配置EAP链接与TEAP

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

配置

- 思科ISE配置
- Windows原生Supplicant客户端配置

验证

- 详细的身份验证报告
- 计算机身份验证
- 用户和机器身份验证

故障排除

- 实时日志分析
  - 计算机身份验证
  - 用户和机器身份验证

相关信息

简介

本文档介绍如何配置可扩展身份验证协议(EAP)链接的ISE和Windows请求方与TEAP。

先决条件

要求

Cisco 建议您了解以下主题：

- ISE
- Windows请求方的配置

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科ISE版本3.0
- Windows 10版本2004
- 基于协议隧道的可扩展身份验证协议(TEAP)知识

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

TEAP是基于隧道的可扩展身份验证协议方法，用于建立安全隧道并在该安全隧道的保护下执行其他EAP方法。

TEAP身份验证在初始EAP身份请求/响应交换后分两个阶段进行。在第一阶段，TEAP使用TLS握手来提供经过身份验证的密钥交换并建立受保护的隧道。隧道建立后，第二阶段开始是对等方和服务器进行进一步的会话，以建立所需的身份验证和授权策略。

Cisco ISE 2.7及更高版本支持TEAP协议。类型长度值(TLV)对象在隧道内用于在EAP对等体和EAP服务器之间传输身份验证相关数据。Microsoft在2020年5月发布的Windows版本10 2004中引入了对TEAP的支持。

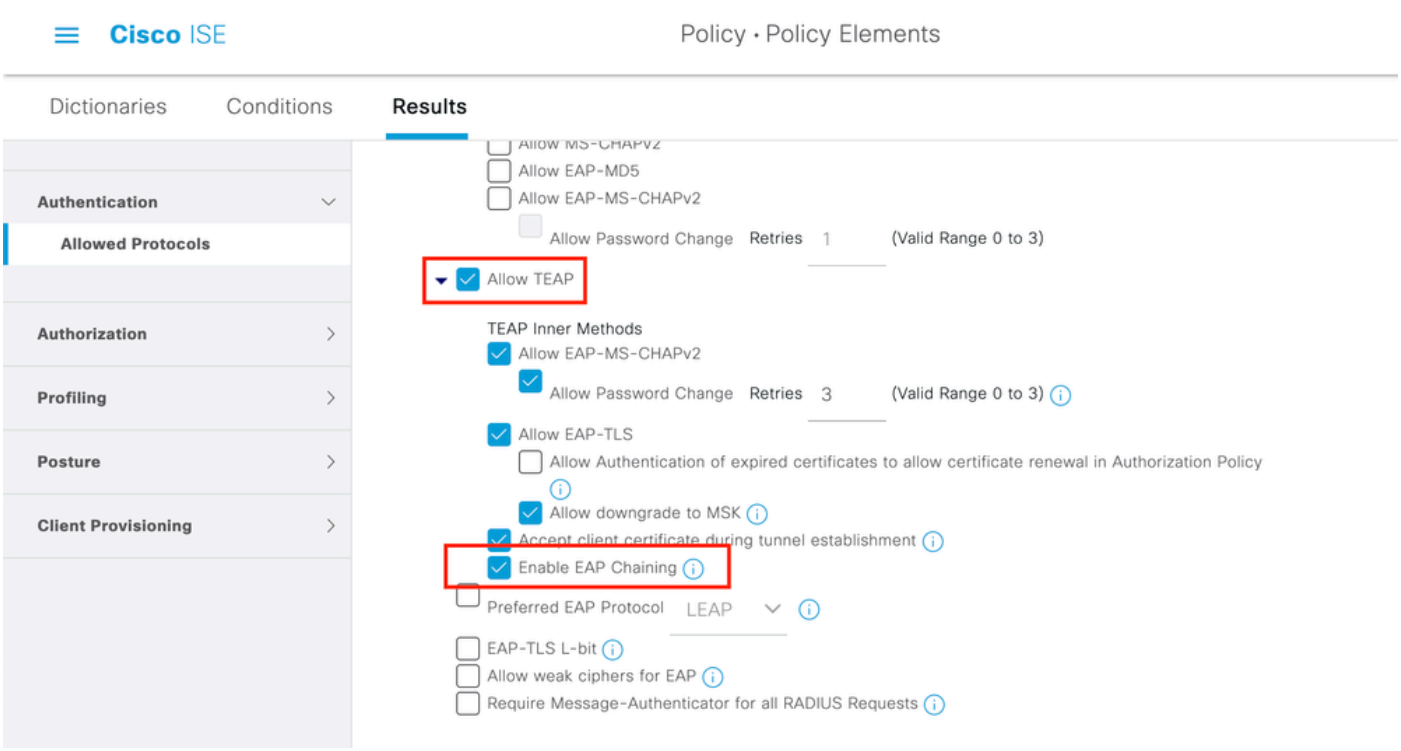
EAP链接允许在一个EAP/Radius会话内进行用户和计算机身份验证，而不是两个单独的会话。以前，要实现此目的，您必须具有Cisco AnyConnect NAM模块，并在Windows请求方上使用EAP-FAST，因为本地Windows请求方不支持此功能。现在，您可以使用Windows原生Supplicant客户端通过TEAP执行与ISE 2.7的EAP链接。

配置

思科ISE配置

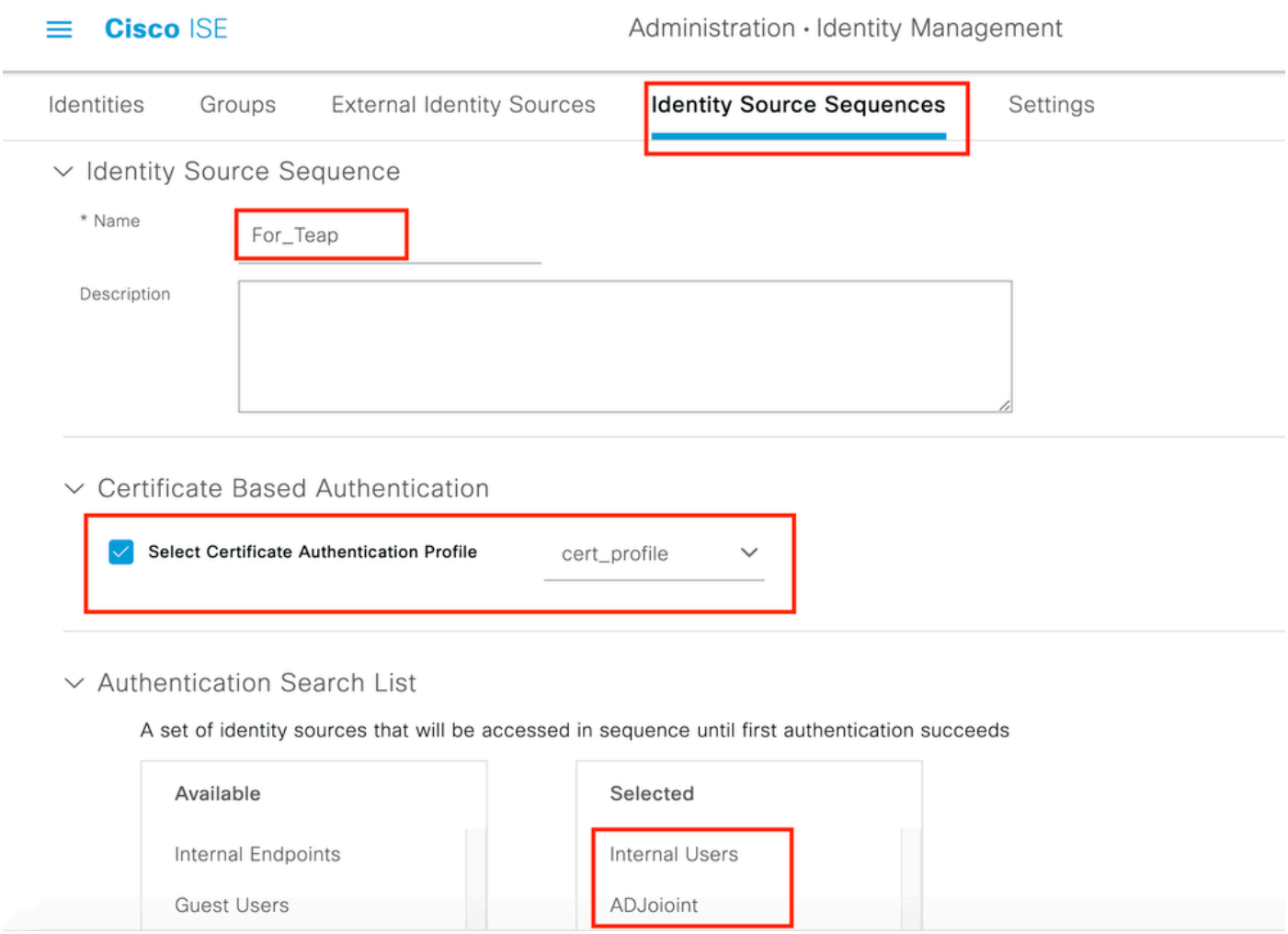
1.您必须编辑“允许的协议”以启用TEAP和EAP链接。

2.导航至ISE > Policy > Policy Elements > Results > Authentication > Allowed Protocols > Add New. Check the TEAP and EAP chaining复选框。



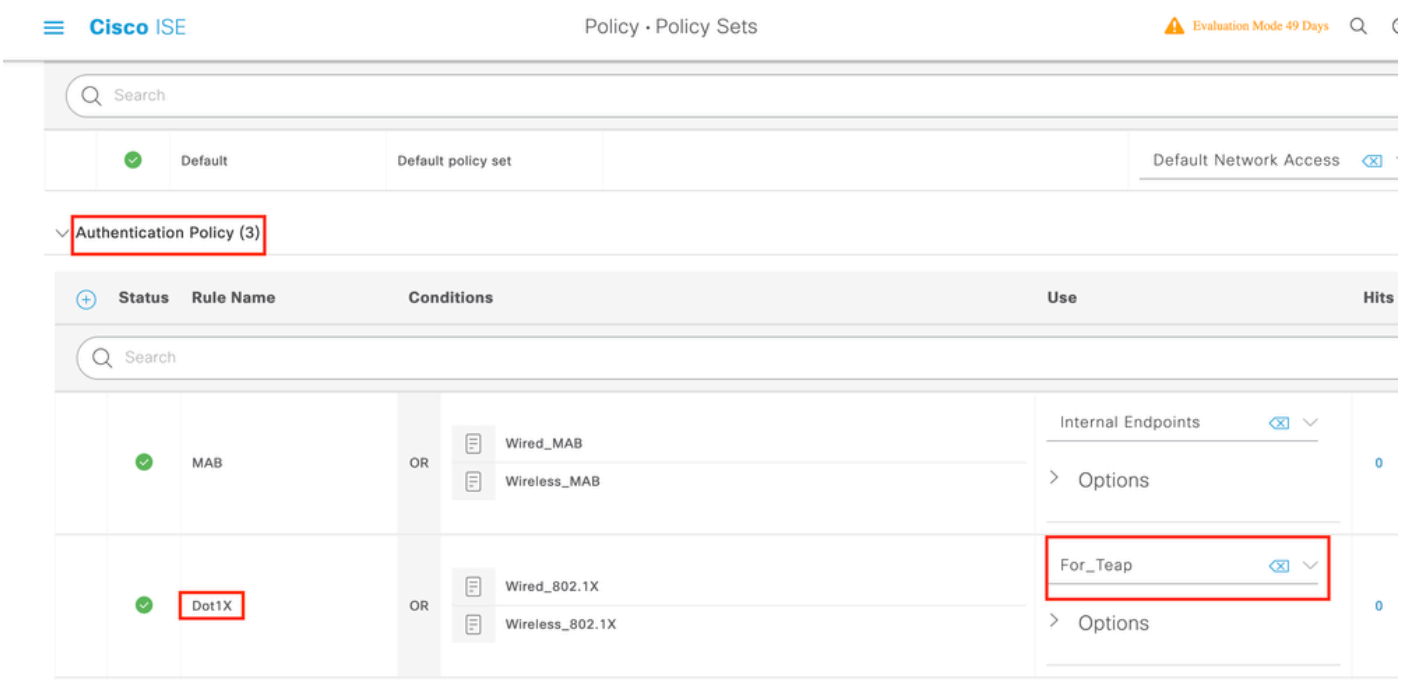
3.创建证书配置文件并将其添加到身份源序列。

4.导航到ISE > Administration > Identities > identity Source Sequence，然后选择Certificate Authentication Profile。



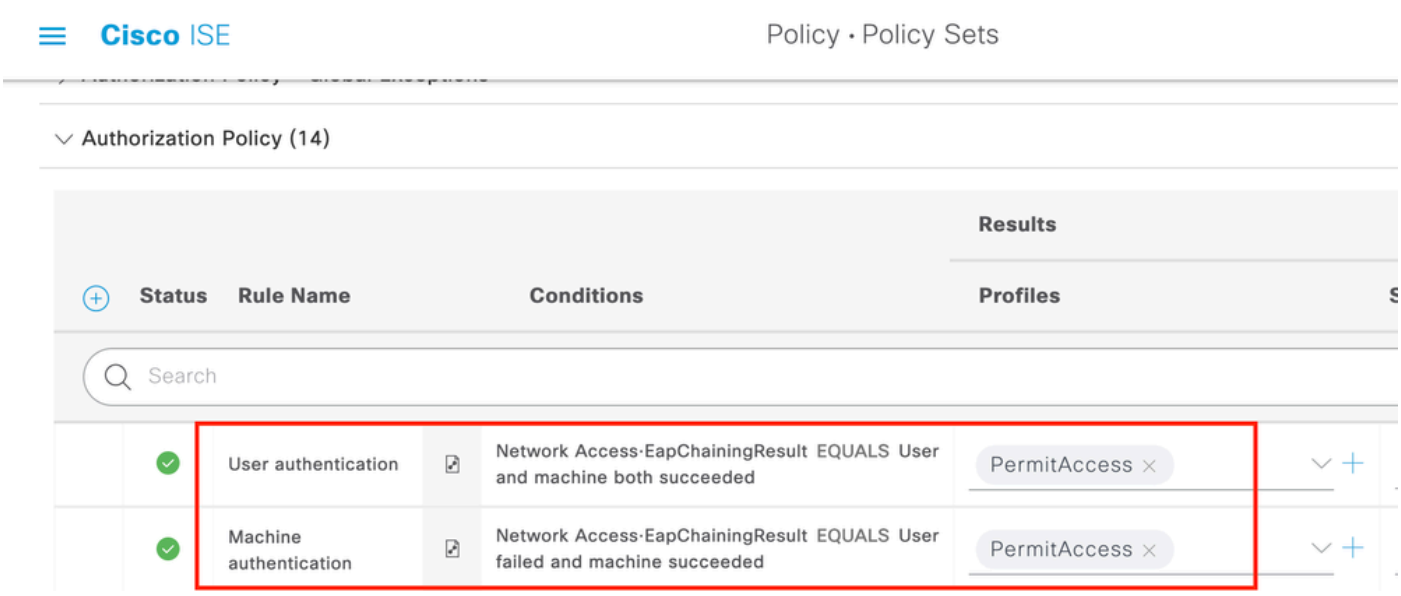
5.必须在身份验证策略中调用此序列。

6.导航到ISE > Policy > Policy Sets. Choose the Policy Set for Dot1x > Authentication Policy，然后选择Identity Source Sequences（在步骤3中创建）。



7.现在，您必须修改Dot1x策略集下的授权策略。

8.导航到ISE > Policy > Policy . Sets为Dot1x > Authentication Policy选择Policy Set。您必须创建两个规则。第一条 规则检查计算机是否已进行身份验证，但用户未进行身份验证。第二条 规则验证用户和机器现在都已通过身份验证。



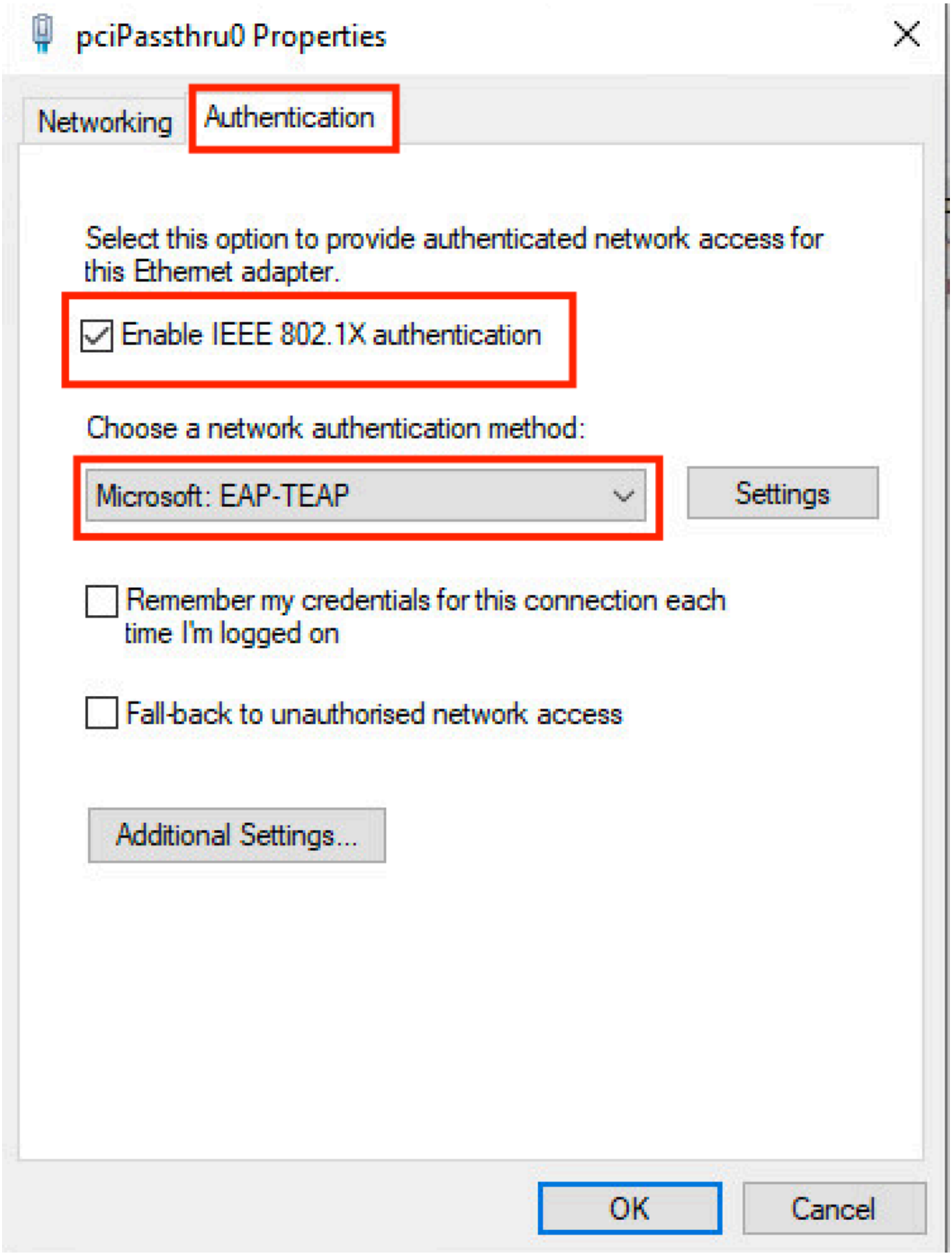
9.从ISE服务器端完成配置。

Windows原生Supplicant客户端配置

配置本文档中的有线身份验证设置。

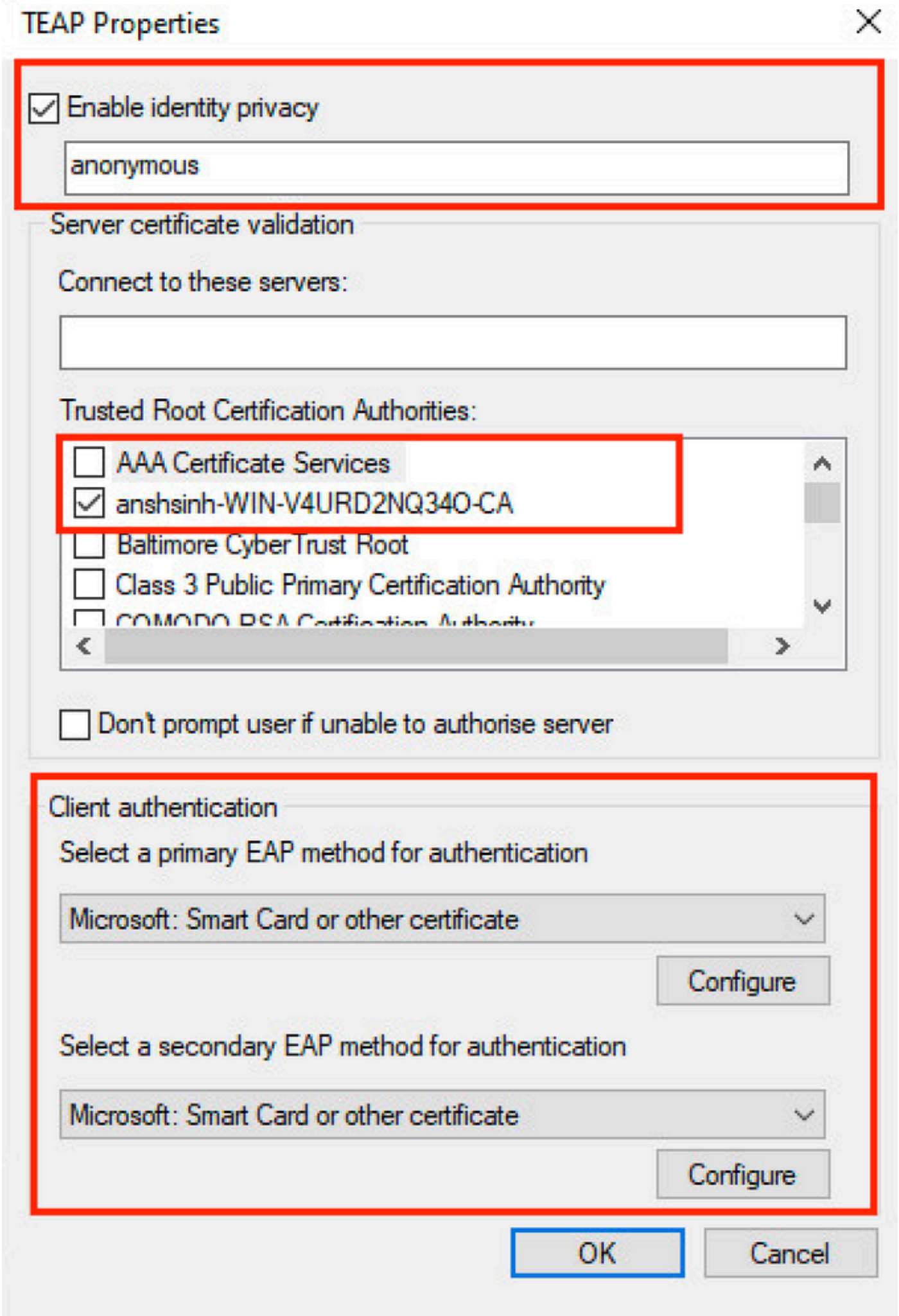
1.导航到控制面板>网络和共享中心>更改适配器设置，然后右键单击LAN连接>属性。单击 Authentication 选项卡。

2.单击Authentication下拉列表并选择Microsoft EAP-TEAP。


pciPassthru0 Properties
Networking
Authentication
Select this option to provide authenticated network access for this Ethernet adapter.
Enable IEEE 802.1X authentication
Choose a network authentication method:
Microsoft: EAP-TEAP
Settings
Remember my credentials for this connection each time I'm logged on
Fall-back to unauthorised network access
Additional Settings...
OK
Cancel

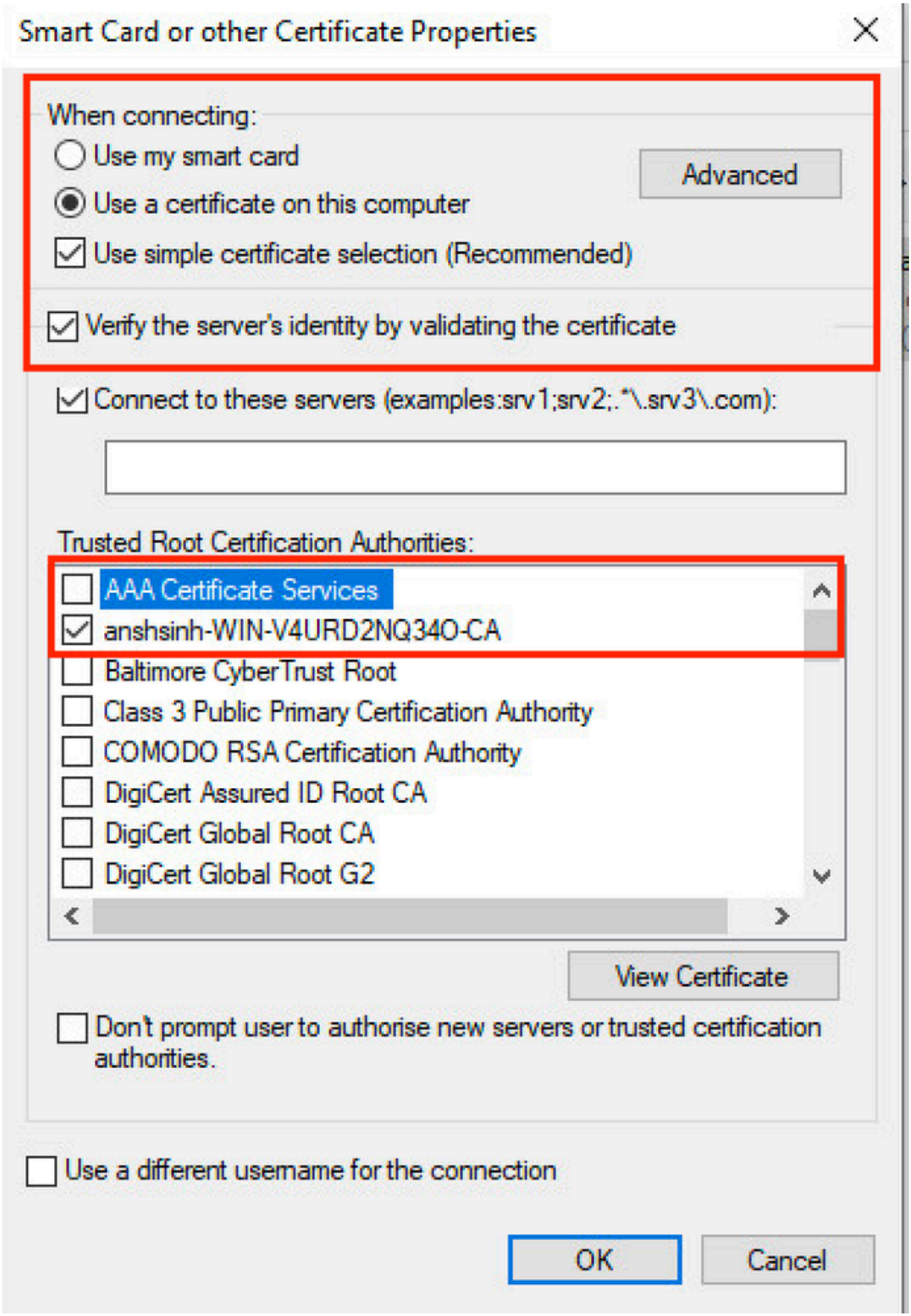
3.单击 Settings 按钮。

a. 使用anonymous保持启用身份隐私处于启用状态 作为身份。
b. 在受信任的根证书颁发机构下，在根CA服务器旁边放置一个复选标记，此证书用于签署ISE PSN上的EAP身份验证证书。


TEAP Properties
Enable identity privacy
anonymous
Server certificate validation
Connect to these servers:
Trusted Root Certification Authorities:
AAA Certificate Services
anshsinh-WIN-V4URD2NQ34O-CA
Baltimore CyberTrust Root
Class 3 Public Primary Certification Authority
Don't prompt user if unable to authorise server
Client authentication
Select a primary EAP method for authentication
Microsoft: Smart Card or other certificate
Configure
Select a secondary EAP method for authentication
Microsoft: Smart Card or other certificate
Configure
OK
Cancel

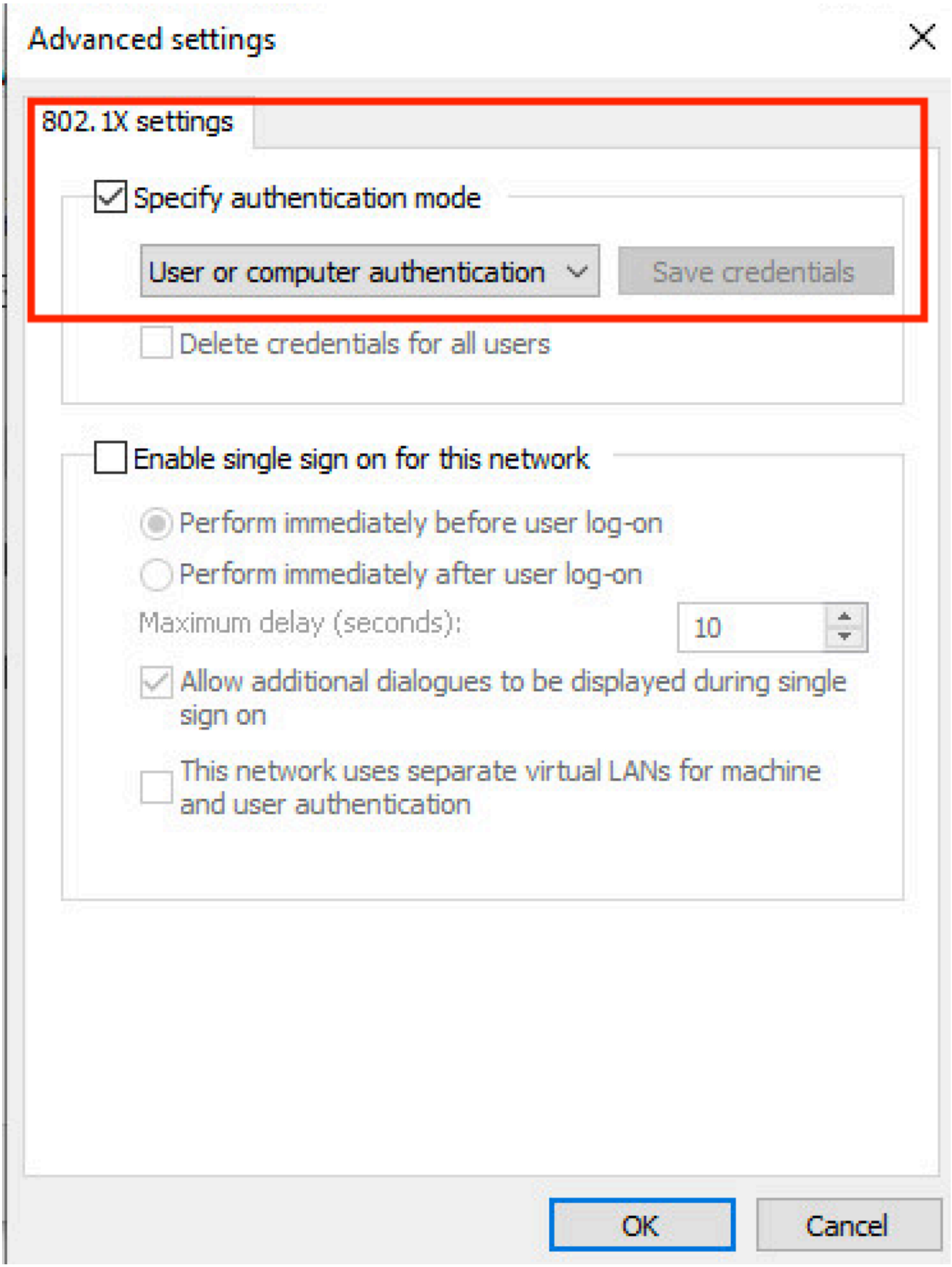
4.在Client Authentication下，选择Microsoft身份验证的EAP方法：其他证书的智能卡。

5.对于每个EAP方法下拉列表，单击Configure按钮并根据要求进行修改，然后单击OK。


Smart Card or other Certificate Properties
When connecting:
Use my smart card
Use a certificate on this computer
Advanced
Use simple certificate selection (Recommended)
Verify the server's identity by validating the certificate
Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):
Trusted Root Certification Authorities:
AAA Certificate Services
anshsinh-WIN-V4URD2NQ34O-CA
Baltimore CyberTrust Root
Class 3 Public Primary Certification Authority
COMODO RSA Certification Authority
DigiCert Assured ID Root CA
DigiCert Global Root CA
DigiCert Global Root G2
View Certificate
Don't prompt user to authorise new servers or trusted certification authorities.
Use a different username for the connection
OK
Cancel

6.单击“其他设置” 按钮。

a. 启用指定身份验证模式。
b. 将下拉菜单设置为适当的设置。
c. 选择User or computer authentication，以便两者均通过身份验证，然后单击OK。

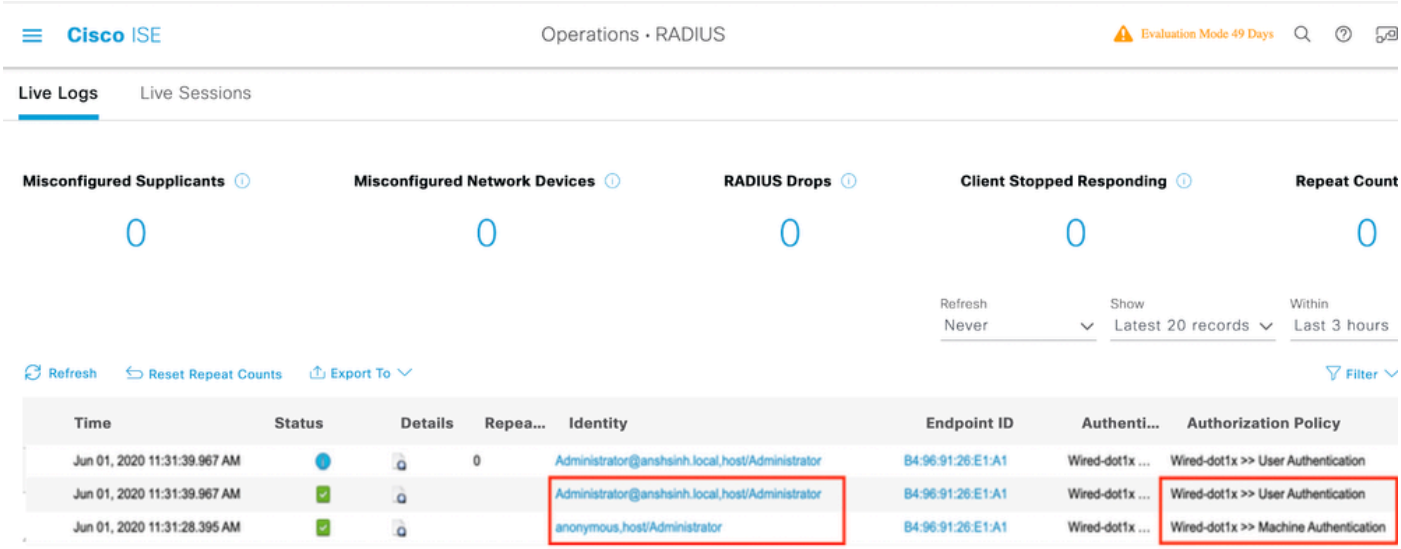

Advanced settings
802.1X settings
Specify authentication mode
User or computer authentication
Save credentials
Delete credentials for all users
Enable single sign on for this network
Perform immediately before user log-on
Perform immediately after user log-on
Maximum delay (seconds):
10
Allow additional dialogues to be displayed during single sign on
This network uses separate virtual LANs for machine and user authentication
OK
Cancel

验证

您可以重新启动Windows 10计算机，也可以先注销，然后再登录。显示Windows登录屏幕时，会触发计算机身份验证。

在实时日志中，可以在身份字段中看到匿名主机/管理员（此示例显示计算机名称）。您看到anonymous，因为您已在上方配置了身份隐私的请求方。

当您使用凭证登录到PC时，您会看到实时日志为Administrator@example.local，主机/管理员。这是EAP链，其中用户和机器身份验证都在一个EAP会话中发生。



详细的身份验证报告

在Live Log Details中，计算机身份验证只显示一个条目，但是，链接用户和计算机身份验证显示两个条NACRadiusUsername目（一个用于用户，一个用于计算机）。 此外，您在Authentication Details部分下看到，TEAP(EAP-TLS)已用于身份验证协议。如果将MSCHAPv2用于计算机和用户身份验证，则身份验证协议显示TEAP(Microsoft:安全密码(EAP-MSCHAP v2.)

计算机身份验证

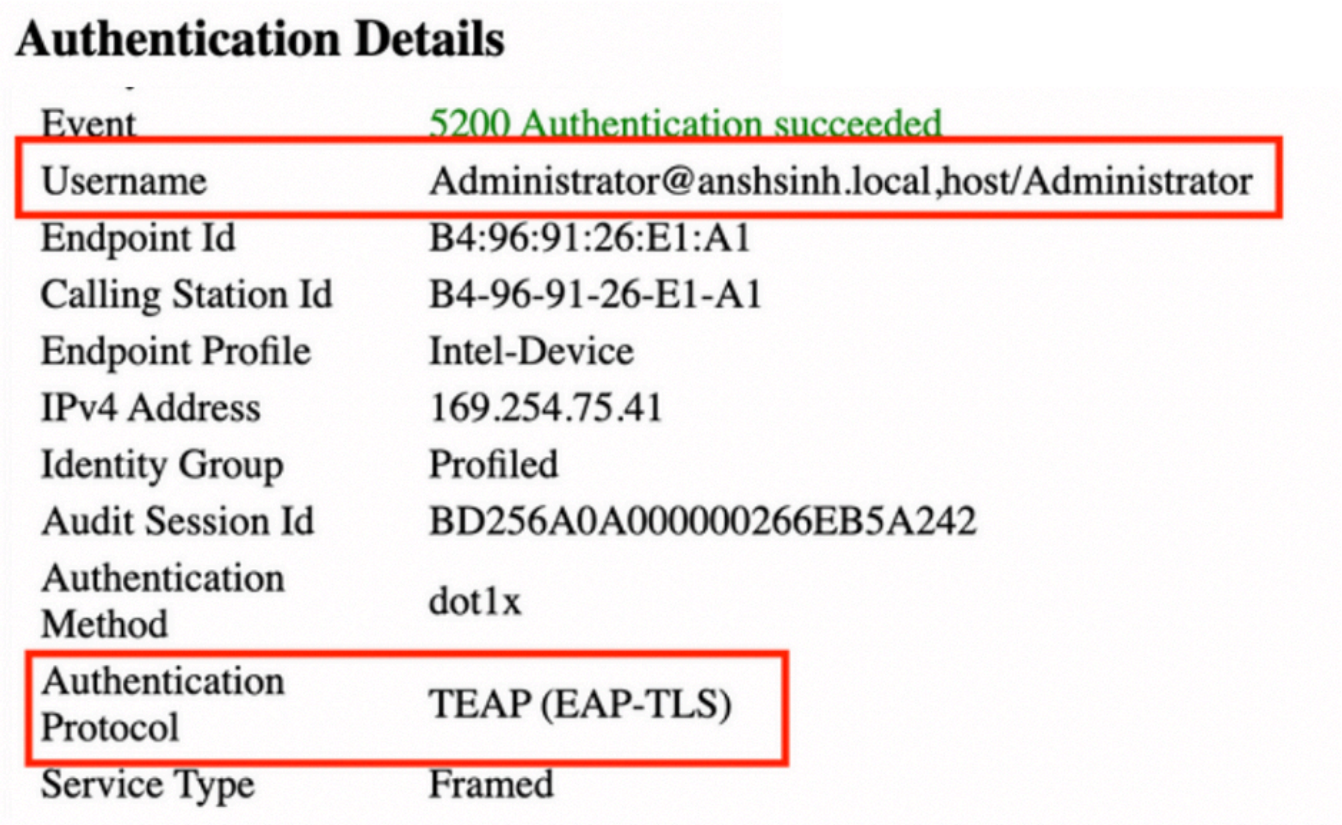
Authentication Details

Event	5200 Authentication succeeded
Username	anonymous,host/Administrator
Endpoint Id	B4:96:91:26:E1:A1
Calling Station Id	B4-96-91-26-E1-A1
Endpoint Profile	Intel-Device
IPv4 Address	169.254.75.41
Identity Group	Profiled
Audit Session Id	BD256A0A000000266EB5A242
Authentication Method	dot1x
Authentication Protocol	TEAP (EAP-TLS)
Service Type	Framed

Other Attributes

UseCase	Eap Chaining
NACRadiusUserName	host/Administrator
SelectedAuthenticationIdentityStores	cert_profile
AuthenticationStatus	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatchedRule	Machine Authentication
Serial Number	47 00 00 00 1C 84 F9 DB 39 FA 16 4F EB 00 00 00 00 00 1C
EndPointMACAddress	B4-96-91-26-E1-A1
EapChainingResult	User failed and machine succeeded

用户和机器身份验证



Authentication Details

Event	5200 Authentication succeeded
Username	Administrator@anshsinh.local,host/Administrator
Endpoint Id	B4:96:91:26:E1:A1
Calling Station Id	B4-96-91-26-E1-A1
Endpoint Profile	Intel-Device
IPv4 Address	169.254.75.41
Identity Group	Profiled
Audit Session Id	BD256A0A000000266EB5A242
Authentication Method	dot1x
Authentication Protocol	TEAP (EAP-TLS)
Service Type	Framed

Other Attributes

UseCase	Eap Chaining
NACRadiusUserName	Administrator@anshsinh.local
NACRadiusUserName	host/Administrator
SelectedAuthenticationIdentityStores	cert_profile
AuthenticationStatus	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatchedRule	User Authentication
Serial Number	47 00 00 00 1C 84 F9 DB 39 FA 16 4F EB 00 00 00 00 00 1C
EndPointMACAddress	B4-96-91-26-E1-A1
EapChainingResult	User and machine both succeeded

故障排除

您必须在ISE上启用这些调试：

- 运行时AAA
- nsf
- NSF会话
- Active Directory（排除ISE和AD之间的故障）

在Windows上，您可以检查事件查看器日志。

实时日志分析

计算机身份验证

<#root>

```
11001 Received RADIUS Access-Request
11017 RADIUS created a new session
...
...
11507 Extracted EAP-Response/Identity

12756 Prepared EAP-Request proposing TEAP with challenge

...
...

12758 Extracted EAP-Response containing TEAP challenge-response and accepting TEAP 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
12809 Prepared TLS CertificateRequest message
...
...
12811 Extracted TLS Certificate message containing client certificate
12812 Extracted TLS ClientKeyExchange message
12813 Extracted TLS CertificateVerify message
12804 Extracted TLS Finished message
12801 Prepared TLS ChangeCipherSpec message
12802 Prepared TLS Finished message
12816 TLS handshake succeeded
...
...

11559 Client certificate was requested but not received inside the tunnel. Will continue with inner meth
11620 TEAP full handshake finished successfully
```

```
...
...

11627 Starting EAP chaining
11573 Selected identity type 'User'


11564 TEAP inner method started
11521 Prepared EAP-Request/Identity for inner EAP method
...
...
11567 Identity type provided by client is equal to requested
11522 Extracted EAP-Response/Identity for inner EAP method

11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge


11596 Prepared EAP-Request with another TEAP challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
...
...

11515 Supplicant declined inner EAP method selected by Authentication Policy but did not proposed anothe
11520 Prepared EAP-Failure for inner EAP method
11566 TEAP inner method finished with failure


22028 Authentication failed and the advanced options are ignored
33517 Sent TEAP Intermediate Result TLV indicating failure
11596 Prepared EAP-Request with another TEAP challenge
...
...

11574 Selected identity type 'Machine'
11564 TEAP inner method started


11521 Prepared EAP-Request/Identity for inner EAP method
...
...
11567 Identity type provided by client is equal to requested
11522 Extracted EAP-Response/Identity for inner EAP method

11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge


11596 Prepared EAP-Request with another TEAP challenge
...
...

12523 Extracted EAP-Response/NAK for inner method requesting to use EAP-TLS instead


12522 Prepared EAP-Request for inner method proposing EAP-TLS with challenge
12625 Valid EAP-Key-Name attribute received
11596 Prepared EAP-Request with another TEAP challenge
...
...
12524 Extracted EAP-Response containing EAP-TLS challenge-response for inner method and accepting EAP-T
12800 Extracted first TLS record; TLS handshake started
12545 Client requested EAP-TLS session ticket
```

12546 The EAP-TLS session ticket received from supplicant. Inner EAP-TLS does not support stateless ses
12805 Extracted TLS ClientHello message
12806 Prepared TLS ServerHello message
12807 Prepared TLS Certificate message
12808 Prepared TLS ServerKeyExchange message
12809 Prepared TLS CertificateRequest message
12527 Prepared EAP-Request for inner method with another EAP-TLS challenge
...
...
12571 ISE will continue to CRL verification if it is configured for specific CA - certificate for Users
12811 Extracted TLS Certificate message containing client certificate
12812 Extracted TLS ClientKeyExchange message
12813 Extracted TLS CertificateVerify message
12804 Extracted TLS Finished message
12801 Prepared TLS ChangeCipherSpec message
12802 Prepared TLS Finished message
12816 TLS handshake succeeded
12509 EAP-TLS full handshake finished successfully
...
...
12527 Prepared EAP-Request for inner method with another EAP-TLS challenge
11596 Prepared EAP-Request with another TEAP challenge
...
...
61025 Open secure connection with TLS peer
15041 Evaluating Identity Policy
22072 Selected identity source sequence - forAD1
22070 Identity name is taken from certificate attribute

22037 Authentication Passed
12528 Inner EAP-TLS authentication succeeded

11519 Prepared EAP-Success for inner EAP method
11565 TEAP inner method finished successfully

...
...
33516 Sent TEAP Intermediate Result TLV indicating success
11596 Prepared EAP-Request with another TEAP challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
11595 Extracted EAP-Response containing TEAP challenge-response
11637 Inner method supports EMSK but the client provided only MSK. Allow downgrade as per configuration

11576 TEAP cryptobinding verification passed

...
...

15036 Evaluating Authorization Policy

24209 Looking up Endpoint in Internal Endpoints IDStore - anonymous,host/Administrator
24211 Found Endpoint in Internal Endpoints IDStore
11055 User name change detected for the session. Attributes for the session will be removed from the ca
15048 Queried PIP - Network Access.EapChainingResult
15016 Selected Authorization Profile - PermitAccess
33514 Sent TEAP Result TLV indicating success

...
...

11597 TEAP authentication phase finished successfully
11503 Prepared EAP-Success
11002 Returned RADIUS Access-Accept

用户和机器身份验证

<#root>

11001 Received RADIUS Access-Request
11017 RADIUS created a new session
...
...

12756 Prepared EAP-Request proposing TEAP with challenge

...
...

12758 Extracted EAP-Response containing TEAP challenge-response and accepting TEAP 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
12809 Prepared TLS CertificateRequest message
11596 Prepared EAP-Request with another TEAP challenge
...
...
12811 Extracted TLS Certificate message containing client certificate
12812 Extracted TLS ClientKeyExchange message
12813 Extracted TLS CertificateVerify message
12804 Extracted TLS Finished message
12801 Prepared TLS ChangeCipherSpec message
12802 Prepared TLS Finished message
12816 TLS handshake succeeded
11559 Client certificate was requested but not received inside the tunnel. Will continue with inner met

11620 TEAP full handshake finished successfully

11596 Prepared EAP-Request with another TEAP challenge
...
...
11595 Extracted EAP-Response containing TEAP challenge-response

11627 Starting EAP chaining

11573 Selected identity type 'User'

11564 TEAP inner method started

11521 Prepared EAP-Request/Identity for inner EAP method
11596 Prepared EAP-Request with another TEAP challenge
...
...
11567 Identity type provided by client is equal to requested
11522 Extracted EAP-Response/Identity for inner EAP method

11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge

11596 Prepared EAP-Request with another TEAP challenge
...
...

12523 Extracted EAP-Response/NAK for inner method requesting to use EAP-TLS instead

12522 Prepared EAP-Request for inner method proposing EAP-TLS with challenge
...
...
11595 Extracted EAP-Response containing TEAP challenge-response
12524 Extracted EAP-Response containing EAP-TLS challenge-response for inner method and accepting EAP-T
12800 Extracted first TLS record; TLS handshake started
12545 Client requested EAP-TLS session ticket
12546 The EAP-TLS session ticket received from supplicant. Inner EAP-TLS does not support stateless ses
12805 Extracted TLS ClientHello message
12806 Prepared TLS ServerHello message
12807 Prepared TLS Certificate message
12808 Prepared TLS ServerKeyExchange message
12809 Prepared TLS CertificateRequest message
12527 Prepared EAP-Request for inner method with another EAP-TLS challenge
...
...
12526 Extracted EAP-Response for inner method containing TLS challenge-response
12571 ISE will continue to CRL verification if it is configured for specific CA - certificate for Users
12811 Extracted TLS Certificate message containing client certificate
12812 Extracted TLS ClientKeyExchange message
12813 Extracted TLS CertificateVerify message
12804 Extracted TLS Finished message
12801 Prepared TLS ChangeCipherSpec message
12802 Prepared TLS Finished message
12816 TLS handshake succeeded
12509 EAP-TLS full handshake finished successfully
12527 Prepared EAP-Request for inner method with another EAP-TLS challenge
...
...
12526 Extracted EAP-Response for inner method containing TLS challenge-response
61025 Open secure connection with TLS peer
15041 Evaluating Identity Policy
22072 Selected identity source sequence - forAD1
22070 Identity name is taken from certificate attribute

22037 Authentication Passed

12528 Inner EAP-TLS authentication succeeded
11519 Prepared EAP-Success for inner EAP method

11565 TEAP inner method finished successfully

33516 Sent TEAP Intermediate Result TLV indicating success
11596 Prepared EAP-Request with another TEAP challenge
...
...
11595 Extracted EAP-Response containing TEAP challenge-response
11637 Inner method supports EMSK but the client provided only MSK. Allow downgrade as per configuration

11576 TEAP cryptobinding verification passed
11574 Selected identity type 'Machine'

11564 TEAP inner method started
...
...

11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge

11596 Prepared EAP-Request with another TEAP challenge
...
...

12523 Extracted EAP-Response/NAK for inner method requesting to use EAP-TLS instead

12522 Prepared EAP-Request for inner method proposing EAP-TLS with challenge

...
...

12524 Extracted EAP-Response containing EAP-TLS challenge-response for inner method and accepting EAP-TL

12800 Extracted first TLS record; TLS handshake started

12545 Client requested EAP-TLS session ticket

12546 The EAP-TLS session ticket received from supplicant. Inner EAP-TLS does not support stateless sess

12805 Extracted TLS ClientHello message
12806 Prepared TLS ServerHello message
12807 Prepared TLS Certificate message
12808 Prepared TLS ServerKeyExchange message
12809 Prepared TLS CertificateRequest message
12527 Prepared EAP-Request for inner method with another EAP-TLS challenge
...
...
12526 Extracted EAP-Response for inner method containing TLS challenge-response
12571 ISE will continue to CRL verification if it is configured for specific CA - certificate for Users
12811 Extracted TLS Certificate message containing client certificate
12812 Extracted TLS ClientKeyExchange message
12813 Extracted TLS CertificateVerify message
12804 Extracted TLS Finished message
12801 Prepared TLS ChangeCipherSpec message
12802 Prepared TLS Finished message
12816 TLS handshake succeeded
12509 EAP-TLS full handshake finished successfully
12527 Prepared EAP-Request for inner method with another EAP-TLS challenge
11596 Prepared EAP-Request with another TEAP challenge

```
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
11595 Extracted EAP-Response containing TEAP challenge-response
12526 Extracted EAP-Response for inner method containing TLS challenge-response
61025 Open secure connection with TLS peer
15041 Evaluating Identity Policy
22072 Selected identity source sequence - forAD1
22070 Identity name is taken from certificate attribute

22037 Authentication Passed
12528 Inner EAP-TLS authentication succeeded
11519 Prepared EAP-Success for inner EAP method

11565 TEAP inner method finished successfully
33516 Sent TEAP Intermediate Result TLV indicating success
11596 Prepared EAP-Request with another TEAP challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
11595 Extracted EAP-Response containing TEAP challenge-response
11637 Inner method supports EMSK but the client provided only MSK. Allow downgrade as per configuration
11576 TEAP cryptobinding verification passed

15036 Evaluating Authorization Policy

24209 Looking up Endpoint in Internal Endpoints IDStore - Administrator@example.local,host/Administrato
24211 Found Endpoint in Internal Endpoints IDStore
11055 User name change detected for the session. Attributes for the session will be removed from the ca
15048 Queried PIP - Network Access.EapChainingResult
15016 Selected Authorization Profile - PermitAccess
33514 Sent TEAP Result TLV indicating success
11596 Prepared EAP-Request with another TEAP challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
11595 Extracted EAP-Response containing TEAP challenge-response

11597 TEAP authentication phase finished successfully
11503 Prepared EAP-Success
11002 Returned RADIUS Access-Accept
```

相关信息

- 隧道可扩展身份验证协议(TEAP)版本1
- 无需服务器端状态的传输层安全(TLS)会话恢复
- 了解AnyConnect NAM和ISE上的EAP-FAST和链接实施
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。