

Trustsec용 ISE와 NAD 간에 ISE 3.4 PAC 없는 인증 설정

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[정보](#)

[구성](#)

[설정](#)

[스위치 구성](#)

[ISE 구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

소개

이 문서에서는 Trustsec 환경 데이터 다운로드를 위해 ISE와 NAD 클라이언트 간의 PAC 없는 컨피그레이션의 초기 설정에 대해 설명합니다.

사전 요구 사항

요구 사항

- 네트워크 보안 솔루션으로서의 Cisco TrustSec에 대한 지식
- 네트워크 보안 관리를 위한 ISE(Identity Services Engine) 지식
- 인증 정보 전송을 위한 프레임워크로서 EAP(Extensible Authentication Protocol)에 대한 기본적인 이해

사용되는 구성 요소

ISE(Identity Services Engine) 릴리스 3.4.x

Cisco IOS® 17.15.1 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

정보

PAC를 사용하지 않는 모드에서는 TrustSec 정책을 구현하기가 더 쉽습니다. PAC(Protected Access Credential)가 필요하지 않기 때문입니다. PAC는 일반적으로 디바이스와 ISE(Identity Services Engine) 간의 보안 통신에 필요합니다. 이 접근 방식은 여러 ISE 노드가 있는 환경에서 특히 유용합니다. 기본 노드가 오프라인일 경우, 디바이스는 자격 증명을 다시 설정할 필요 없이 자동으로 백업으로 전환하여 중단을 줄일 수 있습니다. PAC 없는 인증은 프로세스를 간소화하여 확장성과 사용자 친화성을 높이고 제로 트러스트 원칙에 부합하는 최신 보안 방법을 지원합니다.

이 모드에서는 디바이스가 사용자 이름 및 비밀번호를 포함하는 요청을 전송하는 것으로 시작합니다. ISE는 보안 세션을 제안하여 응답합니다. 이 세션이 설정되면 ISE는 보안 통신에 필요한 중요한 정보를 제공합니다. 여기에는 보안을 위한 키 및 서버 ID 및 타이밍과 같은 세부사항이 포함됩니다. 이 정보는 필요한 정책 및 데이터에 대한 안전하고 지속적인 액세스를 보장하는 데 사용됩니다.

구성

설정

스위치 구성

이 문서에서는 Cisco C9300 스위치를 사용하여 PAC 없는 인증을 구성합니다. 버전 17.15.1 이상을 실행하는 모든 스위치는 ISE(Identity Services Engine)를 사용하여 PAC 없는 인증을 수행할 수 있습니다.

1단계: 스위치의 컨피그레이션 터미널 아래에 있는 스위치의 RADIUS 서버 및 RADIUS 그룹을 구성합니다.

Radius 서버:

```
radius server
```

```
address ipv4
```

```
auth-port 1812 acct-port 1813
```

```
key
```

Radius 그룹:

```
aaa group server radius trustsec
server name
```

2단계: PAC-less 인증을 위해 RADIUS 서버 그룹을 cts authorization 및 dot1x에 매핑합니다.

CTS 매핑:

```
<#root>
cts authorization list
cts-mlist
    // cts-mlist is the name of the authorization list
```

Dot1x 인증:

```
<#root>
aaa authentication dot1x default group

aaa authorization network
cts-mlist
    group
```

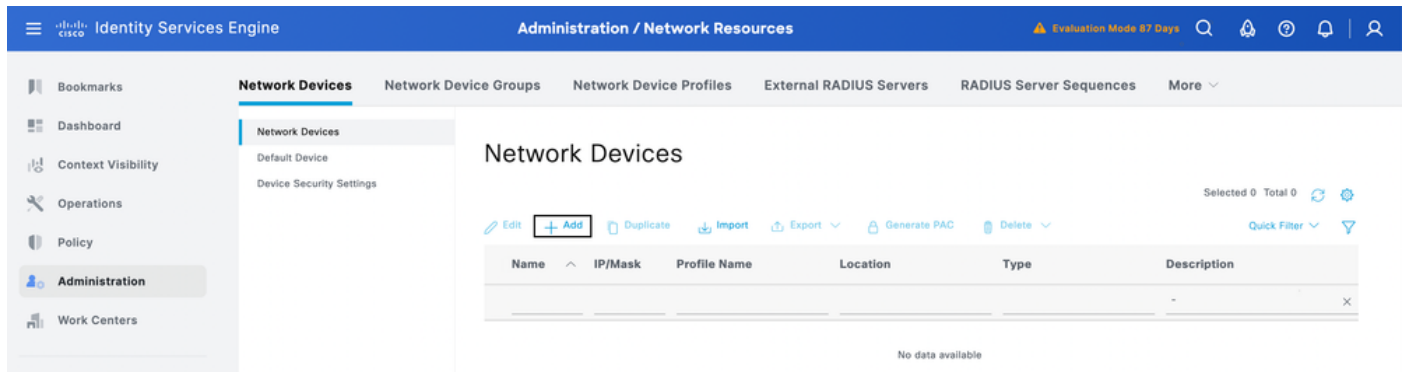
3단계: 스위치의 enable 모드에서 CTS-ID 및 비밀번호를 구성합니다

```
cts credentials id

password
```

ISE 구성

1. ISE에서 Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스) > Network Devices(네트워크 디바이스)에서 네트워크 디바이스를 구성합니다. ISE 서버에 스위치를 추가하려면 add(추가)를 클릭합니다.



2. ISE의 ip address 필드에 NAD IP 주소를 추가하여 스위치에서 trustsec 인증에 대한 radius 요청을 처리합니다.

3. NAD 클라이언트에 대한 Radius 인증 설정을 활성화 하고 Radius 공유 비밀 키를 입력 합니다.

4. 고급 Trustsec 설정을 활성화하고 디바이스 이름을 CTS-ID로 업데이트하고 비밀번호 필드를 명령의 비밀번호로 업데이트합니다(cts credentials id <CTS-ID> password <Password>).

Network Devices List 1 Test

Network Devices

Name test

Description

IP Address 10.10.10.10 32

Device Profile Cisco

Model Name

Software Version

Network Device Group

Location All Locations Set To Default

IPSEC No Set To Default

Device Type All Device Types Set To Default

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

Shared Secret Show

Use Second Shared Secret

Second Shared Secret Show

CoA Port 1700 Set To Default

RADIUS DTLS Settings

DTLS Required

Shared Secret radius/DTLS

CoA Port 2083 Set To Default

Issue CA of ISE Certificates for CoA Select if required (optional)

DNS Name

General Settings

Enable KeyWrap

Key Encryption Key Show

Message Authenticator Code Key Show

Key Input Format

ASCII HEXADECIMAL

TACACS Authentication Settings

SNMP Settings

Advanced TrustSec Settings

Device Authentication Settings

Use Device ID for TrustSec Identification

Device ID test

Password Show

HTTP REST API settings

Enable HTTP REST API

Username

Password

Support TrustSec Verification reports

TrustSec Notifications and Updates

Download environment data every 1 Days

Download peer authorization policy every 1 Days

Reauthentication every 1 Days

Live Logs

Live Sessions

Misconfigured Supplicants

Misconfigured Network Devices

RADIUS Drops

Client Stopped Responding

Repeat Counter

0

0

11

0

0

Refresh

Never

Show

Latest 20 records

Within

Last 3 hours

Reset Repeat Counts

Export To

Filter

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorizati...
Feb 23, 2025 08:16:12.0...	✓	🔒		#CTSREQUEST#			NetworkDeviceAuthorization	NetworkDevic...
Feb 23, 2025 08:16:05.7...	✓	🔒		#CTSREQUEST#			NetworkDeviceAuthorization	NetworkDevic...

Cisco ISE

Overview

Event

5233 TrustSec Data Download Succeeded

Username

#CTSREQUEST#

Endpoint Id

90:77:EE:EC:78:80

Endpoint Profile

Authentication Policy

NetworkDeviceAuthorization

Authorization Policy

NetworkDeviceAuthorization >> Default

Authorization Result

Authentication Details

Source Timestamp

2025-02-23 19:14:46.407

Received Timestamp

2025-02-23 19:14:46.407

Policy Server

ise341

Event

5233 TrustSec Data Download Succeeded

Username

#CTSREQUEST#

Endpoint Id

90:77:EE:EC:78:80

Calling Station Id

90:77:ee:ec:78:80

Authentication Method

webauth

Steps

Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request	
11017	RADIUS created a new session	0
12237	PAC-less request	0
11117	Generated a new session ID	1
15012	Selected Access Service	0
12238	Successfully processed PAC-less	0
15036	Evaluating Authorization Policy	0
15006	Matched Default Rule	6
11002	Returned RADIUS Access-Accept	3

문제 해결

문제를 해결하려면 스위치에서 다음 디버그를 실행하십시오.

Debug Command:

```
debug cts environment-data all
debug cts env
debug cts aaa
debug radius
debug cts ifc events
```

```
debug cts authentication details
```

debug cts authorization all debug

디버그 코드 조각:

*2월 23일 14:48:14.974: CTS 환경 데이터: 강제로 환경 데이터 새로 고침 비트 마스크 0x2

*2월 23일 14:48:14.974: CTS 환경 데이터: download transport-type =
CTS_TRANSPORT_IP_UDP

*2월 23일 14:48:14.974: cts_env_data 완료: 상태 env_data_complete 중에 이벤트
0(env_data_request)을 가져왔습니다.

*2월 23일 14:48:14.974: @@ cts_env_data 완료: env_data_complete -> env_data_waiting_rsp

*2월 23일 14:48:14.974: env_data_waiting_rsp_enter 상태 = WAITING_RESPONSE

*2월 23일 14:48:14.974: 디바이스에 보안 키가 있으며 pac-less env-data 다운로드를 진행하고 스
위치에서 PAC-Less 인증을 시작합니다.

*2월 23일 14:48:14.974: cts_aaa_is_fragmented: (CTS env-data SM)NOT-FRAG attr_q(0)

*2월 23일 14:48:14.974: 환경 데이터 요청 작업: 상태 = WAITING_RESPONSE

*2월 23일 14:48:14.974: env_data_download_complete:

상태(FALSE), req(x0), rec(x0)

*2월 23일 14:48:14.974: 상태(FALSE), req(x0), rec(x0), expect(x81),

wait_for_server_list(x85), wait_for_multicast_SGT(xB5), wait_for_SGName_mapping_tbl(x1485),

wait_for_SG-EPG_tbl(x18085), wait_for_default_EPG_tbl(xC0085),

wait_for_default_SGT_tbl(x600085) wait_for_default_SERVICE_ENTRY_tbl(xC000085)

*2월 23일 14:48:14.974: 환경 데이터 요청 작업: 상태 = WAITING_RESPONSE, 수신 = 0x0 요청 =
0x0

*2월 23일 14:48:14.974: cts_env_data_aaa_req_setup: aaa_id = 15

*2월 23일 14:48:14.974: cts_aaa_req_setup: (CTS env-data SM)Private group is appears DEAD,
attempt public group

*2월 23일 14:48:14.974: cts_aaa_attr_add: AAA 요청(0x7AB57A6AA2C0)

*2월 23일 14:48:14.974: 사용자 이름 = #CTSREQUEST#

*2월 23일 14:48:14.974: AAA 컨텍스트 특성 추가: (CTS env-data SM)attr(테스트)

*2월 23일 14:48:14.974: cts-environment-data = 테스트

*2월 23일 14:48:14.974: cts_aaa_attr_add: AAA 요청(0x7AB57A6AA2C0)

*2월 23일 14:48:14.974: AAA 컨텍스트 특성 추가: (CTS env-data SM)attr(env-data-fragment)

*2월 23일 14:48:14.974: cts-device-capability = env-data-fragment

*2월 23일 14:48:14.974: cts_aaa_attr_add: AAA 요청(0x7AB57A6AA2C0)

*2월 23일 14:48:14.975: AAA 컨텍스트 특성 추가: (CTS env-data SM)attr(다중 서버 IP 지원)

*2월 23일 14:48:14.975: cts-device-capability = 다중 서버 ip 지원

*2월 23일 14:48:14.975: cts_aaa_attr_add: AAA 요청(0x7AB57A6AA2C0)

*2월 23일 14:48:14.975: AAA 컨텍스트 특성 추가: (CTS env-data SM)attr(wnlx)

*2월 23일 14:48:14.975: clid = wnlx

*2월 23일 14:48:14.975: cts_aaa_req_send: AAA req(0x7AB57A6AA2C0)가 AAA에게 성공적으로 전송되었습니다.

*2월 23일 14:48:14.975: RADIUS/ENCODE(0000000F):원래 구성 요소 유형 = CTS

*2월 23일 14:48:14.975: RADIUS(0000000F): 구성 NAS IP: 0.0.0.0

*2월 23일 14:48:14.975: vrfid: [65535] ipv6 tableid: [0]

*2월 23일 14:48:14.975: idb가 NULL입니다.

*2월 23일 14:48:14.975: RADIUS(0000000F): 구성 NAS IPv6: ::

*2월 23일 14:48:14.975: RADIUS/ENCODE(0000000F): 계정_세션_id: 4003

*2월 23일 14:48:14.975: RADIUS(0000000F): 전송

*2월 23일 14:48:14.975: RADIUS: PAC less mode(PAC 없음 모드), secret is present(암호가 있음)

*2월 23일 14:48:14.975: RADIUS: CTS pacless 특성을 radius 요청에 추가했습니다.

*2월 23일 14:48:14.975: RADIUS/인코딩: Radius-Server 10.127.196.169용 최상의 로컬 IP 주소 10.127.196.234

*2월 23일 14:48:14.975: RADIUS: PAC less mode(PAC 없음 모드), secret is present(암호가 있음)

*2월 23일 14:48:14.975: RADIUS(0000000F): 스위치에서 10.127.196.169:1812 id 1645/11, len 249 // Radius Access Request로 액세스 요청 전송

RADIUS: 인증자 78 8A 70 5C E5 D3 DD F1 - B4 82 57 E2 1F 95 3B 92

*2월 23일 14:48:14.975: RADIUS: 사용자 이름 [1] 14 "#CTSREQUEST#"

*2월 23일 14:48:14.975: RADIUS: 공급업체, Cisco [26] 33

*2월 23일 14:48:14.975: RADIUS: Cisco AVpair [1] 27 "cts-environment-data=test"

*2월 23일 14:48:14.975: RADIUS: 공급업체, Cisco [26] 47

*2월 23일 14:48:14.975: RADIUS: Cisco AVpair [1] 41 "cts-device-capability=env-data-fragment"

*2월 23일 14:48:14.975: RADIUS: 공급업체, Cisco [26] 58

*2월 23일 14:48:14.975: RADIUS: Cisco AVpair [1] 52 "cts-device-capability=multiple-server-ip-supported"

*2월 23일 14:48:14.975: RADIUS: 사용자 암호 [2] 18 *

*2월 23일 14:48:14.975: RADIUS: Calling-Station-Id [31] 8 "wnlx"

*2월 23일 14:48:14.975: RADIUS: Service-Type [6] 6 Outbound [5]

*2월 23일 14:48:14.975: RADIUS: NAS-IP-Address [4] 6 10.127.196.234

*2월 23일 14:48:14.975: RADIUS: 공급업체, Cisco [26] 39

*2월 23일 14:48:14.975: RADIUS: Cisco AVpair [1] 33 "cts-pac-capability=cts-pac-less" // CTS PAC Less cv-pair 특성은 ISE가 PAC 없는 인증을 위해 패킷을 처리하도록 하는 요청에 추가합니다

*2월 23일 14:48:14.975: RADIUS(0000000F): IPv4 Radius 패킷 전송

*2월 23일 14:48:14.975: RADIUS(0000000F): 5초 시간 초과 시작됨

*2월 23일 14:48:14.990: RADIUS: id 1645/11 10.127.196.169:1812에서 수신, Access-Accept, len 313. // 인증 성공

RADIUS: 인증자 92 4C 21 5C 99 28 64 8B - 23 06 4B 87 F6 FF 66 3C

*2월 23일 14:48:14.990: RADIUS: 사용자 이름 [1] 14 "#CTSREQUEST#"

*2월 23일 14:48:14.990: RADIUS: 클래스 [25] 78

RADIUS: 43 41 43 53 3A 30 61 37 66 63 34 61 39 54 37 68 [CACS:0a7fc4a9T7h]

RADIUS: 39 79 44 42 70 2F 7A 6A 64 66 66 56 49 55 74 4D [9yDBp/zjdffVIUtM]

RADIUS: 78 34 68 63 50 4C 4A 45 49 76 75 79 51 62 4C 70 [x4hcPLJElvuyQbLp]

RADIUS: 31 48 7A 35 50 45 39 38 3A 69 73 65 33 34 31 2F [1Hz5PE98:ise341/]

RADIUS: 35 32 39 36 36 39 30 32 31 2F 32 31 [529669021/21]

*2월 23일 14:48:14.990: RADIUS: 공급업체, Cisco [26] 39

*2월 23일 14:48:14.990: RADIUS: Cisco AVpair [1] 33 "cts-pac-capability=cts-pac-less"

*2월 23일 14:48:14.990: RADIUS: 공급업체, Cisco [26] 43

*2월 23일 14:48:14.991: RADIUS: Cisco AVpair [1] 37 "cts:server-list=CTSServerList1-0001"

*2월 23일 14:48:14.991: RADIUS: 공급업체, Cisco [26] 38

*2월 23일 14:48:14.991: RADIUS: Cisco AVpair [1] 32 "cts:security-group-tag=0002-00"

*2월 23일 14:48:14.991: RADIUS: 공급업체, Cisco [26] 41

*2월 23일 14:48:14.991: RADIUS: Cisco AVpair [1] 35 "cts:environment-data-expiry=86400"

*2월 23일 14:48:14.991: RADIUS: 공급업체, Cisco [26] 40

*2월 23일 14:48:14.991: RADIUS: Cisco AVpair [1] 34 "cts:security-group-table=0001-17"

*2월 23일 14:48:14.991: RADIUS: PAC less mode(PAC 없음 모드), secret is present(암호가 있음)

*2월 23일 14:48:14.991: RADIUS(0000000F): ID 1645/11에서 수신됨

*2월 23일 14:48:14.991: cts_aaa_callback: (CTS env-data SM)AAA req(0x7AB57A6AA2C0) 응답 성공

*2월 23일 14:48:14.991: AAA CTX FRAG 정상: (CTS env-data SM)attr(테스트)

*2월 23일 14:48:14.991: AAA CTX FRAG 정상: (CTS env-data SM)attr(env-data-fragment)

*2월 23일 14:48:14.991: AAA CTX FRAG 정상: (CTS env-data SM)attr(다중 서버 IP 지원)

*2월 23일 14:48:14.991: AAA CTX FRAG 정상: (CTS env-data SM)attr(wnlx)

*2월 23일 14:48:14.991: AAA 속성: 알 수 없는 유형(450)입니다.

*2월 23일 14:48:14.991: AAA 속성: 알 수 없는 유형(1324)입니다.

*2월 23일 14:48:14.991: AAA 속성: server-list = CTSServerList1-0001.

*2월 23일 14:48:14.991: SLIST 이름을 받았습니다. cts_is_slist_send_to_binos_req를 FALSE로 설정

*2월 23일 14:48:14.991: AAA 속성: security-group-tag = 0002-00.

*2월 23일 14:48:14.991: AAA 속성: environment-data-expiry = 86400.

*2월 23일 14:48:14.991: AAA 속성: security-group-table = 0001-17.CTS 환경 데이터: AAA 특성 수신 // 환경 데이터 다운로드

CTS_AAA_SLIST

첫 번째 Access-Accept에서 slist 이름(CTSServerList1)을 받았습니다.

slist 이름(CTSServerList1)이 있습니다.

CTS_AAA_SECURITY_GROUP_TAG

CTS_AAA_ENVIRONMENT_DATA_EXPIRY = 86400.

CTS_AAA_SGT_NAME_LIST

테이블(0001)이 첫 번째 Access-Accept에서 수신됨

변경되지 않았으므로 테이블(0001)을 설치됨에서 수신됨으로 복사합니다.

새 이름(0001), 세대(17)

CTS_AAA_DATA_END

*2월 23일 14:48:14.991: cts_env_data WAITING_RESPONSE 상태 env_data_waiting_rsp 중에 이벤트 1(env_data_received)을 가져왔습니다.

*2월 23일 14:48:14.991: @@ cts_env_data 대기 중_응답: env_data_waiting_rsp -> env_data_assing

*2월 23일 14:48:14.991: env_data_assessing_enter: 상태 = 평가 중

*2월 23일 14:48:14.991: cts_aaa_is_fragmented: (CTS env-data SM)NOT-FRAG attr_q(0)

*2월 23일 14:48:14.991: env_data_assessing_action: 상태 = 평가 중

*2월 23일 14:48:14.991: env_data_download_complete:

상태(FALSE), 요청(x81), rec(xC87)

*2월 23일 14:48:14.991: 수신과 동일

*2월 23일 14:48:14.991: 상태(TRUE), 요청(x81), rec(xC87), 예상(x81),

wait_for_server_list(x85), wait_for_multicast_SGT(xB5), wait_for_SGName_mapping_tbl(x1485),

wait_for_SG-EPG_tbl(x18085), wait_for_default_EPG_tbl(xC0085),

wait_for_default_SGT_tbl(x600085) wait_for_default_SERVICE_ENTRY_tbl(xC000085)

*2월 23일 14:48:14.991: cts_env_data 평가: 상태 env_data_assessing 중 이벤트 4(env_data_complete)를 가져왔습니다.

*2월 23일 14:48:14.991: @@ cts_env_data 평가: env_data_assessing -> env_data_complete

*2월 23일 14:48:14.991: env_data_complete_enter: 상태 = 완료

*2월 23일 14:48:14.991: CTS-ifc-ev: env data reporting to core, 결과: 성공

*2월 23일 14:48:14.991: env_data_install_action state = COMPLETE.types 0x0

*2월 23일 14:48:14.991: env_data_install_action 정상 설치된 sgt<->sgname 테이블

*2월 23일 14:48:14.991: 설치된 sg-epg 목록 정리

*2월 23일 14:48:14.991: 설치된 기본 EPG 목록 정리

*2월 23일 14:48:14.991: env_data_install_action mcast_sgt 테이블 업데이트됨

*2월 23일 14:48:14.991: 환경 데이터를 대기 상태로 동기화 2

*2월 23일 14:48:14.991: SLIST는 이전 새로 고침과 동일합니다. BINOS로 보낼 필요 없음

*2월 23일 14:48:14.991: CTS-sg-epg-events:환경 데이터에 default_sg 0 설정

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.