

# TEAP를 통한 EAP 연결

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[Cisco ISE 컨피그레이션](#)

[Windows 네이티브 서플리컨트 구성](#)

[다음을 확인합니다.](#)

[세부 인증 보고서](#)

[머신 인증](#)

[사용자 및 머신 인증](#)

[문제 해결](#)

[라이브 로그 분석](#)

[머신 인증](#)

[사용자 및 머신 인증](#)

[관련 정보](#)

## 소개

이 문서에서는 터널 기반 TEAP(Extensible Authentication Protocol)를 사용하여 EAP(Extensible Authentication Protocol) 체이닝을 위한 ISE 및 Windows 신청자를 구성하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ISE
- Windows 서플리컨트 구성

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ISE 버전 3.0
- Windows 10 빌드 2004
- 프로토콜 TEAP 지식

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 배경 정보

TEAP는 보안 터널을 설정하고 해당 보안 터널의 보호 하에 다른 EAP 방법을 실행하는 터널 기반 확장 가능 인증 프로토콜 방법입니다.

TEAP 인증은 초기 EAP ID 요청/응답 교환 후 2단계로 발생합니다.

첫 번째 단계에서 TEAP는 TLS 핸드셰이크를 사용하여 인증된 키 교환을 제공하고 보호된 터널을 설정합니다. 터널이 설정되면 두 번째 단계는 피어에서 시작하며 서버는 필요한 인증 및 권한 부여 정책을 설정하기 위해 추가 대화를 시작합니다.

Cisco ISE 2.7 이상은 TEAP 프로토콜을 지원합니다. TLV(type-length-value) 객체는 EAP 피어와 EAP 서버 간에 인증 관련 데이터를 전송하기 위해 터널 내에서 사용됩니다.

Microsoft는 2020년 5월에 릴리스된 Windows 10 2004 버전에서 TEAP에 대한 지원을 도입했습니다.

EAP 체이닝은 두 개의 개별 세션 대신 하나의 EAP/Radius 세션 내에서 사용자 및 머신 인증을 허용합니다.

이전에는 이를 위해 Cisco AnyConnect NAM 모듈이 필요했으며 기본 Windows 신청자가 이를 지원하지 않으므로 Windows 신청자에서 EAP-FAST를 사용해야 했습니다. 이제 Windows 기본 신청자를 사용하여 TEAP를 사용하여 ISE 2.7과의 EAP 연결을 수행할 수 있습니다.

## 구성

### Cisco ISE 컨피그레이션

1단계. TEAP 및 EAP 연결을 활성화하려면 허용되는 프로토콜을 수정해야 합니다.

탐색 ISE > Policy > Policy Elements > Results > Authentication > Allowed Protocols > Add New . TEAP 및 EAP 연결 확인란을 선택합니다.

Dictionaryes   Conditions   **Results**

- 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 ⓘ

2단계. 인증서 프로필을 생성하고 ID 소스 시퀀스에 추가합니다.

탐색 ISE > Administration > Identities > identity Source Sequence 인증서 프로필을 선택합니다.

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

Identity Source Sequence

\* Name

Description

Certificate Based Authentication

Select Certificate Authentication Profile

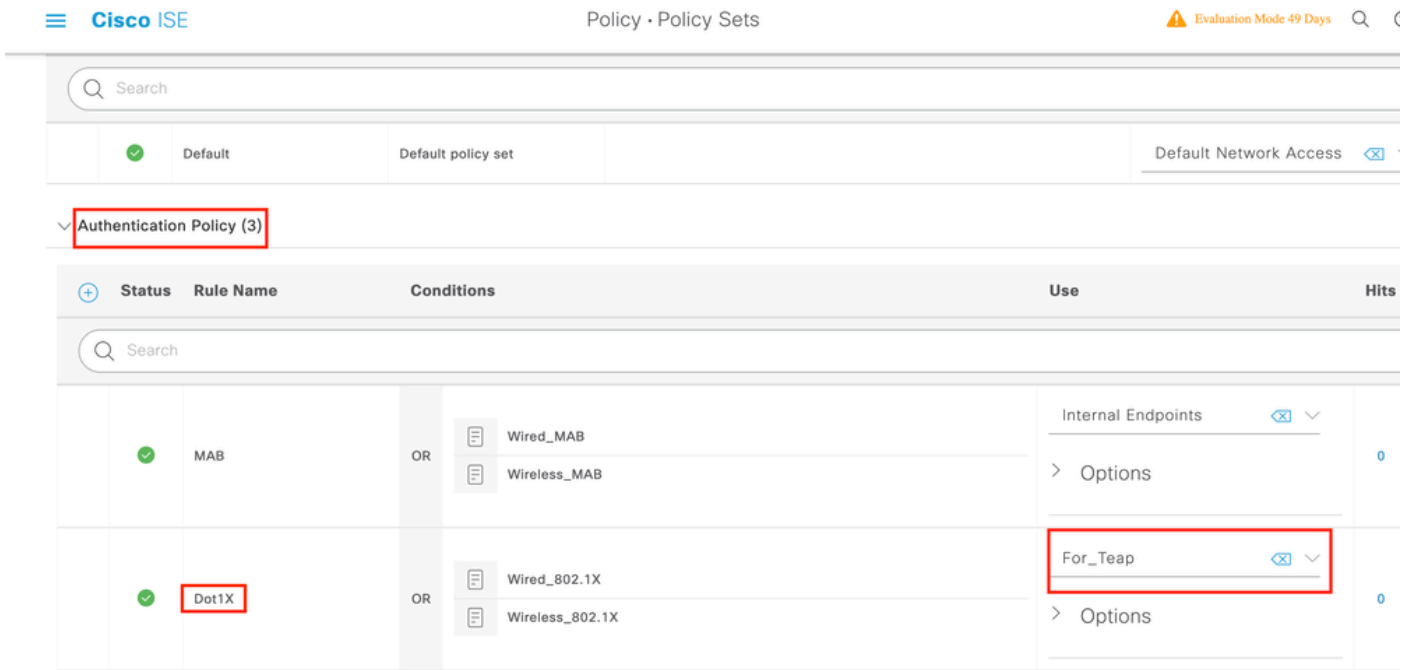
Authentication Search List

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

Available	Selected
Internal Endpoints	Internal Users
Guest Users	ADJoint

3단계. 인증 정책에서 이 시퀀스를 호출해야 합니다.

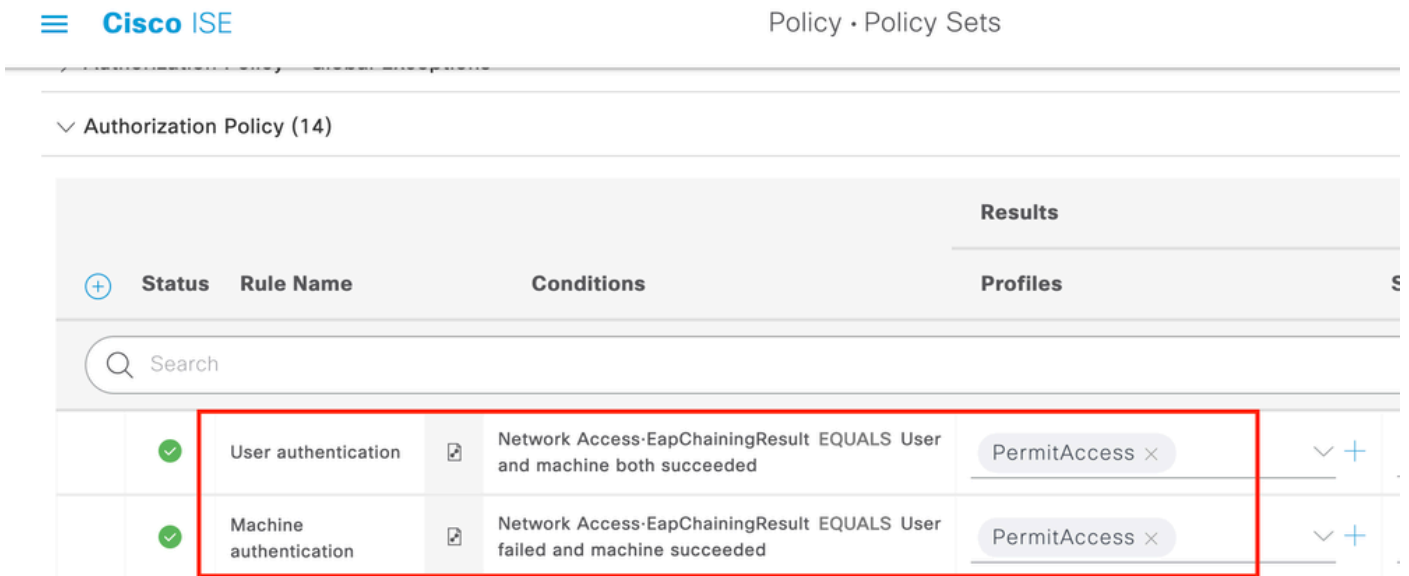
탐색 ISE > Policy > Policy Sets . Choose the Policy Set for Dot1x > Authentication Policy 2단계에서 생성한 ID 소스 시퀀스를 선택합니다.



4단계. 이제 Dot1x 정책 집합에서 권한 부여 정책을 수정해야 합니다.

탐색 ISE > Policy > Policy Sets . Choose the Policy Set for Dot1x > Authentication Policy .

두 개의 규칙을 생성해야 합니다. 첫 번째 규칙은 시스템이 인증되었지만 사용자가 인증되지 않았음을 확인합니다. 두 번째 규칙은 사용자와 머신 모두 인증되었음을 확인합니다.



이렇게 하면 ISE 서버 측에서 컨피그레이션이 완료됩니다.

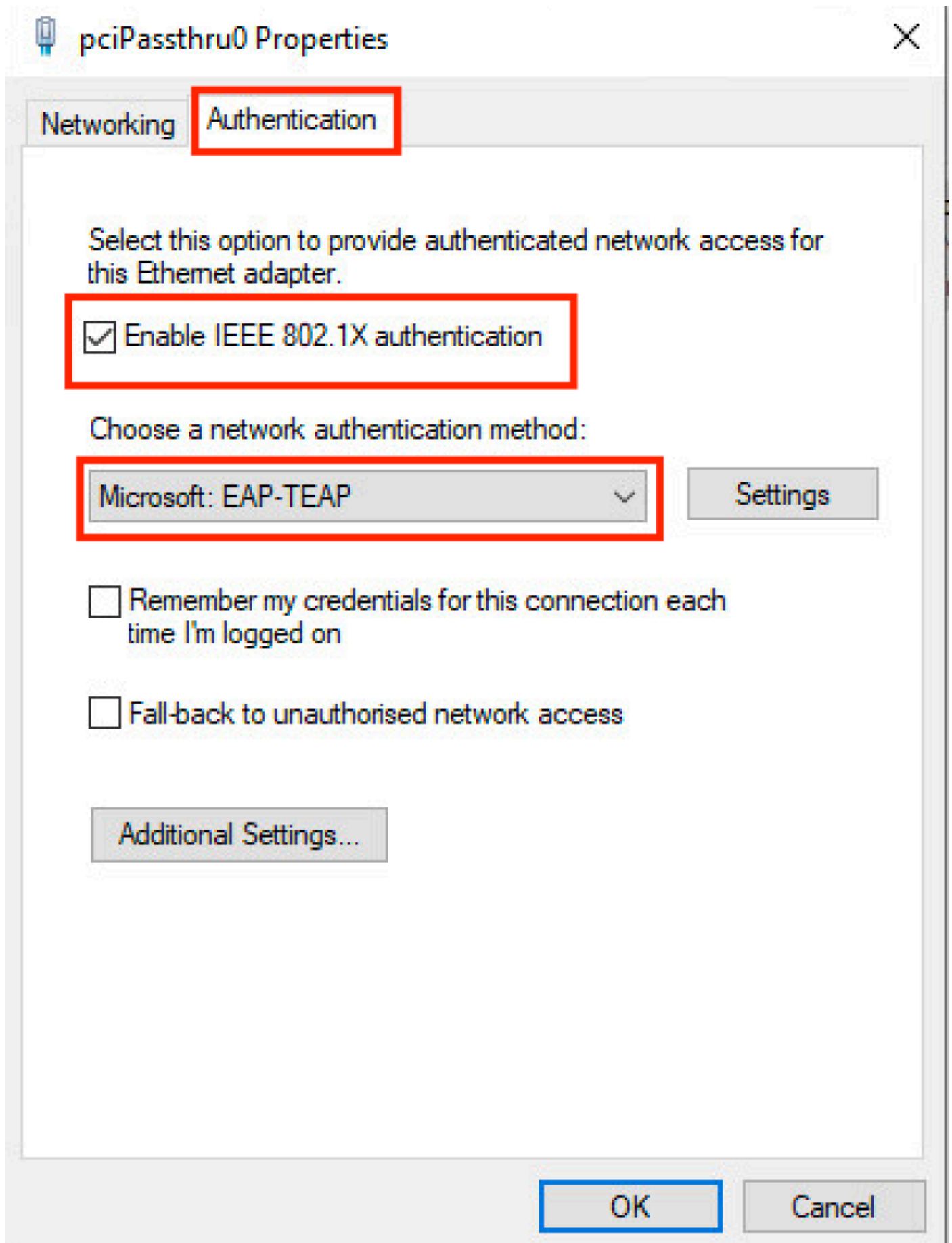
## Windows 네이티브 서플리컨트 구성

이 문서의 유선 인증 설정을 구성합니다.

탐색 Control Panel > Network and Sharing Center > Change Adapter Settings 마우스 오른쪽 버튼으로 LAN Connection

> Properties. 다음을 클릭합니다. Authentication 탭을 클릭합니다.

1단계. 클릭 Authentication 드롭다운 메뉴를 선택하고 Microsoft EAP-TEAP.



2단계. 다음을 클릭합니다. **Settings** TEAP 옆의 버튼을 클릭합니다.

1. 유지 Enable Identity Privacy 사용 anonymous ID를 입력합니다.
2. ISE PSN에서 EAP 인증을 위한 인증서를 서명하는 데 사용되는 신뢰할 수 있는 루트 인증 기관의 루트 CA 서버 옆에 확인 표시를 합니다.



이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.