

Configure Machine and User Authentication with EAP-TTLS

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Network Topology](#)

[Configure](#)

[Configurations](#)

[Part 1: Download and Install Secure Client NAM \(Network Access Manager\)](#)

[Part 2: Download and Install Secure Client NAM Profile Editor](#)

[Part 3: Allow Windows Cache Credentials to be Accessed by NAM](#)

[Part 4: Configure NAM Profile using NAM Profile Editor](#)

[Part 5: Configure Wired Network for EAP-TTLS](#)

[Part 6: Save the Network Configuration File](#)

[Part 7: Configure AAA on the Switch](#)

[Part 8: ISE Configurations](#)

[Verify](#)

[Analyze ISE RADIUS Live Logs](#)

[Machine Authentication](#)

[User Authentication](#)

[Analyze NAM Logs](#)

[Machine Authentication](#)

[User Authentication](#)

[Troubleshoot](#)

[Secure Client \(NAM\) Logs](#)

[Cisco ISE Logs](#)

[Switch Logs](#)

[Basic Debugs](#)

[Advanced Debugs \(if Required\)](#)

[Show Commands](#)

[User Authentication Failure due to Invalid Credentials](#)

[Known Defects](#)

Introduction

This document describes how to configure machine and user authentication with EAP-TTLS (EAP-MSCHAPv2) on Secure Client NAM and Cisco ISE.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics before proceeding with this deployment:

- Cisco Identity Services Engine (ISE)
- Secure Client Network Analysis Module (NAM)
- EAP Protocols

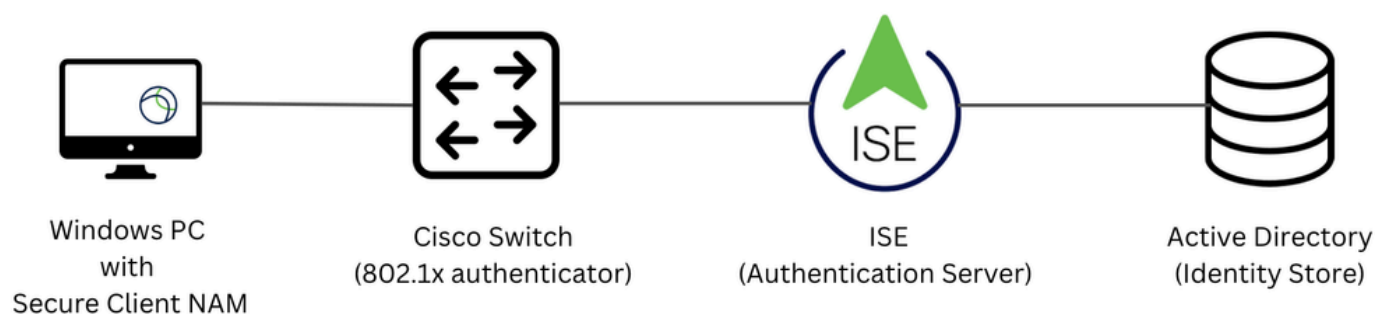
Components Used

The information in this document is based on these software and hardware versions:

- Identity Services Engine (ISE) version 3.4
- C9300 switch with Cisco IOS® XE Software, Version 16.12.01
- Windows 10 Pro Version 22H2 Built 19045.3930

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Network Topology



Network Topology

Configure

Configurations

Part 1: Download and Install Secure Client NAM (Network Access Manager)

Step 1. Go to [Cisco Software Download](#). In the product search bar, enter **Secure Client 5**.

This configuration example uses version **5.1.11.388**. The installation is performed using the **pre-deploy method**.

On the download page, locate and download **Cisco Secure Client Pre-Deployment Package (Windows)**.

Cisco Secure Client Pre-Deployment Package (Windows) - includes individual MSI files

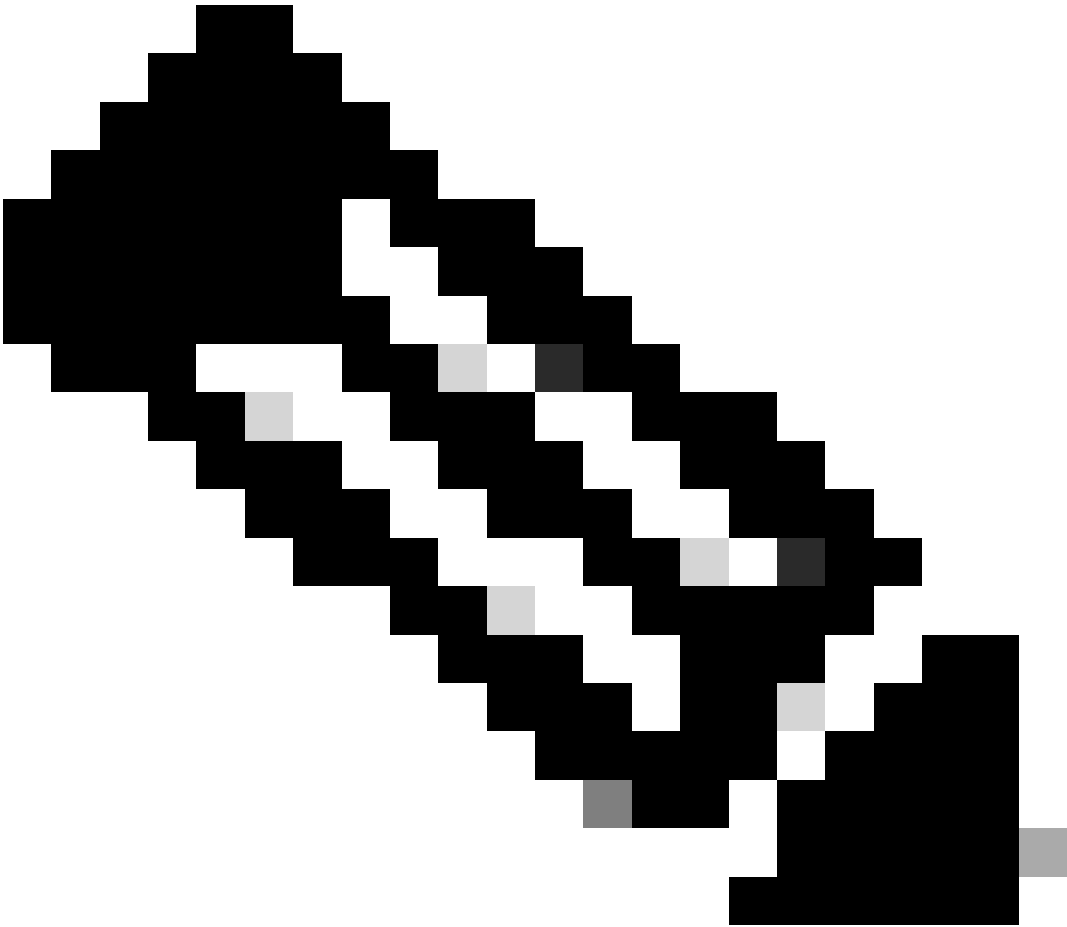
22-Aug-2025

129.05 MB



cisco-secure-client-win-5.1.11.388-predeploy-k9.zip

[Advisories](#)

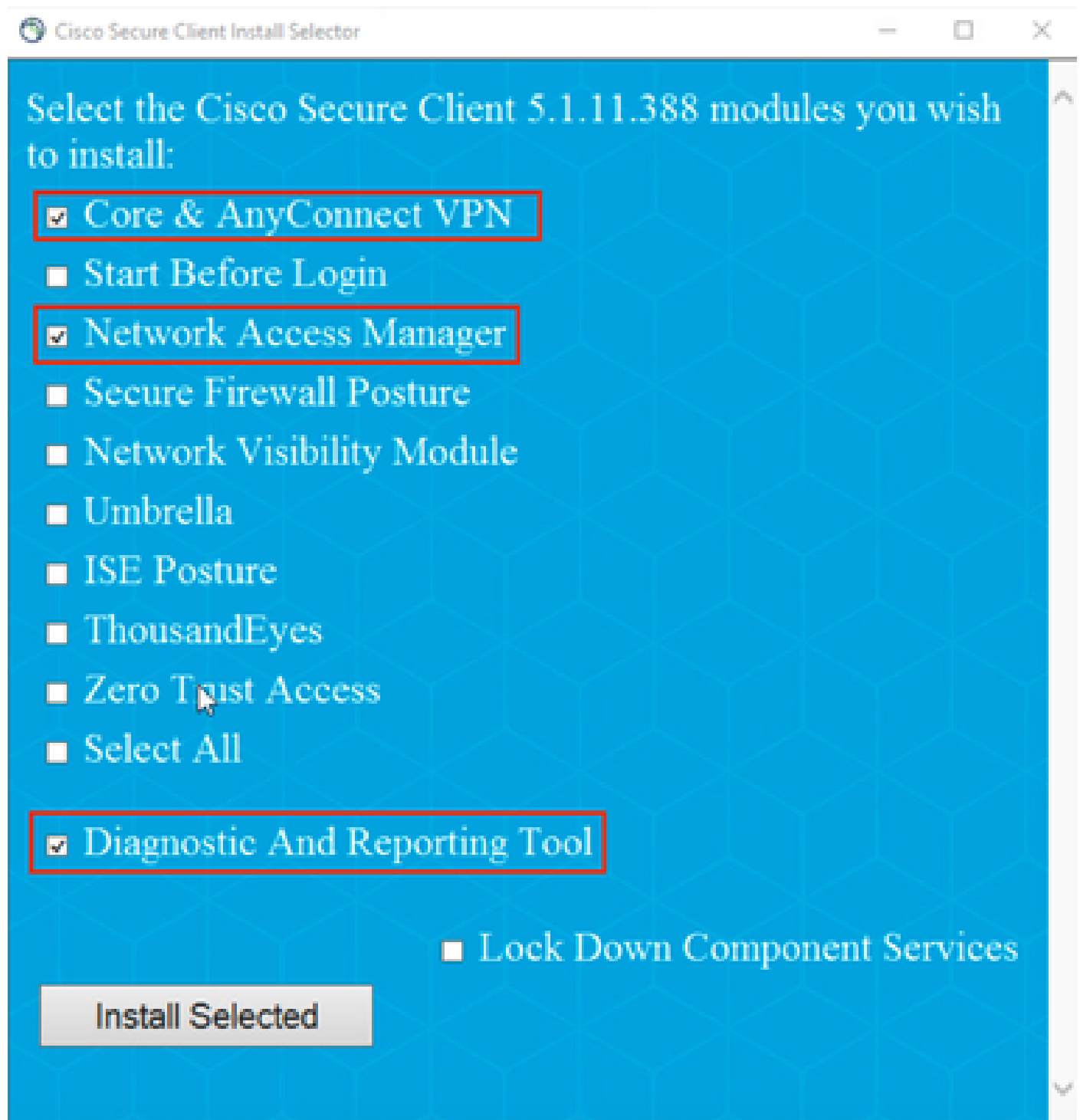


Note: Cisco AnyConnect has been deprecated and is no longer available on the Cisco Software Download site.

Step 2. Once downloaded and extracted, click**Setup**.

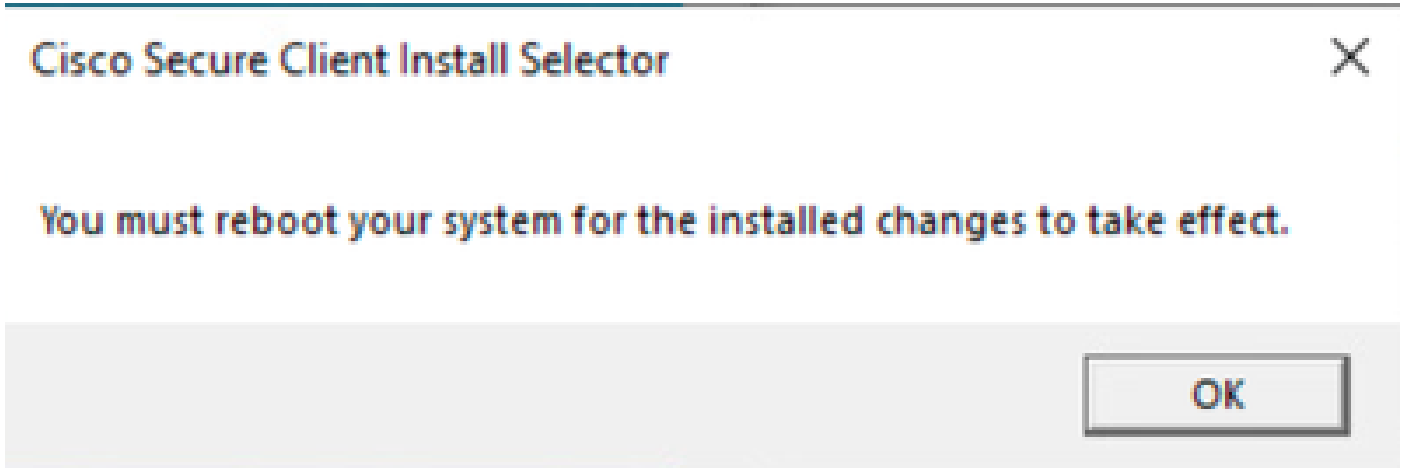
Profiles	File folder						8/14/2025 4:55 PM
Setup	File folder						8/14/2025 4:56 PM
cisco-secure-client-win-2.9.0-thou...	Windows Installer Package	10,172 KB	No	11,204 KB	10%		8/14/2025 4:04 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	19,886 KB	No	22,535 KB	12%		8/14/2025 4:47 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

Step 3. Install the **Core & AnyConnect VPN**, **Network Access Manager**, and the **Diagnostics and Reporting Tool** modules.



Click Install Selected.





Step 4. A reboot is required after installation. Click **OK** and restart your device.



Reboot Required Pop-up

Part 2: Download and Install Secure Client NAM Profile Editor

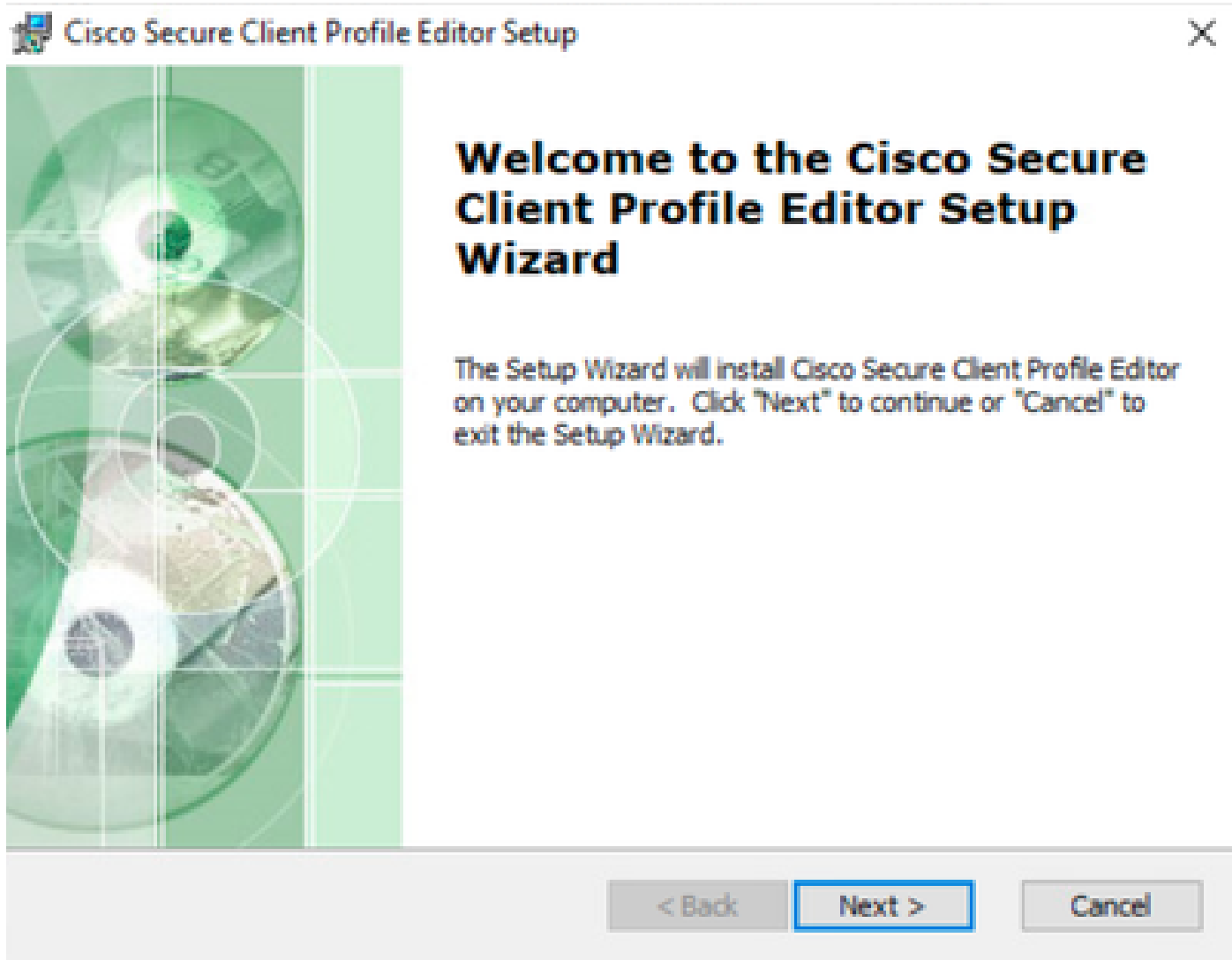
Step 1. The Profile Editor can be found on the same downloads page as the Secure Client. This configuration example uses version **5.1.11.388**.

Profile Editor (Windows) 	22-Aug-2025	14.76 MB	 
tools-cisco-secure-client-win-5.1.11.388-profileeditor-k9.msi			
Advisories 			

Profile Editor

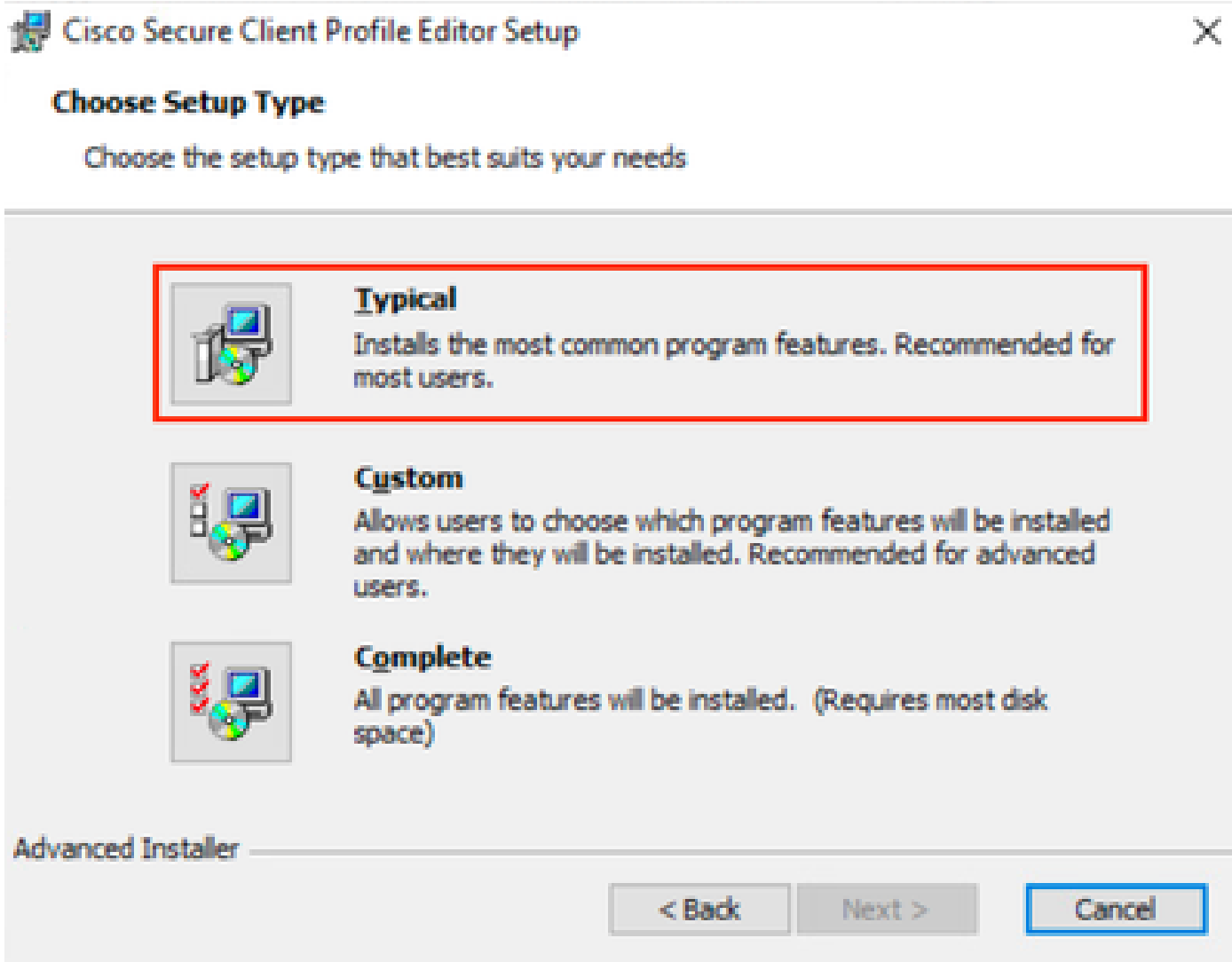
Download and install the **Profile Editor**.

Step 2. Run the MSI file.



Profile Editor Setup Start

Step 3. Use the **Typical** setup option and install the **NAM Profile Editor**.

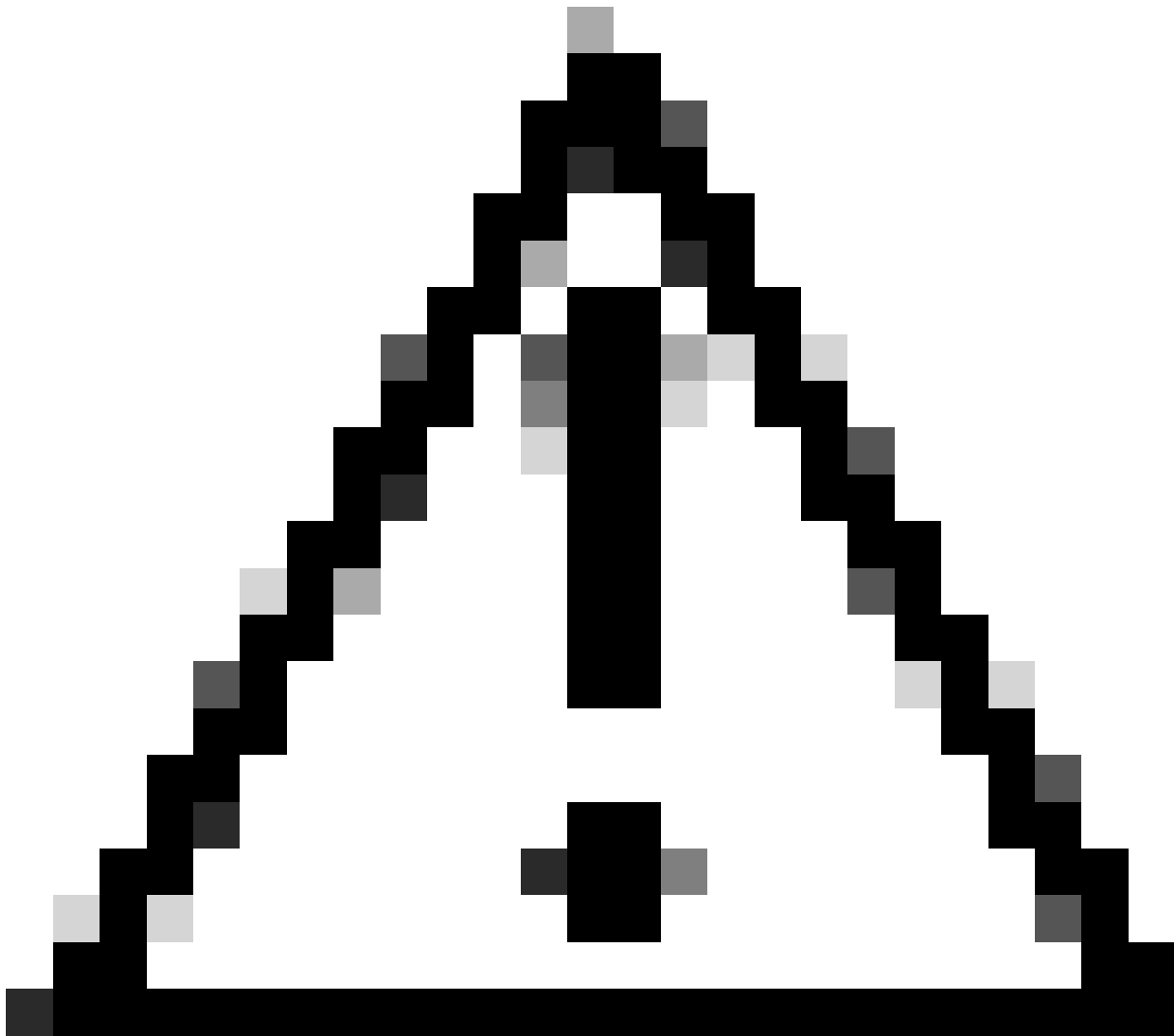


Profile Editor Setup

Part 3: Allow Windows Cache Credentials to be Accessed by NAM

By default, on Windows 10, Windows 11, and Windows Server 2012, the operating system prevents Network Access Manager (NAM) from retrieving the machine password required for machine authentication. As a result, machine authentication using the machine password does not work unless a registry fix is applied.

To enable NAM to access the machine credentials, apply the [Microsoft KB 2743127](https://support.microsoft.com/en-us/topic/fix-issues-with-network-access-manager-authentication-2743127) fix on the client desktop.



Caution: Editing the Windows registry incorrectly can cause serious problems. Make sure you back up the registry before making changes.

Step 1. In the Windows search bar, enter **regedit**, and then click **Registry Editor**.

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



In this example, the PSN node certificate is issued by varshaah.varshaah.local. Hence, the rule **Common Name ends with .local** is used. This rule validates the certificate that the server presents during the EAP-TTLS flow.

You can also specify the common name of the **Policy Service Node (PSN) EAP authentication certificate**.

- Under **Certificate Trusted Authority**, two options are available.
In this scenario, the option **Trust any Root Certificate Authority (CA) installed on the OS** is used instead of adding a specific CA certificate.

With this option, the Windows device trusts any EAP certificate that is signed by a certificate included in **Certificates – Current User > Trusted Root Certification Authorities > Certificates** (managed by the operating system).

- Click **Next** to continue.

Networks

Profile: Untitled

Certificate Trusted Server Rules

<new>

Common Name ends with .local

Certificate Field	Match	Value
Common Name	ends with	.local

RemoveSave

Certificate Trusted Authority

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

☐ Include Root Certificate Authority (CA) Certificates

Add

Remove

Next

Cancel

NAM Profile Editor Certificates

Step 6. In the **Machine Credentials** section, select **Use Machine Credentials**, and then click **Next**.

Networks

Profile: Untitled

Machine Identity

Unprotected Identity Pattern:

Protected Identity Pattern:

Machine Credentials

☒ Use Machine Credentials

☐ Use Static Credentials

Password:

Next

Cancel

NAM Profile Editor Credentials

Step 7. Configure **User Auth** section.

- Select **EAP-TTLS** under **EAP Methods**.
- Under **Inner Methods**, select **Use EAP Methods** and select **EAP-MSCHAPv2**.
- Click **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-TTLS Settings

☒ Validate Server Identity
☒ Enable Fast Reconnect

Inner Methods

☒ **Use EAP Methods**
☐ EAP-MD5
☒ **EAP-MSCHAPv2**
☐ PAP (legacy) ☐ MSCHAP (legacy)
☐ CHAP (legacy) ☐ MSCHAPv2 (legacy)

Next **Cancel**

NAM Profile Editor User Authentication

Step 8. In **Certificates**, configure the same certificate validation rules as described in Step 5.

Step 9. In **User Credentials**, select **Use Single Sign-On Credentials**, and then click **Done**.

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:

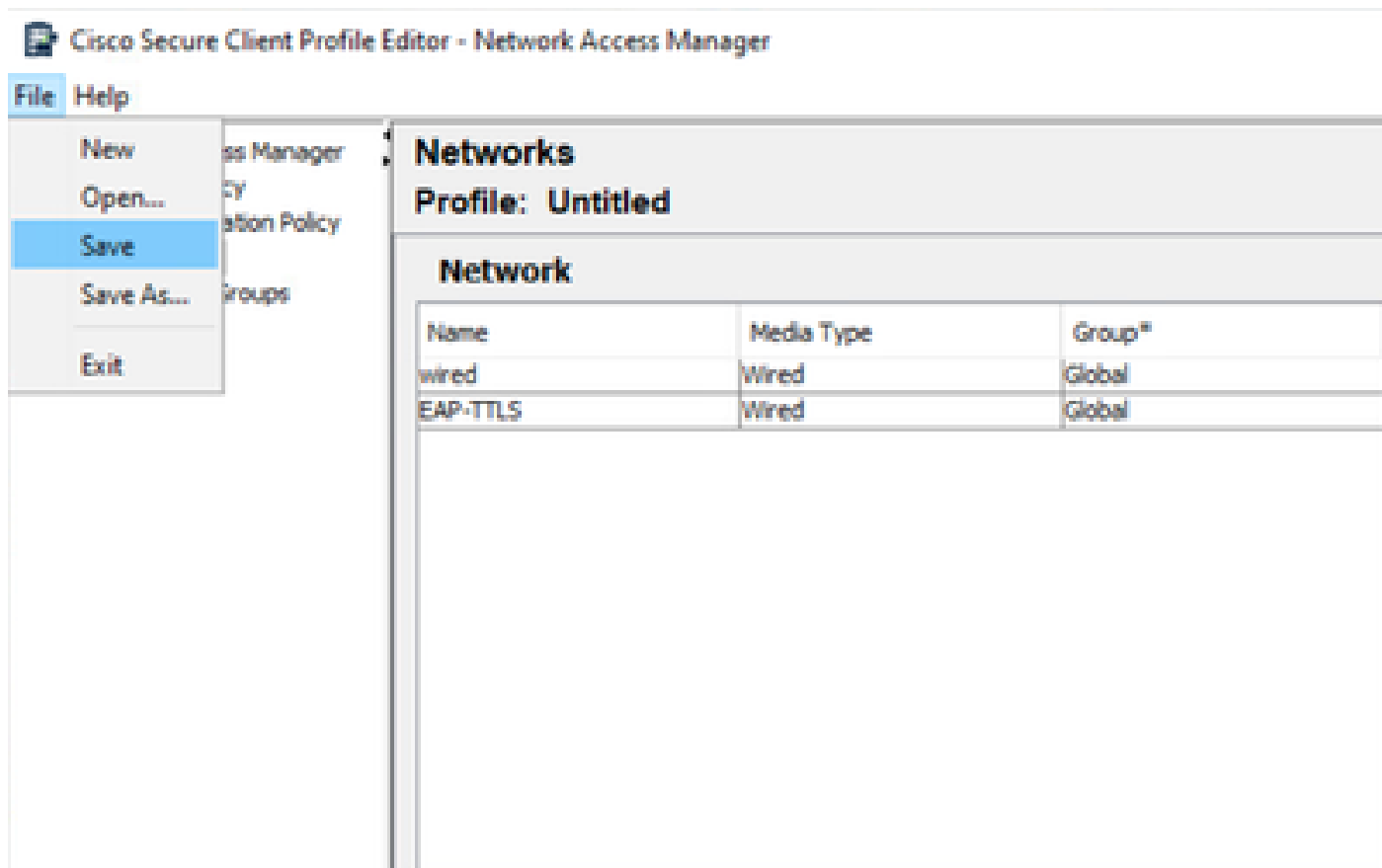
Done

Cancel

NAM Profile Editor User Credentials

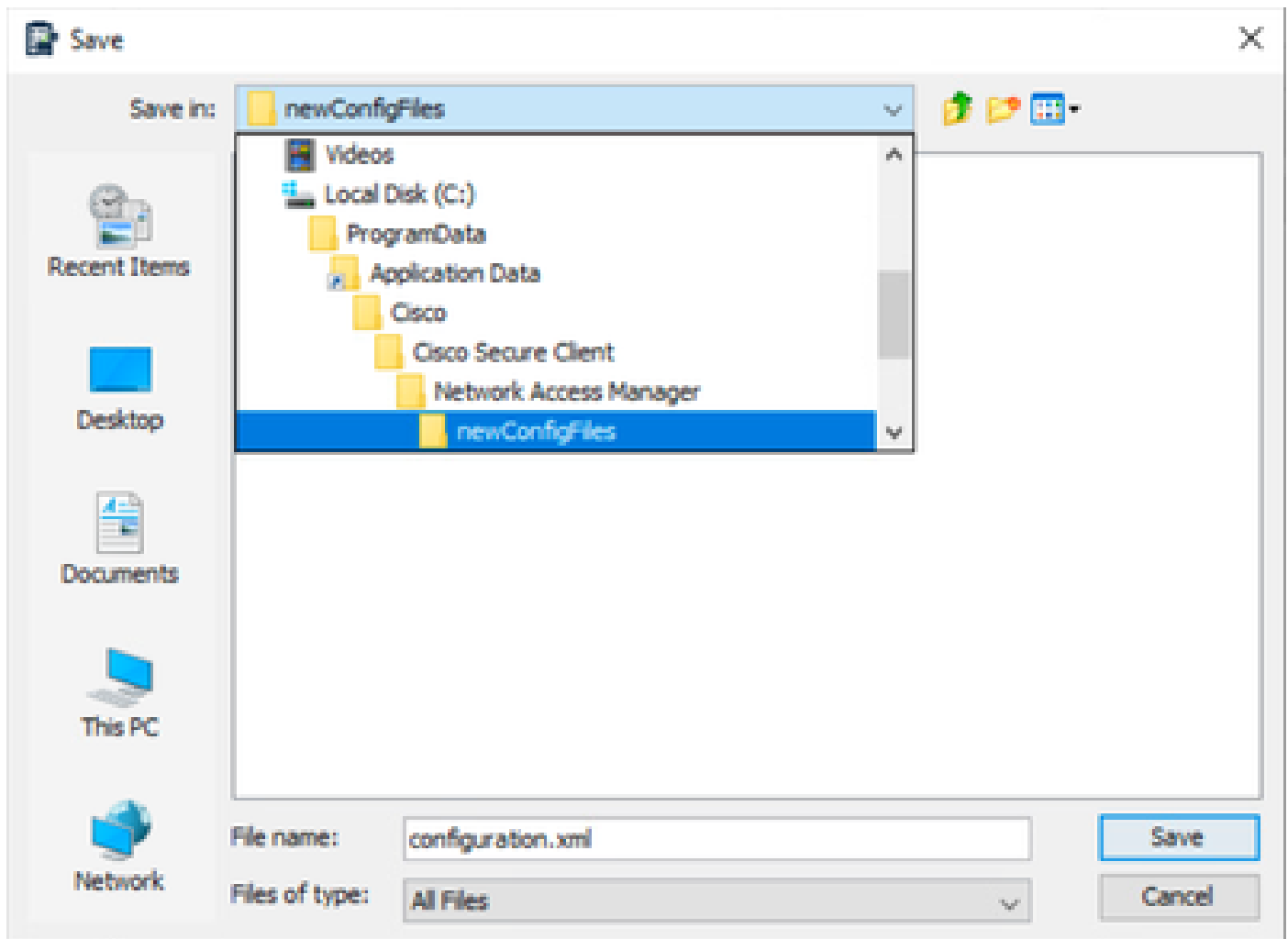
Part 6: Save the Network Configuration File

Step 1. Click **File > Save**.



NAM Profile Editor Save Network Configuration

Step 2. Save the file as **configuration.xml** in the **newConfigFiles** folder.



Save Network Configuration

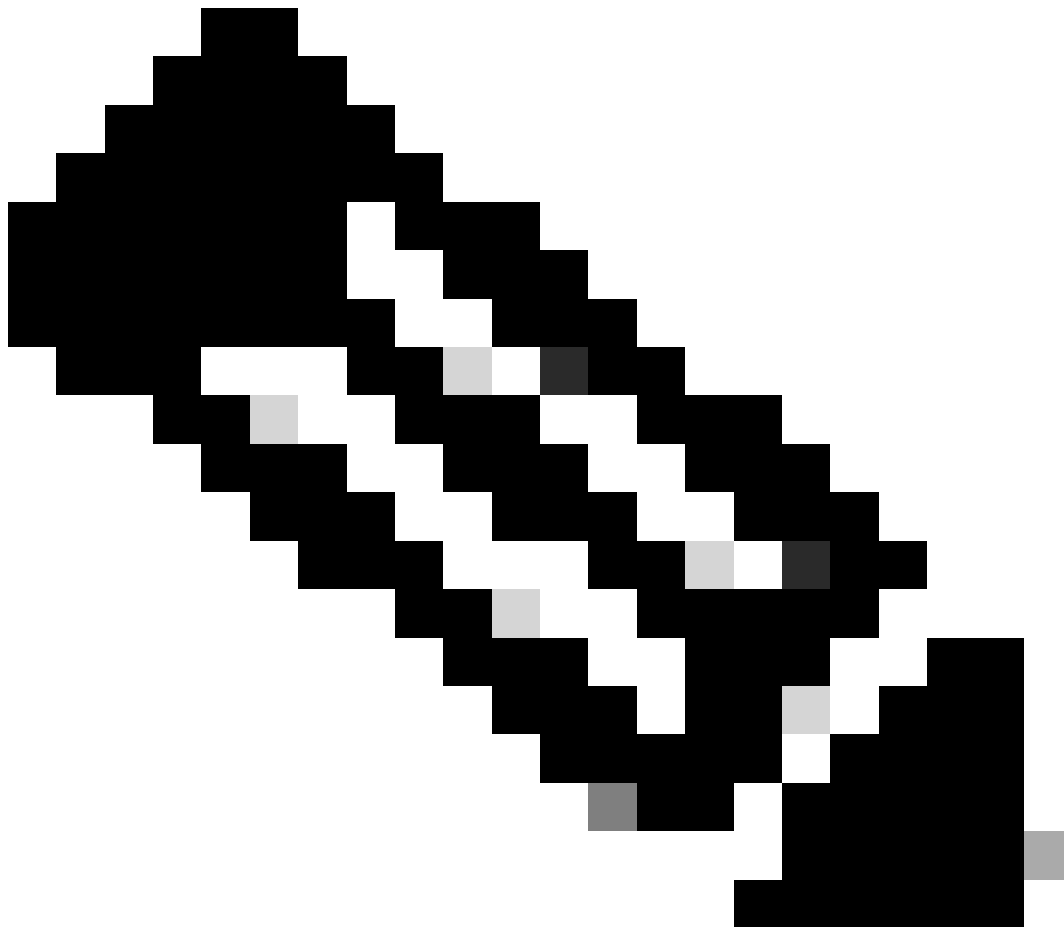
Part 7: Configure AAA on the Switch

```
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: The dot1x system-auth-control command does not appear in the show running-config output, but it is required to enable 802.1X globally.

Configure the Switch Interface for 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

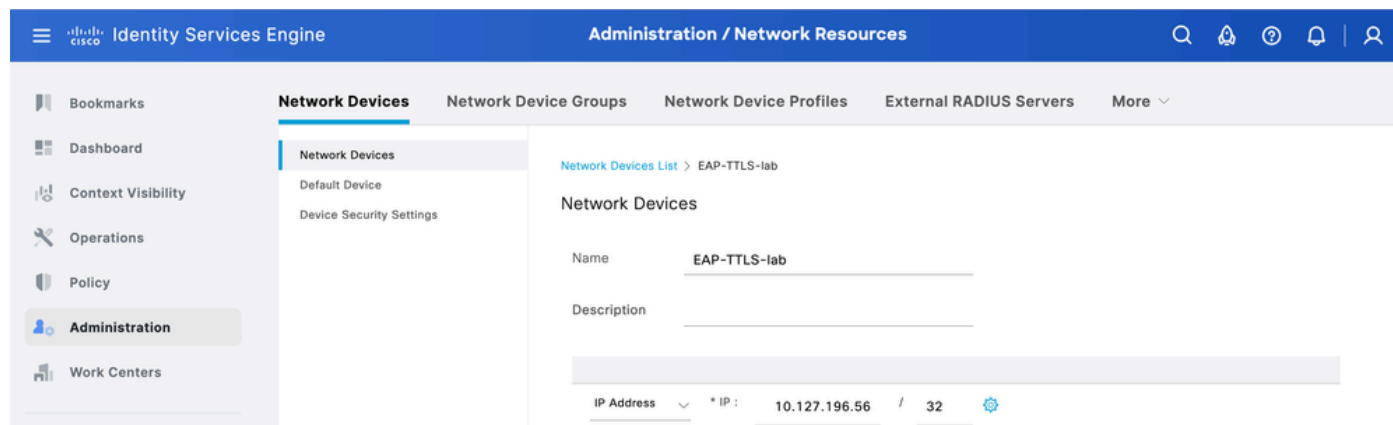
```

Part 8: ISE Configurations

Step 1. Configure switch on ISE.

Navigate to **Administration > Network Resources > Network Devices** and click **Add**.

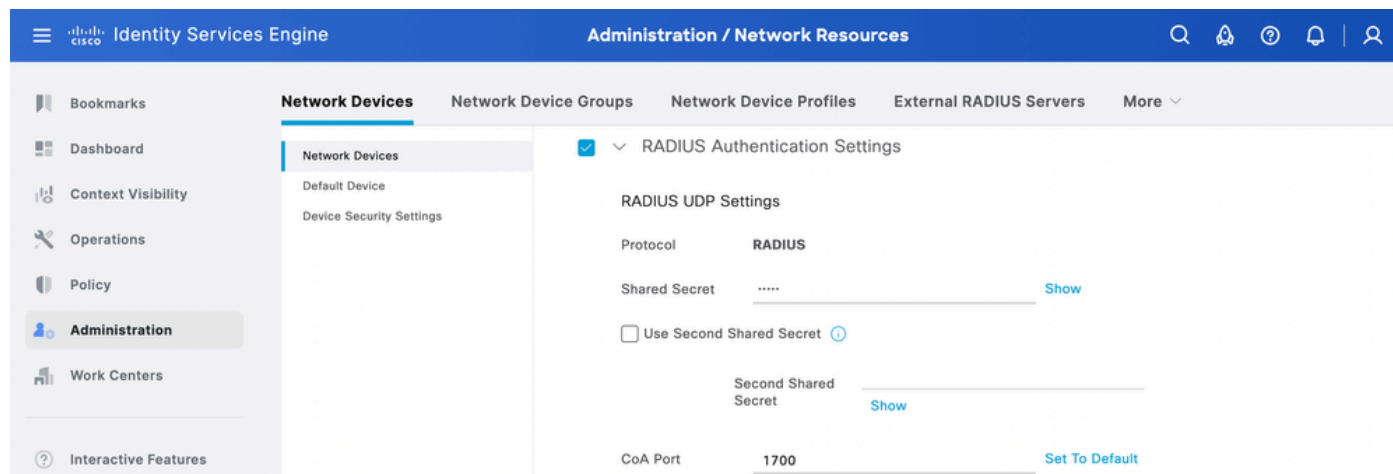
Enter the switch name and IP address here.



The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes the Cisco logo, 'Identity Services Engine', and 'Administration / Network Resources'. The left sidebar contains various navigation options: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (highlighted), and Work Centers. The main content area is titled 'Network Devices' and shows a list of devices. A new device named 'EAP-TTLS-lab' is being added. The 'IP Address' field is set to '10.127.196.56 / 32'.

Adding Network Device ISE

Enter the RADIUS shared secret, the same as the one configured earlier on the switch.



The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes the Cisco logo, 'Identity Services Engine', and 'Administration / Network Resources'. The left sidebar contains various navigation options: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (highlighted), and Work Centers. The main content area is titled 'Network Devices' and shows a list of devices. The 'RADIUS Authentication Settings' section is expanded, showing fields for 'Protocol' (RADIUS), 'Shared Secret' (masked), 'Use Second Shared Secret' (unchecked), 'Second Shared Secret' (masked), and 'CoA Port' (1700).

Step 2. Configure identity source sequence.

- Navigate to **Administration > Identity Management > Identity Source Sequences**.
- Click **Add** to create a new identity source sequence.
- Configure the identity sources under **Authentication Search List**.

[Identity Source Sequences List](#) > EAP_TTLS

Identity Source Sequence

Identity Source Sequence

Name

EAP_TTLS

Description

Certificate Based Authentication

☐

Select Certificate Authentication Profile

Certificate_Profile

Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available

All_AD_Join_Points

bbh

Selected

varshaah-ad

Internal Users

ISE Identity Source Sequence

Step 3. Configure policy set.









Navigate to **Policy > Policy Sets** and create a new policy set. Configure the conditions as Wired_802.1x OR Wireless_802.1x. For Allowed Protocols, choose **Default Network Access**:

Policy Sets

[Reset](#)

[Reset Policyset Hitcounts](#)

[Save](#)

	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
<div>Search</div>								
	EAP-TTLS		OR	<div><div></div>Wired_802.1X</div> <div><div></div>Wireless_802.1X</div>	Default Network Access  	0		

Create the authentication policy for dot1x and choose the identity source sequence created in Step 4.

Authentication Policy(2)

+	Status	Rule Name	Conditions	Use	Hits
			Search		
	✓	Dot1x	OR <ul style="list-style-type: none"> Wired_802.1X Wireless_802.1X 	EAP_TTLS <ul style="list-style-type: none"> Options 	0
	✓	Default		All_User_ID_Stores <ul style="list-style-type: none"> Options 	0

EAP-TTLS Authentication Policy

For authorization policy, create the rule with three conditions. The first condition checks for the condition that EAP-TTLS tunnel is used. The second condition checks that EAP-MSCHAPv2 is used as the inner EAP method. The third condition checks for the respective AD group.

Authorization Policy(3)

				Results			
+	Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
			Search				
	✓	User Authentication	AND <ul style="list-style-type: none"> Network Access-EapTunnel EQUALS EAP-TTLS Network Access-EapAuthentication EQUALS EAP-MSCHAPv2 varshaah-ad-ExternalGroups EQUALS varshaah.local/Builtin/Users 	PermitAccess	Select from list	0	⚙️
⋮	✓	Machine Authentication	AND <ul style="list-style-type: none"> Network Access-EapTunnel EQUALS EAP-TTLS Network Access-EapAuthentication EQUALS EAP-MSCHAPv2 varshaah-ad-ExternalGroups EQUALS varshaah.local/Users/Domain Computers 	PermitAccess	Select from list	0	⚙️

Dot1x Authorization Policy

Verify

You can reboot the Windows 10 machine or you can sign out and then sign in. Whenever the windows log in screen is displayed, machine authentication is triggered.

↶ Reset Repeat Counts ↶ Export To				Filter ⌵ ⚙️					
Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles
⌵				Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles
Sep 23, ...	●	🔒	0	host/DESKTOP-QSCE4P3	B4:96:91:26:E9:AB	Intel-Device	EAP-TTLS >> Dot1x	EAP-TTLS >> Machine Authentication	PermitAccess
Sep 23, ...	✅	🔒		host/DESKTOP-QSCE4P3	B4:96:91:26:E9:AB	Intel-Device	EAP-TTLS >> Dot1x	EAP-TTLS >> Machine Authentication	PermitAccess

Live Log Machine Authentication

When you log in to the PC with credentials, user authentication is triggered.

Cisco Secure Client | EAP-TTLS

✕

Please enter your username and password for the network: EAP-TTLS

Username:

labuser

Password:

☐ Show Password

OK

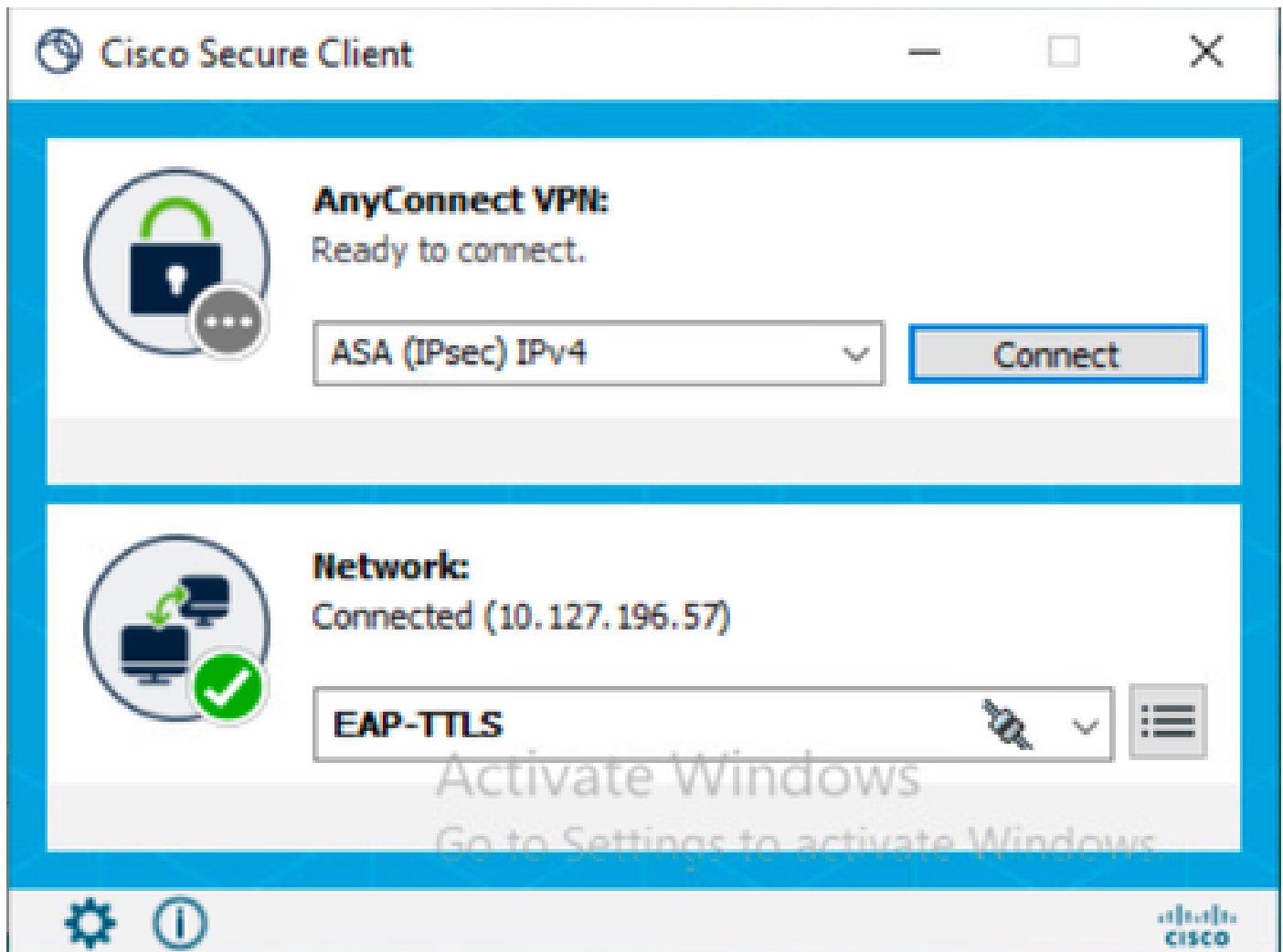
Cancel

User Authentication Credentials



Note: This example uses Active Directory user credentials for authentication. Alternatively, you can create an internal user in Cisco ISE and use those credentials for log in.

After the credentials are entered and successfully verified, the endpoint is connected to the network with user authentication.



EAP-TTLS Connected

↺ Reset Repeat Counts ↗ Export To ↕ Filter ⚙

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles
×	▼			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

Live Log User Authentication

Analyze ISE RADIUS Live Logs

This section illustrates the RADIUS live log entries for successful machine and user authentication.

Machine Authentication

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

User Authentication

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

Analyze NAM Logs

NAM logs, especially after you enable Extended Logging, contains a large amount of data, most of which are irrelevant and can be ignored. This section lists out the debug lines to demonstrate each step NAM takes to establish a network connection. When you work through a log, these key phrases can be helpful to locate part of the log relevant to the issue.

Machine Authentication

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

The client receives an EAP-TTLS packet from the network switch, initiating the EAP-TTLS session. This is the starting point for the machine authentication tunnel.

```
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
```


The client receives the **Server Hello** from ISE and begins validating the server certificate (CN=varshaah.varshaah.local). The certificate is found in the client's trust store and added for validation.

```
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
```

The server certificate is successfully validated, completing TLS tunnel establishment.

```
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-
```

The client signals that **authentication has passed**. The interface is unblocked, and the internal state machine transitions to *USER_T_NOT_DISCONNECTED*, indicating the machine can now pass traffic.

```
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-
```

The adapter reports **authenticated**, and the NAM AccessStateMachine transitions to *ACCESS_AUTHENTICATED*. This confirms the machine has successfully completed authentication and has full network access.

User Authentication

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

The NAM client begins the EAP-TTLS connection process.

```
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
```

NAM binds the physical adapter to the EAP-TTLS network and moves into the **ACCESS_ATTACHED** state, confirming that the adapter is ready for authentication.

```
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
```

The client transitions from **ATTACHED** to **CONNECTING**, beginning the 802.1X exchange.

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

The client sends an **EAPOL-Start** to trigger the authentication process.

```
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
```

The switch requests an identity, and the client prepares to respond with an outer identity.

```
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
```

NAM sends the outer identity. By default, this is **anonymous**, indicating that the exchange is for user authentication (not machine).

```
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
```

Both client and server agree to use **EAP-TTLS** as the outer method.

```
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
```

The client sends **Client Hello** and receives the **Server Hello**, which includes the ISE certificate.

```
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

The server certificate is presented. The client looks up the CN varshaah.varshaah.local, finds a match, and validates the certificate. The handshake pauses while the X.509 certificate is checked.

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

The tunnel is established. NAM now requests and prepares the **protected identity** and credentials for inner authentication.

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

The TLS handshake completes. A secure tunnel is now established for inner authentication.

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

The protected identity (username) is sent and accepted by 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

ISE requests the password. NAM sends the protected password inside the TLS tunnel.

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]: ST
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]: ST
1855: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: ST

ISE validates the password, sends **EAP-Success**, and NAM transitions to **AUTHENTICATED**. At this

point, user authentication is complete and the client is allowed network access.

Troubleshoot

When troubleshooting Network Access Manager (NAM) issues with Cisco ISE and switch integration, logs must be collected from all three components: **Secure Client (NAM)**, **Cisco ISE**, and the **switch**.

Secure Client (NAM) Logs

1. Enable **NAM extended logging** by following [these](#) steps.
2. Reproduce the issue. If the network profile does not apply, run [Network Repair](#) in Secure Client.
3. Collect the [DART bundle](#) using the Diagnostics and Reporting Tool (DART).

Cisco ISE Logs

Enable these debugs on ISE to capture authentication and directory interactions:

- runtime-AAA
- nsf
- nsf-session

Switch Logs

Basic Debugs

```
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
```

Advanced Debugs (if Required)

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

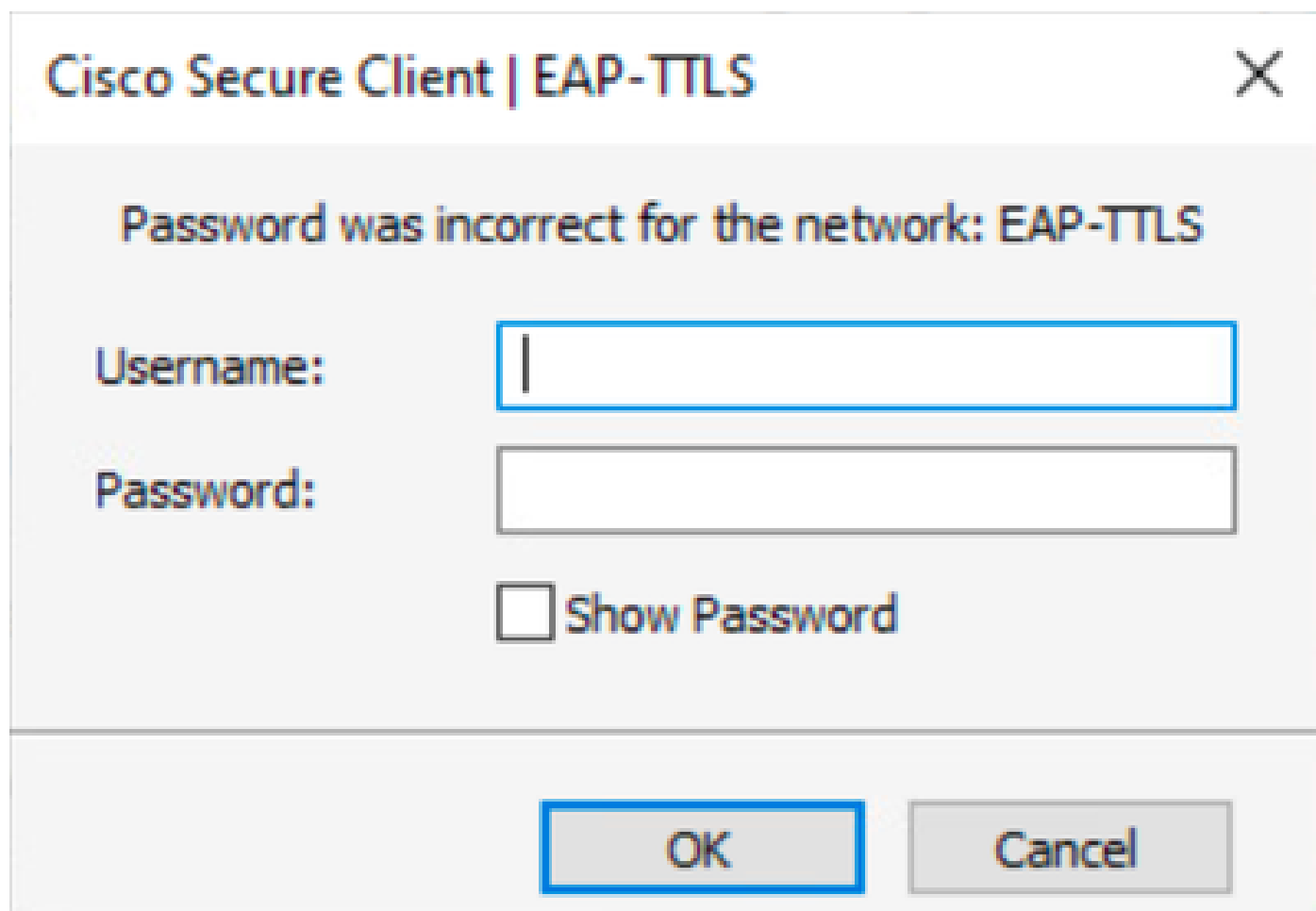
Show Commands

```
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
```

User Authentication Failure due to Invalid Credentials

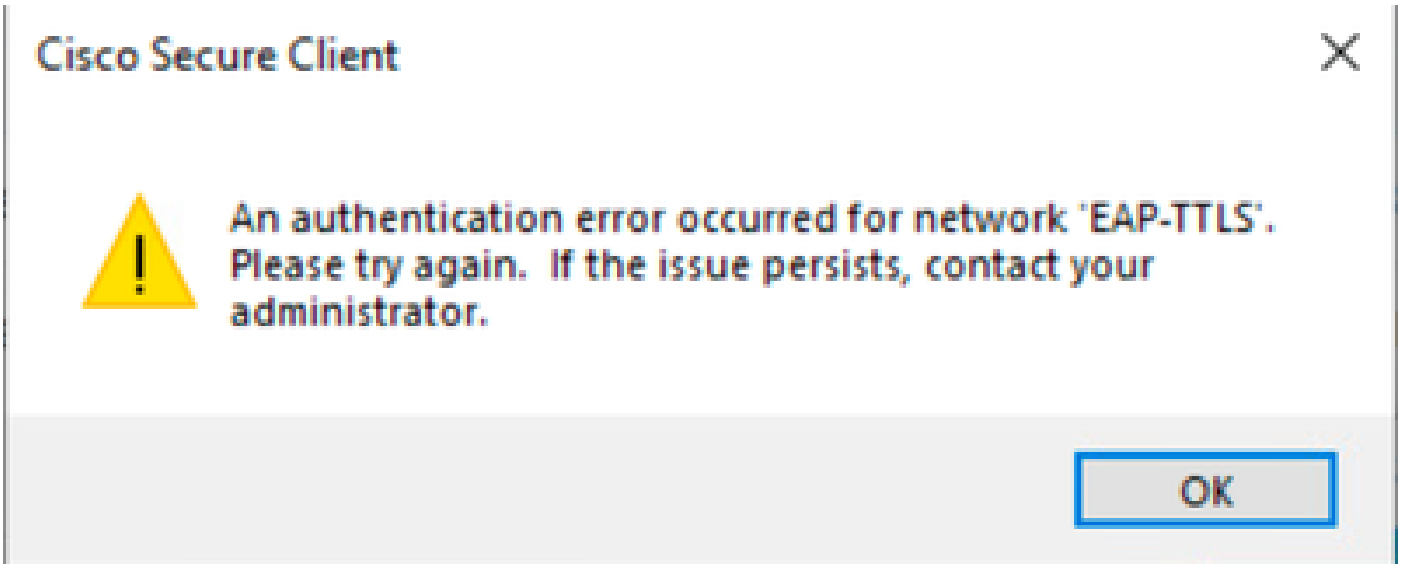
When a user enters incorrect credentials, Secure Client displays a generic **Password was incorrect for the network: EAP-TTLS** message. The on-screen error does not specify whether the issue is due to an invalid username or password.



The screenshot shows a dialog box titled "Cisco Secure Client | EAP-TTLS" with a close button (X) in the top right corner. The main message in the center is "Password was incorrect for the network: EAP-TTLS". Below this message, there are two input fields: "Username:" and "Password:". The "Username:" field is currently empty, and the "Password:" field is also empty. Below the "Password:" field, there is a checkbox labeled "Show Password". At the bottom of the dialog box, there are two buttons: "OK" and "Cancel".

Incorrect Password Error

If authentication fails twice consecutively, Secure Client displays this message: An authentication error occurred for network 'EAP-TTLS'. Please try again. If the issue persists, contact your administrator.



User Authentication Issue

To identify the cause, review the NAM logs.

1. Incorrect password:

When a user enters an incorrect password, NAM logs show entries similar to this output:

```
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
```

In Cisco ISE live logs, the corresponding event appears as:

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

Incorrect Password

```
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. Incorrect Username:

When a user enters an incorrect username, NAM logs show entries similar to this output:

```
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
```

In Cisco ISE live logs, the corresponding event appears as:

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 resolution settings or if they do not support the current authentication protocol.
Root cause	Subject not found in the applicable identity store(s).

Incorrect Username

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**

Known Defects

Bug ID	Description
<u>Cisco bug ID 63395</u>	ISE 3.0 cannot locate REST ID store after services restart