Configurar a autenticação de máquina e usuário com EAP-TTLS

Contents

Introdução

Este documento descreve como configurar a autenticação de máquina e usuário com EAP-TTLS (EAP-MSCHAPv2) no Secure Client NAM e no Cisco ISE.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos antes de prosseguir com esta implantação:

- Cisco Identity Services Engine (ISE)
- Módulo de Análise de Rede de Cliente Seguro (NAM)
- Protocolos EAP

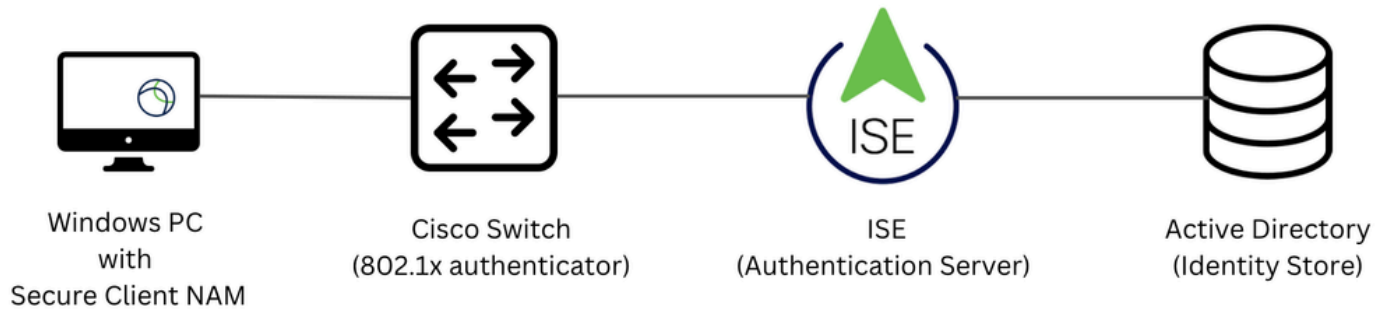
Componentes Utilizados

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

- Identity Services Engine (ISE) versão 3.4
- Switch C9300 com software Cisco IOS® XE, versão 16.12.01
- Windows 10 Pro Versão 22H2 Construído 19045.3930

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.

Topologia de rede



Topologia de rede

Configurar

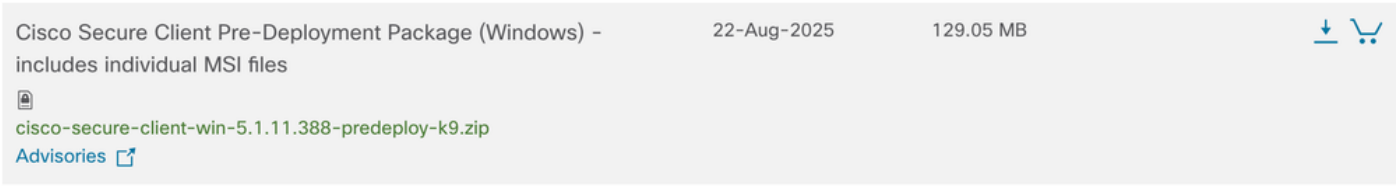
Configurações

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

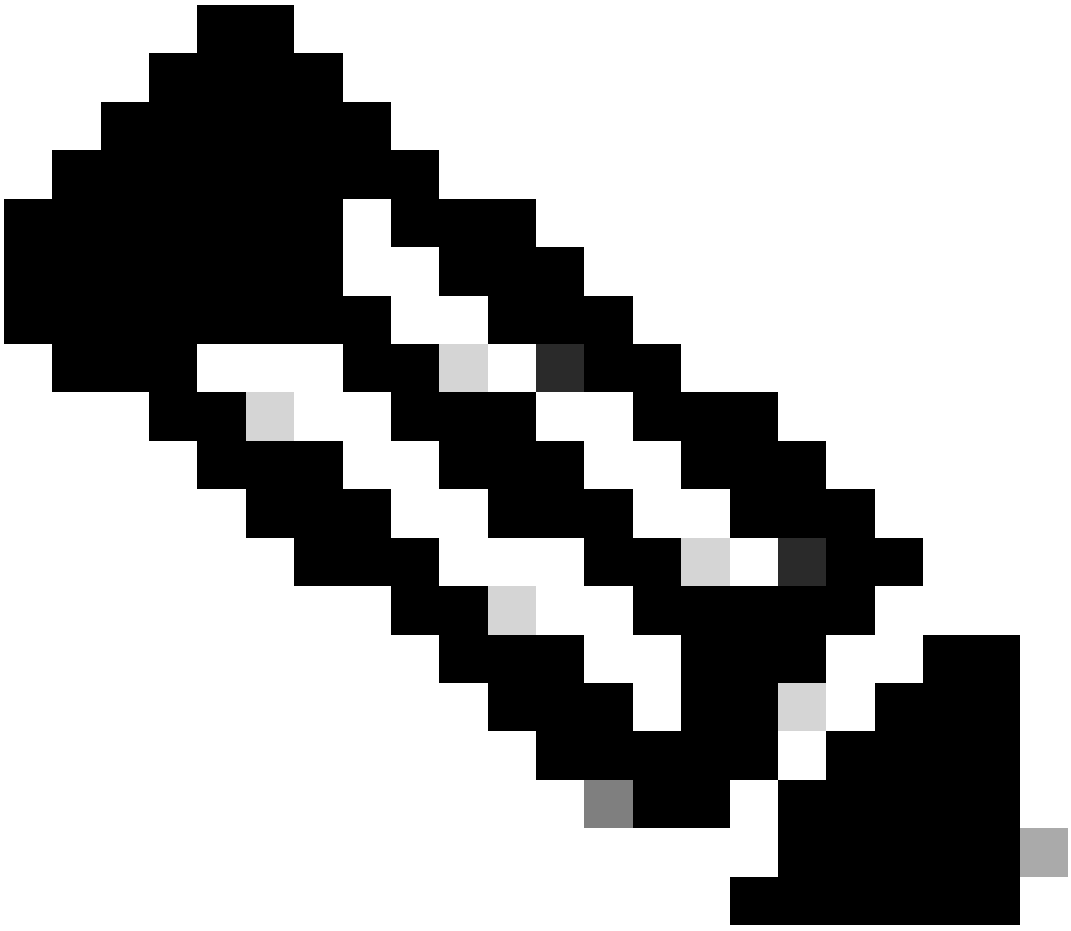
Etapa 1. Vá para Download do Software Cisco. Na barra de pesquisa de produtos, digite Secure Client 5.

Este exemplo de configuração usa a versão 5.1.11.388. A instalação é executada usando o método de pré-implantação.

Na página de download, localize e baixe o Cisco Secure Client Pre-Deployment Package (Windows).

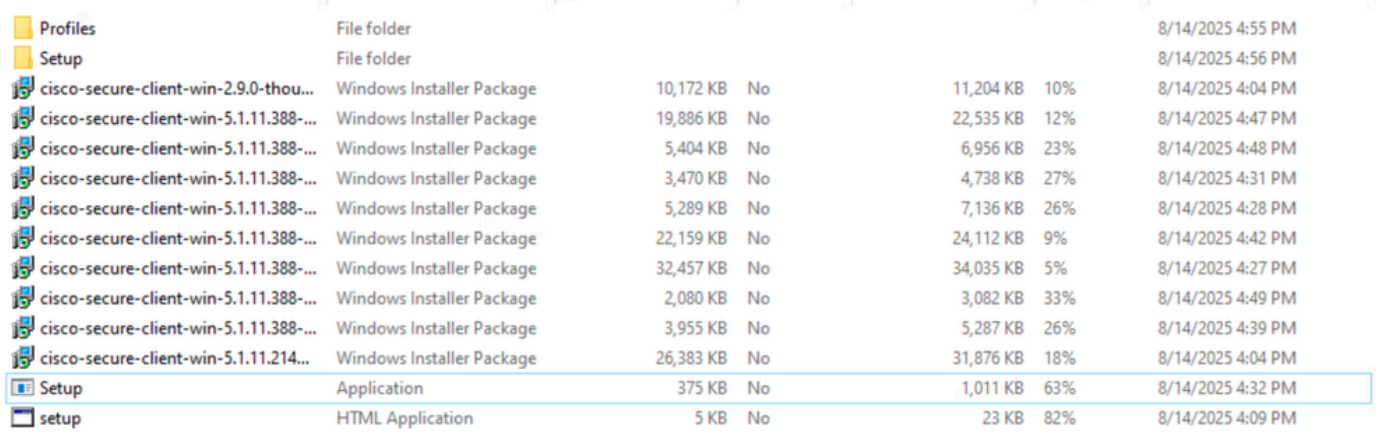


Arquivo zip de pré-implantação



> Note: O Cisco AnyConnect foi preterido e não está mais disponível no site de download de software da Cisco.

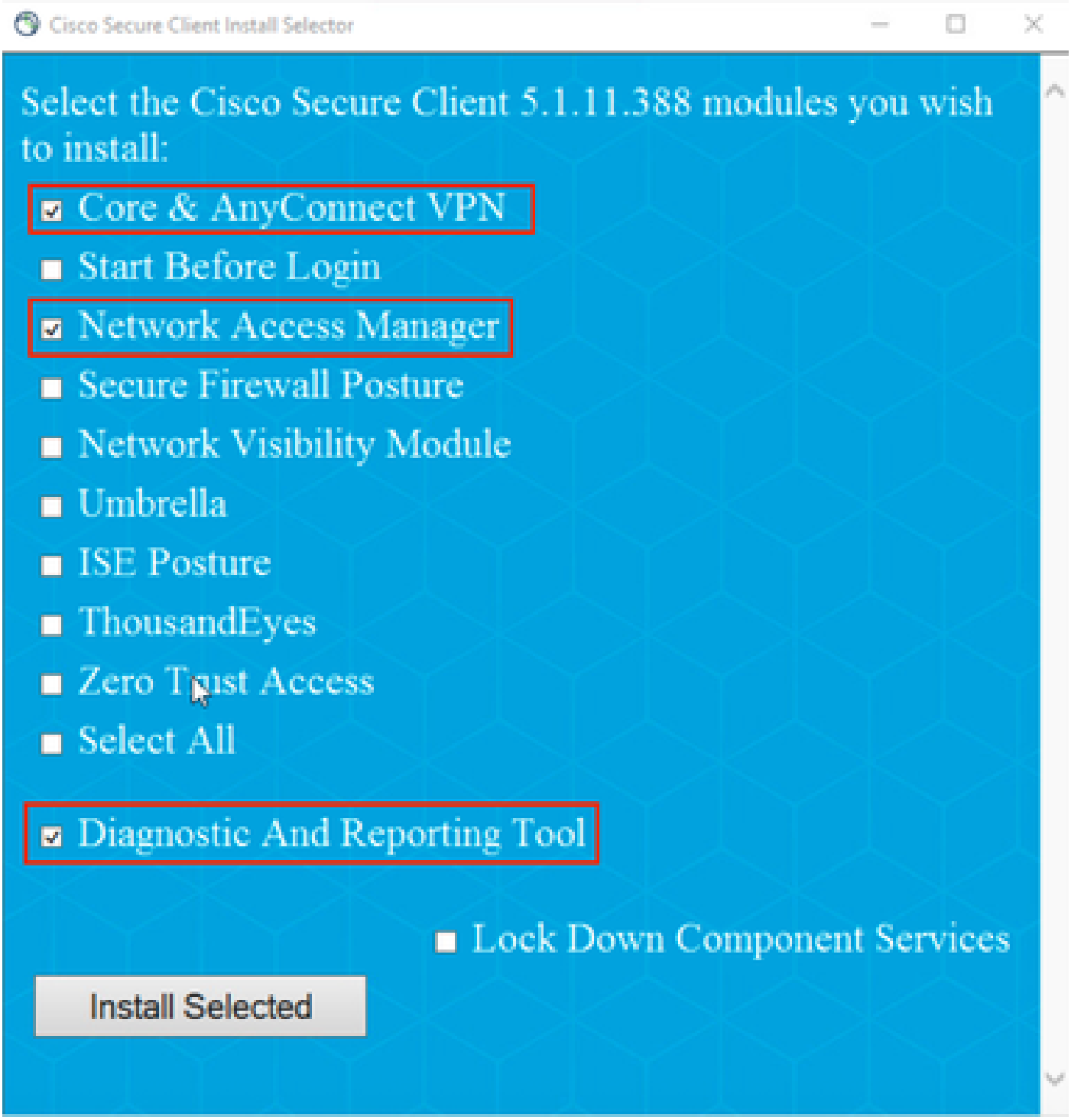
Etapa 2. Depois de fazer o download e extrair o arquivo, clique emSetup.



Profiles	File folder					8/14/2025 4:55 PM
Setup	File folder					8/14/2025 4:56 PM
cisco-secure-client-win-2.9.0-thou...	Windows Installer Package	10,172 KB	No	11,204 KB	10%	8/14/2025 4:04 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	19,886 KB	No	22,535 KB	12%	8/14/2025 4:47 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	5,404 KB	No	6,956 KB	23%	8/14/2025 4:48 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	3,470 KB	No	4,738 KB	27%	8/14/2025 4:31 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	5,289 KB	No	7,136 KB	26%	8/14/2025 4:28 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	22,159 KB	No	24,112 KB	9%	8/14/2025 4:42 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	32,457 KB	No	34,035 KB	5%	8/14/2025 4:27 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	2,080 KB	No	3,082 KB	33%	8/14/2025 4:49 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	3,955 KB	No	5,287 KB	26%	8/14/2025 4:39 PM
cisco-secure-client-win-5.1.11.214...	Windows Installer Package	26,383 KB	No	31,876 KB	18%	8/14/2025 4:04 PM
Setup	Application	375 KB	No	1,011 KB	63%	8/14/2025 4:32 PM
setup	HTML Application	5 KB	No	23 KB	82%	8/14/2025 4:09 PM

Arquivo Zip Pré-Implantação

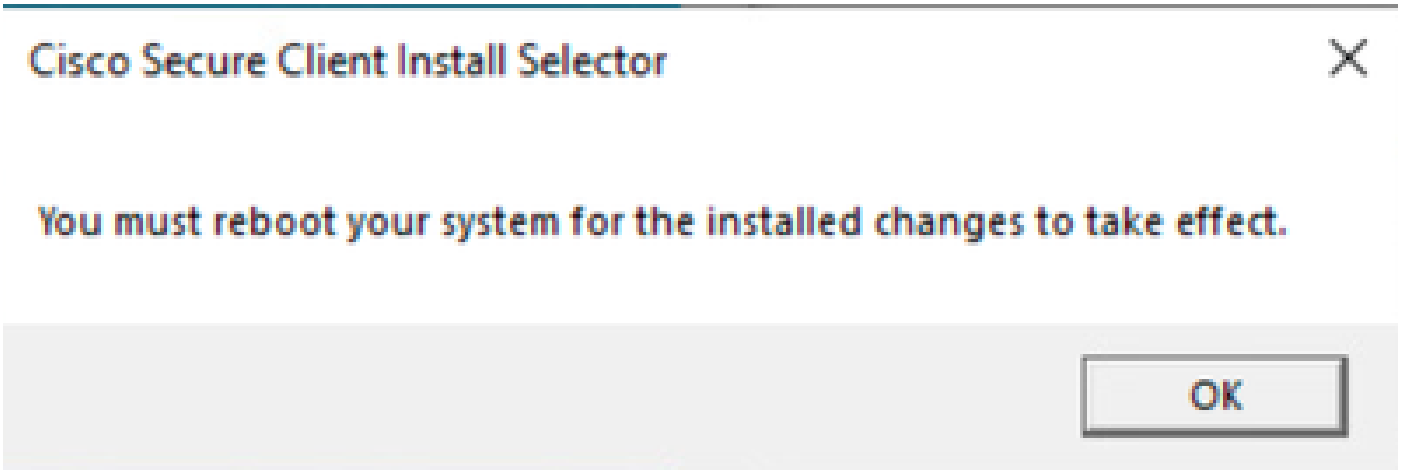
Etapa 3. Instale oCore & AnyConnect VPN, o Network Access Manager e os módulos Diagnostics and Reporting.



Instalador de cliente seguro

Clique em Instalar selecionado.

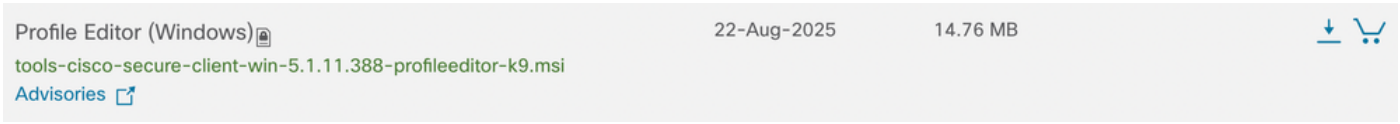
Etapa 4. Uma reinicialização é necessária após a instalação. Clique em OK e reinicie o dispositivo.



Pop-up Reinicialização Necessária

Parte 2: Baixe e instale o Secure Client NAM Profile Editor

Etapa 1. O Editor de Perfis pode ser encontrado na mesma página de downloads que o Cliente Seguro. Este exemplo de configuração usa a versão 5.1.11.388.



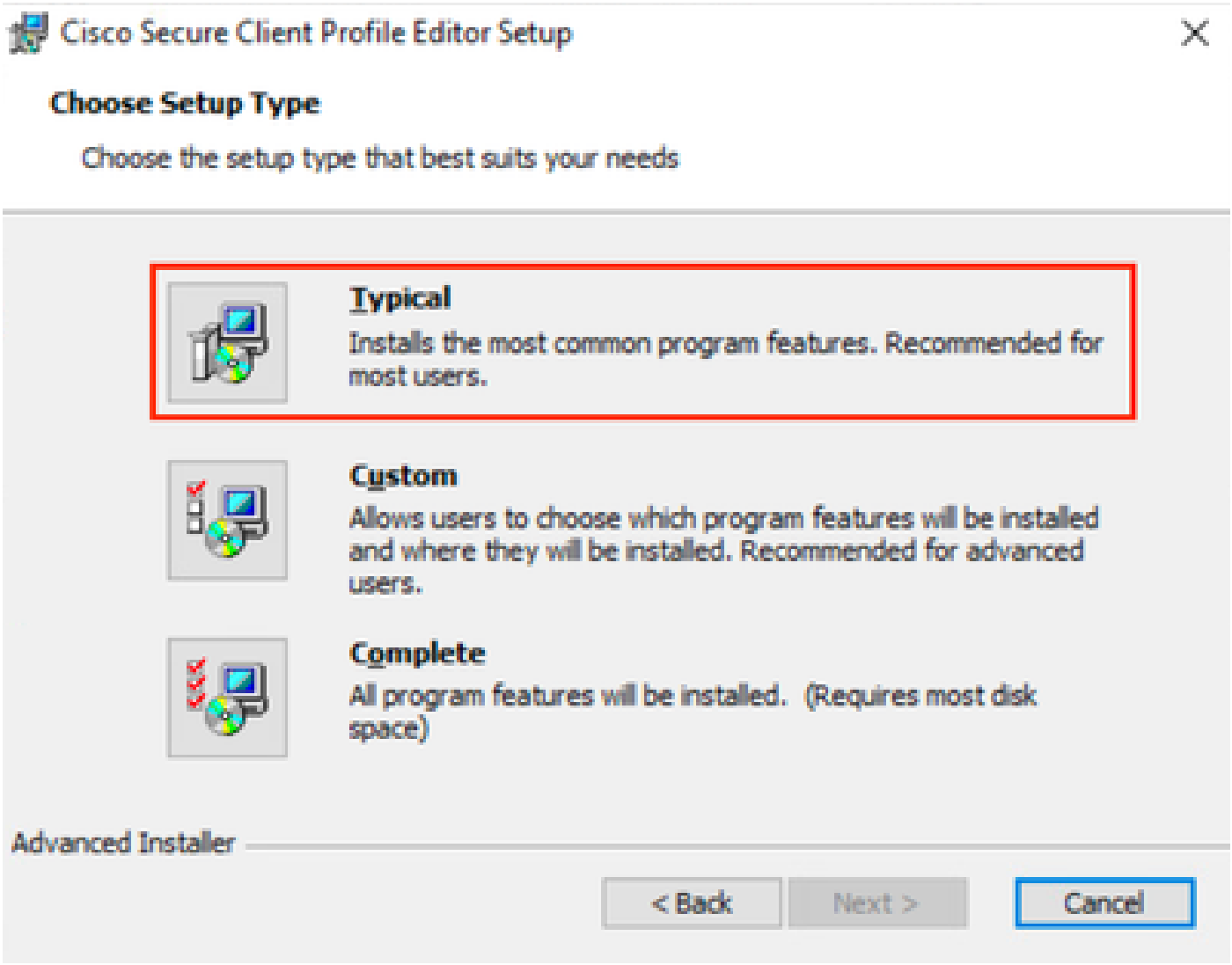
Editor de perfis

Baixe e instale o Editor de perfis.

Etapa 2. Execute o arquivo MSI.

Início da Instalação do Editor de Perfis

Etapa 3. Use a opção de configuração Typical e instale o NAM Profile Editor.

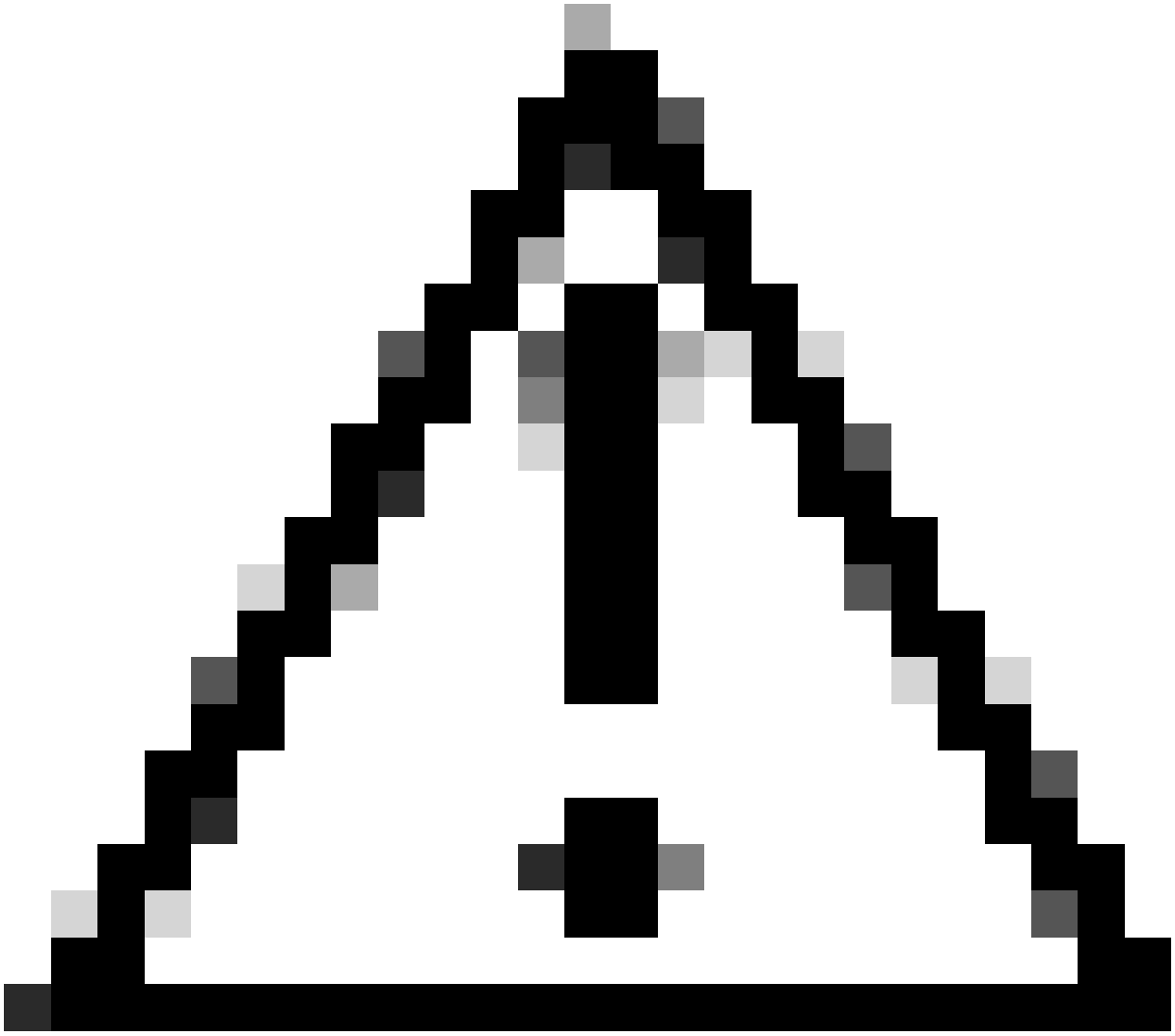


Configuração do Editor de perfis

Parte 3: Permitir que as Credenciais de Cache do Windows sejam Acessadas pelo NAM

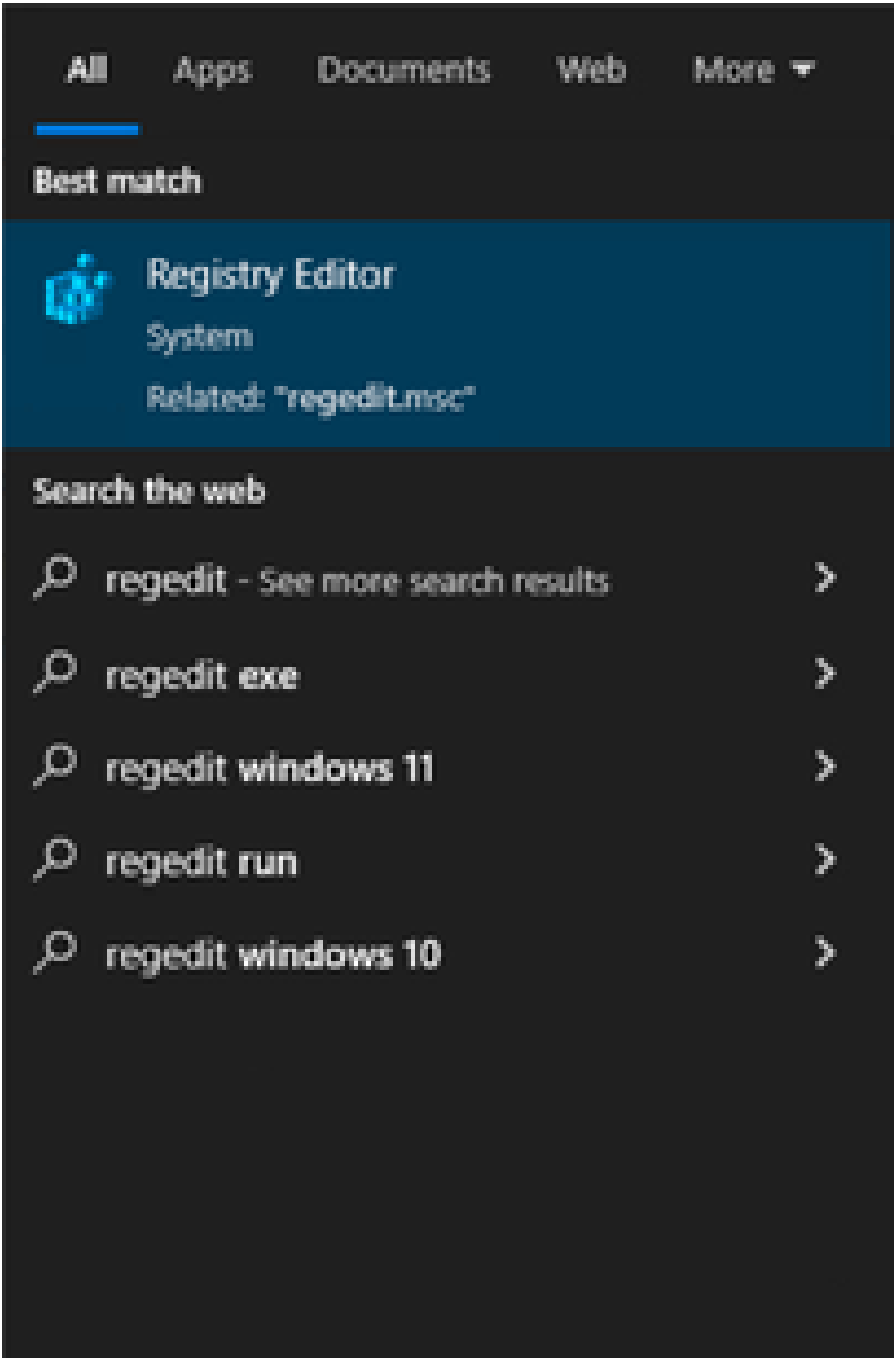
Por padrão, no Windows 10, no Windows 11 e no Windows Server 2012, o sistema operacional impede que o Network Access Manager (NAM) recupere a senha da máquina necessária para a autenticação da máquina. Como resultado, a autenticação da máquina usando a senha da máquina não funciona a menos que uma correção de registro seja aplicada.

Para permitir que o NAM acesse as credenciais da máquina, aplique a correção Microsoft KB 2743127 na área de trabalho do cliente.



Caution: A edição incorreta do Registro do Windows pode causar problemas sérios. Certifique-se de fazer backup do registro antes de fazer alterações.

Etapa 1. Na barra de pesquisa do Windows, digite regedit e clique em Editor do Registro.

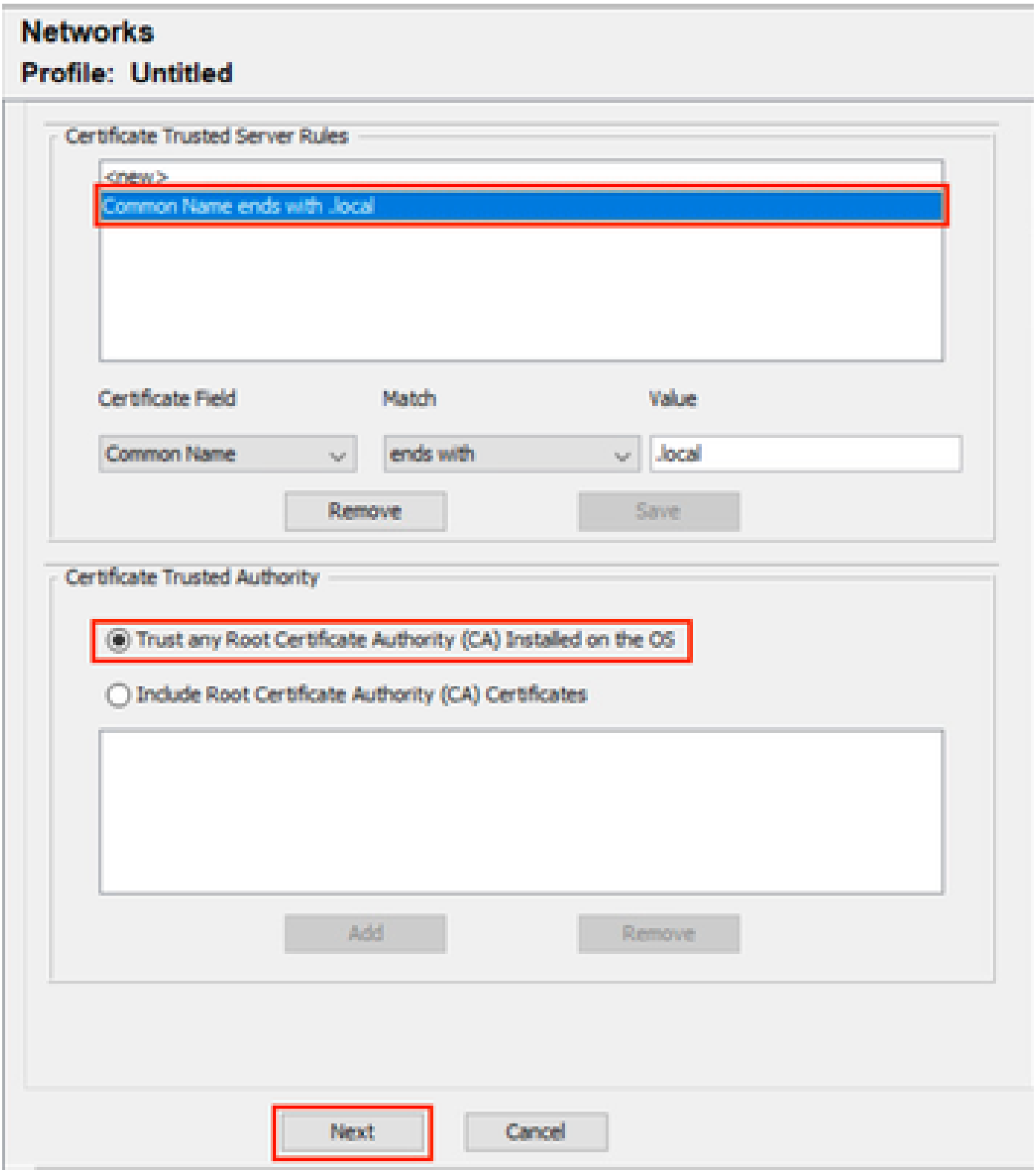

All
Apps
Documents
Web
More
Best match
Registry Editor
System
Related: "regedit.msc"
Search the web
regedit - See more search results
regedit exe
regedit windows 11
regedit run
regedit windows 10

Neste exemplo, o certificado do nó PSN é emitido por varshaah.varshaah.local. Assim, a regra Nome comum termina com .local é usada. Esta regra valida o certificado que o servidor apresenta durante o fluxo EAP-TTLS.

Você também pode especificar o nome comum do certificado de autenticação EAP do Policy Service Node (PSN).

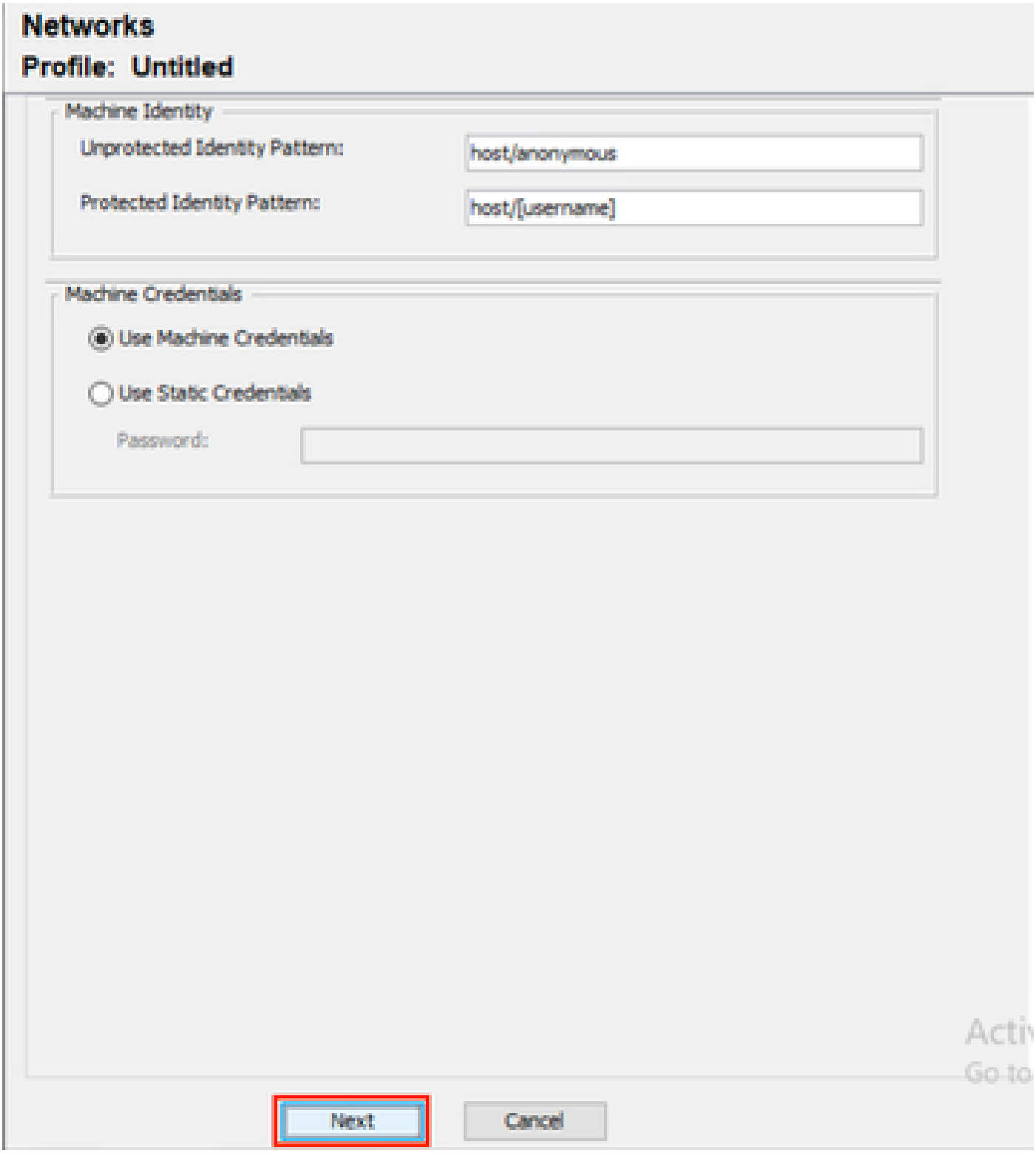
- Em Certificate Trusted Authority, duas opções estão disponíveis.
  Neste cenário, a opção Trust any Root Certificate Authority (CA) instalada no SO é usada em vez de adicionar um certificado CA específico.

  Com esta opção, o dispositivo Windows confia em qualquer certificado EAP assinado por um certificado incluído em Certificados - Usuário atual > Autoridades de Certificação Raiz Confiáveis > Certificados (gerenciado pelo sistema operacional).
- Clique em Avançar para continuar.



Certificados do Editor de Perfis do NAM

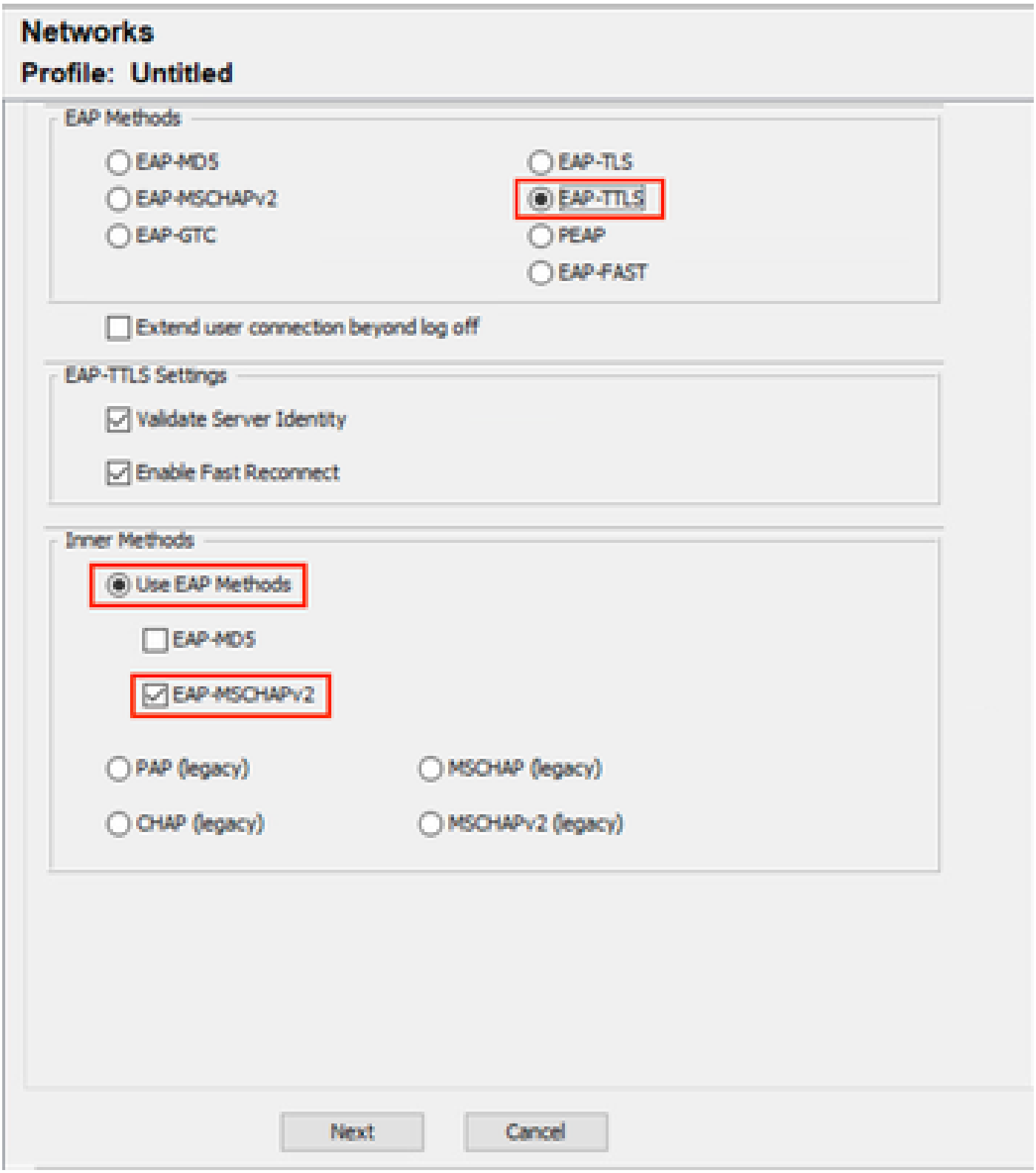
Etapa 6. Na seção Credenciais da máquina, selecione Usar credenciais da máquina e clique em Avançar.



Credenciais do Editor de Perfis do NAM

Etapa 7. Configure a seção User Auth.

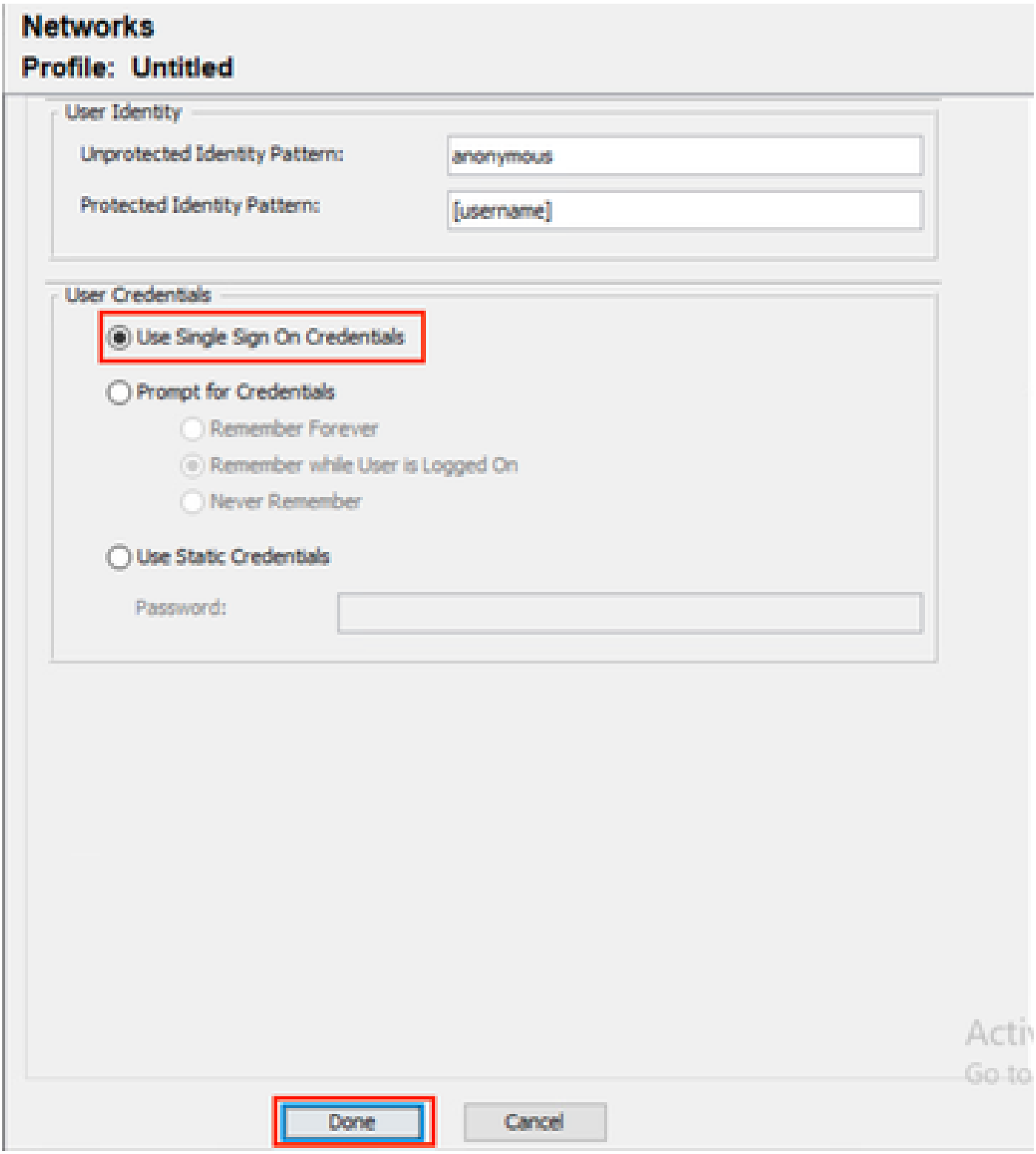
- Selecione EAP-TTLS em Métodos EAP.
- Em Inner Methods, selecione Use EAP Methods e selecione EAP-MSCHAPv2.
- Clique em Next.



Autenticação de Usuário do Editor de Perfil NAM

Etapa 8. Em Certificados, configure as mesmas regras de validação de certificado descritas na Etapa 5.

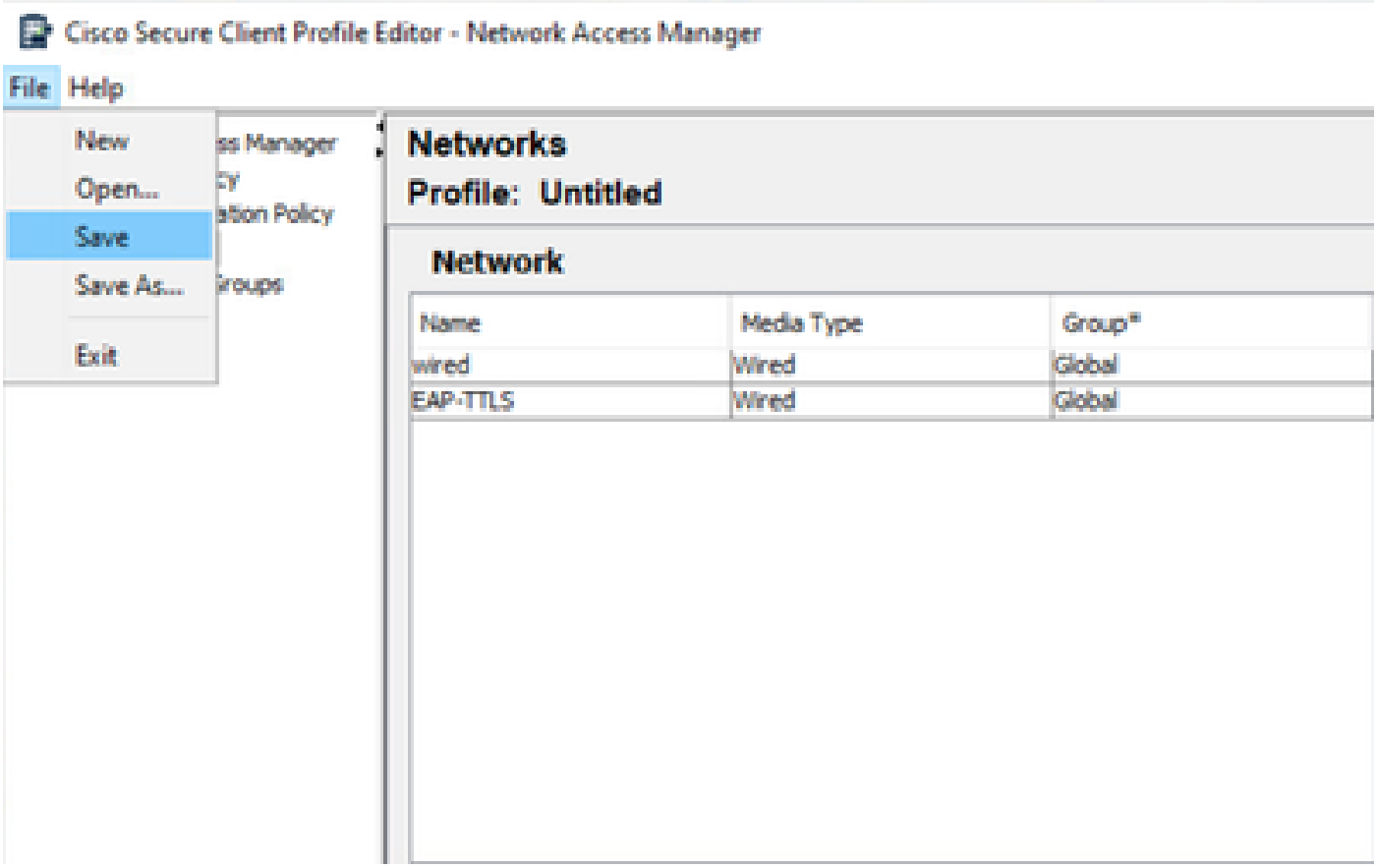
Etapa 9. Em Credenciais do Usuário, selecione Usar Credenciais do Signon Único e clique em Concluído.



Credenciais do usuário do Editor de perfis do NAM

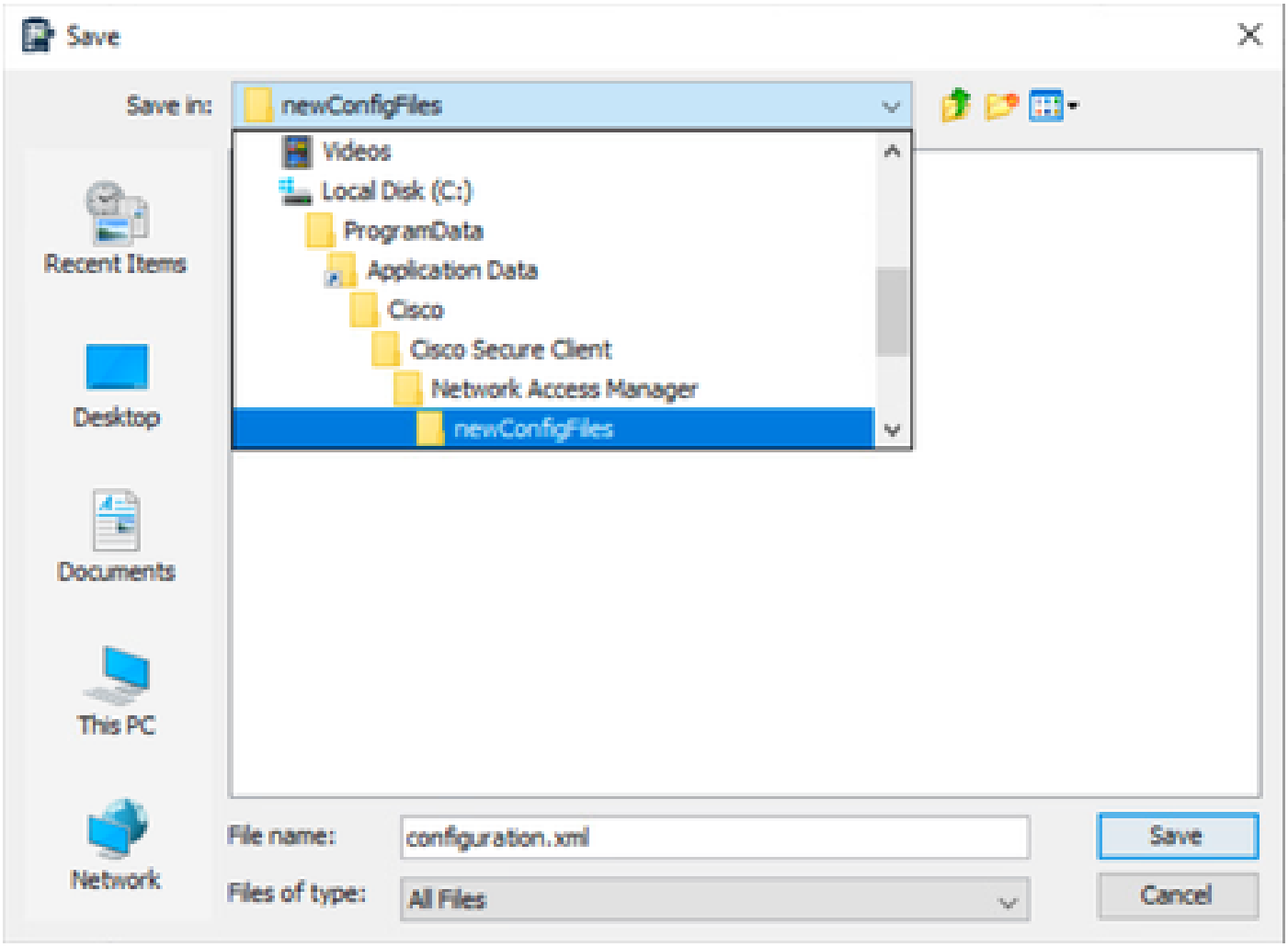
Parte 6: Salvar o arquivo de configuração de rede

Etapa 1. Clique em Arquivo > Salvar.



NAM Profile Editor Salvar Configuração de Rede

Etapa 2. Salve o arquivo como configuration.xml na pasta newConfigFiles.

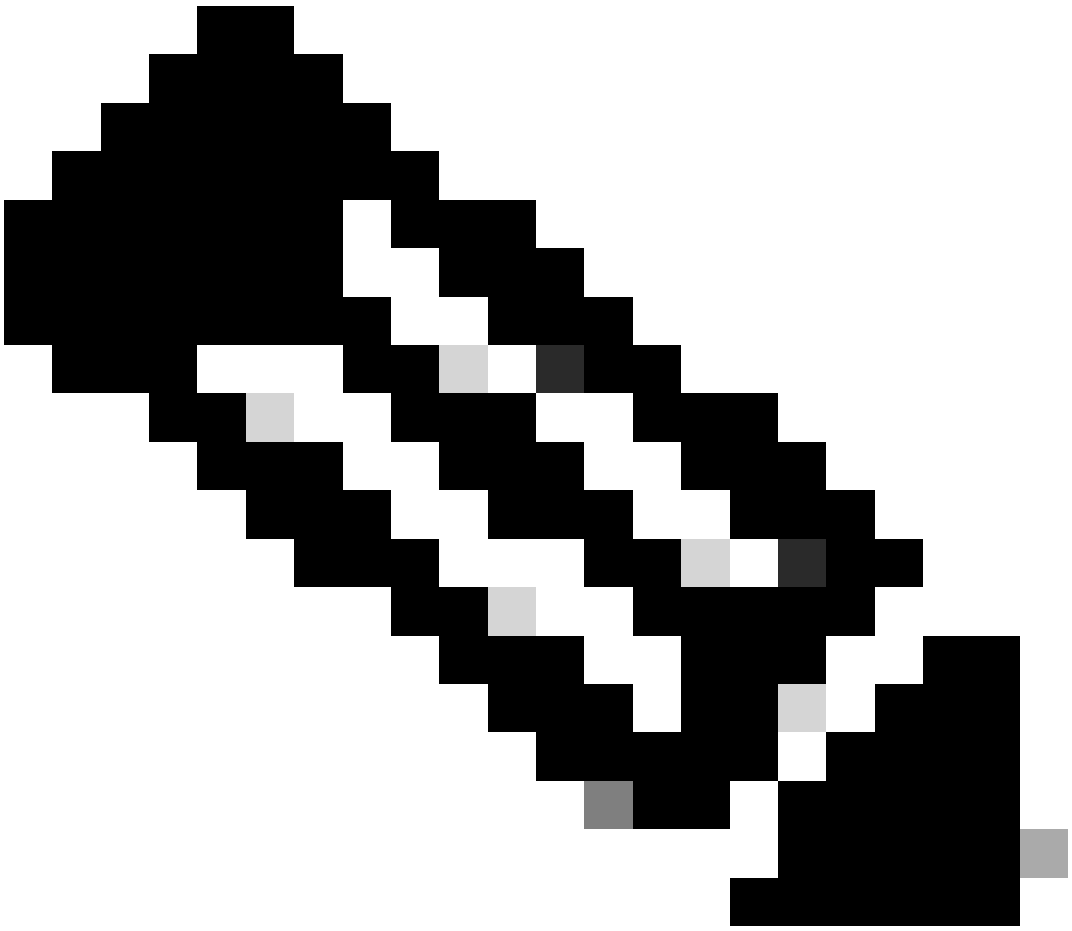


Salve a configuração de rede

Parte 7: Configurar AAA no Switch

```
C9300-1#sh run aaa
!
aaa authentication dot1x default group labgroup
aaa authorization network default group labgroup
aaa accounting dot1x default start-stop group labgroup
aaa accounting update newinfo periodic 2880
!
!
!
!
aaa server radius dynamic-author
 client 10.76.112.135 server-key cisco
!
!
radius server labserver
 address ipv4 10.76.112.135 auth-port 1812 acct-port 1813
 key cisco
!
!
aaa group server radius labgroup
 server name labserver
!
```

```
!
!
!
aaa new-model
aaa session-id common
!
!



C9300-1(config)#dot1x system-auth-control
```



Note: O comando dot1x system-auth-control não é exibido na saída show running-config, mas é necessário habilitar 802.1X globalmente.

Configure a interface do switch para 802.1X:

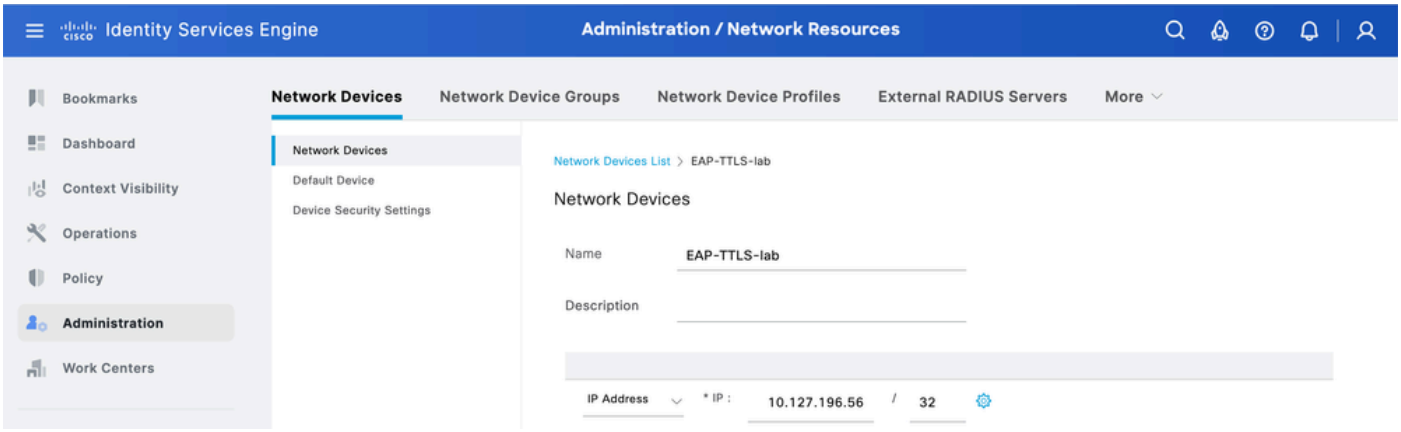
```
C9300-1(config)#do sh run int gig1/0/44
Building configuration...

Current configuration : 242 bytes
!
interface GigabitEthernet1/0/44
 switchport access vlan 96
 switchport mode access
 device-tracking
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication host-mode multi-auth
 authentication periodic

 mab
 dot1x pae authenticator
end
```

Parte 8: Configurações do ISE

Etapa 1. Configurar o switch no ISE.

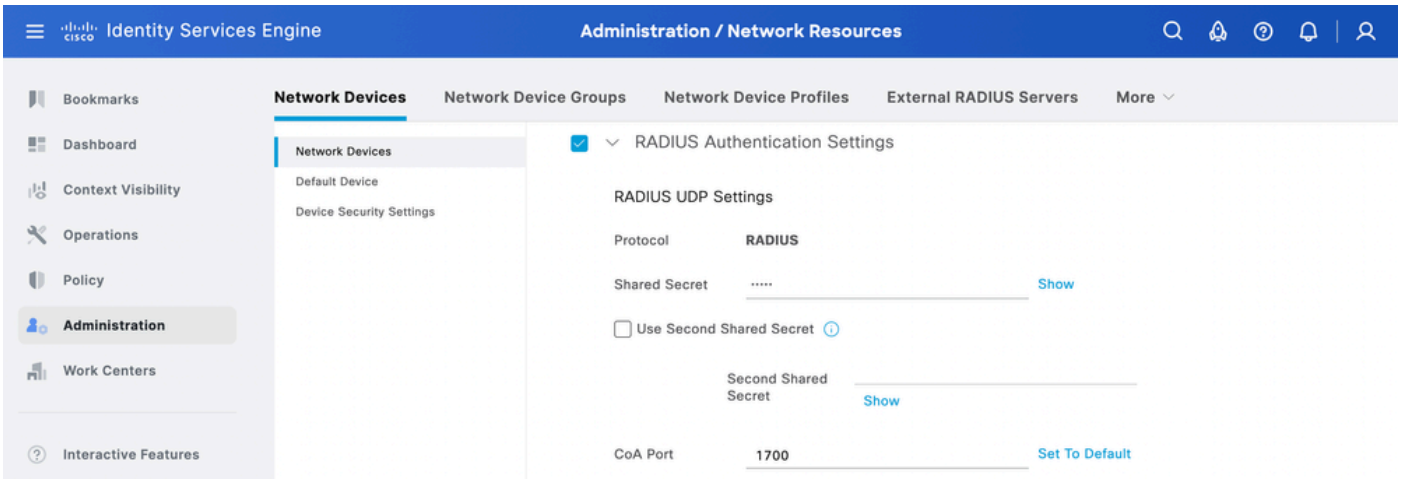
Navegue até Administration > Network Resources > Network Devices e clique em Add.

Digite aqui o nome do switch e o endereço IP.



Adicionando o dispositivo de rede ISE

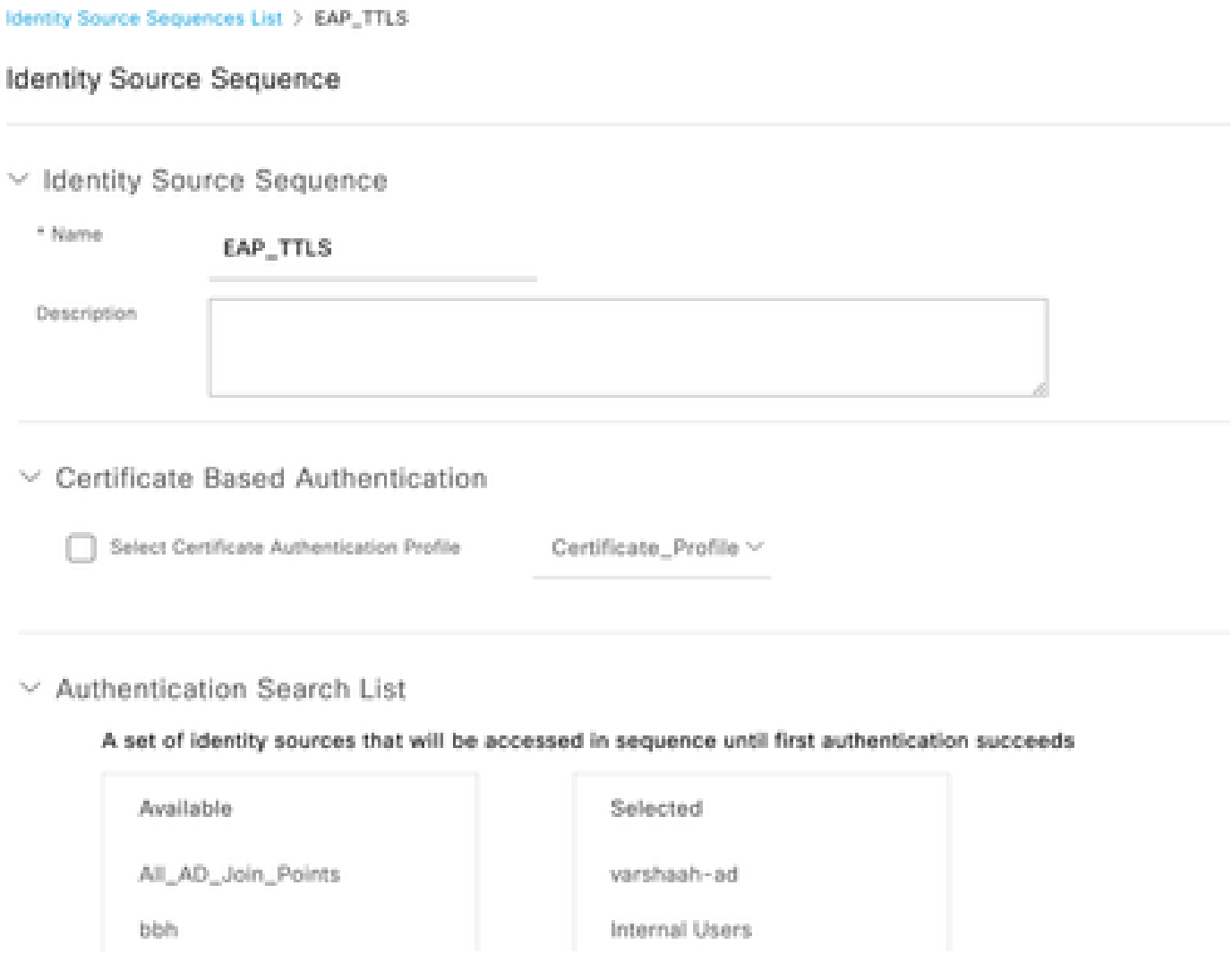
Insira o segredo compartilhado RADIUS, o mesmo que o configurado anteriormente no switch.



ISE de segredo compartilhado RADIUS

Etapa 2. Configurar a sequência de origem da identidade.

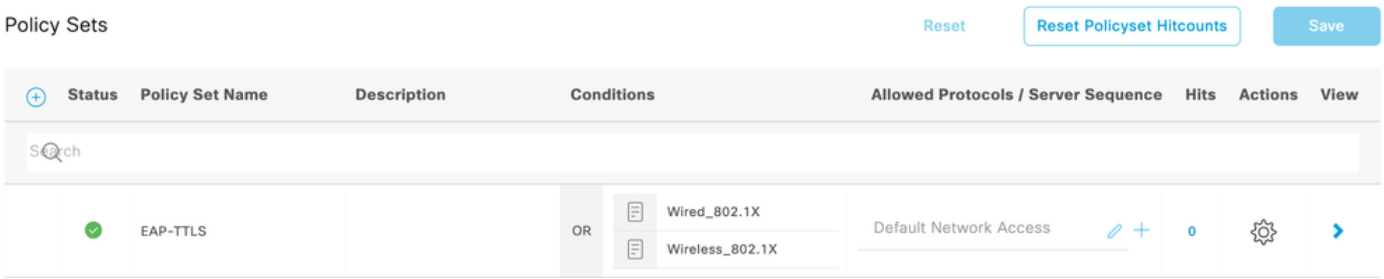
- Navegue até Administração > Gerenciamento de identidades > Sequências de origem de identidade.
- Clique em Adicionar para criar uma nova sequência de origem de identidade.
- Configure as fontes de identidade em Authentication Search List.



Sequência de origem de identidade do ISE

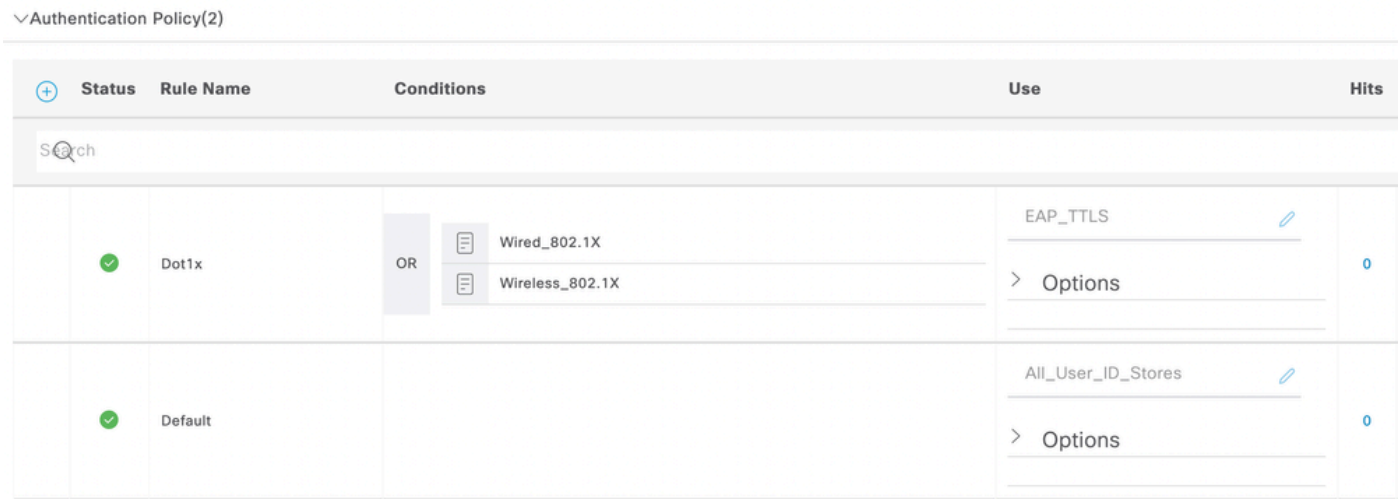
Etapa 3. Configurar o conjunto de políticas.

Navegue para Política > Conjuntos de políticas e crie um novo conjunto de políticas. Configure as condições como Wired_802.1x OU Wireless_802.1x. Para protocolos permitidos, escolha Default Network Access:



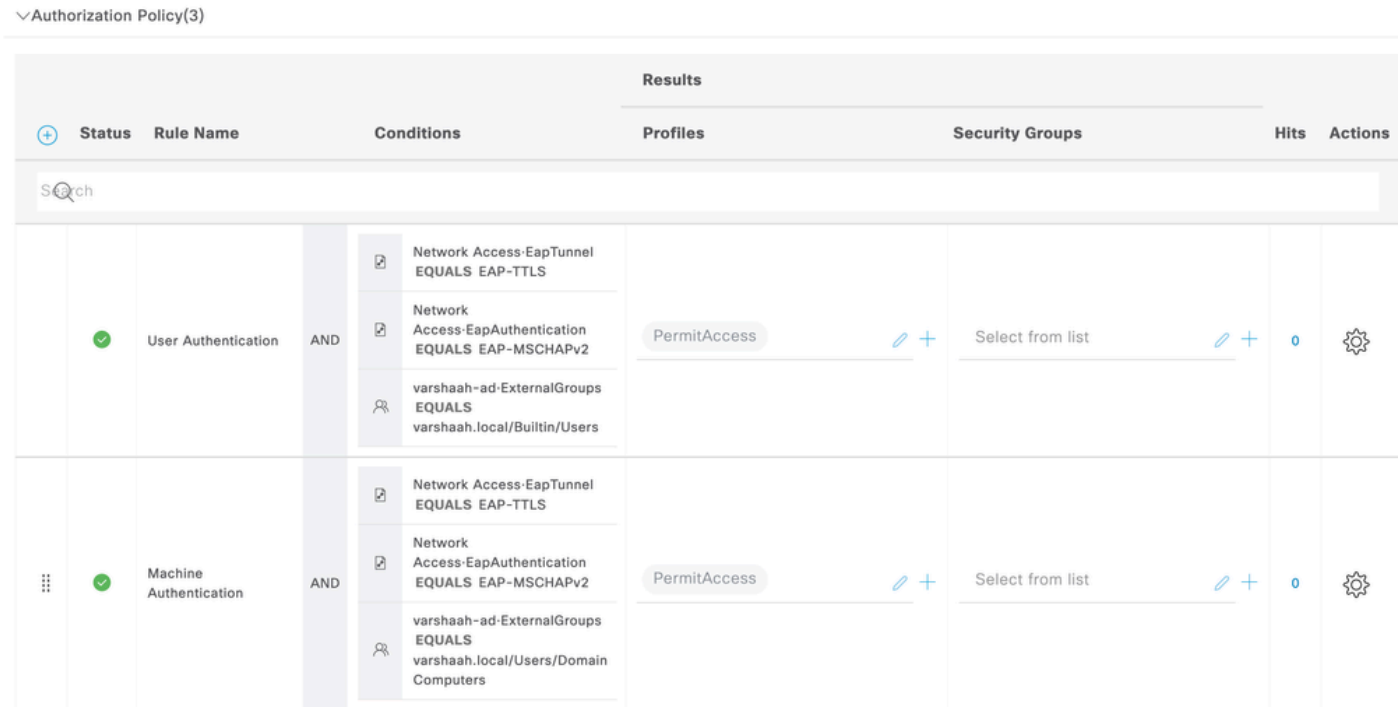
Conjunto de políticas EAP-TTLS

Crie a política de autenticação para dot1x e escolha a sequência de origem de identidade criada na Etapa 4.



Política de autenticação EAP-TTLS

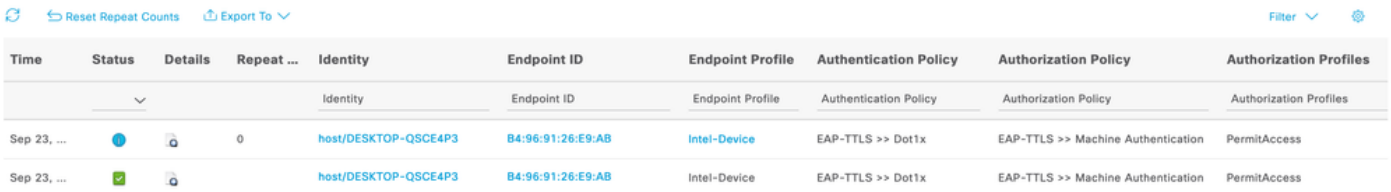
Para a política de autorização, crie a regra com três condições. A primeira condição verifica a condição de que o túnel EAP-TTLS seja usado. A segunda condição verifica se EAP-MSCHAPv2 é usado como o método EAP interno. A terceira condição verifica o respectivo grupo AD.



Política de Autorização Dot1x

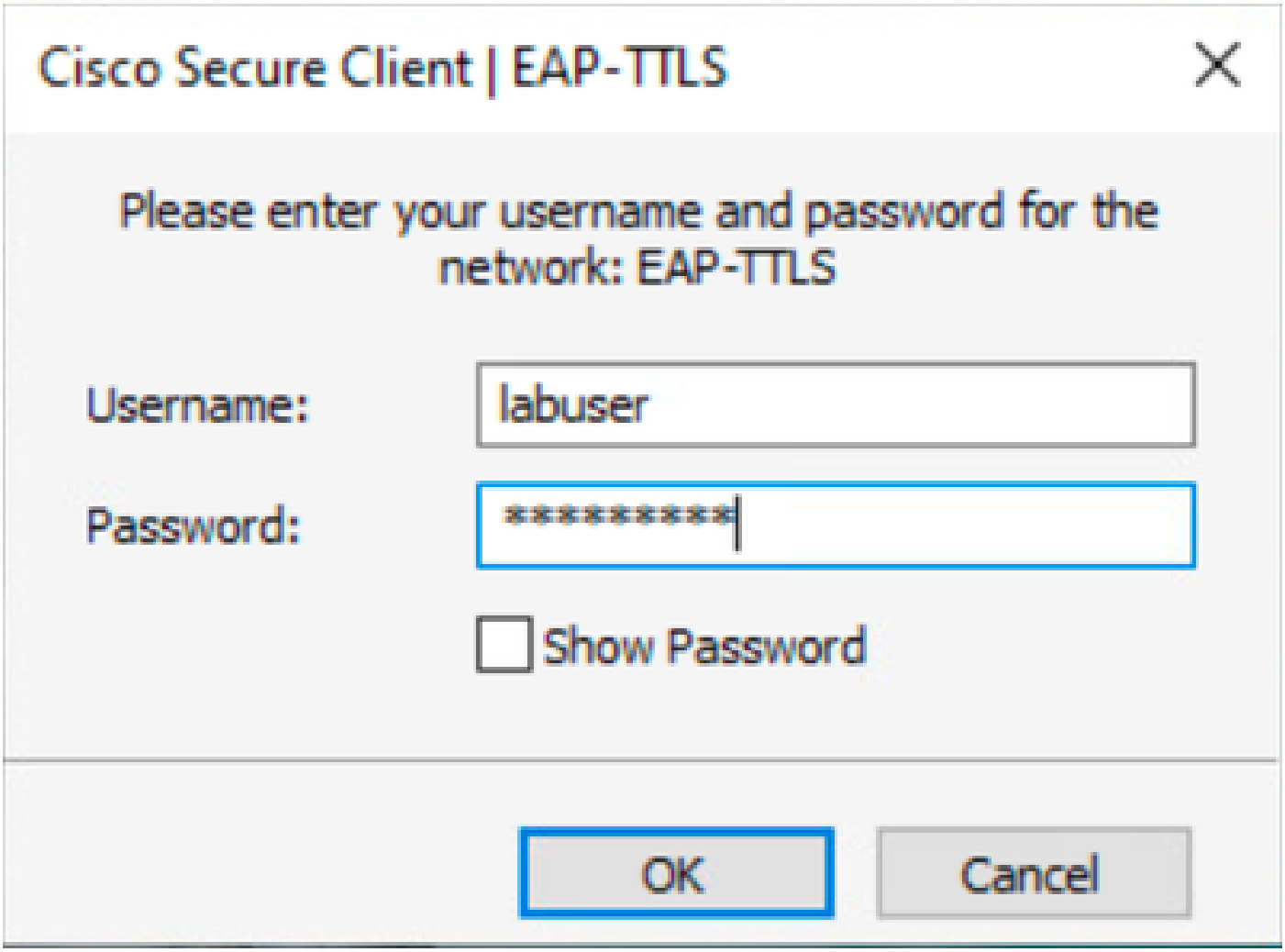
Verificar

Você pode reinicializar a máquina com o Windows 10 ou sair e entrar. Sempre que a tela de login do Windows é exibida, a autenticação da máquina é acionada.

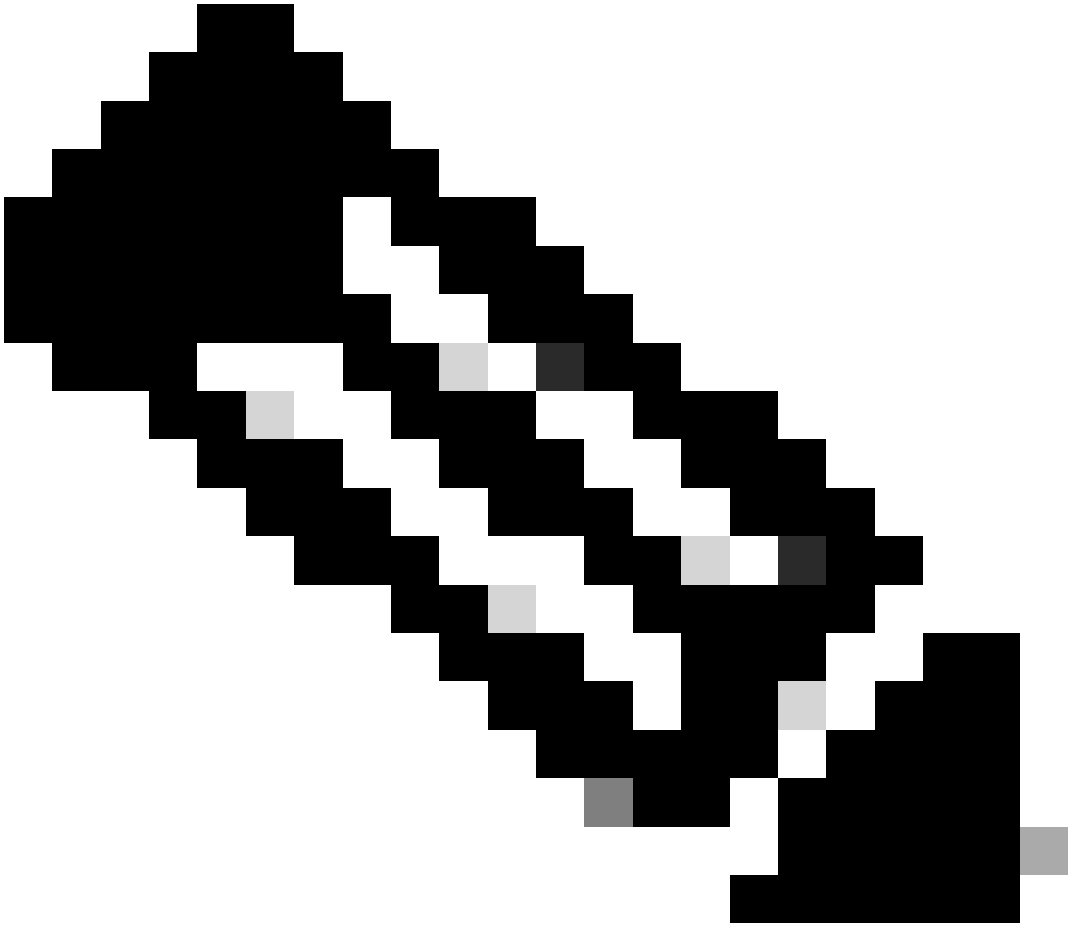


Autenticação do Computador de Log ao Vivo

Quando você faz login no PC com credenciais, a autenticação do usuário é acionada.

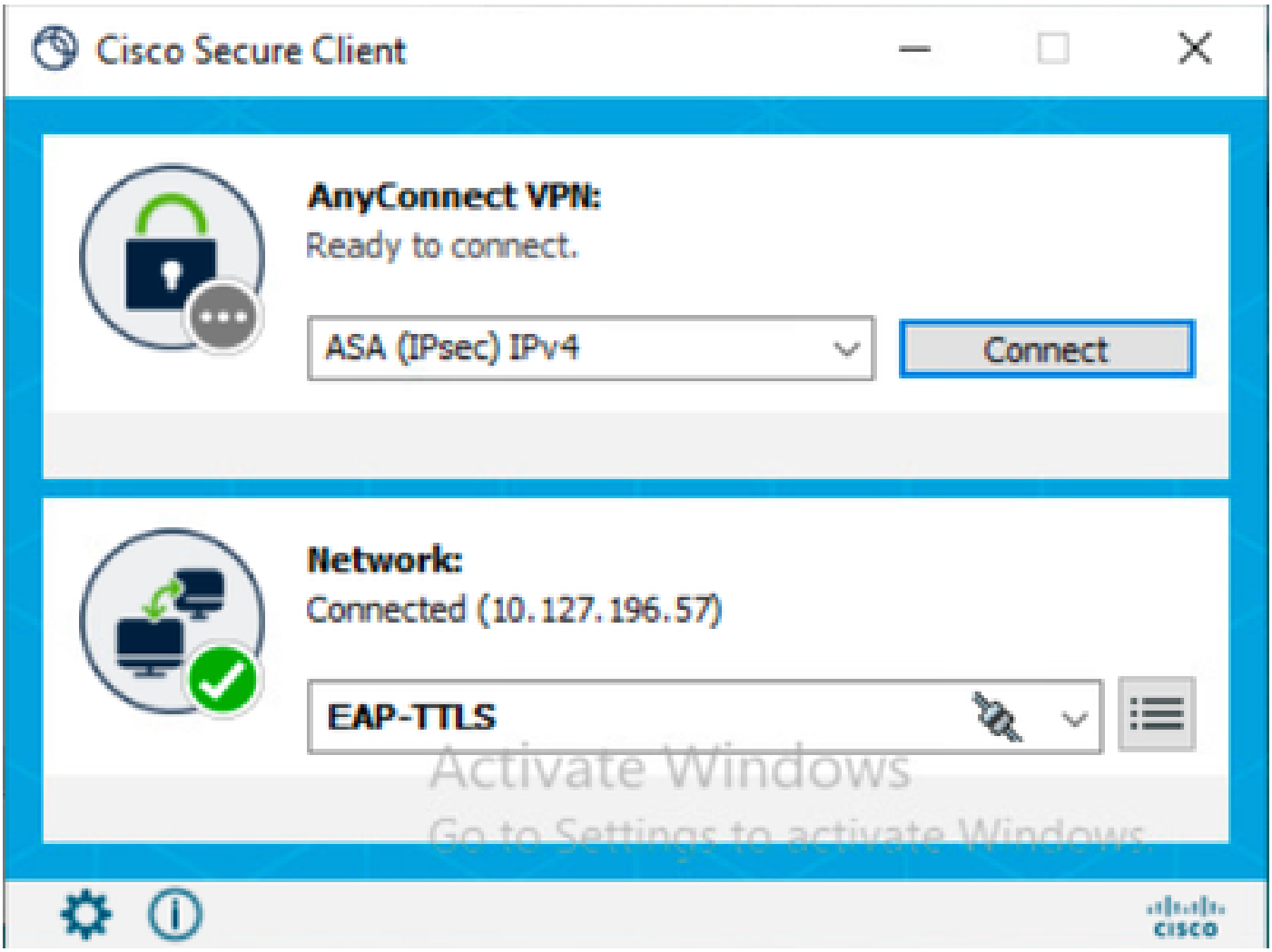


Credenciais de Autenticação de Usuário

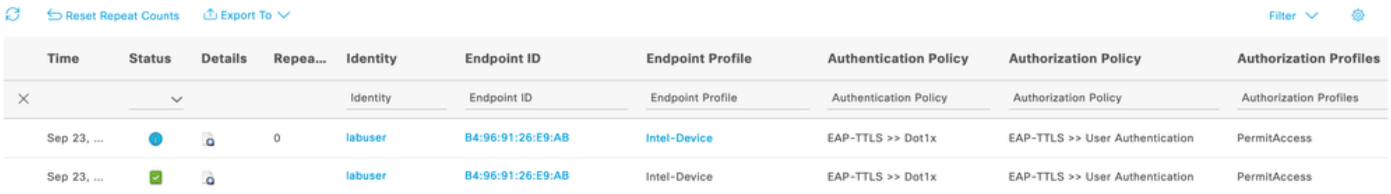


Note: Este exemplo usa credenciais de usuário do Ative Diretory para autenticação. Como alternativa, você pode criar um usuário interno no Cisco ISE e usar essas credenciais para fazer login.

Depois que as credenciais são inseridas e verificadas com êxito, o ponto final é conectado à rede com autenticação de usuário.



EAP-TTLS conectado



Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles
Sep 23, ...			0	labuser	B4:96:91:26:E9:AB	Intel-Device	EAP-TTLS >> Dot1x	EAP-TTLS >> User Authentication	PermitAccess
Sep 23, ...				labuser	B4:96:91:26:E9:AB	Intel-Device	EAP-TTLS >> Dot1x	EAP-TTLS >> User Authentication	PermitAccess

Autenticação de Usuário do Log ao Vivo

Analisar registros em tempo real do ISE RADIUS

Esta seção ilustra as entradas de log ao vivo do RADIUS para autenticação bem-sucedida de máquina e usuário.

Autenticação da máquina

11001 Received RADIUS Access-Request 11017 RADIUS created a new session ... ... 11507 Extracted EAP-Response/Identity **12983 Prepared EAP-Request proposing EAP-TTLS with challenge** ... ... **12978 Extracted EAP-Response containing EAP-TTLS challenge-response and accepting EAP-TTLS as negotiated** 12800 Extracted first TLS record; TLS handshake started 12805 Extracted TLS ClientHello message 12806 Prepared TLS ServerHello message 12807 Prepared TLS Certificate message 12808 Prepared TLS ServerKeyExchange message 12810 Prepared TLS ServerDone message ... ... 12803 Extracted TLS ChangeCipherSpec message 12804 Extracted TLS Finished message

12801 Prepared TLS ChangeCipherSpec message 12802 Prepared TLS Finished message **12816 TLS handshake succeeded** ... ... **11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge** 12985 Prepared EAP-Request with another EAP-TTLS challenge 11006 Returned RADIUS Access-Challenge 11001 Received RADIUS Access-Request ... ... 12971 Extracted EAP-Response containing EAP-TTLS challenge-response **11808 Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated** ... ... 24431 Authenticating machine against Active Directory - varshaah-ad 24325 Resolving identity - host/DESKTOP-QSCE4P3 ... ... 24343 RPC Logon request succeeded - DESKTOP-QSCE4P3$@varshaah.local **24470 Machine authentication against Active Directory is successful - varshaah-ad** 22037 Authentication Passed ... ... 12971 Extracted EAP-Response containing EAP-TTLS challenge-response 11810 Extracted EAP-Response for inner method containing MSCHAP challenge-response 11814 Inner EAP-MSCHAP authentication succeeded 11519 Prepared EAP-Success for inner EAP method **12975 EAP-TTLS authentication succeeded** ... ... 15036 Evaluating Authorization Policy 24209 Looking up Endpoint in Internal Endpoints IDStore - host/DESKTOP-QSCE4P3 24211 Found Endpoint in Internal Endpoints IDStore 15048 Queried PIP - Network Access.Device IP Address 15048 Queried PIP - Network Access.EapTunnel **15016 Selected Authorization Profile - PermitAccess** ... ... 11002 Returned RADIUS Access-Accept

Autenticação de usuário

11001 Received RADIUS Access-Request 11017 RADIUS created a new session ... ... 11507 Extracted EAP-Response/Identity **12983 Prepared EAP-Request proposing EAP-TTLS with challenge** ... ... **12978 Extracted EAP-Response containing EAP-TTLS challenge-response and accepting EAP-TTLS as negotiated** 12800 Extracted first TLS record; TLS handshake started 12805 Extracted TLS ClientHello message 12806 Prepared TLS ServerHello message 12807 Prepared TLS Certificate message 12808 Prepared TLS ServerKeyExchange message 12810 Prepared TLS ServerDone message ... ... 12812 Extracted TLS ClientKeyExchange message 12803 Extracted TLS ChangeCipherSpec message 12804 Extracted TLS Finished message 12801 Prepared TLS ChangeCipherSpec message 12802 Prepared TLS Finished message **12816 TLS handshake succeeded** ... ... **11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge** 12985 Prepared EAP-Request with another EAP-TTLS challenge 11006 Returned RADIUS Access-Challenge 11001 Received RADIUS Access-Request ... ... 12971 Extracted EAP-Response containing EAP-TTLS challenge-response **11808 Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated** ... ... 24430 Authenticating user against Active Directory - varshaah-ad 24325 Resolving identity - labuser@varshaah.local ... ... 24343 RPC Logon request succeeded - labuser@varshaah.local **24402 User authentication against Active Directory succeeded - varshaah-ad** 22037 Authentication Passed ... ... 12971 Extracted EAP-Response containing EAP-TTLS challenge-response 11810 Extracted EAP-Response for inner method containing MSCHAP challenge-response 11814 Inner EAP-MSCHAP authentication succeeded 11519 Prepared EAP-Success for inner EAP method **12975 EAP-TTLS authentication succeeded** ... ... 15036 Evaluating Authorization Policy 24209 Looking up Endpoint in Internal Endpoints IDStore - labuser 24211 Found Endpoint in Internal Endpoints IDStore 15048 Queried PIP - Network Access.Device IP Address 15048 Queried PIP - Network Access.EapTunnel **15016 Selected Authorization Profile - PermitAccess** ... ... 11002 Returned RADIUS Access-Accept

Analisar registros NAM

Os logs do NAM, especialmente depois que você habilita o Log Estendido, contêm uma grande quantidade de dados, a maioria dos quais é irrelevante e pode ser ignorada. Esta seção lista as linhas de depuração para demonstrar cada etapa que o NAM executa para estabelecer uma conexão de rede. Quando você trabalha em um registro, essas frases-chave podem ser úteis para localizar parte do registro relevante para o problema.

Autenticação da máquina

```
2160: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11812][comp=SAE]: 80
```

O cliente recebe um pacote EAP-TTLS do switch de rede, iniciando a sessão EAP-TTLS. Este é o ponto de partida para o túnel de autenticação da máquina.

```
2171: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11812][comp=SAE]: EA
2172: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-6-INFO_MSG: %[tid=11812][comp=SAE]: CER
2173: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-6-INFO_MSG: %[tid=11812][comp=SAE]: CER
```

O cliente recebe o Server Hello do ISE e começa a validar o certificado do servidor (CN=varshaah.varshaah.local). O certificado foi encontrado no repositório de confiança do cliente e adicionado para validação.

```
2222: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-6-INFO_MSG: %[tid=11768]: Validating th
2223: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-6-INFO_MSG: %[tid=11768]: Server certif
```

O certificado do servidor foi validado com êxito, concluindo o estabelecimento do túnel TLS.

```
2563: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.789 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
2564: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.789 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11812][comp=SAE]: NE
2565: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.789 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
```

O cliente sinaliza que a autenticação foi aprovada. A interface é desbloqueada, e a máquina de estado interno faz a transição para USER_T_NOT_DISCONNECTED, indicando que a máquina agora pode transmitir tráfego.

```
2609: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
2610: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11824][comp=SAE]: NE
2611: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
2612: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11824][comp=SAE]: NE
2613: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
2614: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11824][comp=SAE]: NE
2615: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
```

O adaptador relata authenticated, e o NAM AccessStateMachine faz a transição para ACCESS_AUTHENTICATED. Isso confirma que a máquina concluiu com êxito a autenticação e tem acesso total à rede.

Autenticação de usuário

```
100: DESKTOP-QSCE4P3: Sep 25 2025 14:01:26.669 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9664]: Network EAP-TT
```

O cliente NAM inicia o processo de conexão EAP-TTLS.

```
195: DESKTOP-QSCE4P3: Sep 25 2025 15:09:11.780 +0900: %csc_nam-7-DEBUG_MSG: %[tid=3252]: Binding adapte
198: DESKTOP-QSCE4P3: Sep 25 2025 15:09:11.780 +0900: %csc_nam-7-DEBUG_MSG: %[tid=3252]: Network EAP-TT
```

O NAM vincula o adaptador físico à rede EAP-TTLS e entra no estado ACCESS_ATTACHED, confirmando que o adaptador está pronto para a autenticação.

```
204: DESKTOP-QSCE4P3: Sep 25 2025 15:09:11.780 +0900: %csc_nam-7-DEBUG_MSG: %[tid=3252]: Network EAP-TT
247: DESKTOP-QSCE4P3: Sep 25 2025 15:09:11.780 +0900: %csc_nam-7-DEBUG_MSG: %[tid=3680][comp=SAE]: STAT
```

O cliente faz a transição de ATTACHED para CONNECTING, iniciando a troca 802.1X.

```
291: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.388 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6644][comp=SAE]: 8021
```

O cliente envia um EAPOL-Start para disparar o processo de autenticação.

```
331: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.435 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6644][comp=SAE]: PORT
332: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.435 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6644][comp=SAE]: 8021
340: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.435 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6644][comp=SAE]: EAP
```

O switch solicita uma identidade e o cliente se prepara para responder com uma identidade externa.

```
402: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.685 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9580]: EAP-CB: creden
422: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.685 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6088]: EAP: processin
460: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.685 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6088]: EAP: credentia
```

O NAM envia a identidade externa. Por padrão, é anônimo, indicando que a troca é para autenticação de usuário (não máquina).

```
488: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.497 +0900: %csc_nam-6-INFO_MSG: %[tid=6088]: EAP: EAP sugges
```

```
489: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.497 +0900: %csc_nam-6-INFO_MSG: %[tid=6088]: EAP: EAP reques
490: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.497 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6088]: EAP: EAP metho
491: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.497 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6088]: EAP: credentia
```

O cliente e o servidor concordam em usar EAP-TTLS como o método externo.

```
660: DESKTOP-QSCE4P3: Sep 25 2025 14:01:27.185 +0900: %csc_nam-7-DEBUG_MSG: %[tid=8296][comp=SAE]: EAP
661: DESKTOP-QSCE4P3: Sep 25 2025 14:01:27.185 +0900: %csc_nam-7-DEBUG_MSG: %[tid=8296][comp=SAE]: EAP
```

O cliente envia o Hello do cliente e recebe o Hello do servidor, que inclui o certificado ISE.

```
706: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.967 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: 802
717: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.967 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EAP
718: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.967 +0900: %csc_nam-6-INFO_MSG: %[tid=11932][comp=SAE]: CERT
719: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.983 +0900: %csc_nam-6-INFO_MSG: %[tid=11932][comp=SAE]: CERT
726: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.983 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EAP
```

O certificado do servidor é apresentado. O cliente procura o CN varshaah.varshaah.local, encontra uma correspondência e valida o certificado. O handshake é pausado enquanto o certificado X.509 é verificado.

```
729: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.983 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EAP
730: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.983 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11916][comp=SAE]: EAP
1110: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.044 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9644]: Auth[EAP-TTLS
1111: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.044 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9644]: Auth[EAP-TTLS
```

O túnel está estabelecido. O NAM agora solicita e prepara a identidade protegida e as credenciais para autenticação interna.

```
1527: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.169 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11916][comp=SAE]: EA
1528: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.169 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11916][comp=SAE]: EA
1573: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.184 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EA
1574: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.184 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EA
1575: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.184 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EA
```

O handshake TLS é concluído. Um túnel seguro foi estabelecido para autenticação interna.

```
1616: DESKTOP-QSCE4P3: Sep 25 2025 14:01:46.262 +0900: %csc_nam-6-INFO_MSG: %[tid=9664]: Protected iden
1620: DESKTOP-QSCE4P3: Sep 25 2025 14:01:46.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9664]: Auth[EAP-TTLS
```

```
1689: DESKTOP-QSCE4P3: Sep 25 2025 14:01:46.277 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9664]: Auth[EAP-TTLS
```

A identidade protegida (nome de usuário) é enviada e aceita pelo ISE.

```
1708: DESKTOP-QSCE4P3: Sep 25 2025 14:01:46.277 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9456][comp=SAE]: EAP
1738: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.758 +0900: %csc_nam-6-INFO_MSG: %[tid=11768]: Protected pas
1741: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.200 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9644]: Auth[EAP-TTLS
```

O ISE solicita a senha. O NAM envia a senha protegida dentro do túnel TLS.

```
1851: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9644]: Auth[EAP-TTLS
1852: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: STA
1853: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9644]: Auth[EAP-TTLS
1854: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: STA
1855: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: STA
```

O ISE valida a senha, envia as transições EAP-Success e NAM para AUTHENTICATED. Neste ponto, a autenticação do usuário está concluída e o cliente tem permissão para acessar a rede.

Troubleshooting

Ao solucionar problemas do Network Access Manager (NAM) com o Cisco ISE e a integração do switch, os registros devem ser coletados de todos os três componentes: Secure Client (NAM), Cisco ISE e o switch.

Logs de cliente seguro (NAM)

1. Ative o log estendido do NAM seguindo estas etapas.
2. Reproduza o problema. Se o perfil de rede não se aplicar, execute o Reparo de Rede no Cliente Seguro.
3. Colete o pacote DART usando a ferramenta de diagnóstico e relatórios (DART).

Logs do Cisco ISE

Ative estas depurações no ISE para capturar a autenticação e as interações de diretório:

- runtime-AAA
- nsf
- nsf-session

Logs do switch

Depurações básicas

```
request platform software trace rotate all
set platform software trace smd switch active R0 radius debug
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 eap-all debug
debug radius all
```

Depurações avançadas (se necessário)

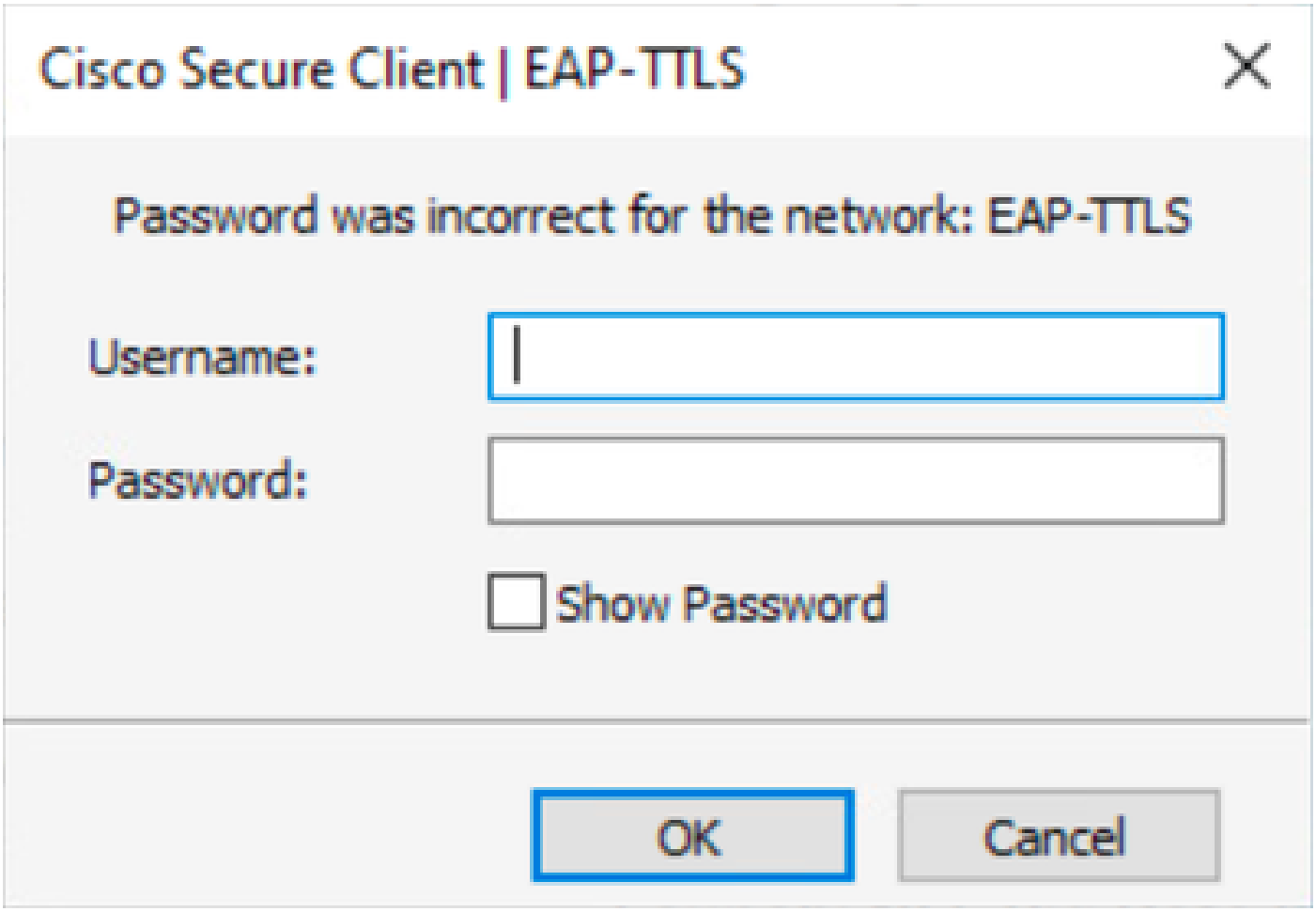
```
set platform software trace smd switch active R0 epm-all debug
set platform software trace smd switch active R0 pre-all debug
```

comandos show

```
show version
show debugging
show running-config aaa
show authentication session interface gix/x details
show dot1x interface gix/x
show aaa servers
show platform software trace message smd switch active R0
```

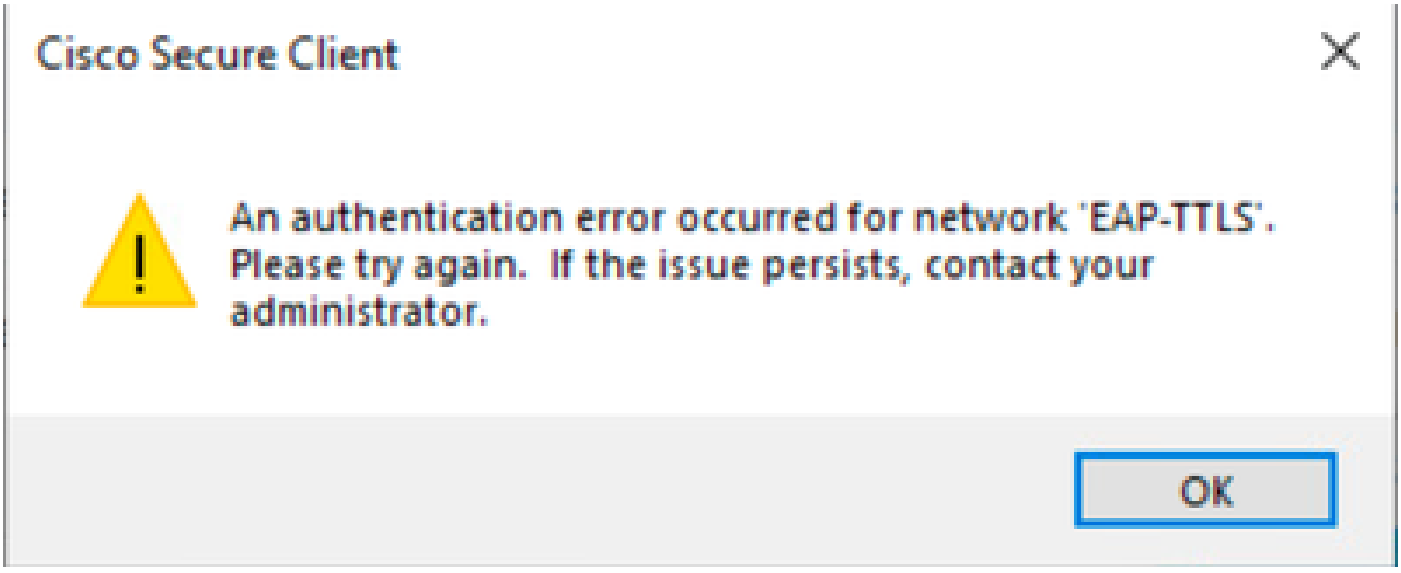
Falha de autenticação de usuário devido a credenciais inválidas

Quando um usuário insere credenciais incorretas, o Secure Client exibe uma senha genérica que estava incorreta para a rede: Mensagem EAP-TTLS. O erro na tela não especifica se o problema é devido a um nome de usuário ou senha inválidos.



Erro de Senha Incorreta

Se a autenticação falhar duas vezes consecutivas, o Secure Client exibirá esta mensagem: Ocorreu um erro de autenticação para a rede 'EAP-TTLS'. Tente novamente. Se o problema persistir, entre em contato com o administrador.



Problema de Autenticação de Usuário

Para identificar a causa, revise os logs do NAM.

1. Senha incorreta:

Quando um usuário digita uma senha incorreta, os registros do NAM mostram entradas semelhantes a esta saída:

```
3775: DESKTOP-QSCE4P3: Oct 02 2025 15:29:39.921 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11300][comp=SAE]: EA
3776: DESKTOP-QSCE4P3: Oct 02 2025 15:29:39.921 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11300][comp=SAE]: EA
3777: DESKTOP-QSCE4P3: Oct 02 2025 15:29:39.922 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11300][comp=SAE]: EA
```

Nos registros em tempo real do Cisco ISE, o evento correspondente aparece como:

Event	5400 Authentication failed
Failure Reason	24408 User authentication against Active Directory failed since user has entered the wrong password
Resolution	Check the user password credentials. If the RADIUS request is using PAP for authentication, also check the Shared Secret configured for the Network Device
Root cause	User authentication against Active Directory failed since user has entered the wrong password

Senha incorreta

11001 Received RADIUS Access-Request 11017 RADIUS created a new session ... ... 11507 Extracted EAP-Response/Identity 10 **12983 Prepared EAP-Request proposing EAP-TTLS with challenge** ... ... **12978 Extracted EAP-Response containing EAP-TTLS challenge-response and accepting EAP-TTLS as negotiated** 12800 Extracted first TLS record; TLS handshake started ... ... 12810 Prepared TLS ServerDone message ... ... 12812 Extracted TLS ClientKeyExchange message 12803 Extracted TLS ChangeCipherSpec message ... ... **12816 TLS handshake succeeded** ... ... **11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge 0** 12985 Prepared EAP-Request with another EAP-TTLS challenge 11006 Returned RADIUS Access-Challenge 0 11001 Received RADIUS Access-Request ... ... 12971 Extracted EAP-Response containing EAP-TTLS challenge-response 0 **11808 Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated** ... ... 15013 Selected Identity Source - varshaah-ad 0 24430 Authenticating user against Active Directory - varshaah-ad 0 24325 Resolving identity - labuser@varshaah.local 4 24313 Search for matching accounts at join point - varshaah.local 0 24319 Single matching account found in forest - varshaah.local 0 24323 Identity resolution detected single matching account 0 **24344 RPC Logon request failed - STATUS_WRONG_PASSWORD, ERROR_INVALID_PASSWORD, labuser@varshaah.local 20 24408 User authentication against Active Directory failed since user has entered the wrong password - varshaah-ad 1** ... ... 11823 EAP-MSCHAP authentication attempt failed ... ... 11815 Inner EAP-MSCHAP authentication failed 0 ... ... 12976 EAP-TTLS authentication failed 0 ... ... 11003 Returned RADIUS Access-Reject

2. Nome de usuário incorreto:

Quando um usuário insere um nome de usuário incorreto, os registros do NAM mostram entradas semelhantes a esta saída:

```
3788: DESKTOP-QSCE4P3: Oct 02 2025 15:29:39.923 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11300][comp=SAE]: EA
3789: DESKTOP-QSCE4P3: Oct 02 2025 15:29:39.923 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11300]: EAP-CB: EAP
```

Nos registros em tempo real do Cisco ISE, o evento correspondente aparece como:

Event	5400 Authentication failed
Failure Reason	22056 Subject not found in the applicable identity store(s)
Resolution	Check whether the subject is present in any one of the chosen identity stores. Note that some identity stores may have been skipped due to identity resoultion settings or if they do not support the current authentication protocol.
Root cause	Subject not found in the applicable identity store(s).

Nome de usuário incorreto

11001 Received RADIUS Access-Request 11017 RADIUS created a new session ... ... 11507 Extracted EAP-Response/Identity **12983 Prepared EAP-Request proposing EAP-TTLS with challenge** ... ... **12978 Extracted EAP-Response containing EAP-TTLS challenge-response and accepting EAP-TTLS as negotiated** 12800 Extracted first TLS record; TLS handshake started ... ... 12810 Prepared TLS ServerDone message ... ... 12812 Extracted TLS ClientKeyExchange message 12803 Extracted TLS ChangeCipherSpec message ... ... **12816 TLS handshake succeeded** ... ... **11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge** 12985 Prepared EAP-Request with another EAP-TTLS challenge 11006 Returned RADIUS Access-Challenge 11001 Received RADIUS Access-Request ... ... 12971 Extracted EAP-Response containing EAP-TTLS challenge-response **11808 Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated** ... ... 15013 Selected Identity Source - All_AD_Join_Points 24430 Authenticating user against Active Directory - varshaah-ad 24325 Resolving identity - user@varshaah.local 24313 Search for matching accounts at join point - varshaah.local ... ... 24352 Identity resolution failed - ERROR_NO_SUCH_USER **24412 User not found in Active Directory - varshaah-ad** ... ... 15013 Selected Identity Source - Internal Users 24210 Looking up User in Internal Users IDStore - user **24216 The user is not found in the internal users identity store** ... ... 22056 Subject not found in the applicable identity store(s) 22058 The advanced option that is configured for an unknown user is used 22061 The 'Reject' advanced option is configured in case of a failed authentication request **11823 EAP-MSCHAP authentication attempt failed** ... ... **11815 Inner EAP-MSCHAP authentication failed** ... ... 12976 EAP-TTLS authentication failed 0 ... ... 11504 Prepared EAP-Failure 1 **11003 Returned RADIUS Access-Reject**

Defeitos conhecidos

ID do bug	Descrição
ID de bug da Cisco 63395	O ISE 3.0 não pode localizar o repositório de ID REST após a reinicialização dos serviços

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.