ISE에서 OCSP를 사용하여 EAP-TLS 인증 구성

목차

소개

이 문서에서는 실시간 클라이언트 인증서 해지 확인을 위해 OCSP를 사용하여 EAP-TLS 인증을 설정하는 데 필요한 단계를 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Identity Services Engine 구성
- Cisco Catalyst 구성
- 온라인 인증서 상태 프로토콜

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

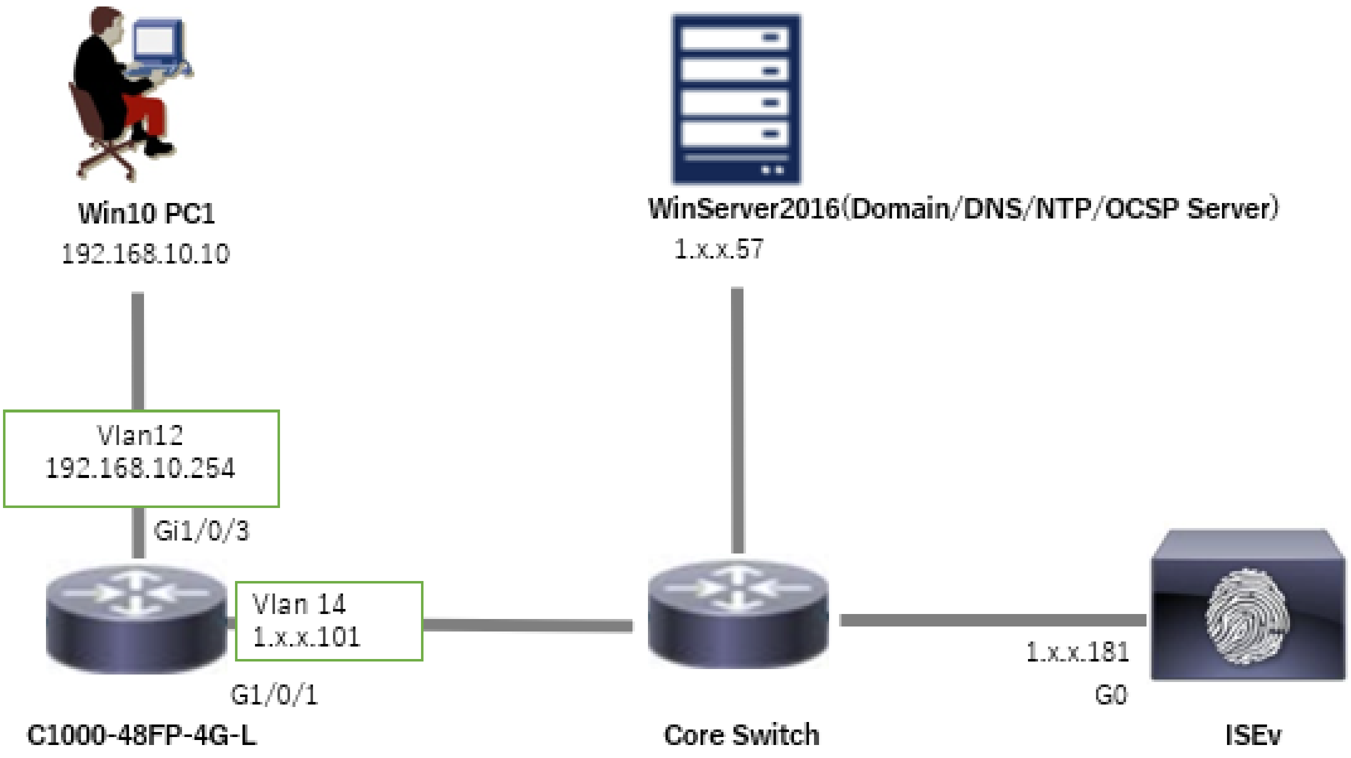
- Identity Services Engine Virtual 3.2 패치 6
- C1000-48FP-4G-L 15.2(7)E9

- Windows Server 2016
- Windows 10

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.

네트워크 다이어그램

이 그림에서는 이 문서의 예에 사용된 토폴로지를 보여줍니다.



네트워크 다이어그램

배경 정보

EAP-TLS에서 클라이언트는 인증 프로세스의 일부로 서버에 디지털 인증서를 제공합니다. 이 문서에서는 ISE가 AD 서버에 대해 인증서 CN(Common Name)을 확인하고 실시간 프로토콜 상태를 제공하는 OCSP(Online Certificate Status Protocol)를 사용하여 인증서가 폐기되었는지 확인하여 클라이언트 인증서를 검증하는 방법에 대해 설명합니다.

Windows Server 2016에 구성된 도메인 이름은 ad.rem-xxx.com이며 이 문서의 예제로 사용됩니다.

이 문서에서 참조하는 OCSP(Online Certificate Status Protocol) 및 AD(Active Directory) 서버가 인증서 검증에 사용됩니다.

- Active Directory FQDN: winserver.ad.rem-xxx.com
- CRL 배포 URL: http://winserver.ad.rem-xxx.com/ocsp-ca.crl
- 권한 URL: http://winserver.ad.rem-xxx.com/ocsp

이는 문서에 사용된 각 인증서의 공통 이름을 가진 인증서 체인입니다.

- CA: ocsp-ca-common-name
- 클라이언트 인증서: clientcertCN
- 서버 인증서: ise32-01.ad.rem-xxx.com
- OCSP 서명 인증서: ocspSignCommonName

설정

C1000의 컨피그레이션

이는 C1000 CLI의 최소 컨피그레이션입니다.

```
aaa new-model

radius server ISE32
address ipv4 1.x.x.181
key cisco123

aaa group server radius AAASERVER
server name ISE32

aaa authentication dot1x default group AAASERVER
aaa authorization network default group AAASERVER
aaa accounting dot1x default start-stop group AAASERVER
dot1x system-auth-control

interface Vlan12
ip address 192.168.10.254 255.255.255.0

interface Vlan14
ip address 1.x.x.101 255.0.0.0

interface GigabitEthernet1/0/1
Switch port access vlan 14
Switch port mode access

interface GigabitEthernet1/0/3
```

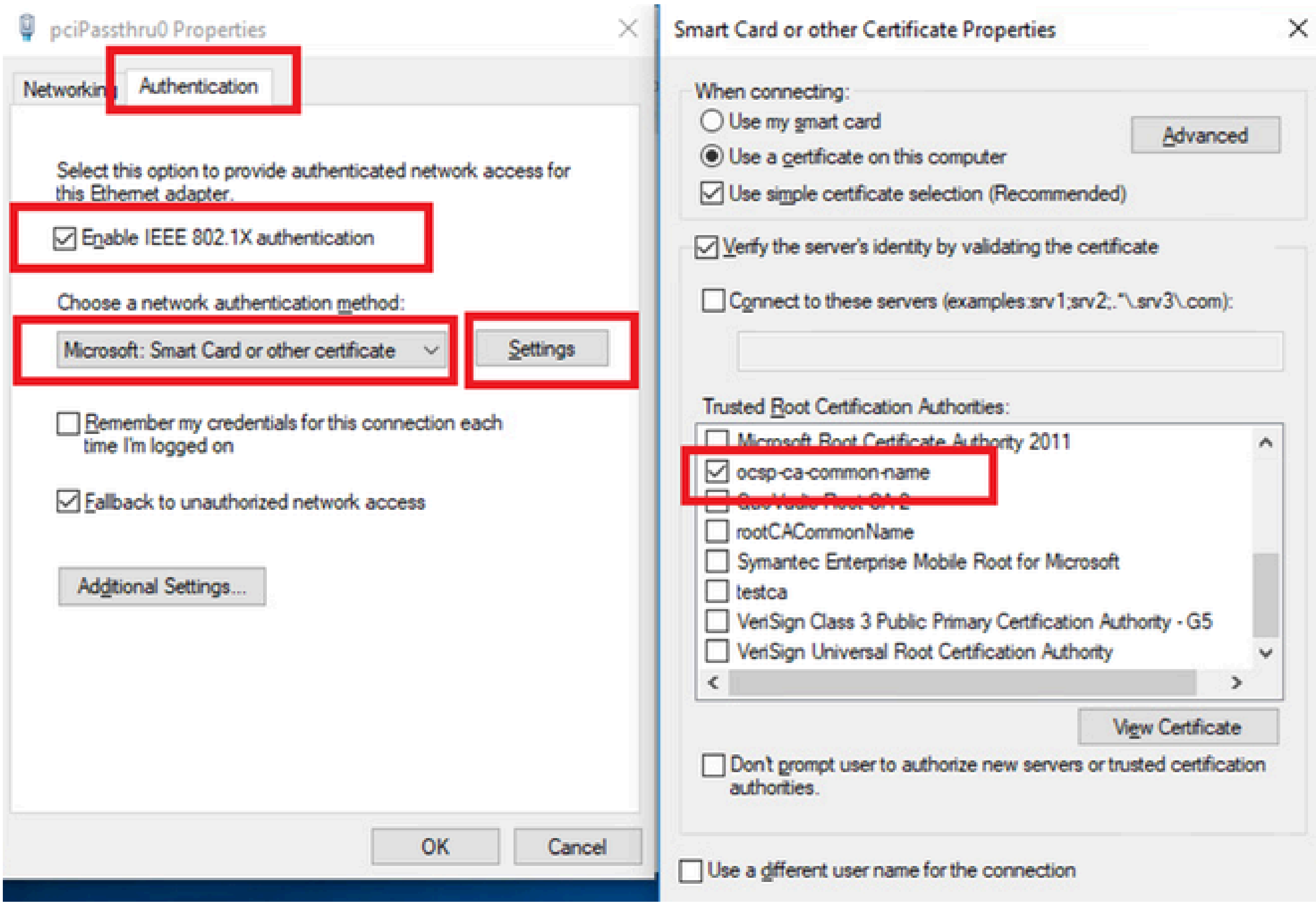
```
switchport access vlan 12
switchport mode access
authentication host-mode multi-auth
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge
```

Windows PC의 구성

1단계. 사용자 인증 구성

Authentication(인증)으로 이동하여 Enable IEEE 802.1X authentication(IEEE 802.1X 인증 활성화)을 선택하고 Microsoft: Smart Card or other certificate(Microsoft: 스마트 카드 또는 기타 인증서)를 선택합니다.

설정단추를 클릭하고 이 컴퓨터의 인증서 사용을 선택한 다음 Windows PC의 신뢰할 수 있는 CA를 선택합니다.



pciPassthru0 Properties

Select this option to provide authenticated network access for this Ethernet adapter.

☑ Enable IEEE 802.1X authentication

Choose a network authentication method:
Microsoft: Smart Card or other certificate

☐ Remember my credentials for this connection each time I'm logged on

☑ Fallback to unauthorized network access

Smart Card or other Certificate Properties

When connecting:
○ Use my smart card
● Use a certificate on this computer
☑ Use simple certificate selection (Recommended)

☑ Verify the server's identity by validating the certificate

☐ Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):

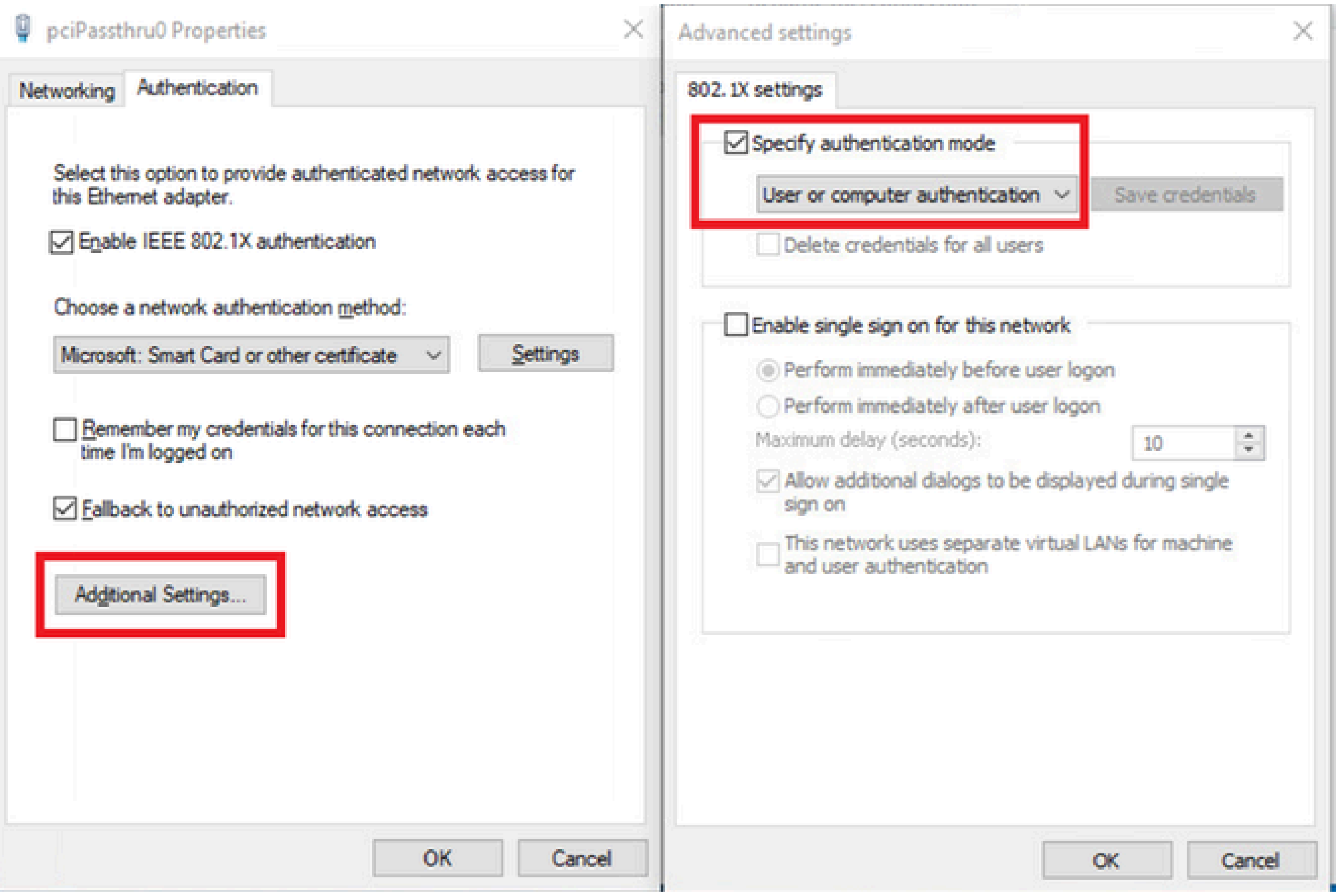
Trusted Root Certification Authorities:
☐ Microsoft Root Certificate Authority 2011
☑ ocsp-ca-common-name
☐ QuoVadis Root CA 2
☐ rootCACommonName
☐ Symantec Enterprise Mobile Root for Microsoft
☐ testca
☐ VeriSign Class 3 Public Primary Certification Authority - G5
☐ VeriSign Universal Root Certification Authority

☐ Don't prompt user to authorize new servers or trusted certification authorities.

☐ Use a different user name for the connection

인증서 인증 활성화

Authentication(인증), Additional Settings(추가 설정)로 이동합니다. 드롭다운 목록에서 사용자 또는 컴퓨터 인증을 선택합니다.



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: Smart Card or other certificate | Settings

☐ Remember my credentials for this connection each time I'm logged on

☑ Fallback to unauthorized network access

Additional Settings...

OK | Cancel

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 logon

○ Perform immediately after user logon

Maximum delay (seconds): 10

☑ Allow additional dialogs to be displayed during single sign on

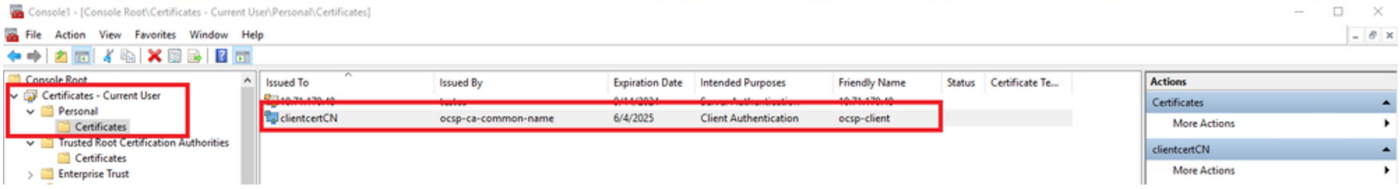
☐ This network uses separate virtual LANs for machine and user authentication

OK | Cancel

인증 모드 지정

2단계. 클라이언트 인증서 확인

Certificates - Current User > Personal > Certificates로 이동하고 인증에 사용되는 클라이언트 인증서를 확인합니다.



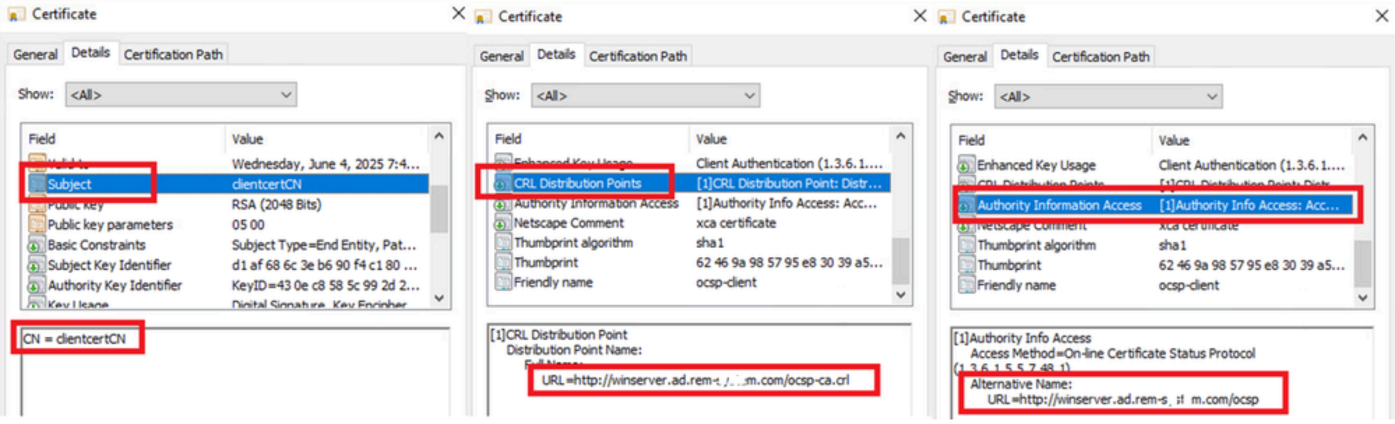
Console1 - [Console Root\Certificates - Current User\Personal\Certificates]

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Te...
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]		
clientcertCN	ocsp-ca-common-name	6/4/2025	Client Authentication	ocsp-client		

클라이언트 인증서 확인

클라이언트 인증서를 두 번 클릭하고 Details(세부사항)로 이동한 다음 Subject(주체), CRL Distribution Points(CRL 배포 지점), Authority Information Access(권한 정보 액세스)의 세부사항을 확인합니다.

- 제목: CN = clientcertCN
- CRL 배포 지점: http://winserver.ad.rem-xxx.com/ocsp-ca.crl
- 권한 정보 액세스: http://winserver.ad.rem-xxx.com/ocsp



Certificate

General Details Certification Path

Show: <All>

Field	Value
Valid to	Wednesday, June 4, 2025 7:4...
Subject	clientcertCN
Public key	RSA (2048 Bits)
Public key parameters	05 00
Basic Constraints	Subject Type=End Entity, Pat...
Subject Key Identifier	d1 af 68 6c 3e b6 90 f4 c1 80 ...
Authority Key Identifier	KeyID=43 0e c8 58 5c 99 2d 2...
Key Usage	Digital Signature, Key Enciphen

CN = clientcertCN

Field	Value
Enhanced Key Usage	Client Authentication (1.3.6.1....
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Netscape Comment	xca certificate
Thumbprint algorithm	sha1
Thumbprint	62 46 9a 98 57 95 e8 30 39 a5...
Friendly name	ocsp-client

[1]CRL Distribution Point
Distribution Point Name:
Full Name:
URL=http://winserver.ad.rem-s[redacted]m.com/ocsp-ca.crl

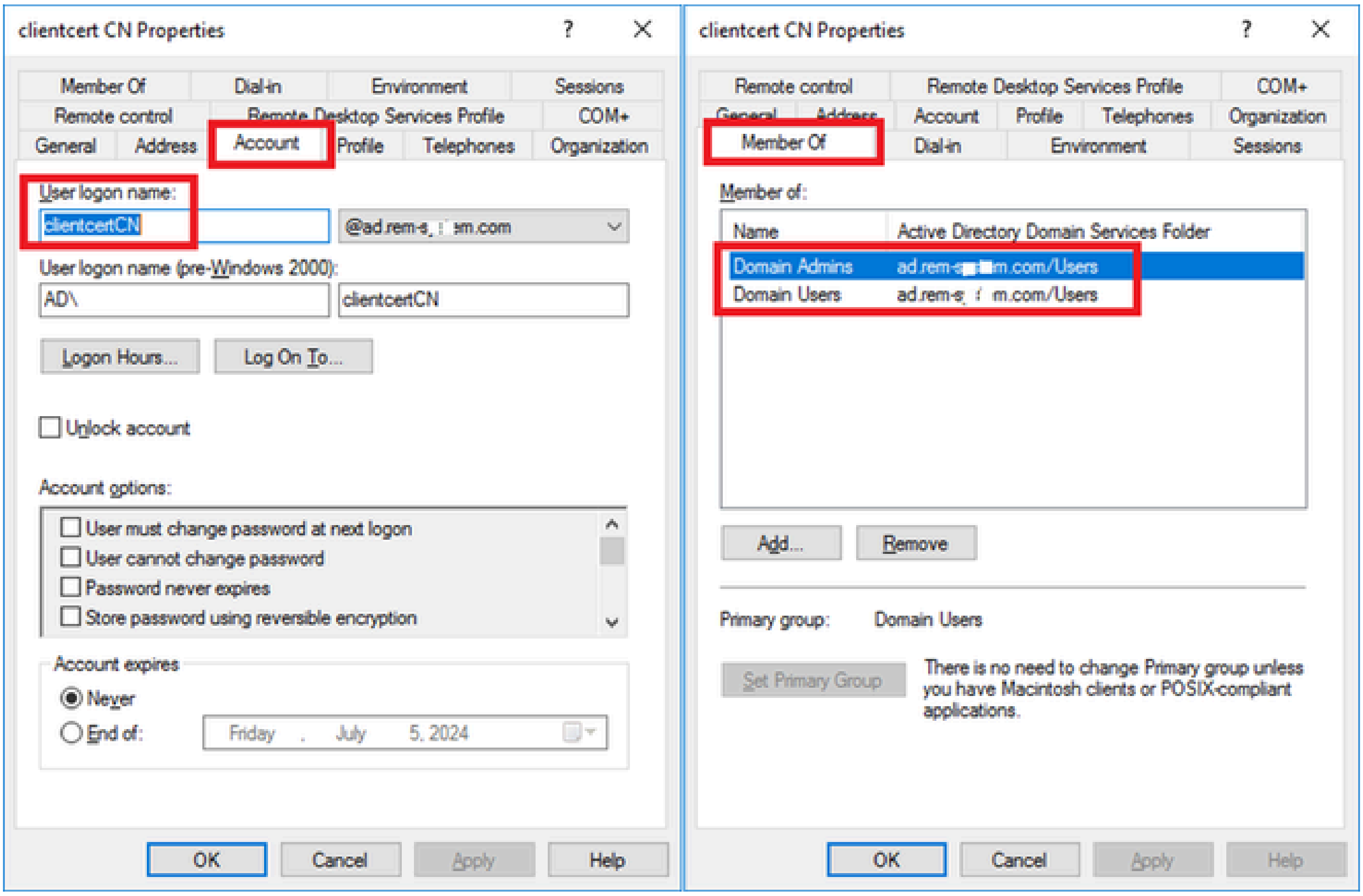
[1]Authority Info Access
Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)
Alternative Name:
URL=http://winserver.ad.rem-s[redacted]m.com/ocsp

클라이언트 인증서 세부 정보

Windows Server의 구성

1단계. 사용자 추가

Active Directory 사용자 및 컴퓨터로 이동한 다음 사용자를 클릭합니다. 사용자 로그온 이름으로 clientcertCN을 추가합니다.



clientcert CN Properties

Account

User logon name: clientcertCN @ad.rem-s[redacted]m.com

User logon name (pre-Windows 2000): AD\ clientcertCN

Account options:

- ☐ User must change password at next logon
- ☐ User cannot change password
- ☐ Password never expires
- ☐ Store password using reversible encryption

Account expires

- ● Never
- ○ End of: Friday , July 5, 2024

clientcert CN Properties

Member Of

Member of:

Name	Active Directory Domain Services Folder
Domain Admins	ad.rem-s[redacted]m.com/Users
Domain Users	ad.rem-s[redacted]m.com/Users

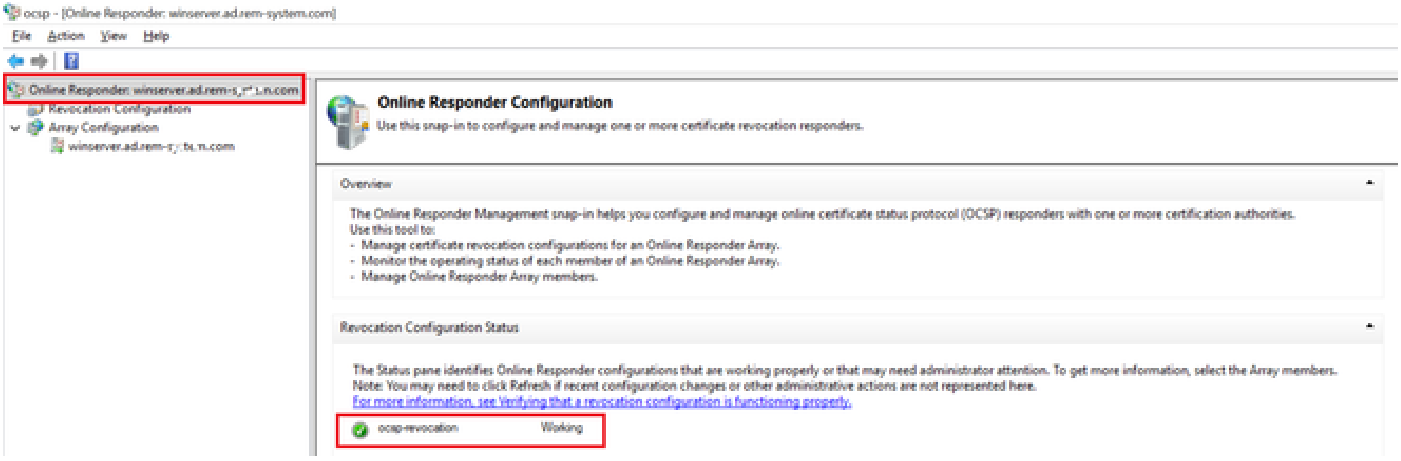
Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

사용자 로그온 이름

2단계. OCSP 서비스 확인

Windows로 이동하여 Online Responder Management를 클릭합니다. OCSP 서버의 상태를 확인합니다.


ocsp - [Online Responder: winserver.ad.rem-system.com]
File
Action
View
Help
Online Responder: winserver.ad.rem-s...n.com
Revocation Configuration
Array Configuration
winserver.ad.rem-s...n.com

Online Responder Configuration

Use this snap-in to configure and manage one or more certificate revocation responders.

Overview

The Online Responder Management snap-in helps you configure and manage online certificate status protocol (OCSP) responders with one or more certification authorities.
Use this tool to:
- Manage certificate revocation configurations for an Online Responder Array.
- Monitor the operating status of each member of an Online Responder Array.
- Manage Online Responder Array members.

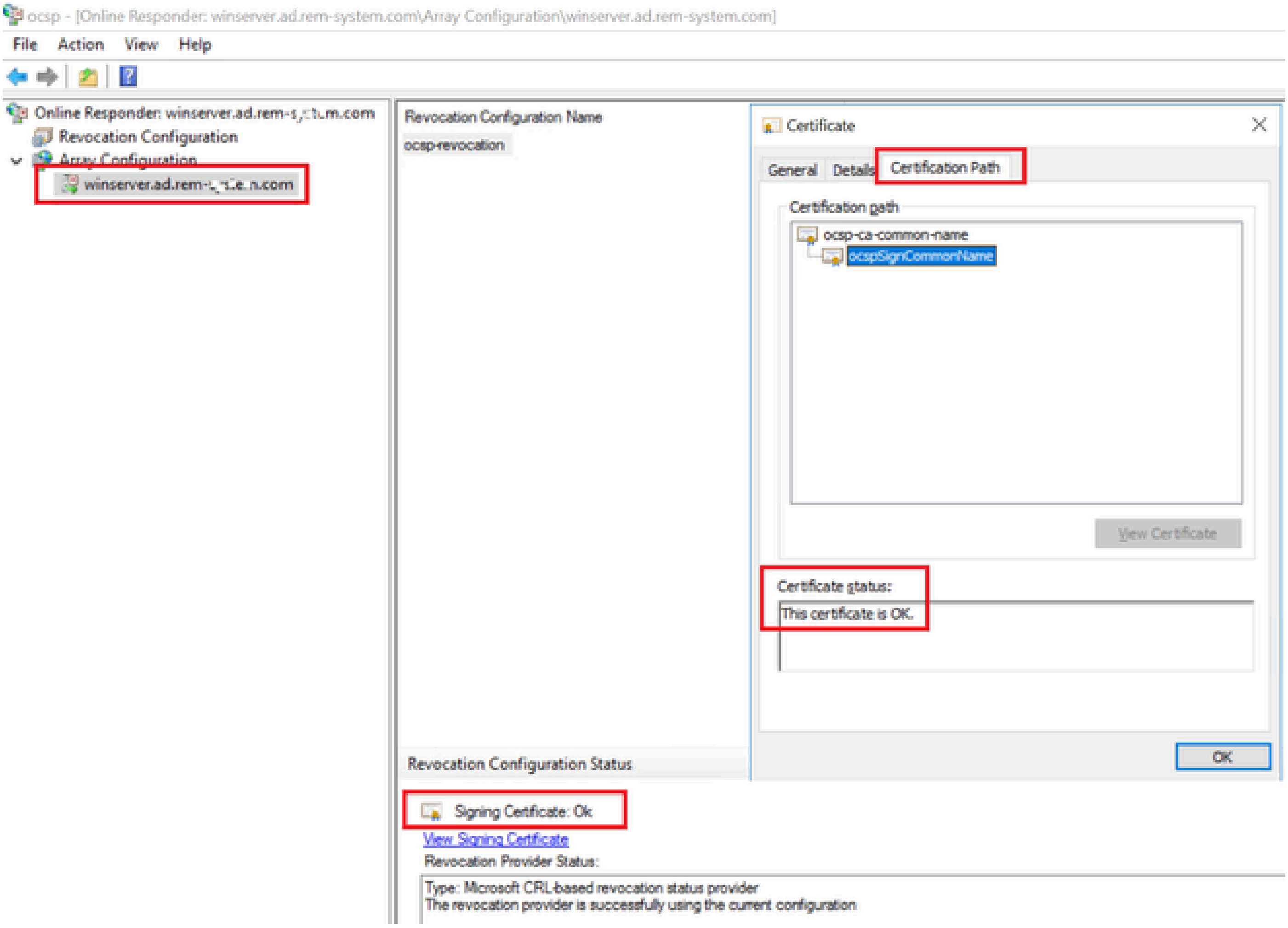
Revocation Configuration Status

The Status pane identifies Online Responder configurations that are working properly or that may need administrator attention. To get more information, select the Array members.
Note: You may need to click Refresh if recent configuration changes or other administrative actions are not represented here.
For more information, see Verifying that a revocation configuration is functioning properly.

ocsp-revocation Working

OCSP 서버 상태

winserver.ad.rem-xxx.com을 클릭하고 OCSP 서명 인증서의 상태를 확인합니다.


ocsp - [Online Responder: winserver.ad.rem-system.com\Array Configuration\winserver.ad.rem-system.com]
File
Action
View
Help
Online Responder: winserver.ad.rem-s...m.com
Revocation Configuration
Array Configuration
winserver.ad.rem-...e.n.com
Revocation Configuration Name
Certificate
General
Details
Certification Path
Certification path
ocsp-ca-common-name
ocspSignCommonName
View Certificate
OK
Revocation Configuration Status
View Signing Certificate

ocsp-revocation

Certificate status:
This certificate is OK.

Signing Certificate: Ok

Revocation Provider Status:
Type: Microsoft CRL-based revocation status provider
The revocation provider is successfully using the current configuration

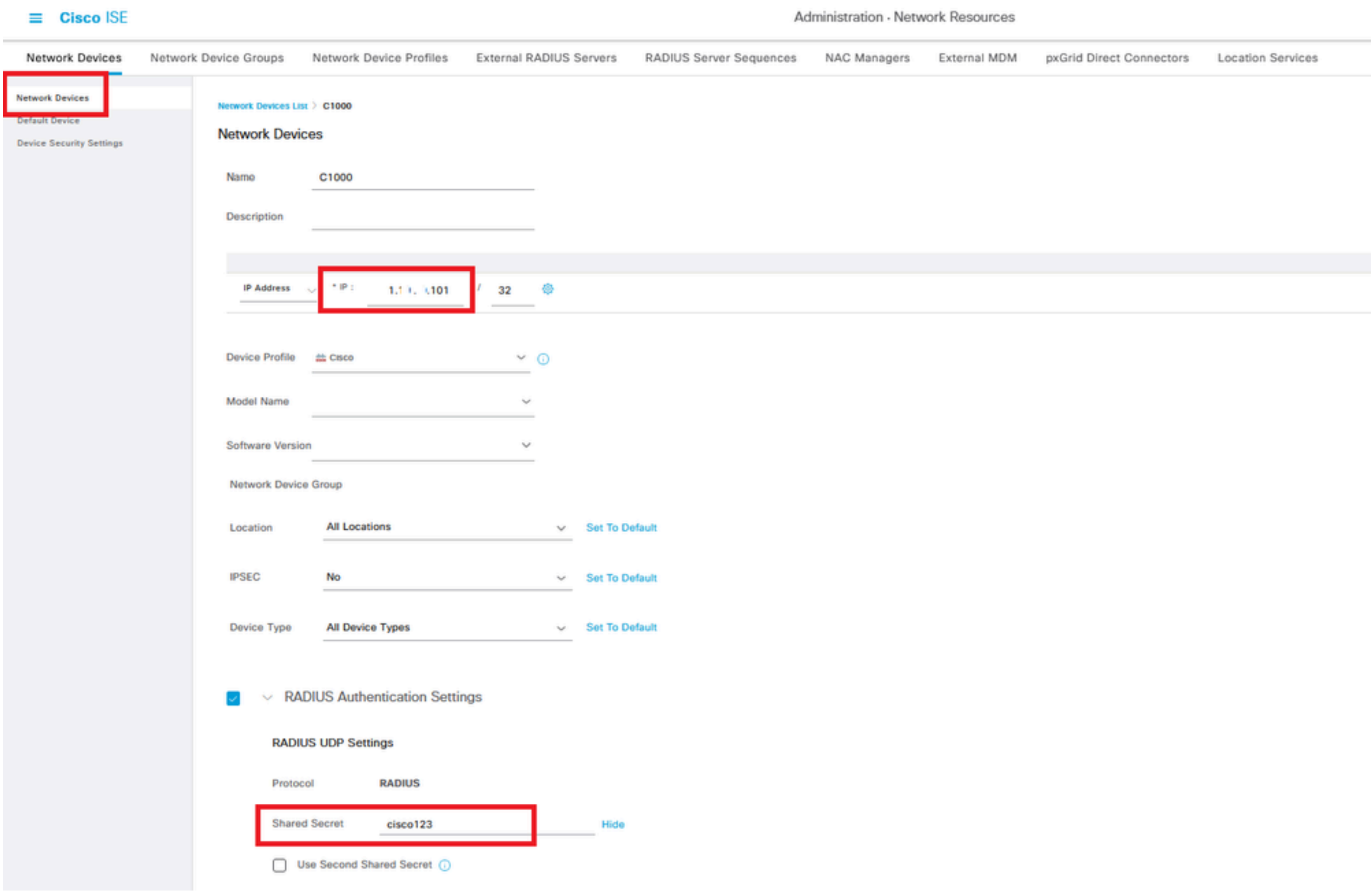
OCSP 서명 인증서 상태

ISE의 컨피그레이션

1단계. 장치 추가

Administration(관리) > Network Devices(네트워크 디바이스)로 이동하고 Add(추가)button(버튼)을

클릭하여 C1000 디바이스를 추가합니다.



Network Devices

Name: C1000

Description:

IP Address | * IP : 1.[redacted].101 / 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: cisco123 — Hide

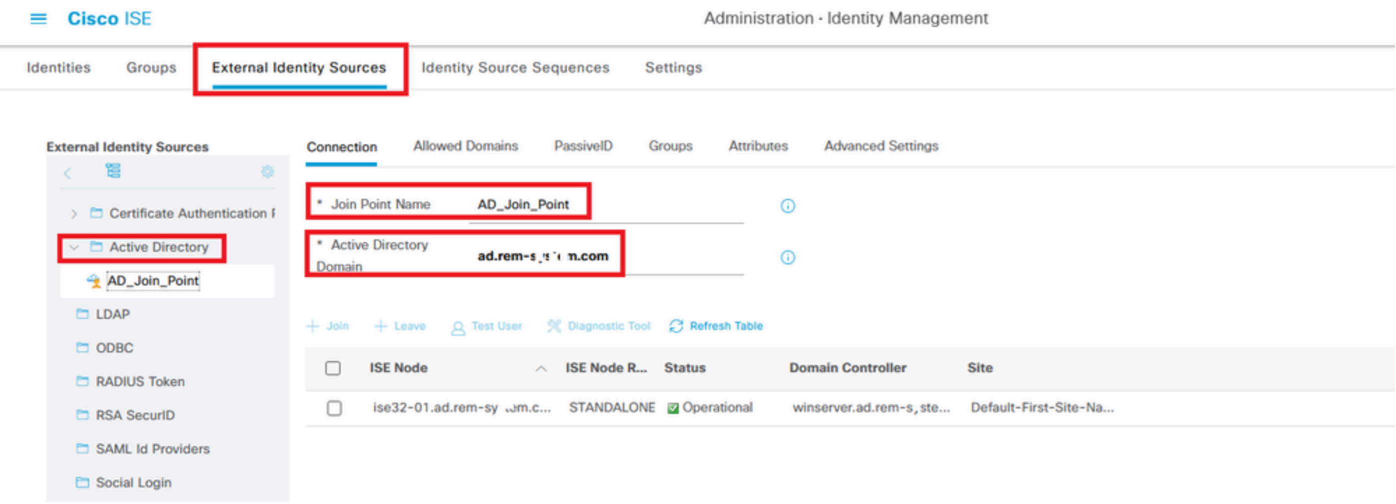
□ Use Second Shared Secret

장치 추가

2단계. Active Directory 추가

Administration(관리) > External Identity Sources(외부 ID 소스) > Active Directory로 이동하고 Connectiontab(연결 탭)을 클릭한 다음 Active Directory를 ISE에 추가합니다.

- 조인 지점 이름: AD_Join_Point
- Active Directory 도메인: ad.rem-xxx.com



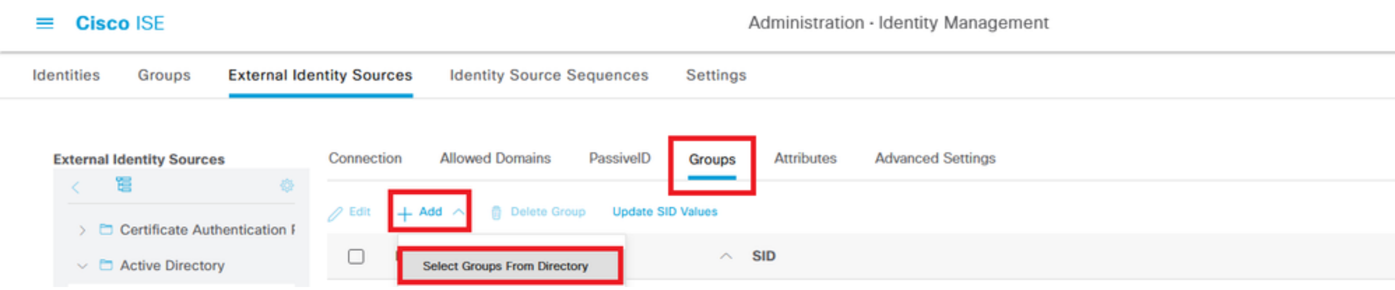
* Join Point Name: AD_Join_Point

* Active Directory Domain: ad.rem-s[redacted]n.com

□	ISE Node	ISE Node R...	Status	Domain Controller	Site
□	ise32-01.ad.rem-sy[redacted]m.c...	STANDALONE	✓ Operational	winserver.ad.rem-s[redacted]ste...	Default-First-Site-Na...

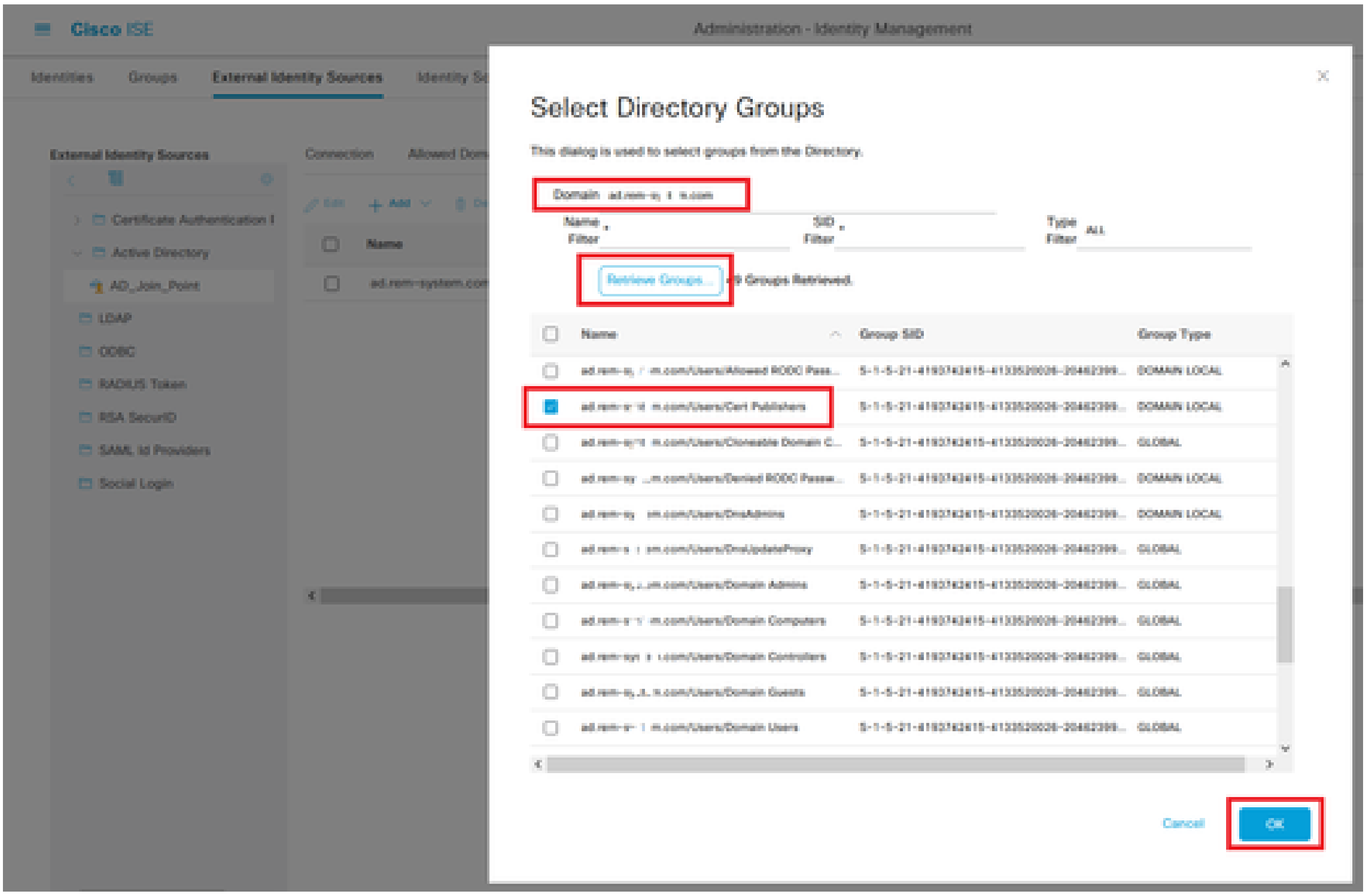
Active Directory 추가

그룹 탭으로 이동하고 드롭다운 목록에서 디렉터리에서 그룹 선택을 선택합니다.


Cisco ISE
Administration · Identity Management
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
External Identity Sources
Certificate Authentication I
Active Directory
Connection
Allowed Domains
PassiveID
Groups
Attributes
Advanced Settings
Edit
+ Add
Delete Group
Update SID Values
Select Groups From Directory
SID

디렉터리에서 그룹 선택

그룹 검색(Retrieve Groups)시작(From) 드롭다운 목록을 누릅니다. Checkad.rem-xxx.com/Users/Cert Publishers(게시자)를 클릭하고 OK(확인)를 클릭합니다.



Select Directory Groups

This dialog is used to select groups from the Directory.

Domain ad.rem-sy...m.com

Name Filter

SID Filter

Type Filter ALL

49 Groups Retrieved.

	Name	Group SID	Group Type
□	ad.rem-sy...m.com/Users/Allowed RODC Pass...	S-1-5-21-4193742415-4133520026-20462399...	DOMAIN LOCAL
☑	ad.rem-sy...m.com/Users/Cert Publishers	S-1-5-21-4193742415-4133520026-20462399...	DOMAIN LOCAL
□	ad.rem-sy...m.com/Users/Cloneable Domain C...	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
□	ad.rem-sy...m.com/Users/Denied RODC Passw...	S-1-5-21-4193742415-4133520026-20462399...	DOMAIN LOCAL
□	ad.rem-sy...m.com/Users/DnsAdmins	S-1-5-21-4193742415-4133520026-20462399...	DOMAIN LOCAL
□	ad.rem-sy...m.com/Users/DnsUpdateProxy	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
□	ad.rem-sy...m.com/Users/Domain Admins	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
□	ad.rem-sy...m.com/Users/Domain Computers	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
□	ad.rem-sy...m.com/Users/Domain Controllers	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
□	ad.rem-sy...m.com/Users/Domain Guests	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
□	ad.rem-sy...m.com/Users/Domain Users	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL

인증서 게시자 확인

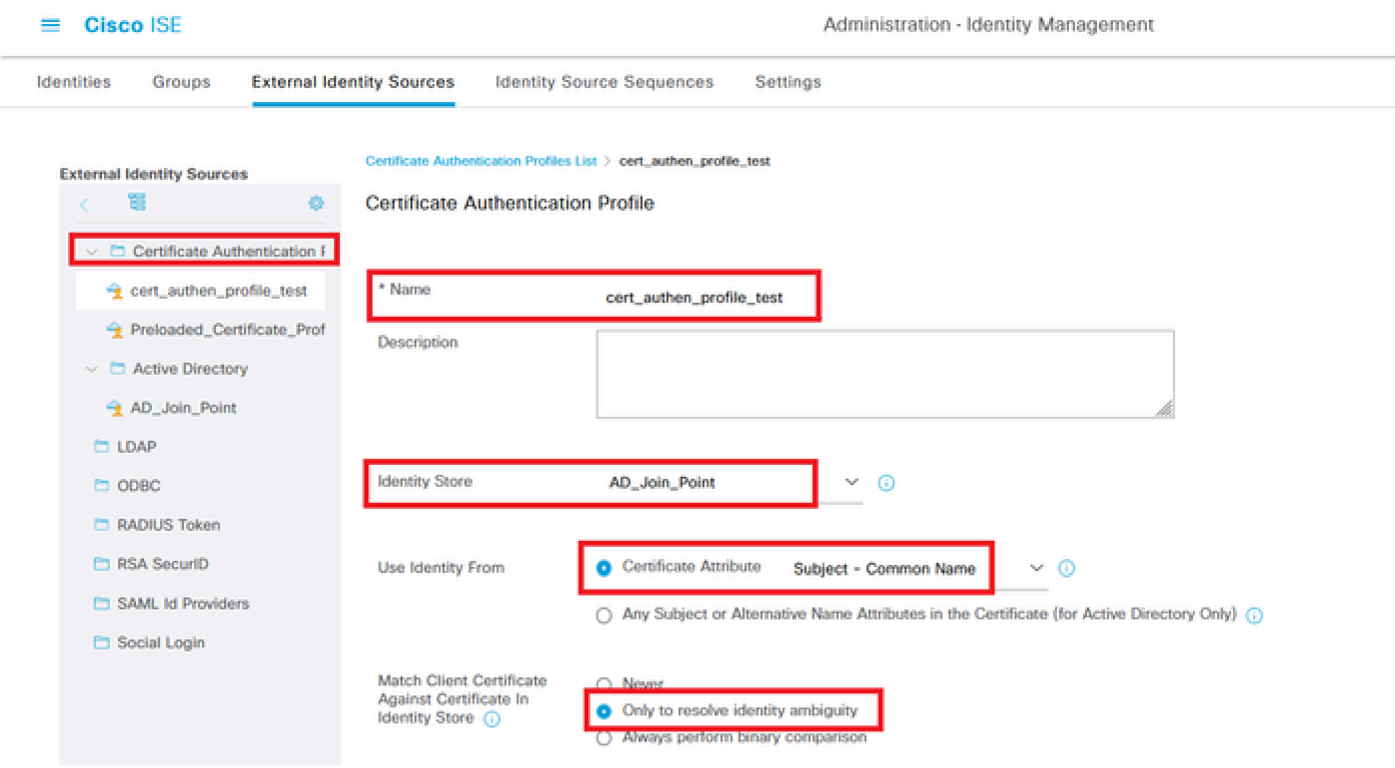
3단계. 인증서 인증 프로파일 추가

Administration(관리) > External Identity Sources(외부 ID 소스) > Certificate Authentication Profile(인증서 인증 프로파일)로 이동하고 Add(추가) 버튼을 클릭하여 새 인증서 인증 프로파일을 추가합니다.

- 이름: cert_authen_profile_test
- ID 저장소: AD_Join_Point
- Use Identity From Certificate Attribute: Subject - Common Name(인증서의 ID 사용 특성:

Subject - 공용 이름)

- ID 저장소의 인증서와 클라이언트 인증서 일치: ID 모호성을 해결하는 용도로만 사용됩니다.


≡ Cisco ISE
Administration · Identity Management
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
External Identity Sources
Certificate Authentication F
cert_authen_profile_test
Preloaded_Certificate_Prof
Active Directory
AD_Join_Point
LDAP
ODBC
RADIUS Token
RSA SecurID
SAML Id Providers
Social Login
Certificate Authentication Profiles List > cert_authen_profile_test

Certificate Authentication Profile

* Name cert_authen_profile_test

Description

Identity Store AD_Join_Point

Use Identity From ● Certificate Attribute Subject - Common Name
○ Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only)

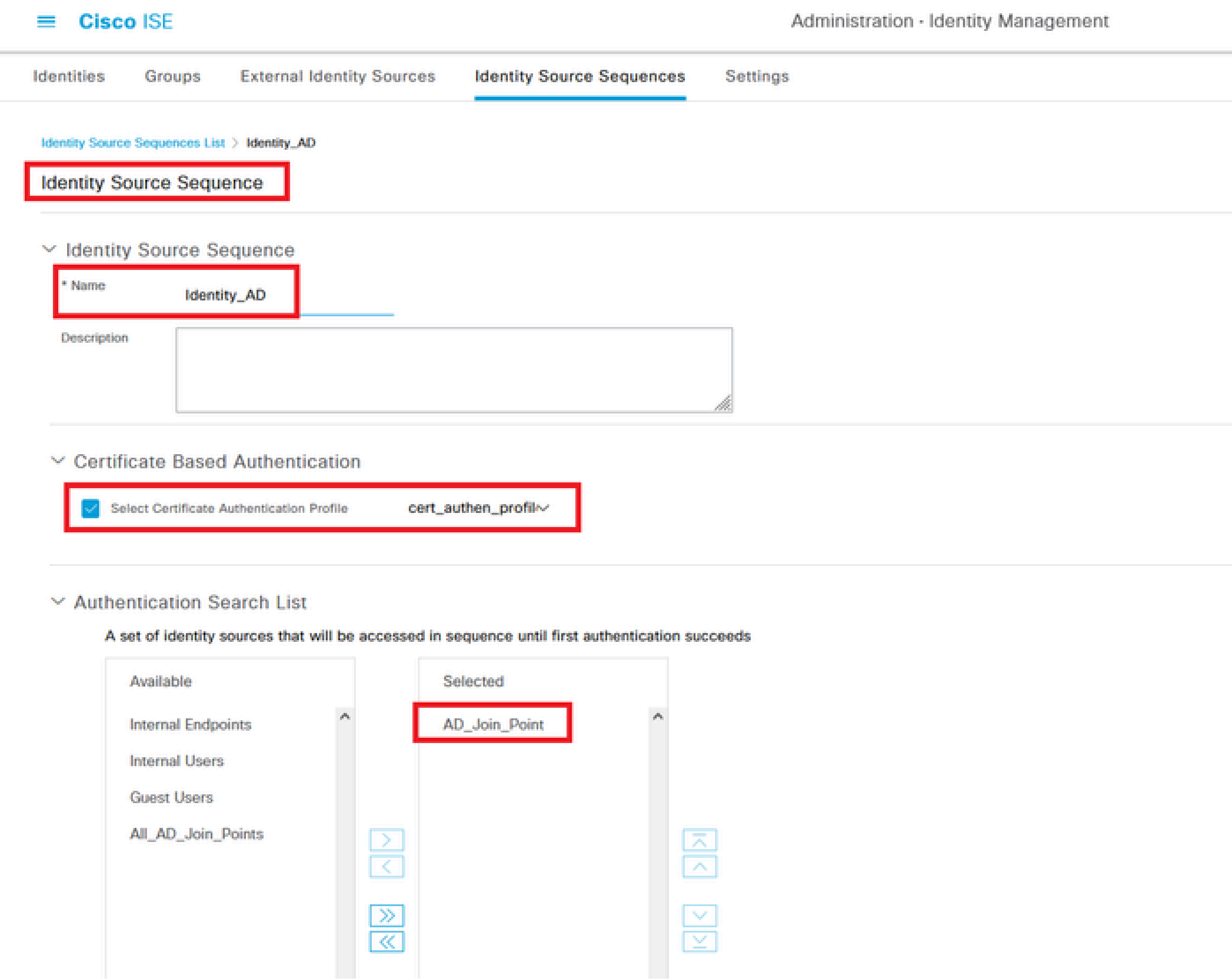
Match Client Certificate Against Certificate In Identity Store
○ Never
● Only to resolve identity ambiguity
○ Always perform binary comparison

인증서 인증 프로파일 추가

4단계. ID 소스 시퀀스 추가

Administration(관리) > Identity Source Sequences(ID 소스 시퀀스)로 이동하여 ID 소스 시퀀스를 추가합니다.

- 이름: Identity_AD
- Certificate Authentication Pro를 선택합니다file: cert_authen_profile_test
- 인증 검색 목록: AD_Join_Point


Cisco ISE
Administration · Identity Management
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
Identity Source Sequences List > Identity_AD

Identity Source Sequence

Identity Source Sequence

* Name Identity_AD

Description

Certificate Based Authentication

☑ Select Certificate Authentication Profile cert_authen_profil

Authentication Search List

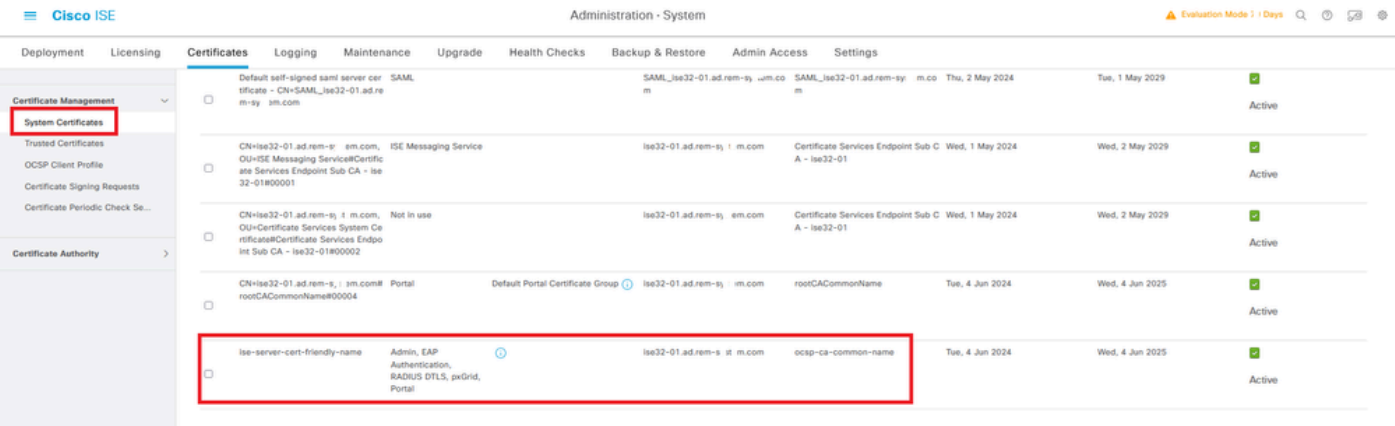
A set of identity sources that will be accessed in sequence until first authentication succeeds

Available	Selected
Internal Endpoints	AD_Join_Point
Internal Users	
Guest Users	
All_AD_Join_Points	

ID 소스 시퀀스 추가

5단계. ISE의 인증서 확인

Administration > Certificates > System Certificates로 이동하여 서버 인증서가 신뢰할 수 있는 CA에 의해 서명되었는지 확인합니다.



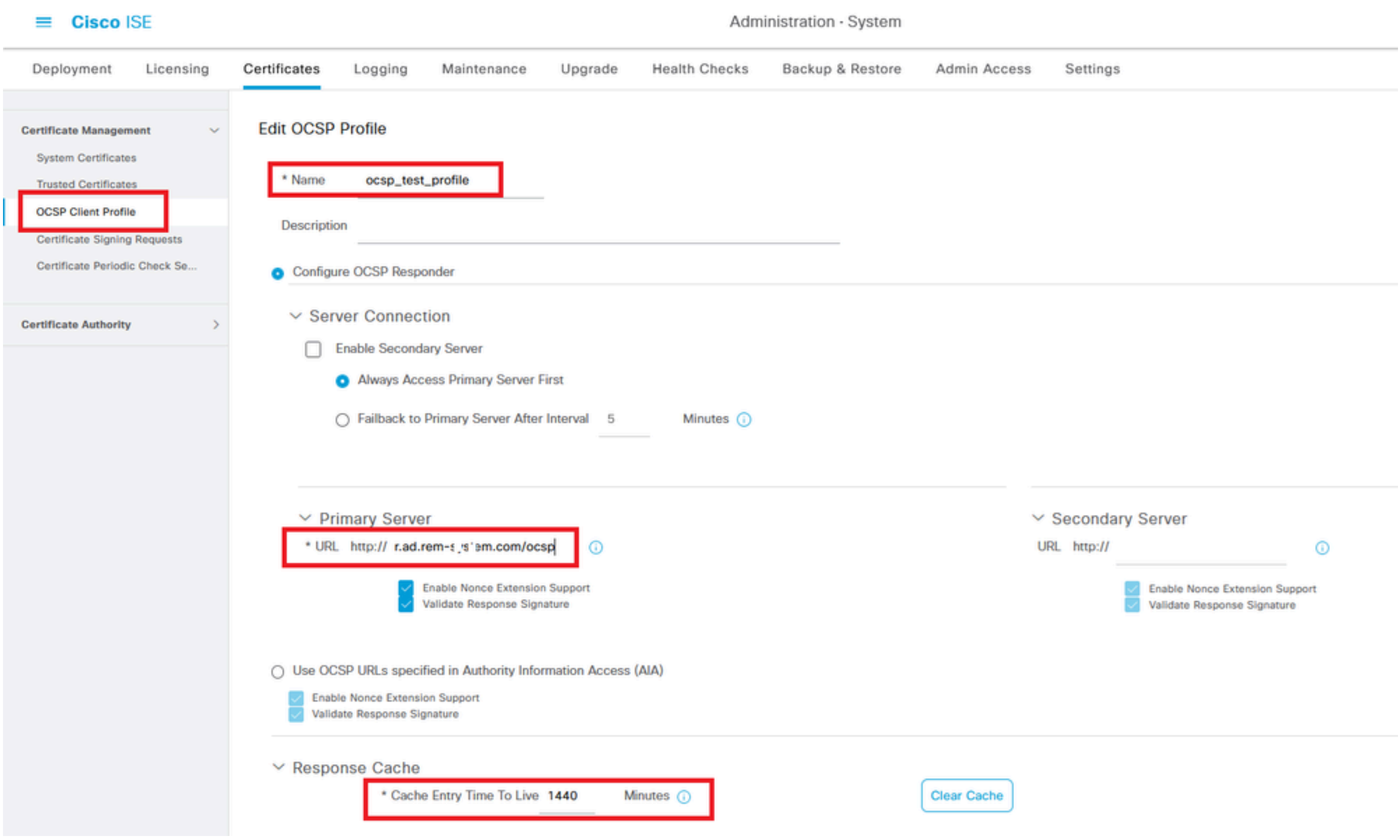
□	Default self-signed saml server certificate - CN=SAML_ise32-01.ad.rem-sy m.com	SAML		SAML_ise32-01.ad.rem-sy m.com	SAML_ise32-01.ad.rem-sy m.com	Thu, 2 May 2024	Tue, 1 May 2029	✓ Active
□	CN=ise32-01.ad.rem-s em.com, OU=ISE Messaging Service#Certificate Services Endpoint Sub CA - ise32-01#00001	ISE Messaging Service		ise32-01.ad.rem-sy m.com	Certificate Services Endpoint Sub CA - ise32-01	Wed, 1 May 2024	Wed, 2 May 2029	✓ Active
□	CN=ise32-01.ad.rem-sy m.com, OU=Certificate Services System Certificate#Certificate Services Endpoint Sub CA - ise32-01#00002	Not in use		ise32-01.ad.rem-sy em.com	Certificate Services Endpoint Sub CA - ise32-01	Wed, 1 May 2024	Wed, 2 May 2029	✓ Active
□	CN=ise32-01.ad.rem-s m.com#rootCACommonName#00004	Portal	Default Portal Certificate Group ⓘ	ise32-01.ad.rem-sy m.com	rootCACommonName	Tue, 4 Jun 2024	Wed, 4 Jun 2025	✓ Active
□	ise-server-cert-friendly-name	Admin, EAP Authentication, RADIUS DTLS, pxGrid, Portal	ⓘ	ise32-01.ad.rem-s m.com	ocsp-ca-common-name	Tue, 4 Jun 2024	Wed, 4 Jun 2025	✓ Active

서버 인증서

Administration(관리) > Certificates(인증서) > OCSP Client Profile(OCSP 클라이언트 프로파일)로

이동하고 Add(추가) 버튼을 클릭하여 새 OCSP 클라이언트 프로파일을 추가합니다.

- 이름: ocsp_test_profile
- OCSP 응답자 URL 구성: http://winserver.ad.rem-xxx.com/ocsp



Edit OCSP Profile

* Name ocsp_test_profile

Description

● Configure OCSP Responder

Server Connection

□ Enable Secondary Server

● Always Access Primary Server First

○ Failback to Primary Server After Interval 5 Minutes

Primary Server

* URL http:// r.ad.rem-s ,s 'em.com/ocsp

☑ Enable Nonce Extension Support
☑ Validate Response Signature

Secondary Server

URL http://

☑ Enable Nonce Extension Support
☑ Validate Response Signature

○ Use OCSP URLs specified in Authority Information Access (AIA)

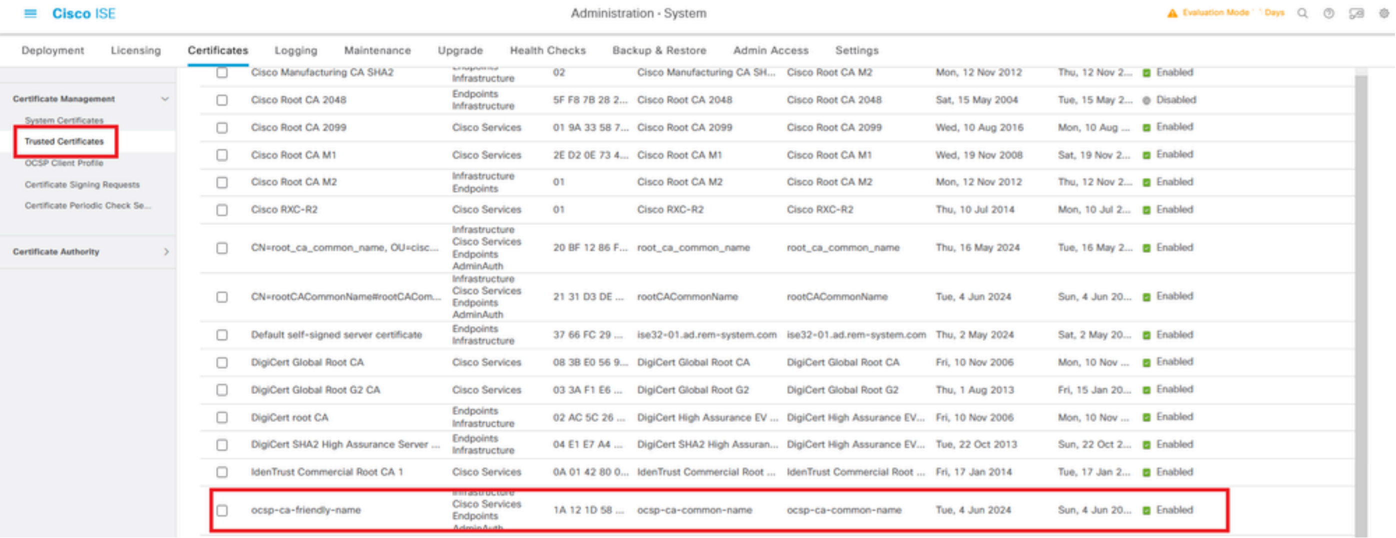
☑ Enable Nonce Extension Support
☑ Validate Response Signature

Response Cache

* Cache Entry Time To Live 1440 Minutes

OCSP 클라이언트 프로파일

Administration > Certificates > Trusted Certificates로 이동하여 신뢰할 수 있는 CA를 ISE로 가져오는지 확인합니다.

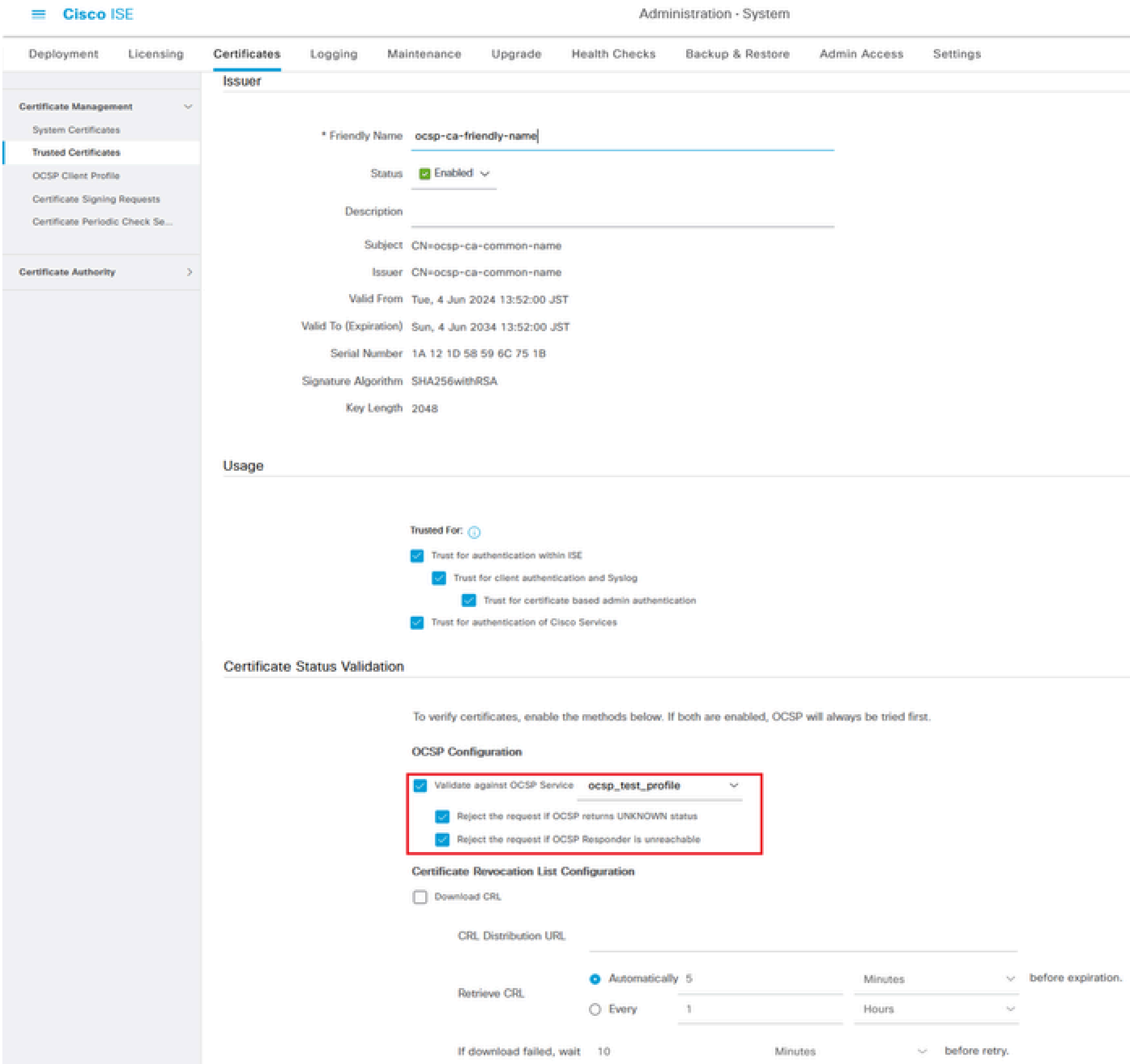


□	Cisco Manufacturing CA SHA2	Endpoints Infrastructure	02	Cisco Manufacturing CA SH...	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2...	🟩 Enabled
□	Cisco Root CA 2048	Endpoints Infrastructure	5F F8 7B 28 2...	Cisco Root CA 2048	Cisco Root CA 2048	Sat, 15 May 2004	Tue, 15 May 2...	● Disabled
□	Cisco Root CA 2099	Cisco Services	01 9A 33 58 7...	Cisco Root CA 2099	Cisco Root CA 2099	Wed, 10 Aug 2016	Mon, 10 Aug ...	🟩 Enabled
□	Cisco Root CA M1	Cisco Services	2E D2 0E 73 4...	Cisco Root CA M1	Cisco Root CA M1	Wed, 19 Nov 2008	Sat, 19 Nov 2...	🟩 Enabled
□	Cisco Root CA M2	Infrastructure Endpoints	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2...	🟩 Enabled
□	Cisco RXC-R2	Cisco Services	01	Cisco RXC-R2	Cisco RXC-R2	Thu, 10 Jul 2014	Mon, 10 Jul 2...	🟩 Enabled
□	CN=root_ca_common_name, OU=cisc...	Infrastructure Cisco Services Endpoints AdminAuth	20 BF 12 86 F...	root_ca_common_name	root_ca_common_name	Thu, 16 May 2024	Tue, 16 May 2...	🟩 Enabled
□	CN=rootCACommonName#rootCACom...	Infrastructure Cisco Services Endpoints AdminAuth	21 31 D3 DE ...	rootCACommonName	rootCACommonName	Tue, 4 Jun 2024	Sun, 4 Jun 20...	🟩 Enabled
□	Default self-signed server certificate	Endpoints Infrastructure	37 66 FC 29 ...	ise32-01.ad.rem-system.com	ise32-01.ad.rem-system.com	Thu, 2 May 2024	Sat, 2 May 20...	🟩 Enabled
□	DigiCert Global Root CA	Cisco Services	08 3B E0 56 9...	DigiCert Global Root CA	DigiCert Global Root CA	Fri, 10 Nov 2006	Mon, 10 Nov ...	🟩 Enabled
□	DigiCert Global Root G2 CA	Cisco Services	03 3A F1 E6 ...	DigiCert Global Root G2	DigiCert Global Root G2	Thu, 1 Aug 2013	Fri, 15 Jan 20...	🟩 Enabled
□	DigiCert root CA	Endpoints Infrastructure	02 AC 5C 26 ...	DigiCert High Assurance EV ...	DigiCert High Assurance EV...	Fri, 10 Nov 2006	Mon, 10 Nov ...	🟩 Enabled
□	DigiCert SHA2 High Assurance Server ...	Endpoints Infrastructure	04 E1 E7 A4 ...	DigiCert SHA2 High Assuran...	DigiCert High Assurance EV...	Tue, 22 Oct 2013	Sun, 22 Oct 2...	🟩 Enabled
□	IdenTrust Commercial Root CA 1	Cisco Services	0A 01 42 80 0...	IdenTrust Commercial Root ...	IdenTrust Commercial Root ...	Fri, 17 Jan 2014	Tue, 17 Jan 2...	🟩 Enabled
□	ocsp-ca-friendly-name	Infrastructure Cisco Services Endpoints AdminAuth	1A 12 1D 58 ...	ocsp-ca-common-name	ocsp-ca-common-name	Tue, 4 Jun 2024	Sun, 4 Jun 20...	🟩 Enabled

신뢰할 수 있는 CA

CA를 선택하고 Edit(편집) 버튼을 클릭하여 Certificate Status Validation(인증서 상태 검증)에 대한 OCSP 컨피그레이션의 세부 정보를 입력합니다.

- OCSP 서비스에 대해 확인: ocsp_test_profile
- OCSP가 UNKNOWN 상태를 반환하는 경우 요청 거부: check
- OCSP 응답기에 연결할 수 없는 경우 요청을 거부합니다.



Issuer

* Friendly Name: ocsp-ca-friendly-name

Status: Enabled

Description:

Subject: CN=ocsp-ca-common-name

Issuer: CN=ocsp-ca-common-name

Valid From: Tue, 4 Jun 2024 13:52:00 JST

Valid To (Expiration): Sun, 4 Jun 2034 13:52:00 JST

Serial Number: 1A 12 1D 58 59 6C 75 1B

Signature Algorithm: SHA256withRSA

Key Length: 2048

Usage

Trusted For:

☑ Trust for authentication within ISE

☑ Trust for client authentication and Syslog

☑ Trust for certificate based admin authentication

☑ Trust for authentication of Cisco Services

Certificate Status Validation

To verify certificates, enable the methods below. If both are enabled, OCSP will always be tried first.

OCSP Configuration

☑ Validate against OCSP Service: ocsp_test_profile

☑ Reject the request if OCSP returns UNKNOWN status

☑ Reject the request if OCSP Responder is unreachable

Certificate Revocation List Configuration

□ Download CRL

CRL Distribution URL:

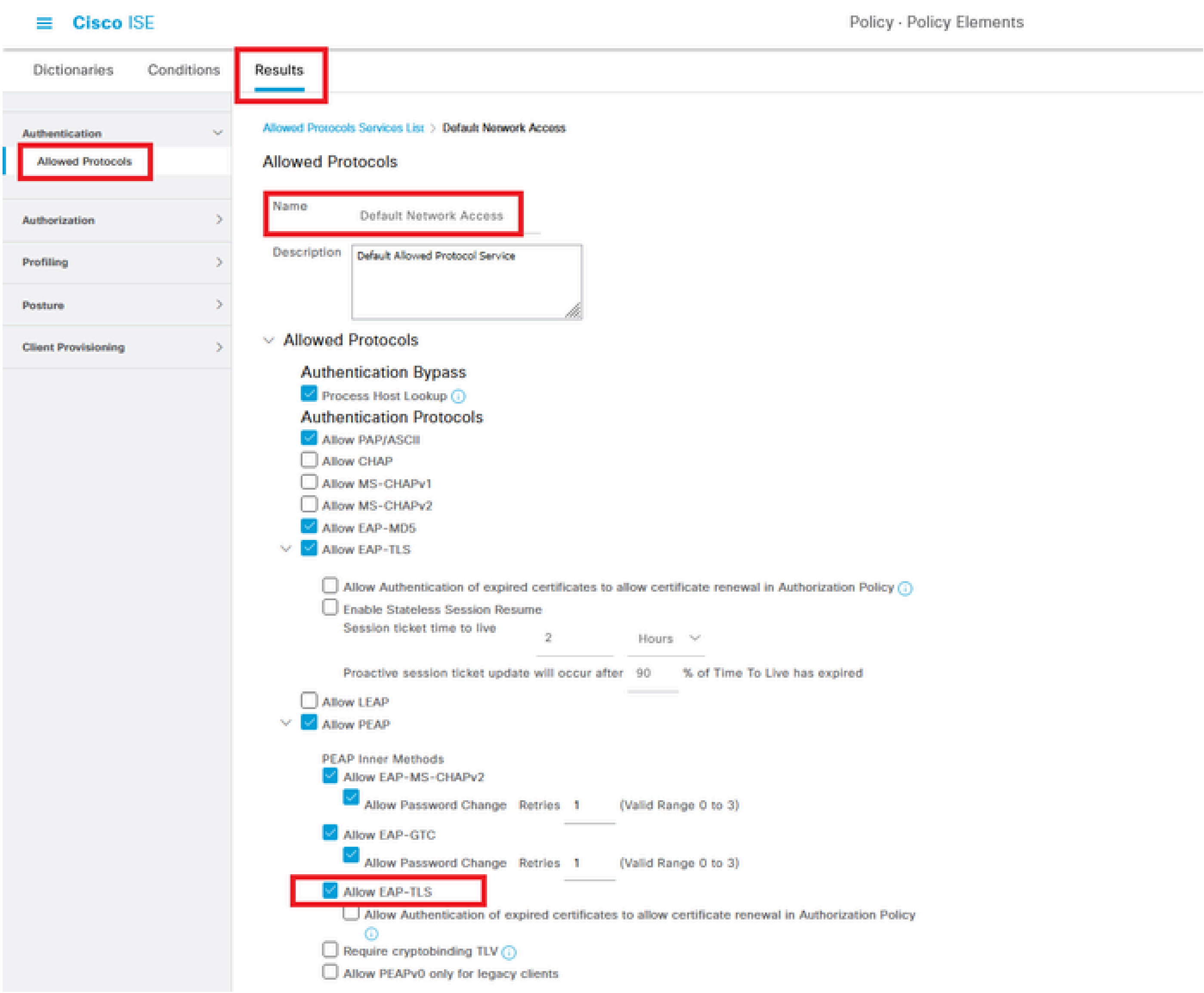
Retrieve CRL: ● Automatically 5 Minutes before expiration. ○ Every 1 Hours

If download failed, wait 10 Minutes before retry.

인증서 상태 검증

6단계. 허용되는 프로토콜 추가

Policy(정책) > Results(결과) > Authentication(인증) > Allowed Protocols(허용된 프로토콜)로 이동하고 Default Network Access(기본 네트워크 액세스) 서비스 목록을 수정한 다음 Allow EAP-TLS(EAP-TLS 허용)를 선택합니다.



Cisco ISE — Policy · Policy Elements

Dictionaries | Conditions | Results

Authentication
- Allowed Protocols

Authorization
Profiling
Posture
Client Provisioning

Allowed Protocols Services List > Default Network Access

Allowed Protocols

Name: Default Network Access

Description: Default Allowed Protocol Service

Allowed Protocols

Authentication Bypass

☑ Process Host Lookup

Authentication Protocols

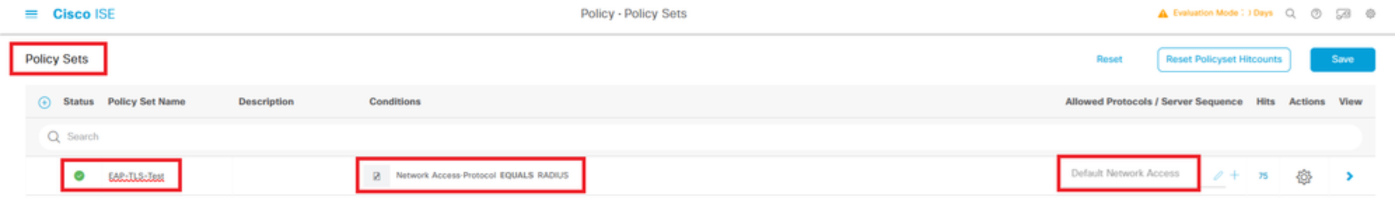
☑ Allow PAP/ASCII
☐ Allow CHAP
☐ Allow MS-CHAPv1
☐ Allow MS-CHAPv2
☑ Allow EAP-MD5
☑ Allow EAP-TLS
  ☐ Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy
  ☐ Enable Stateless Session Resume
  Session ticket time to live 2 Hours
  Proactive session ticket update will occur after 90 % of Time To Live has expired
☐ Allow LEAP
☑ Allow PEAP
  PEAP Inner Methods
  ☑ Allow EAP-MS-CHAPv2
    ☑ Allow Password Change Retries 1 (Valid Range 0 to 3)
  ☑ Allow EAP-GTC
    ☑ Allow Password Change Retries 1 (Valid Range 0 to 3)
  ☑ Allow EAP-TLS
    ☐ Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy
  ☐ Require cryptobinding TLV
  ☐ Allow PEAPv0 only for legacy clients

EAP-TLS 허용

7단계. 정책 집합 추가

Policy(정책) > Policy Sets(정책 세트)로 이동하고 +를 클릭하여 정책 세트를 추가합니다.

- 정책 집합 이름: EAP-TLS-Test
- 조건: RADIUS와 같은 네트워크 액세스 프로토콜
- 허용되는 프로토콜/서버 시퀀스: 기본 네트워크 액세스



Cisco ISE — Policy · Policy Sets

Policy Sets

Reset | Reset Policyset Hitcounts | Save

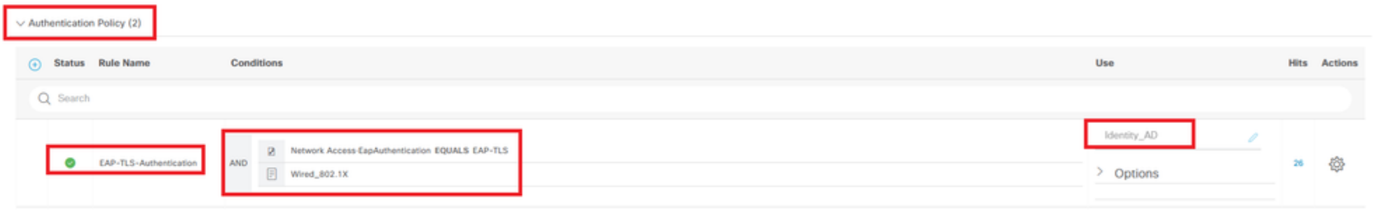
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	EAP-TLS-Test		Network Access·Protocol EQUALS RADIUS	Default Network Access	75	⚙	>

정책 집합 추가

8단계. 인증 정책 추가

인증 정책을 추가하려면 Policy Sets(정책 집합)로 이동하고 EAP-TLS-Tests를 클릭합니다.

- 규칙 이름: EAP-TLS-Authentication
- 조건: 네트워크 액세스 EapAuthentication은 EAP-TLS 및 Wired_802.1 X와 같음
- 사용: Identity_AD



Authentication Policy (2)

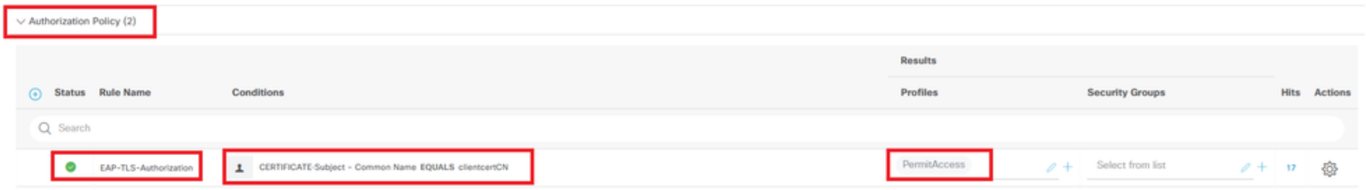
Status	Rule Name	Conditions	Use	Hits	Actions
●	EAP-TLS-Authentication	AND Network Access·EapAuthentication EQUALS EAP-TLS Wired_802.1X	Identity_AD Options	26	⚙

인증 정책 추가

9단계. 권한 부여 정책 추가

Policy Sets(정책 집합)로 이동하고 EAP-TLS-Test를 클릭하여 권한 부여 정책을 추가합니다.

- 규칙 이름: EAP-TLS-Authorization
- 조건: CERTIFICATE Subject - Common Name EQUALS clientcertCN(인증서 주체 - 공통 이름이 clientcertCN)
- 결과: Permit Access



Authorization Policy (2)

			Results			
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
●	EAP-TLS-Authorization	CERTIFICATE·Subject - Common Name EQUALS clientcertCN	PermitAccess	Select from list	17	⚙

권한 부여 정책 추가

다음을 확인합니다.

1단계. 인증 세션 확인

C1000에서 인증 세션을 확인하려면 명령을 실행합니다show authentication sessions interface GigabitEthernet1/0/3 details.

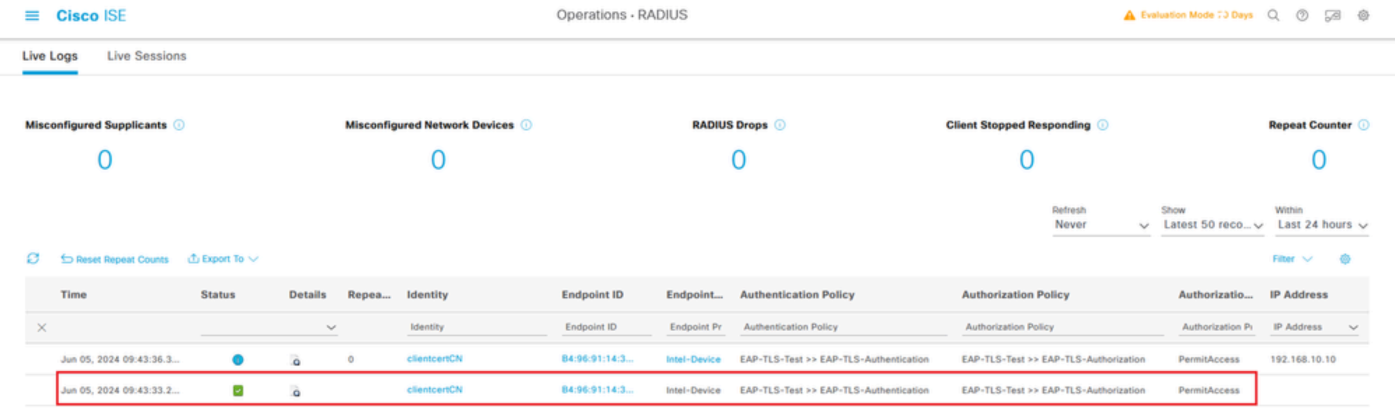
<#root>

Switch#

```
show authentication sessions interface GigabitEthernet1/0/3 details


Interface: GigabitEthernet1/0/3
MAC Address: b496.9114.398c
IPv6 Address: Unknown
IPv4 Address: 192.168.10.10
User-Name: clientcertCN
Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
Restart timeout: N/A
Periodic Acct timeout: N/A
Session Uptime: 111s
Common Session ID: 01C20065000000933E4E87D9
Acct Session ID: 0x00000078
Handle: 0xB6000043
Current Policy: POLICY_Gi1/0/3

Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:


Method status list:
Method State

dot1x Authc Success
```

2단계. Radius 라이브 로그 확인

ISE GUI에서 **Operations(운영) > RADIUS** > **Live** Log(라이브 로그)로 이동하여 인증을 위한 라이브 로그를 확인합니다.



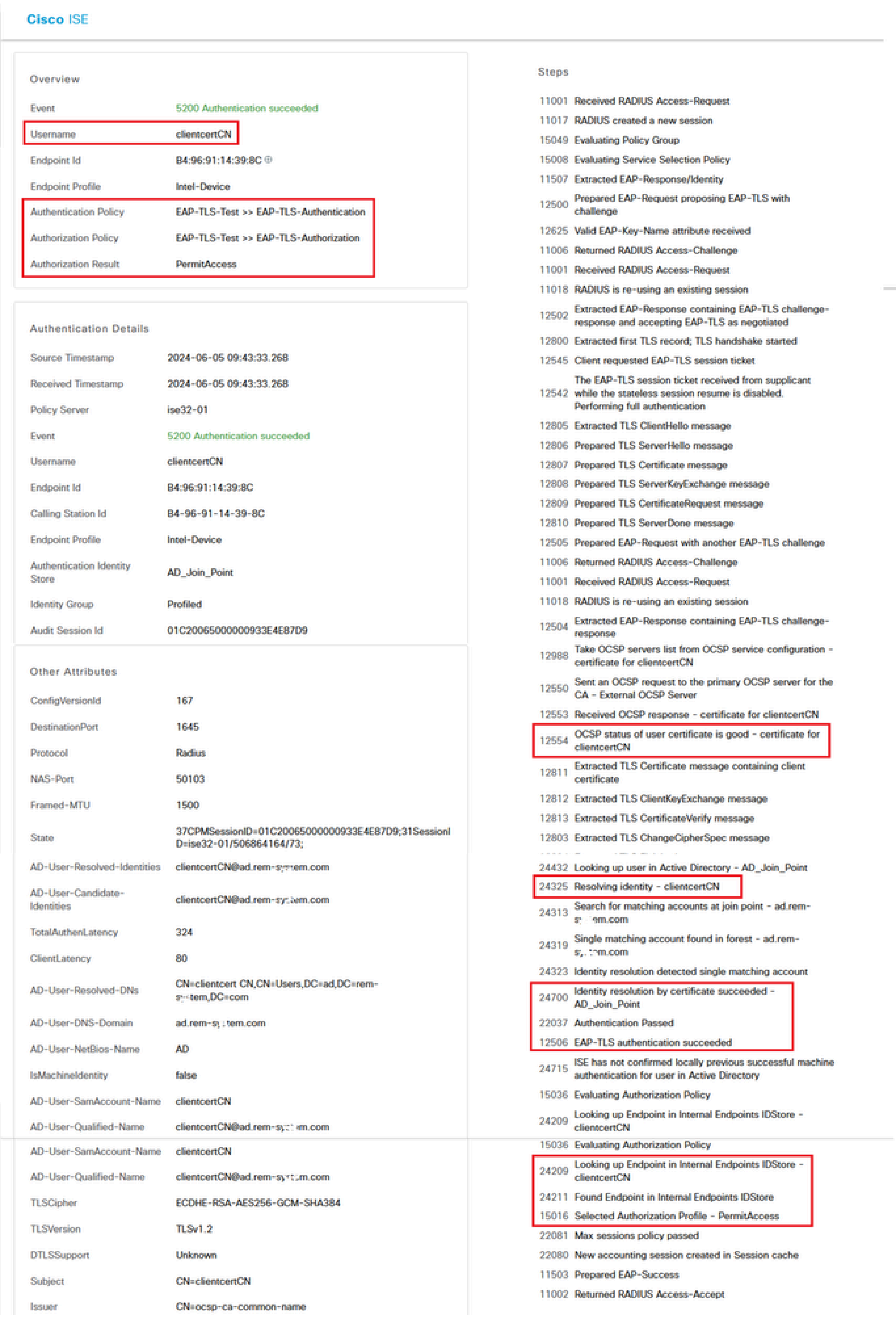
Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	0	0	0

Refresh: Never
Show: Latest 50 reco...
Within: Last 24 hours

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authentication Policy	Authorization Policy	Authorizatio...	IP Address
Jun 05, 2024 09:43:36.3...	●		0	clientcertCN	B4:96:91:14:3...	Intel-Device	EAP-TLS-Test >> EAP-TLS-Authentication	EAP-TLS-Test >> EAP-TLS-Authorization	PermitAccess	192.168.10.10
Jun 05, 2024 09:43:33.2...	✓			clientcertCN	B4:96:91:14:3...	Intel-Device	EAP-TLS-Test >> EAP-TLS-Authentication	EAP-TLS-Test >> EAP-TLS-Authorization	PermitAccess	

Radius 라이브 로그

자세한 인증 라이브 로그를 확인합니다.



Cisco ISE

Overview

Event	5200 Authentication succeeded
Username	clientcertCN
Endpoint Id	B4:96:91:14:39:8C
Endpoint Profile	Intel-Device
Authentication Policy	EAP-TLS-Test >> EAP-TLS-Authentication
Authorization Policy	EAP-TLS-Test >> EAP-TLS-Authorization
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2024-06-05 09:43:33.268
Received Timestamp	2024-06-05 09:43:33.268
Policy Server	ise32-01
Event	5200 Authentication succeeded
Username	clientcertCN
Endpoint Id	B4:96:91:14:39:8C
Calling Station Id	B4-96-91-14-39-8C
Endpoint Profile	Intel-Device
Authentication Identity Store	AD_Join_Point
Identity Group	Profiled
Audit Session Id	01C20065000000933E4E87D9

Other Attributes

ConfigVersionId	167
DestinationPort	1645
Protocol	Radius
NAS-Port	50103
Framed-MTU	1500
State	37CPMSessionID=01C20065000000933E4E87D9;31SessionID=ise32-01/506864164/73;
AD-User-Resolved-Identities	clientcertCN@ad.rem-s em.com
AD-User-Candidate-Identities	clientcertCN@ad.rem-sy em.com
TotalAuthenLatency	324
ClientLatency	80
AD-User-Resolved-DNs	CN=clientcert CN,CN=Users,DC=ad,DC=rem-s tem,DC=com
AD-User-DNS-Domain	ad.rem-s tem.com
AD-User-NetBios-Name	AD
IsMachineIdentity	false
AD-User-SamAccount-Name	clientcertCN
AD-User-Qualified-Name	clientcertCN@ad.rem-s m.com
AD-User-SamAccount-Name	clientcertCN
AD-User-Qualified-Name	clientcertCN@ad.rem-sy m.com
TLSCipher	ECDHE-RSA-AES256-GCM-SHA384
TLSVersion	TLSv1.2
DTLSSupport	Unknown
Subject	CN=clientcertCN
Issuer	CN=ocsp-ca-common-name

Steps

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
11507	Extracted EAP-Response/Identity
12500	Prepared EAP-Request proposing EAP-TLS with challenge
12625	Valid EAP-Key-Name attribute received
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12502	Extracted EAP-Response containing EAP-TLS challenge-response and accepting EAP-TLS as negotiated
12800	Extracted first TLS record; TLS handshake started
12545	Client requested EAP-TLS session ticket
12542	The EAP-TLS session ticket received from supplicant while the stateless session resume is disabled. Performing full authentication
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
12810	Prepared TLS ServerDone message
12505	Prepared EAP-Request with another EAP-TLS challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12504	Extracted EAP-Response containing EAP-TLS challenge-response
12988	Take OCSP servers list from OCSP service configuration - certificate for clientcertCN
12550	Sent an OCSP request to the primary OCSP server for the CA - External OCSP Server
12553	Received OCSP response - certificate for clientcertCN
12554	OCSP status of user certificate is good - certificate for clientcertCN
12811	Extracted TLS Certificate message containing client certificate
12812	Extracted TLS ClientKeyExchange message
12813	Extracted TLS CertificateVerify message
12803	Extracted TLS ChangeCipherSpec message
24432	Looking up user in Active Directory - AD_Join_Point
24325	Resolving identity - clientcertCN
24313	Search for matching accounts at join point - ad.rem-s em.com
24319	Single matching account found in forest - ad.rem-s m.com
24323	Identity resolution detected single matching account
24700	Identity resolution by certificate succeeded - AD_Join_Point
22037	Authentication Passed
12506	EAP-TLS authentication succeeded
24715	ISE has not confirmed locally previous successful machine authentication for user in Active Directory
15036	Evaluating Authorization Policy
24209	Looking up Endpoint in Internal Endpoints IDStore - clientcertCN
15036	Evaluating Authorization Policy
24209	Looking up Endpoint in Internal Endpoints IDStore - clientcertCN
24211	Found Endpoint in Internal Endpoints IDStore
15016	Selected Authorization Profile - PermitAccess
22081	Max sessions policy passed
22080	New accounting session created in Session cache
11503	Prepared EAP-Success
11002	Returned RADIUS Access-Accept

인증 세부 정보

```
Crypto,2024-06-05 09:43:33,064,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, CryptoLib.CSSL.OCSP Callback -

starting OCSP request to primary

,SSL.cpp:1444
Crypto,2024-06-05 09:43:33,064,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, Crypto.OcspClient::pe

Start processing OCSP request


,

URL=http://winserver.ad.rem-xxx.com/ocsp

, use nonce=1,OcspClient.cpp:144

Crypto,2024-06-05 09:43:33,104,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, Crypto.OcspClient::pe

Received OCSP server response

,OcspClient.cpp:411
Crypto,2024-06-05 09:43:33,104,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, Crypto.OcspClient::pe

Crypto,2024-06-05 09:43:33,104,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, Crypto.OcspClient::pe
Crypto,2024-06-05 09:43:33,104,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, Crypto.OcspClient::pe

Crypto,2024-06-05 09:43:33,104,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, Crypto.OcspClient::pe
Crypto,2024-06-05 09:43:33,104,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, Crypto.OcspClient::pe

Crypto,2024-06-05 09:43:33,104,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, Crypto.OcspClient::pe

User certificate status: Good

,OcspClient.cpp:598
Crypto,2024-06-05 09:43:33,104,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, CryptoLib.CSSL.OCSP C

perform OCSP request succeeded

, status: Good,SSL.cpp:1684

// Radius session
Radius,2024-06-05 09:43:33,120,DEBUG,0x7f982d7b9700,cntx=0000017387,sesn=ise32-01/506864164/73,CPMSessi

Code=1(AccessRequest)

 Identifier=238 Length=324
[1] User-Name - value: [

clientcertCN

]
[4] NAS-IP-Address - value: [1.x.x.101]
[5] NAS-Port - value: [50103]
[24] State - value: [37CPMSessionID=01C2006500000933E4E87D9;31SessionID=ise32-01/506864164/73;]
[87] NAS-Port-Id - value: [GigabitEthernet1/0/3]

Radius,2024-06-05 09:43:33,270,DEBUG,0x7f982d9ba700,cntx=0000017387,sesn=ise32-01/506864164/73,CPMSessi

Code=2(AccessAccept)

 Identifier=238 Length=294
[1] User-Name - value: [clientcertCN]

Radius,2024-06-05 09:43:33,342,DEBUG,0x7f982d1b6700,cntx=0000017401,sesn=ise32-01/506864164/74,CPMSessi

Code=4(AccountingRequest)
```

```
 Identifier=10 Length=286
[1] User-Name - value: [clientcertCN]
[4] NAS-IP-Address - value: [1.x.x.101]
[5] NAS-Port - value: [50103]
[40] Acct-Status-Type - value: [Interim-Update]
[87] NAS-Port-Id - value: [GigabitEthernet1/0/3]
[26] cisco-av-pair - value: [audit-session-id=01C20065000000933E4E87D9]
[26] cisco-av-pair - value: [method=dot1x] ,RADIUSHandler.cpp:2455

Radius,2024-06-05 09:43:33,350,DEBUG,0x7f982e1be700,cntx=0000017401,sesn=ise32-01/506864164/74,CPMSessi
```

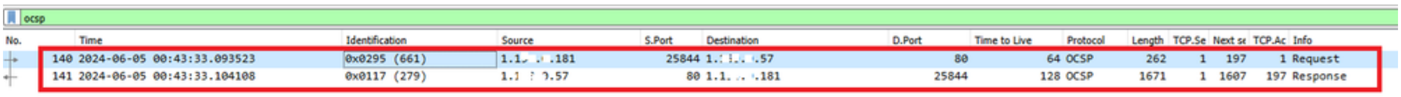
Code=5(AccountingResponse)

```
 Identifier=10 Length=20,RADIUSHandler.cpp:2455
```

2. TCP 덤프

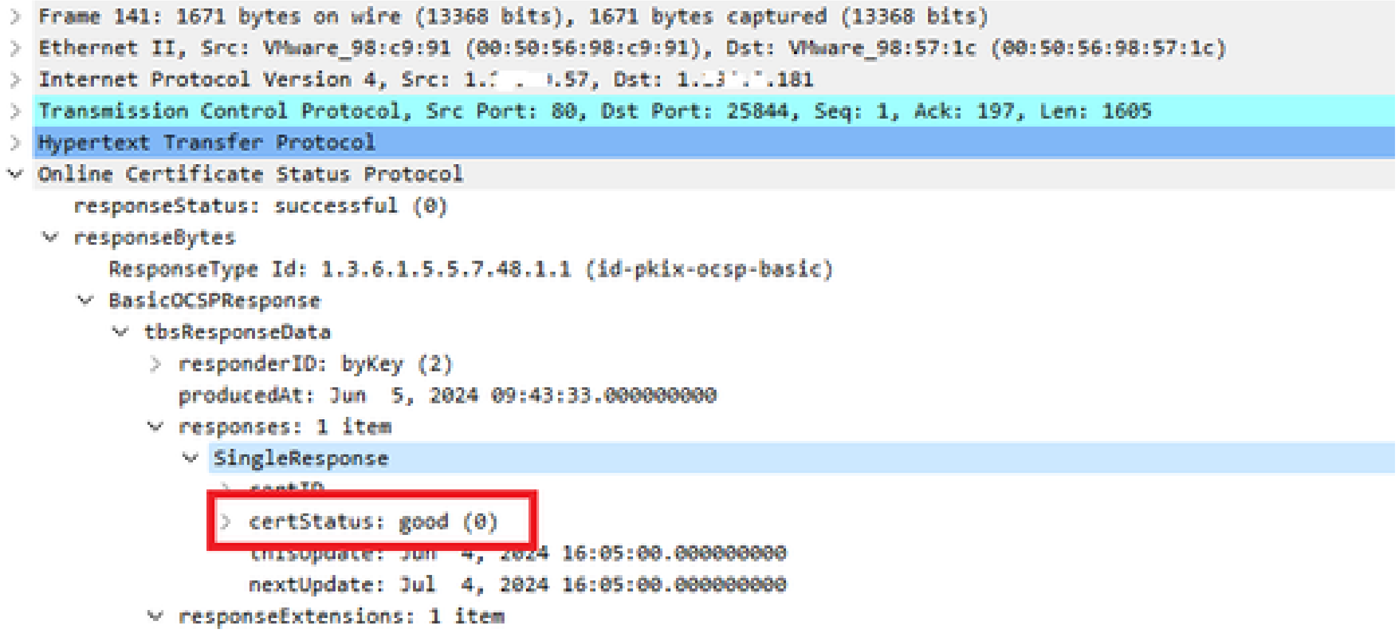
ISE의 TCP 덤프에서 OCSP 응답 및 Radius 세션에 대한 정보를 찾을 수 있습니다.

OCSP 요청 및 응답:



```
No.  Time                        Identification  Source              S.Port  Destination         D.Port  Time to Live  Protocol  Length  TCP.Se  Next se  TCP.Ac  Info
140  2024-06-05 00:43:33.093523  0x0295 (661)    1.1.[redacted].181  25844   1.[redacted].57     80      64            OCSP      262     1       197      1       Request
141  2024-06-05 00:43:33.104108  0x0117 (279)    1.[redacted].57     80      1.1.[redacted].181  25844   128           OCSP      1671    1       1607     197     Response
```

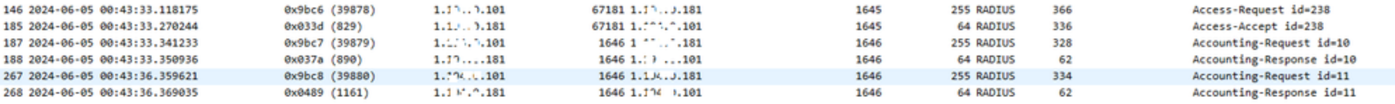
OCSP 요청 및 응답의 패킷 캡처



```
> Frame 141: 1671 bytes on wire (13368 bits), 1671 bytes captured (13368 bits)
> Ethernet II, Src: VMware_98:c9:91 (00:50:56:98:c9:91), Dst: VMware_98:57:1c (00:50:56:98:57:1c)
> Internet Protocol Version 4, Src: 1.[redacted].57, Dst: 1.[redacted].181
> Transmission Control Protocol, Src Port: 80, Dst Port: 25844, Seq: 1, Ack: 197, Len: 1605
> Hypertext Transfer Protocol
v Online Certificate Status Protocol
     responseStatus: successful (0)
   v responseBytes
        ResponseType Id: 1.3.6.1.5.5.7.48.1.1 (id-pkix-ocsp-basic)
      v BasicOCSPResponse
         v tbsResponseData
            > responderID: byKey (2)
              producedAt: Jun  5, 2024 09:43:33.000000000
            v responses: 1 item
               v SingleResponse
                  > certID
                  > certStatus: good (0)
                    thisUpdate: Jun  4, 2024 16:05:00.000000000
                    nextUpdate: Jul  4, 2024 16:05:00.000000000
            v responseExtensions: 1 item
```

OCSP 응답의 세부사항 캡처

Radius 세션:



```
146 2024-06-05 00:43:33.118175  0x9bc6 (39878)  1.[redacted].101        67181 1.[redacted].181  1645  255 RADIUS  366  Access-Request id=238
185 2024-06-05 00:43:33.270244  0x033d (829)    1.1.[redacted].181      67181 1.[redacted].101  1645   64 RADIUS  336  Access-Accept id=238
187 2024-06-05 00:43:33.341233  0x9bc7 (39879)  1.[redacted].101         1646 1[redacted].181   1646  255 RADIUS  328  Accounting-Request id=10
188 2024-06-05 00:43:33.350936  0x037a (890)    1.[redacted].181         1646 1.[redacted].101  1646   64 RADIUS   62  Accounting-Response id=10
267 2024-06-05 00:43:36.359621  0x9bc8 (39880)  1.[redacted].101         1646 1.1[redacted].181 1646  255 RADIUS  334  Accounting-Request id=11
268 2024-06-05 00:43:36.369035  0x0489 (1161)   1.[redacted].181         1646 1.[redacted].101  1646   64 RADIUS   62  Accounting-Response id=11
```

Radius 세션의 패킷 캡처

관련 정보

ISE를 사용하여 EAP-TLS 인증 구성

ISE에서 TLS/SSL 인증서 구성

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.