

# Configure EAP Chaining with TEAP

## Contents

---

### [Introduction](#)

### [Prerequisites](#)

[Requirements](#)

[Components Used](#)

### [Background Information](#)

### [Configure](#)

[Cisco ISE Configuration](#)

[Windows Native Supplicant Configuration](#)

### [Verify](#)

[Detailed Authentication Report](#)

[Machine Authentication](#)

[User and Machine Authentication](#)

### [Troubleshoot](#)

[Live Log Analysis](#)

[Machine Authentication](#)

[User and Machine Authentication](#)

### [Related Information](#)

---

## Introduction

This document describes how to configure ISE and Windows supplicant for Extensible Authentication Protocol (EAP) Chaining with TEAP.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- ISE
- Configuration of windows supplicant

### Components Used

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

- Cisco ISE version 3.0
- Windows 10 build 2004
- Knowledge of protocol Tunnel-based Extensible Authentication Protocol (TEAP)

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.

## Background Information

TEAP is a tunnel-based Extensible Authentication Protocol method that establishes a secure tunnel and executes other EAP methods under the protection of that secured tunnel.

TEAP authentication occurs in two phases after the initial EAP identity request/response exchange. In the first phase, TEAP uses the TLS handshake to provide an authenticated key exchange and to establish a protected tunnel. Once the tunnel is established, the second phase begins with the peer and the server engaging in further conversation to establish the required authentications and authorization policies.

Cisco ISE 2.7 and later supports the TEAP Protocol. The type-length-value (TLV) objects are used within the tunnel to transport authentication-related data between the EAP peer and the EAP server.

Microsoft introduced support for TEAP in Windows version 10 2004 released in May 2020.

EAP chaining allows the user and machine authentication within one EAP/Radius session instead of two separate sessions. Previously, to achieve this you needed the Cisco AnyConnect NAM module and use EAP-FAST on the windows supplicant as the native Windows supplicant did not support this. Now, you can use the Windows Native Supplicant to perform EAP Chaining with ISE 2.7 with the use of TEAP.

## Configure

### Cisco ISE Configuration

Step 1. You need to edit the Allowed Protocols to enable TEAP and EAP Chaining.

Navigate to ISE > Policy > Policy Elements > Results > Authentication > Allowed Protocols > Add New. Check the TEAP and EAP chaining check boxes.

The screenshot shows the Cisco ISE configuration interface for 'Policy > Policy Elements'. The 'Results' tab is active, and the 'Allowed Protocols' section is expanded. The following settings are visible:

- 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 ⓘ

Step 2. Create a certificate profile and add it to the Identity Source Sequence.

Navigate to ISE > Administration > Identities > identity Source Sequence and choose the certificate Profile.

The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is Administration > Identity Management. The main menu includes Identities, Groups, External Identity Sources, Identity Source Sequences (highlighted with a red box), and Settings. Under Identity Source Sequence, the Name field is set to 'For\_Teap' (highlighted with a red box). The Description field is empty. Under Certificate Based Authentication, the 'Select Certificate Authentication Profile' checkbox is checked, and the dropdown menu is set to 'cert\_profile' (highlighted with a red box). Under Authentication Search List, the 'Available' column contains 'Internal Endpoints' and 'Guest Users', while the 'Selected' column contains 'Internal Users' and 'ADJoint' (highlighted with a red box). A description below the search list states: 'A set of identity sources that will be accessed in sequence until first authentication succeeds'.

Step 3. You need to call this sequence in the Authentication Policy.

Navigate to ISE > Policy > Policy Sets. Choose the Policy Set forDot1x > Authentication Policy and choose the Identity source sequence created in Step 2.

Status	Rule Name	Conditions	Use	Hits
✓	Default	Default policy set	Default Network Access	
Authentication Policy (3)				
✓	MAB	OR Wired_MAB Wireless_MAB	Internal Endpoints > Options	0
✓	Dot1X	OR Wired_802.1X Wireless_802.1X	For_Teap > Options	0

Step 4. Now you need to modify the Authorization Policy under the Dot1x Policy Set.

Navigate to ISE > Policy > Policy Sets. Choose the Policy Set for Dot1x > Authentication Policy.

You need to create two rules. The first rule checks that the machine is authenticated but the user is not. The second rule verifies that both the user and the machine are authenticated.

Status	Rule Name	Conditions	Profiles	Results
Authorization Policy (14)				
✓	User authentication	Network Access-EapChainingResult EQUALS User and machine both succeeded	PermitAccess	
✓	Machine authentication	Network Access-EapChainingResult EQUALS User failed and machine succeeded	PermitAccess	

This completes the configuration from the ISE Server side.

## Windows Native Supplicant Configuration

Configure the wired authentication setting in this document.

Navigate to Control Panel > Network and Sharing Center > Change Adapter Settings and right-click LAN Connection > Properties. Click the Authentication tab.

Step 1. Click Authentication drop-down and choose 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

Step 2. Click the Settings button next to TEAP.

1. **Keep** Enable Identity Privacy **enabled with** anonymous as the identity.
2. Put a checkmark next to the root CA server(s) under Trusted Root Certification Authorities that are used to sign the certificate for EAP authentication on the 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

Configure

Select a secondary EAP method for authentication

Microsoft: Smart Card or other certificate

Configure

OK

Cancel

2. Set the drop-down to the appropriate setting.
3. Choose User or computer authentication so that both are authenticated and click 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

**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.

In the live logs, you see anonymous, host/Administrator (here is the machine name) in the identity field. You see anonymous because you configured supplicant for identity privacy above.

When you log in to the PC with credentials, you can see in the live logs Administrator@example.local, host/Administrator. This is EAP chaining where both user and machine authentication happened in one EAP session.

The screenshot shows the Cisco ISE Live Logs 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. Below the summary cards, there are controls for 'Refresh', 'Reset Repeat Counts', 'Export To', and 'Filter'. The main table displays authentication logs with columns for Time, Status, Details, Repeat Count, Identity, Endpoint ID, Authentication Protocol, and Authorization Policy. Three rows are visible, with the Identity and Authorization Policy columns highlighted by red boxes.

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

## Detailed Authentication Report

In the Live Log Details, Machine authentications only show a single NACRadiusUsername entry but the chained user and machine authentication shows two entries (one for the user, and one for the machine). Also, you see under the Authentication Details section, that TEAP (EAP-TLS) was used for the Authentication Protocol. If you use MSCHAPv2 for machine and user authentication, the authentication protocol shows TEAP (Microsoft: Secured password (EAP-MSCHAP v2)).

## Machine Authentication

## 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

### User and Machine Authentication

## 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

## Troubleshoot

You need to enable these debugs on ISE:

- runtime-AAA
- nsf
- nsf-session
- Active Directory (to troubleshoot between ISE and AD)

On Windows, you can check the Event Viewer logs.

## Live Log Analysis

### Machine Authentication

<#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 method

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 another  
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-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 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

## User and Machine Authentication

<#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 method  
  
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-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 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-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 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/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 cache  
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

## Related Information

- [Tunnel Extensible Authentication Protocol \(TEAP\) Version 1](#)
- [Transport Layer Security \(TLS\) Session Resumption without Server-Side State](#)
- [Understand EAP-FAST and Chaining Implementations on AnyConnect NAM and ISE](#)
- [Technical Support & Documentation - Cisco Systems](#)