WindowsでのISE 3.3によるセキュアなクライアントNAMプロファイルの設定と導入

内容

はじめに

このドキュメントでは、Identity Services Engine(ISE)を介してCisco Secure Client Network Access Manager(NAM)プロファイルを導入する方法について説明します。

背景説明

EAP-FAST認証は2つのフェーズで行われます。最初のフェーズでは、EAP-FASTはTLSハンドシェイクを使用して、Type-Length-Value(TLV)オブジェクトを使用したキー交換を提供および認証し、保護されたトンネルを確立します。これらのTLVオブジェクトは、クライアントとサーバの間で認証関連のデータを伝送するために使用されます。トンネルが確立されると、2番目のフェーズが開始され、クライアントとISEノードがさらに対話して、必要な認証および認可ポリシーを確立します。

NAM設定プロファイルは、認証方式としてEAP-FASTを使用するように設定され、管理上定義されたネットワークで使用できます。
さらに、マシンとユーザの両方の接続タイプをNAM設定プロファイル内で設定できます。
企業のWindowsデバイスは、ポスチャチェック付きのNAMを使用して企業のフルアクセスを取得します。
パーソナルWindowsデバイスは、同じNAM設定を使用して、制限されたネットワークにアクセスします。

このドキュメントでは、Web展開を使用したIdentity Services Engine(ISE)ポスチャポータル経由でのCisco Secure Client Network Access Manager(NAM)プロファイルの展開手順と、ポスチャコンプライアンスチェックについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Identity Services Engine（ISE）
- AnyConnect NAMおよびプロファイルエディタ
- ポスチャ ポリシー
- 802.1xサービス用のCisco Catalyst設定

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

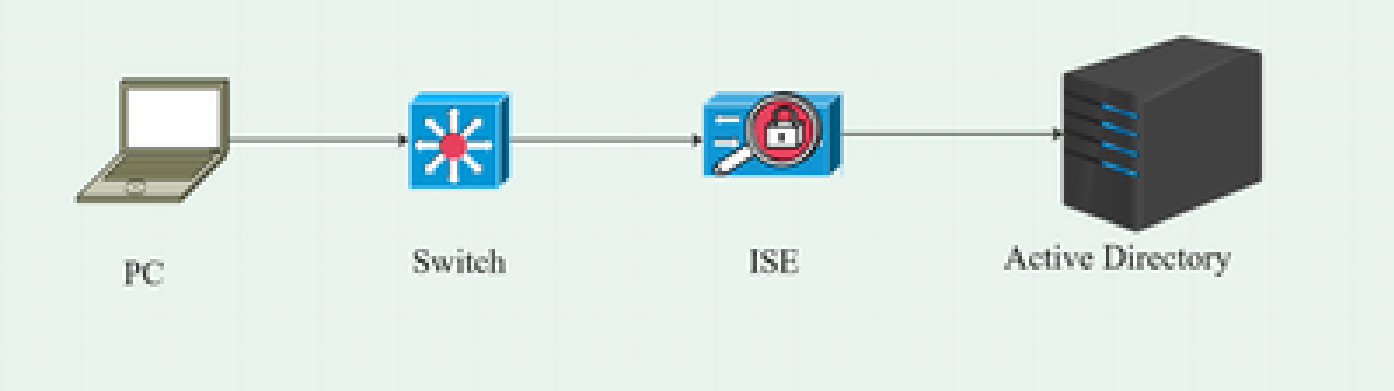
- Cisco ISE リリース 3.3 以降
- Cisco Secure Mobility Client 5.1.4.74以降がインストールされたWindows 10
- ソフトウェアCisco IOS® XE 17.6.5以降が稼働するCisco Catalyst 9200スイッチ
- Active Directory 2016

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して

ください。

コンフィギュレーション

ネットワーク図



データフロー

PCがネットワークに接続すると、ISEはポスチャポータルへのリダイレクト用の認可ポリシーを提供します。
PC上のhttpトラフィックは、ISEからNSAアプリケーションがダウンロードされるISEクライアントプロビジョニングページにリダイレクトされます。
その後、NSAはPCにセキュアクライアントエージェントモジュールをインストールします。
エージェントのインストールが完了すると、エージェントはISEで設定されたポスチャプロファイルとNAMプロファイルをダウンロードします。
NAMモジュールをインストールすると、PCの再起動がトリガーされます。
再起動後、NAMモジュールはNAMプロファイルに基づいてEAP-FAST認証を実行します。
その後、ポスチャスキャンがトリガーされ、ISEポスチャポリシーに基づいてコンプライアンスがチェックされます。

スイッチの設定

dot1x認証およびリダイレクション用にアクセススイッチを設定します。

```
aaa new-model

aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius ( aaaアカウンティングdot1xデフォルトの開始/停止グループradius )
aaaサーバradius dynamic-author
クライアント10.127.197.53サーバキーQwerty123
認証タイプany

aaa session-id共通
```

```
ip radius送信元インターフェイスVlan1000
radius-server attribute 6 on-for-login-auth
radius-server属性8 include-in-access-req
radius-server attribute 25 access-requestには次のものがあります
radius-server attribute 31 mac format ietf大文字
radiusサーバRAD1
address ipv4 <ISE server IP> auth-port 1812 acct-port 1813（オプション）
key <秘密キー>

dot1x system-auth-control
```

ユーザがISEクライアントプロビジョニングポータルにリダイレクトされるようにリダイレクトACLを設定します。

```
ipアクセスリスト拡張リダイレクトacl
10 deny udp any any eq domain（udpの拒否とeqドメイン）
20 deny tcp any any eq domain（tcpの拒否anyのeqドメイン）
30 deny udp any eq bootpc any eq bootps（udpのいずれかのeqのブートアップを拒否）
40 deny ip any host <ISEサーバIP>
50 permit tcp any any eq www
60 permit tcp any any eq 443
```

スイッチでデバイストラッキングとhttpリダイレクションを有効にします。

```
device-tracking policy <デバイストラッキングポリシー名>
 トラッキングの有効化
interface <interface name>
 device-tracking attach-policy <デバイストラッキングポリシー名>

ip http server
ip http secure-server（セキュアサーバ）
```

Secure Client Packageのダウンロード

プロファイルエディタ、セキュアクライアントウィンドウ、およびコンプライアンスモジュールwebdeployファイルを[software.cisco.com](software.cisco.com)から手動でダウンロードします。

製品名の検索バーで、「Secure Client 5」と入力します。

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

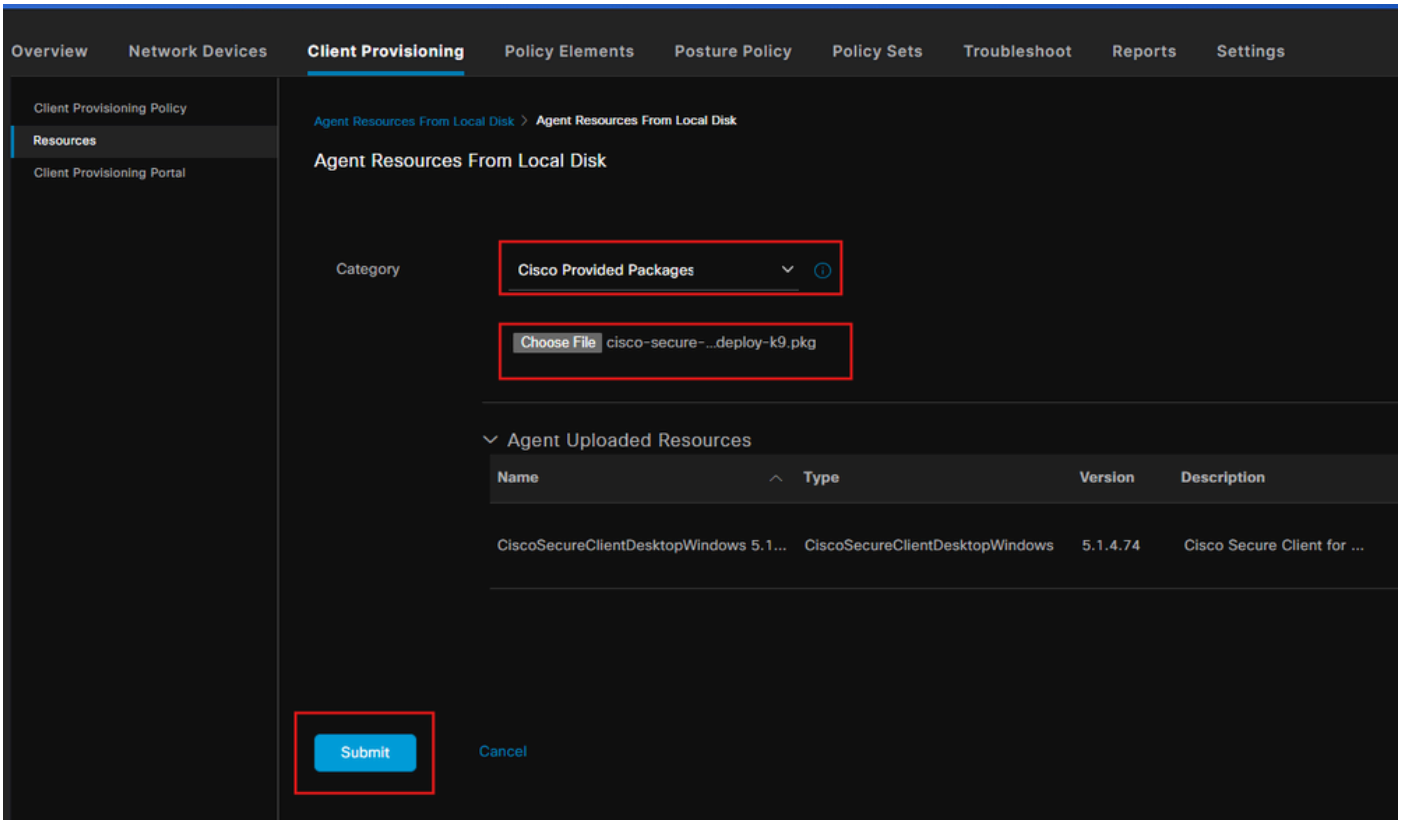
- cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg（入手可能）
- cisco-secure-client-win-4.3.4164.8192-isecompliance-webdeploy-k9.pkg（入手可能）

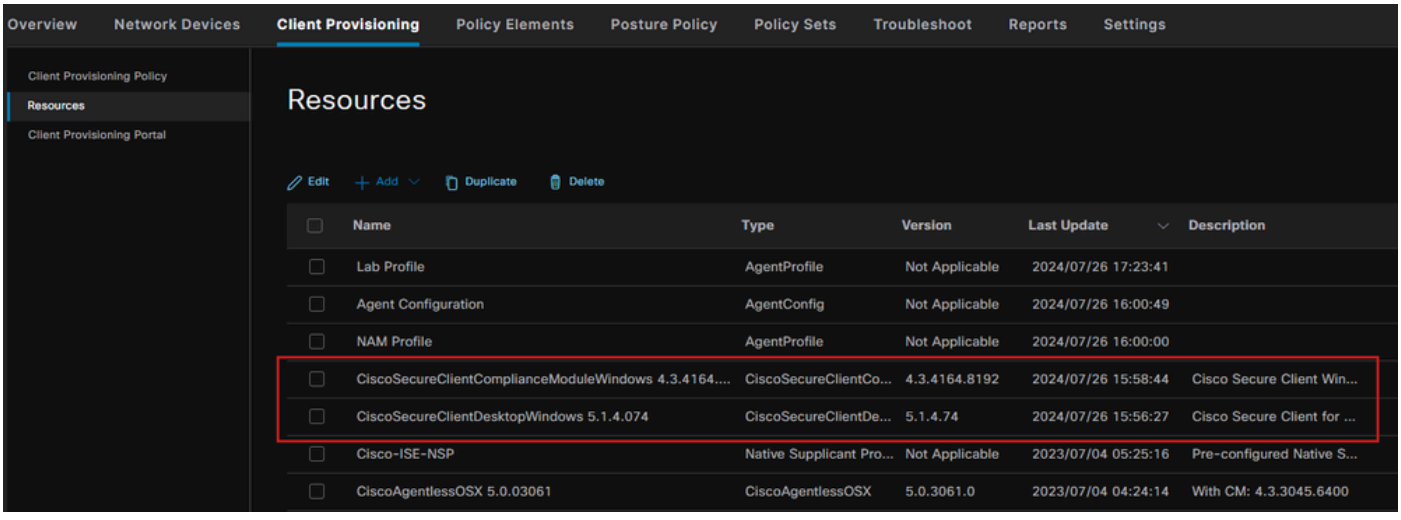
- ツール：cisco-secure-client-win-5.1.4.74-profileeditor-k9.msi

ISE 設定

ステップ 1：ISEでのパッケージのアップロード

ISEにセキュアクライアントおよびコンプライアンスモジュールWeb展開パッケージをアップロードするには、ローカルディスクからWorkcenter > Posture > Client Provisioning > Resources > Add > Agent Resourcesの順に移動します。





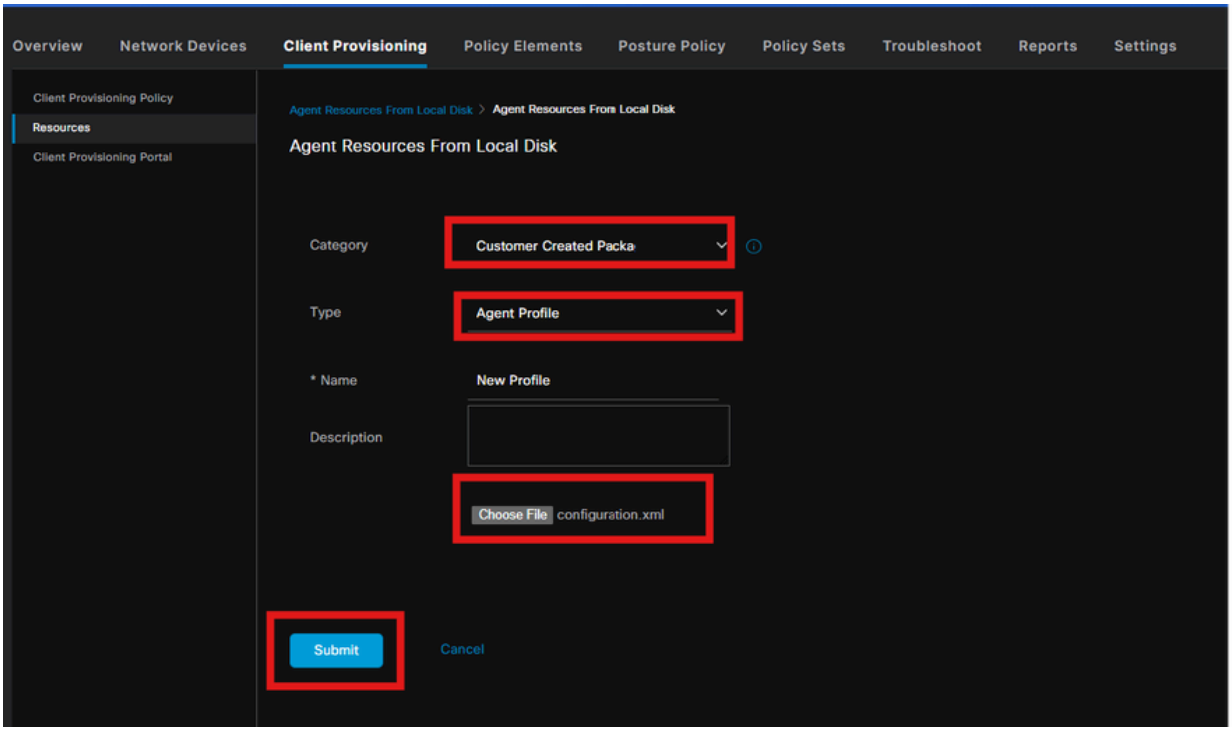
ステップ 2：プロファイルエディタツールからのNAMプロファイルの作成

NAMプロファイルの設定方法については、このガイドの「セキュアなクライアントNAMプロファ

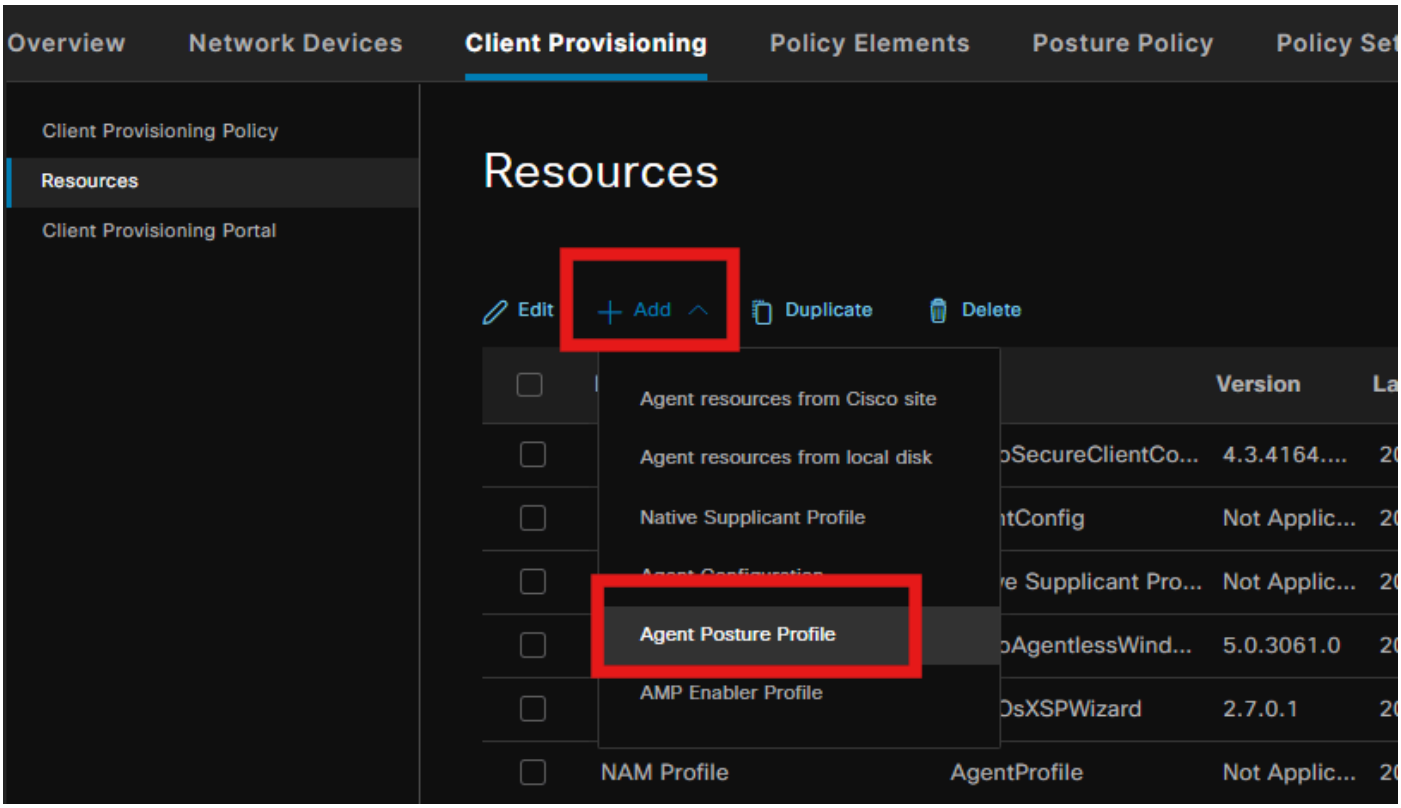
イルの設定」を参照してください。

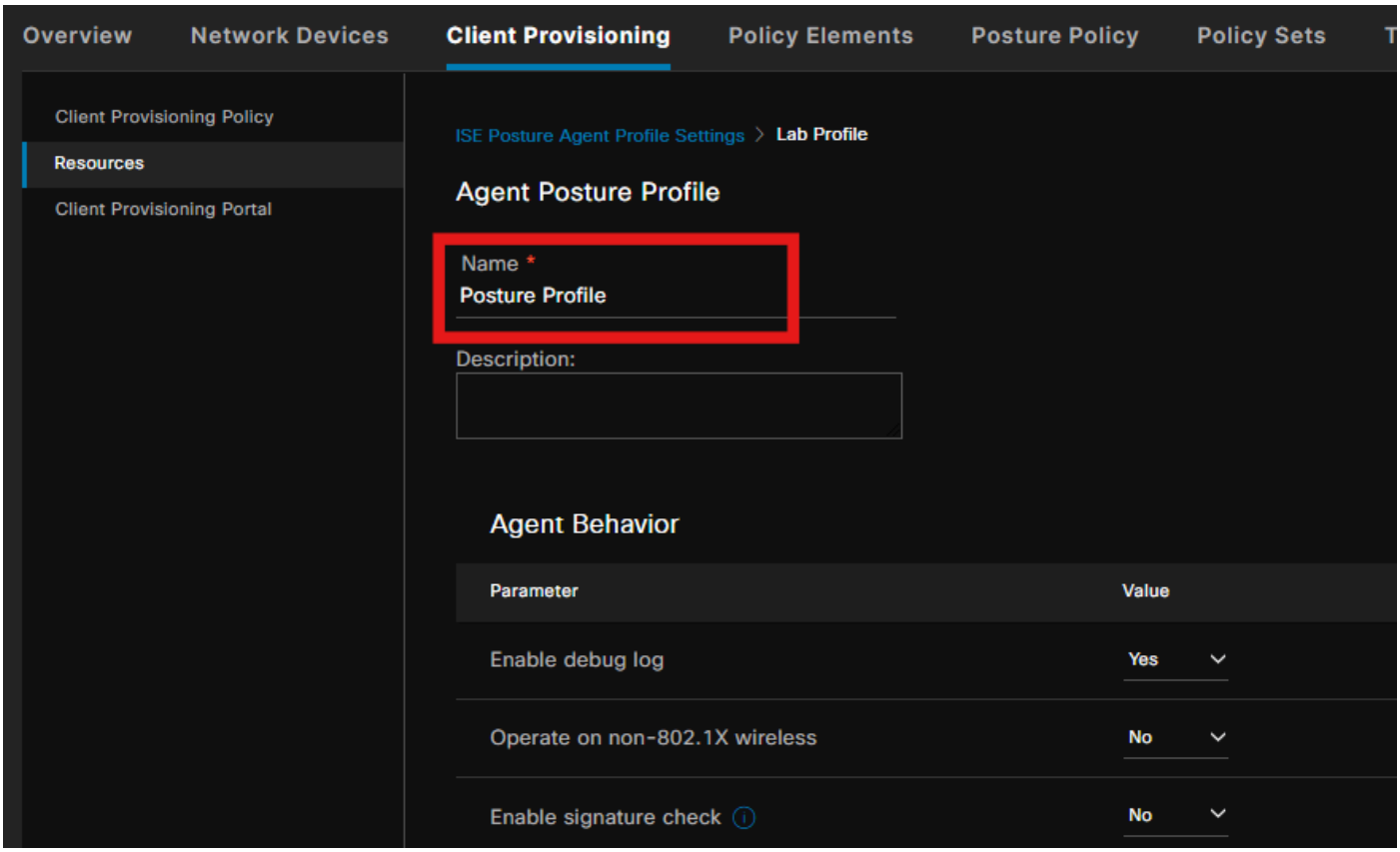
ステップ 3：ISEでのNAMプロファイルのアップロード

NAMプロファイル「Configuration.xml」をエージェントプロファイルとしてISEにアップロードするには、Client Provisioning > Resources > Agent Resources From Local Diskの順に移動します。



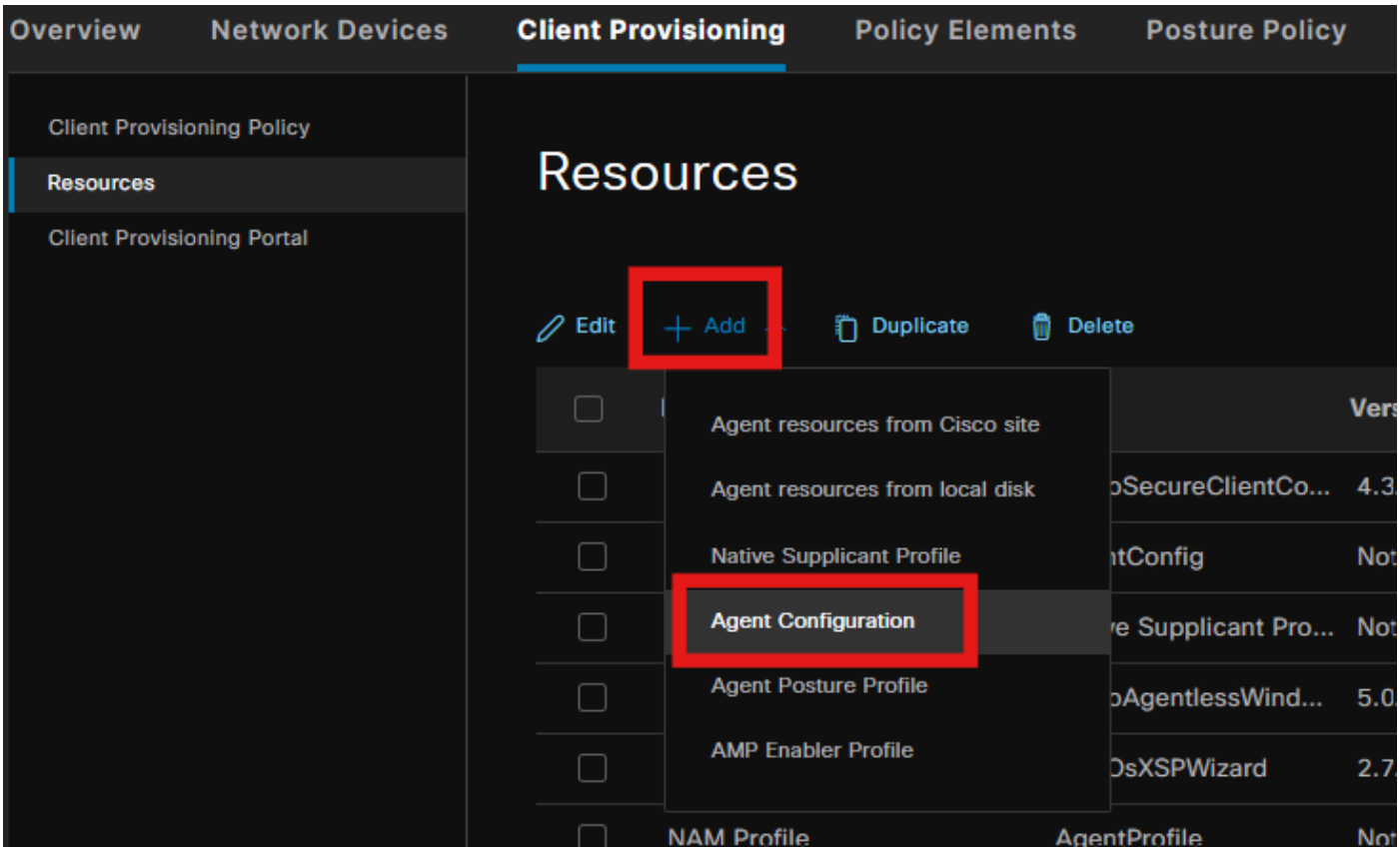
ステップ 4：ポスチャプロファイルの作成



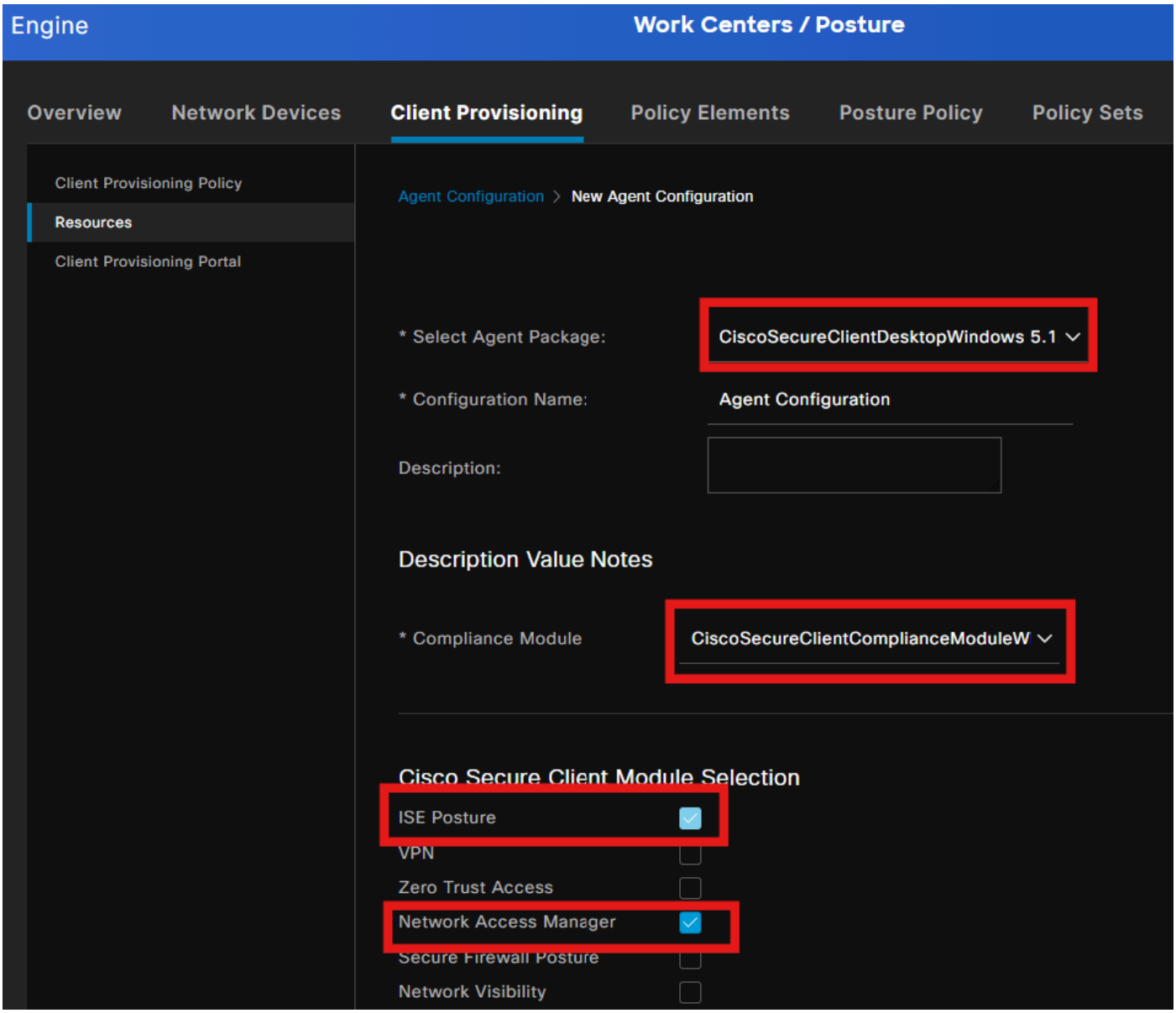


[Posture Protocol] セクションでは、エージェントがすべてのサーバに接続できるようにするために、* を忘れずに追加してください。

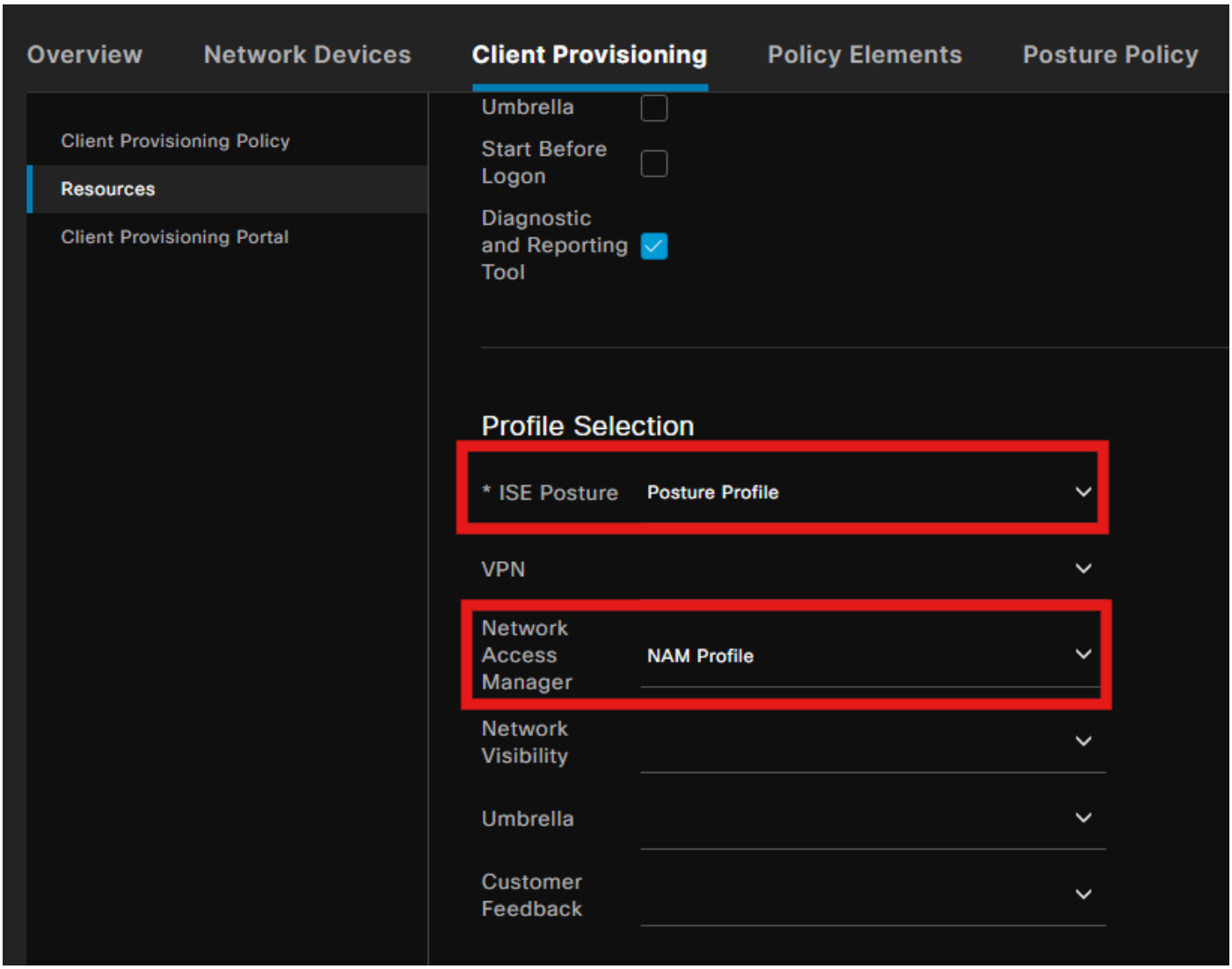
ステップ 5：エージェント構成の作成



アップロードされたセキュアクライアントとコンプライアンスモジュールパッケージを選択し、モジュール選択でISEポスチャ、NAM、およびDARTモジュールを選択します

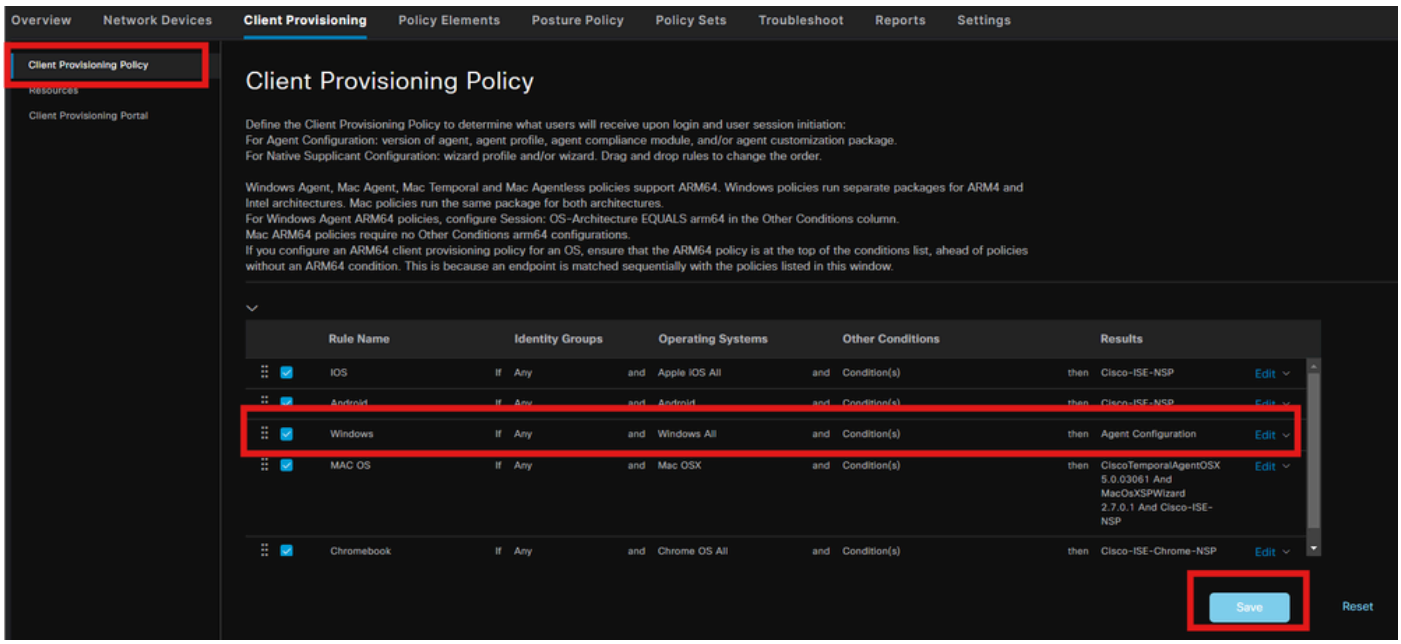


Profile selectで、PostureおよびNAMプロファイルを選択し、Submitをクリックします。



手順 6：クライアントプロビジョニングポリシー

Windowsオペレーティングシステム用のクライアントプロビジョニングポリシーを作成し、前の手順で作成したエージェント設定を選択します。

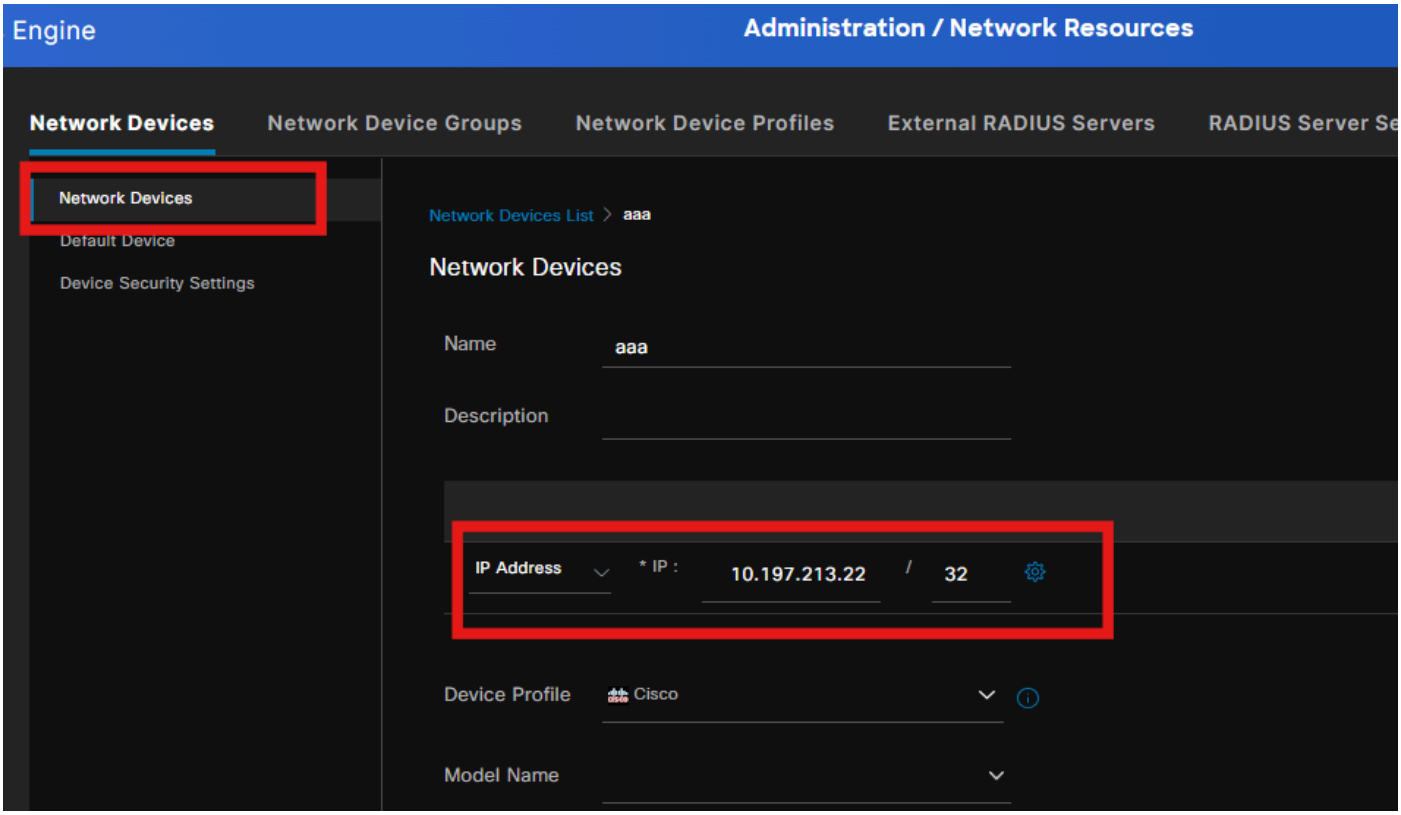


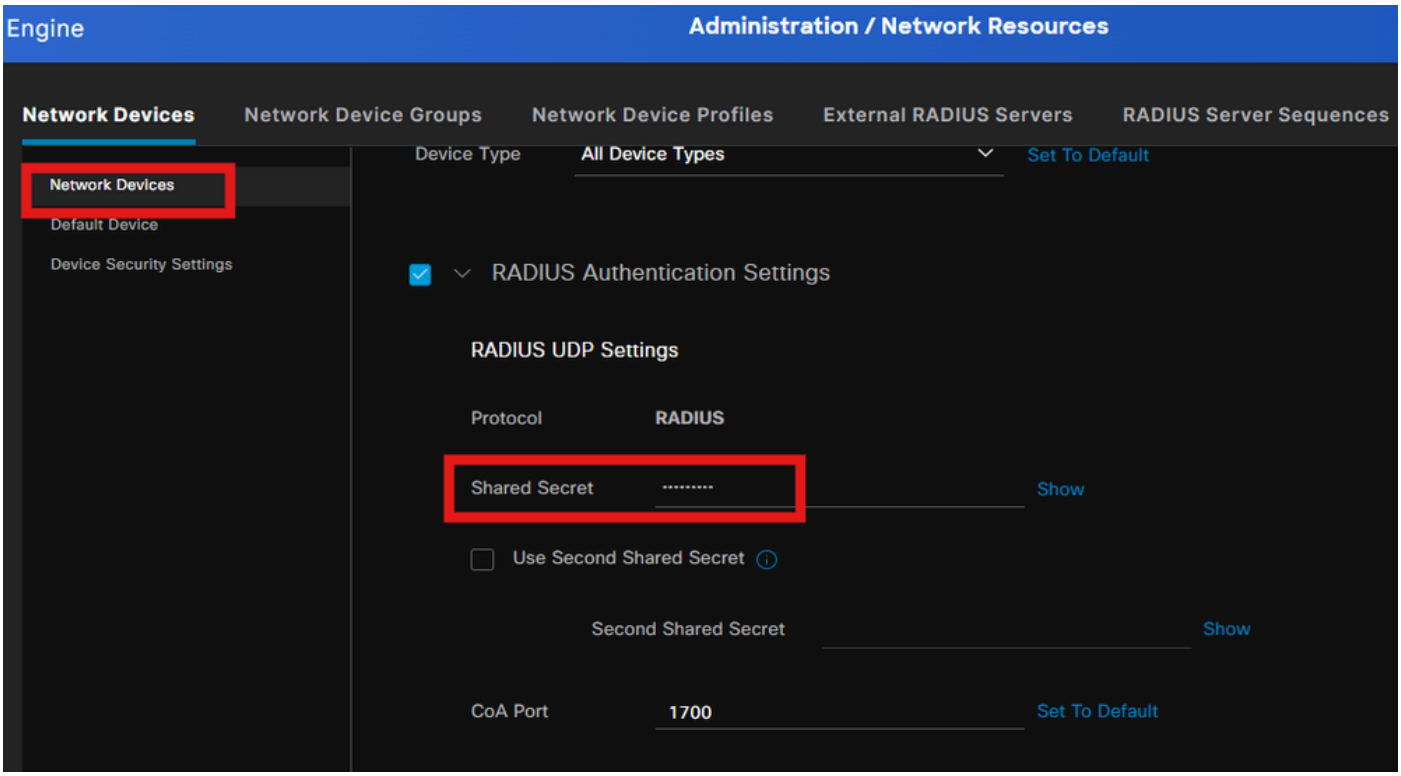
手順 7：ポスチャ ポリシー

ポスチャポリシーと条件の作成方法については、このガイドの『ISEポスチャ規範的導入ガイド』を参照してください。

ステップ 8：ネットワーク デバイスの追加

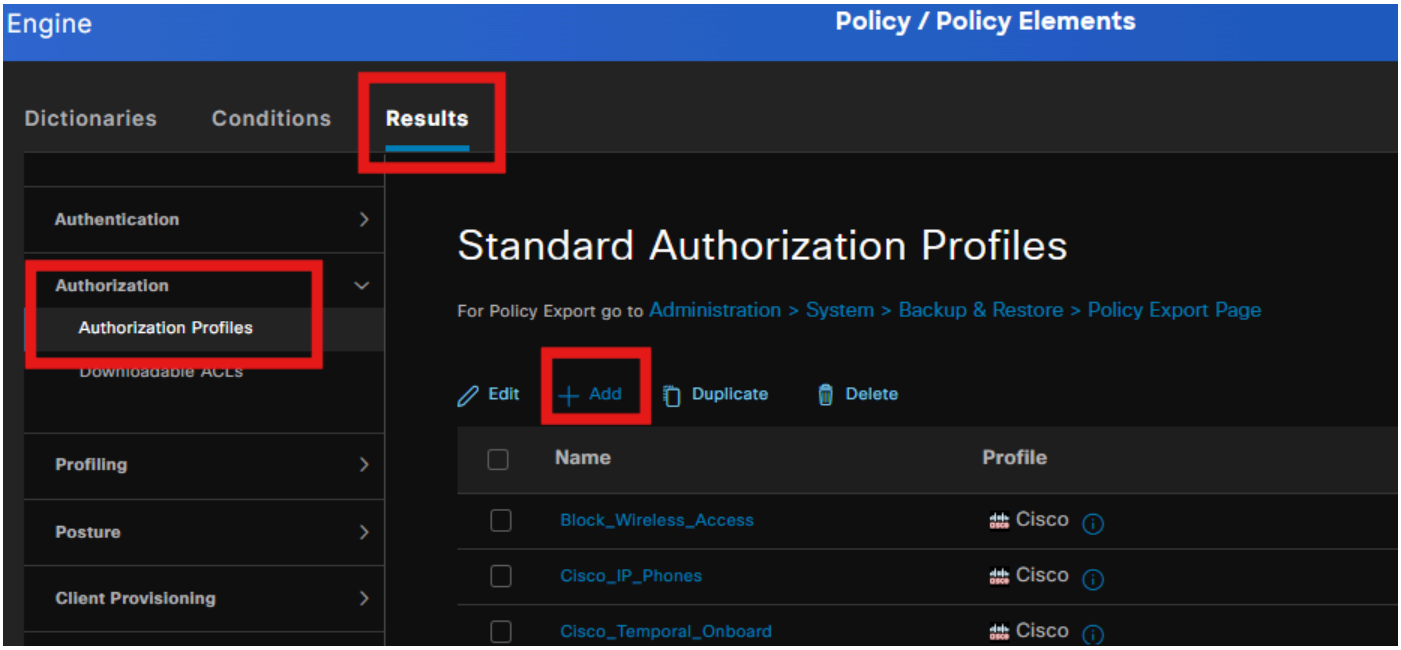
スイッチのIPアドレスとRADIUS共有秘密キーを追加するには、Administration > Network Resourcesの順に移動します。



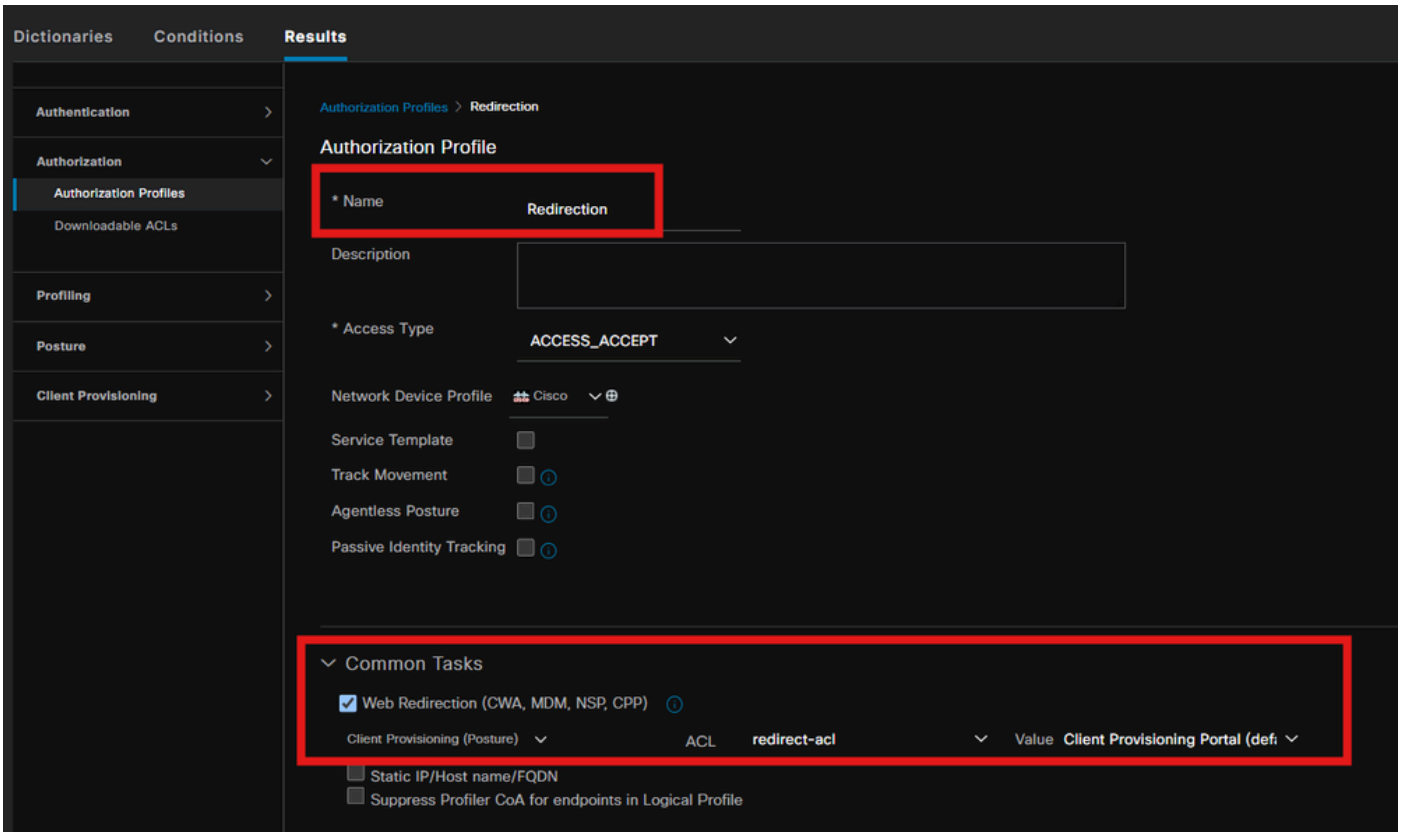


ステップ 9：許可プロファイル

ポスチャリダイレクトプロファイルを作成するには、Policy > Policy Elements > Resultsの順に移動します。

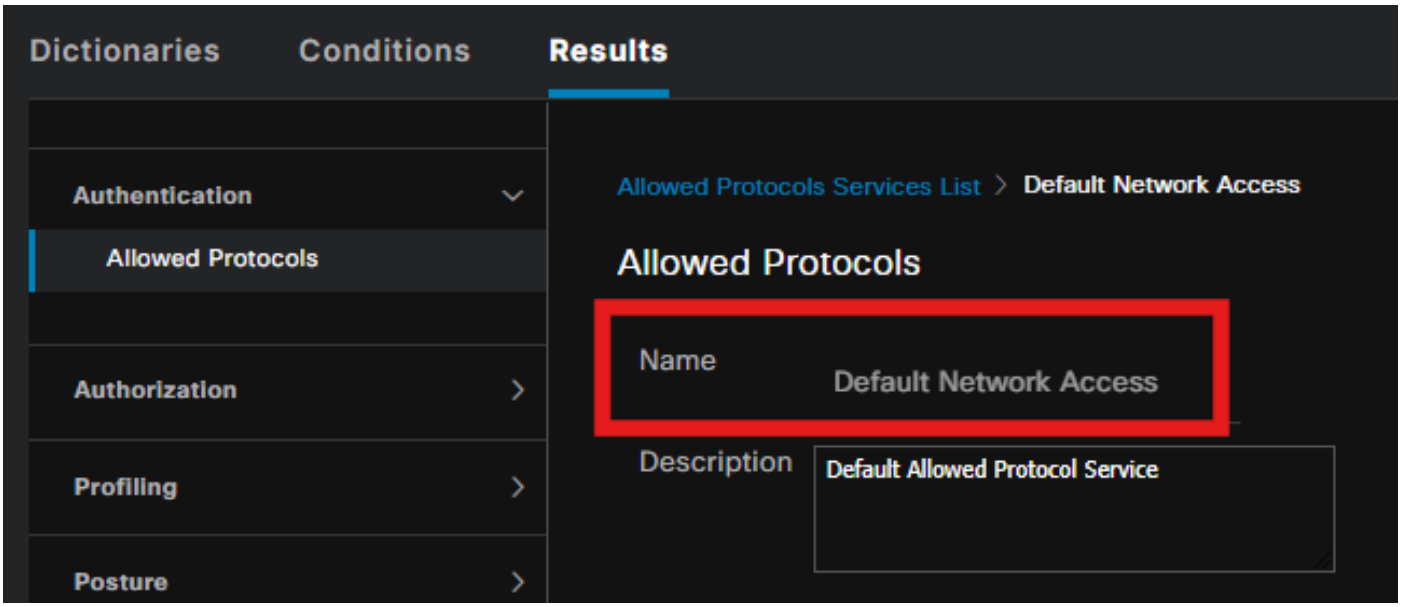


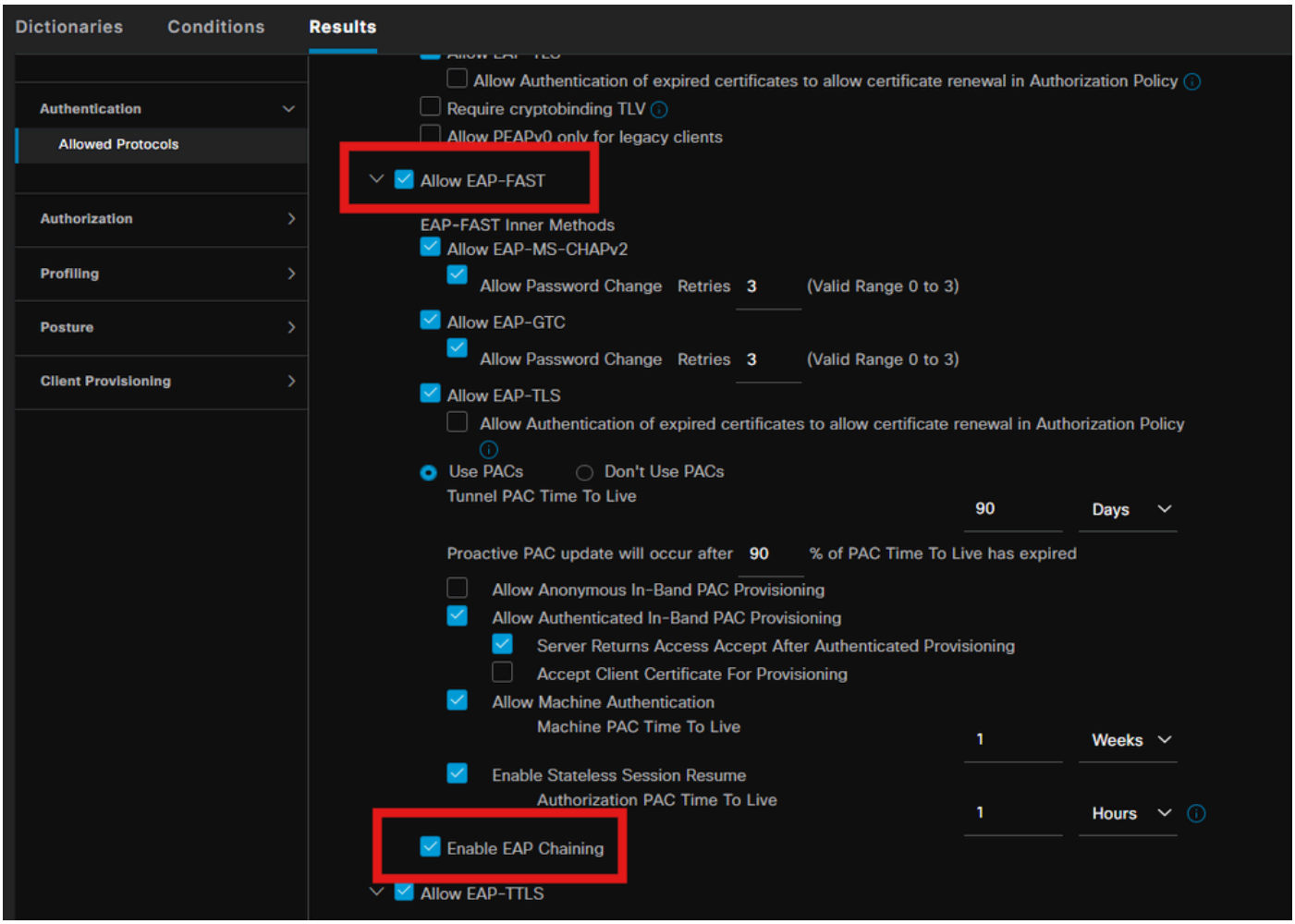
コマンドタスクで、リダイレクトACLを使用するクライアントプロビジョニングポータルを選択します。



ステップ 10：許可されたプロトコル

Policy > Policy elements > Results > Authentication > Allowed Protocolsの順に移動し、EAP Chaining設定を選択します。

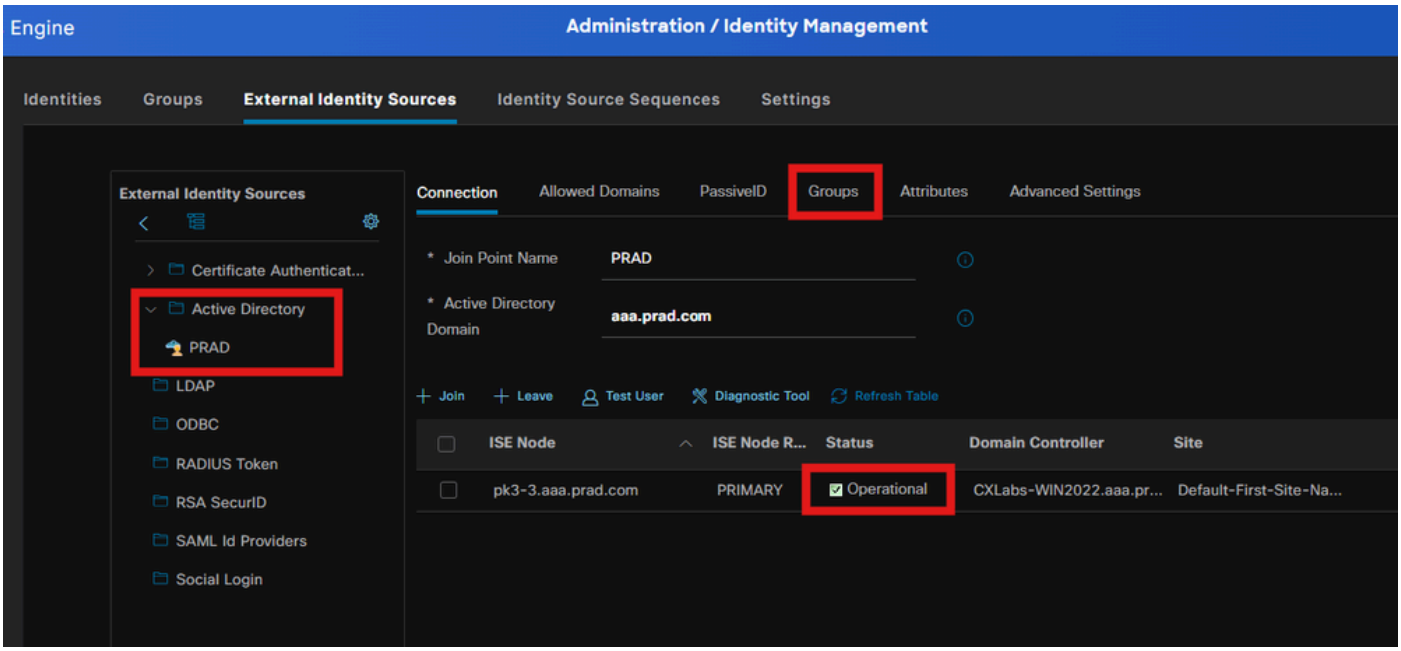




ステップ 11Active Directory

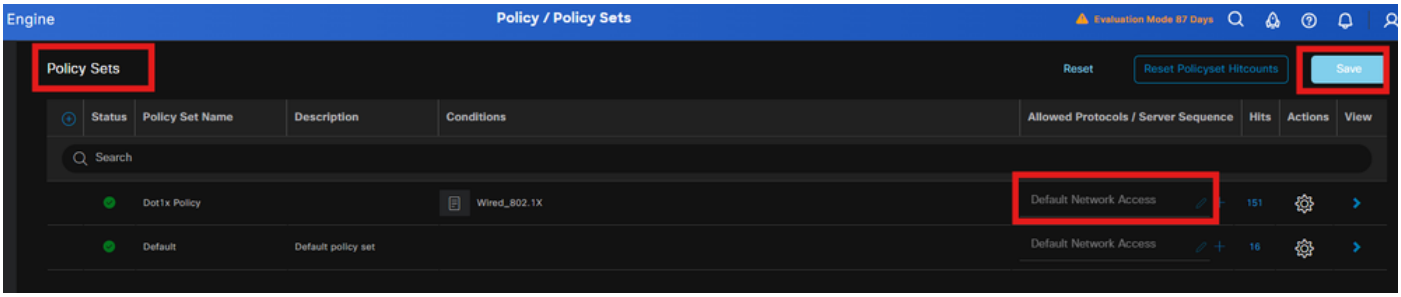
ISEがActive Directoryドメインに参加していること、および許可条件で必要な場合はドメイングループが選択されていることを確認します。

[管理]>[アイデンティティ管理]>[外部アイデンティティ・ソース]>[Active Directory]

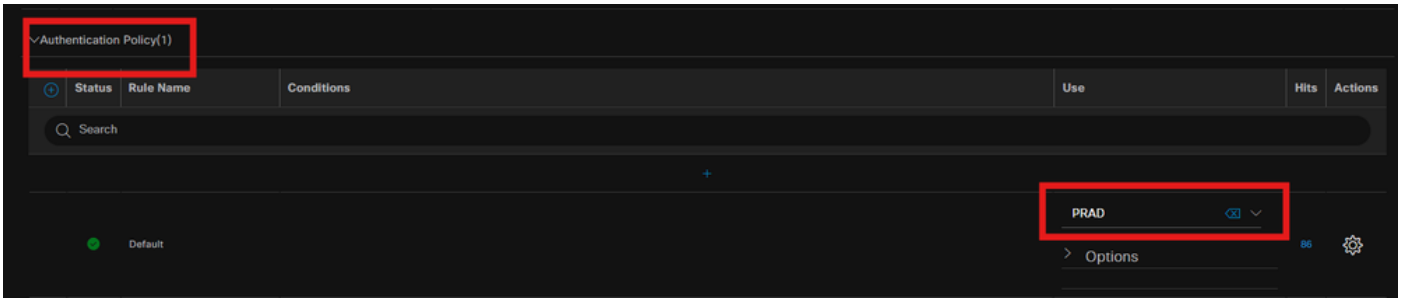


ステップ 12ポリシーセット

dot1x要求を認証するためのポリシーセットをISEで作成します。Policy > Policy setsの順に移動します。



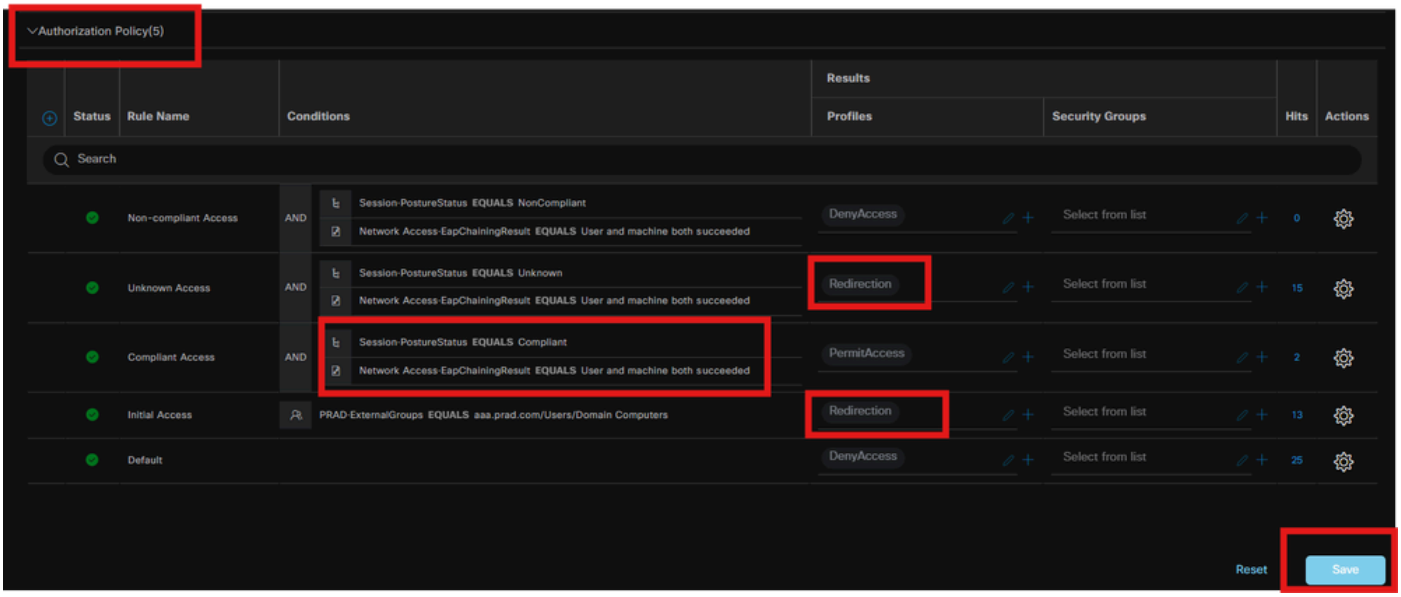
認証ポリシーのアイデンティティ・ ソースとしてActive Directoryを選択します。



不明なポスチャステータス、非準拠、および準拠のポスチャステータスに基づいて、異なる認証ルールを設定します。

この使用例では、

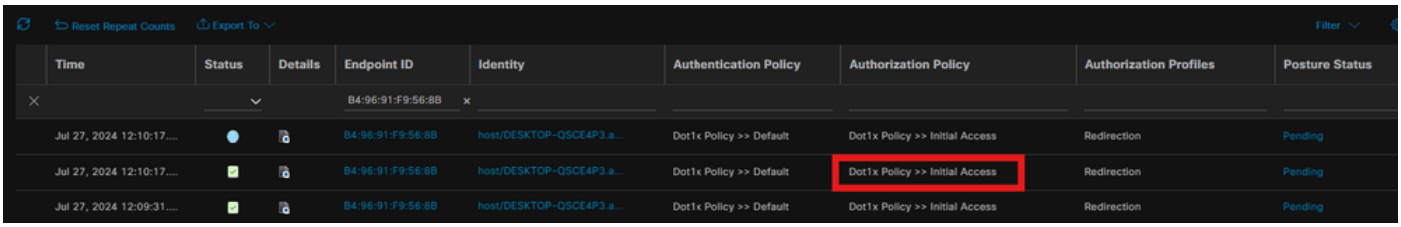
- 初期アクセス：セキュアクライアントエージェントとNAMプロファイルをインストールするためのISEクライアントプロビジョニングポータルへのリダイレクト
- 不明なアクセス：リダイレクトベースのポスチャ検出のためのクライアントプロビジョニングポータルへのアクセス
- 準拠アクセス：フルネットワークアクセス
- 非準拠：アクセスの拒否



確認

ステップ 1：ISEからのセキュアクライアントポスチャ/NAMモジュールのダウンロードとインストール

「Initial Access」認可ルールを使用して、dot1xで認証されたエンドポイントを選択します。Operations > Radius > Live Logsの順に移動します。



スイッチで、エンドポイントに適用されるリダイレクトURLとACLを指定します。

```
Switch#show authentication session interface te1/0/24の詳細
インターフェイス：TenGigabitEthernet1/0/24
IIF-ID: 0x19262768
MACアドレス：x4x6.xxxx.xxxx
IPv6アドレス：不明
IPv4アドレス： <client-IP>
ユーザ名：host/DESKTOP-xxxxxx.aaa.prad.com
ステータス：承認済み
ドメイン：DATA
Operホストモード：単一ホスト
Oper control dir:both（オペレーションコントロールディレクトリ：両方）
セッションタイムアウト：該当なし
共通セッションID:16D5C50A0000002CF067366B
アカウントセッションID: 0x0000001f
```

ハンドル： 0x7a000017
現在のポリシー：POLICY_Te1/0/24

ローカルポリシー：
サービステンプレート：DEFAULT_LINKSEC_POLICY_SHOULD_SECURE（優先度150）
セキュリティポリシー：セキュリティ保護すべき
セキュリティの状態：リンクは保護されていません

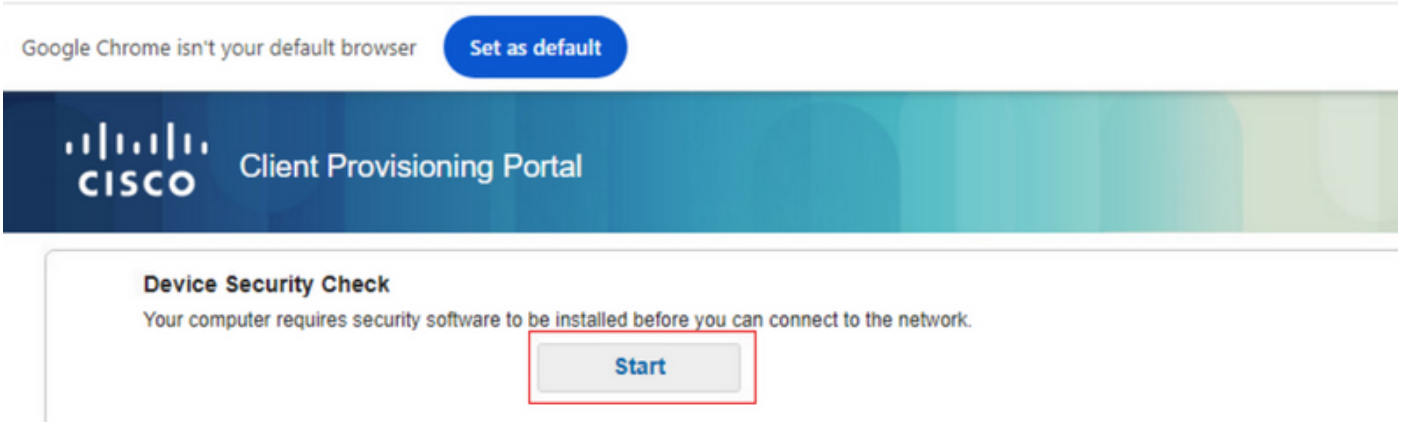
サーバポリシー：
URLリダイレクトACL:redirect-acl
URLリダイレクト
：https://ise33.aaa.prad.com:8443/portal/gateway?sessionId=16D5C50A0000002CF067366A&portal=ee
7180-4995-8aa2-9fb282645a8f&action=cpp&token=518f857900a37f9afc6d2da8b6fe3bc2
ACS ACL:xACSACLx-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3

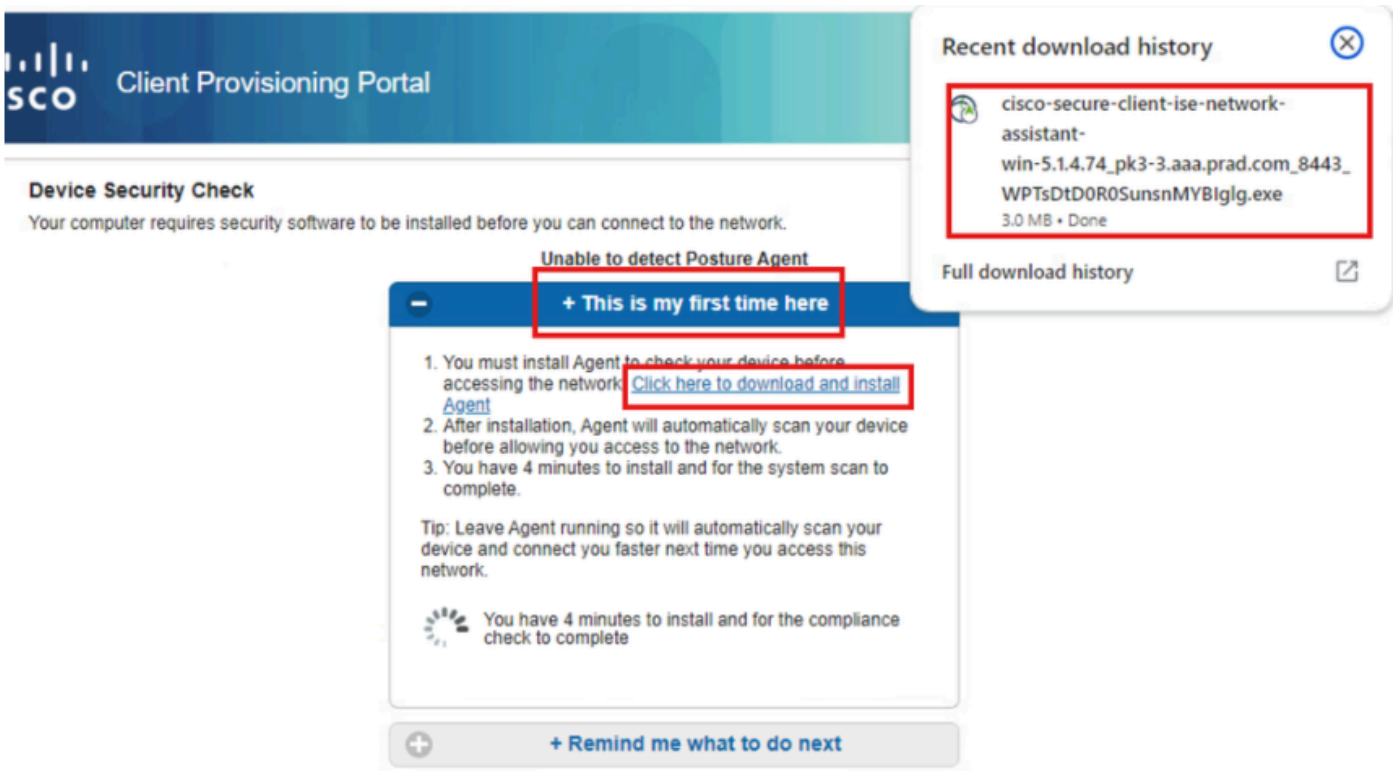
メソッドステータスリスト：
メソッドの状態
dot1x認証成功

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

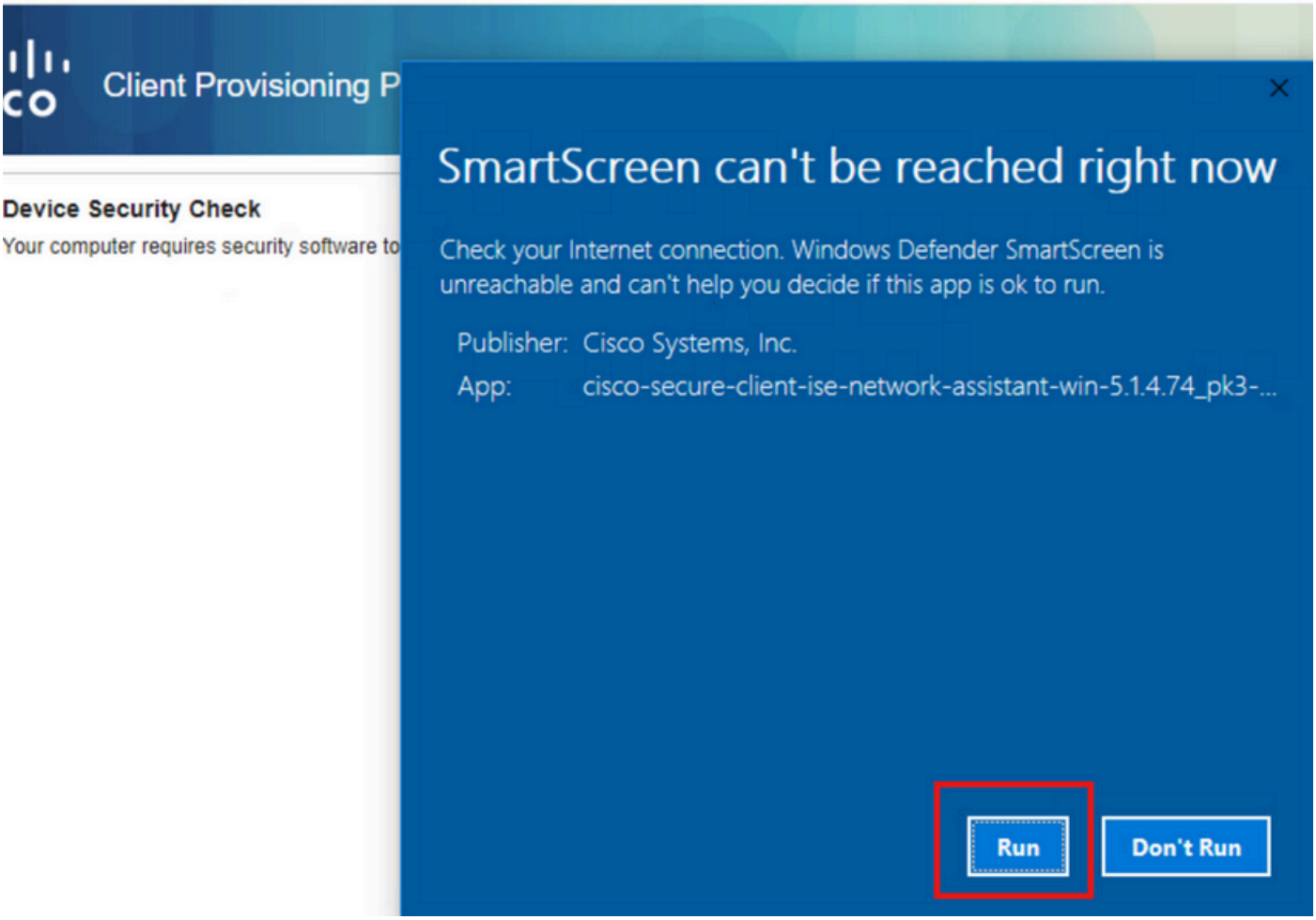
ネットワーク層アドレスリンク層アドレスインターフェイスvlan prlvl経過時間ステート残り時間
ARP X.X.X.X b496.91f9.568b Te1/0/24 1000 0005 4mn REACHABLE 39 s try 0

エンドポイントで、ISEポスチャにリダイレクトされたトラフィックを確認し、Startをクリックしてエンドポイントの Network Setup Assistantをダウンロードします。



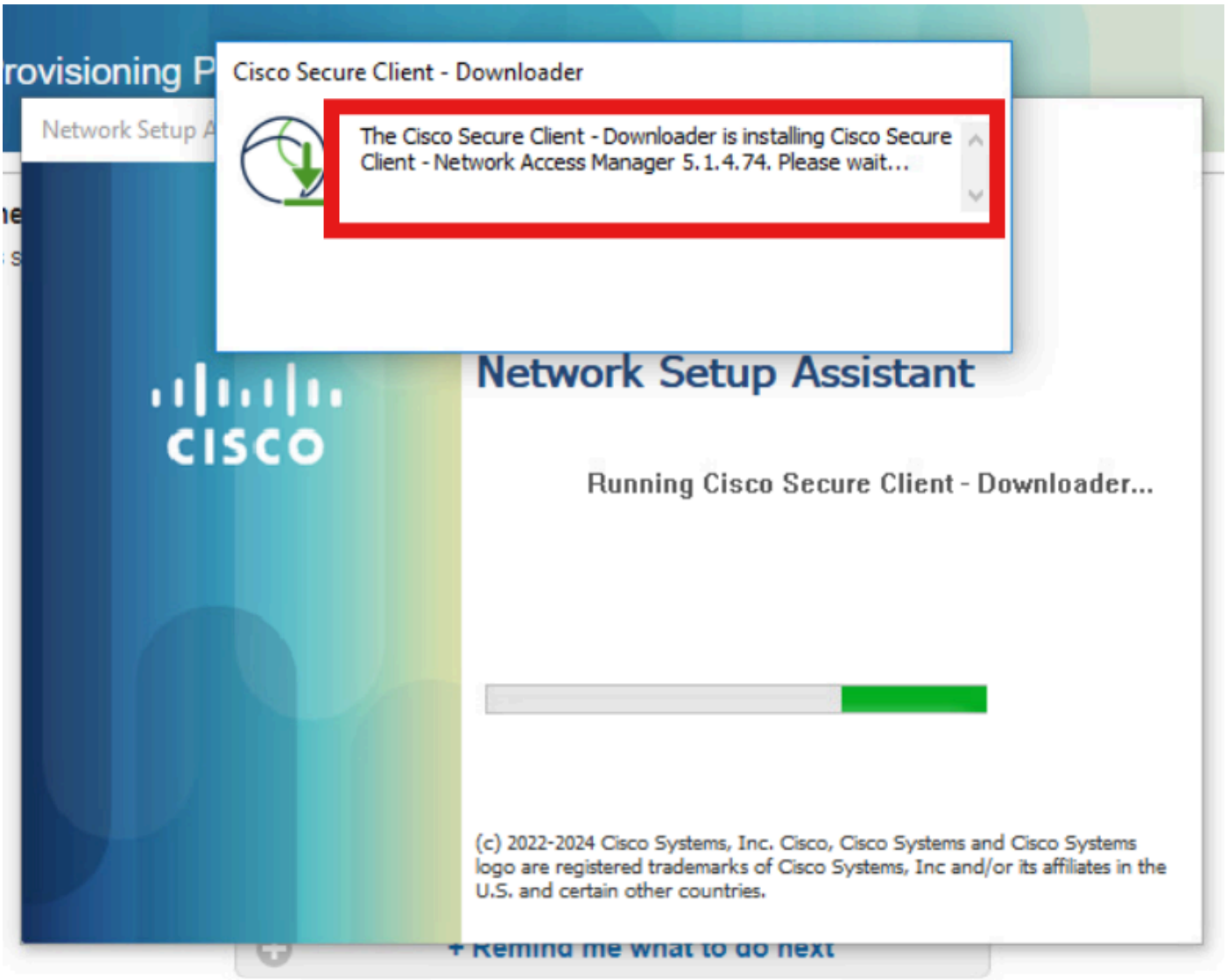


Runをクリックして、NSAアプリケーションをインストールします。

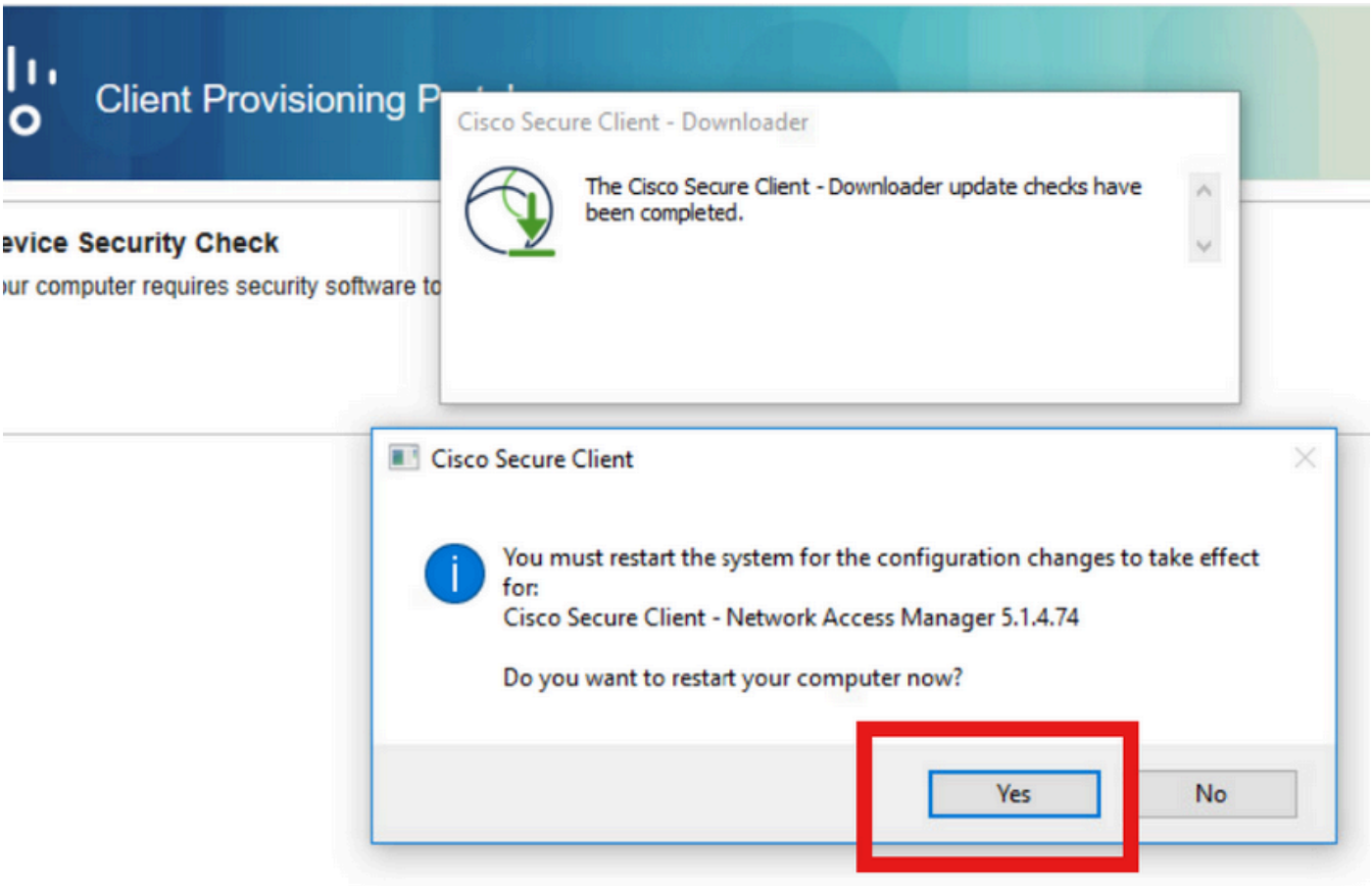


これで、NSAはISEからセキュアクライアントエージェント(CSA)ダウンロードを起動し、ポスチ

ャ、NAMモジュール、およびNAMプロファイルconfiguration.xmlをインストールします。



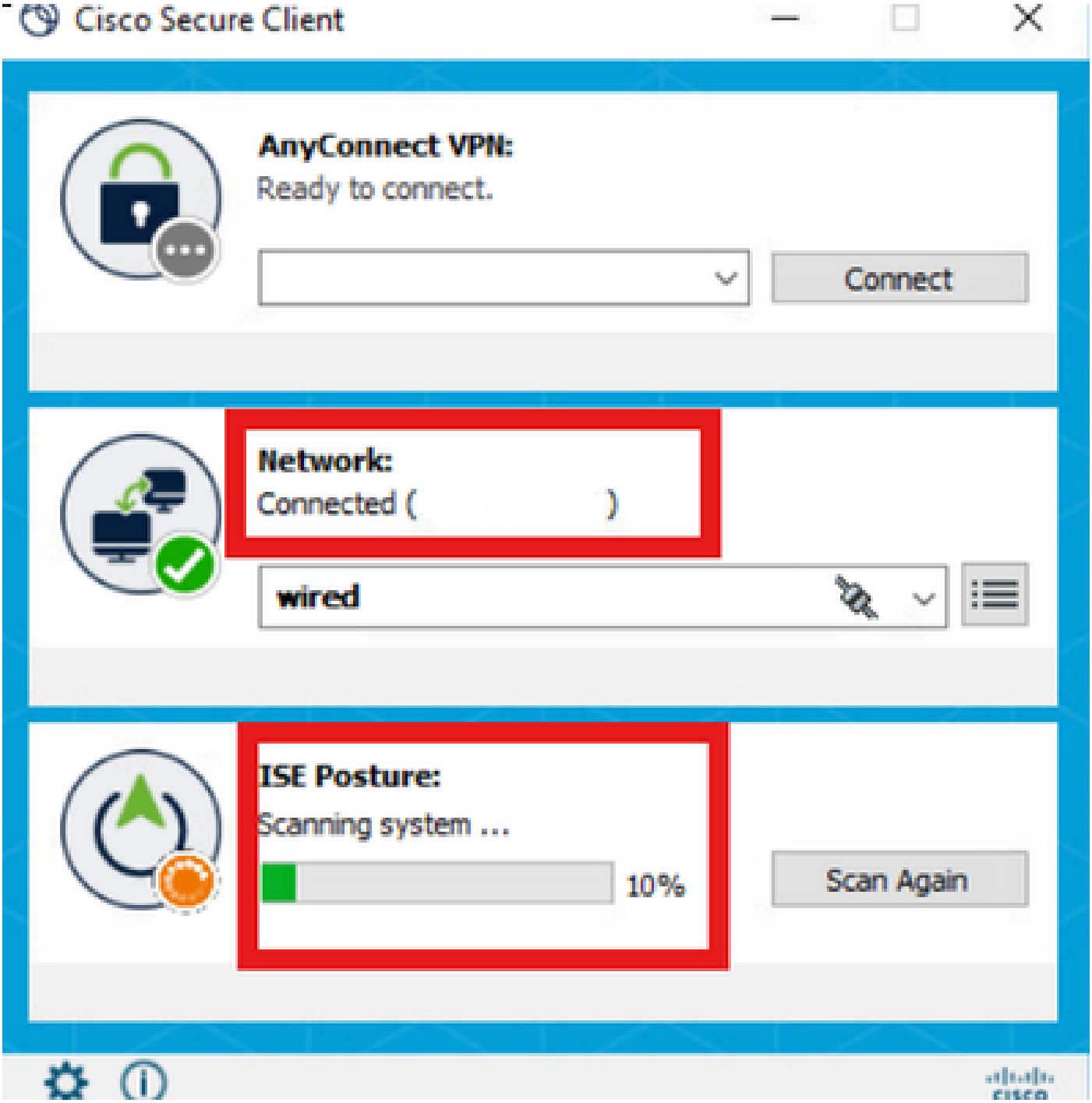
NAMのインストール後に再起動プロンプトが表示される。[Yes] をクリックします。



ステップ 2：EAP-FAST

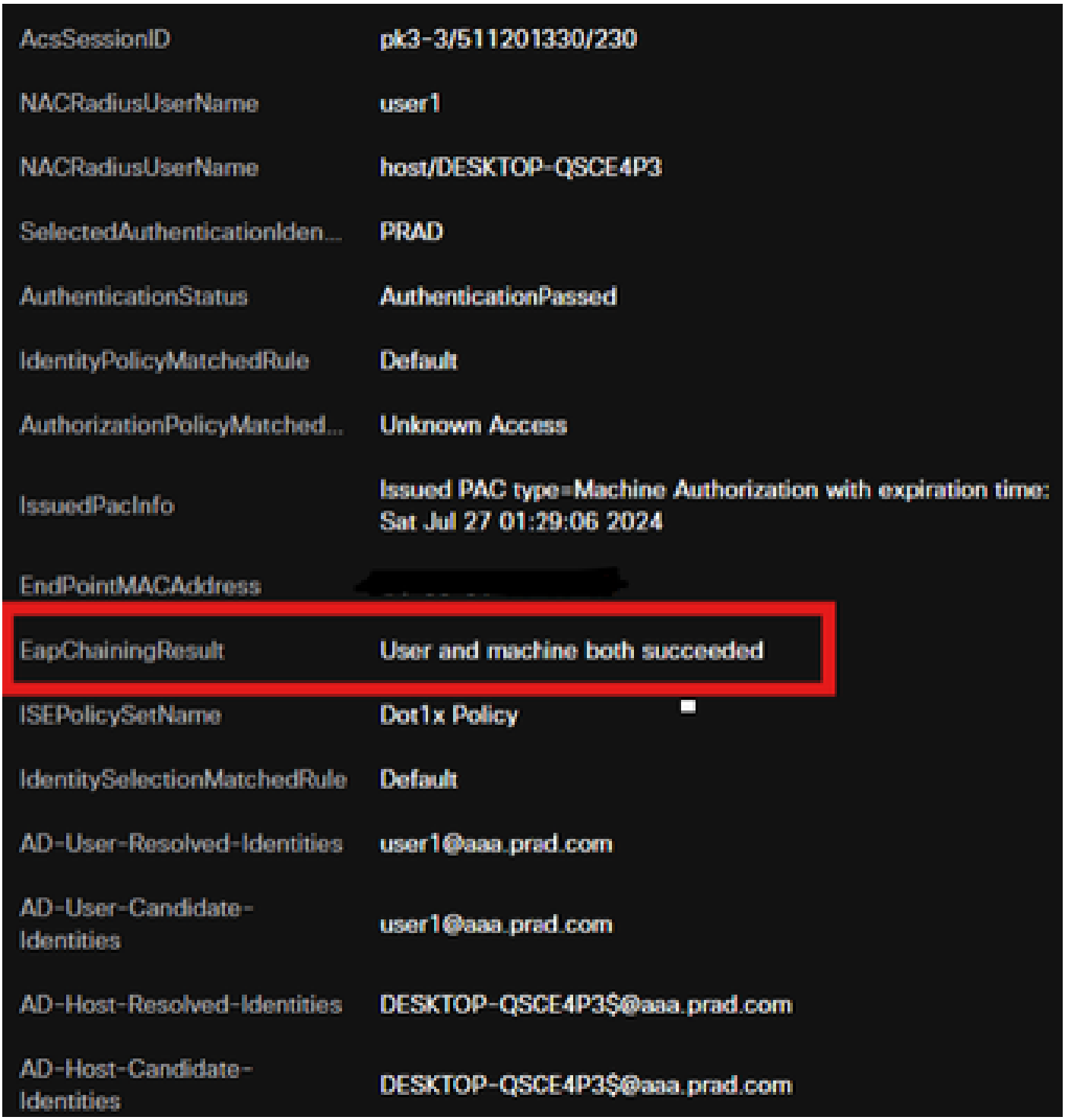
PCが再起動し、ユーザがログインすると、NAMはEAP-FASTを使用してユーザとマシンの両方を認証します。

エンドポイントが正しく認証されると、NAMは接続されていることを表示し、ポスチャモジュールがポスチャスキャンをトリガーします。



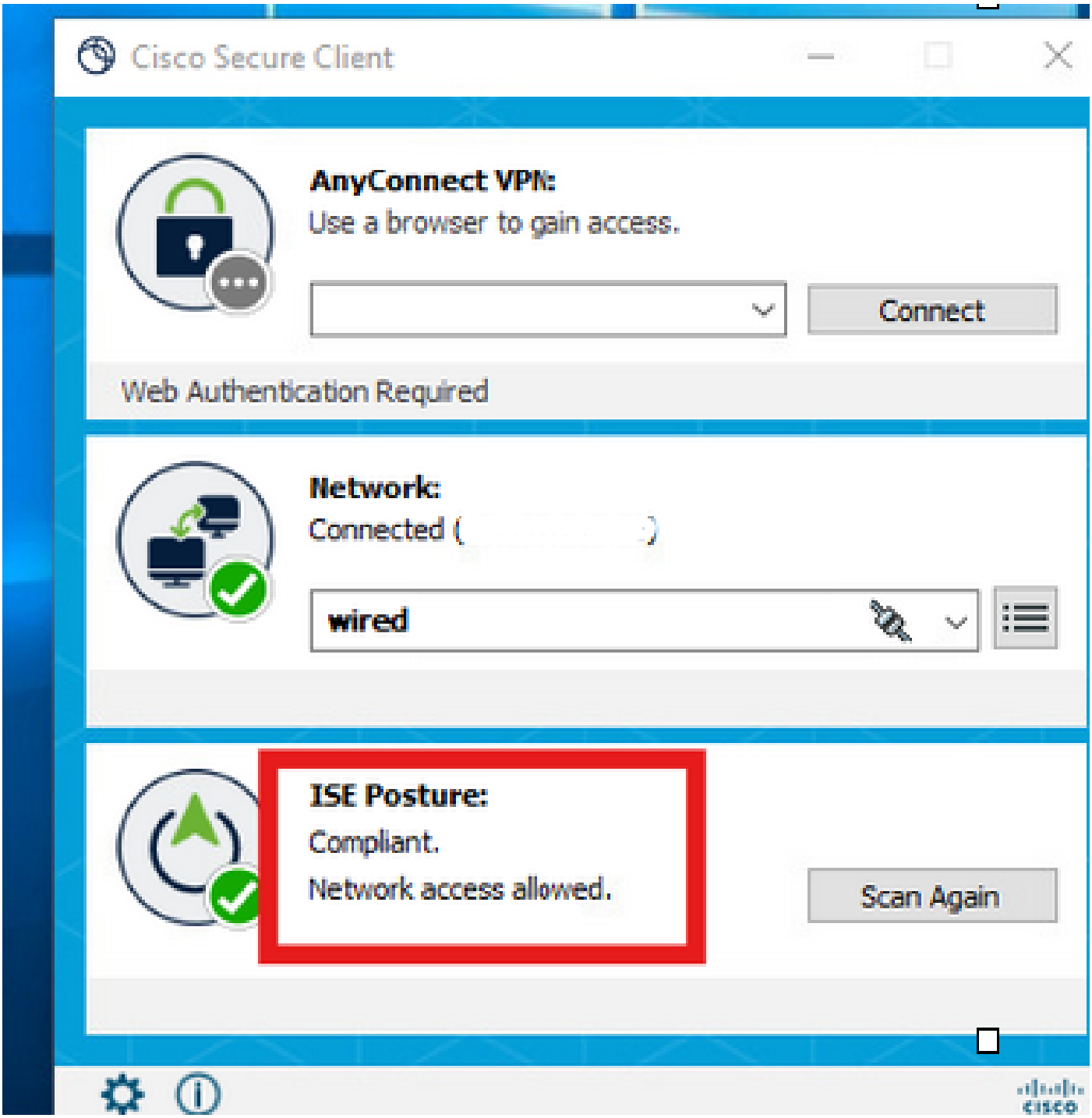
ISEライブログで、エンドポイントが不明なアクセスルールに該当するようになりました。

これで、認証プロトコルはNAMプロファイル設定に基づいてEAP-FASTになり、EAPチェーンの結果は「Success」になります。

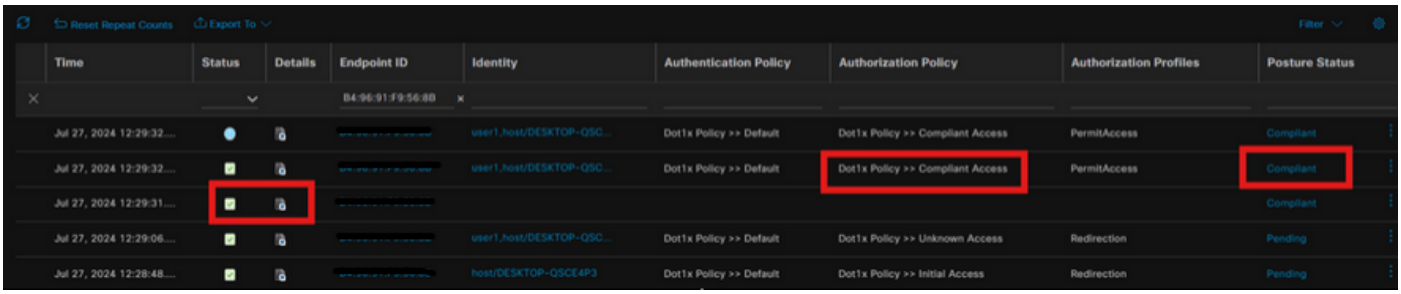


ステップ 3：ポスチャスキャン

セキュアクライアントポスチャモジュールは、ポスチャスキャンをトリガーし、ISEポスチャポリシーに基づいて準拠としてマークされます。



CoAはポスチャスキャンの後でトリガーされ、エンドポイントが準拠アクセスポリシーに一致します。

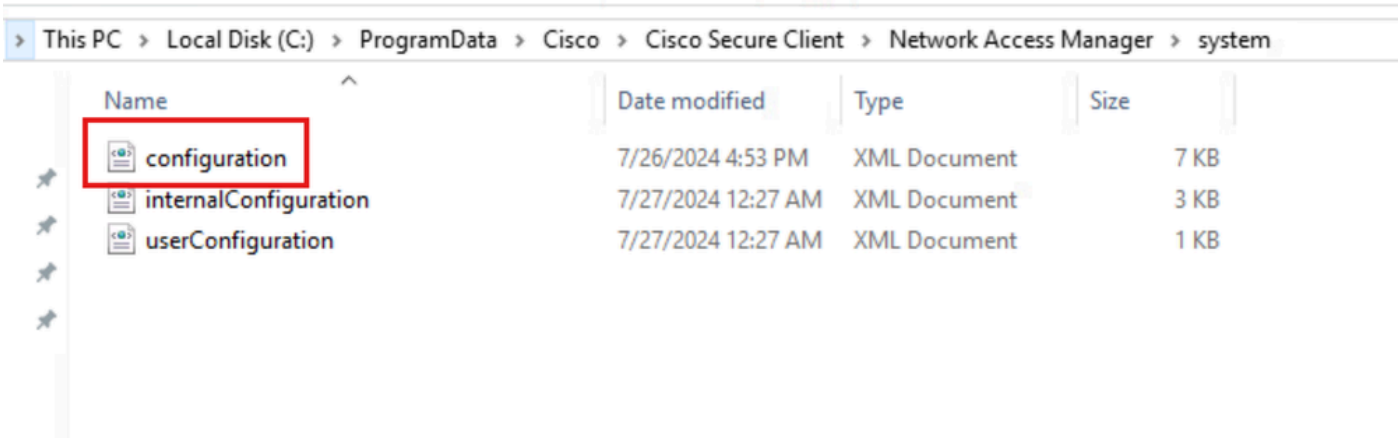


トラブルシュート

ステップ 1：NAMプロファイル

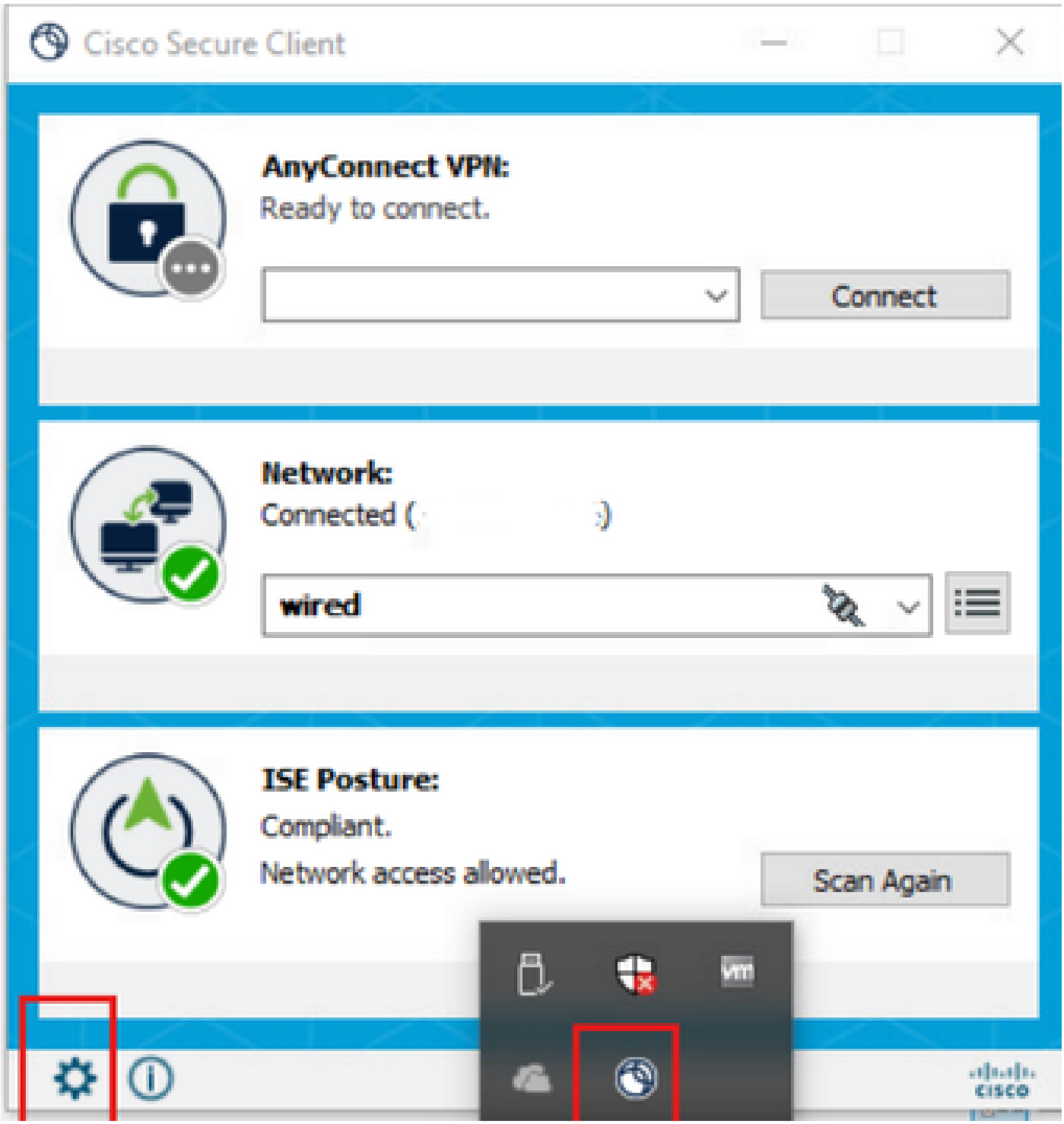
NAMモジュールのインストール後、PC上のこのパスにNAMプロファイルconfiguration.xmlが存在することを確認します。

C:\ProgramData\Cisco\Ciscoセキュアクライアント\Network Access Manager\system



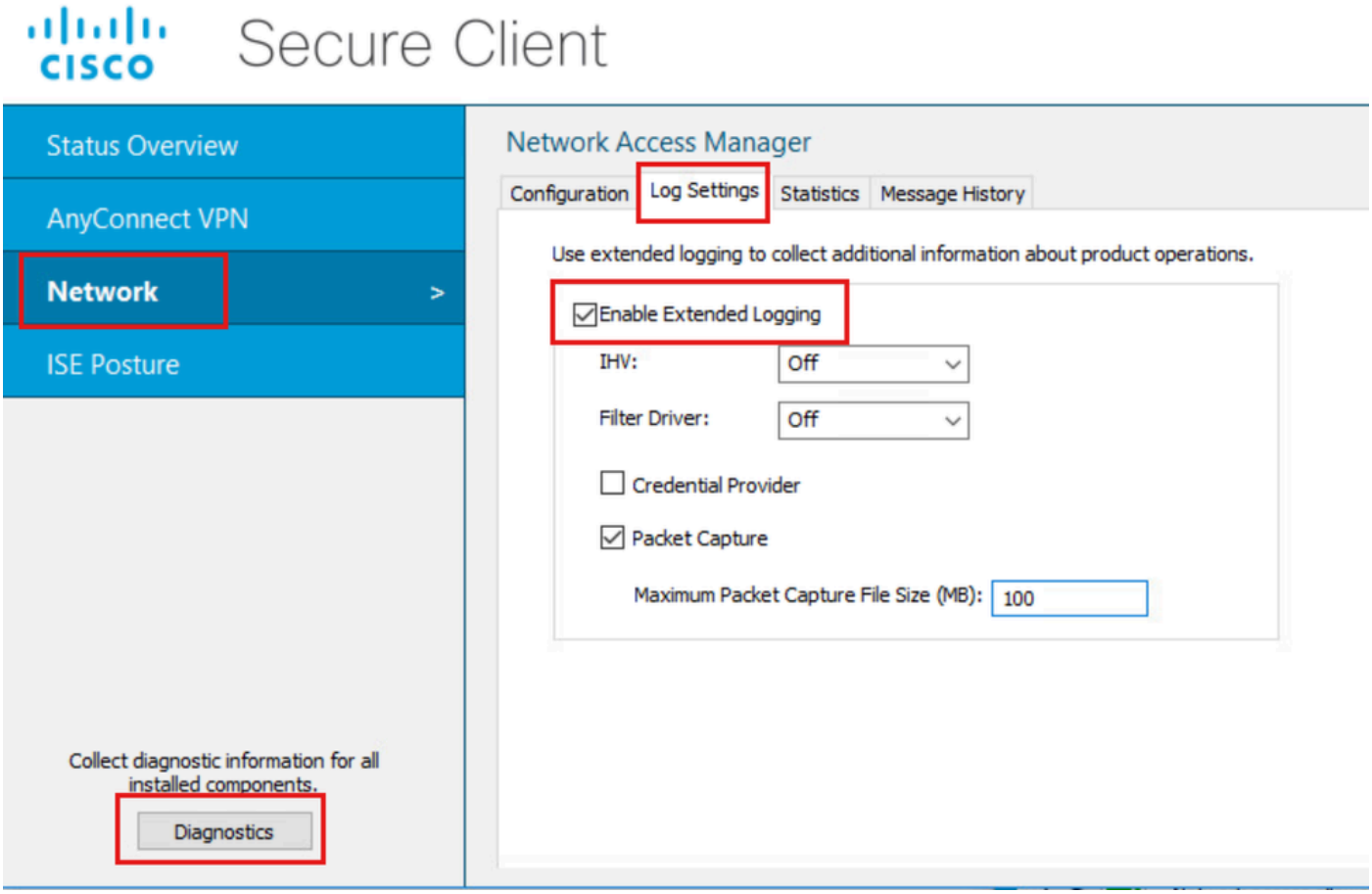
ステップ 2：NAM拡張ロギング

タスクバーからセキュアクライアントアイコンをクリックし、「設定」アイコンを選択します。



Network > Log Settingsタブに移動します。Enable Extended Loggingチェックボックスにチェックマークを入れます。
パケットキャプチャファイルサイズを100 MBに設定します。

問題を再現したら、Diagnosticsをクリックして、エンドポイントにDARTバンドルを作成します。



メッセージ履歴セクションには、NAMが実行したすべてのステップの詳細が表示されます。

ステップ 3： スイッチのデバッグ

dot1xとリダイレクトフローのトラブルシューティングを行うには、スイッチで次のデバッグを有効にします。

debug ip http all（IOSのみ）

debug ip http transactions（httpトランザクションのデバッグ）

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デバッグ

set platform software trace smd switch active R0 epm-redirectデバッグ

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

set platform software trace smd switch active R0 webauth-httpd debug

ログを表示するには

show logging

show logging process smd internal

ステップ 4：ISE でのデバッグ

次の属性を持つISEサポートバンドルを収集し、デバッグレベルに設定します。

- ポスチャ
- ポータル
- プロビジョニング
- ランタイムAAA
- nsf
- nsf-session
- swiss
- クライアントWebアプリ

関連情報

セキュアなクライアントNAMの設定

ISEポスチャ規範的な導入ガイド

Catalyst 9000シリーズスイッチのDot1xのトラブルシューティング

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。