

# 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 (Tunnel-based Extensible Authentication Protocol)

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, le protocole TEAP utilise la connexion TLS pour fournir un échange de clés 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 TLV (type-length-value) sont utilisés dans le tunnel pour transporter des 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 la machine dans une session EAP/RADIUS au lieu de deux sessions distinctes. Auparavant, pour ce faire, vous aviez besoin du module NAM Cisco AnyConnect et utilisiez 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

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

**Accédez à** ISE > Policy > Policy Elements > Results > Authentication > Allowed Protocols > Add New. Cochez les cases de chaînage TEAP et EAP.

Dictionaryes Conditions **Results**

**Authentication** ▾

**Allowed Protocols**

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 ⓘ

Étape 2. Créez un profil de certificat et ajoutez-le à la séquence source d'identité.

Accédez à ISE > Administration > Identities > identity Source Sequence et sélectionnez le profil de certificat.

Identities Groups External Identity Sources **Identity Source Sequences** Settings

▾ Identity Source Sequence

\* Name

Description

▾ Certificate Based Authentication

**Select Certificate Authentication 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	ADJooint

Étape 3. Vous devez appeler cette séquence dans la stratégie d'authentification.

Naviguez jusqu'à ISE > Policy > Policy Sets. Choose the Policy Set forDot1x > Authentication Policy la séquence source d'identité créée à l'étape 2 et choisissez-la.

The screenshot shows the Cisco ISE interface for Policy Sets. The top navigation bar includes the Cisco ISE logo, the path 'Policy · Policy Sets', and a warning for 'Evaluation Mode 49 Days'. Below the navigation bar is a search bar and a list of policy sets. The 'Authentication Policy (3)' is selected and expanded. It contains two rules:

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

Étape 4. Vous devez maintenant modifier la stratégie d'autorisation sous l'ensemble de stratégies Dot1x.

Accédez à ISE > Policy > Policy Sets. Choose the 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 authentifiés.

The screenshot shows the Cisco ISE interface for Authorization Policy (14). The top navigation bar includes the Cisco ISE logo, the path 'Policy · Policy Sets', and a warning for 'Evaluation Mode 49 Days'. Below the navigation bar is a search bar and a list of policy sets. The 'Authorization Policy (14)' is selected and expanded. It contains two rules:

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

La configuration est ainsi terminée du côté du serveur ISE.

Configuration du demandeur natif Windows

Configurez le paramètre d'authentification câblée dans ce document.

Accédez à Control Panel > Network and Sharing Center > Change Adapter Settings et cliquez avec le bouton droit de la souris LAN Connection > Properties. Cliquez sur l'Authenticationonglet.

Étape 1. Cliquez sur la Authenticationliste déroulante 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

1. Restez Enable Identity Privacy activé avec anonymous comme identité.

- Cochez la case en regard du ou des serveurs d'autorité de certification racine sous Autorités de certification racine de confiance qui sont utilisées 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  
 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

Configure

Select a secondary EAP method for authentication

Microsoft: Smart Card or other certificate

Configure

OK

Cancel



1. Enable : spécifiez le mode d'authentification.
2. Définissez la liste déroulante sur le paramètre approprié.
3. Choisissez User or computer authentication de sorte 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

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

Dans les journaux en direct, vous voyez anonymous, host/Administrator (ici 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, vous pouvez voir dans les journaux en direct 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.

The screenshot shows the Cisco ISE Operations - RADIUS interface. At the top, there are navigation tabs for 'Live Logs' and 'Live Sessions'. Below this, there are five summary cards: 'Misconfigured Supplicants', 'Misconfigured Network Devices', 'RADIUS Drops', 'Client Stopped Responding', and 'Repeat Count', each showing a count of 0. To the right of these cards are controls for 'Refresh' (set to Never), 'Show' (set to Latest 20 records), and 'Within' (set to Last 3 hours). Below the summary cards is a table of live logs with columns: Time, Status, Details, Repea..., Identity, Endpoint ID, Authenti..., and Authorization Policy. The table contains three rows of log entries. The second and third rows are highlighted with red boxes. The second row shows 'Administrator@anshsinh.local,host/Administrator' with 'Wired-dot1x ...' authentication and 'Wired-dot1x >> User Authentication' policy. The third row shows 'anonymous,host/Administrator' with 'Wired-dot1x ...' authentication and 'Wired-dot1x >> Machine Authentication' policy.

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

### Rapport d'authentification détaillé

Dans les détails du journal en direct, les authentifications de machine n'affichent qu'une seule NACRadiusUsername entrée, mais l'authentification d'utilisateur et de machine en chaîne affiche deux entrées (une pour l'utilisateur et une pour la machine). En outre, vous voyez sous la Authentication Details section, que TEAP (EAP-TLS) a été utilisée pour le Authentication Protocol. Si vous utilisez MSCHAPv2 pour l'authentification des ordinateurs et des utilisateurs, le protocole d'authentification affiche TEAP (Microsoft: Secured password (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 1C
EndPointMACAddress	B4-96-91-26-E1-A1
EapChainingResult	User failed and machine succeeded

## 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 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

Authentication 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

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

... ..

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 another

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

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

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 TLV

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

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

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

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-TLS  
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 sessions  
12805 Extracted TLS ClientHello message 12806 Prepared TLS ServerHello message 12807 Prepared TLS Certificate  
22037 Authentication Passed 12528 Inner EAP-TLS authentication succeeded 11519 Prepared EAP-Success for inner method  
11565 TEAP inner method finished successfully 33516 Sent TEAP Intermediate Result TLV indicating success  
15036 Evaluating Authorization Policy  
24209 Looking up Endpoint in Internal Endpoints IDStore - Administrator@example.local,host/Administrator@...  
11597 TEAP authentication phase finished successfully 11503 Prepared EAP-Success 11002 Returned RADIUS Attributes

#### 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.