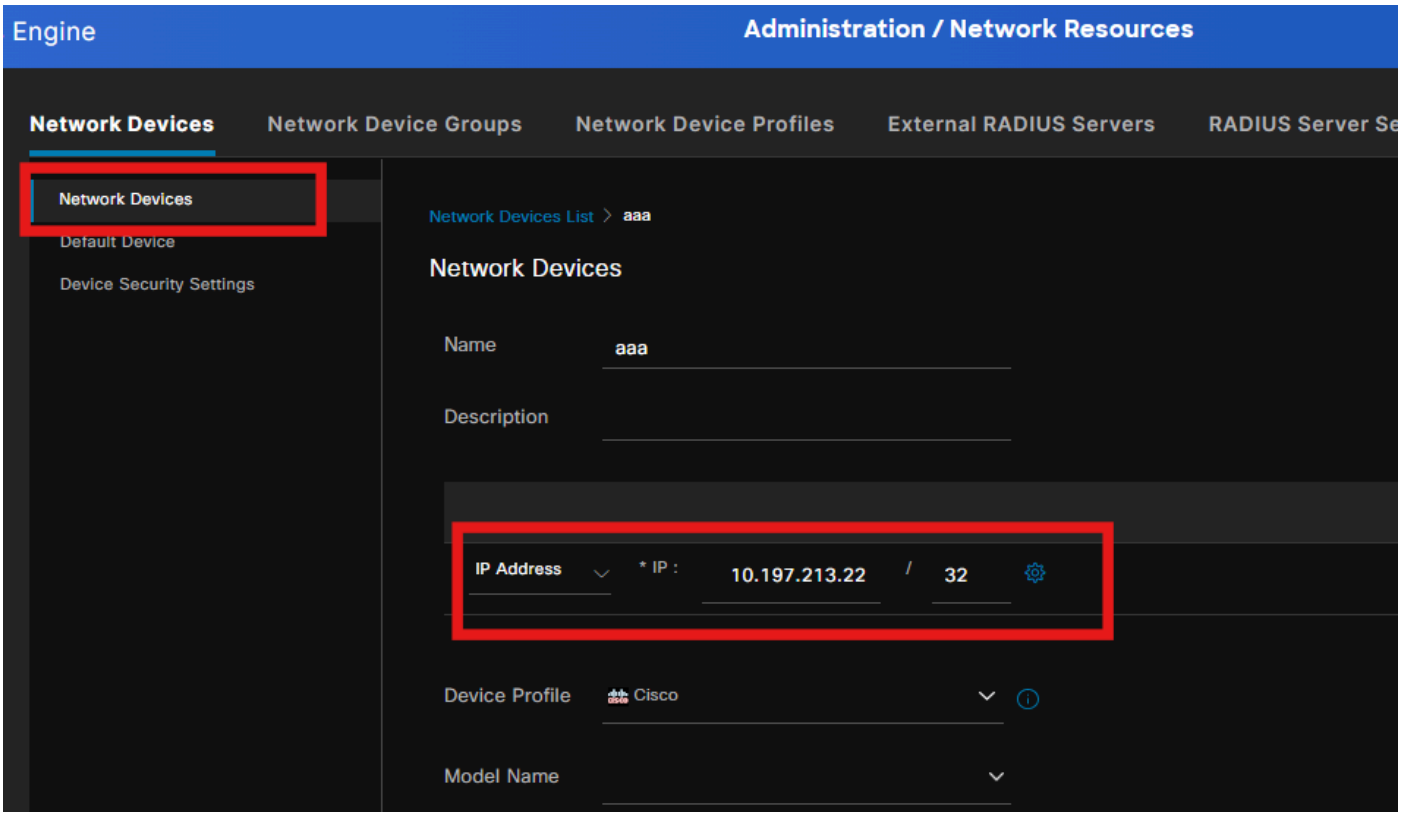


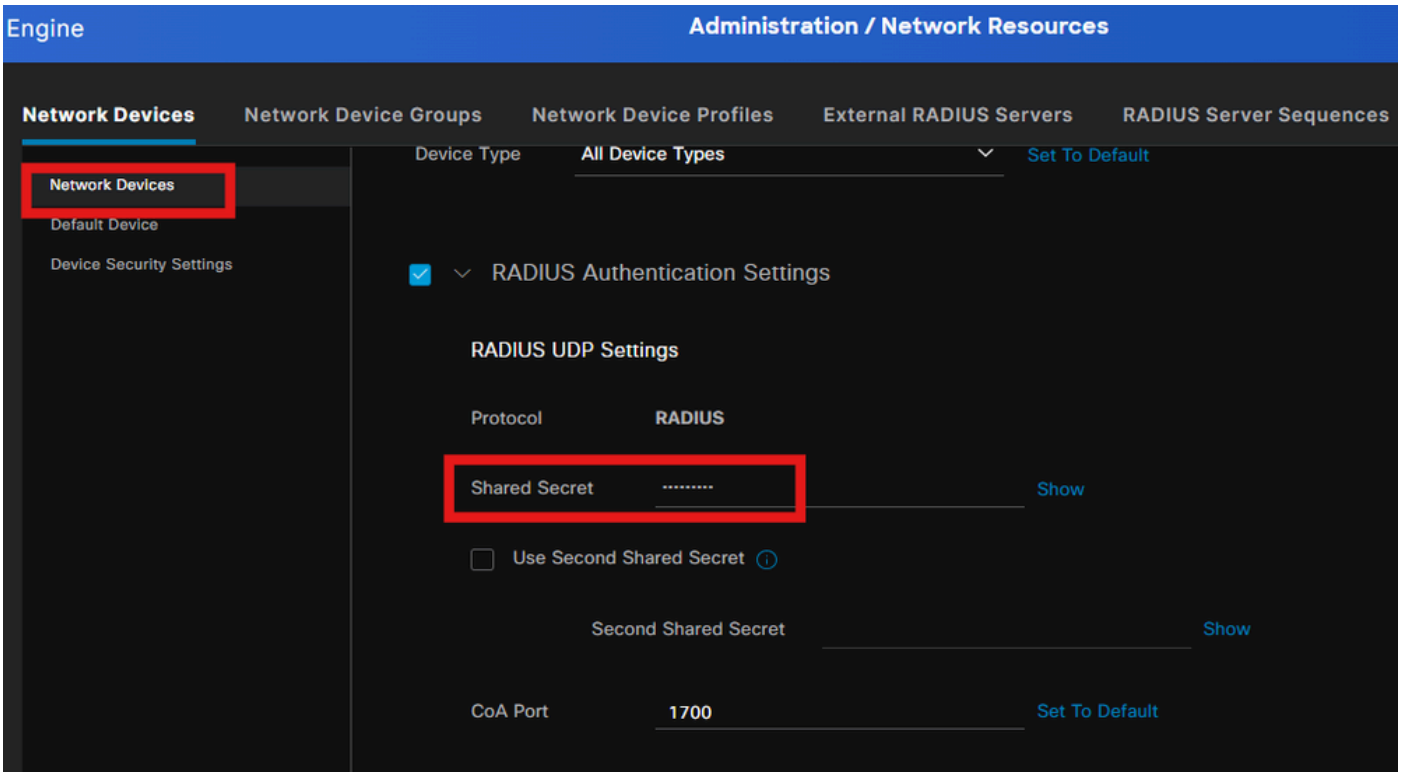
步骤7.状态策略

有关如何创建安全评估策略和条件的信息，请参阅ISE安全评估规范部署指南。

步骤8.添加网络设备

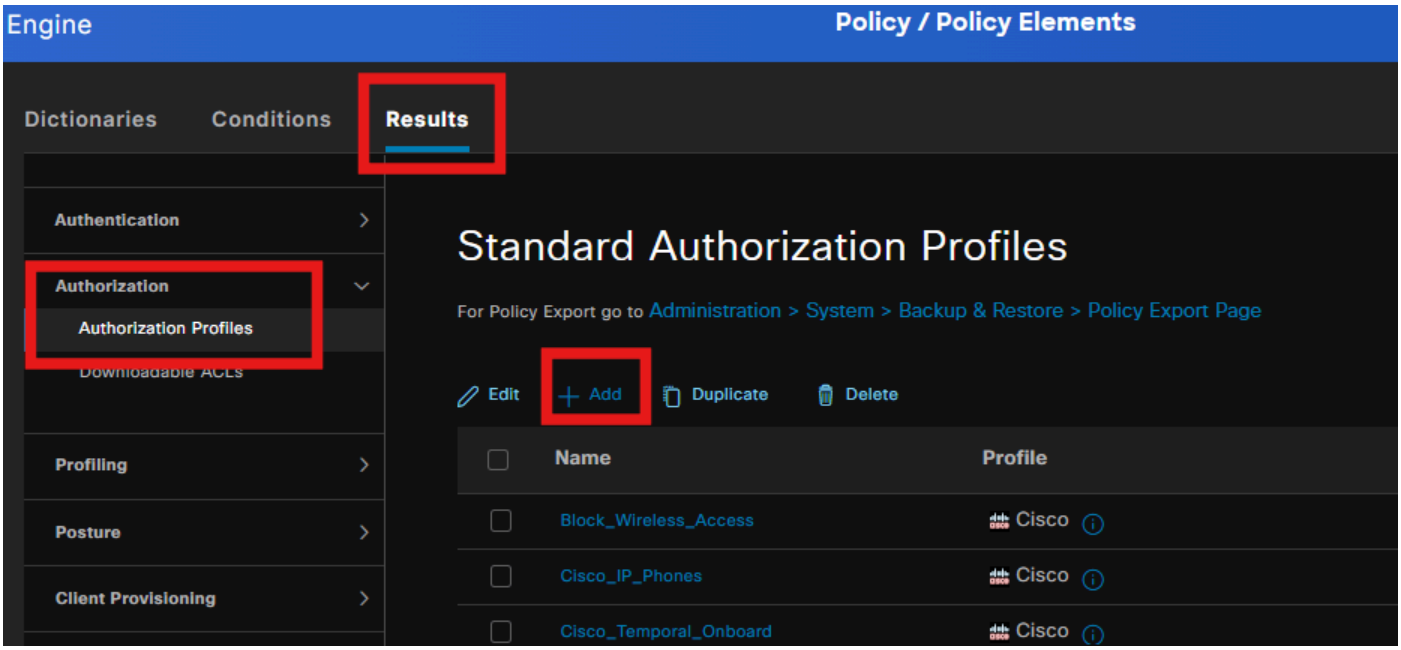
要添加交换机IP地址和radius共享密钥，请导航到管理>网络资源。



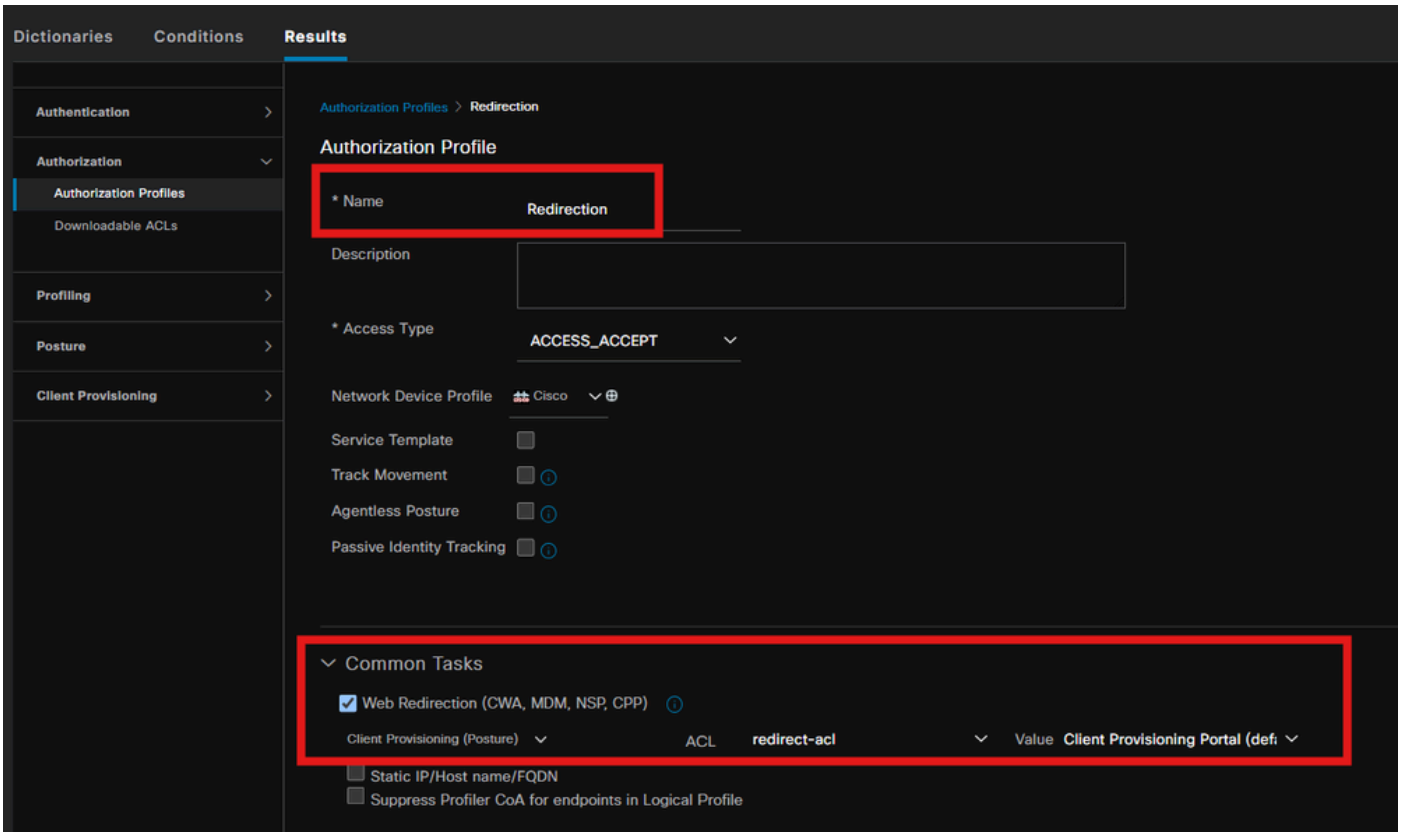


步骤9.授权配置文件

1.要创建安全评估重定向配置文件，请导航到策略>策略元素>结果。

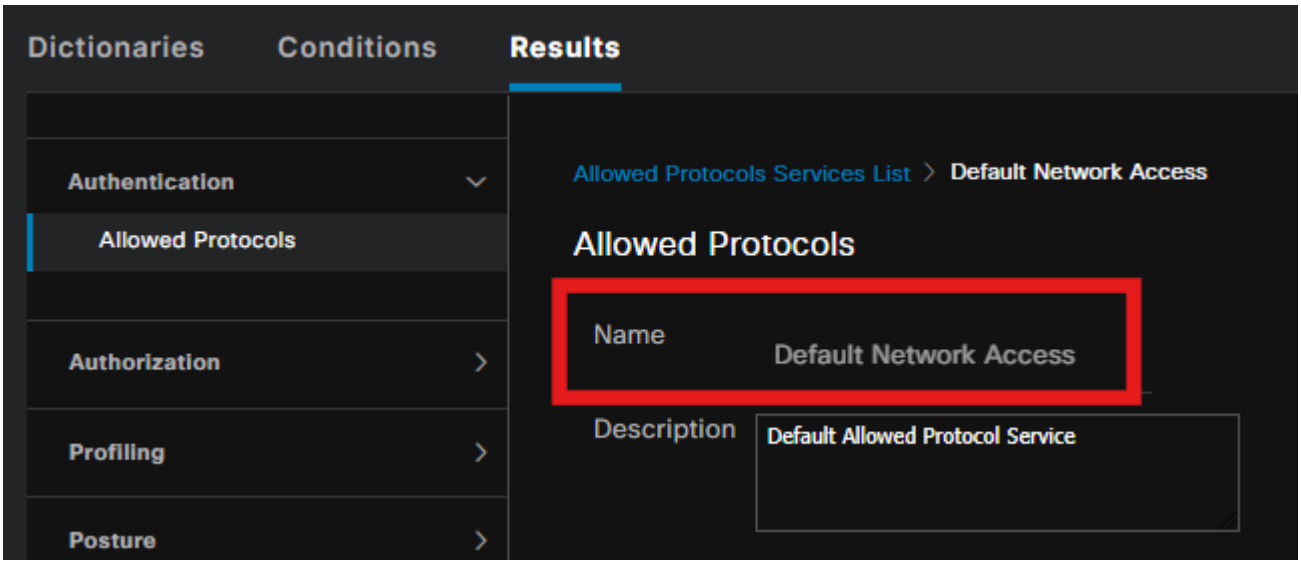


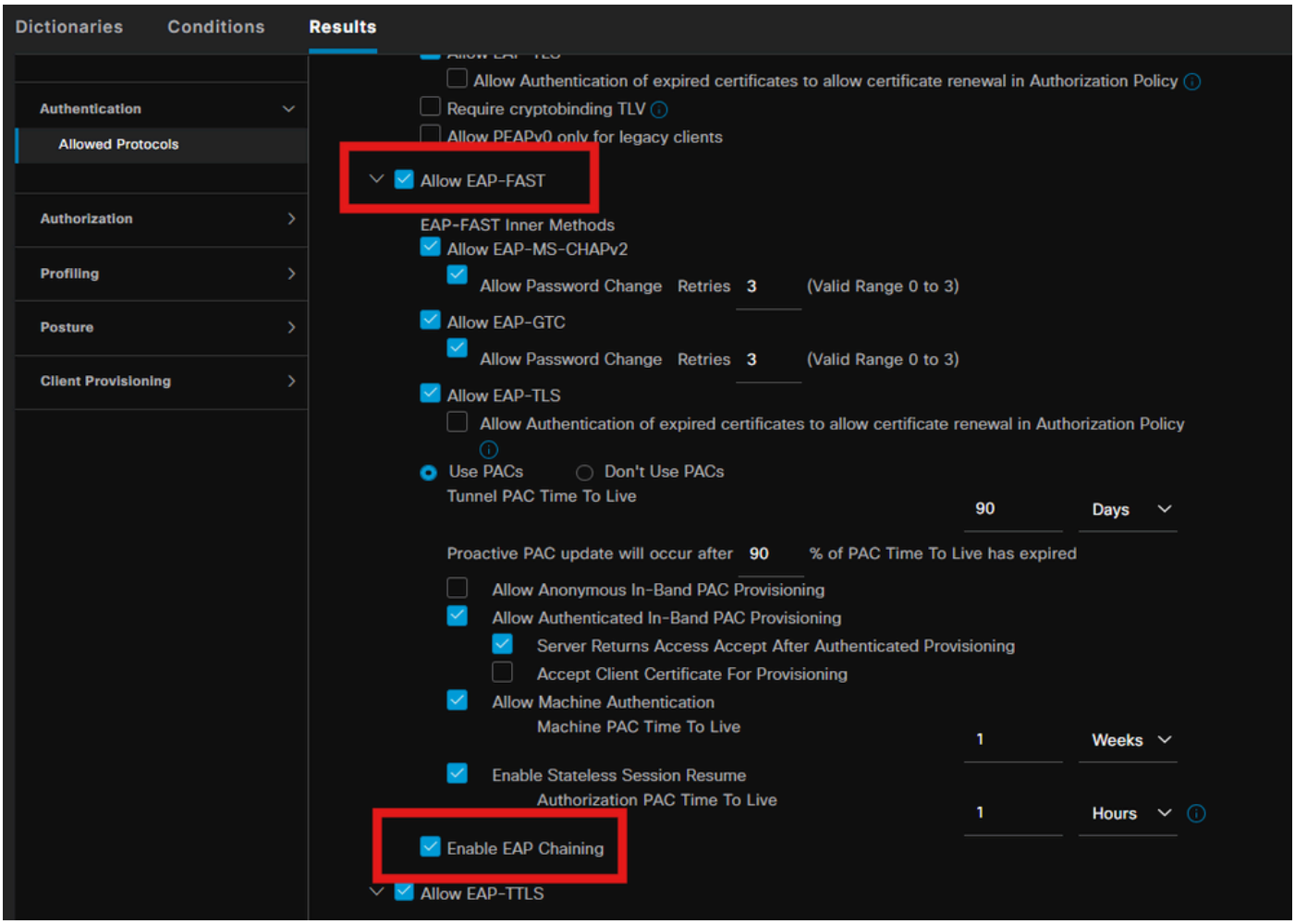
2.在常见任务下，选择Client Provisioning Portal with Redirect ACL。



步骤10.允许的协议

1.导航到策略>策略元素>结果>身份验证>允许的协议，选择EAP链设置。

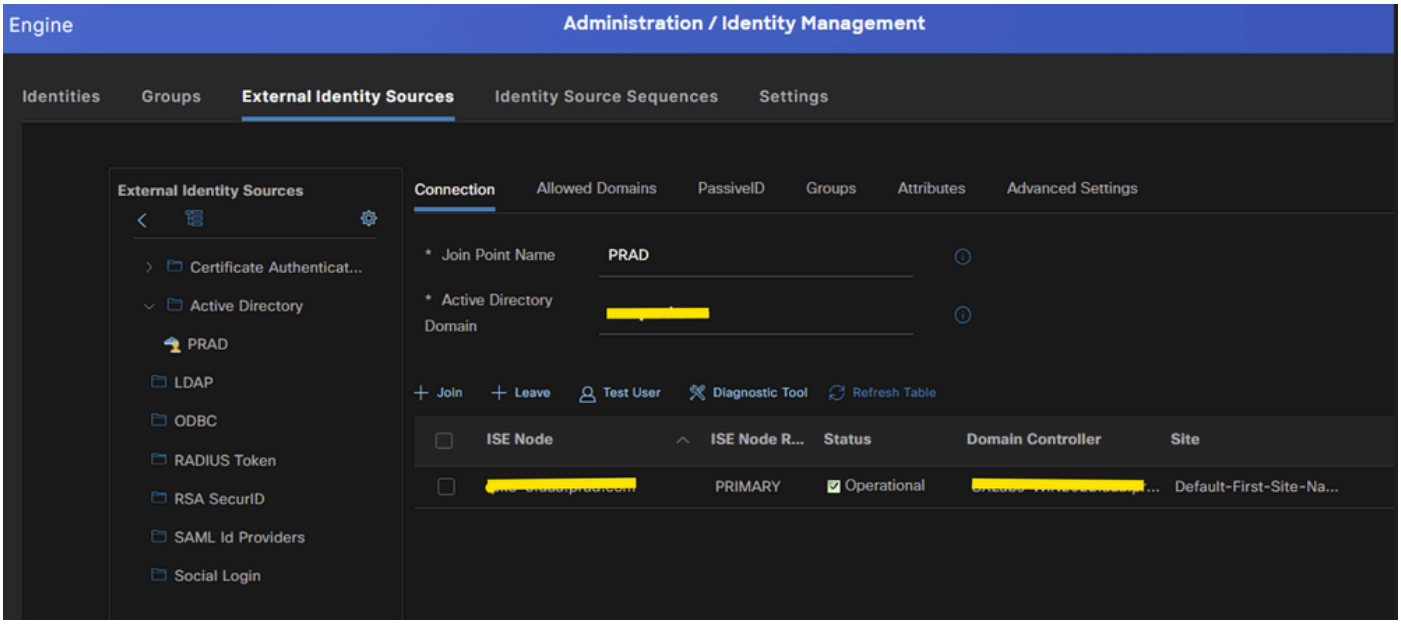

Dictionaries
Conditions
Results
Authentication
Allowed Protocols
Authorization
Profiling
Posture
Allowed Protocols Services List > Default Network Access
Allowed Protocols
Name
Default Network Access
Description
Default Allowed Protocol Service


Dictionaries
Conditions
Results
Authentication
Allowed Protocols
Authorization
Profiling
Posture
Client Provisioning
Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy
Require cryptobinding TLV
Allow PEAPv0 only for legacy clients
Allow EAP-FAST
EAP-FAST Inner Methods
Allow EAP-MS-CHAPv2
Allow Password Change Retries 3 (Valid Range 0 to 3)
Allow EAP-GTC
Allow Password Change Retries 3 (Valid Range 0 to 3)
Allow EAP-TLS
Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy
Use PACs
Don't Use PACs
Tunnel PAC Time To Live
90
Days
Proactive PAC update will occur after 90 % of PAC Time To Live has expired
Allow Anonymous In-Band PAC Provisioning
Allow Authenticated In-Band PAC Provisioning
Server Returns Access Accept After Authenticated Provisioning
Accept Client Certificate For Provisioning
Allow Machine Authentication
Machine PAC Time To Live
1
Weeks
Enable Stateless Session Resume
Authorization PAC Time To Live
1
Hours
Enable EAP Chaining
Allow EAP-TTLS

步骤11. Active Directory

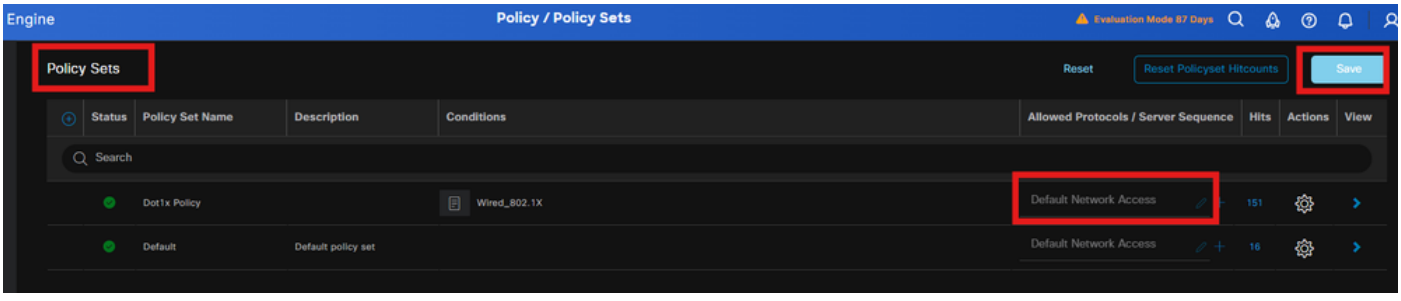
1.验证ISE已加入Active Directory域，并且已选择域组（如果需要），以满足授权条件。

管理>身份管理>外部身份源> Active Directory

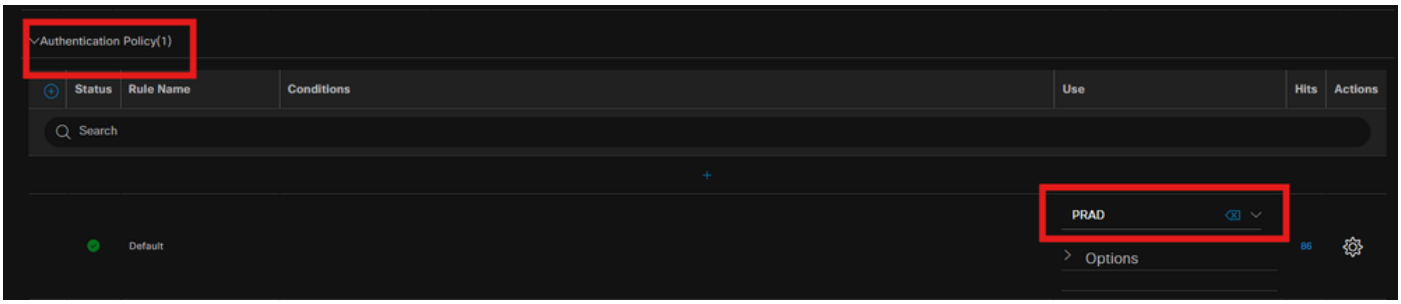


步骤12.策略设置

1.在ISE上创建策略集以对dot1x请求进行身份验证。导航到Policy > Policy Sets。



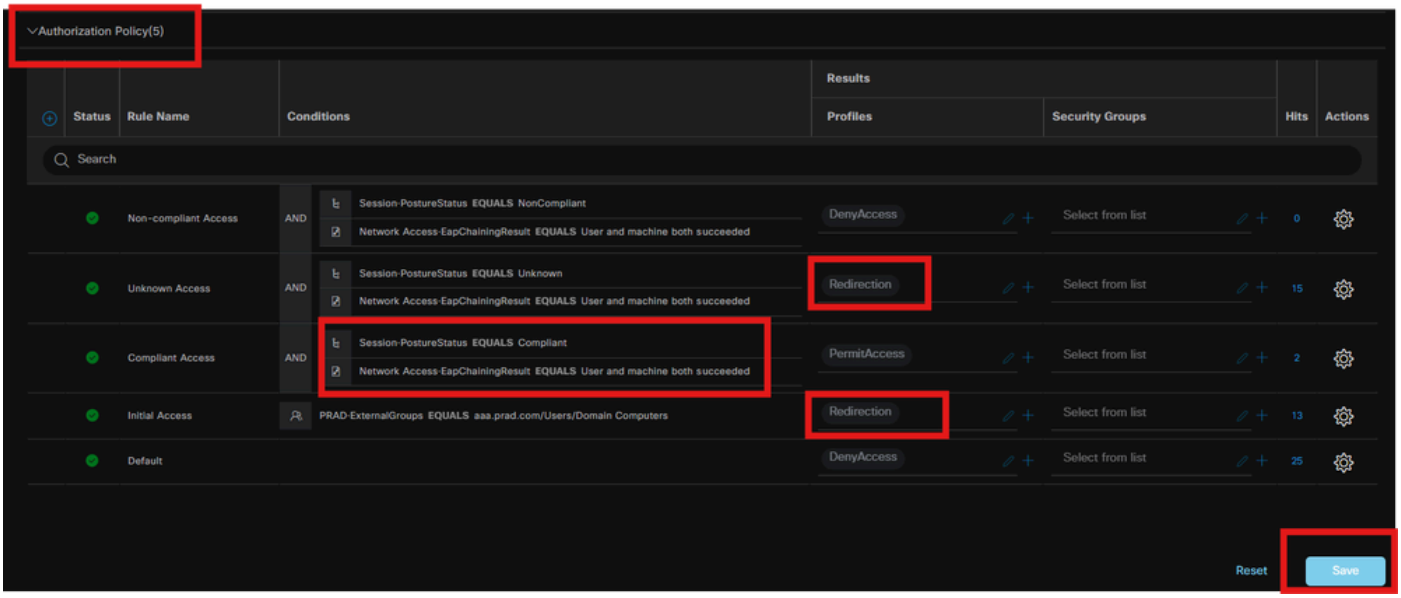
2.选择Active Directory作为身份验证策略的身份源。



3.根据未知、不合规和合规的安全状态配置不同的授权规则。

在本使用案例中：

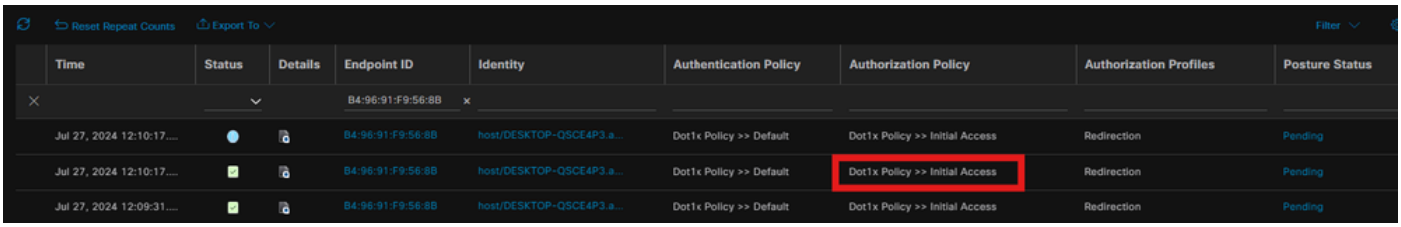
- 初始访问:重定向至ISE客户端调配门户以安装安全客户端代理和NAM配置文件。
- 未知访问:访问客户端调配门户以根据状态发现进行重定向。
- 合规访问:完全网络访问。
- 不合规:拒绝访问.



验证

步骤1.从ISE下载并安装安全客户端状态/NAM模块

1.通过dot1x选择经过身份验证的终端，点击Initial Access Authorization规则。导航到操作> Radius >实时日志。



2.在交换机上，指定重定向URL和应用于终端的ACL。

```
Switch#show authentication session interface te1/0/24详细信息
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.xxx
状态:已授权
域名： 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
客户会话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:应安全
安全状态:链路不安全

服务器策略：
URL重定向ACL:redirect-acl
```

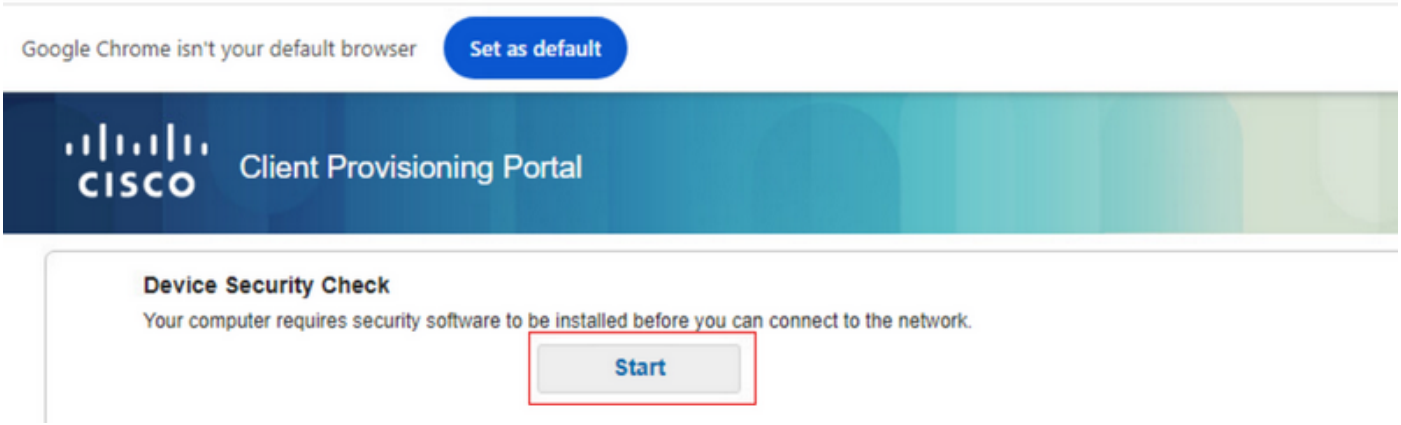
URL重定向
：https://ise33.xxxx:8443/portal/gateway?sessionId=16D5C50A0000002CF067366A&portal=ee39fd08-7180-4995-8aa2-9fb282645a8f&action=cpp&token=518f857900a37f9afc6d2da8b6fe3bc2
ACS ACL:xACSACLx-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3

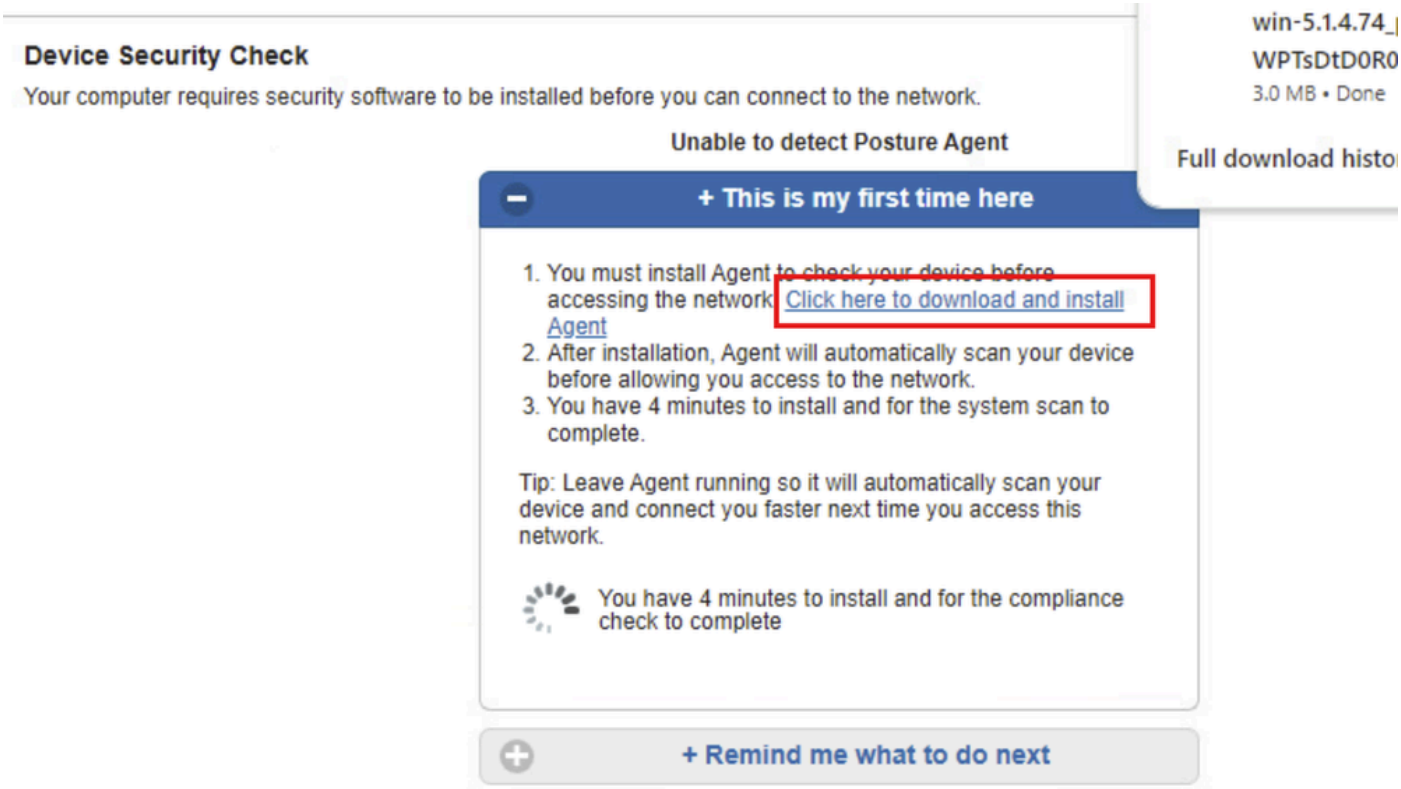
方法状态列表：
方法状态
dot1x身份验证成功

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

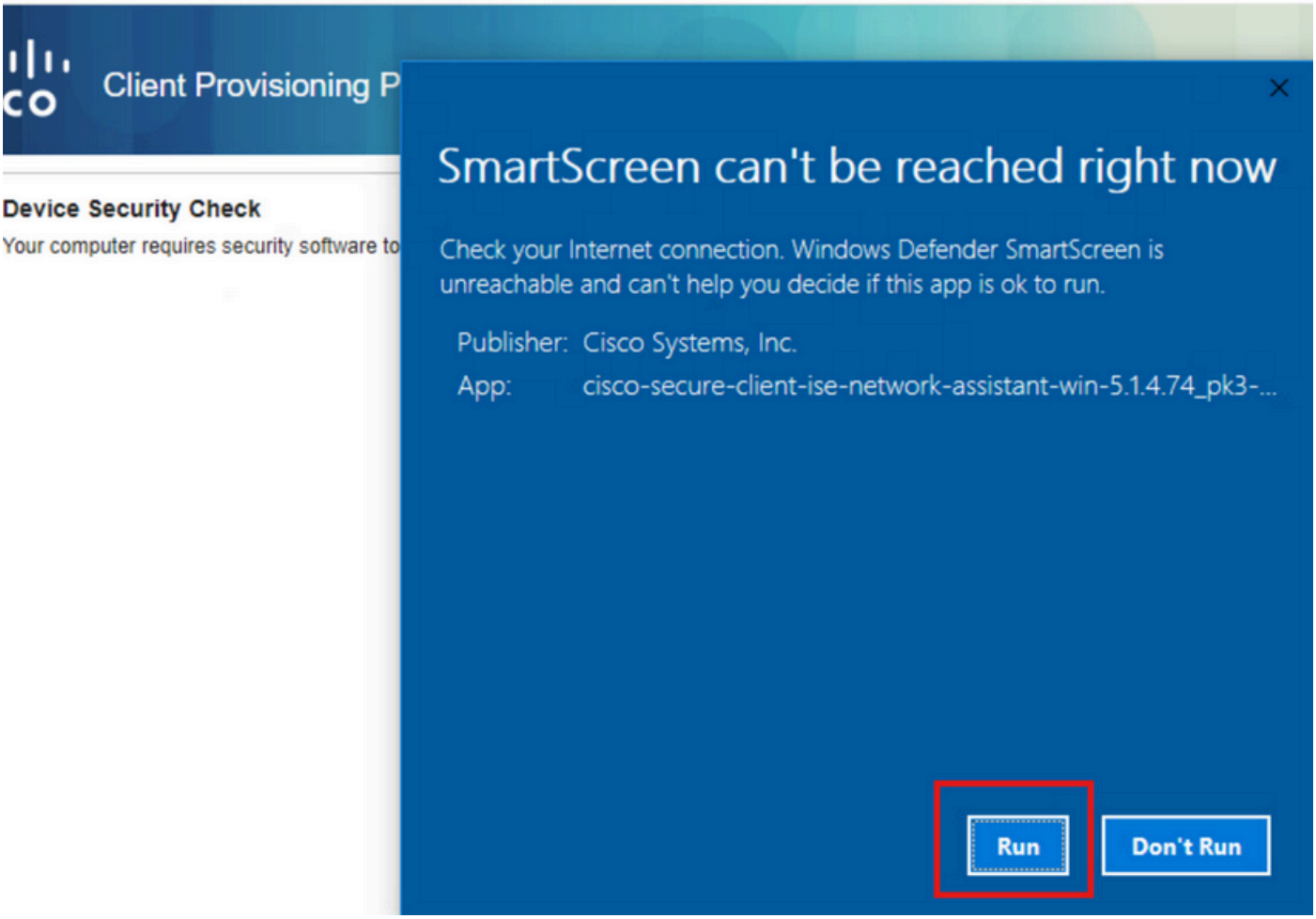
网络层地址链路层地址接口vlan端口老化状态剩余时间
ARP X.X.X.X b496.91f9.568b Te1/0/24 1000 005 4mn可访问39秒尝试0

3.在终端上，验证重定向到ISE终端安全评估的流量，然后单击开始在终端上下载网络设置助手。

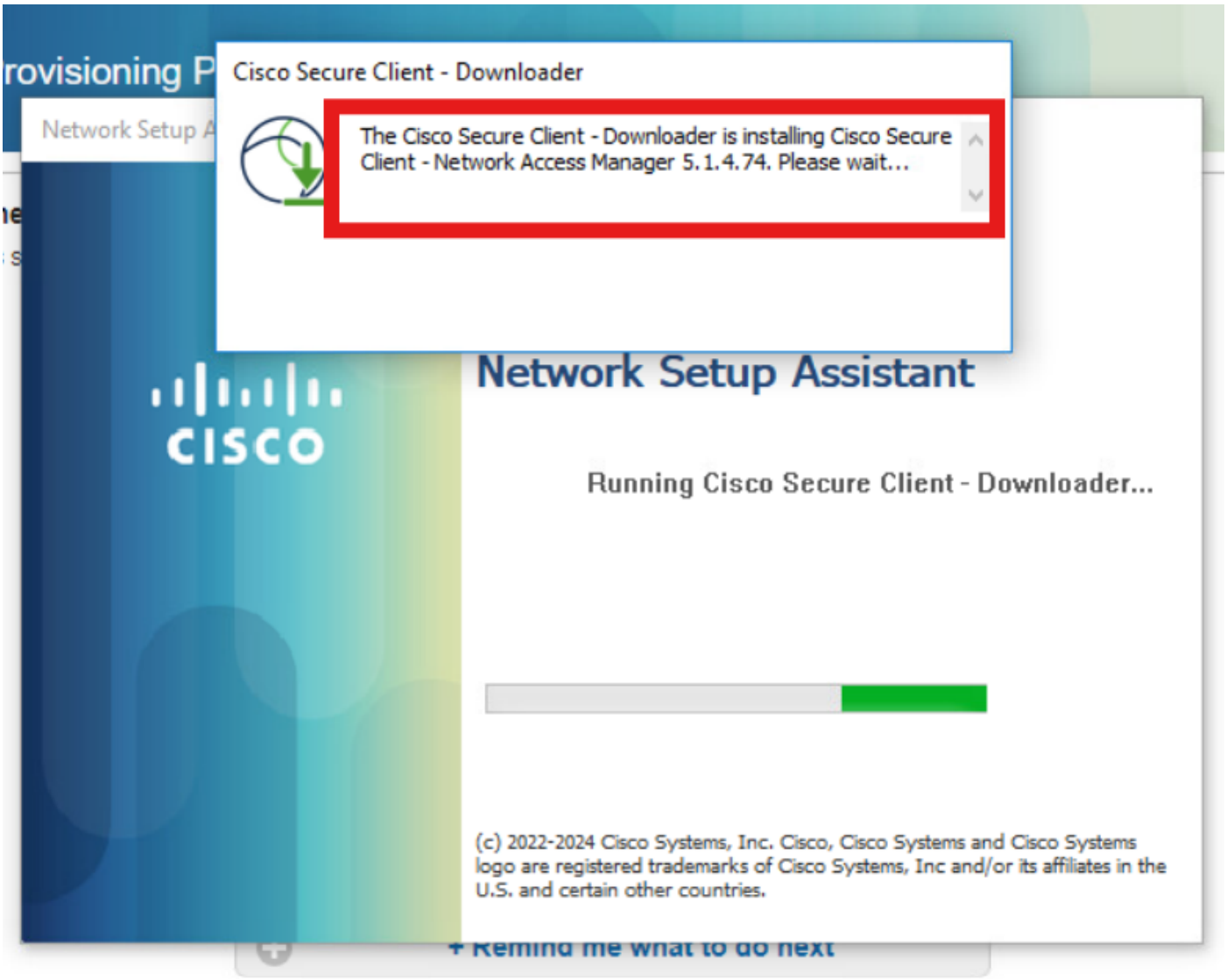




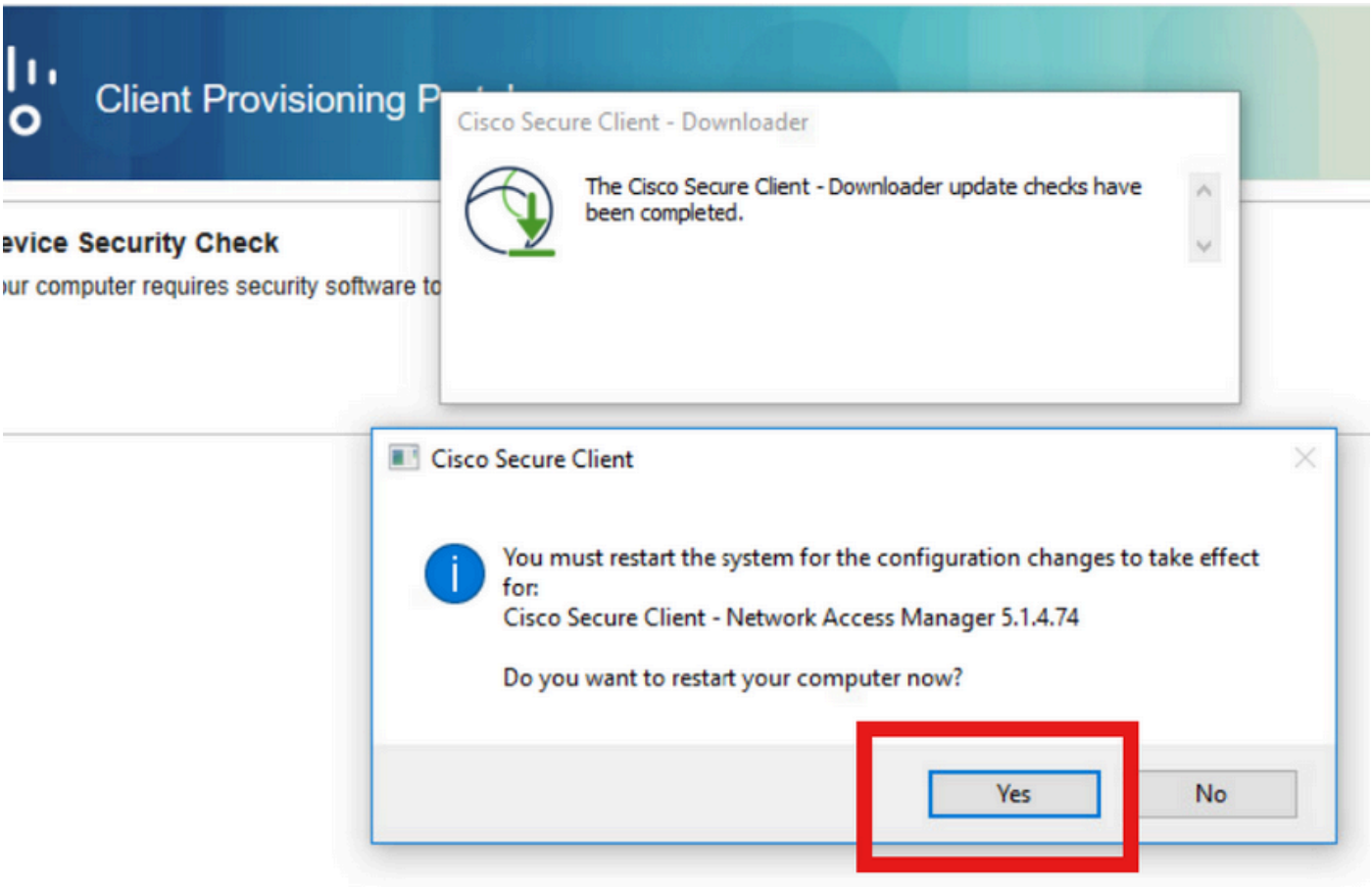
4.单击运行安装NSA应用程序。



2.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。

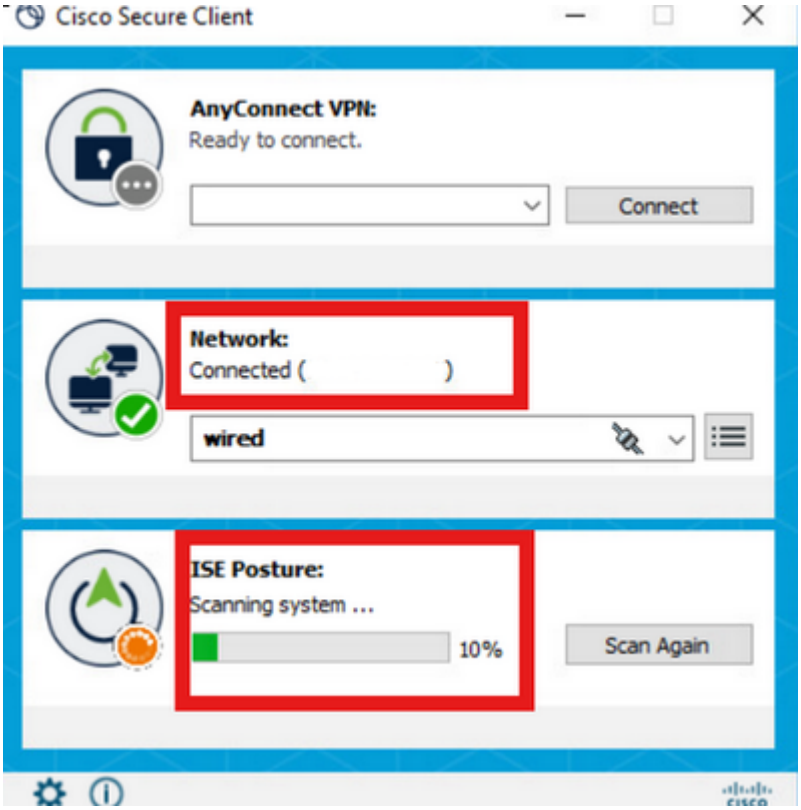


3.在NAM安装后会触发重新启动提示。单击 Yes。



步骤2. EAP-FAST

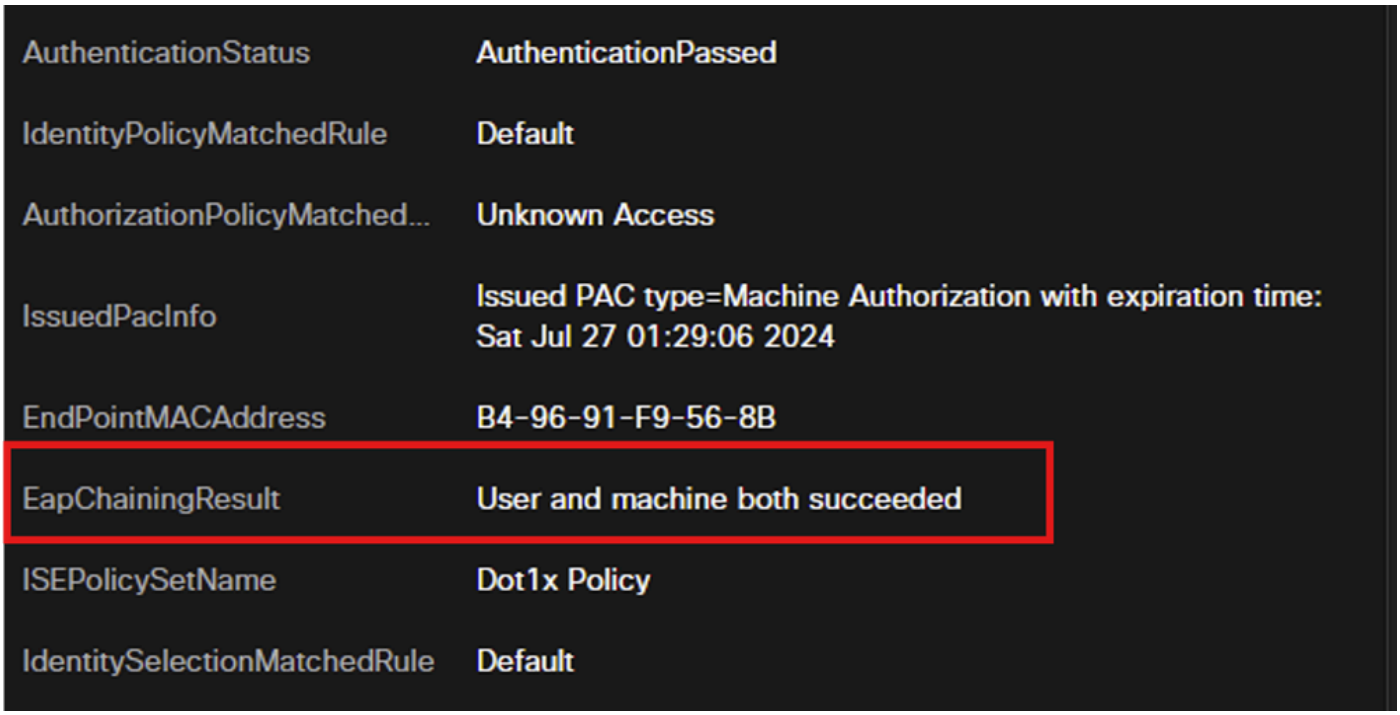
1.在PC重新启动且用户登录后，NAM通过EAP-FAST对用户和计算机进行身份验证。如果终端身份验证正确，NAM显示其已连接，并且终端安全评估模块触发终端安全评估扫描。



2.在ISE实时日志中，终端现在触碰未知访问规则。

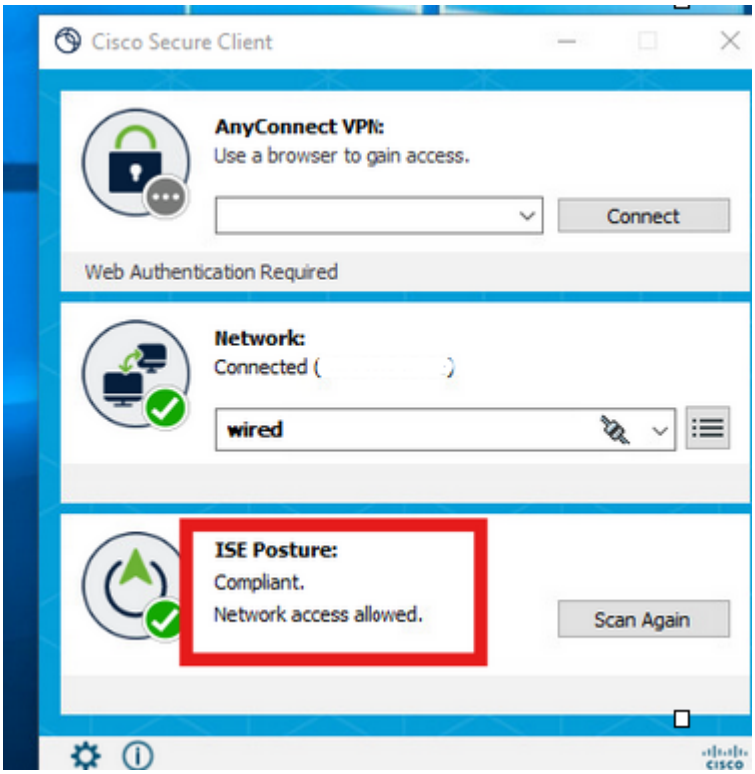


3.现在，根据NAM配置文件配置，身份验证协议为EAP-FAST，并且EAP-Chaining结果为Successful。



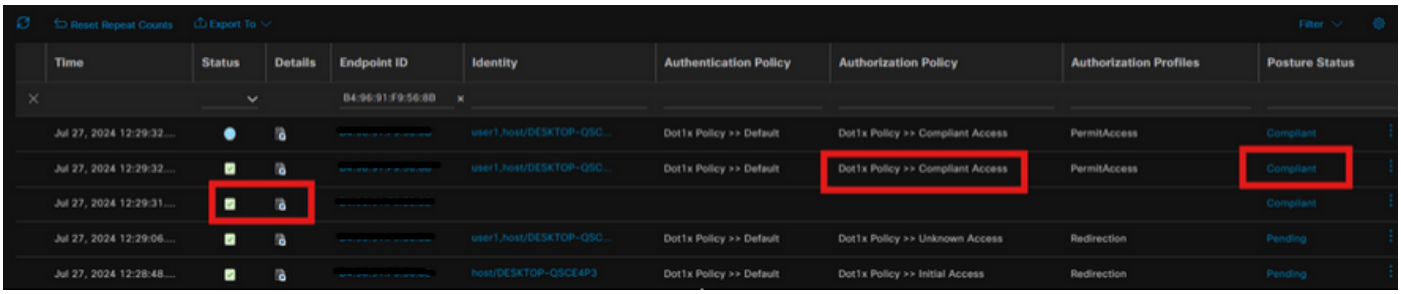
步骤3.状态扫描

1.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。



---

2. CoA在终端安全评估扫描后触发，且终端现在符合投诉访问策略。

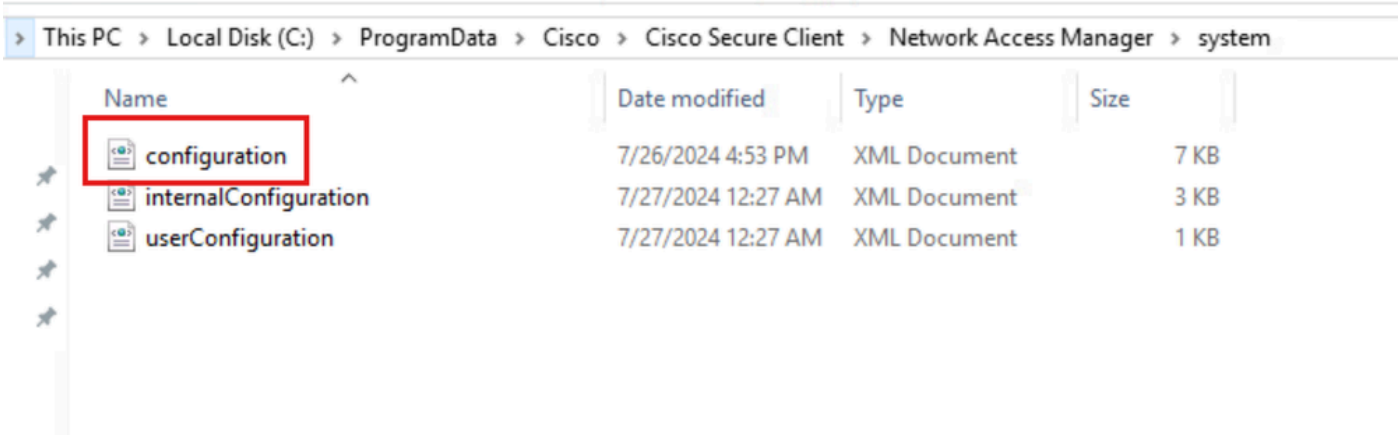


故障排除

步骤1. NAM配置文件

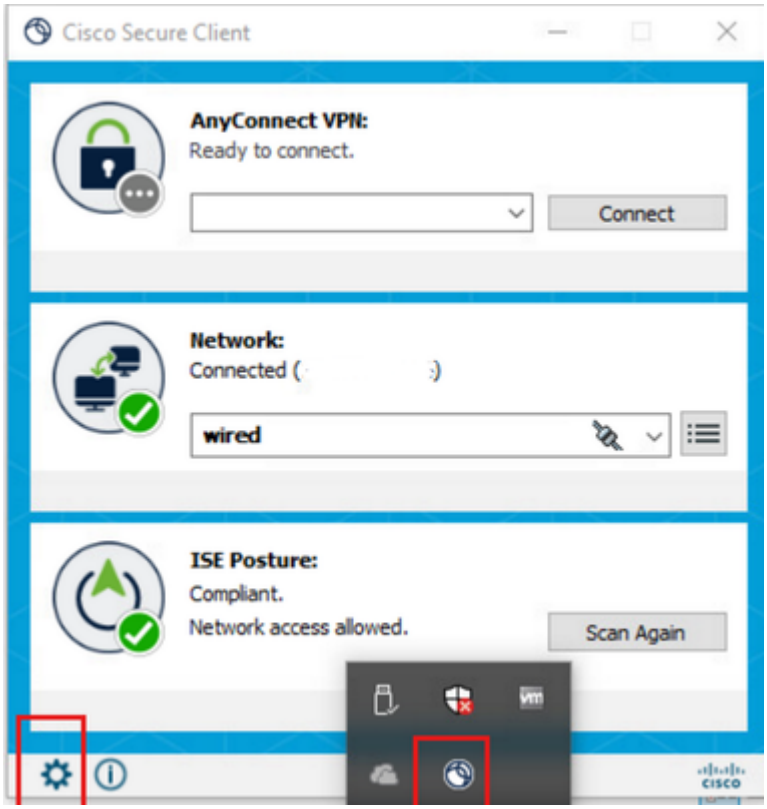
1.在安装NAM模块后，验证NAM配置文件configuration.xml是否存在于您的PC上的此路径中：C:\ProgramData\Cisco\Cisco Secure Client\Network Access Manager\system

---



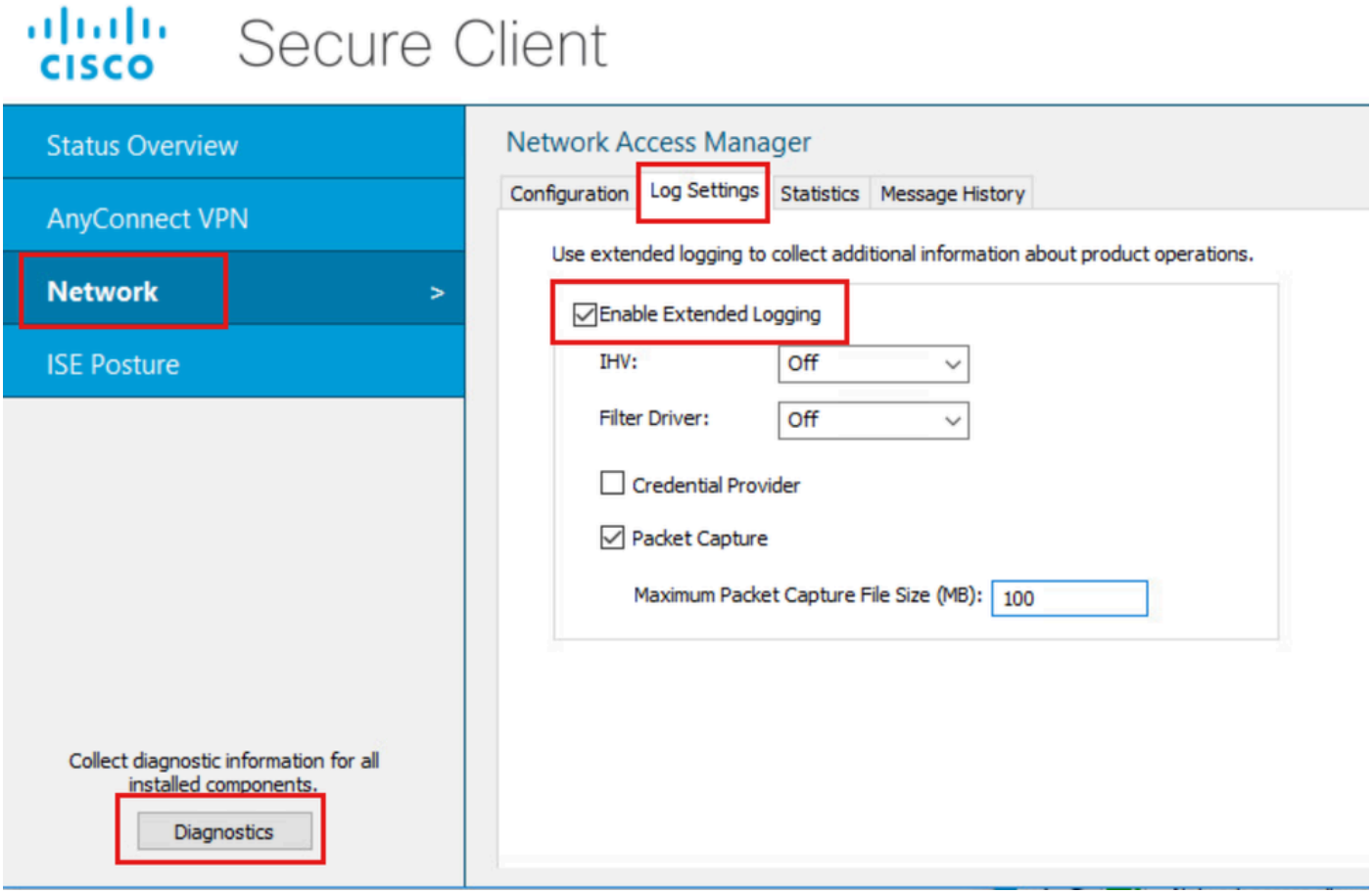
步骤2. NAM扩展日志记录

1.从任务栏中单击Secure Client图标，然后选择Settings图标。



2.定位至网络>日志设置标签。选中Enable Extended Logging复选框。

3.将数据包捕获文件大小设置为100 MB。重现问题后，点击诊断在终端上创建DART捆绑包。



---

4. 消息历史记录部分显示已完成的每个步骤的详细信息。

步骤3.在交换机上进行调试

1.在交换机上启用这些调试，以排除dot1x和重定向流程故障：

- 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

---

要查看日志，请执行以下操作：

- show logging
- show logging process smd internal

步骤4.在ISE上进行调试

1.收集具有以下属性的ISE支持捆绑包，在调试级别设置：

- 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

- 使用Windows和ISE 3.2为Dot1x配置安全客户端NAM
- ISE终端安全评估规范部署指南
- Cisco IOS® XE 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）。