Configuration du chaînage EAP avec TEAP

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Configurer

- Configuration de Cisco ISE
- Configuration du demandeur natif Windows

Vérifier

- Rapport d'authentification détaillé
- Authentification machine
- Authentification des utilisateurs et des machines

Dépannage

- Analyse du journal en direct
  - Authentification machine
  - Authentification des utilisateurs et des machines

Informations connexes

Introduction

Ce document décrit comment configurer ISE et le demandeur Windows pour le chaînage EAP (Extensible Authentication Protocol) avec TEAP.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- ISE
- Configuration du demandeur Windows

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco ISE version 3.0
- Windows 10 version 2004
- Connaissance du protocole TEAP (Extensible Authentication Protocol) basé sur un tunnel

---

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

TEAP est une méthode de protocole d'authentification extensible basée sur un tunnel qui établit un tunnel sécurisé et exécute d'autres méthodes EAP sous la protection de ce tunnel sécurisé.

L’authentification TEAP se produit en deux phases après l’échange initial de requête/réponse d’identité EAP. Dans la première phase, TEAP utilise la connexion TLS pour fournir un échange de clé authentifié et pour établir un tunnel protégé. Une fois le tunnel établi, la deuxième phase commence avec l'homologue et le serveur qui engagent une conversation supplémentaire pour établir les authentifications et les politiques d'autorisation requises.

Cisco ISE 2.7 et versions ultérieures prennent en charge le protocole TEAP. Les objets type-length-value (TLV) sont utilisés dans le tunnel pour transporter les données liées à l'authentification entre l'homologue EAP et le serveur EAP. Microsoft a introduit la prise en charge de TEAP dans Windows version 10/2004 publiée en mai 2020.

Le chaînage EAP permet l'authentification de l'utilisateur et de l'ordinateur dans une session EAP/Radius au lieu de deux sessions distinctes. Auparavant, pour ce faire, vous deviez disposer du module NAM Cisco AnyConnect et utiliser EAP-FAST sur le demandeur Windows, car le demandeur Windows natif ne le prenait pas en charge. Vous pouvez désormais utiliser le demandeur natif Windows pour effectuer le chaînage EAP avec ISE 2.7 à l'aide de TEAP.

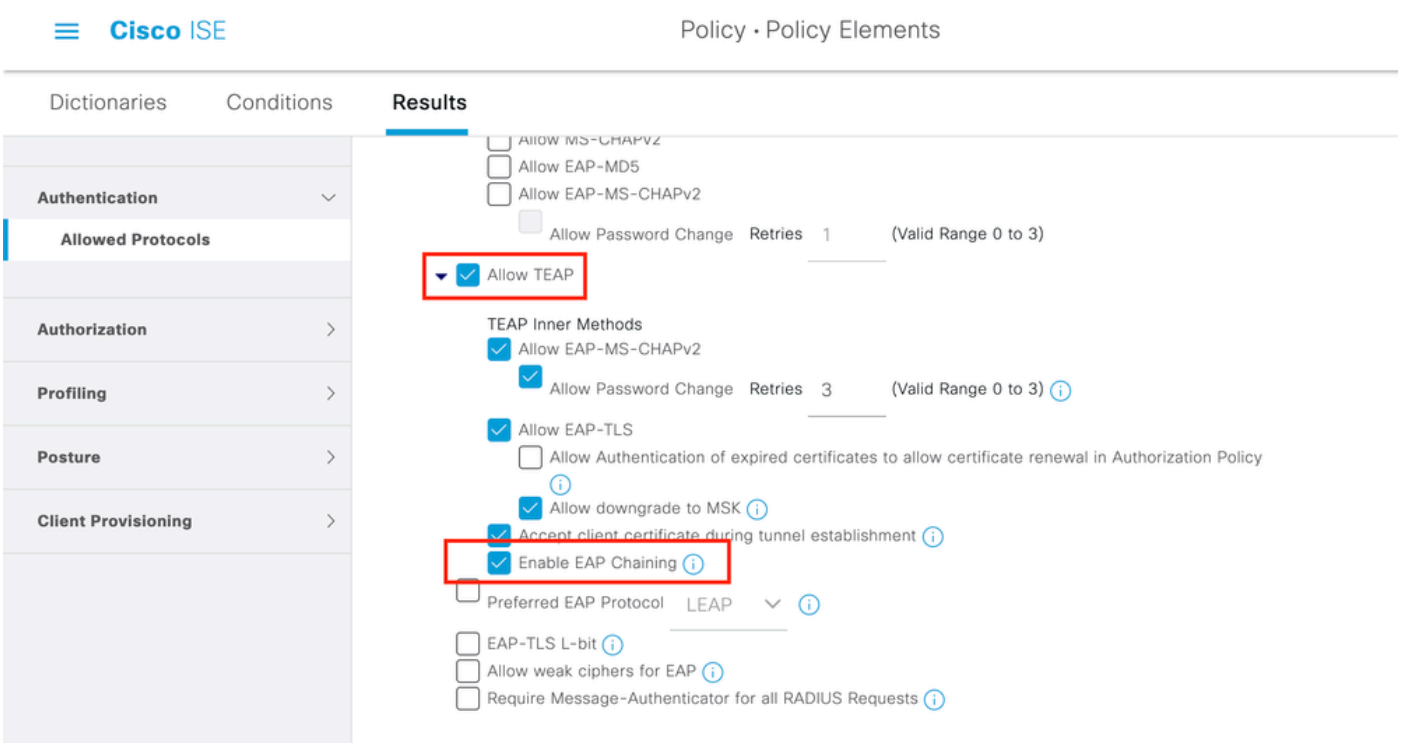
Configurer

Configuration de Cisco ISE

1. Vous devez modifier les protocoles autorisés pour activer le chaînage TEAP et EAP.

---

2. Accédez à ISE > Policy > Policy Elements > Results > Authentication > Allowed Protocols > Add New.. Cochez les cases TEAP et EAP chaining.

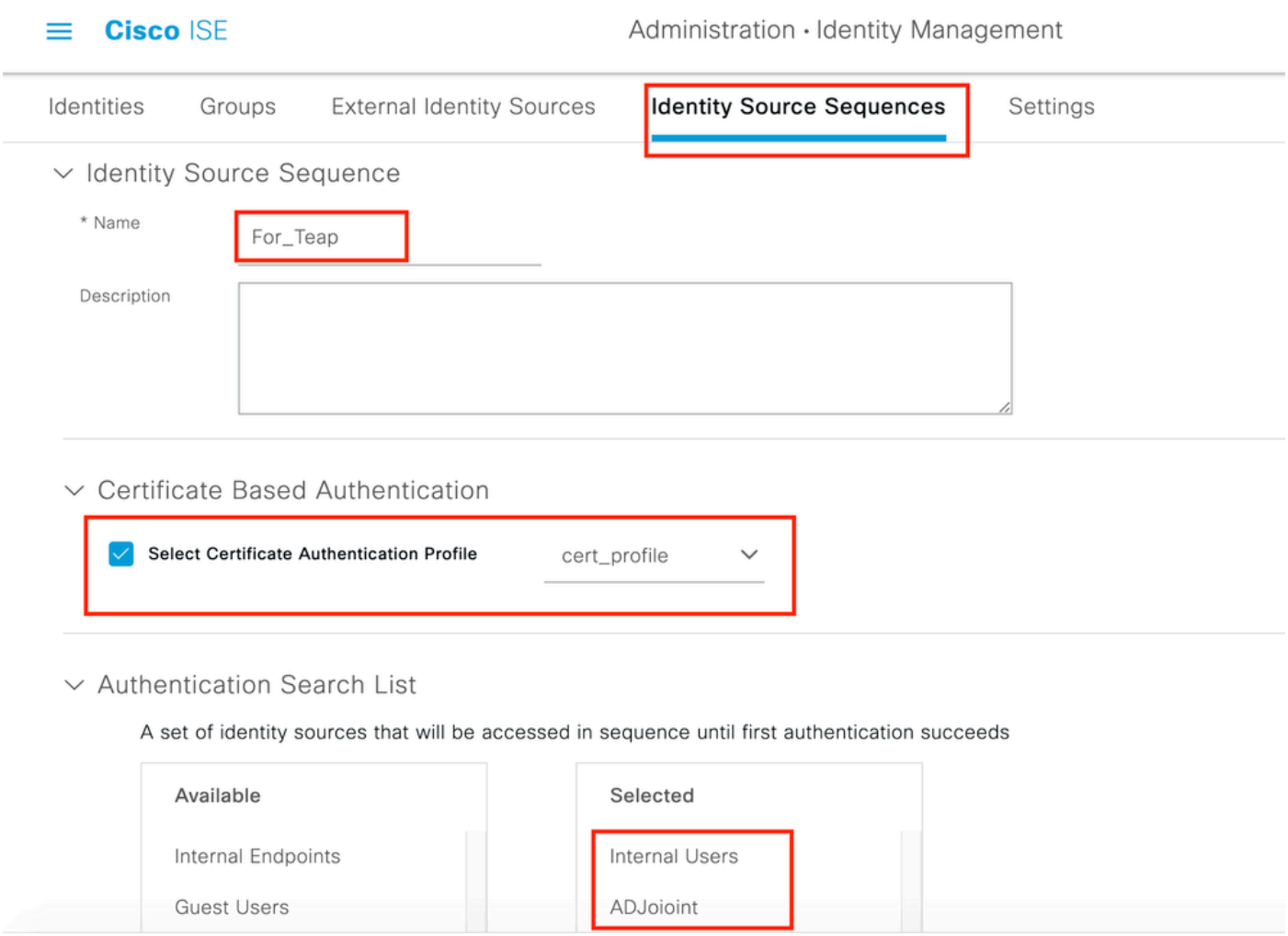


---

3. Créez un profil de certificat et ajoutez-le à la séquence source d'identité.

---

4. Accédez à ISE > Administration > Identities > identity Source Sequence et choisissez le profil d'authentification de certificat.

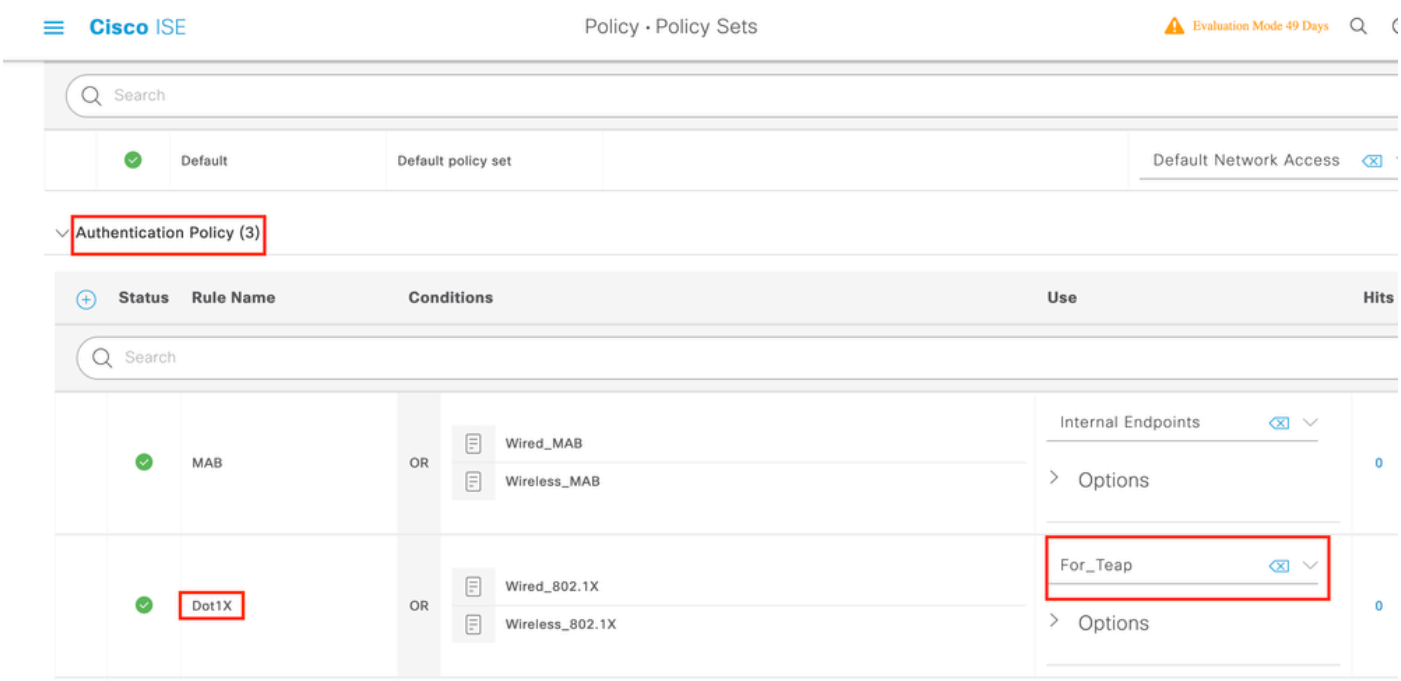


---

5. Vous devez appeler cette séquence dans la stratégie d'authentification.

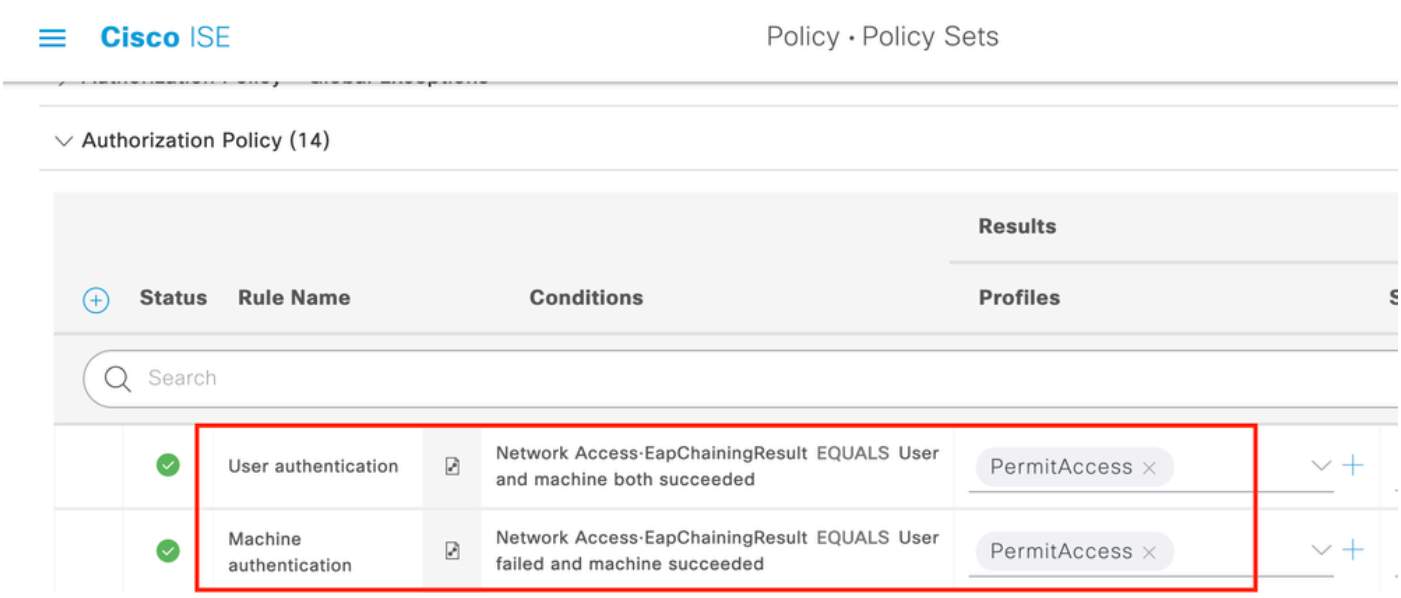
---

6. Accédez à ISE > Policy > Policy Sets. Choose the Policy Set forDot1x > Authentication Policy et choisissez les séquences source d'identité créées à l'étape 3.



7. Vous devez maintenant modifier la stratégie d'autorisation sous l'ensemble de stratégies Dot1x.

8. Accédez à ISE > Policy > Policy. SetsChoisissez le Policy Set for Dot1x > Authentication Policy. Vous devez créer deux règles. La première règle vérifie que la machine est authentifiée, mais pas l'utilisateur. La deuxième règle vérifie que l'utilisateur et la machine sont désormais authentifiés.



9. La configuration est terminée du côté du serveur ISE.

Configuration du demandeur natif Windows

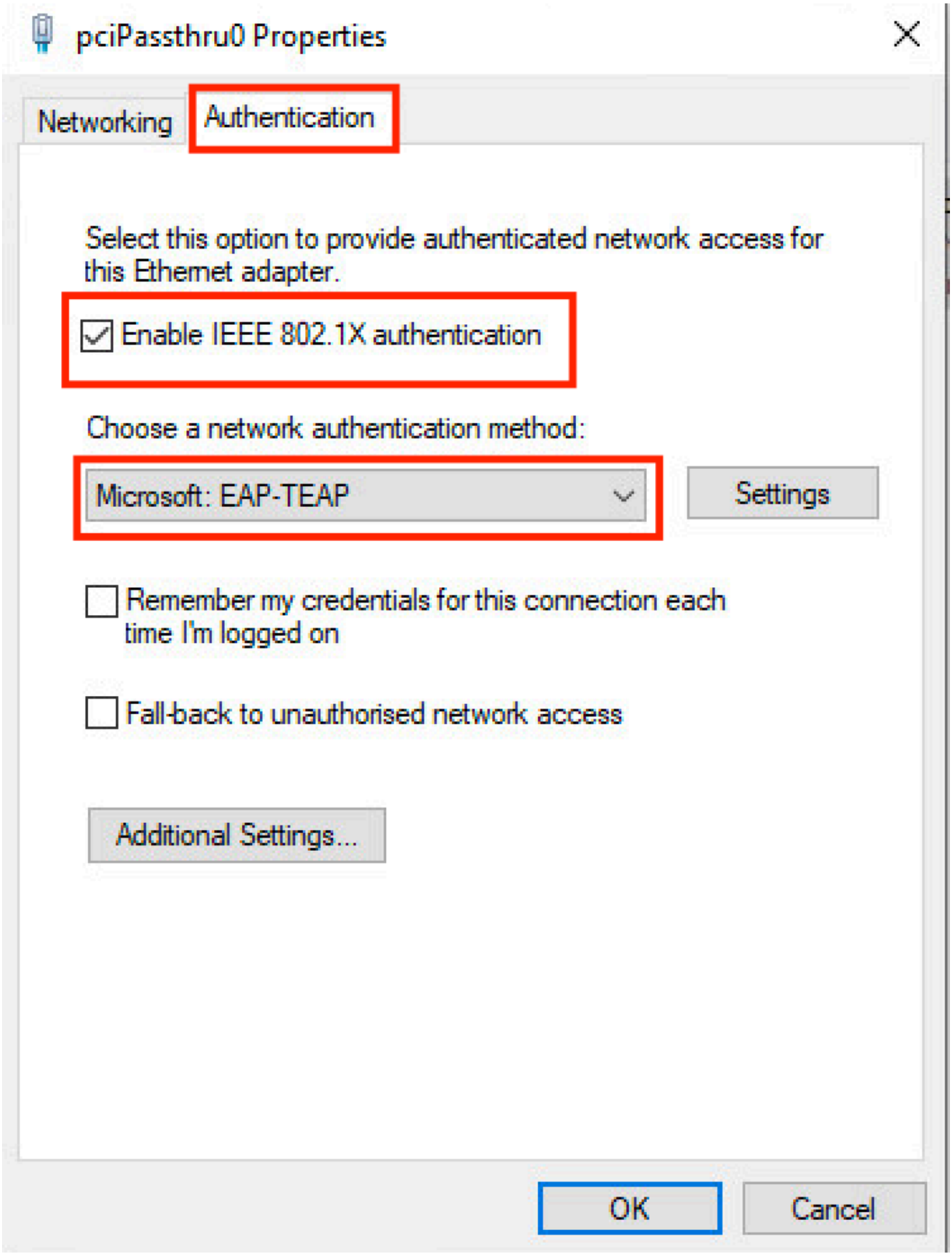
Configurez le paramètre d'authentification câblée dans ce document.

---

1. Accédez à Panneau de configuration > Centre Réseau et partage > Modifier les paramètres de la carte et cliquez avec le bouton droit sur Connexion au réseau local > Propriétés. Cliquez sur l'onglet Authentication.

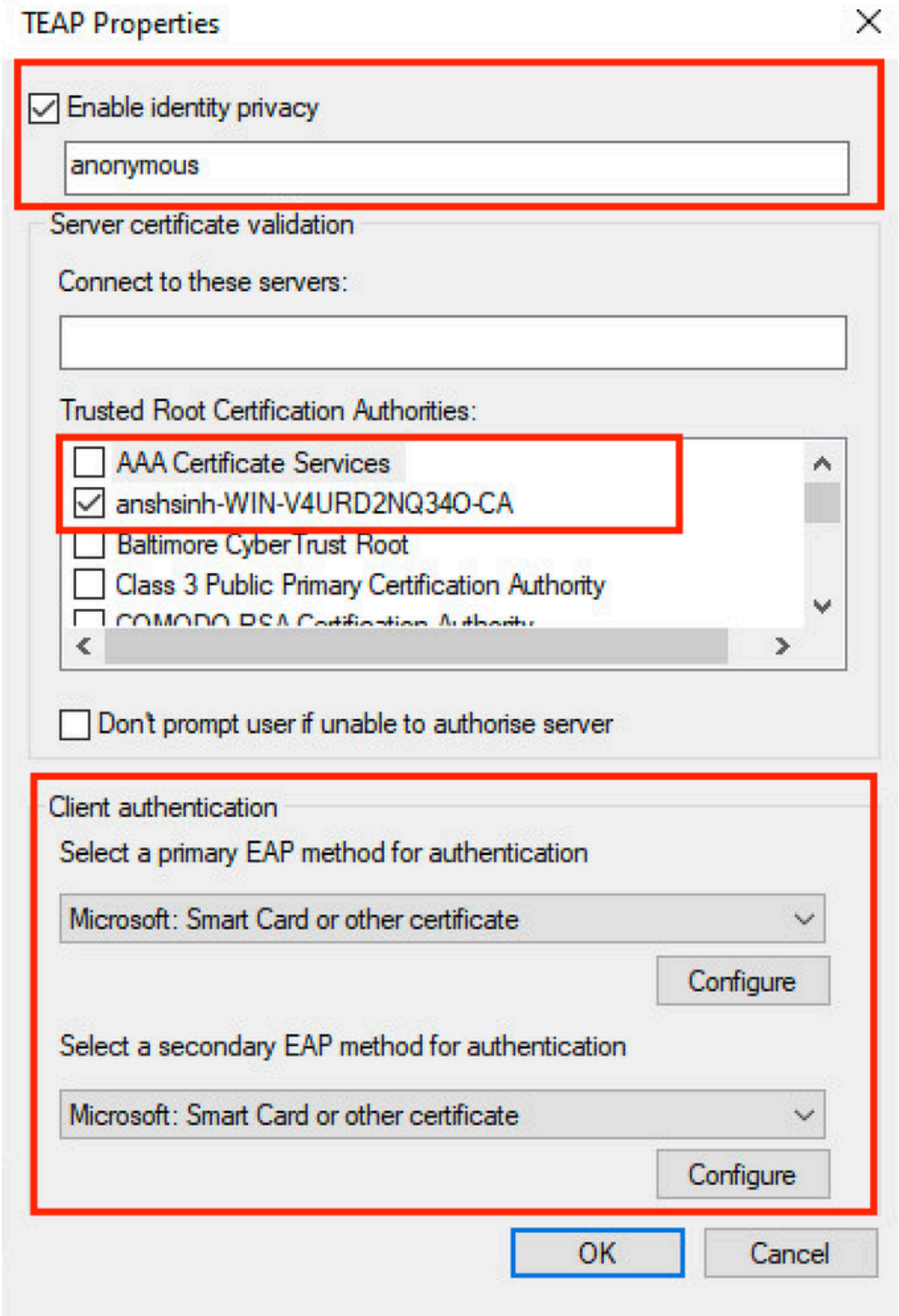
---

2. Cliquez sur la liste déroulante Authentication et choisissez 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. Cliquez sur le bouton Settings en regard de TEAP.

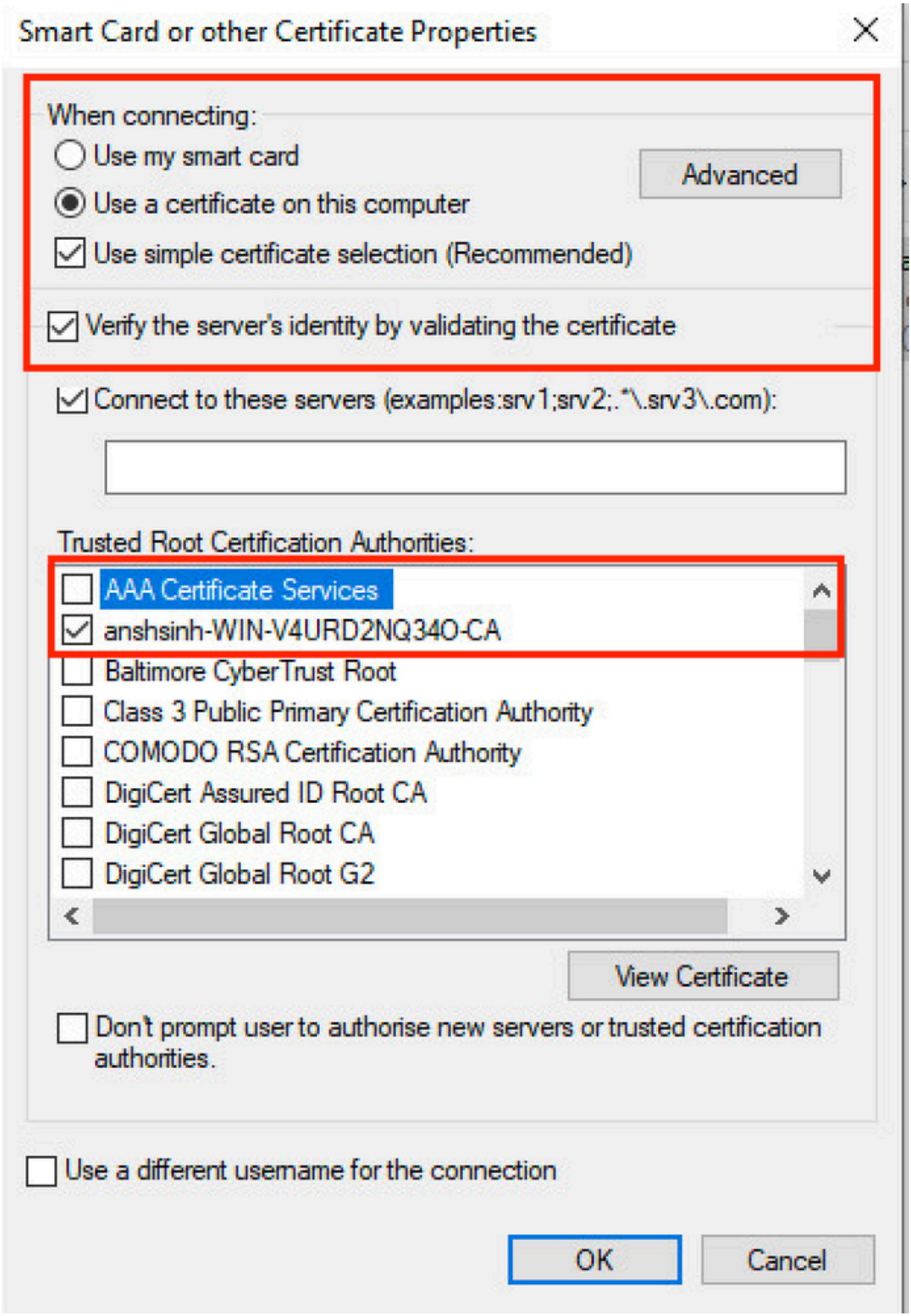
a. Maintenir la confidentialité des identités activée avec anonymous en tant qu'identité.
b. Cochez la case en regard du ou des serveurs CA racine sous Autorités de certification racine de confiance. Cette case est utilisée pour signer le certificat pour l'authentification EAP sur le PSN ISE.


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. Sous Client Authentication, choisissez la méthode EAP pour l'authentification à Microsoft : Carte à puce d'un autre certificat.

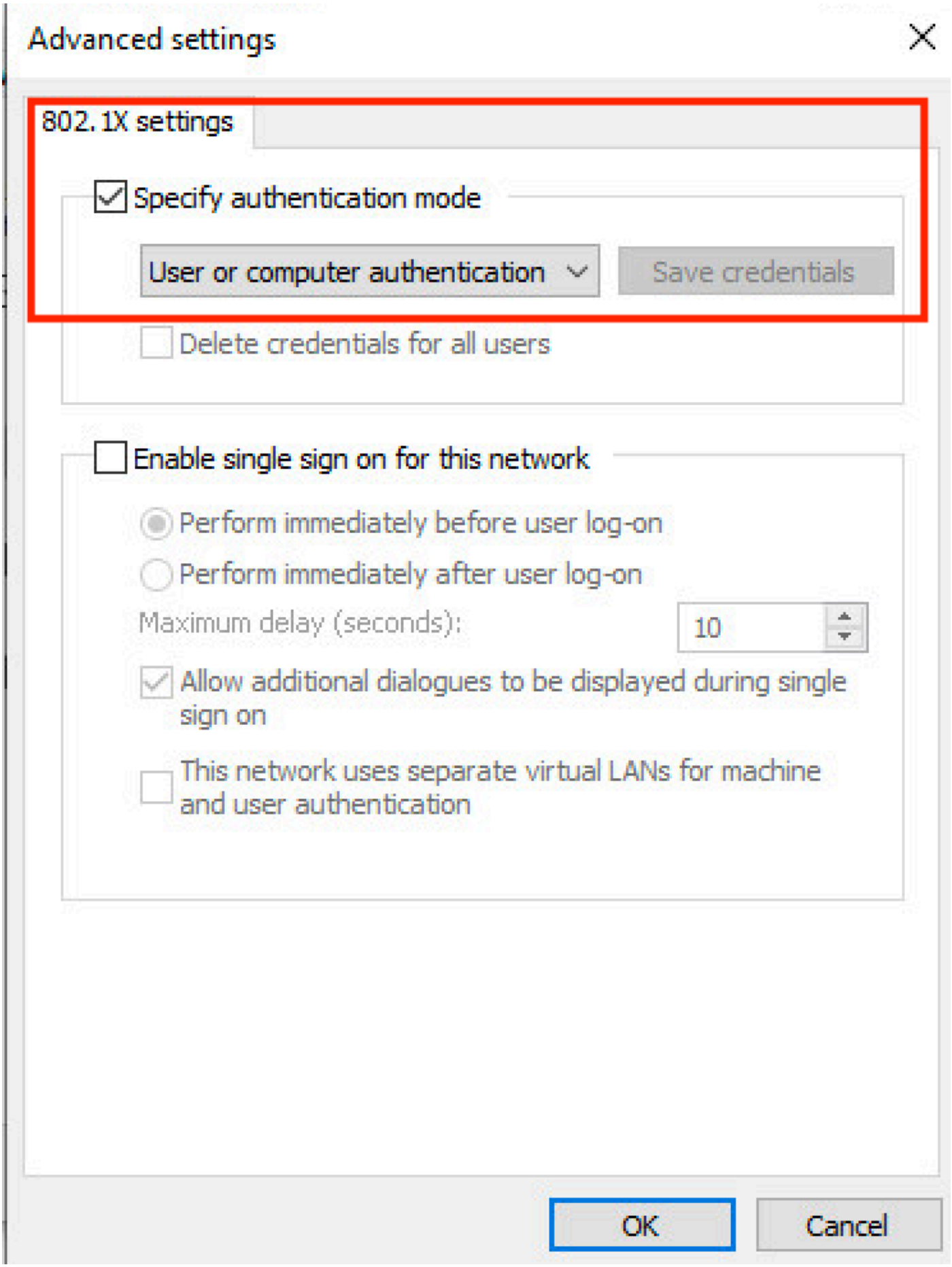
---

5. Pour chaque méthode EAP, cliquez sur le bouton Configure et modifiez selon le besoin et cliquez sur 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. Cliquez sur Additional Settings en bas de l'écran.

a. Activer Spécifiez le mode d'authentification.
b. Définissez le paramètre approprié dans le menu déroulant.
c. Choisissez User or computer authentication afin que les deux soient authentifiés et cliquez sur OK.

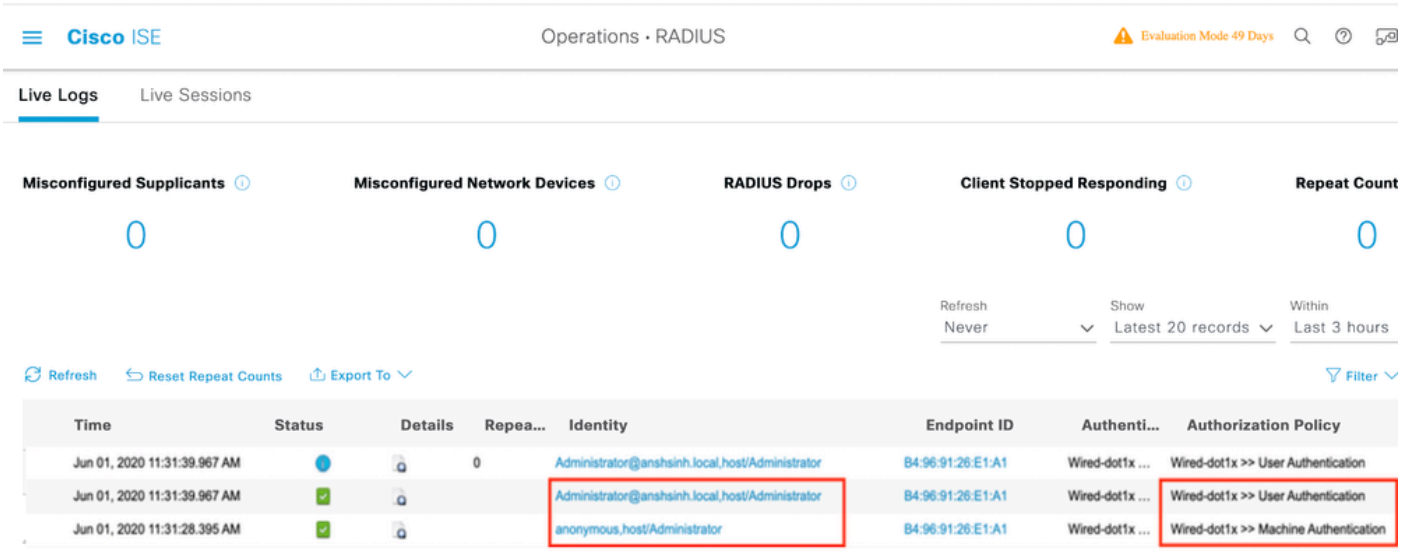

Advanced settings
802.1X settings
Specify authentication mode
User or computer authentication
Save credentials
Delete credentials for all users
Enable single sign on for this network
Perform immediately before user log-on
Perform immediately after user log-on
Maximum delay (seconds):
10
Allow additional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

Vérifier

Vous pouvez redémarrer l'ordinateur Windows 10 ou vous déconnecter, puis vous connecter. Lorsque l'écran de connexion à Windows s'affiche, l'authentification de l'ordinateur est déclenchée.

Dans les journaux en direct, vous voyez anonymous, host/Administrator (cet exemple affiche le nom de la machine) dans le champ d'identité. Vous voyez anonyme parce que vous avez configuré le demandeur pour la confidentialité de l'identité ci-dessus.

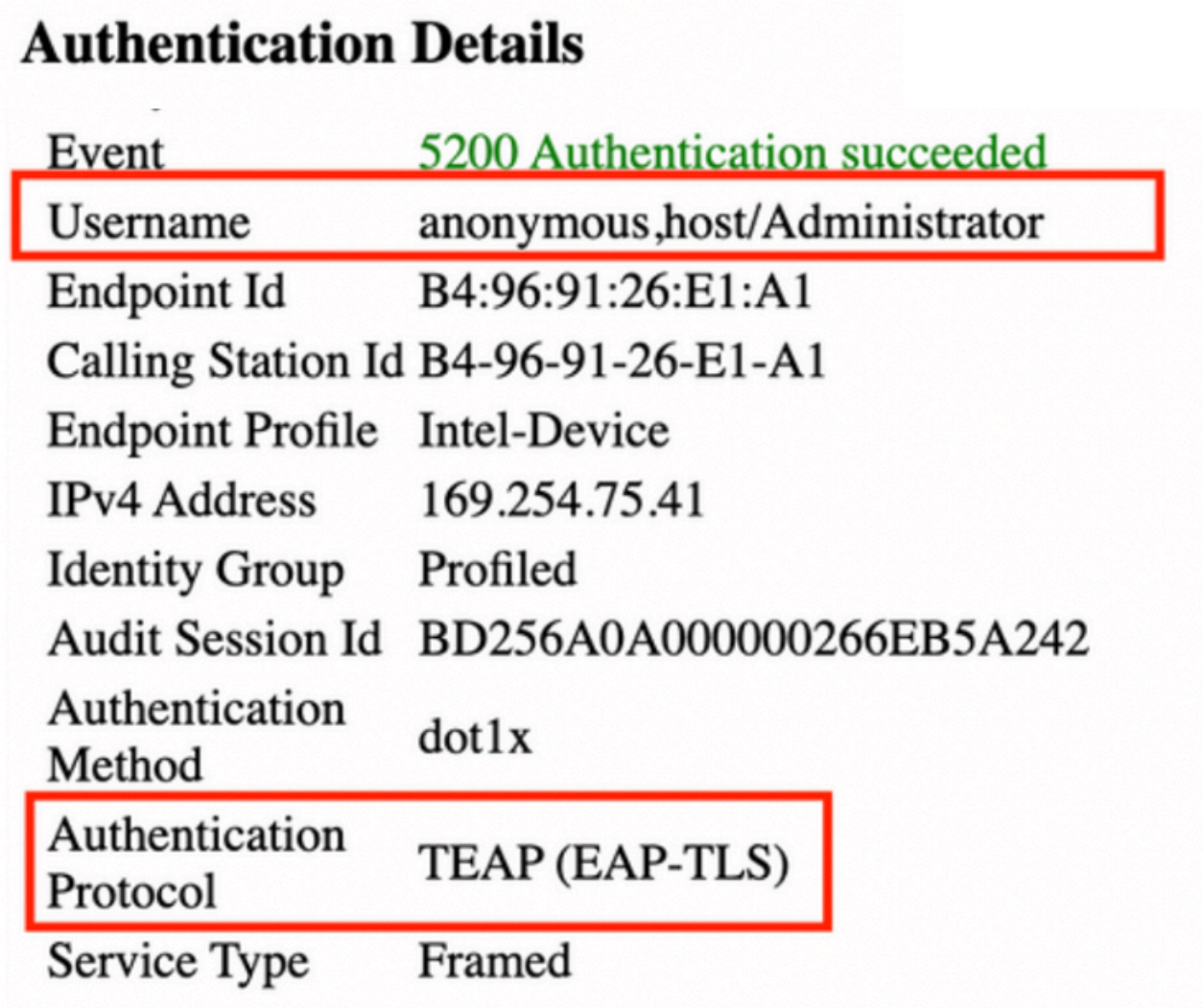
Lorsque vous vous connectez au PC avec des informations d'identification, les journaux en direct s'affichent sous la forme Administrator@example.local, host/Administrator. Il s'agit du chaînage EAP où l'authentification de l'utilisateur et de la machine s'est produite dans une session EAP.



Rapport d'authentification détaillé

Dans les détails du journal en direct, les authentifications de la machine n'affichent qu'une seule NACRadiusUsername entrée. Toutefois, l'authentification de l'utilisateur et de la machine en chaîne affiche deux entrées (une pour l'utilisateur et une pour la machine). En outre, vous voyez dans la section Authentication Details , que TEAP (EAP-TLS) a été utilisé pour le protocole d'authentification. Si vous utilisez MSCHAPv2 pour l'authentification de l'ordinateur et de l'utilisateur, le protocole d'authentification affiche TEAP (Microsoft : Mot de passe sécurisé (EAP-MSCHAP v2.)

Authentification machine



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

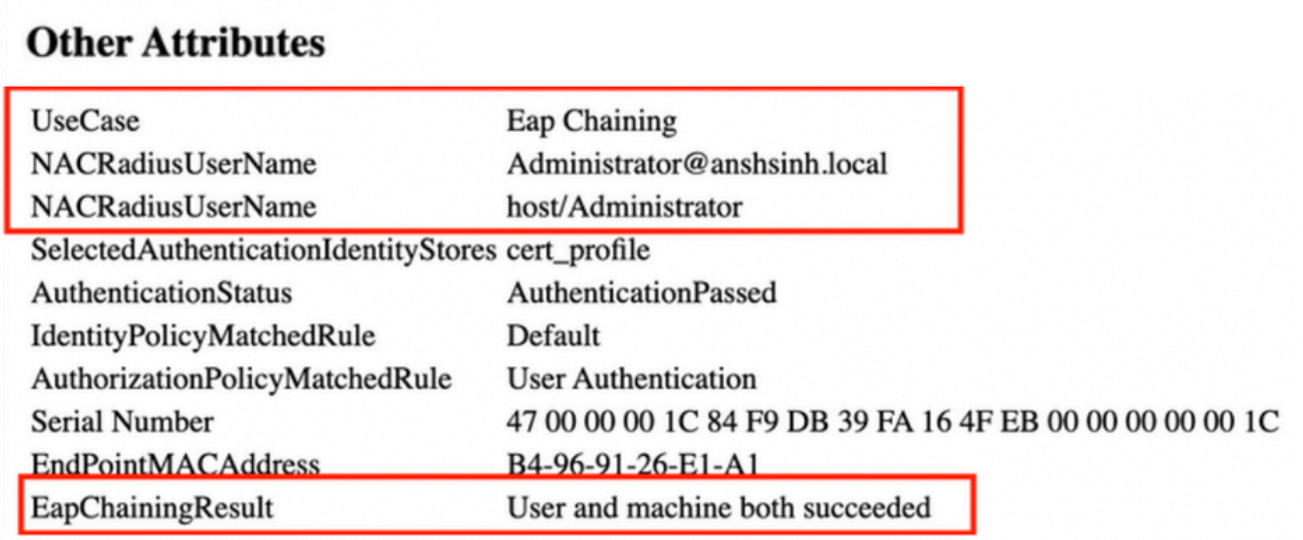
Other Attributes

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

Authentification des utilisateurs et des machines

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

Dépannage

Vous devez activer ces débogages sur ISE :

- runtime-AAA
- nsf
- nsf-session
- Active Directory (pour le dépannage entre ISE et AD)

Sous Windows, vous pouvez consulter les journaux de l'Observateur d'événements.

Analyse du journal en direct

Authentification machine

<#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

Authentification des utilisateurs et des machines

<#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
```

Informations connexes

- Protocole TEAP (Tunnel Extensible Authentication Protocol) version 1
- Reprise de session TLS (Transport Layer Security) sans état côté serveur
- Comprendre les implémentations EAP-FAST et de chaînage sur AnyConnect NAM et ISE
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.