

Configure o NAM do Secure Client para Dot1x usando o Windows e o ISE 3.2

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[1. Baixe e instale o Secure Client NAM \(Network Access Manager\)](#)

[2. Baixe e instale o Secure Client NAM Profile Editor.](#)

[3. Configurações Padrão Gerais](#)

[4. Cenário 1: Configurar Cliente Seguro NAM Requerente para Autenticação de Usuário PEAP \(MS-CHAPv2\)](#)

[5. Cenário 2: Configurar o Solicitante NAM de Cliente Seguro para Autenticação Simultânea de Usuário e Máquina EAP-FAST](#)

[6. Cenário 3: Configurar um Requerente de NAM de Cliente Seguro para Autenticação de Certificado de Usuário TLS EAP](#)

[7. Configurar ISR 1100 e ISE para Permitir Autenticações com Base no Cenário 1 PEAP MSCHAPv2](#)

[Verificar](#)

[Troubleshooting](#)

[Problema: o perfil NAM não é usado pelo Secure Client.](#)

[Problema 2: Os registros precisam ser coletados para análise posterior.](#)

[1. Habilitar log estendido do NAM](#)

[2. Reproduza o problema.](#)

[3. Colete o pacote Secure Client DART.](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar o NAM (Secure Client Network Analysis Module) no Windows.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Compreensão básica do que é um suplicante RADIUS
- Ponto1x
- PEAP
- PKI

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Windows 10 Pro Versão 22H2 Construído 19045.3930
- ISE 3.2
- Software Cisco C1117 Cisco IOS® XE, versão 17.12.02
- Active Directory 2016

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Este documento descreve como configurar o NAM do Secure Client no Windows. A opção de pré-implantação e o Editor de perfis para executar a autenticação dot1x são usados. Além disso, são fornecidos alguns exemplos de como isso é obtido.

Em redes, um suplicante é uma entidade em uma extremidade de um segmento de LAN ponto-a-ponto que busca ser autenticada por um autenticador conectado à outra extremidade desse link. O padrão IEEE 802.1X usa o termo suplicante para se referir a hardware ou software. Na prática, um requerente é um aplicativo de software instalado em um computador de usuário final. O usuário chama o solicitante e envia as credenciais para conectar o computador a uma rede segura. Se a autenticação for bem-sucedida, o autenticador geralmente permitirá que o computador se conecte à rede.

Sobre o gerenciador de acesso à rede

O Network Access Manager é um software cliente que fornece uma rede segura de Camada 2 de acordo com suas políticas. Ele detecta e seleciona a rede de acesso de Camada 2 ideal e executa a autenticação de dispositivo para acesso a redes com e sem fio. O gerenciador de acesso à rede gerencia a identidade do usuário e do dispositivo e os protocolos de acesso à rede necessários para acesso seguro. Ele funciona de forma inteligente para evitar que os usuários finais façam conexões que violem as políticas definidas pelo administrador.

O gerenciador de acesso à rede foi projetado para ser single-homed, permitindo apenas uma conexão de rede por vez. Além disso, as conexões com fio têm prioridade mais alta do que as conexões sem fio. Assim, se você estiver conectado à rede com uma conexão com fio, o adaptador sem fio será desativado sem nenhum endereço IP.

Configurar

Diagrama de Rede

É crucial entender que para autenticações dot1x são necessárias 3 partes; o suplicante que pode fazer dot1x, o autenticador também conhecido como NAS/NAD, que serve como um proxy encapsulando o tráfego dot1x dentro do RADIUS, e o Servidor de autenticação.

Neste exemplo, o suplicante é instalado e configurado de diferentes maneiras. Mais tarde, é mostrado um cenário com a configuração do dispositivo de rede e o servidor de autenticação.

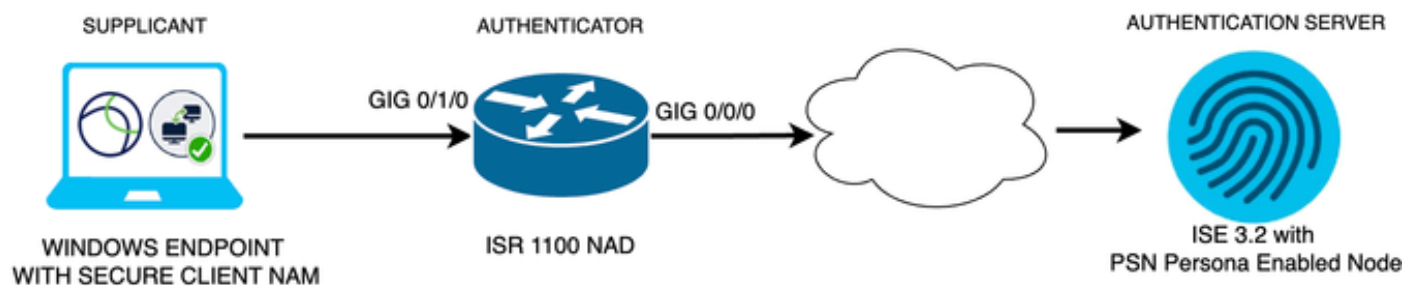


Diagrama de Rede

Configurações

1. Baixe e instale o Secure Client NAM (Network Access Manager).
2. Baixe e instale o editor de perfil NAM do Secure Client.
3. Configurações padrão gerais
4. Cenário 1: Configurar a autenticação de usuário do Secure Client NAM Supplicant for PEAP (MS-CHAPv2).
5. Cenário 2: configurar o Secure Client NAM Supplicant para EAP-FAST simultaneamente à medida que a autenticação de usuário e de máquina for configurada.
6. Cenário 3 Parte 1: Configurar o Secure Client NAM Supplicant para EAP-TLS.
7. Cenário 3 Parte 2: Configurar a demonstração do NAD e do ISE.

1. Baixe e instale o Secure Client NAM (Network Access Manager)

[Download de software da Cisco](#)

Na barra de pesquisa do nome do produto, digite Secure Client 5.



Downloads Home > Segurança > Clientes de segurança de VPN e endpoint > Cliente seguro (incluindo AnyConnect) > Cliente seguro 5 > Software AnyConnect VPN Client.

Neste exemplo de configuração, a versão 5.1.2.42 é a usada.

Há várias maneiras de implantar o Secure Client em dispositivos Windows; do SCCM, do mecanismo de serviço de identidade e do headend da VPN. No entanto, neste artigo, o método













de instalação usado é o método de pré-implantação.

Na página, pesquise o arquivo Pacote de implantação de headend do cliente seguro da Cisco (Windows).

| | | | |
|--|-------------|-----------|---|
| Cisco Secure Client Pre-Deployment Package (Windows) - includes individual MSI files | 06-Feb-2024 | 108.30 MB |   |
| cisco-secure-client-win-5.1.2.42-predeploy-k9.zip | | | |
| Advisories | | | |

Arquivo zip Msi

Após o download e a extração, clique em Setup.

| | |
|--|------------------|
| Profiles | 4/4/2024 7:16 PM |
| Setup | 4/4/2024 7:16 PM |
|  cisco-secure-client-win-1.182.3-thousandeyes-predeploy-k9 | 4/4/2024 7:16 PM |
|  cisco-secure-client-win-5.1.2.42-core-vpn-predeploy-k9 | 4/4/2024 7:16 PM |
|  cisco-secure-client-win-5.1.2.42-dart-predeploy-k9 | 4/4/2024 7:16 PM |
|  cisco-secure-client-win-5.1.2.42-iseposture-predeploy-k9 | 4/4/2024 7:16 PM |
|  cisco-secure-client-win-5.1.2.42-nam-predeploy-k9 | 4/4/2024 7:16 PM |
|  cisco-secure-client-win-5.1.2.42-nvm-predeploy-k9 | 4/4/2024 7:16 PM |
|  cisco-secure-client-win-5.1.2.42-posture-predeploy-k9 | 4/4/2024 7:16 PM |
|  cisco-secure-client-win-5.1.2.42-sbl-predeploy-k9 | 4/4/2024 7:16 PM |
|  cisco-secure-client-win-5.1.2.42-umbrella-predeploy-k9 | 4/4/2024 7:16 PM |
|  cisco-secure-client-win-5.1.2.5191-zta-predeploy-k9 | 4/4/2024 7:16 PM |
|  Setup | 4/4/2024 7:16 PM |
|  setup | 4/4/2024 7:16 PM |

Proteger arquivos do cliente

Instale os módulos Network Access Manager e Diagnostics and Reporting Tool.



Aviso: se você usar o Cisco Secure Client Wizard, o módulo VPN será instalado automaticamente e ficará oculto na GUI. O NAM não funcionará se o módulo VPN não estiver instalado. Se você usar arquivos MSI individuais ou um método de instalação diferente, certifique-se de instalar o módulo VPN.

Select the Cisco Secure Client 5.1.2.42 modules you wish to install:

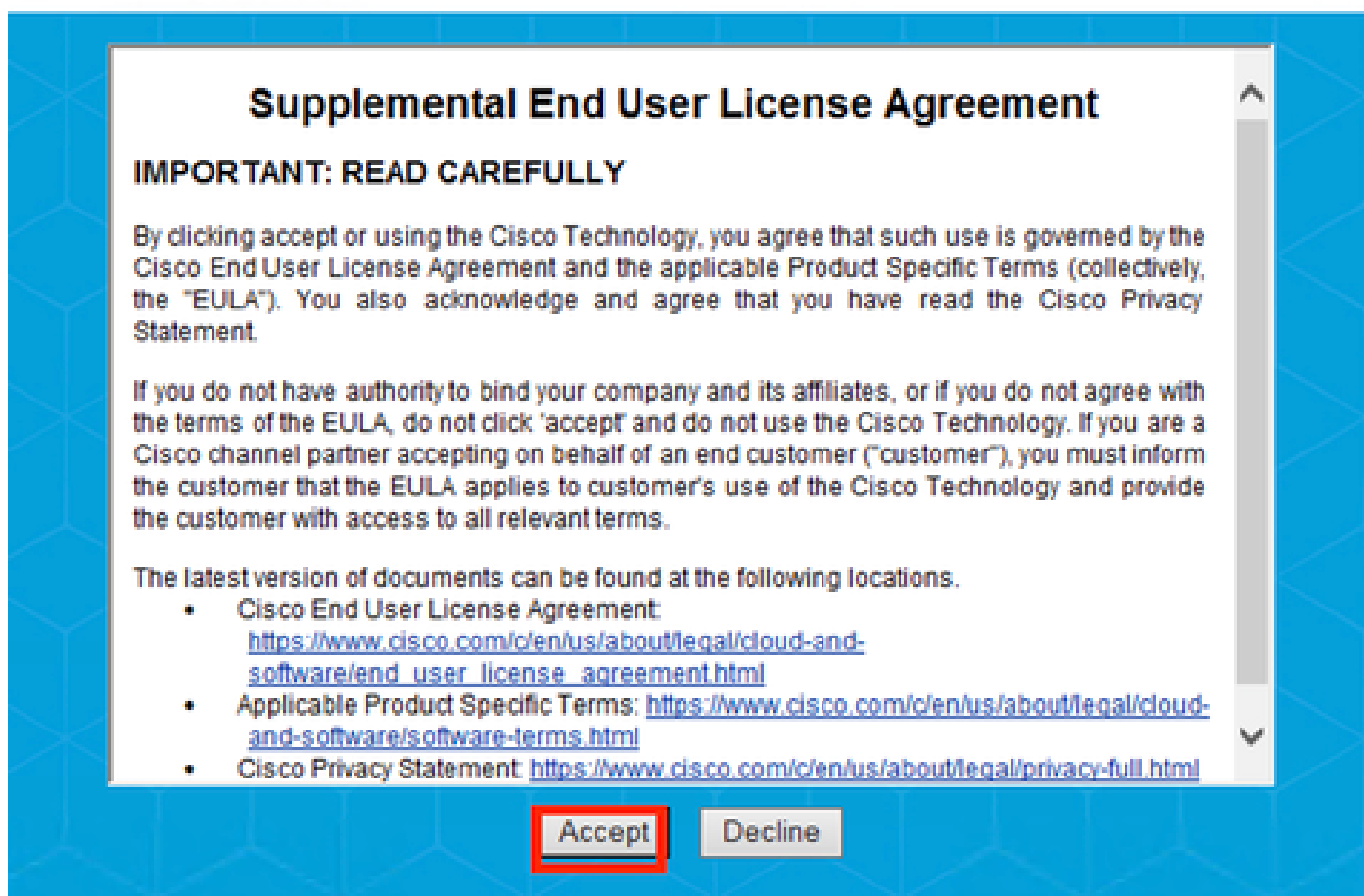
- Core & AnyConnect VPN
- Start Before Login
- Network Access Manager
- Secure Firewall Posture
- Network Visibility Module
- Umbrella
- ISE Posture
- ThousandEyes
- Zero Trust Access
- Select All
- Diagnostic And Reporting Tool
- Lock Down Component Services

Install Selected

Seletor de instalação

Clique em Instalar selecionado.

Aceite o EULA.



Janela do EULA

É necessário reiniciar após a instalação do NAM.

Cisco Secure Client Install Selector

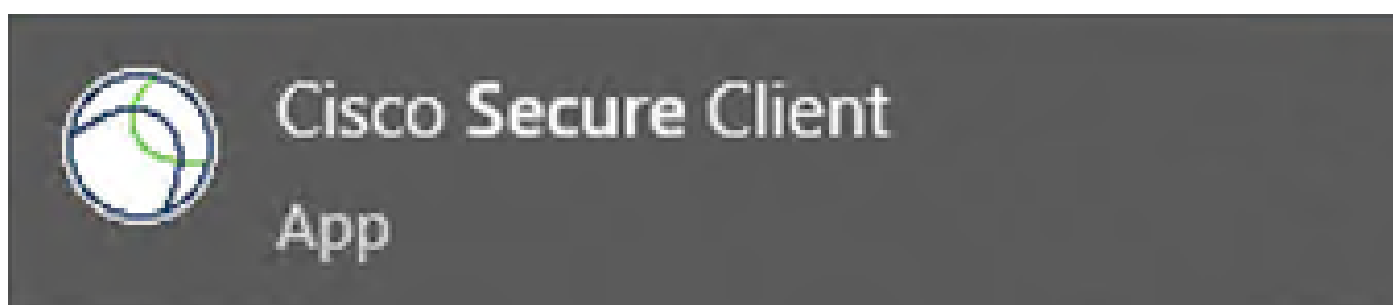


You must reboot your system for the installed changes to take effect.

OK

Janela de Requisitos de Reinicialização

Uma vez instalado, ele pode ser encontrado e aberto na barra do Windows Search.

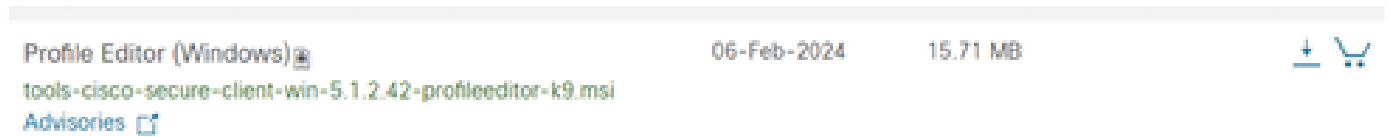


2. Baixe e instale o Secure Client NAM Profile Editor.

O Cisco Network Access Manager Profile Editor é necessário para configurar as preferências Dot1x.

Na mesma página em que o Secure Client é baixado, a opção Profile Editor é encontrada.

Este exemplo usa a opção com a versão 5.1.2.42.



Editor de perfis

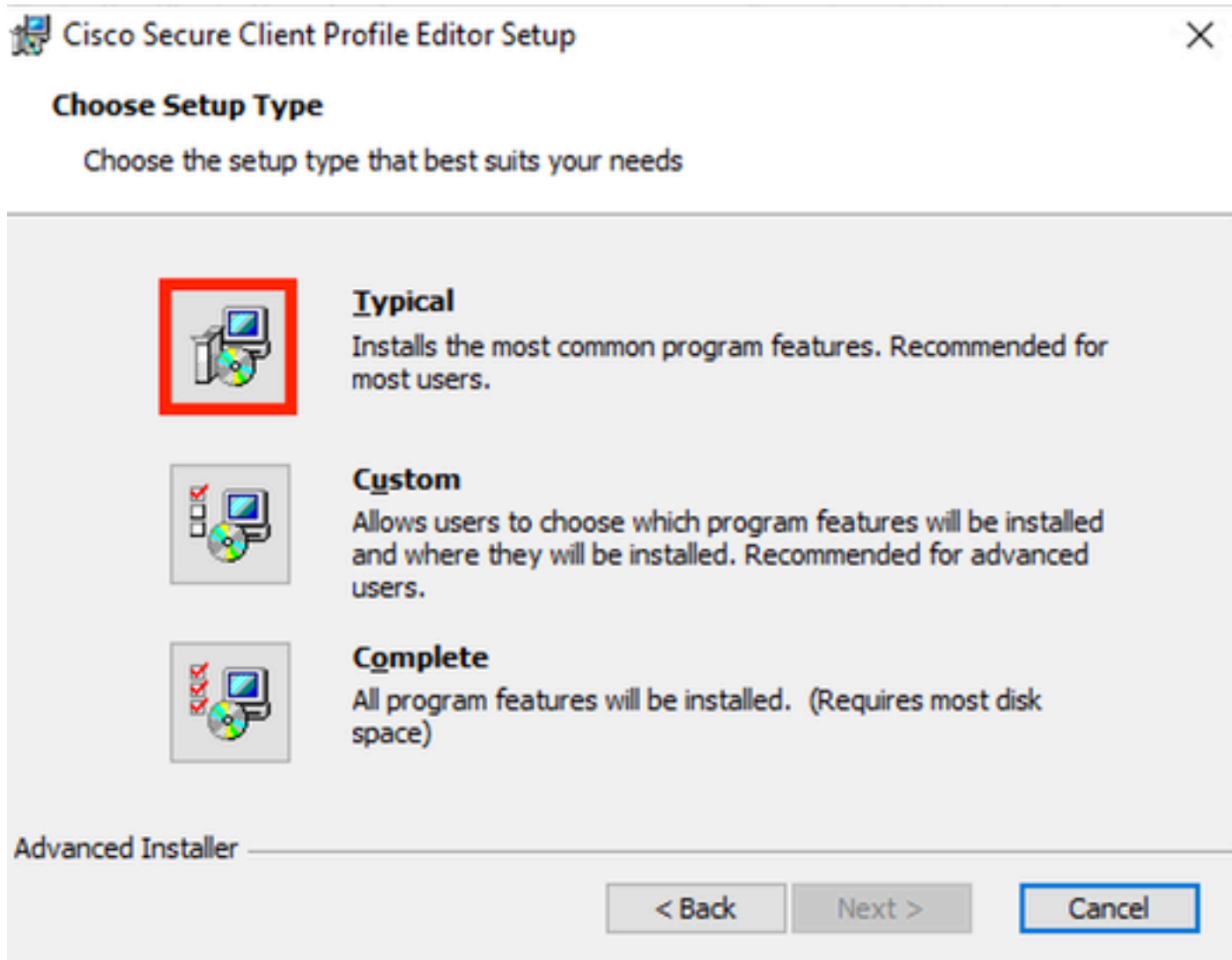
Após o download, continue com a instalação.

Execute o arquivo msi.

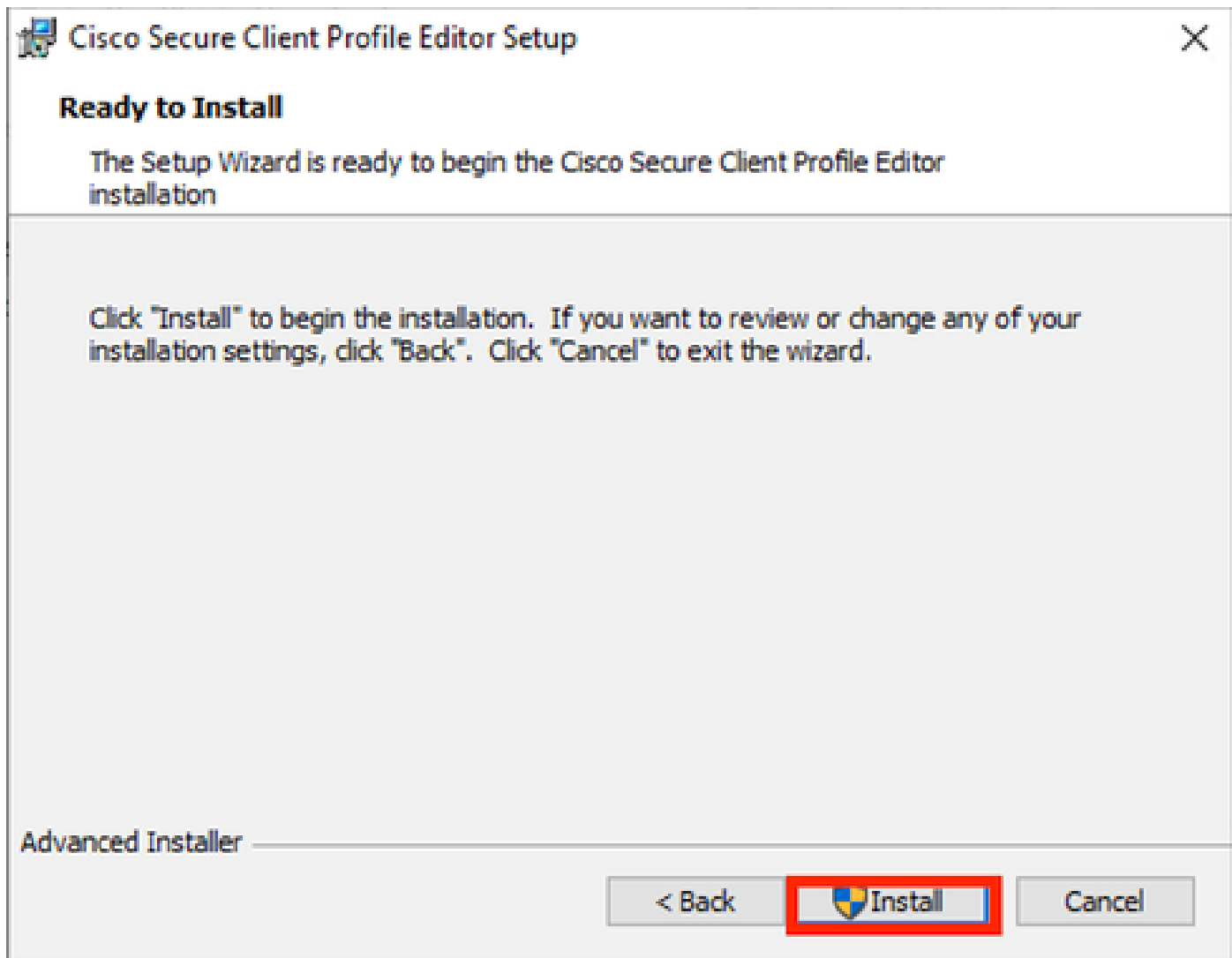


Janela Configuração do Editor de perfis

Use a opção de configuração Typical.



Configuração do Editor de perfis



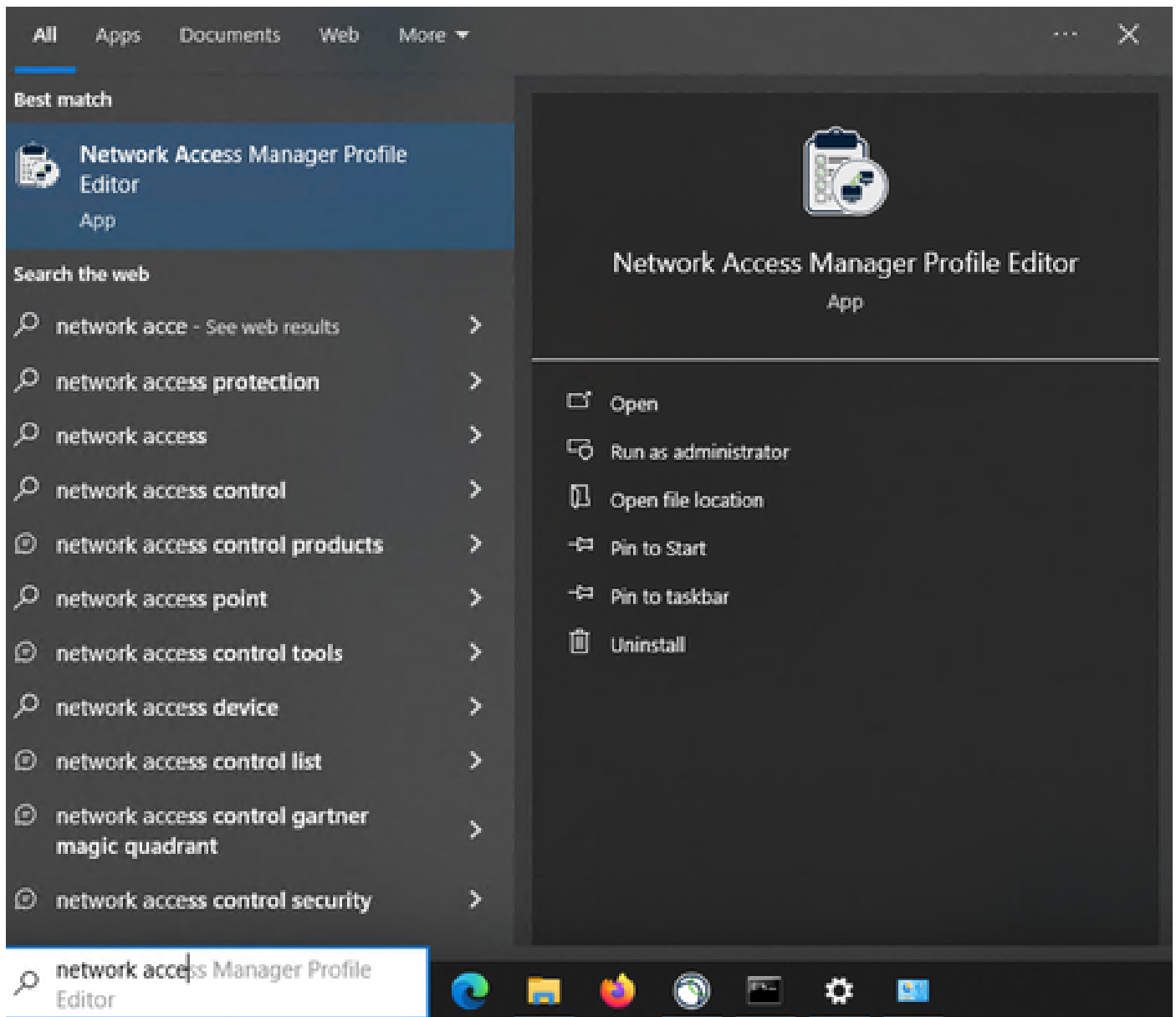
Janela de instalação

Clique em Finish.



Fim da Configuração do Editor de Perfis

Uma vez instalado, abra o Network Access Manager Profile Editor na barra de pesquisa.



Editor de perfis para NAM na barra de pesquisa

A instalação do Gerenciador de Acesso à Rede e do Editor de Perfis foi concluída.

3. Configurações Padrão Gerais

Todos os cenários apresentados neste artigo contêm configurações para:

- Política do cliente
- Política de autenticação
- Grupos de rede

Network Access Manager

- Client Policy
- Authentication Policy
- Networks
- Network Groups

Client Policy

Profile: Untitled

Connection Settings

Default Connection Timeout (sec.)

Connection Attempt:

Before user logon

Time to wait before allowing user to logon (sec.)

After user logon

Media

Manage Wi-Fi (wireless) Media

- Enable validation of WPA/WPA2/WPA3 handshake
- Enable Randomized MAC Address

Default Association Timeout (sec.)

Manage Wired (802.3) Media

Manage Mobile Broadband (3G) Media

- Enable Data Roaming

End-user Control

Allow end-user to:

- Disable Client
- Display user groups
- Specify a script or application to run when connected
- Auto-connect

Select machine connection type

Enable by default

Administrative Status

Service Operation: Enable Disable

FIPS Mode: Enable Disable

Captive Portal Detection: Enable Disable

Política do Cliente do Editor de Perfis do NAM

- Network Access Manager
 - Client Policy
 - Authentication Policy**
 - Networks
 - Network Groups

Authentication Policy

Profile: Untitled

Allow Association Modes

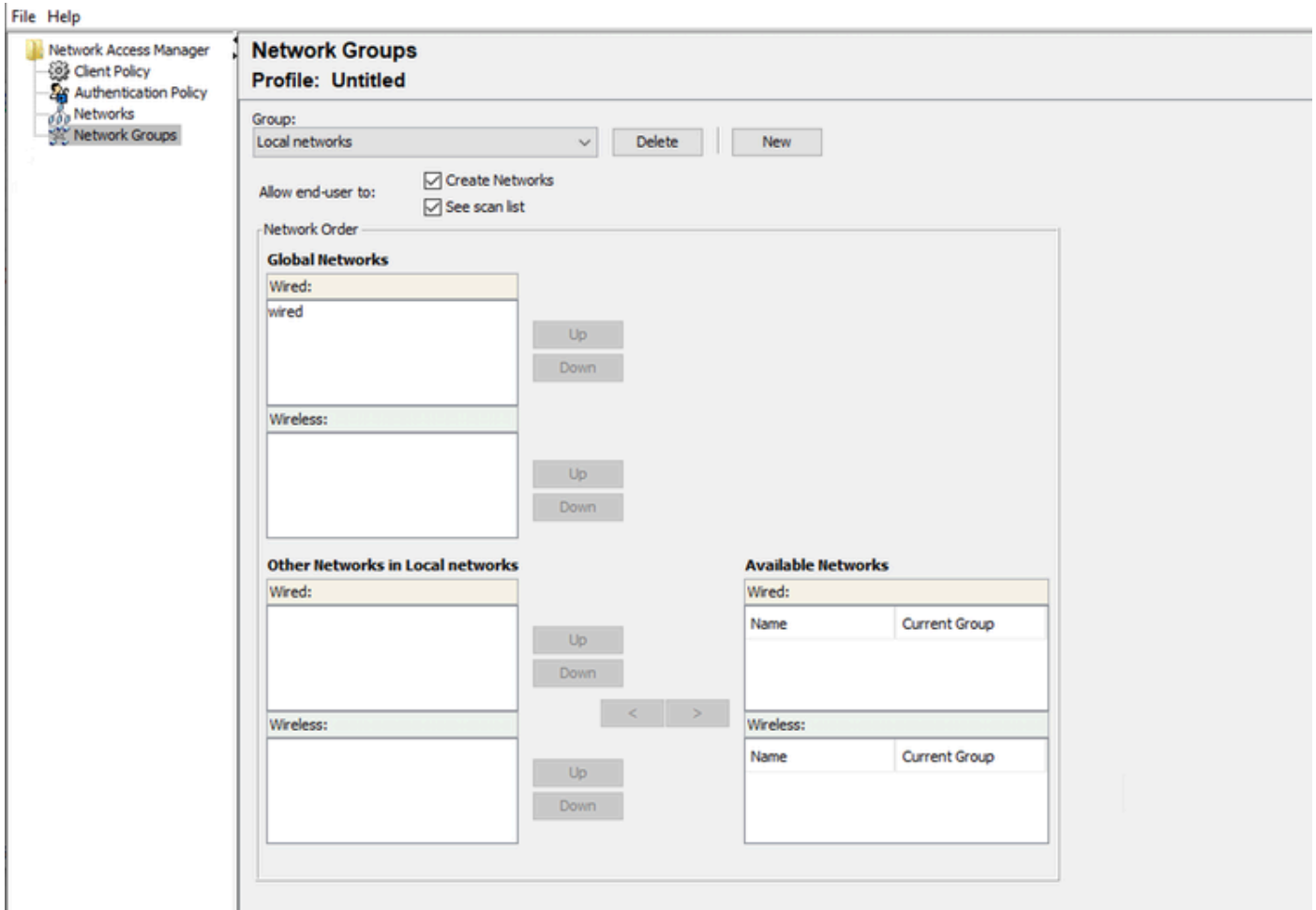
- Select All (Personal)
 - Open (no encryption)
 - Open (Static WEP)
 - Shared (WEP)
 - WPA Personal TKIP
 - WPA Personal AES
 - WPA2 Personal TKIP
 - WPA2 Personal AES
 - WPA3 Open (OWE)
 - WPA3 Personal AES (SAE)
- Select All (Enterprise)
 - Open (Dynamic (802.1X) WEP)
 - WPA Enterprise TKIP
 - WPA Enterprise AES
 - WPA2 Enterprise TKIP
 - WPA2 Enterprise AES
 - CKM Enterprise TKIP
 - CKM Enterprise AES
 - WPA3 Enterprise AES

Allowed Authentication Modes

- Select All Outer
 - EAP-FAST
 - EAP-GTC
 - EAP-MSCHAPv2
 - EAP-TLS
 - EAP-TLS
 - EAP-TTLS
 - EAP-MD5
 - EAP-MSCHAPv2
 - PAP (legacy)
 - CHAP (legacy)
 - MSCHAP (legacy)
 - MSCHAPv2 (legacy)
 - LEAP
 - PEAP
 - EAP-GTC
 - EAP-MSCHAPv2
 - EAP-TLS

Allowed Wired Security

- Select All
 - Open (no encryption)
 - 802.1x only
 - 802.1x with MacSec
 - AES-GCM-128
 - AES-GCM-256



Guia Grupos de rede

4. Cenário 1: Configurar Cliente Seguro NAM Requerente para Autenticação de Usuário PEAP (MS-CHAPv2)

Navegue até a seção Redes.

O perfil de rede padrão pode ser excluído.

Clique em Add.

Networks

Profile: Untitled

Network

| Name | Media Type | Group* |
|------|------------|--------|
|------|------------|--------|

Add...

Edit...

Delete

* A network in group 'Global' is a member of *all* groups.

Criação de perfil de rede

Nomeie o perfil Network.

Selecione Global para Associação de grupo. Selecione Wired Network media.

Networks

Profile: Untitled

| | | |
|---------------------------------------|--|----------------|
| Name: | <input type="text" value="PEAP MSCHAPv2"/> | Media Type |
| Group Membership | <input type="radio"/> In group: <input type="text" value="Local networks"/> | Security Level |
| | <input checked="" type="radio"/> In all groups (Global) | |
| Choose Your Network Media | <input checked="" type="radio"/> Wired (802.3) Network Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable. | |
| | <input type="radio"/> Wi-Fi (wireless) Network Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point. | |
| | SSID (max 32 chars): <input type="text"/> | |
| | <input type="checkbox"/> Hidden Network | |
| | <input type="checkbox"/> Corporate Network | |
| Association Timeout | <input type="text" value="5"/> seconds | |
| Common Settings | Script or application on each user's machine to run when connected. <input type="text"/> | |
| | <input type="button" value="Browse Local Machine"/> | |
| Connection Timeout | <input type="text" value="40"/> seconds | |
| <input type="button" value="Next"/> | | |
| <input type="button" value="Cancel"/> | | |

Seção Tipo de Mídia de Perfil de Rede

Clique em Next.

Selecione Authenticating Network e use o padrão para o restante das opções na seção Security Level.

Networks
Profile: Untitled

Security Level

Open Network
Open networks have no security, and are open to anybody within range. This is the least secure type of network.

Authenticating Network
Authenticating networks provide the highest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure.

Media Type
Security Level
Connection Type

802.1X Settings

| | | | |
|-------------------|----|--------------------|---|
| authPeriod (sec.) | 30 | startPeriod (sec.) | 3 |
| heldPeriod (sec.) | 60 | maxStart | 2 |

Security

Key Management
None

Encryption

AES GCM 128
 AES GCM 256

Port Authentication Exception Policy

Enable port exceptions

Allow data traffic before authentication

Allow data traffic after authentication even if

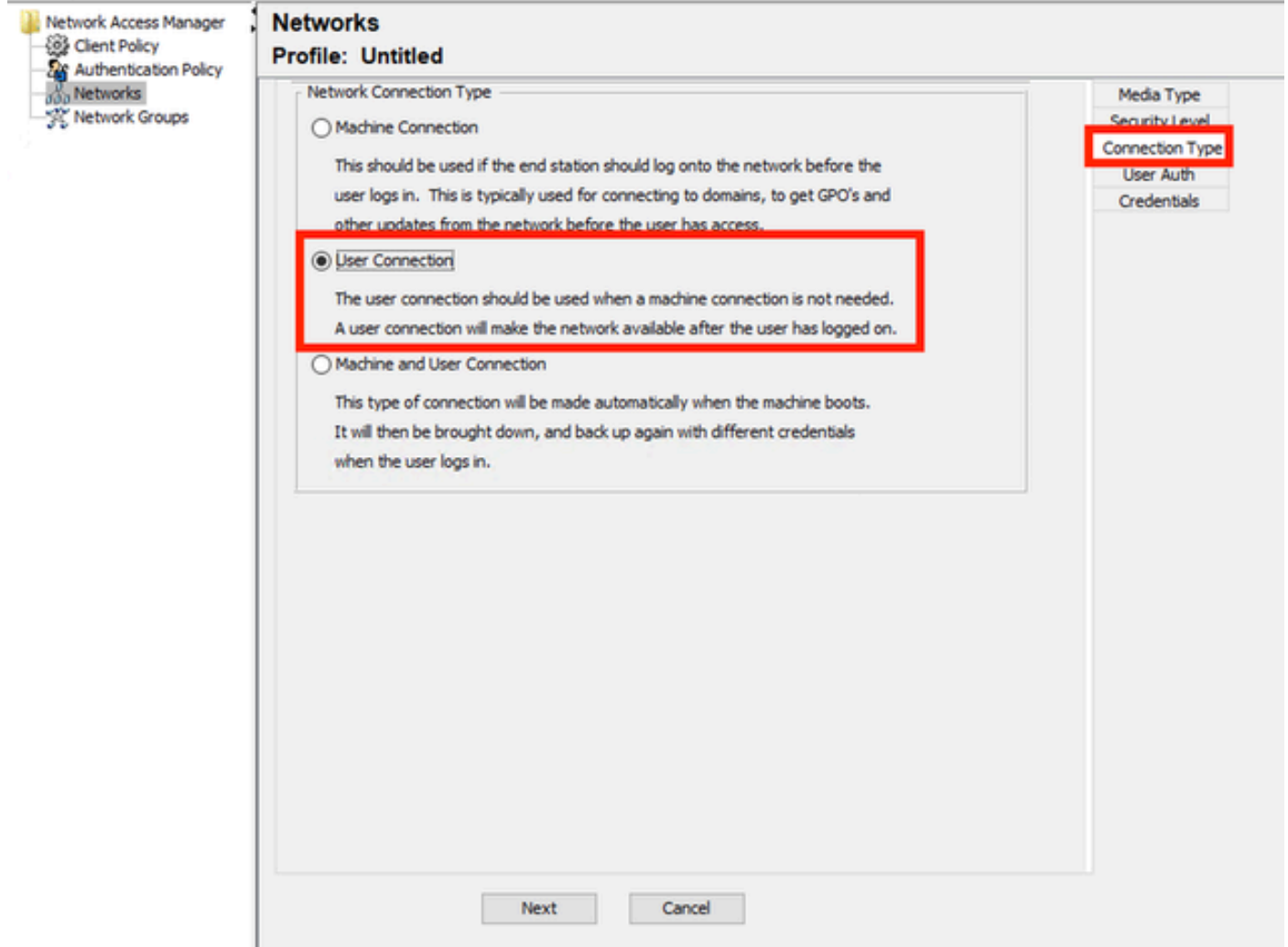
EAP fails

EAP succeeds but key management fails

Next Cancel

Nível de Segurança do Perfil de Rede

Clique em Avançar para continuar com a seção Tipo de conexão.



Tipo de Conexão de Perfil de Rede

Selecione o tipo de conexão User Connection.

Clique em Next para continuar com a seção User Auth que está disponível agora.

Selecione PEAP como o Método EAP geral.

Networks
Profile: Untitled

EAP Methods

EAP-MD5 EAP-TLS
 EAP-MSCHAPv2 EAP-TTLS
 EAP-GTC PEAP EAP-FAST

Extend user connection beyond log off

EAP-PEAP Settings

Validate Server Identity
 Enable Fast Reconnect
 Disable when using a Smart Card

Inner Methods based on Credentials Source

Authenticate using a Password
 EAP-MSCHAPv2
 EAP-GTC
 EAP-TLS, using a Certificate
 Authenticate using a Token and EAP-GTC

Media Type
Security Level
Connection Type
User Auth
Certificates
Credentials

Next Cancel

Autenticação de Usuário do Perfil de Rede

Não altere os valores padrão nas Configurações EAP-PEAP.

Continue com a seção Métodos internos baseados na fonte de credenciais.

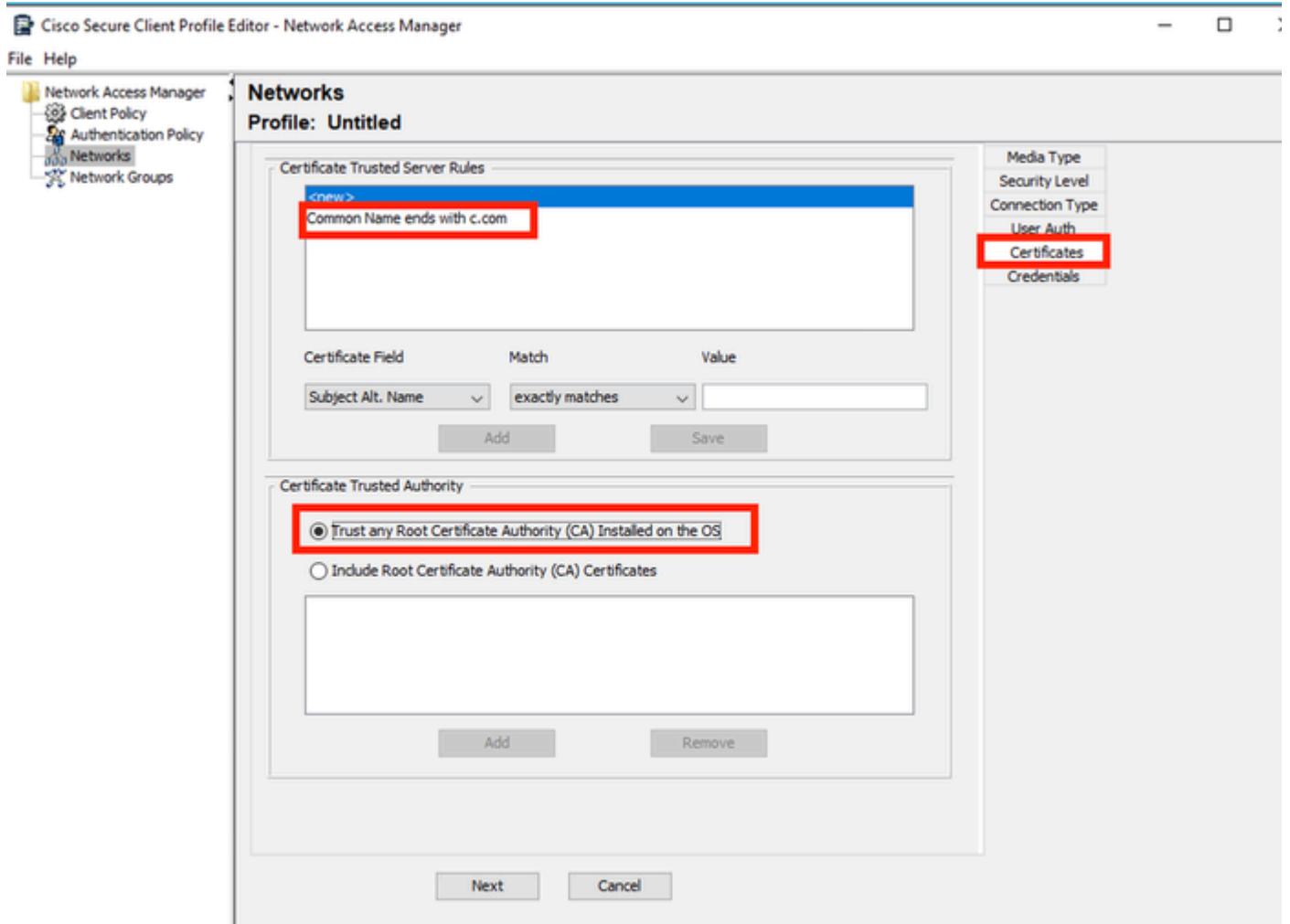
A partir dos vários métodos internos existentes para EAP PEAP, selecione Authenticate using a Password e selecione EAP-MSCHAPv2.

Clique em Avançar para continuar na seção Certificado.



Observação: a seção Certificado é exibida porque a opção Validar identidade do servidor em Configurações EAP-PEAP está selecionada. Para EAP PEAP, ele faz o encapsulamento usando o certificado do servidor.

Na seção Certificados, em Regras do servidor confiável de certificados, a regra Nome comum termina com c.com é usada. Esta seção da configuração se refere ao certificado que o servidor usa durante o fluxo PEAP EAP. Se o Identity Service Engine (ISE) for usado em seu ambiente, você poderá usar o nome comum do Certificado EAP do Nó do Servidor de Políticas.

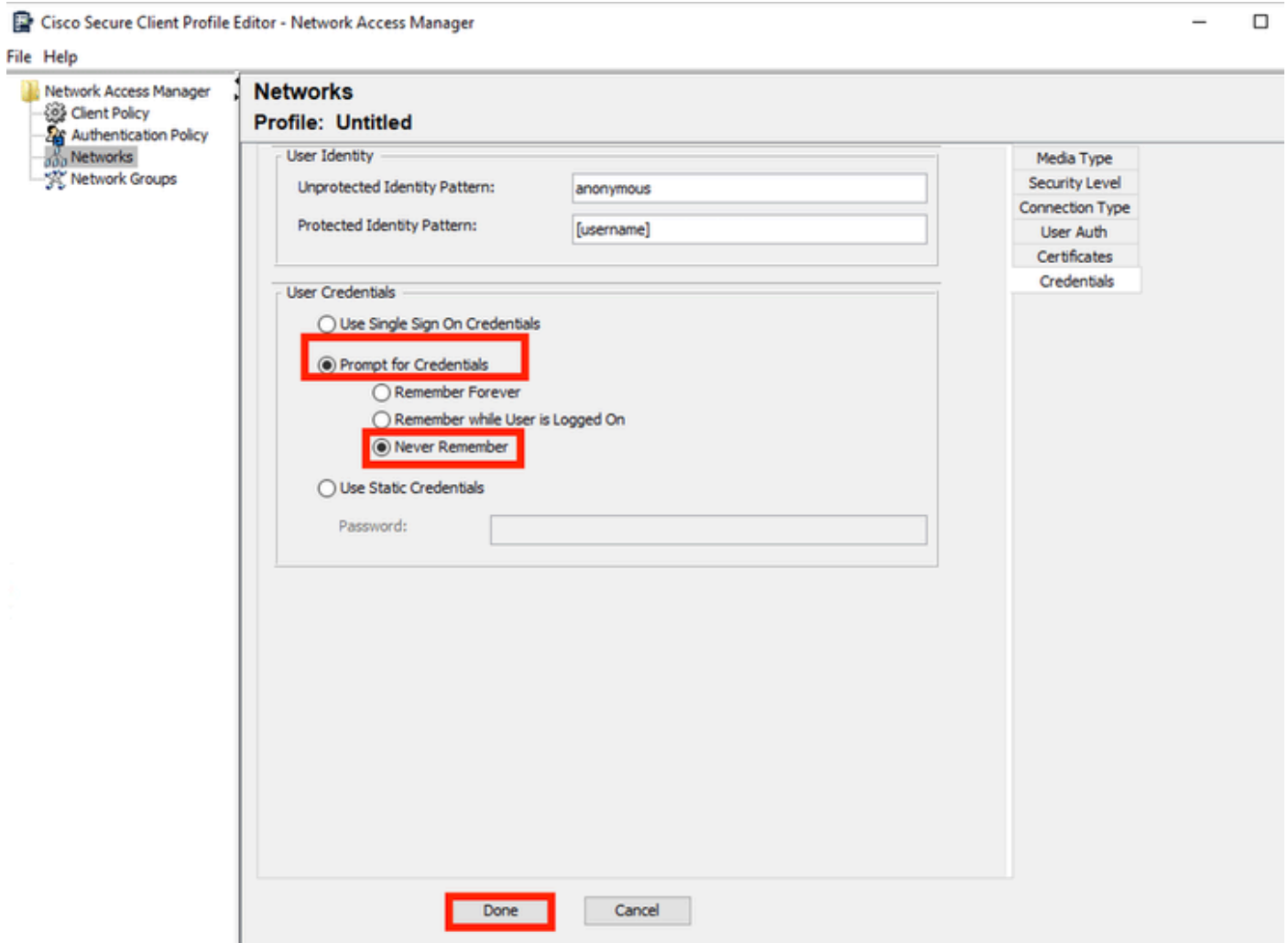


Seção Certificado de Perfil de Rede

Duas opções podem ser selecionadas em Autoridade de Certificação Confiável. Para esse cenário, em vez de adicionar um Certificado de CA específico que assinou o certificado RADIUS EAP, a opção Trust any Root Certificate Authority (CA) Installed on the OS é usada.

Com esta opção, o dispositivo Windows confia em qualquer certificado EAP assinado por um certificado incluído no programa Gerenciar certificados de usuário Certificados — Usuário atual > Autoridades de certificação raiz confiáveis > Certificados.

Clique em Next.



Seção Credenciais de Perfil de Rede

Na seção Credenciais, apenas a seção Credenciais do usuário é alterada.

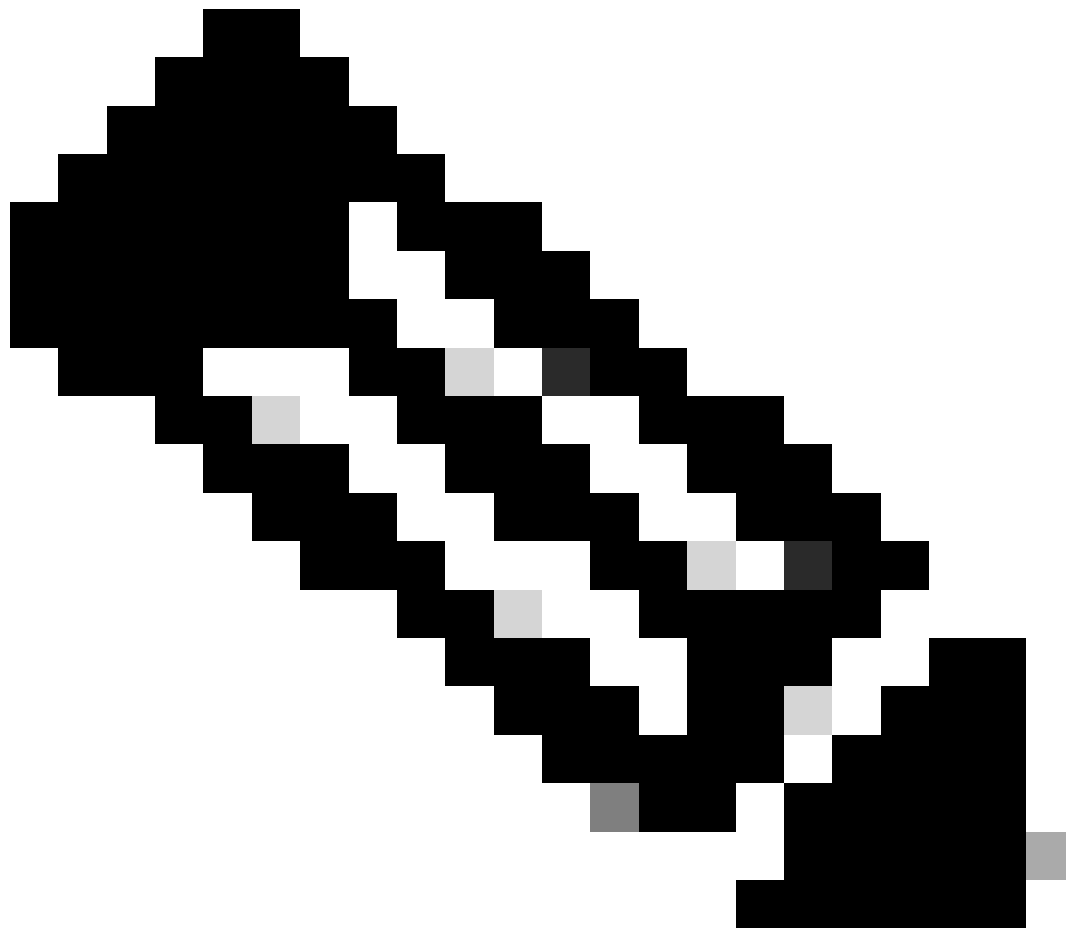
A opção Prompt for Credentials > Never Remember está selecionada, portanto, em cada autenticação, o usuário que faz a autenticação deve inserir suas credenciais.

Clique em Concluído.

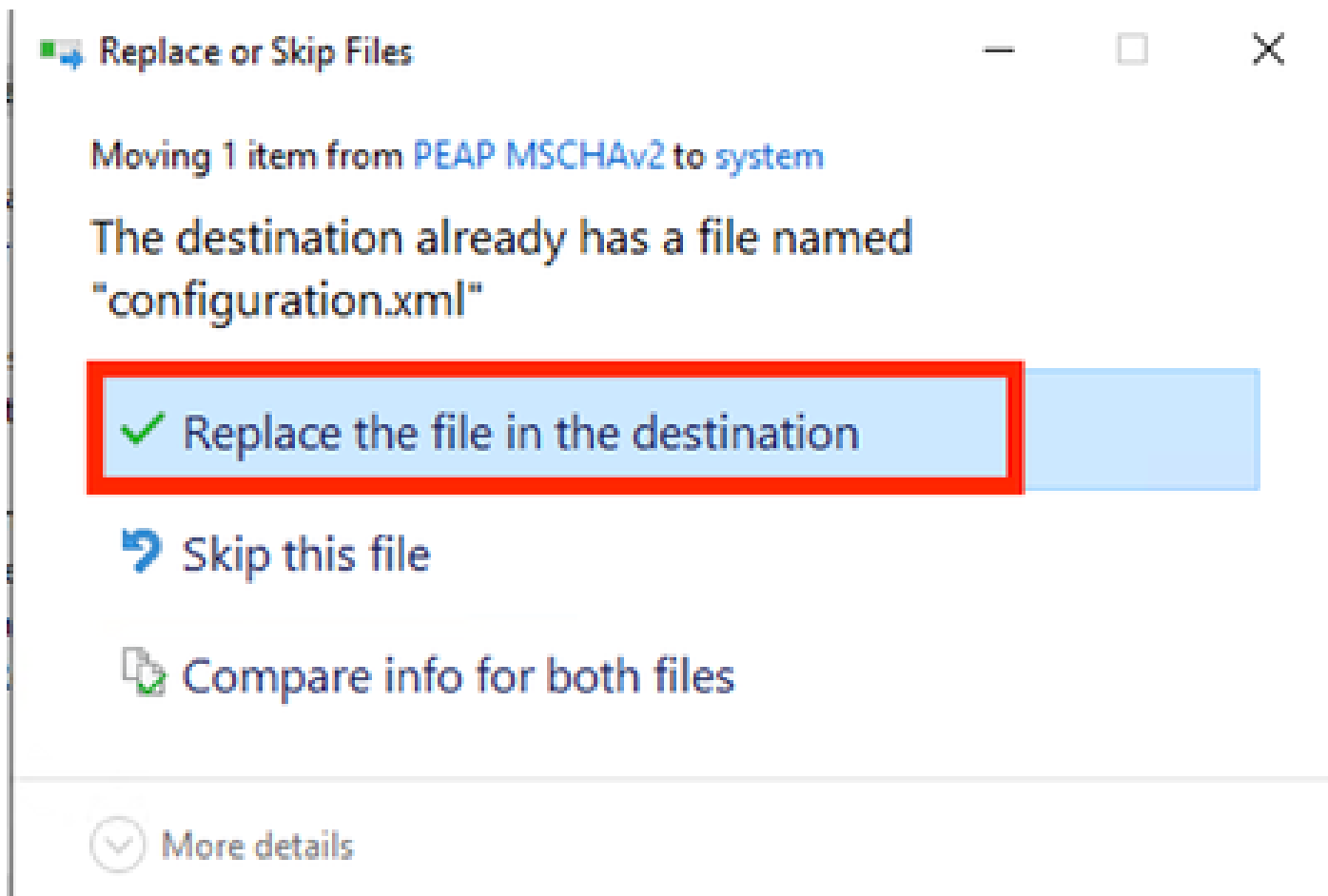
Salve o perfil Secure Client Network Access Manager, como configuration.xml com a opção File > Save As.

Para fazer com que o Secure Client Network Access Manager use o perfil que acabou de ser criado, substitua o arquivo configuration.xml no próximo diretório pelo novo:

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



Observação: o arquivo deve ser nomeado como configuration.xml, caso contrário ele não funcionará.



Substituir Seção de Arquivo

5. Cenário 2: Configurar o Solicitante NAM de Cliente Seguro para Autenticação Simultânea de Usuário e Máquina EAP-FAST

Abra o NAM Profile Editor e navegue para a seção Redes.

Clique em Add.

Networks

Profile: Untitled

Network

| Name | Media Type | Group* |
|------|------------|--------|
|------|------------|--------|

Add...

Edit...

Delete

* A network in group 'Global' is a member of *all* groups.

Guia Rede do Editor de perfis do NAM

Digite um nome no perfil de rede.

Selecione Global para Associação de grupo. Selecione WiredNetwork Media.

File Help

Networks
Profile: Untitled

Name: **EAP-FAST**

Group Membership

In group: Local networks

In all groups (Global)

Choose Your Network Media

Wired (802.3) Network
Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable.

Wi-Fi (wireless) Network
Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point.

SSID (max 32 chars):

Hidden Network
 Corporate Network

Association Timeout: seconds

Common Settings

Script or application on each user's machine to run when connected.

Connection Timeout: seconds

Media Type
Security Level

Seção Tipo de Mídia

Clique em Next.

Selecione Authenticating Network e não altere os valores padrão para o restante das opções nesta seção.

File Help

Networks
Profile: Untitled

Security Level

Open Network
Open networks have no security, and are open to anybody within range. This is the least secure type of network.

Authenticating Network
Authenticating networks provide the highest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure.

802.1X Settings

| | | | |
|-------------------|---------------------------------|--------------------|--------------------------------|
| authPeriod (sec.) | <input type="text" value="30"/> | startPeriod (sec.) | <input type="text" value="3"/> |
| heldPeriod (sec.) | <input type="text" value="60"/> | maxStart | <input type="text" value="2"/> |

Port Authentication Exception Policy

Enable port exceptions

Allow data traffic before authentication

Allow data traffic after authentication even if

EAP fails

EAP succeeds but key management fails

Security

Key Management
None

Encryption

AES GCM 128

AES GCM 256

Media Type
Security Level
Connection Type

Next Cancel

Seção Editor de perfil de nível de segurança

Clique em Avançar para continuar com a seção Tipo de conexão.

File Help

Networks
Profile: Untitled

Network Connection Type

Machine Connection

This should be used if the end station should log onto the network before the user logs in. This is typically used for connecting to domains, to get GPO's and other updates from the network before the user has access.

User Connection

The user connection should be used when a machine connection is not needed. A user connection will make the network available after the user has logged on.

Machine and User Connection

This type of connection will be made automatically when the machine boots. It will then be brought down, and back up again with different credentials when the user logs in.

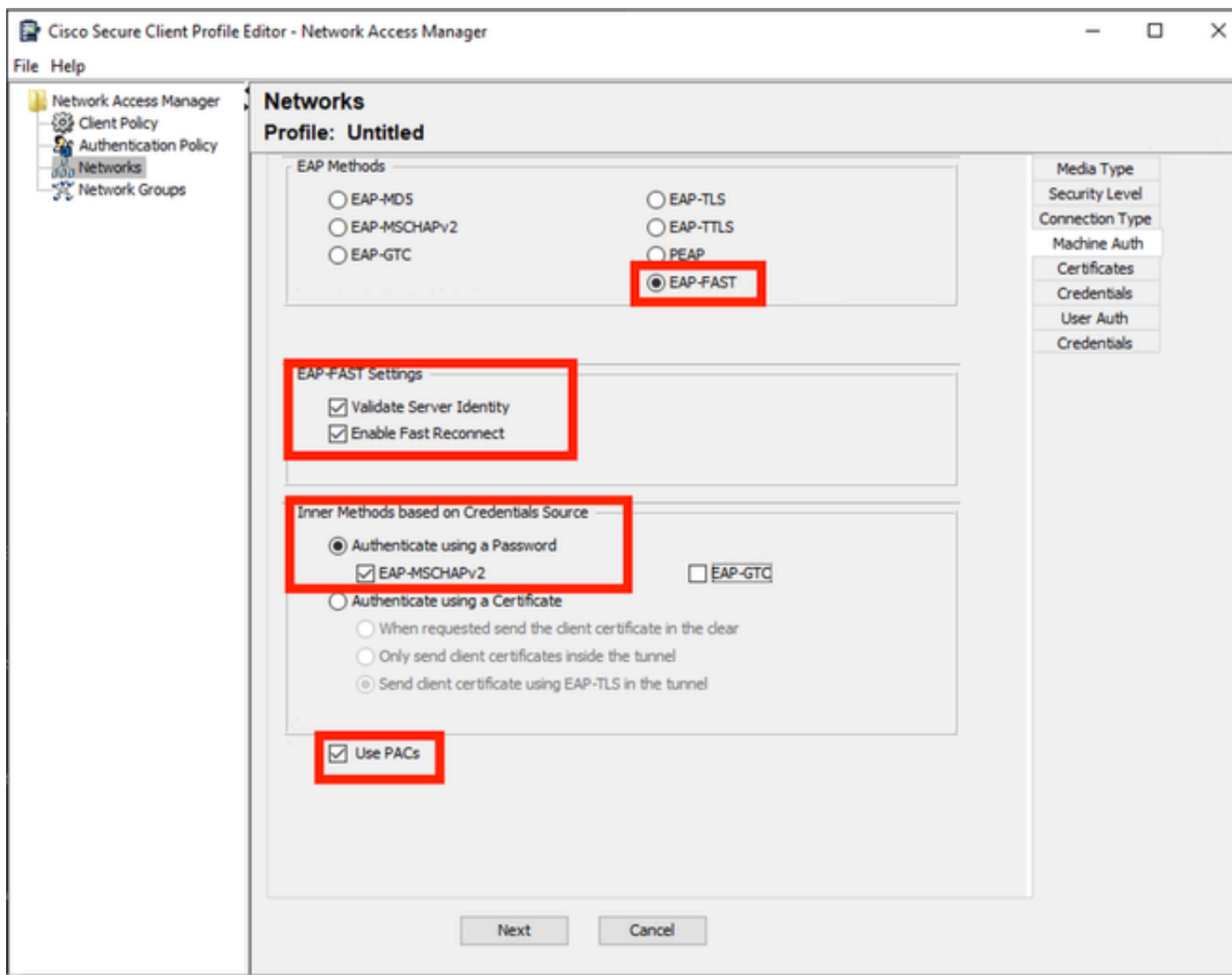
Media Type
Security Level
Connection Type
Machine Auth
Credentials
User Auth
Credentials

Next Cancel

Seção Tipo de Conexão

Configure a autenticação de usuário e máquina simultaneamente selecionando a terceira opção.

Clique em Next.



Seção de Autenticação da Máquina

Na seção Machine Auth, selecione EAP-FAST como o método EAP. Não altere os valores padrão das configurações EAP FAST. Na seção Métodos internos baseados na origem de credenciais, selecione Autenticar usando uma senha e EAP-MSCHAPv2 como o método. Em seguida, selecione a opção Usar PACs.

Clique em Next.

Na seção Certificados, em Regras do servidor confiável de certificados, o nome comum da regra termina com c.com. Esta seção se refere ao certificado que o servidor usa durante o fluxo PEAP EAP. Se o Identity Service Engine (ISE) for usado em seu ambiente, o nome comum do Certificado EAP do Nó do Servidor de Políticas poderá ser usado.

Networks

Profile: Untitled

Certificate Trusted Server Rules

| |
|--|
| <new> |
| Subject Alternative Name ends with c.com |

| Certificate Field | Match | Value |
|-------------------|-----------------|-------|
| Subject Alt. Name | exactly matches | |

Add Save

Certificate Trusted Authority

Trust any Root Certificate Authority (CA) Installed on the OS

Include Root Certificate Authority (CA) Certificates

| |
|--|
| |
|--|

Add Remove

Next Cancel

Media Type

Security Level

Connection Type

Machine Auth

Certificates

Credentials

User Auth

Certificates

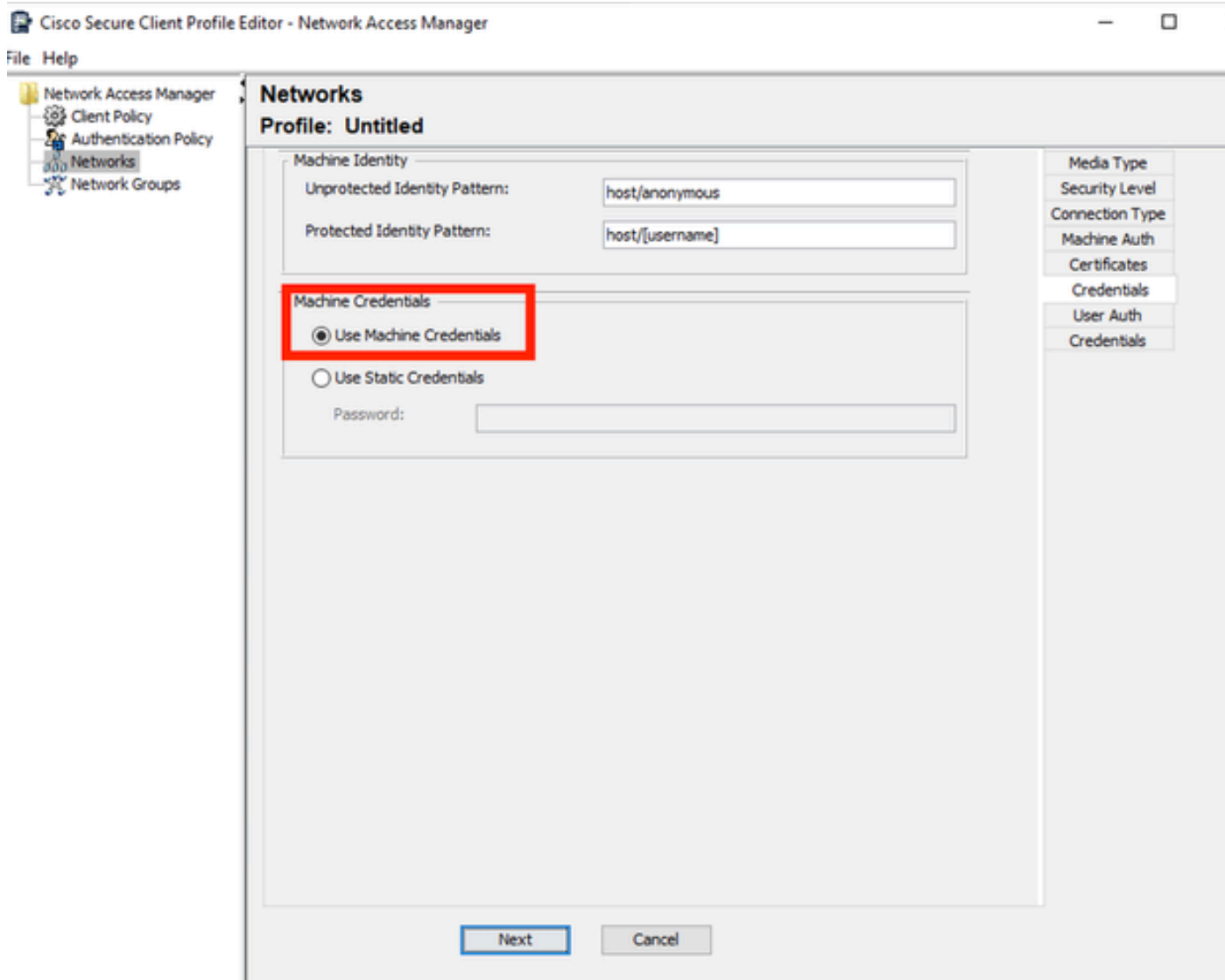
Credentials

Seção Confiança de Certificado de Servidor de Autenticação de Computador

Duas opções podem ser selecionadas em Autoridade de Certificação Confiável. Para este cenário, em vez de adicionar um Certificado CA específico que assinou o certificado RADIUS EAP, use a opção Trust any Root Certificate Authority (CA) Installed on the OS.

Com esta opção, o Windows confia em qualquer certificado EAP assinado por um certificado incluído no programa Gerenciar Certificados de Usuário (Usuário Atual > Autoridades de Certificação Raiz Confiáveis > Certificados).

Clique em Next.



Seção Credenciais de Autenticação de Máquina

Selecione Use Machine Credentials na seção Machine Credentials.

Clique em Next.

Networks
Profile: Untitled

EAP Methods

EAP-MD5 EAP-TLS
 EAP-MSCHAPv2 EAP-TTLS
 EAP-GTC PEAP
 EAP-FAST

Extend user connection beyond log off

EAP-FAST Settings

Validate Server Identity
 Enable Fast Reconnect
 Disable when using a Smart Card

Inner Methods based on Credentials Source

Authenticate using a Password
 EAP-MSCHAPv2 EAP-GTC
 Authenticate using a Certificate
 When requested send the client certificate in the clear
 Only send client certificates inside the tunnel
 Send client certificate using EAP-TLS in the tunnel
 Authenticate using a Token and EAP-GTC

Use PACs

Media Type
Security Level
Connection Type
Machine Auth
Certificates
Credentials
User Auth
Certificates
Credentials

Next Cancel

Seção Autenticação de Usuário

Para User Auth, selecione EAP-FAST como o Método EAP.

Não altere os valores padrão na seção de configurações de EAP-FAST.

Para a seção Método interno baseado na origem das credenciais, selecione Autenticar usando uma senha e EAP-MSCHAPv2 como o método.

Selecione Usar PACs.

Clique em Next.

Na seção Certificados, em Regras do servidor confiável de certificado, a regra é Nome comum termina com c.com. Essas configurações são para o certificado que o servidor usa durante o fluxo PEAP EAP. Se o ISE for usado em seu ambiente, o nome comum do certificado EAP do nó do servidor de políticas poderá ser usado.

Networks

Profile: C:\Users\LAB 5\Desktop\EAP FAST\configuration.xml

The screenshot shows the 'Networks' configuration window for a profile named 'C:\Users\LAB 5\Desktop\EAP FAST\configuration.xml'. The window is divided into several sections:

- Certificate Trusted Server Rules:** A list box contains one rule: 'Common Name ends with c.com', which is highlighted in blue and has a red box around it. Below the list is a table with columns 'Certificate Field', 'Match', and 'Value'. The table contains one row: 'Common Name' (with a dropdown arrow), 'ends with' (with a dropdown arrow), and 'c.com'. Below the table are 'Remove' and 'Save' buttons.
- Certificate Trusted Authority:** Two radio button options are present: 'Trust any Root Certificate Authority (CA) Installed on the OS' (which is selected) and 'Include Root Certificate Authority (CA) Certificates'. Below these is an empty list box and 'Add' and 'Remove' buttons.
- Navigation:** 'Next' and 'Cancel' buttons are at the bottom.
- Right Panel:** A vertical list of tabs: 'Media Type', 'Security Level', 'Connection Type', 'Machine Auth', 'Certificates', 'Credentials', 'User Auth', 'Certificates', and 'Credentials'. The second 'Certificates' tab is highlighted with a red box.

Seção Confiança de Certificado do Servidor de Autenticação de Usuário

Duas opções podem ser selecionadas em Autoridade de Certificação Confiável. Para esse cenário, em vez de adicionar um Certificado de CA específico que assinou o certificado RADIUS EAP, a opção Trust any Root Certificate Authority (CA) Installed on the OS é usada.

Clique em Next.

Networks

Profile: Untitled

User Identity

Unprotected Identity Pattern:

Protected Identity Pattern:

User Credentials

Use Single Sign On Credentials

Prompt for Credentials

- Remember Forever
- Remember while User is Logged On
- Never Remember

Use Static Credentials

Password:

Media Type

Security Level

Connection Type

Machine Auth

Certificates

Credentials

User Auth

Certificates

Credentials

Done Cancel

Credenciais de Autenticação do Usuário

Na seção Credenciais, apenas a seção Credenciais do usuário é alterada.

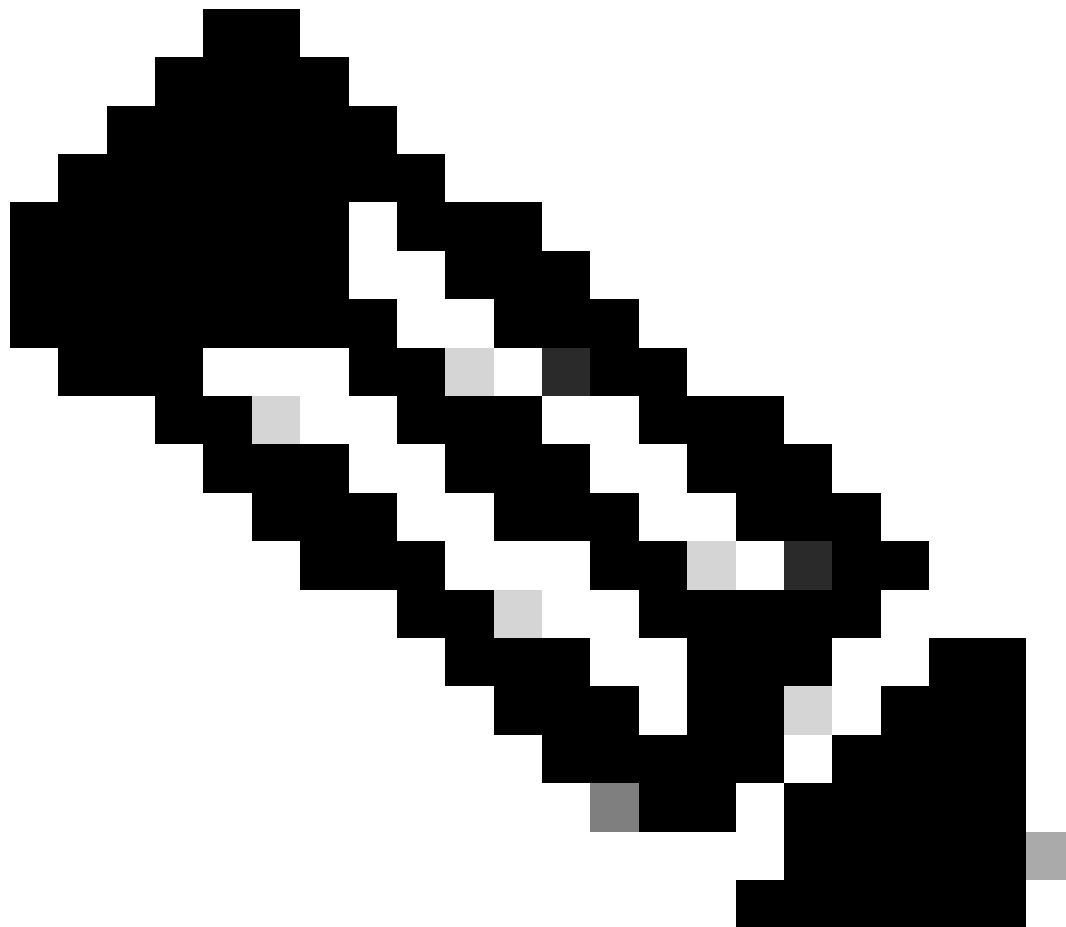
A opção Solicitar credenciais > Nunca lembrar está selecionada. Portanto, em cada autenticação, o usuário que estiver autenticando deverá inserir suas credenciais.

Clique no botão Concluído.

Selecione File > Save as e salve o perfil Secure Client Network Access Manager como configuration.xml.

Para fazer com que o Secure Client Network Access Manager use o perfil que acabou de ser criado, substitua o arquivo configuration.xml no próximo diretório pelo novo:

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



Observação: o arquivo deve ser nomeado como configuration.xml, caso contrário ele não funcionará.

6. Cenário 3: Configurar um Requerente de NAM de Cliente Seguro para Autenticação de Certificado de Usuário TLS EAP

Abra o NAM Profile Editor e navegue para a seção Redes.

Clique em Add.

Networks

Profile: Untitled

Network

| Name | Media Type | Group* |
|------|------------|--------|
|------|------------|--------|

Add...

Edit...

Delete

* A network in group 'Global' is a member of *all* groups.

Seção de criação de rede

Nomeie o perfil de rede, nesse caso, o nome é com o protocolo EAP usado para esse cenário.

Selecione Global para Associação de grupo. E Meios De Rede Com Fio.

Networks
Profile: Untitled

Name:

Group Membership

In group:

In all groups (Global)

Choose Your Network Media

Wired (802.3) Network

Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable.

Wi-Fi (wireless) Network

Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point.

SSID (max 32 chars):

Hidden Network

Corporate Network

Association Timeout: seconds

Common Settings

Script or application on each user's machine to run when connected.

Connection Timeout: seconds

Media Type
Security Level

Seção Tipo de Mídia

Clique em Next.

Selecione Authenticating Network e não altere os valores padrão para o restante das opções na seção Security Level.

Network Access Manager

- Client Policy
- Authentication Policy
- Networks**
- Network Groups

Networks

Profile: Untitled

Security Level

Open Network
Open networks have no security, and are open to anybody within range. This is the least secure type of network.

Authenticating Network
Authenticating networks provide the highest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure.

802.1X Settings

authPeriod (sec.) startPeriod (sec.)

heldPeriod (sec.) maxStart

Port Authentication Exception Policy

Enable port exceptions

Allow data traffic before authentication

Allow data traffic after authentication even if

EAP fails

EAP succeeds but key management fails

Security

Key Management

None

Encryption

AES GCM 128

AES GCM 256

Media Type

Security Level

Connection Type

Next Cancel

Nível de segurança

Este cenário é para autenticação de usuário usando um certificado. Por esse motivo, a opção User Connection é usada.

Network Access Manager

- Client Policy
- Authentication Policy
- Networks**
- Network Groups

Networks

Profile: Untitled

Network Connection Type

Machine Connection
This should be used if the end station should log onto the network before the user logs in. This is typically used for connecting to domains, to get GPO's and other updates from the network before the user has access.

User Connection
The user connection should be used when a machine connection is not needed. A user connection will make the network available after the user has logged on.

Machine and User Connection
This type of connection will be made automatically when the machine boots. It will then be brought down, and back up again with different credentials when the user logs in.

Media Type

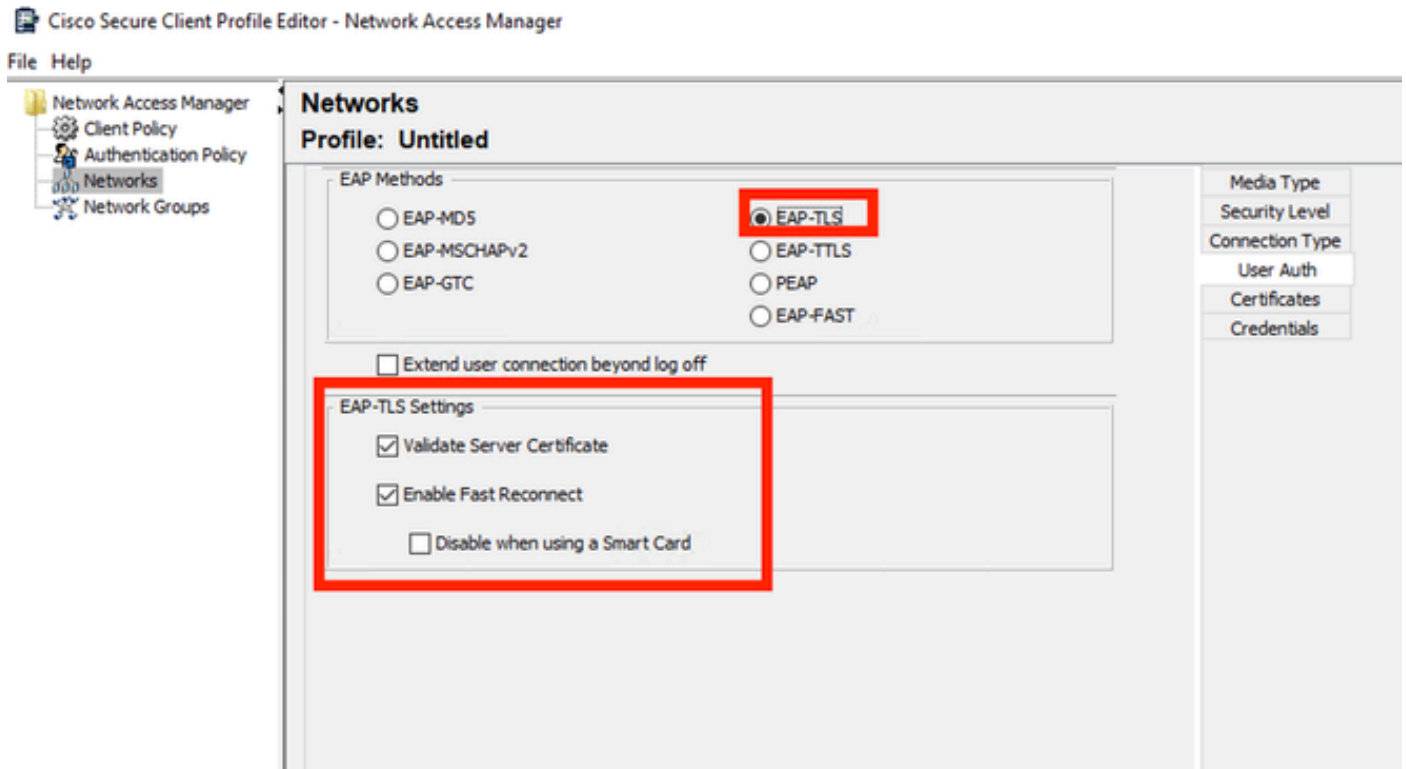
Security Level

Connection Type

User Auth

Credentials

Configure EAP-TLS como o método EAP. Não altere os valores padrão na seção Configurações de EAP-TLS.



Seção Autenticação de Usuário

Para a seção Certificados, crie uma regra que corresponda ao certificado AAA EAP-TLS. Se você estiver usando o ISE, encontre essa regra na seção Administração > Sistema > Certificados.

Na seção Certificate Trusted Authority, selecione Trust any Root Certificate Authority (CA) installed no SO.

The screenshot shows the 'Networks' section of the Cisco Secure Client Profile Editor. The main window is titled 'Profile: Untitled'. On the left, a navigation pane shows 'Network Access Manager', 'Client Policy', 'Authentication Policy', 'Networks', and 'Network Groups'. The 'Networks' section is active, displaying two configuration panels. The first panel, 'Certificate Trusted Server Rules', contains a list of rules with one rule highlighted: 'Common Name ends with c.com'. Below this list is a table for defining new rules with columns for 'Certificate Field', 'Match', and 'Value'. The 'Certificate Field' is set to 'Subject Alt. Name', the 'Match' is 'exactly matches', and the 'Value' field is empty. The second panel, 'Certificate Trusted Authority', shows two radio button options: 'Trust any Root Certificate Authority (CA) Installed on the OS' (which is selected) and 'Include Root Certificate Authority (CA) Certificates'. Below these options is an empty list box with 'Add' and 'Remove' buttons. At the bottom of the window are 'Next' and 'Cancel' buttons. On the right side, a vertical menu contains 'Media Type', 'Security Level', 'Connection Type', 'User Auth', 'Certificates', and 'Credentials', with 'Certificates' highlighted.

Configurações de Confiança de Certificado do Servidor de Autenticação de Usuário

Clique em Next.

Na seção Credenciais do usuário, não altere os valores padrão na primeira parte.

Networks

Profile: Untitled

User Identity

Unprotected Identity Pattern:

User Credentials

Use Single Sign On Credentials (Requires Smart Card)

Prompt for Credentials

- Remember Forever
- Remember while User is Logged On
- Never Remember

Certificate Source

Smart Card or OS certificates

Smart Card certificates only

Remember Smart Card Pin

Remember Forever

Remember while User is Logged On

Never Remember

Smart Card Removal Policy

Disconnect from Network

Use Certificate Matching Rule (Max 10)

Rule Logic OR AND

| Field | Operator | Value |
|-------|----------|-------|
| | | |
| | | |
| | | |

Media Type

Security Level

Connection Type

User Auth

Certificates

Credentials

Done

Cancel

Seção Credenciais de Autenticação do Usuário

É importante configurar uma regra que corresponda ao certificado de identidade que o usuário envia durante o processo EAP TLS. Para fazer isso, clique na caixa de seleção ao lado de Usar regra de correspondência de certificado (máx. 10).

Clique em Add.

Certificate Matching Rule Entry [X]

Certificate Field: Issuer.CN Match: Equals

Value: My Internal OR 3rd Party CA.com

OK Cancel

Use Certificate Matching Rule (Max 10)

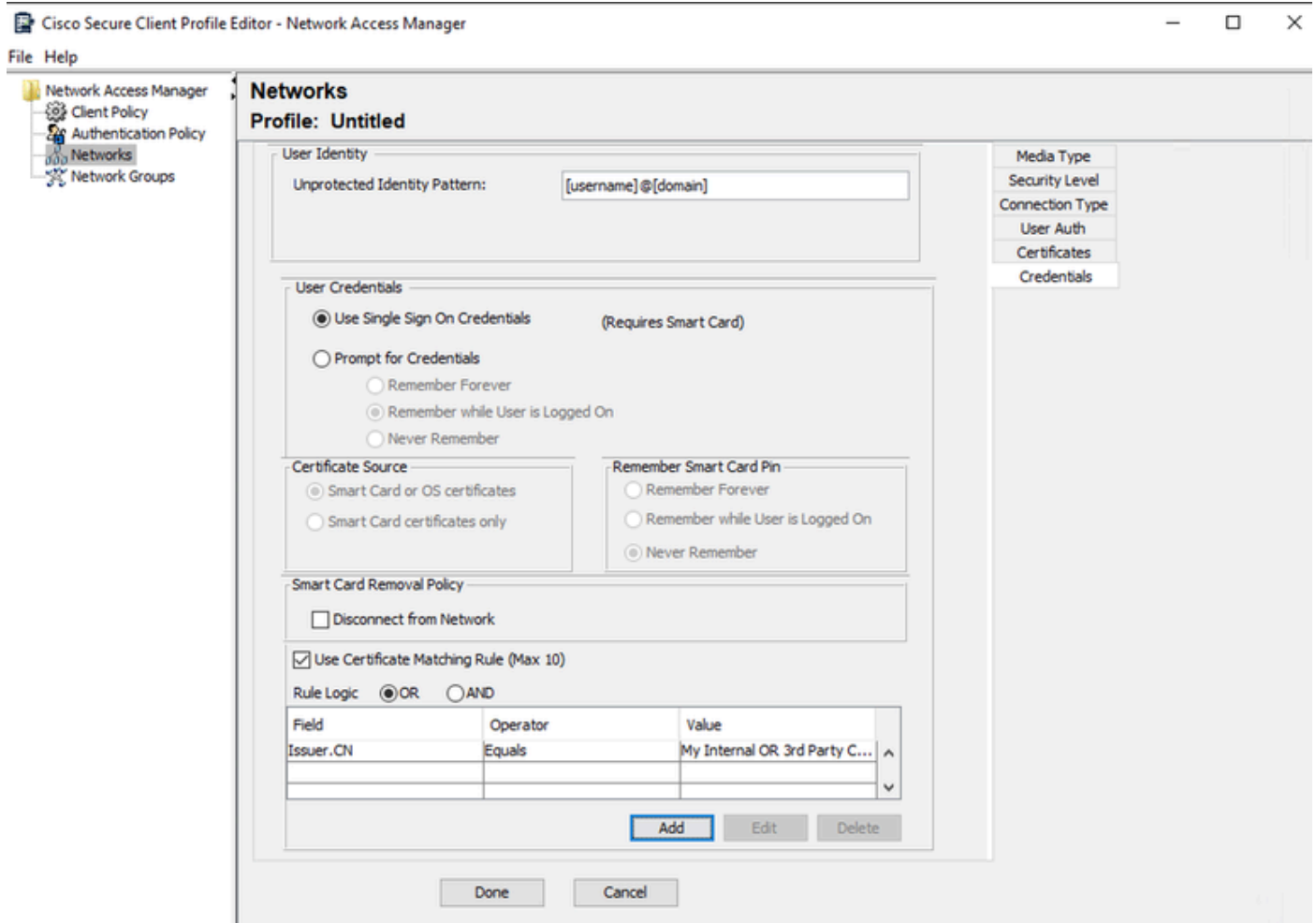
Logic: OR AND

| Id | Operator | Value |
|----|----------|-------|
| | | |
| | | |
| | | |

Add Edit Delete

Janela Regra de Correspondência de Certificado

Substitua a string My Internal OR 3rd Party CA.com pelo CN do certificado do usuário.



Seção Credenciais de Certificado de Autenticação de Usuário

Clique em Done para concluir a configuração.

Selecione File > Save as para salvar o perfil Secure Client Network Access Manager como configuration.xml.

Para fazer com que o Secure Client Network Access Manager use o perfil que acabou de ser criado, substitua o arquivo configuration.xml no próximo diretório pelo novo:

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



Observação: o arquivo deve ser nomeado como configuration.xml, caso contrário ele não funcionará.

7. Configurar ISR 1100 e ISE para Permitir Autenticações com Base no Cenário 1 PEAP MSCHAPv2

Configure o roteador ISR 1100.

Esta seção aborda a configuração básica que o NAD deve ter para fazer com que o dot1x funcione.

Observação: para implantação do ISE com vários nós, aponte para qualquer nó que tenha a persona Policy Server Node habilitada. Para verificar isso, navegue até o ISE na guia Administração > Sistema > Implantação.

```
aaa new-model
aaa session-id common
!
aaa authentication dot1x default group ISE-CLUSTER
aaa authorization network default group ISE-CLUSTER
aaa accounting system default start-stop group ISE-CLUSTER
aaa accounting dot1x default start-stop group ISE-CLUSTER
!
aaa server radius dynamic-author
  client A.B.C.D server-key <Your shared secret>
!
!
radius server ISE-PSN-1
  address ipv4 A.B.C.D auth-port 1645 acct-port 1646
  timeout 15
  key <Your shared secret>
```

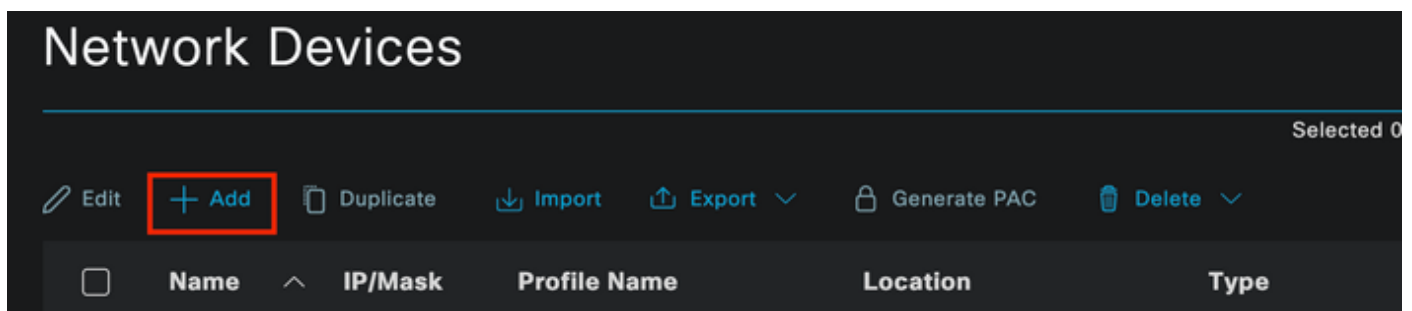
```
!  
!  
aaa group server radius ISE-CLUSTER  
  server name ISE-PSN-1  
!  
interface GigabitEthernet0/1/0  
  description "Endpoint that supports dot1x"  
  switchport access vlan 15  
  switchport mode access  
  authentication host-mode multi-auth  
  authentication order dot1x mab  
  authentication priority dot1x mab  
  authentication port-control auto  
  dot1x pae authenticator  
  spanning-tree portfast
```

Configure o Identity Service Engine 3.2.

Configure o dispositivo de rede.

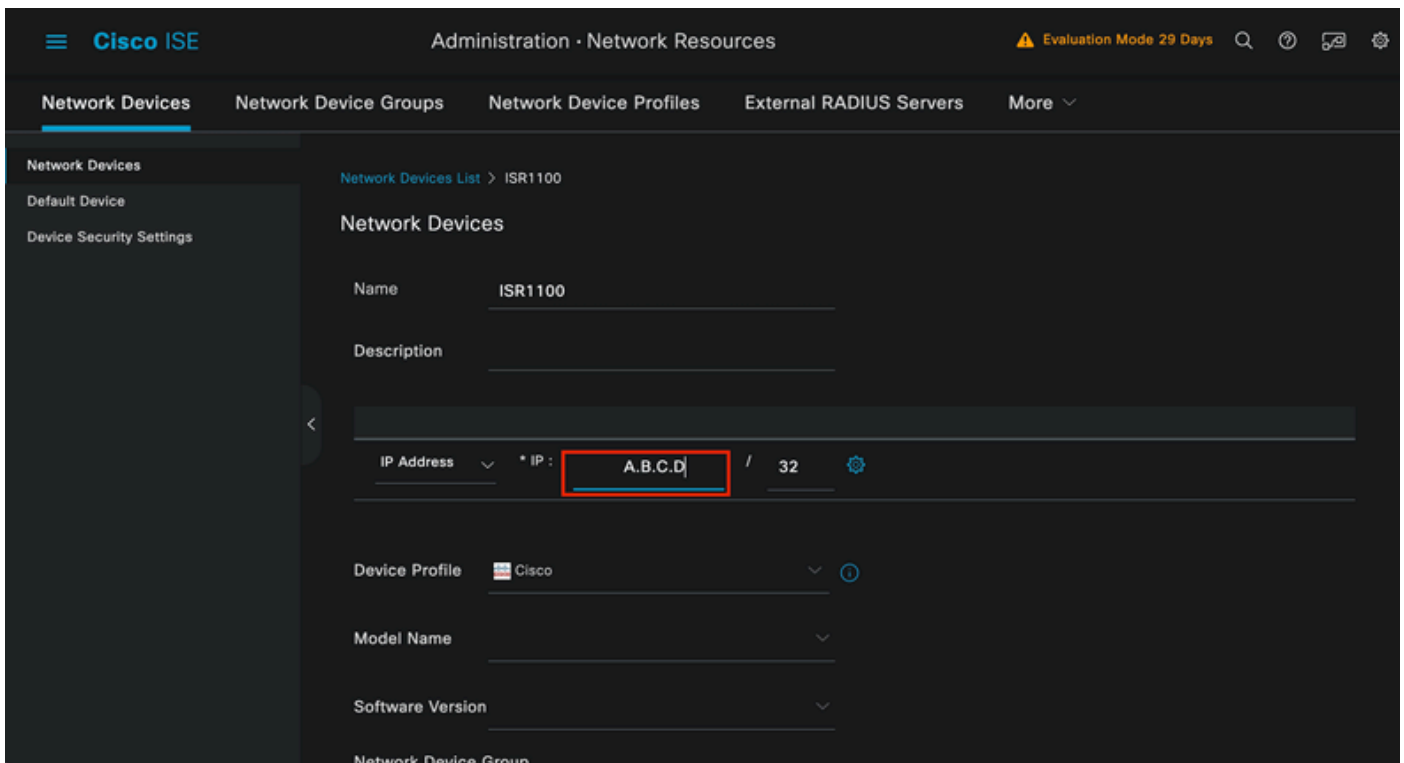
Adicione o ISR NAD ao ISE Administração > Recursos de rede > Dispositivos de rede.

Clique em Add.



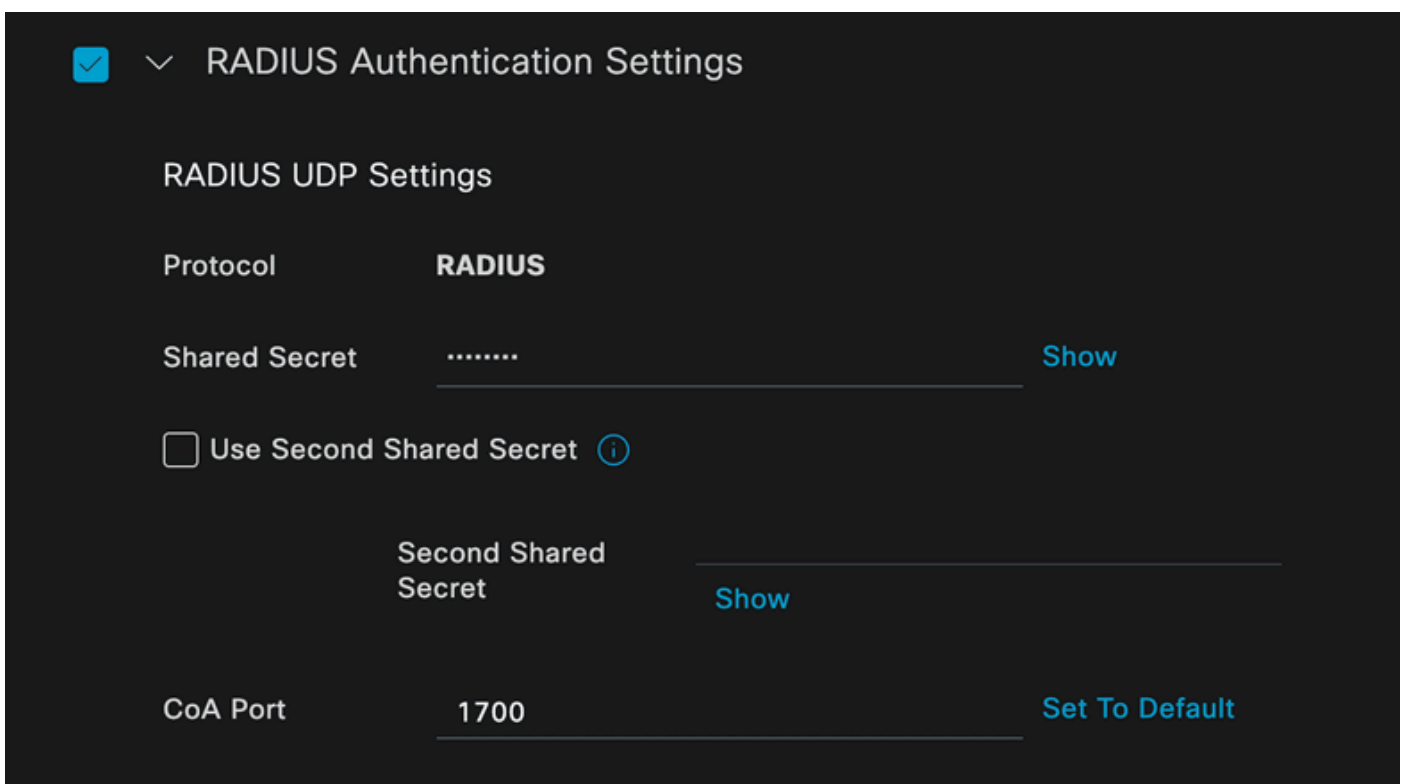
Seção Dispositivo de rede

Atribua um nome ao NAD que você está criando. Adicione o IP do dispositivo de rede.



Criação de dispositivo de rede

Na parte inferior da mesma página, adicione o mesmo Shared Secret que você usou em sua configuração de dispositivo de rede.



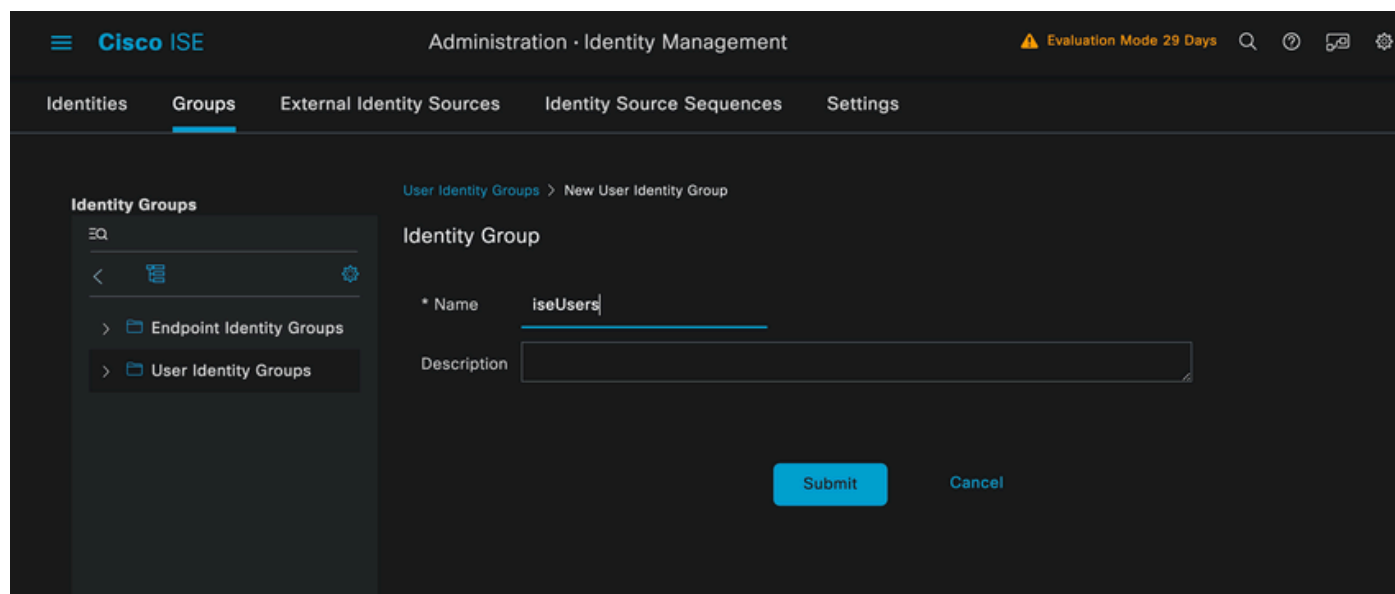
Configurações Radius do Dispositivo de Rede

Salve as alterações.

Configure a identidade que é usada para autenticar o ponto final.

A autenticação local do ISE é usada. A autenticação externa do ISE não é explicada neste artigo.

Navegue até a guia Administração > Gerenciamento de identidades > Grupos e crie o grupo do qual o usuário faz parte. O grupo de identidade criado para esta demonstração é iseUsers.

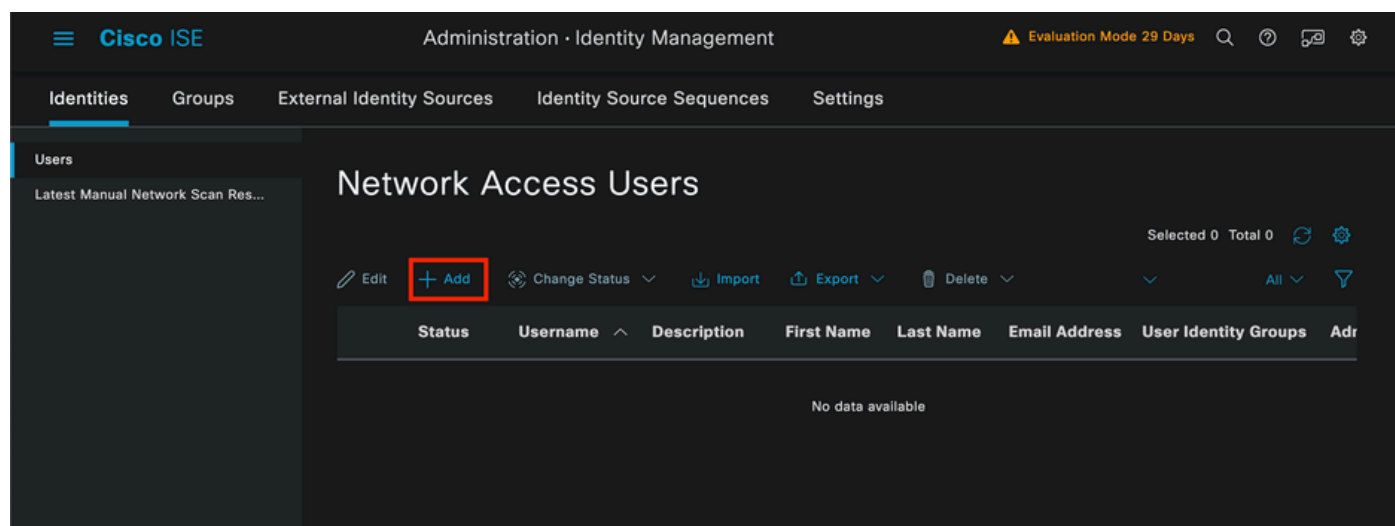


Criação do grupo de identidade

Clique em Submit.

Navegue até a guia Administração > Gerenciamento de identidades > Identidade.

Clique em Add.



Seção Usuários de Acesso à Rede

Como parte dos campos obrigatórios, comece com o nome do usuário. O nome de usuário isiscool é usado neste exemplo.

Network Access User

* Username

Status Enabled

Account Name Alias

Email

Criação de usuário de acesso à rede

Atribua uma senha ao usuário. O VainillaIse97 é usado.

Passwords

Password Type:

Password Lifetime:

- With Expiration
Password will expire in 60 days
- Never Expires

Password

Re-Enter Password

* Login Password

Generate Password

Enable Password

Generate Password

Seção Senha de Criação do Usuário

Atribua o usuário ao grupo iseUsers.

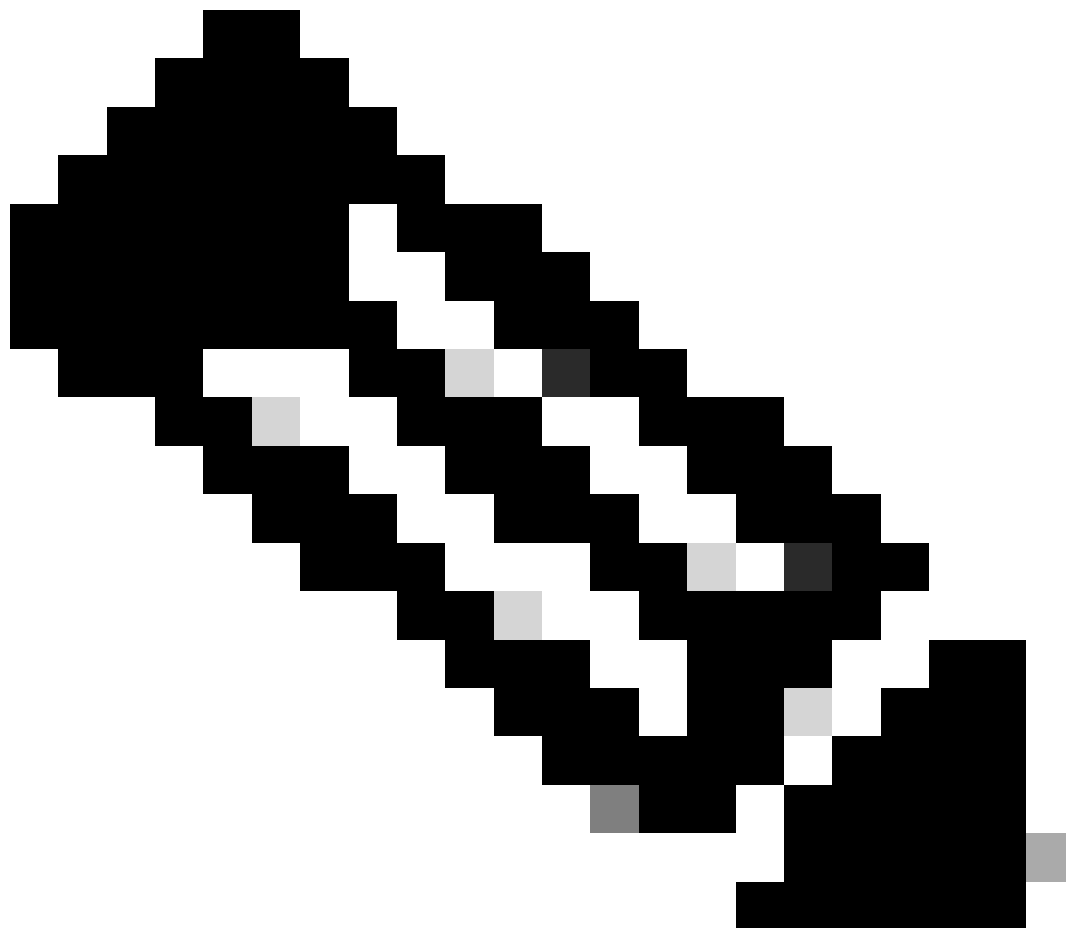
User Groups

Atribuição de grupo de usuários

Configure a Política definida.

Navegue até o menu ISE > Política > Conjuntos de políticas.

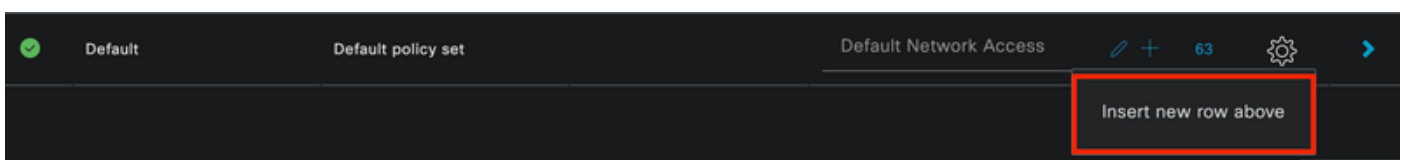
O conjunto de políticas padrão pode ser usado. No entanto, um chamado Com fio é criado para este exemplo.



Observação: classificar e diferenciar os conjuntos de políticas ajuda na solução de problemas,

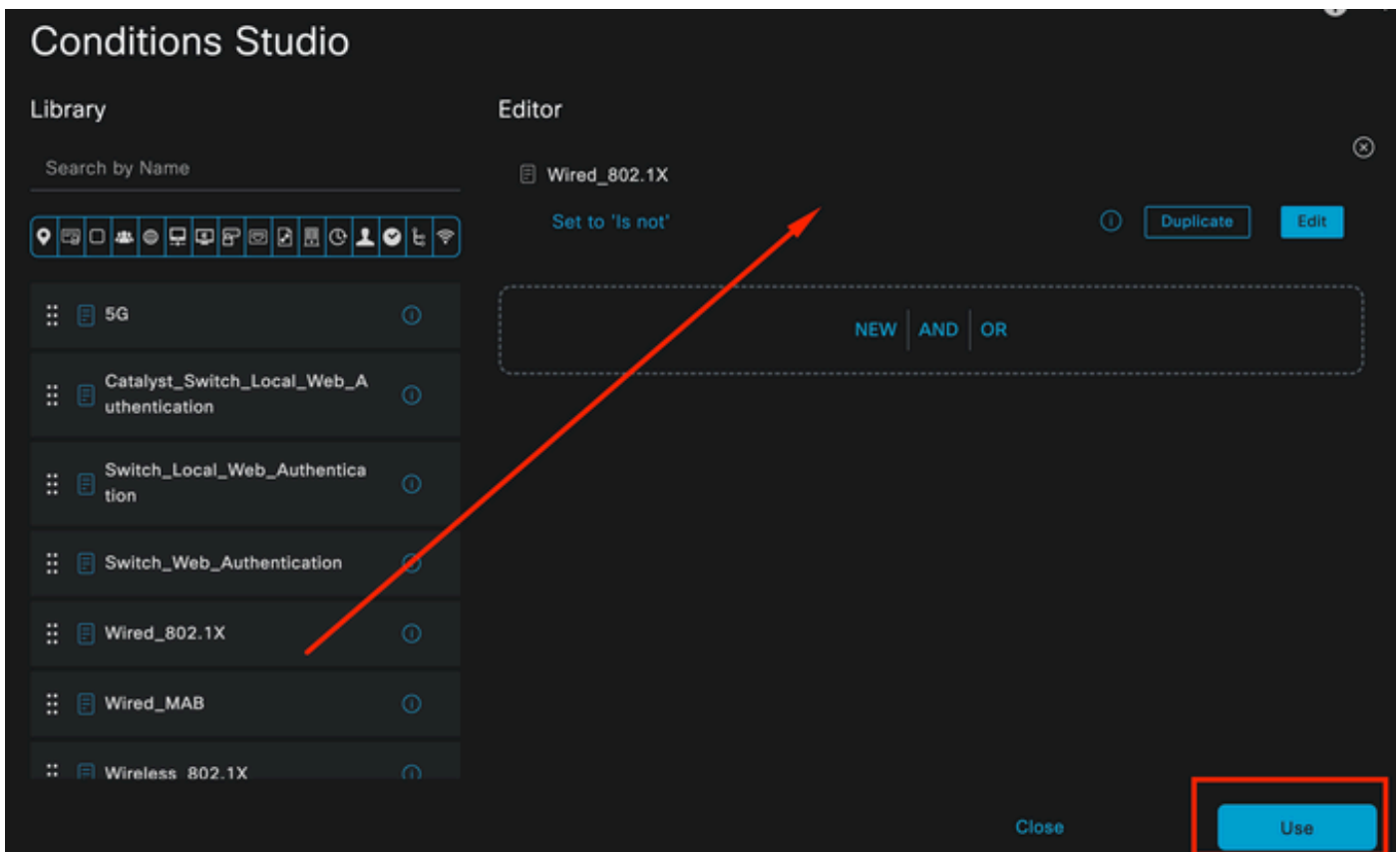


Observação: se o ícone adicionar ou mais não estiver visível, o ícone de engrenagem de qualquer conjunto de políticas poderá ser clicado e, em seguida, selecionar Inserir nova linha acima.



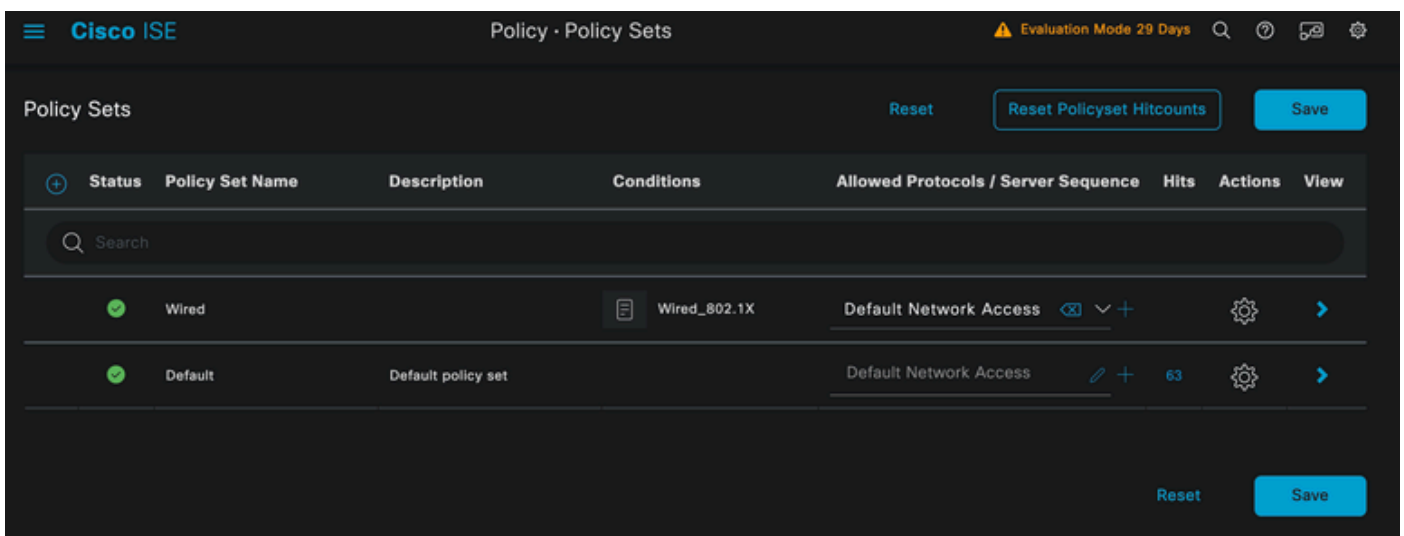
Opções de ícone de engrenagem

A condição usada é Wired 8021x. Arraste-o e clique em Usar.



Estúdio de Condição de Política de Autenticação

Selecione Default Network Access na seção Allowed Protocols.

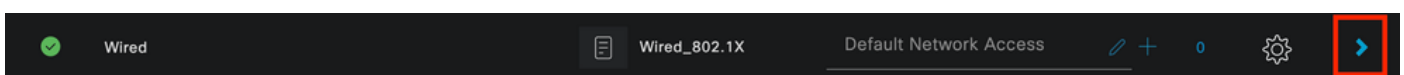


Exibição Geral de Conjuntos de Políticas

Click Save.

2.d. Configure as Políticas de Autenticação e Autorização.

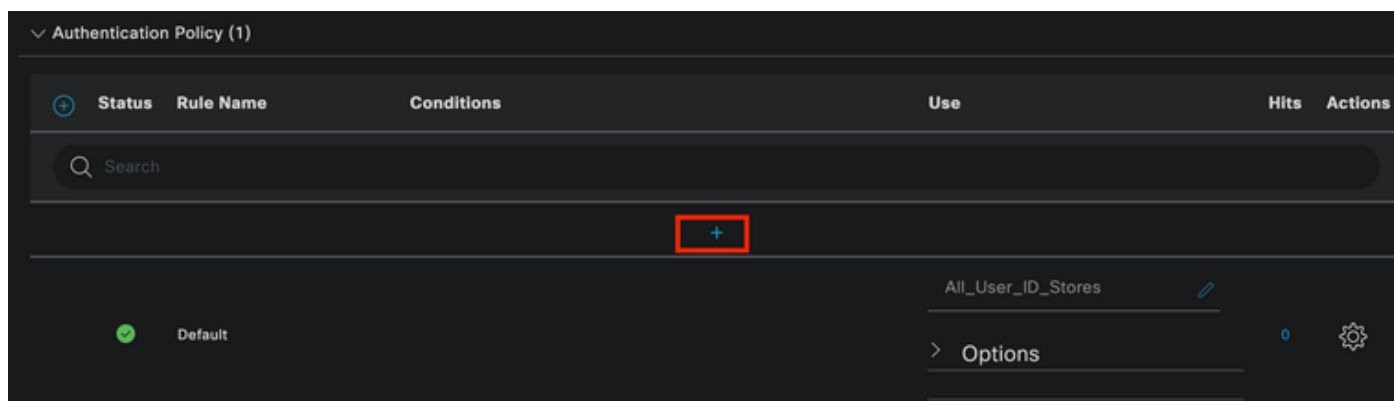
Clique no ícone >.



Conjunto de políticas com fio

Expanda a seção Authentication Policy.

Clique no ícone +.



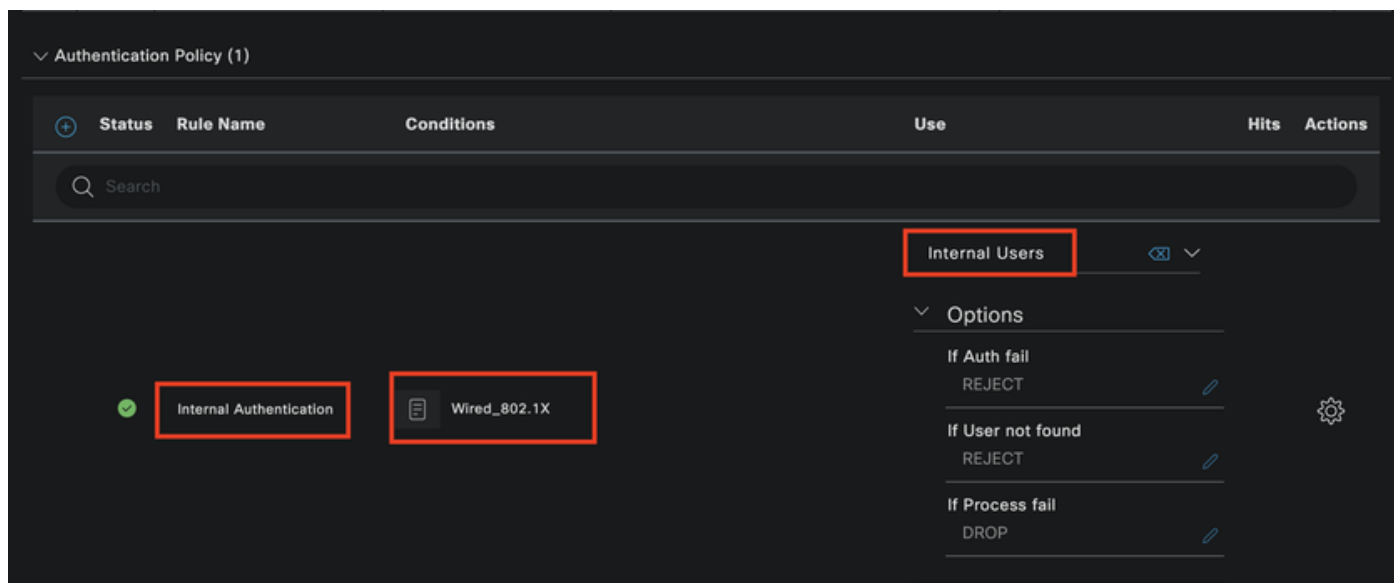
Política de autenticação

Atribua um nome à política de autenticação. A Autenticação Interna é usada neste exemplo.

Clique no ícone + na coluna condições para esta nova Política de autenticação.

A condição pré-configurada Wired Dot1x é usada.

Finalmente, na coluna Usar, selecione Usuários internos.



Política de autenticação

Política de Autorização.

A seção Política de autorização está na parte inferior da página. Expanda-o e clique no ícone +.

The screenshot displays the Cisco ISE interface for configuring Policy Sets. At the top, the navigation bar includes the Cisco ISE logo, the title 'Policy · Policy Sets', and a warning for 'Evaluation Mode 29 Days'. The main content area is divided into sections for 'Authorization Policy - Local Exceptions', 'Authorization Policy - Global Exceptions', and a selected 'Authorization Policy (1)'. Below this, a table lists the policy configurations. The table has columns for Status, Rule Name, Conditions, Profiles, Security Groups, Hits, and Actions. A search bar is located above the table. The 'Default' policy is listed with a status of 'Default'. The 'Conditions' column for this policy has a '+' icon highlighted with a red box. The 'Profiles' column shows 'DenyAccess' and the 'Security Groups' column shows 'Select from list'. At the bottom right, there are 'Reset' and 'Save' buttons.

Política de Autorização

Nomeie a Diretiva de Autorização criada recentemente. Neste exemplo de configuração, o nome Internal ISE Users é usado.

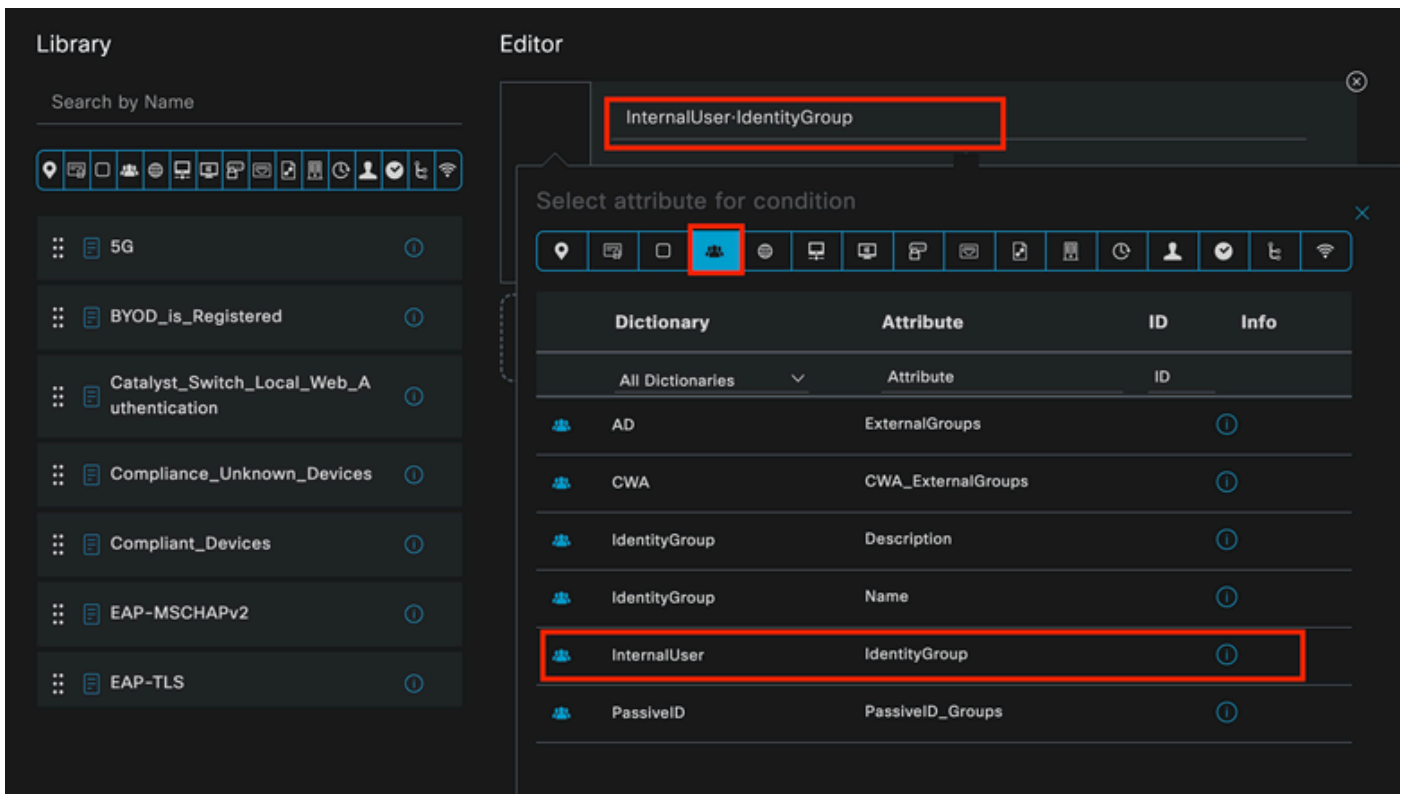
Para criar uma condição para esta Diretiva de autorização, clique no ícone + na coluna Condições.

O grupo IseUsers é usado.

Clique na seção Atributo.

Selecione o ícone IdentityGroup.

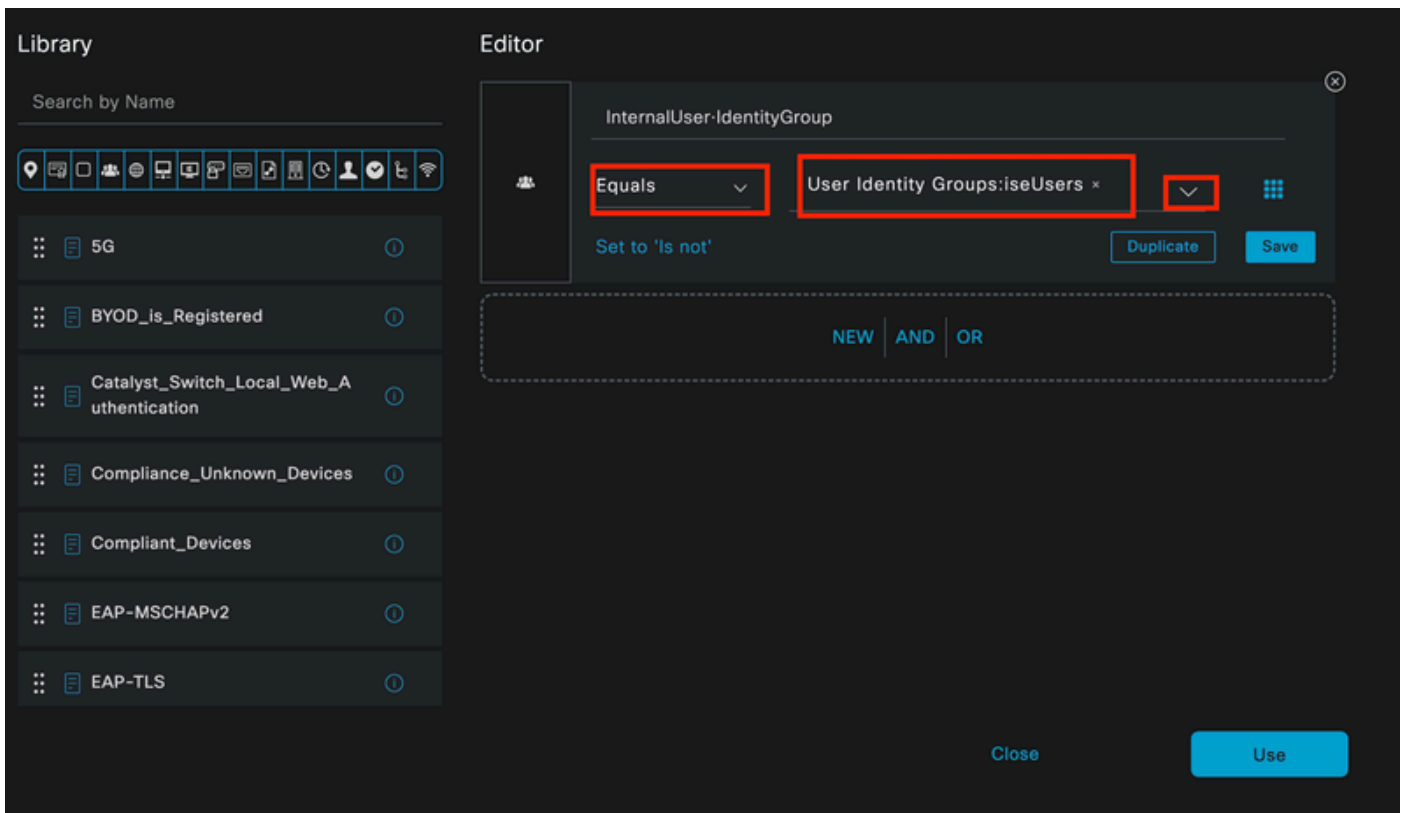
No dicionário, selecione o dicionário InternalUser que vem com o atributo IdentityGroup.



Criação de Condição

Selecione o operador Equals.

Em User Identity Groups, selecione o grupo IseUsers.

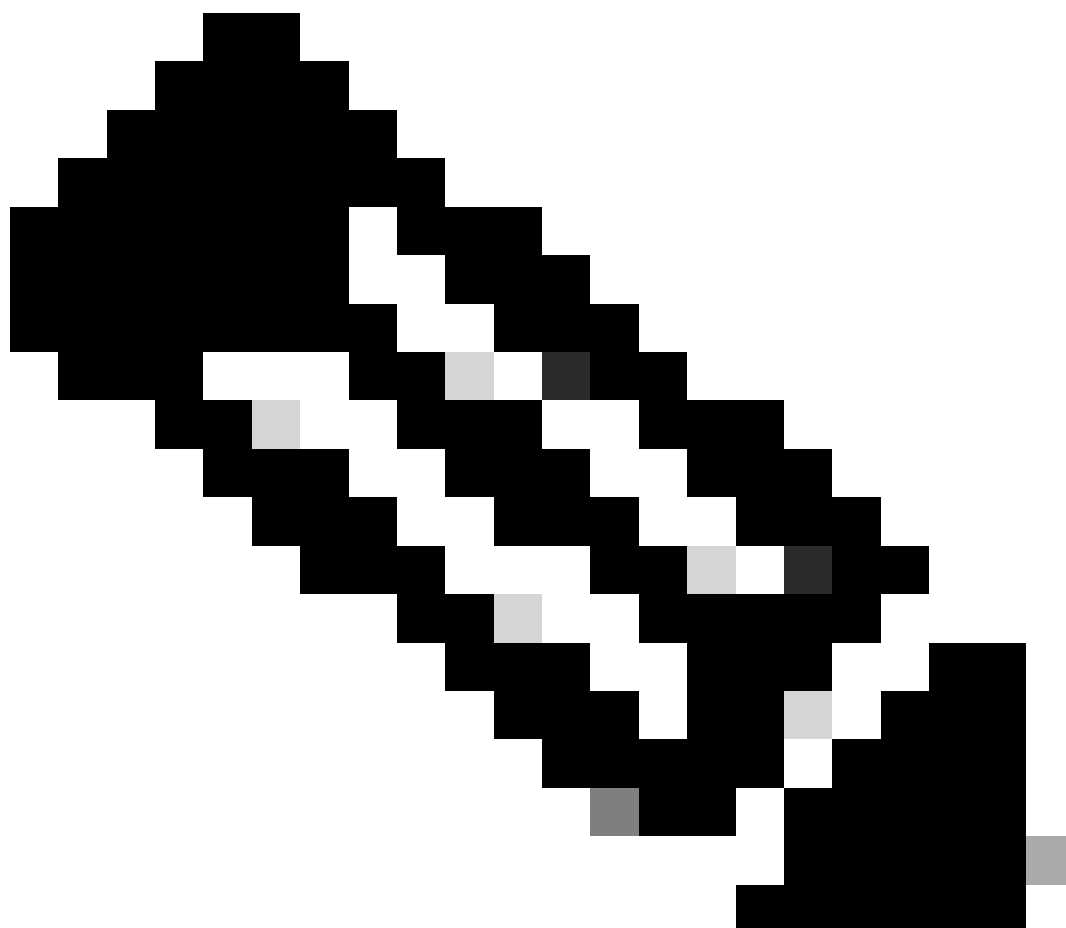


Criação de Condição

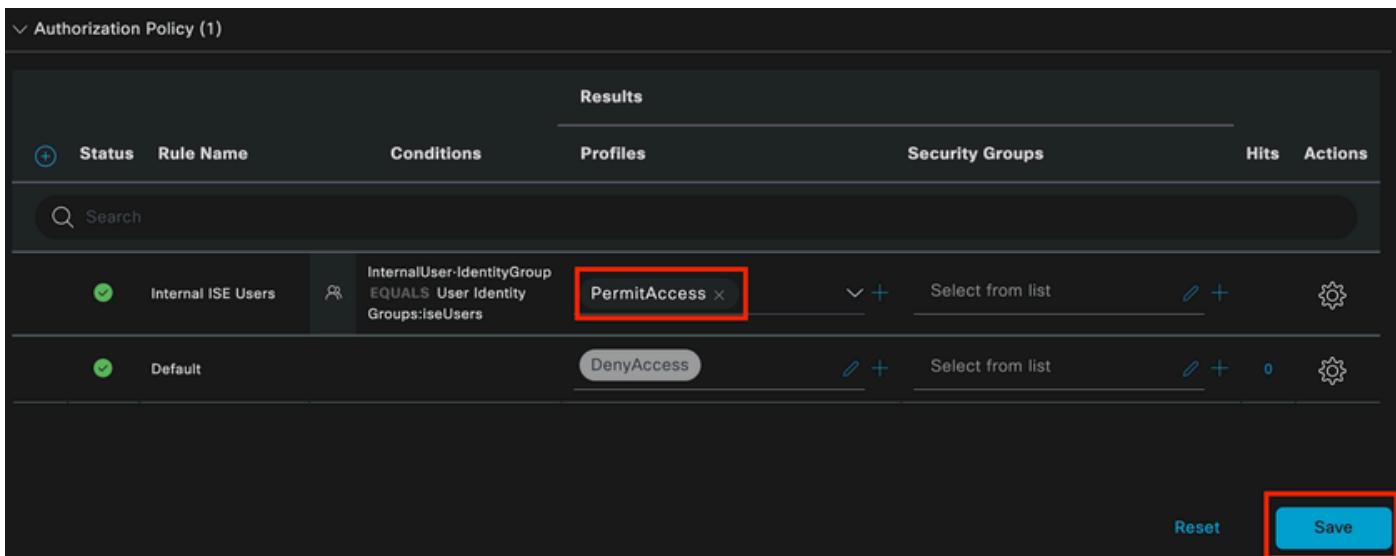
Clique em Usar.

Adicione o perfil de autorização de resultado.

O perfil pré-configurado Permitir Acesso é usado.



Observação: observe que as autenticações que chegam ao ISE atingindo esse conjunto de políticas Wired Dot1x que não fazem parte do grupo de identidade de usuários ISEUsers, atingem a política de autorização padrão, que tem o resultado DenyAccess.



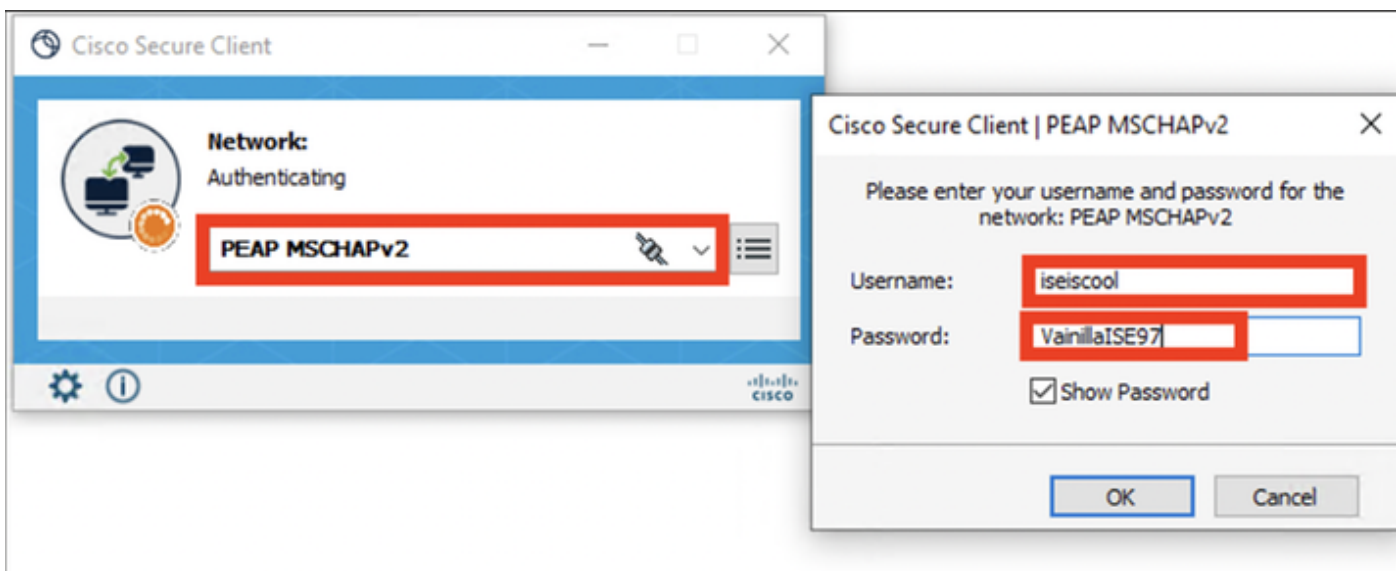
Política de Autorização

Click Save.

Verificar

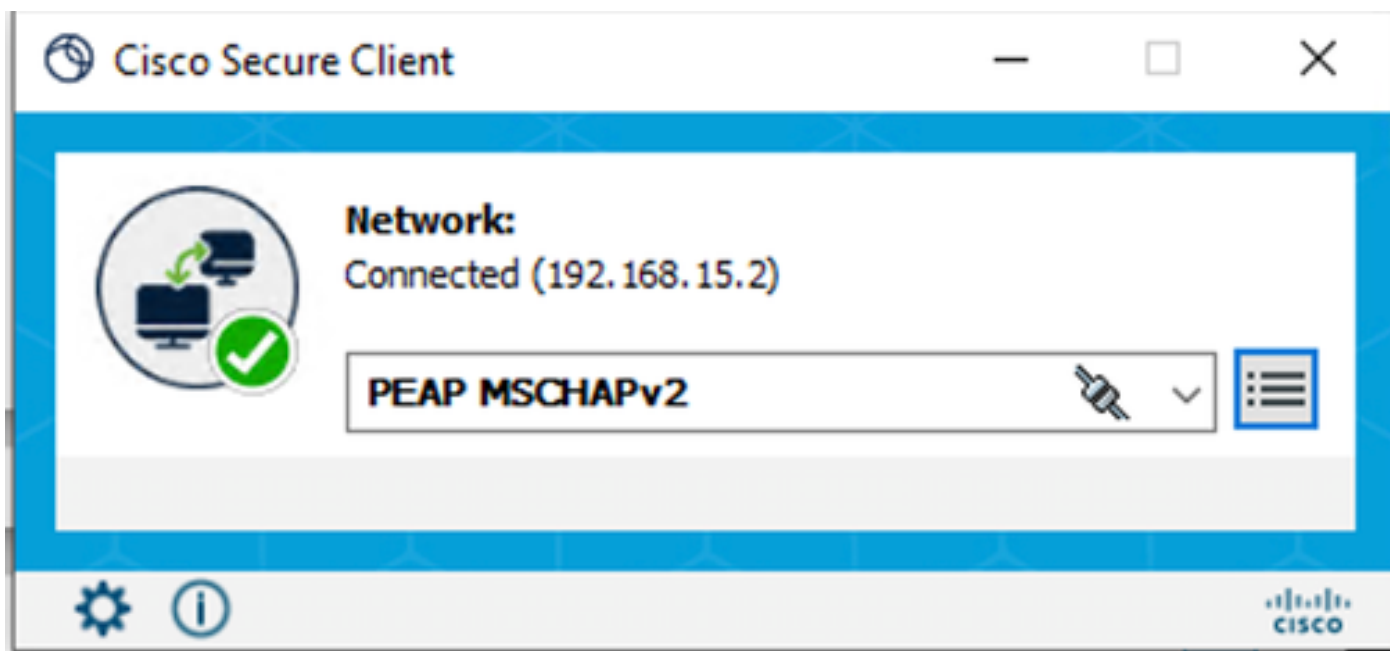
Quando a configuração for concluída, o Secure Client solicitará as credenciais e especificará o uso do perfil PEAP MSCHAPv2.

As credenciais criadas anteriormente são inseridas.



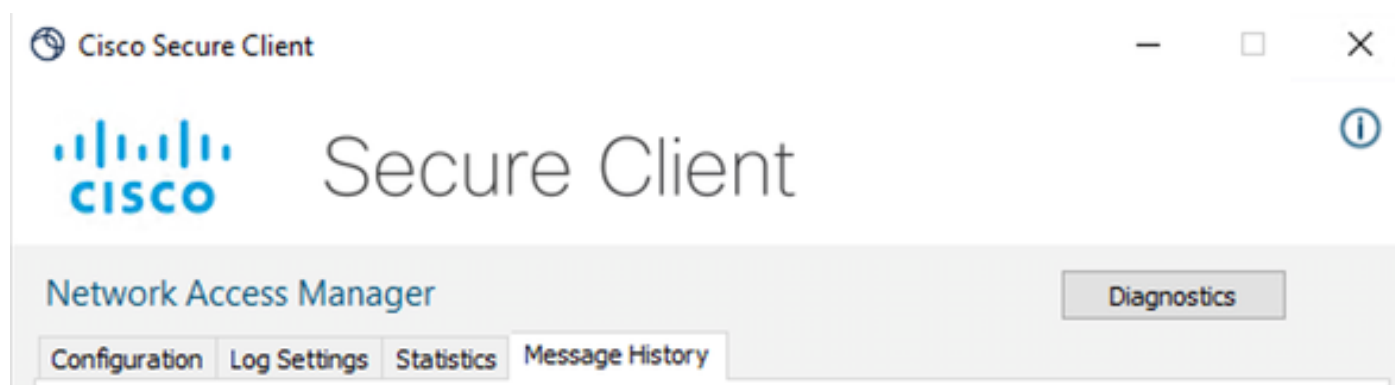
NAM de Cliente Seguro

Se o endpoint for autenticado corretamente, o NAM indica que está conectado.



NAM de Cliente Seguro

Ao clicar no ícone de informações e navegar até a seção Histórico de mensagens, os detalhes de cada etapa realizada pelo NAM são exibidos.



Histórico de mensagens do cliente seguro

```
7:06:01 PM PEAP MSCHAPv2 : Authenticating
7:06:21 PM PEAP MSCHAPv2 : Acquiring IP Address
7:06:21 PM PEAP MSCHAPv2 : Connected
```

Histórico de mensagens do cliente seguro

No ISE, navegue até Operations > Radius LiveLogs para ver os detalhes da autenticação. Como visto na imagem seguinte, o nome de usuário que foi usado é exibido.

Também outros detalhes como:

- Carimbo de data/hora.
- Endereço MAC.
- Conjunto de políticas usado.
- Authentication Policy (Política de autenticação).

- Política de autorização.
- Outras informações relevantes.

The screenshot shows the Cisco ISE Operations - RADIUS interface. At the top, there are navigation tabs for 'Live Logs' and 'Live Sessions'. Below this, there are five summary cards: 'Misconfigured Supplicants' (0), 'Misconfigured Network Devices' (0), 'RADIUS Drops' (25), 'Client Stopped Responding' (0), and 'Repeat Counter' (0). Below the cards, there are controls for 'Refresh' (Never), 'Show' (Latest 20 records), and 'Within' (Last 5 minutes). A table of logs is displayed below, with columns for Time, Status, Details, Repeats, Identity, Endpoint ID, Endpoint Pr, Authentication Policy, Authorization Policy, Authoriz..., IP Address, and Network De... The table shows two entries for 'iselacool' with a status of 'Success' and 'Wired >> Internal Authentication'. At the bottom, it says 'Last Updated: Tue Apr 23 2024 13:02:14 GMT-0600 (Central Standard Time)' and 'Records Shown: 2'.

Logs ao vivo do ISE RADIUS

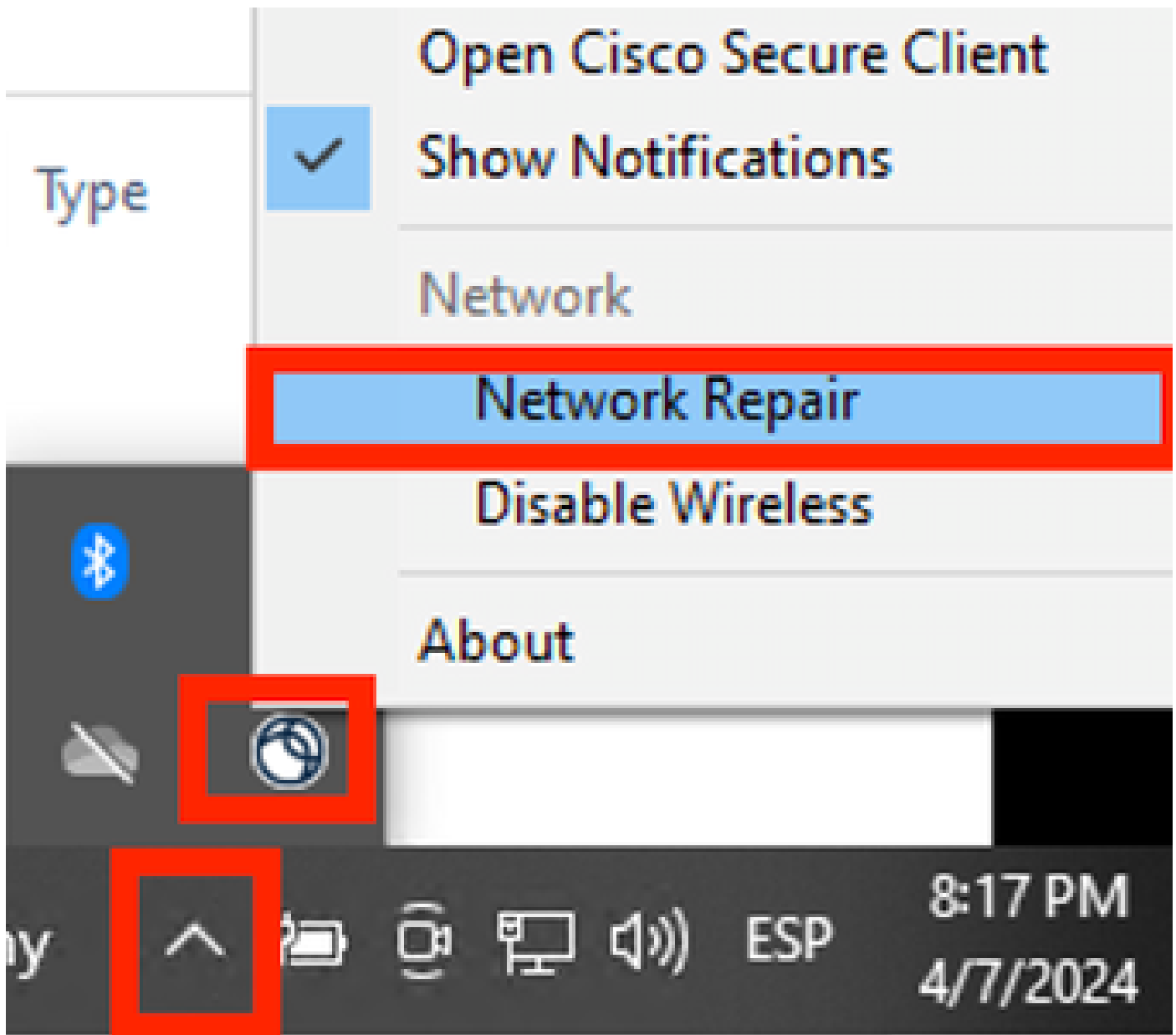
Como você pode ver que ele atinge as políticas corretas e o resultado é um status de autenticação bem-sucedido, conclui-se que a configuração está correta.

Troubleshooting

Problema: o perfil NAM não é usado pelo Secure Client.

Se o novo perfil criado no editor de perfis não for usado pelo NAM, use a opção Network Repair para o Secure Client.

Você pode encontrar essa opção navegando até a Barra do Windows > Clicando no ícone circunflex > Clique com o botão direito do mouse no ícone Secure Client > Clique em Network Repair.



Seção de Reparo de Rede

Problema 2: Os registros precisam ser coletados para análise posterior.

1. Habilitar log estendido do NAM

Abra o NAM e clique no ícone de engrenagem.



Interface NAM

Navegue até a guia Log Settings. Marque a caixa de seleção Enable Extended Logging.

Defina Packet Capture File Size como 100 MB.



Network Access Manager Diagnostics

Configuration Log Settings Statistics Message History

Use extended logging to collect additional information about product operations.

Enable Extended Logging

IHV:

Filter Driver:

Credential Provider

Packet Capture

Maximum Packet Capture File Size (MB):

Configurações de log NAM de cliente seguro

2. Reproduza o problema.

Quando o registro estendido estiver ativado, reproduza o problema várias vezes para garantir que os registros sejam gerados e o tráfego seja capturado.

3. Colete o pacote Secure Client DART.

No Windows, navegue até a barra de pesquisa e digite Cisco Secure Client Diagnostics and Reporting Tool.



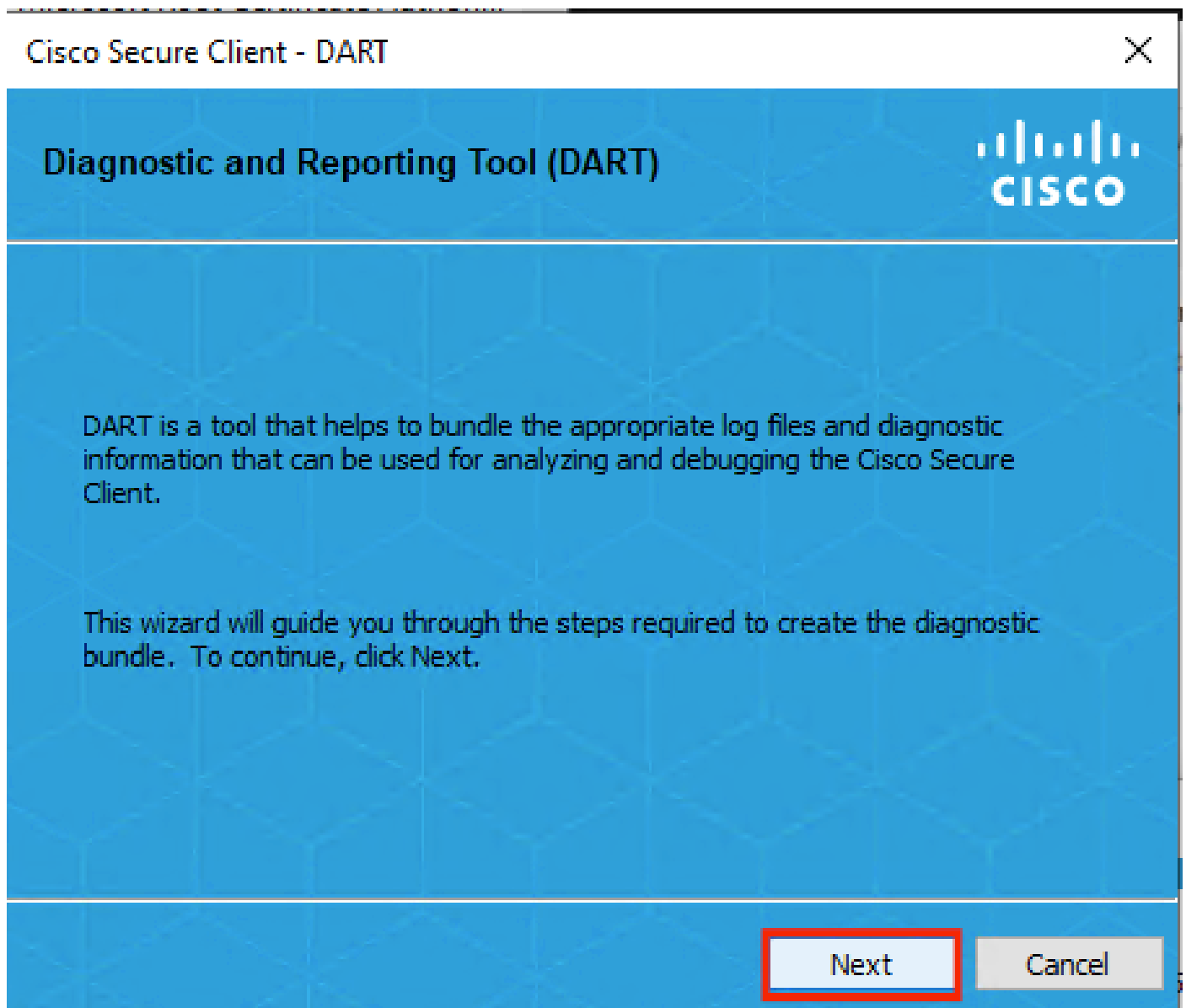
Cisco Secure Client Diagnostics and Reporting Tool

App

Módulo DART

Durante o processo de instalação, você também instalou este módulo. É uma ferramenta que ajuda durante o processo de solução de problemas, coletando registros e informações relevantes sobre a sessão dot1x.

Clique em Avançar na primeira janela.




Módulo DART

Clique novamente em Avançar para que o pacote de log possa ser salvo na área de trabalho.

Cisco Secure Client - DART




Bundle Creation Option 

Select "Default" to include the typical log files and diagnostic information in the bundle. Select "Custom" to choose the list of log files and diagnostic information to be included in the bundle.

Default - Bundle will be saved to Desktop

Custom

 DART requires administrative privileges to clear Cisco Secure Client logs.

[Clear All Logs](#)

[Back](#) [Next](#) [Cancel](#)

Módulo DART

Se necessário, marque a caixa de seleção Enable Bundle Encryption.

Bundle Encryption Option



Enable Bundle Encryption

Mask Password

Encryption Password

Confirm Password

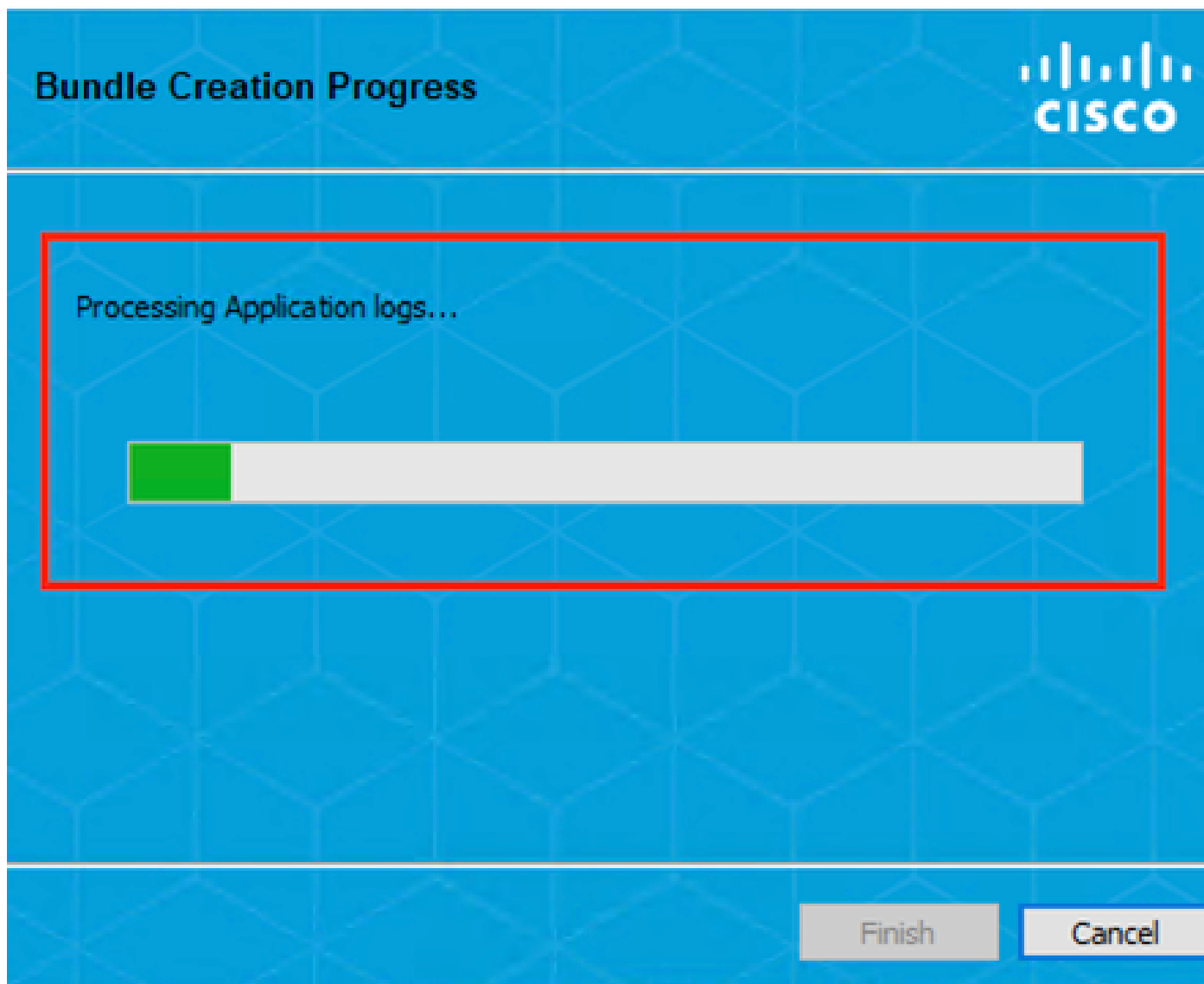
Back

Next

Cancel

Módulo DART

A coleta de logs do DART é iniciada.



Coleta de logs do DART

Pode levar 10 minutos ou mais até que o processo seja concluído.

Bundle Creation Result




The bundle was created successfully in C:\Users\LAB5\Desktop\DARTBundle_0423_1538.zip.

[Email Bundle](#)[Finish](#)

Resultado da criação do pacote DART

O arquivo de resultado do DART pode ser encontrado no diretório da área de trabalho.

| Name | Date modified | Type |
|--|-------------------|----------------------------|
|  DARTBundle_0423_1538 | 4/24/2024 1:14 PM | Compressed (zipped) Folder |

Arquivo de resultado do DART

Informações Relacionadas

- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.