تكوين توصيل EAP باستخدام TEAP

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين ISE ومطالب Windows لتوصيل بروتوكول المصادقة المتوسع (EAP) مع TEAP.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- محرك خدمات كشف الهوية (ISE)
- تكوين ملتمس Windows

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- ISE الإصدار 3.0 من Cisco
- نظام التشغيل Windows 10 Build 2004
- معرفة بروتوكول المصادقة المتوسع المستند إلى البروتوكول (TEAP)

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

TEAP هو أسلوب بروتوكول مصادقة متوسع يستند إلى نفق وينشئ نفقا آمنا وينفذ أساليب EAP الأخرى تحت حماية ذلك النفق المضمون.

تحدث مصادقة TEAP في مرحلتين بعد طلب معرف EAP الأولي/تبادل الاستجابة. وفي المرحلة الأولى، يستخدم فريق التكنولوجيا والتقييم الاقتصادي مصافحة TLS لتوفير تبادل مفاتيح مصدق عليه وإنشاء نفق محمي. وبمجرد إنشاء النفق، تبدأ المرحلة الثانية بمشاركة النظير والخادم في مزيد من المحادثات لإنشاء المصادقة المطلوبة وسياسات التخويل.

يدعم Cisco ISE 2.7 والإصدارات الأحدث بروتوكول TEAP. يتم إستخدام كائنات type-length-value (TLV) داخل النفق لنقل البيانات المتعلقة بالمصادقة بين نظير EAP وخادم EAP.

تمدق Microsoft دعم TEAP في الإصدار 10 من Windows 2004 الذي تم إصداره في مايو 2020.

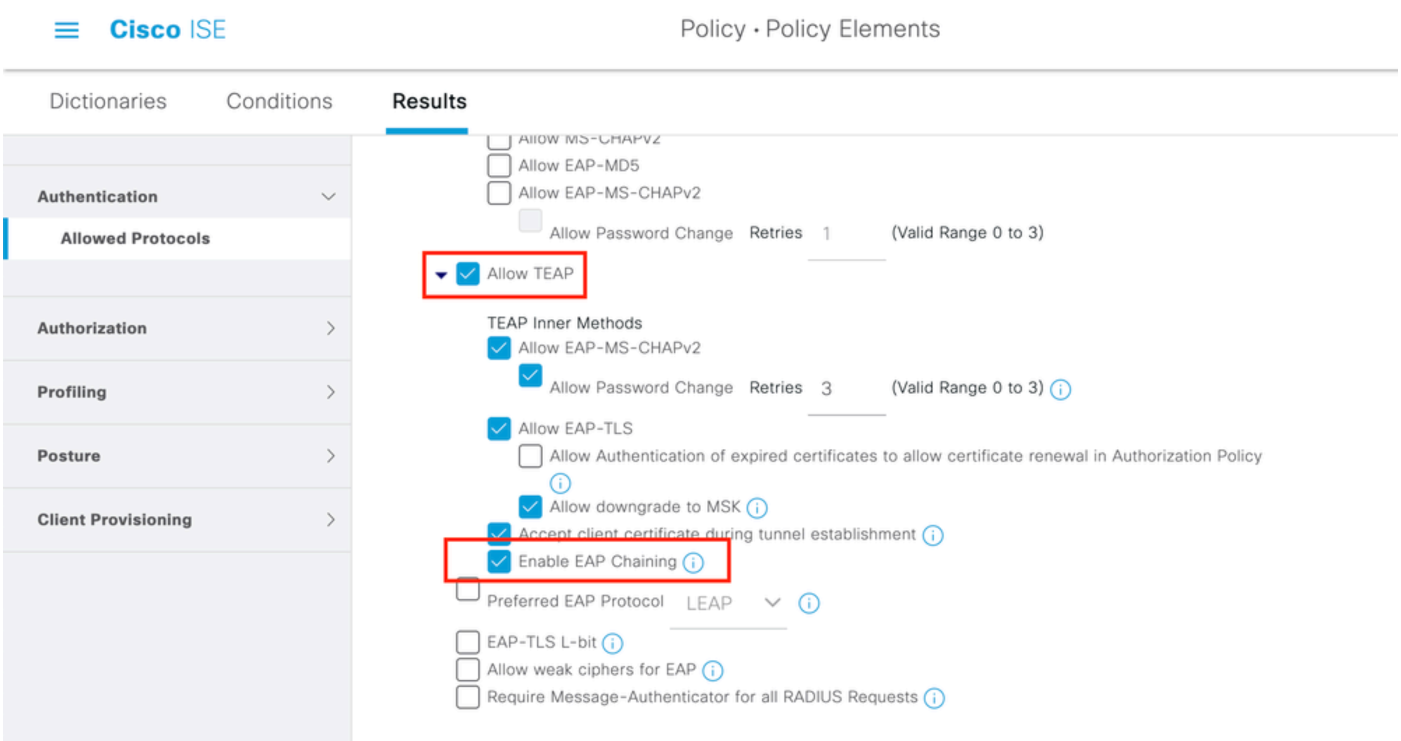
يسمح تسلسل EAP للمستخدم وومصادقة الجهاز خلال جلسة EAP/RADIUS واحدة بدلا من جلستين منفصلتين. فيما سبق، لتحقيق ذلك، كنت تحتاج إلى وحدة Cisco AnyConnect NAM النمطية واستخدام EAP-FAST على طالب Windows حيث أن طالب Windows الأصلي لم يدعم هذا. الآن، يمكنك إستخدام ملتمس Windows الأصلي لإجراء توصيل EAP باستخدام ISE 2.7 باستخدام TEAP.

التكوين

تكوين Cisco ISE

الخطوة 1. تحتاج إلى تحرير البروتوكولات المسموح بها لتمكين توصيل TEAP و EAP.

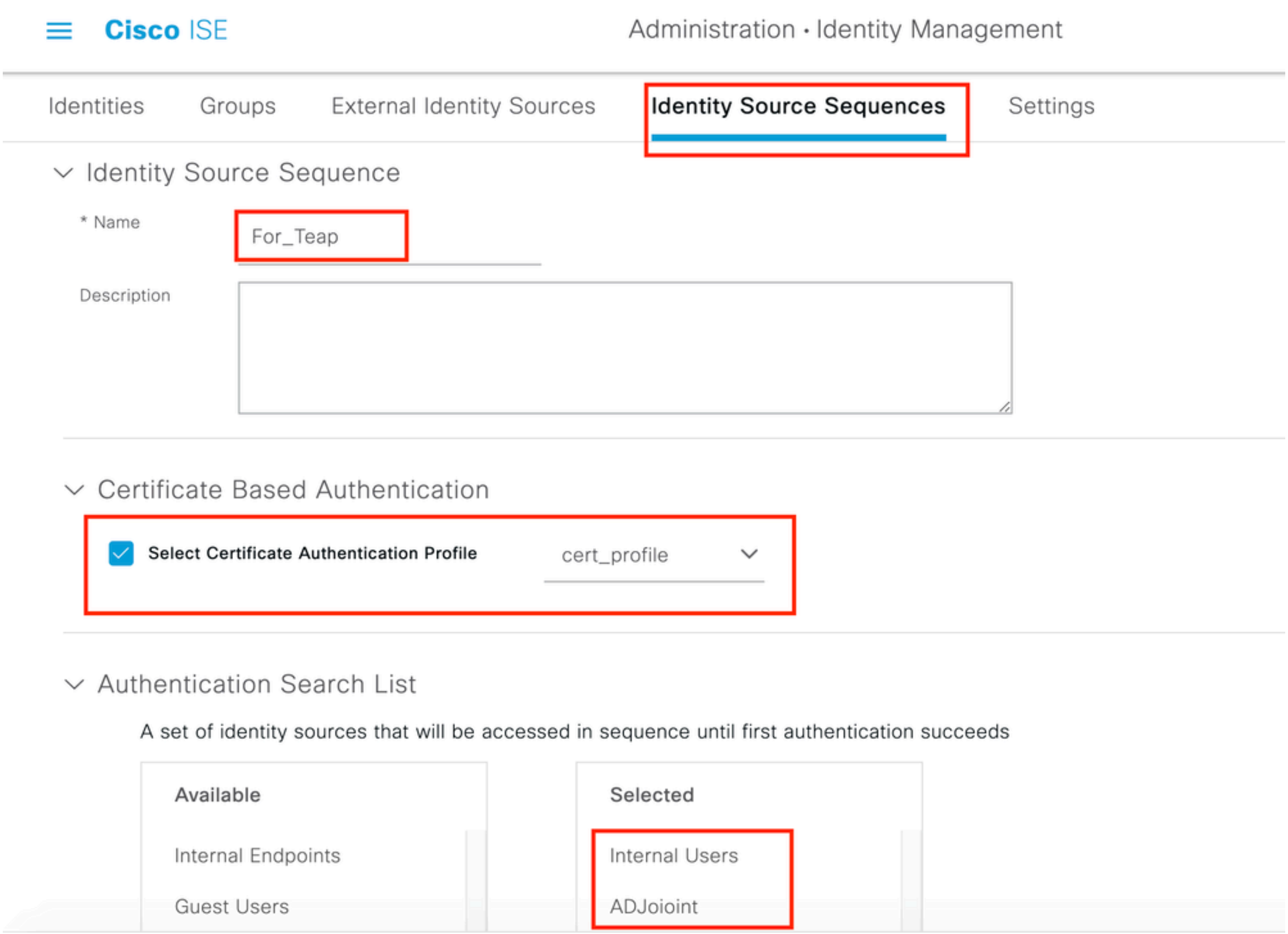
انتقل إلى ISE > Policy > Policy Elements > Results > Authentication > Allowed Protocols > Add New. تحديد خانات الاختيار الخاصة بتوصيل EAP و EAP.



□ Allow MS-CHAPv2
□ Allow EAP-MD5
□ Allow EAP-MS-CHAPv2
□ Allow Password Change Retries 1 (Valid Range 0 to 3)
☑ Allow TEAP
TEAP Inner Methods
☑ Allow EAP-MS-CHAPv2
☑ Allow Password Change Retries 3 (Valid Range 0 to 3)
☑ Allow EAP-TLS
□ Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy
☑ Allow downgrade to MSK
☑ Accept client certificate during tunnel establishment
☑ Enable EAP Chaining
□ Preferred EAP Protocol LEAP
□ EAP-TLS L-bit
□ Allow weak ciphers for EAP
□ Require Message-Authenticator for all RADIUS Requests

الخطوة 2. قم بإنشاء ملف تعريف ترخيص وإضافته إلى تسلسل مصدر الهوية.

انتقل إلى ISE > Administration > Identities > identity Source Sequence واختر ملف تعريف الشهادة.


Cisco ISE
Administration · Identity Management
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings

Identity Source Sequence
* Name For_Teap
Description

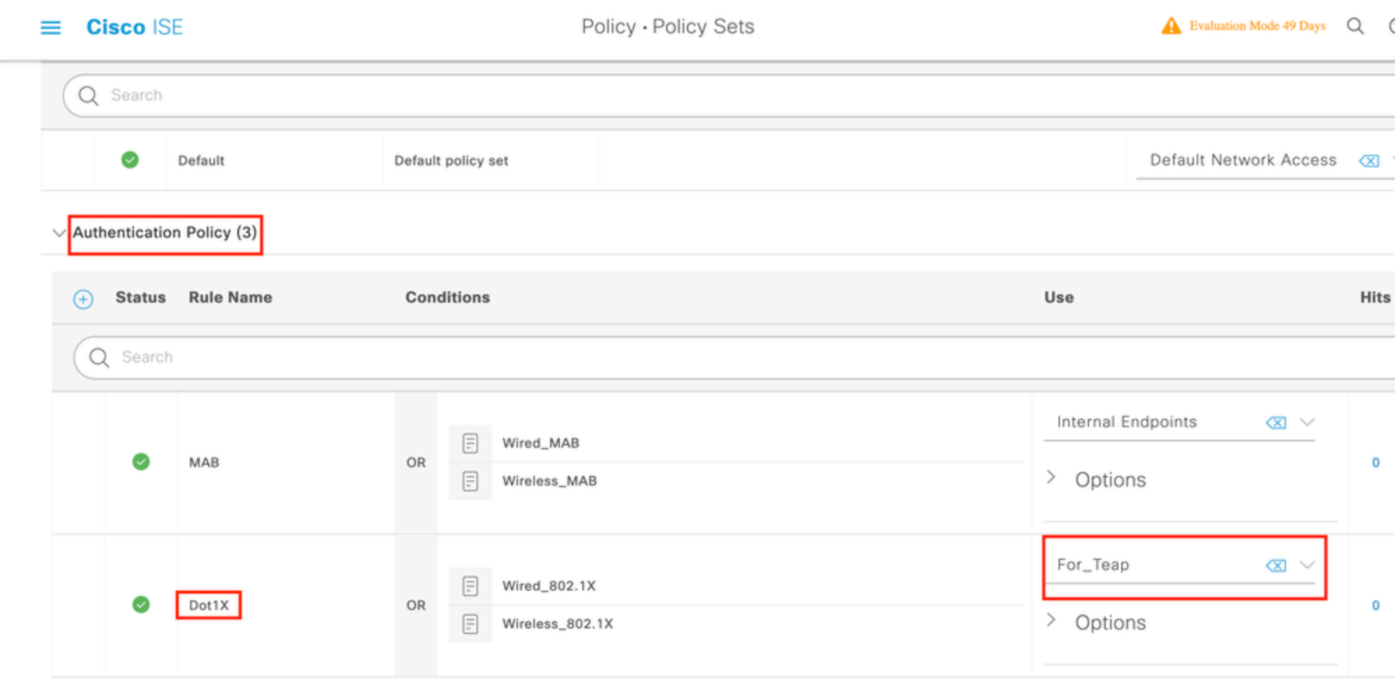
Certificate Based Authentication
☑ Select Certificate Authentication Profile cert_profile

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

Available	Selected
Internal Endpoints	Internal Users
Guest Users	ADJoioint

الخطوة 3. يجب إستدعاء هذا التسلسل في نهج المصادقة.

انتقل إلى ISE > Policy > Policy Sets. Choose the Policy Set forDot1x > Authentication Policy واختر تسلسل مصدر الهوية الذي تم إنشاؤه في الخطوة 2.



Cisco ISE — Policy · Policy Sets — Evaluation Mode 49 Days

Search

	Default	Default policy set	Default Network Access

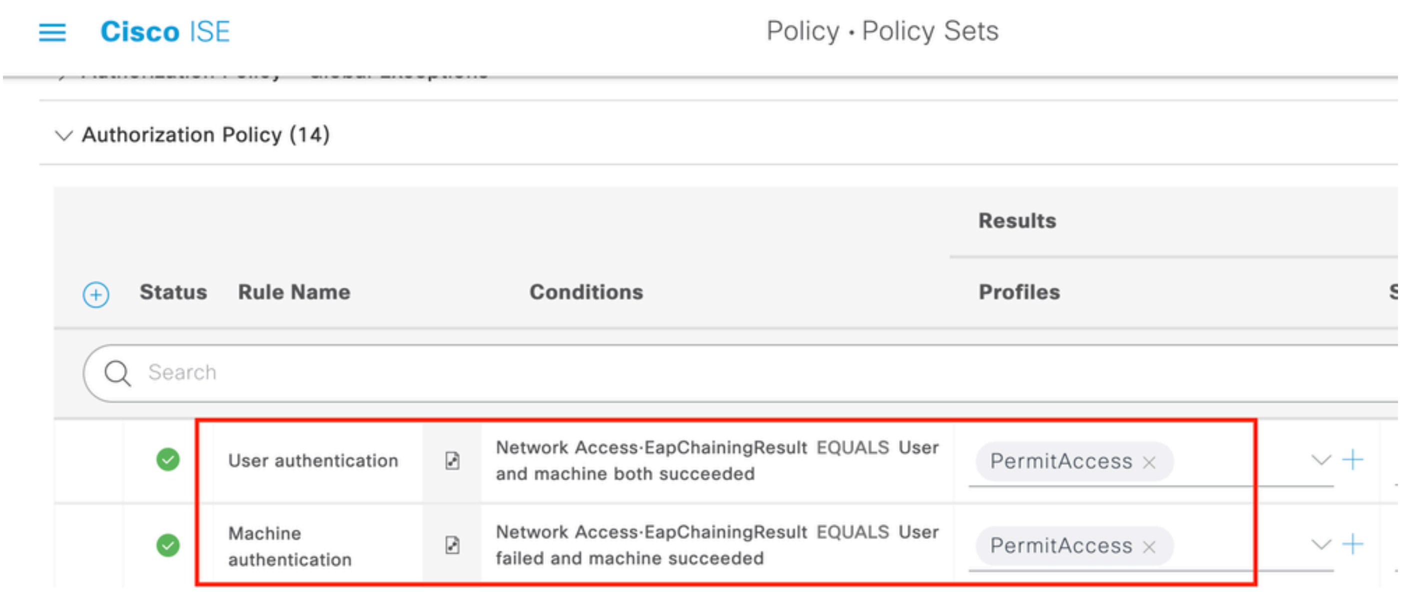
Authentication Policy (3)

Status	Rule Name		Conditions	Use	Hits
✓	MAB	OR	Wired_MAB Wireless_MAB	Internal Endpoints Options	0
✓	Dot1X	OR	Wired_802.1X Wireless_802.1X	For_Teap Options	0

الخطوة 4. تحتاج الآن إلى تعديل نهج التخويل ضمن مجموعة نهج dot1x.

انتقل إلى ISE > Policy > Policy Sets. Choose the Policy Set for Dot1x > Authentication Policy.

تحتاج إلى إنشاء قاعدتين. تتحقق القاعدة الأولى من مصادقة الجهاز ولكن المستخدم غير مصدق. تتحقق القاعدة الثانية من مصادقة كل من المستخدم والجهاز.



Cisco ISE — Policy · Policy Sets

Authorization Policy (14)

Status	Rule Name	Conditions	Results Profiles
✓	User authentication	Network Access·EapChainingResult EQUALS User and machine both succeeded	PermitAccess
✓	Machine authentication	Network Access·EapChainingResult EQUALS User failed and machine succeeded	PermitAccess

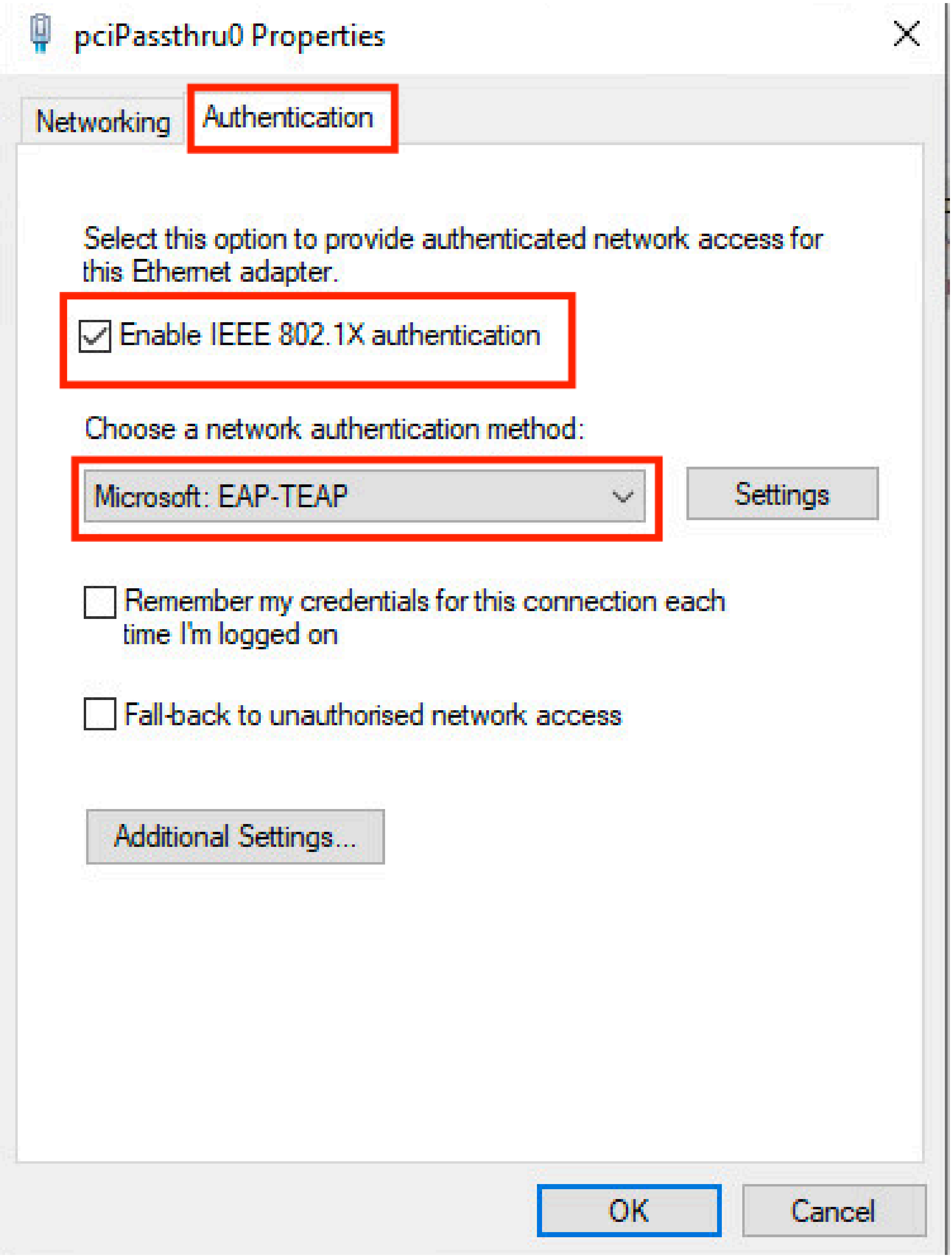
يؤدي هذا إلى اكتمال التكوين من جانب خادم ISE.

تكوين العميل الأصلي ل Windows

قم بتكوين إعداد المصادقة السلكية في هذا المستند.

انتقل إلى Control Panel > Network and Sharing Center > Change Adapter Settings وانقر بزر الماوس الأيمن LAN Connection > Properties. انقر فوق Authentication علامة التبويب.

الخطوة 1. انقر فوق Authenticationالمنسدل واختر Microsoft EAP-TEAP.



pciPassthru0 Properties

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

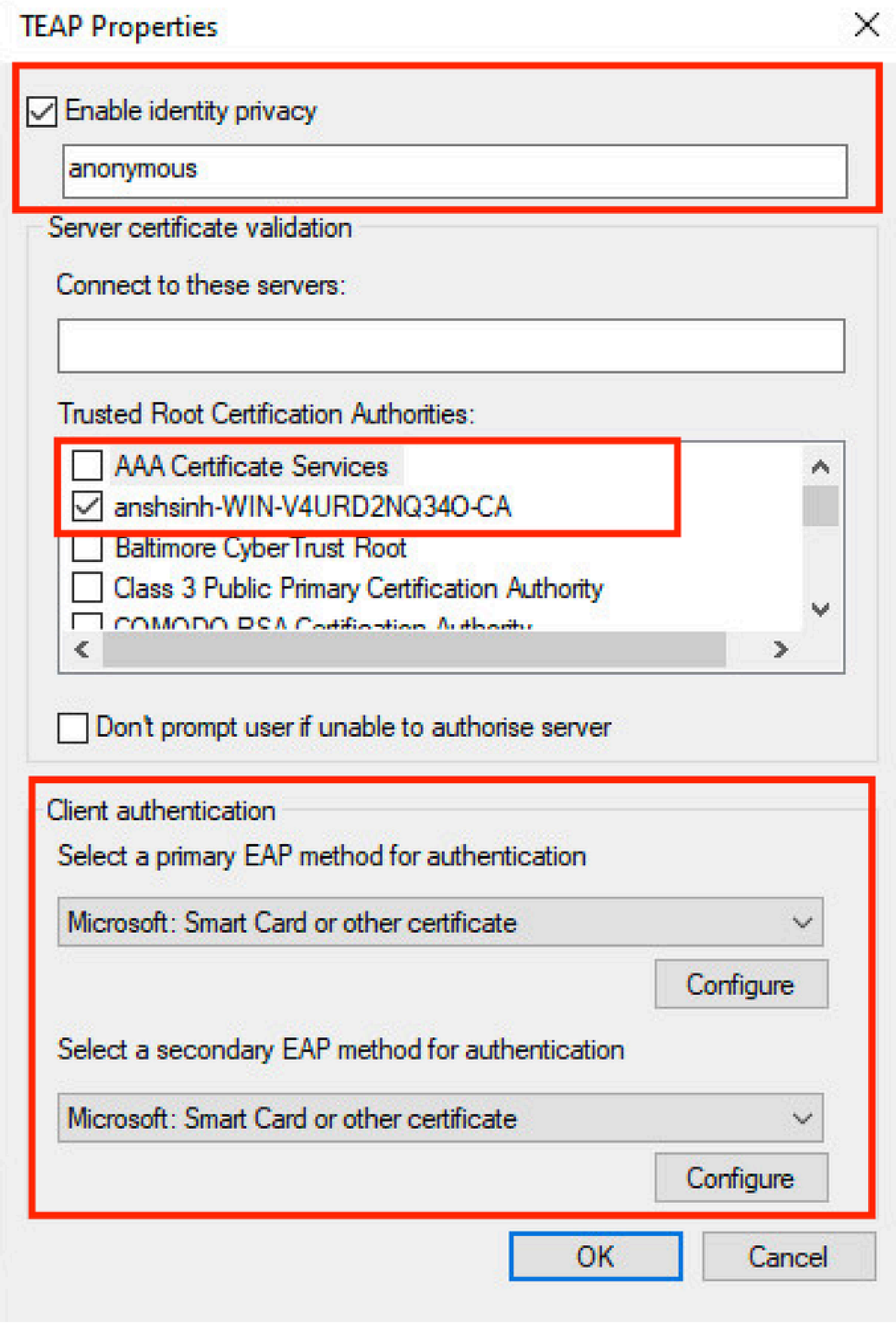
□ Remember my credentials for this connection each time I'm logged on

□ Fall-back to unauthorised network access

الخطوة 2. انقر علىSettings الزر الموجود بجوار TEAP.

1. الاحتفاظ Enable Identity Privacy بإمكانية التمكين anonymous كهوية.

- ضع علامة إختيار بجوار خادم (خوادم) CA الجذر تحت مراجع التصديق الجذر الموثوق بها التي تستخدم لتوقيع شهادة مصادقة EAP على ISE PSN.



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
☐ COMODO RSA 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

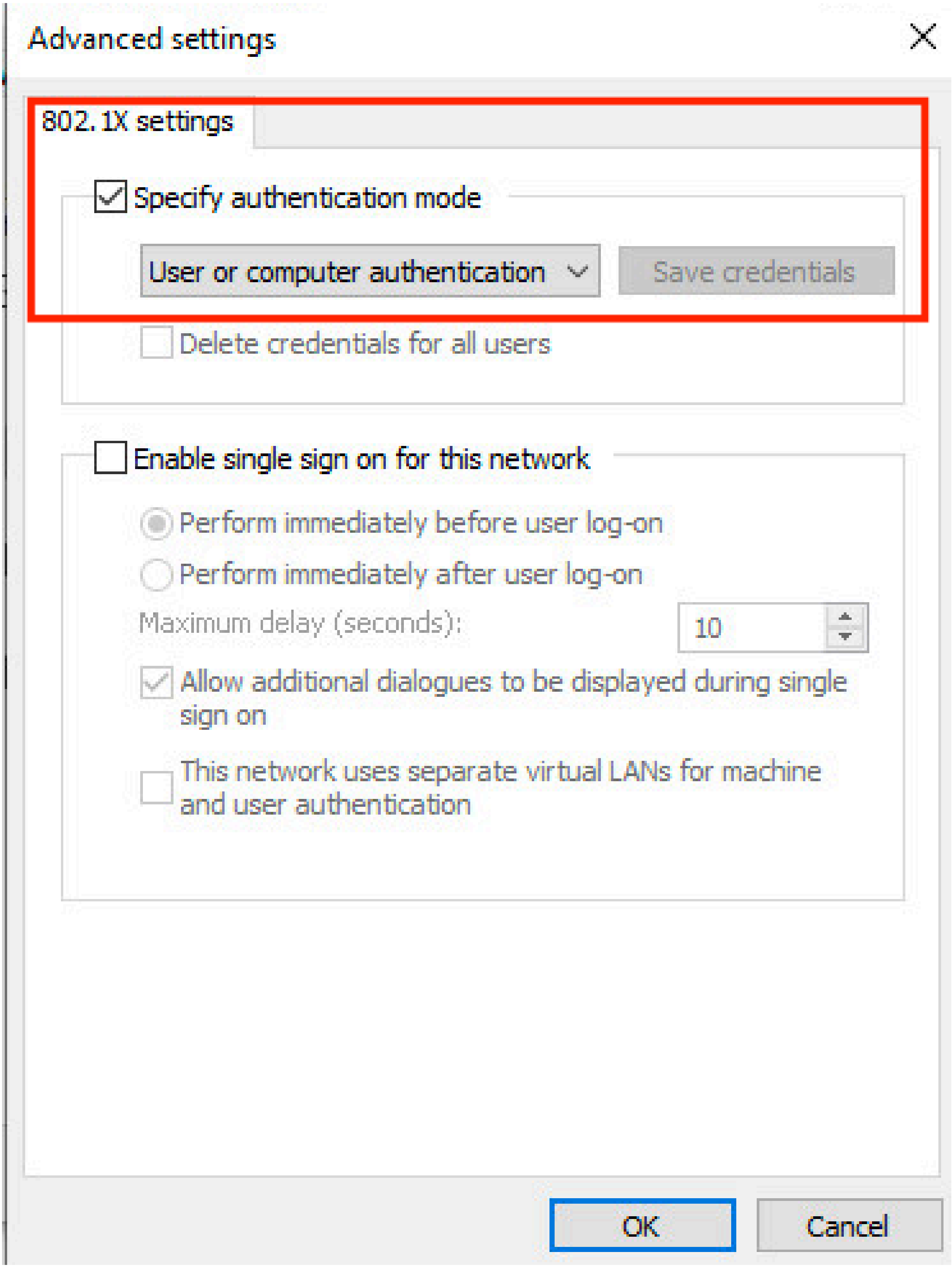
Select a secondary EAP method for authentication

Microsoft: Smart Card or other certificate

1. تمكين تحديد وضع المصادقة.

2. قم بتعيين القائمة المنسدلة إلى الإعداد المناسب.

3. أختر User or computer authentication بحيث يتم التصديق على كليهما وانقر OK.



☑ Specify authentication mode

User or computer authentication

□ 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

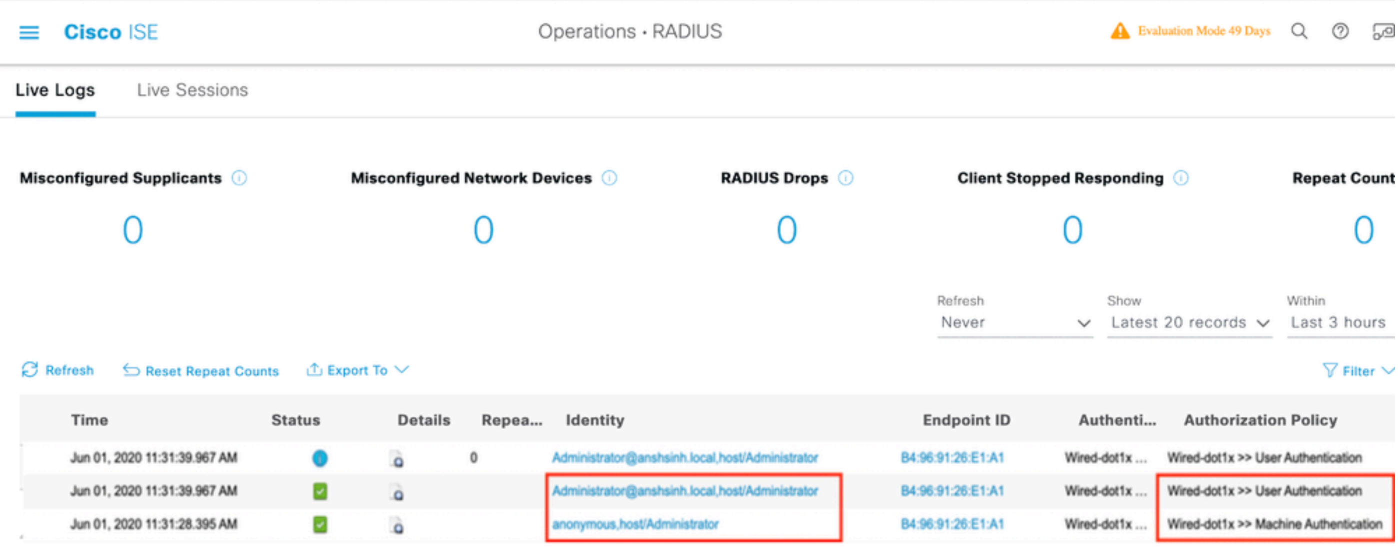
□ This network uses separate virtual LANs for machine and user authentication

التحقق من الصحة

يمكنك إعادة تشغيل جهاز Windows 10 أو يمكنك تسجيل الخروج ثم تسجيل الدخول. عند عرض شاشة تسجيل الدخول إلى Windows، يتم تشغيل مصادقة الجهاز.

في سجلات التشغيل المباشرة، ترى مجهول، مضيف/مسؤول (هنا هو اسم الجهاز) في حقل الهوية. يمكنك رؤية مجهول لأنك قمت بتكوين مطلب لخصوصية الهوية أعلاه.

عندما تقوم بتسجيل الدخول إلى الكمبيوتر باستخدام بيانات الاعتماد، يمكنك الاطلاع على ذلك في السجلات المباشرة على العنوان Administrator@example.local، المضيف/المسؤول. هذا هو التسلسل EAP حيث تحدث مصادقة كل من المستخدم والجهاز في جلسة EAP واحدة.



Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Count
0	0	0	0	0

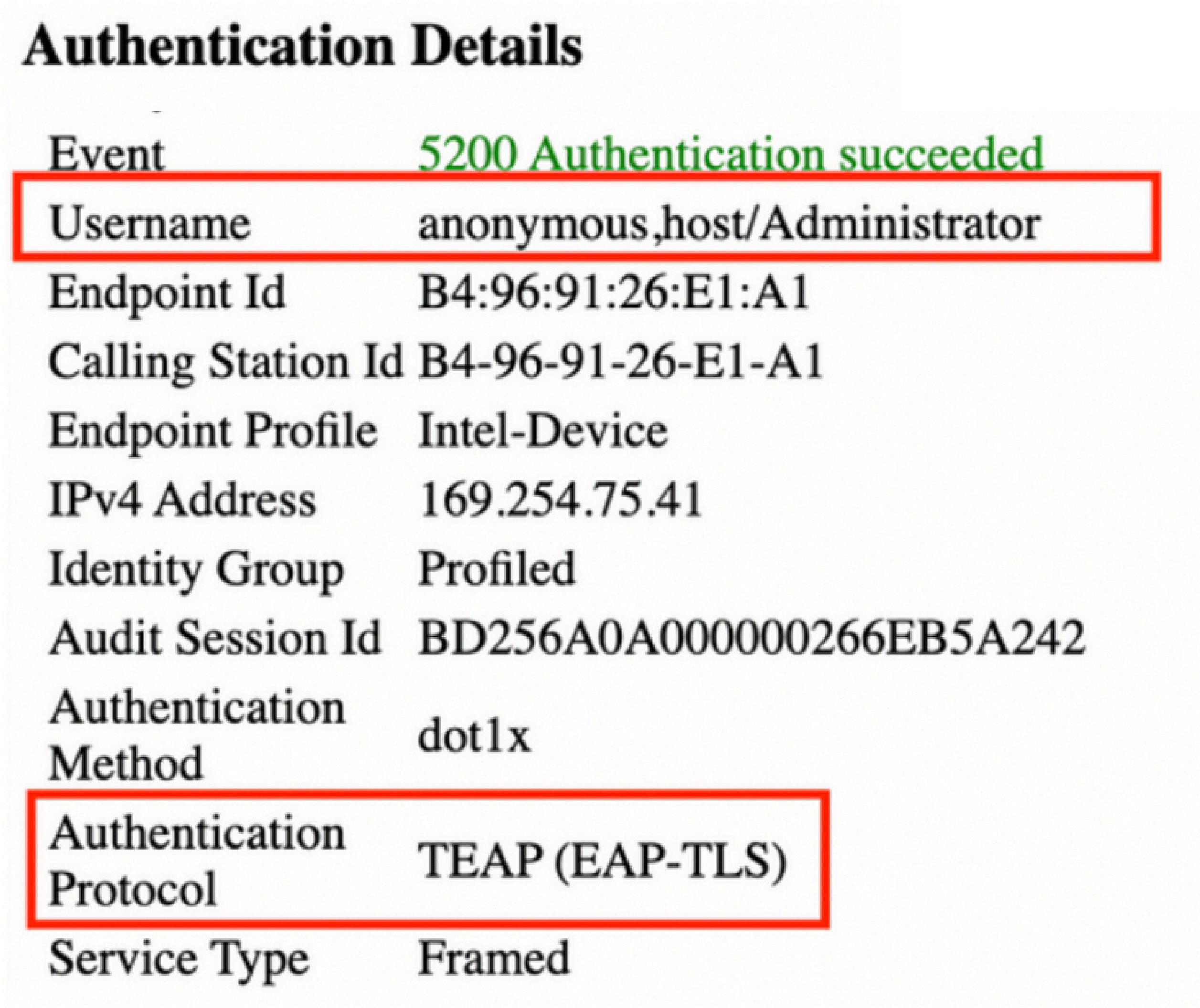
Refresh: Never
Show: Latest 20 records
Within: Last 3 hours

Time	Status	Details	Repea...	Identity	Endpoint ID	Authenti...	Authorization Policy
Jun 01, 2020 11:31:39.967 AM	●		0	Administrator@anshsinh.local,host/Administrator	B4:96:91:26:E1:A1	Wired-dot1x ...	Wired-dot1x >> User Authentication
Jun 01, 2020 11:31:39.967 AM	✓			Administrator@anshsinh.local,host/Administrator	B4:96:91:26:E1:A1	Wired-dot1x ...	Wired-dot1x >> User Authentication
Jun 01, 2020 11:31:28.395 AM	✓			anonymous,host/Administrator	B4:96:91:26:E1:A1	Wired-dot1x ...	Wired-dot1x >> Machine Authentication

تقرير المصادقة التفصيلي

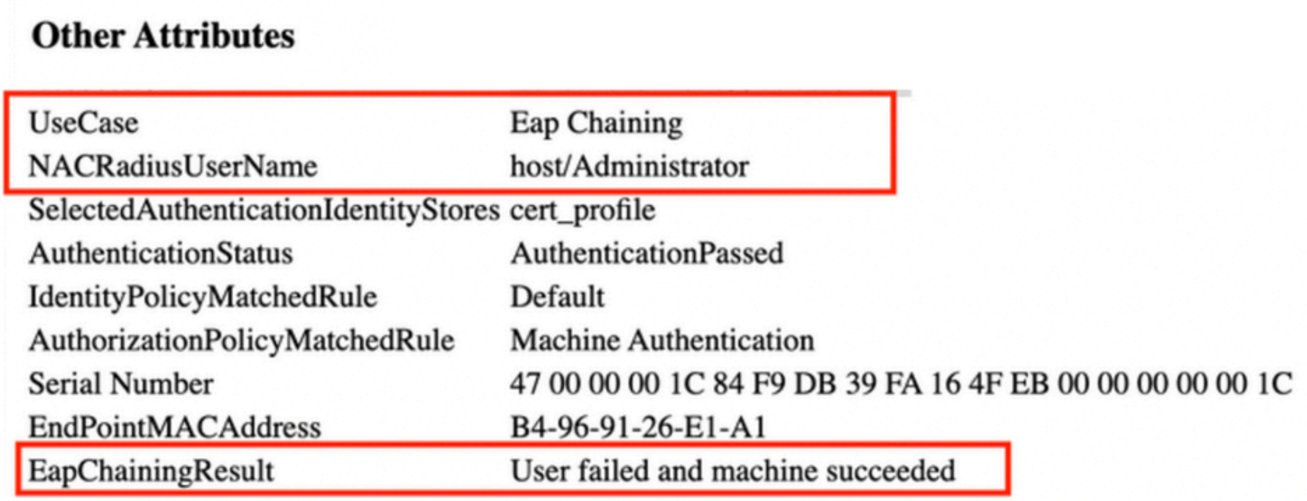
في تفاصيل سجل Live، تظهر مصادقات الجهاز NACRadiusUsername إدخالا واحدا فقط لكن المستخدم المقيد ومصادقة الجهاز تعرض إدخالين (واحد للمستخدم، وواحد للجهاز). أيضا، كما ترى تحت Authentication Details القسم، الذي TEAP (EAP-TLS) كان يستخدم Authentication Protocol. إذا كنت تستخدم MSCHAPv2 لمصادقة الجهاز والمستخدم، يظهر بروتوكول المصادقة TEAP (Microsoft: Secured password (EAP-MSCHAP v2)).

مصادقة الجهاز



Authentication Details

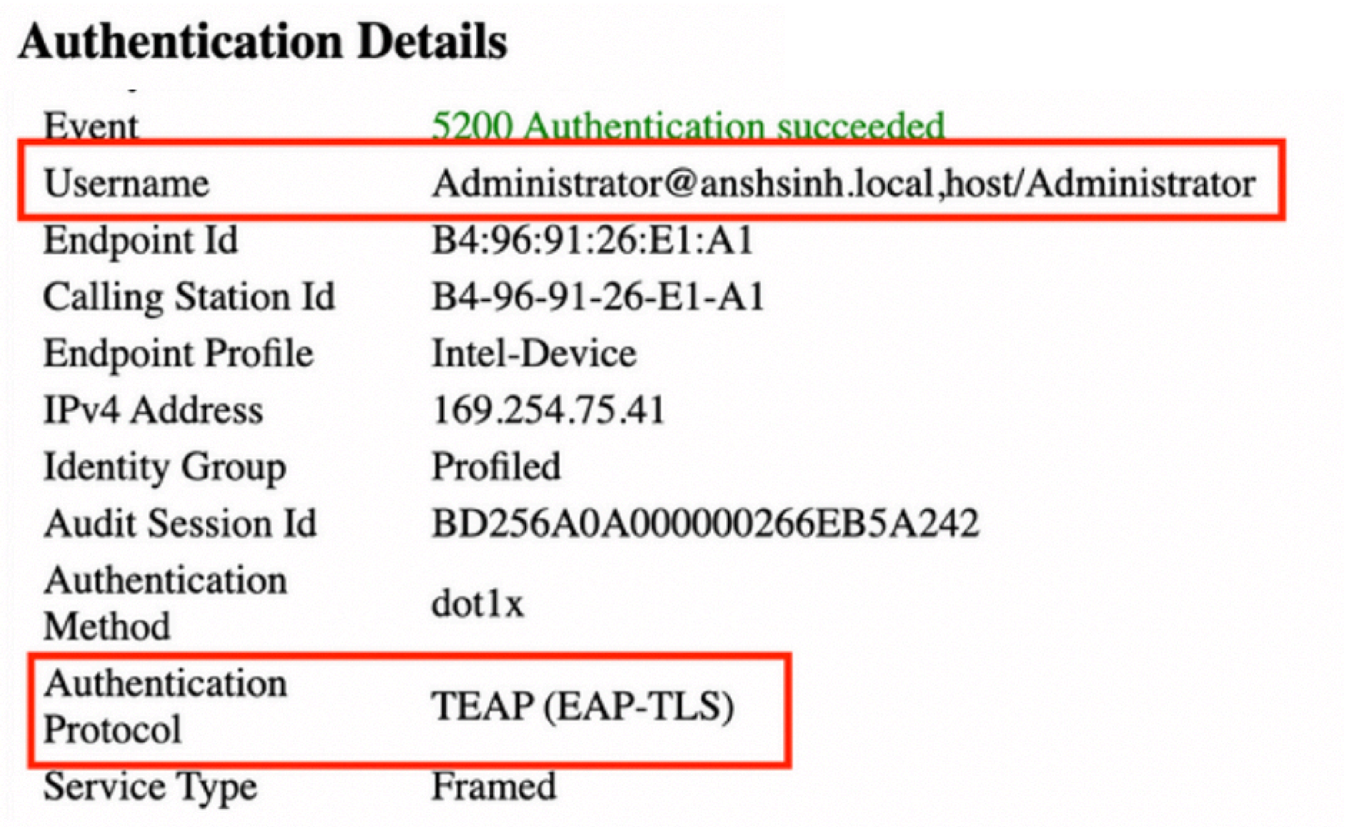
Event	5200 Authentication succeeded
Username	anonymous,host/Administrator
Endpoint Id	B4:96:91:26:E1:A1
Calling Station Id	B4-96-91-26-E1-A1
Endpoint Profile	Intel-Device
IPv4 Address	169.254.75.41
Identity Group	Profiled
Audit Session Id	BD256A0A000000266EB5A242
Authentication Method	dot1x
Authentication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



Other Attributes

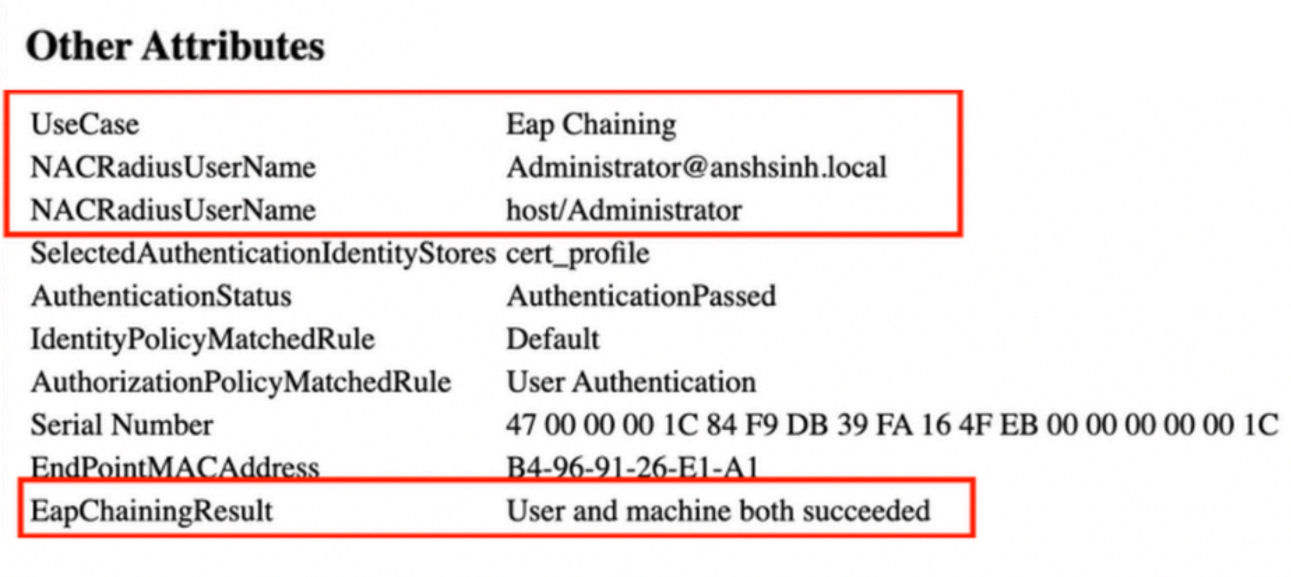
UseCase	Eap Chaining
NACRadiusUserName	host/Administrator
SelectedAuthenticationIdentityStores	cert_profile
AuthenticationStatus	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatchedRule	Machine Authentication
Serial Number	47 00 00 00 1C 84 F9 DB 39 FA 16 4F EB 00 00 00 00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

مصادقة المستخدم والجهاز



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

استكشاف الأخطاء وإصلاحها

أنت تحتاج أن يمكن هذا تصحيح على ISE:

- runtime-AAA
- nsf

- nsf-session
- خدمة Active Directory (استكشاف أخطاء ISE و AD وإصلاحها)

في Windows، يمكنك التحقق من سجلات "عارض الأحداث".

تحليل السجل النشط

مصادقة الجهاز

<#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 

11559 Client certificate was requested but not received inside the tunnel. Will continue with inner meth

 ... ...

11627 Starting EAP chaining 11573 Selected identity type 'User'

 11564 TEAP inner method started 11521 Prepared EAP-Request/Identity for inner EAP method ... ... 11567

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 Re

11515 Supplicant declined inner EAP method selected by Authentication Policy but did not proposed anothe

 22028 Authentication failed and the advanced options are ignored 33517 Sent TEAP Intermediate Result T

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

 11521 Prepared EAP-Request/Identity for inner EAP method ... ... 11567 Identity type provided by clien

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 

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 ano

11576 TEAP cryptobinding verification passed
```

```
 ... ...
15036 Evaluating Authorization Policy
 24209 Looking up Endpoint in Internal Endpoints IDStore - anonymous,host/Administrator 24211 Found End
11597 TEAP authentication phase finished successfully 11503 Prepared EAP-Success 11002 Returned RADIUS A
```

مصادقة المستخدم والجهاز

<#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
11620 TEAP full handshake finished successfully
 11596 Prepared EAP-Request with another TEAP challenge ... ... 11595 Extracted EAP-Response containing
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
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 E
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 TEA
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 Cert
22037 Authentication Passed 12528 Inner EAP-TLS authentication succeeded 11519 Prepared EAP-Success for
 11565 TEAP inner method finished successfully 33516 Sent TEAP Intermediate Result TLV indicating succe
15036 Evaluating Authorization Policy
 24209 Looking up Endpoint in Internal Endpoints IDStore - Administrator@example.local,host/Administrat
11597 TEAP authentication phase finished successfully 11503 Prepared EAP-Success 11002 Returned RADIUS A
```

معلومات ذات صلة

- بروتوكول المصادقة المتوسع للنفق (TEAP) الإصدار 1
- استئناف جلسة عمل أمان طبقة النقل (TLS) بدون حالة من جانب الخادم
- فهم EAP-FAST وتسلسل عمليات التنفيذ على AnyConnect NAM و ISE
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة

ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية
والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم
بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما
هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco
Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى
المستند الإنجليزي الأصلي (الرابط متوفر).