

# Configure EAP-TLS Authentication with OCSP in ISE

## Contents

---

### [Introduction](#)

### [Prerequisites](#)

[Requirements](#)

[Components Used](#)

### [Network Diagram](#)

### [Background Information](#)

### [Configurations](#)

[Configuration in C1000](#)

[Configuration in Windows PC](#)

[Step 1. Configure User Authentication](#)

[Step 2. Confirm Client Certificate](#)

[Configuration in Windows Server](#)

[Step 1. Add Users](#)

[Step 2. Confirm OCSP Service](#)

[Configuration in ISE](#)

[Step 1. Add Device](#)

[Step 2. Add Active Directory](#)

[Step 3. Add Certificate Authentication Profile](#)

[Step 4. Add Identity Source Sequence](#)

[Step 5. Confirm Certificate in ISE](#)

[Step 6. Add Allowed Protocols](#)

[Step 7. Add Policy Set](#)

[Step 8. Add Authentication Policy](#)

[Step 9. Add Authorization Policy](#)

### [Verify](#)

[Step 1. Confirm Authentication Session](#)

[Step 2. Confirm Radius Live Log](#)

### [Troubleshoot](#)

[1. Debug log](#)

[2. TCP Dump](#)

### [Related Information](#)

---

## Introduction

This document describes the steps required to set up EAP-TLS authentication with OCSP for real-time client certificate revocation checks.

## Prerequisites

## Requirements

Cisco recommends that you have knowledge of these topics:

- Configuration of Cisco Identity Services Engine
- Configuration of Cisco Catalyst
- Online Certificate Status Protocol

## Components Used

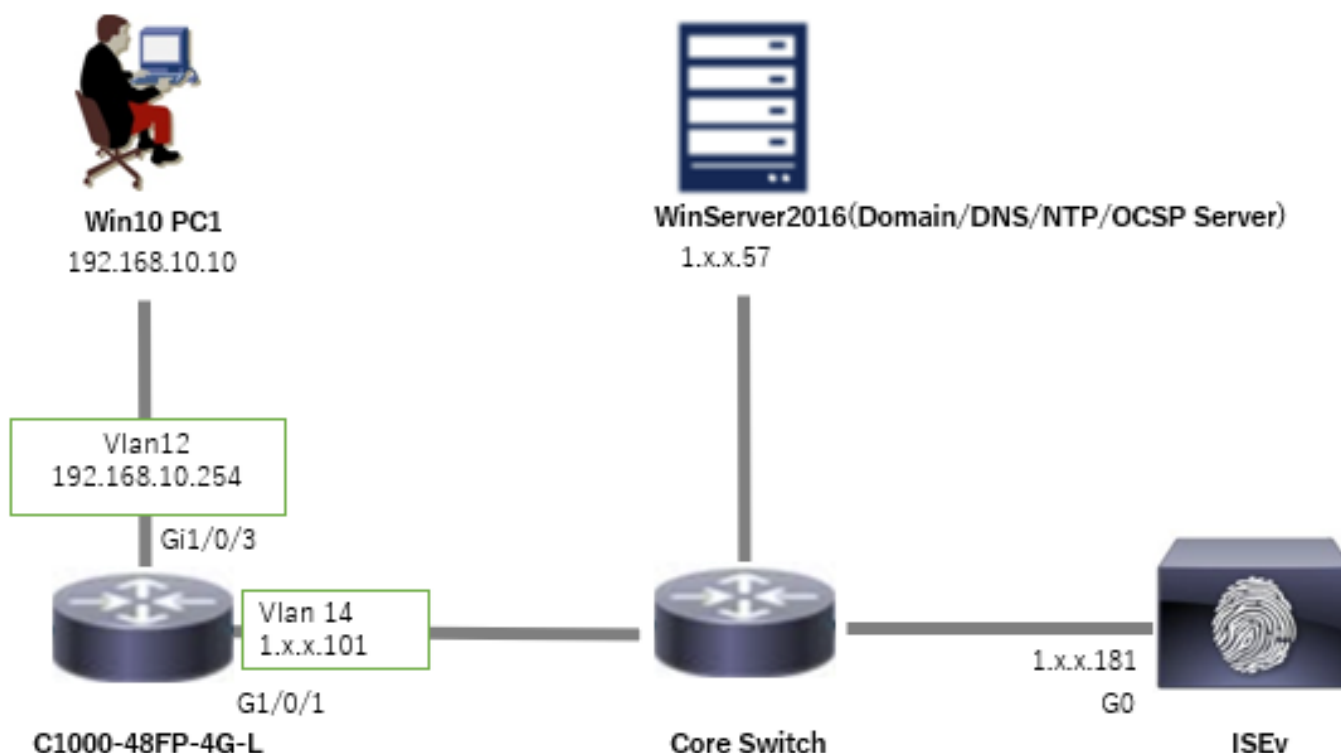
The information in this document is based on these software and hardware versions:

- Identity Services Engine Virtual 3.2 Patch 6
- C1000-48FP-4G-L 15.2(7)E9
- Windows Server 2016
- Windows 10

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.

## Network Diagram

This image shows the topology that is used for the example of this document.



*Network Diagram*

## Background Information

In EAP-TLS, a client presents its digital certificate to the server as part of the authentication process. This document describes how the ISE validates the client certificate by checking the certificate common name (CN) against the AD server and confirming whether the certificate has been revoked by using OCS (Online Certificate Status Protocol), which provides real-time protocol status.

The domain name configured on Windows Server 2016 is ad.rem-xxx.com, which is used as an example in this document.

The OCS (Online Certificate Status Protocol) and AD (Active Directory) server referenced in this document are used for certificate validation.

- Active Directory FQDN: winserver.ad.rem-xxx.com
- CRL Distribution URL: <http://winserver.ad.rem-xxx.com/ocsp-ca.crl>
- Authority URL: <http://winserver.ad.rem-xxx.com/ocsp>

This is the certificate chain with the common name of each certificate used in the document.

- CA: ocsp-ca-common-name
- Client Certificate: clientcertCN
- Server Certificate: ise32-01.ad.rem-xxx.com
- OCS Signing Certificate: ocspSignCommonName

## Configurations

### Configuration in C1000

This is the minimal configuration in C1000 CLI.

```
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
```

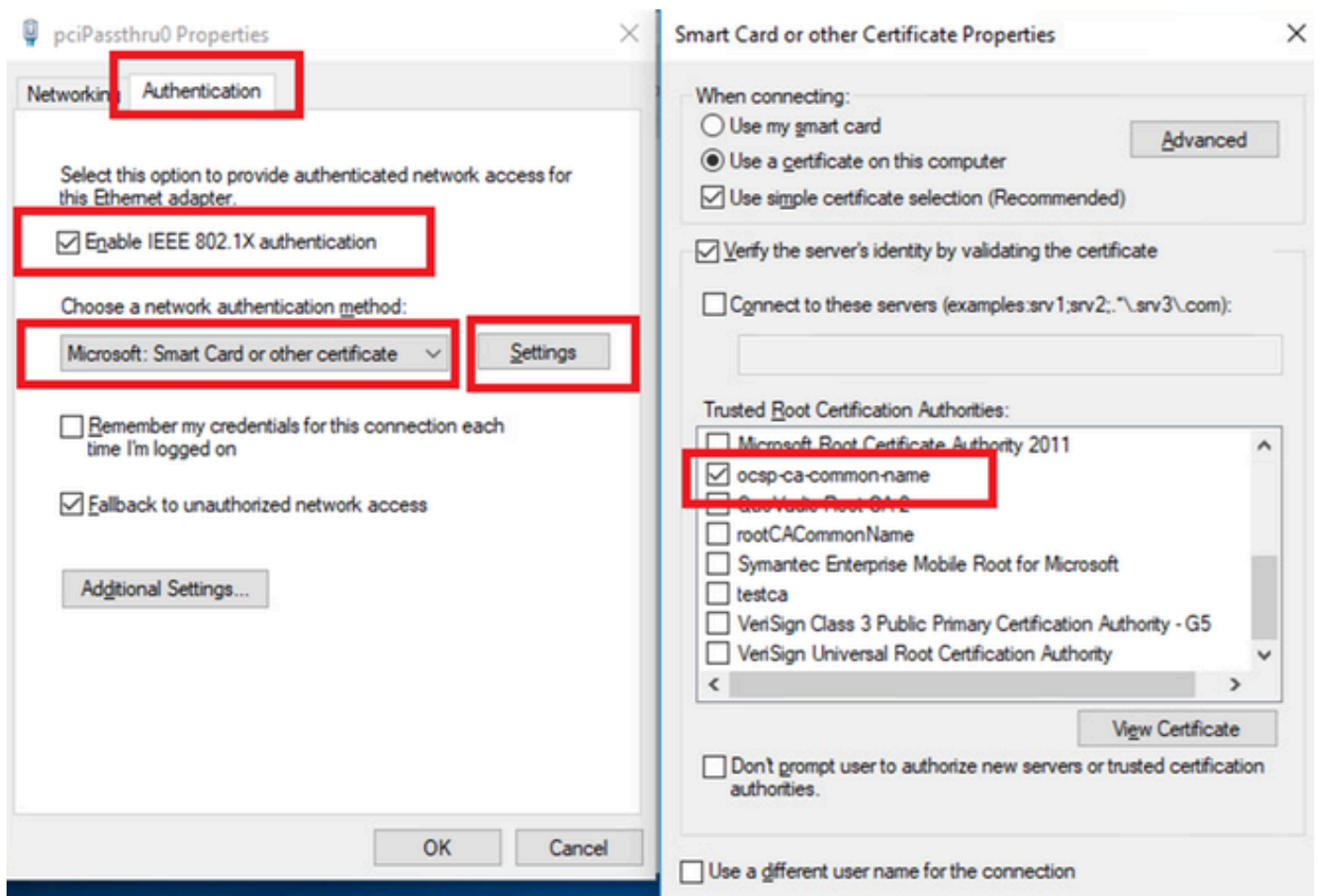
```
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge
```

## Configuration in Windows PC

### Step 1. Configure User Authentication

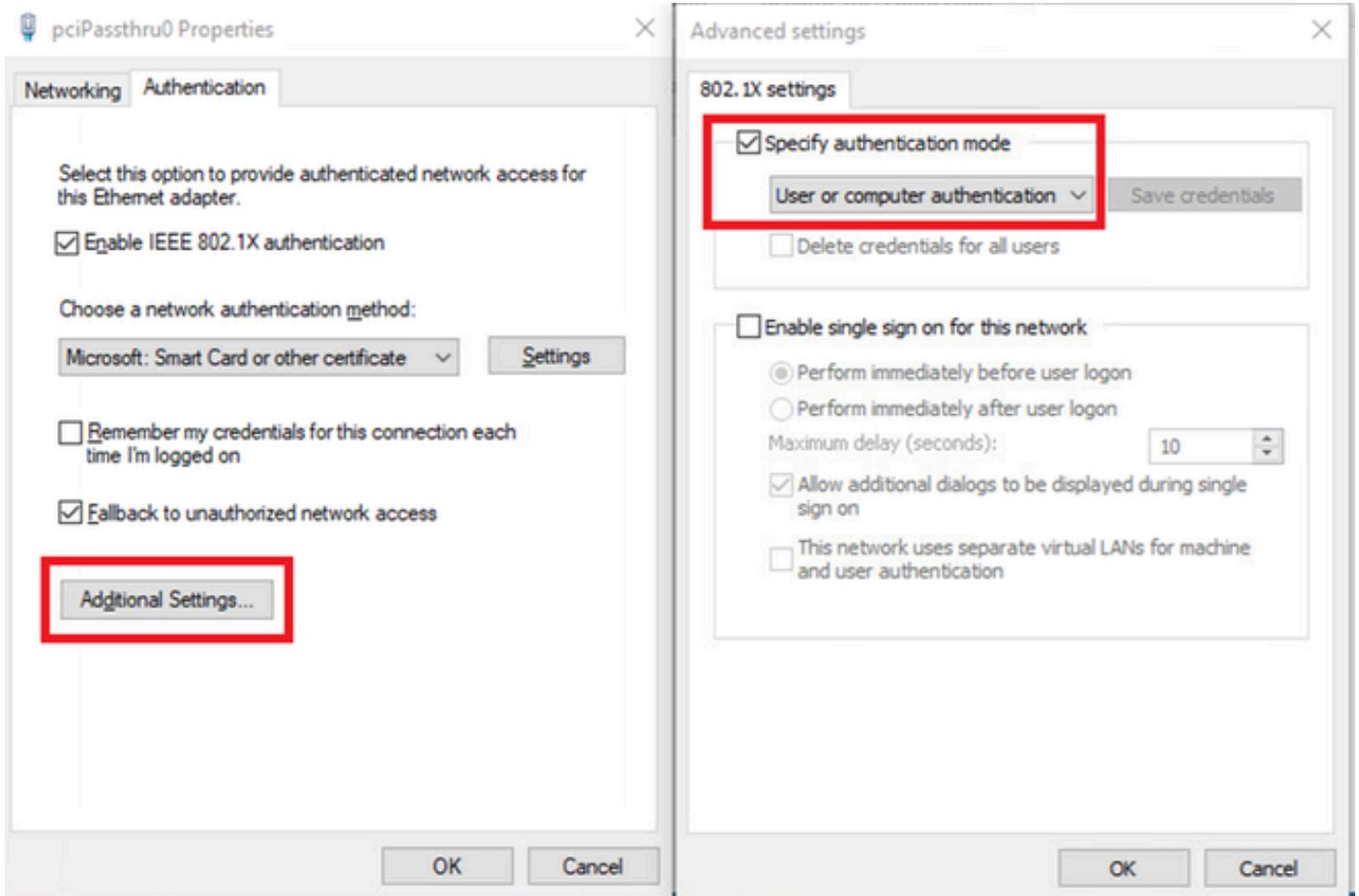
Navigate to **Authentication**, check **Enable IEEE 802.1X authentication** and select **Microsoft: Smart Card or other certificate**.

Click **Settings** button, check **Use a certificate on this computer**, and select the trusted CA of Windows PC.



*Enable Certificate Authentication*

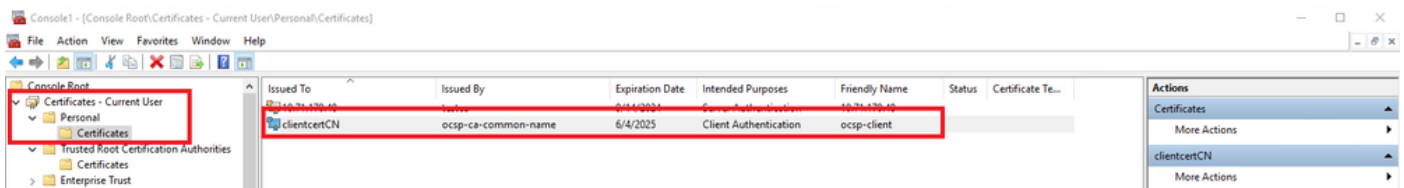
Navigate to **Authentication**, check **Additional Settings**. Select **User or computer authentication** from drop-down list.



Specify Authentication Mode

## Step 2. Confirm Client Certificate

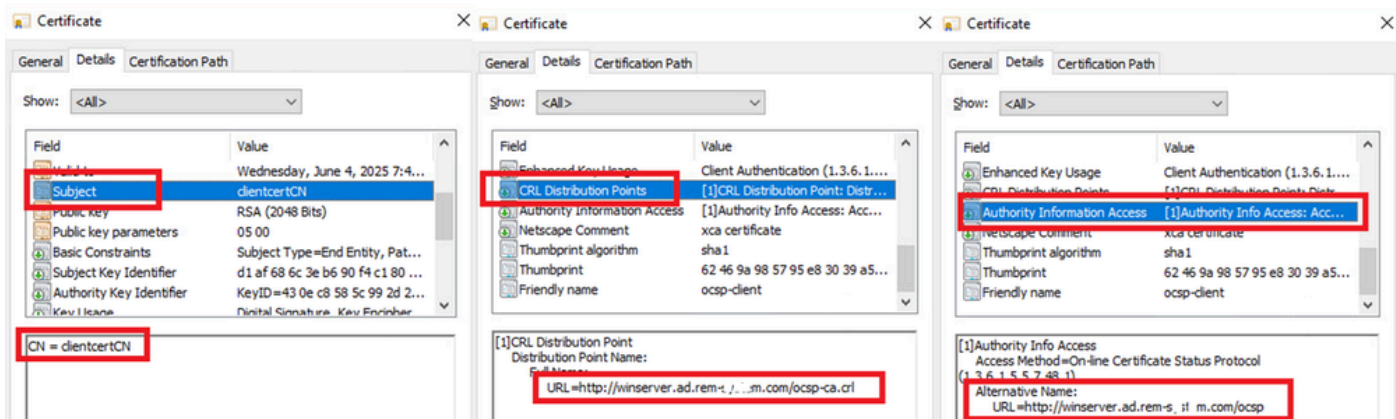
Navigate to **Certificates - Current User > Personal > Certificates**, and check the client certificate used for authentication.



Confirm Client Certificate

Double click the client certificate, navigate to **Details**, check the detail of Subject, CRL Distribution Points, Authority Information Access.

- Subject: CN = clientcertCN
- CRL Distribution Points: <http://winserver.ad.rem-xxx.com/ocsp-ca.crl>
- Authority Information Access: <http://winserver.ad.rem-xxx.com/ocsp>

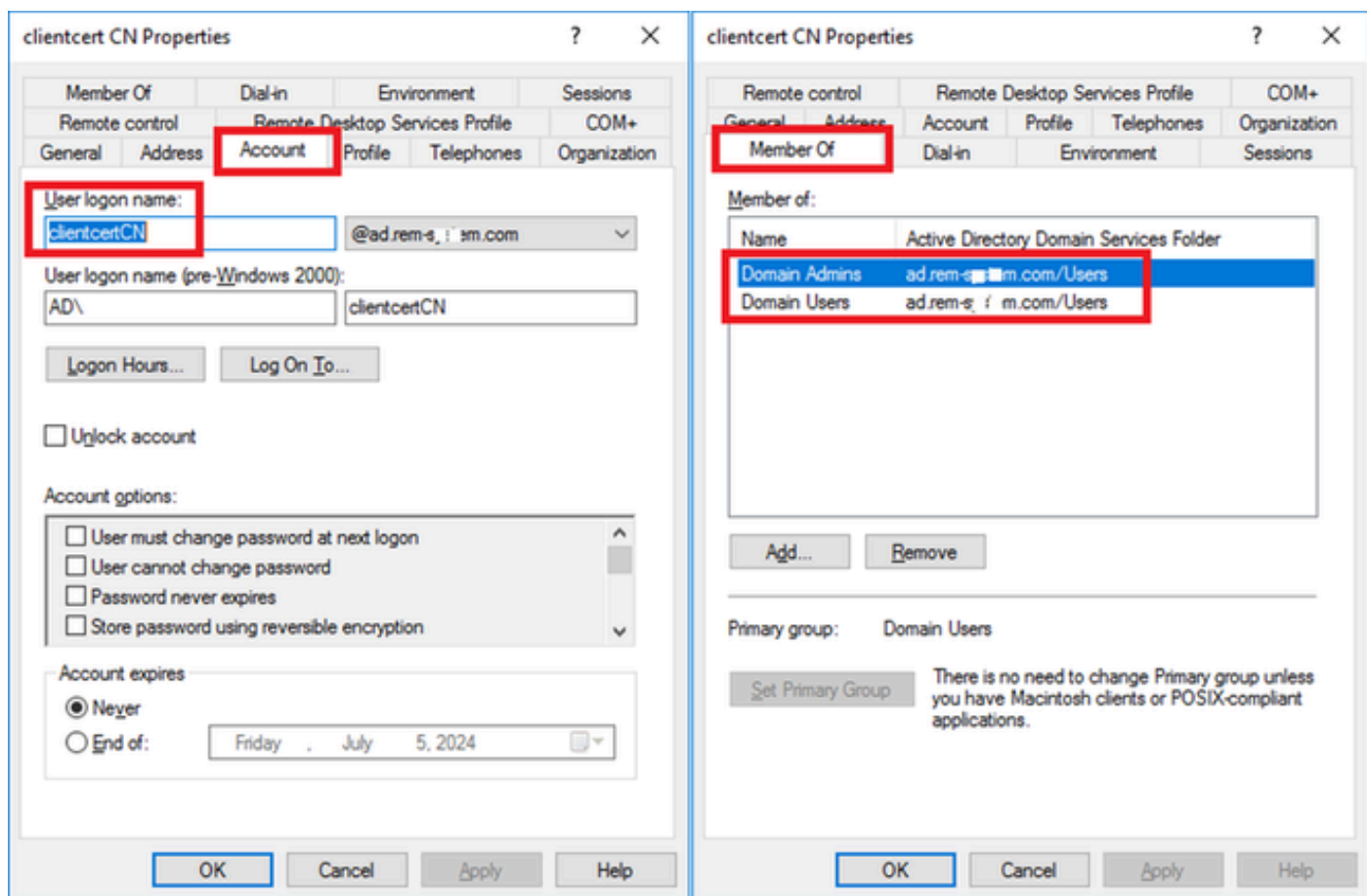


Detail of Client Certificate

## Configuration in Windows Server

### Step 1. Add Users

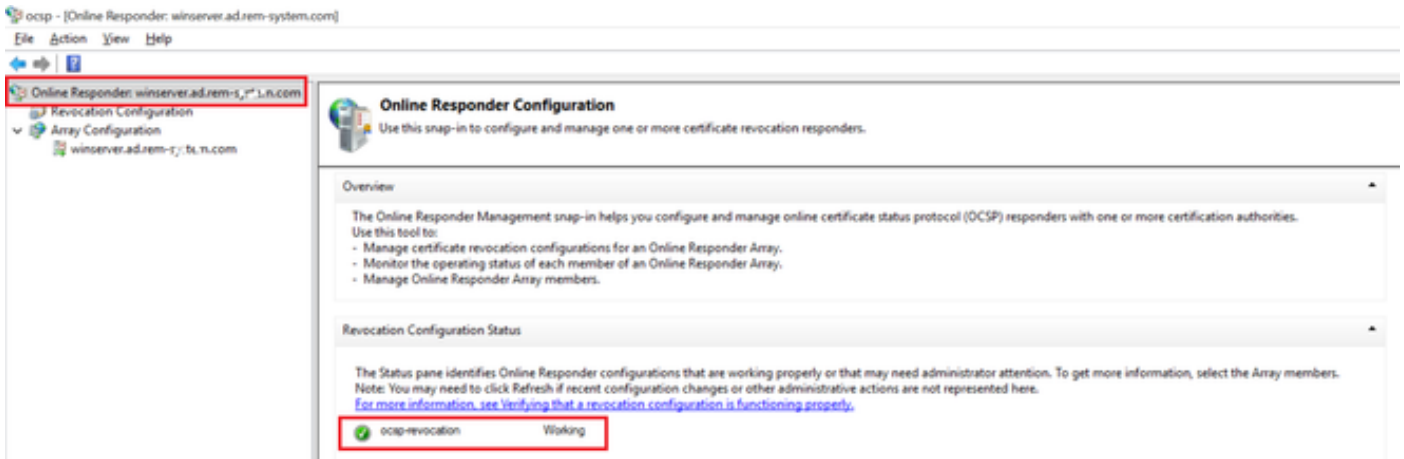
Navigate to **Active Directory Users and Computers**, click **Users**. Add clientcertCN as user logon name.



User Logon Name

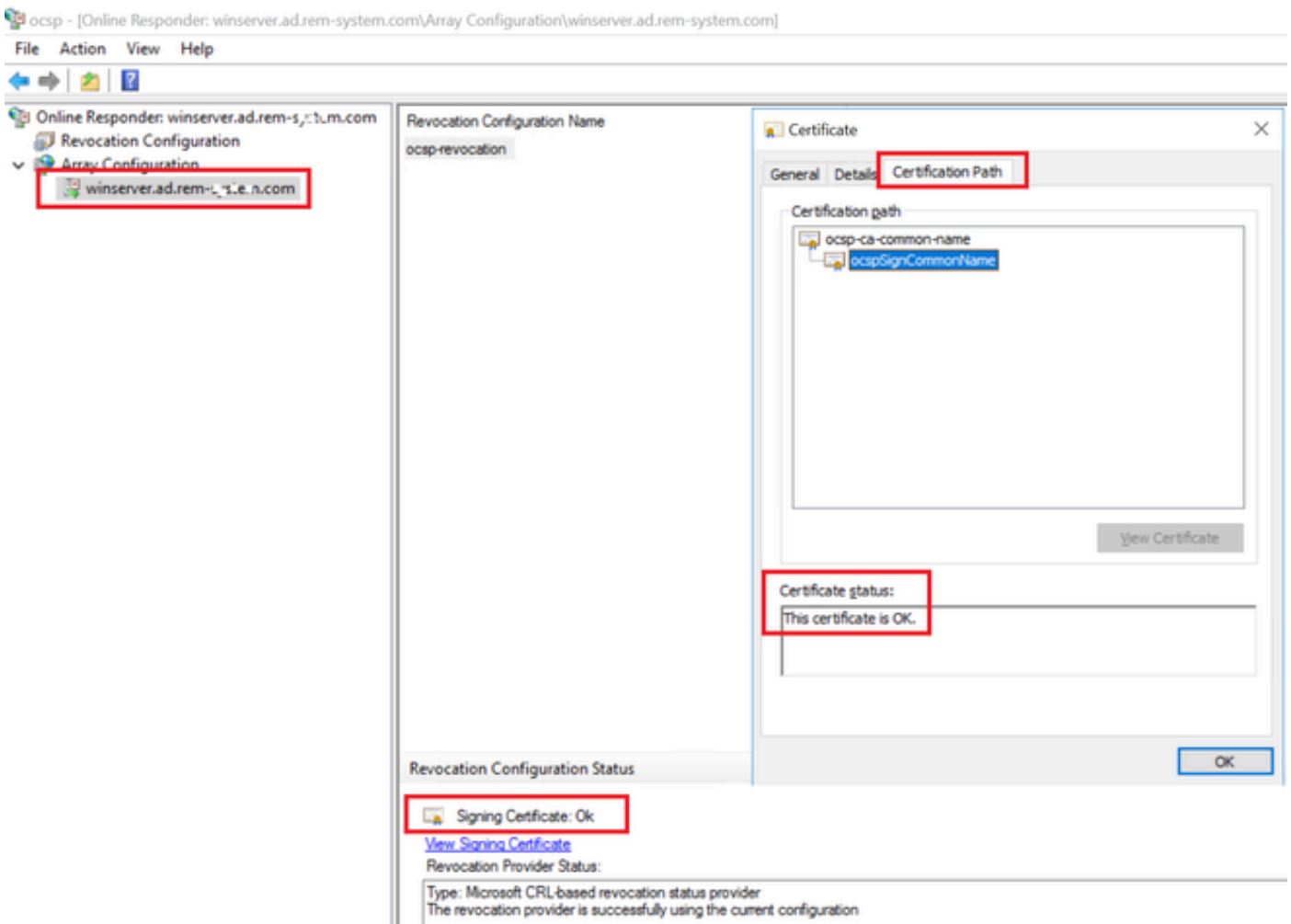
### Step 2. Confirm OCSP Service

Navigate to **Windows**, click **Online Responder Management**. Confirm the status of OCSP server.



Status of OCSP Server

Click **winserver.ad.rem-xxx.com**, check the status of OCSP signing certificate.



Status of OCSP Signing Certificate

## Configuration in ISE

### Step 1. Add Device

Navigate to **Administration > Network Devices**, click **Add** button to add C1000 device.

Cisco ISE Administration - Network Resources

Network Devices | Network Device Groups | Network Device Profiles | External RADIUS Servers | RADIUS Server Sequences | NAC Managers | External MDM | pxGrid Direct Connectors | Location Services

**Network Devices**

Network Devices List > C1000

**Network Devices**

Name: C1000

Description:

IP Address: \* IP: 1.1.1.101 / 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

Add Device

## Step 2. Add Active Directory

Navigate to **Administration > External Identity Sources > Active Directory**, click **Connection** tab, add Active Directory to ISE.

- Join Point Name: AD\_Join\_Point
- Active Directory Domain: ad.rem-xxx.com

Cisco ISE Administration - Identity Management

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

**External Identity Sources**

Active Directory

AD\_Join\_Point

LDAP

ODBC

RADIUS Token

RSA SecurID

SAML Id Providers

Social Login

**Connection** | Allowed Domains | PassiveID | Groups | Attributes | Advanced Settings

\* Join Point Name: AD\_Join\_Point

\* Active Directory Domain: ad.rem-xxx.com

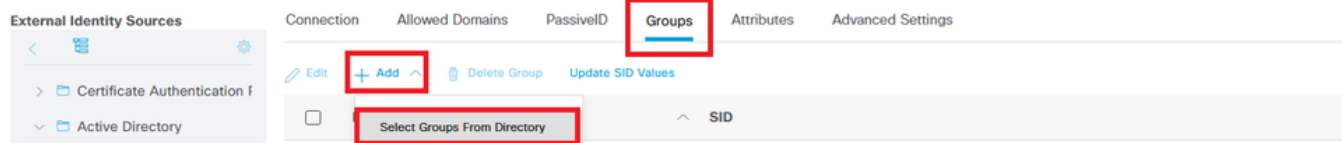
+ Join + Leave Test User Diagnostic Tool Refresh Table

<input type="checkbox"/>	ISE Node	ISE Node R...	Status	Domain Controller	Site
<input type="checkbox"/>	ise32-01.ad.rem-sy...m.c...	STANDALONE	<input checked="" type="checkbox"/> Operational	winserv.ad.rem-s,ste...	Default-First-Site-Na...

Add Active Directory

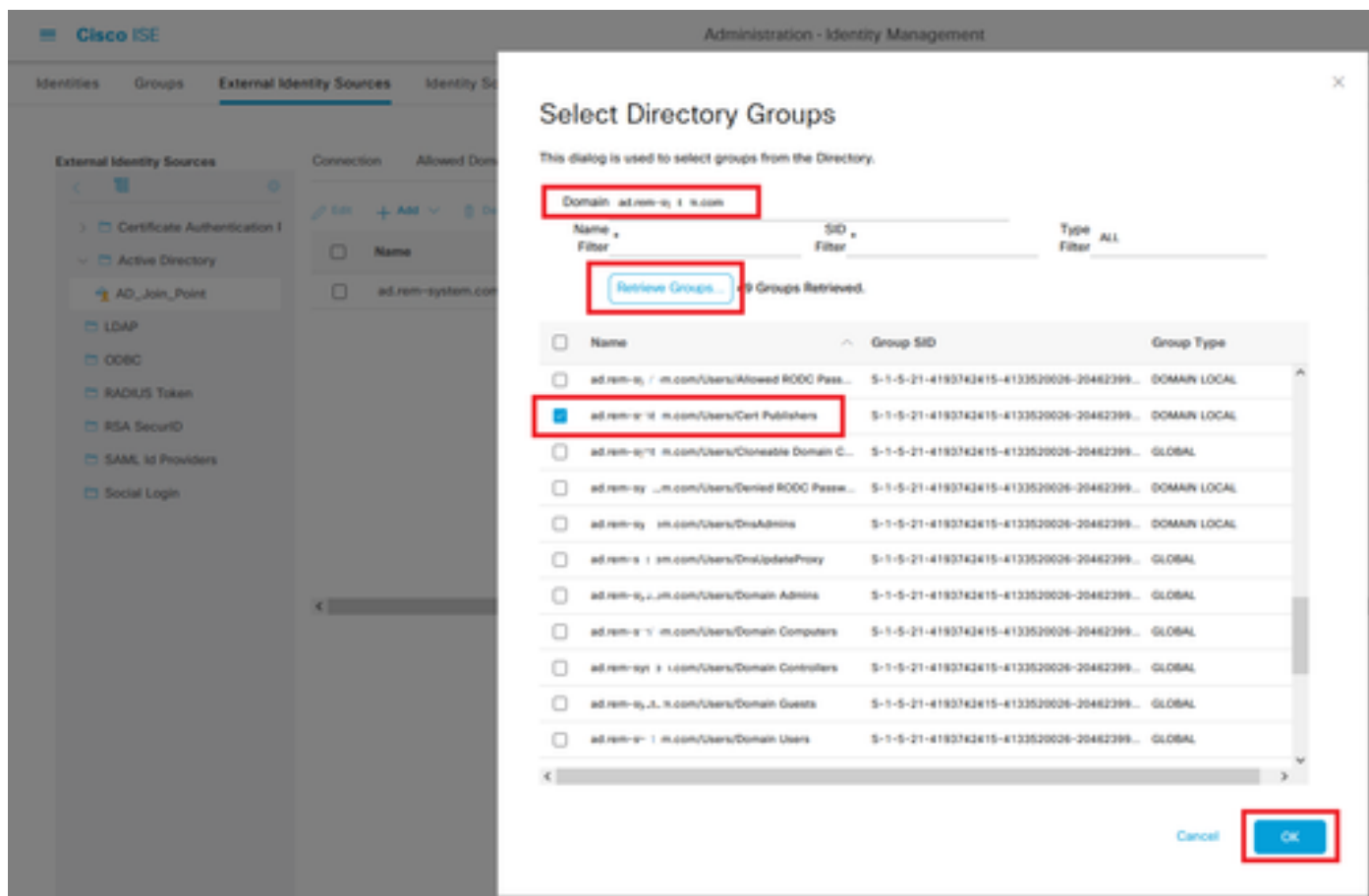
Navigate to **Groups** tab, select **Select Groups From Directory** from drop-down list.





Select Groups from Directory

Click **Retrieve Groups** from drop-down list. Check **ad.rem-xxx.com/Users/Cert Publishers** and click **OK**.



Check Cert Publishers

### Step 3. Add Certificate Authentication Profile

Navigate to **Administration > External Identity Sources > Certificate Authentication Profile**, click **Add** button to add a new certificate authentication profile.

- Name: cert\_authen\_profile\_test
- Identity Store: AD\_Join\_Point
- Use Identity From Certificate Attribute: Subject - Common Name.
- Match Client Certificate Against Certificate In Identity Store: Only to resolve identity ambiguity.

External Identity Sources

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

*Add Certificate Authentication Profile*

#### Step 4. Add Identity Source Sequence

Navigate to **Administration > Identity Source Sequences**, add an Identity Source Sequence.

- Name: Identity\_AD
- Select Certificate Authentication Profile: cert\_authen\_profile\_test
- Authentication Search List: AD\_Join\_Point

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

- Internal Endpoints
- Internal Users
- Guest Users
- All\_AD\_Join\_Points

Selected

- AD\_Join\_Point

Add Identity Source Sequences

### Step 5. Confirm Certificate in ISE

Navigate to **Administration > Certificates > System Certificates**, confirm the server certificate is signed by the trusted CA.

Cisco ISE		Administration - System									
Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings											
Certificate Management	System Certificates	<input type="checkbox"/>	Default self-signed saml server cer...	SAML	SAML_ise32-01.ad.rem-sj...	SAML_ise32-01.ad.rem-sj...	m.co	Thu, 2 May 2024	Tue, 1 May 2029	<input checked="" type="checkbox"/>	Active
	Trusted Certificates	<input type="checkbox"/>	CN=ise32-01.ad.rem-sj...em.com, OU=ISE Messaging Service@Certificate Services Endpoint Sub CA - ise32-01800001	ISE Messaging Service	ise32-01.ad.rem-sj...	ise32-01	Wed, 1 May 2024	Wed, 2 May 2029	<input checked="" type="checkbox"/>	Active	
	OCSP Client Profile	<input type="checkbox"/>	CN=ise32-01.ad.rem-sj...1 m.com, OU=Certificate Services System Certificate@Certificate Services Endpoint Sub CA - ise32-01800002	Not in use	ise32-01.ad.rem-sj...	em.com	Wed, 1 May 2024	Wed, 2 May 2029	<input checked="" type="checkbox"/>	Active	
	Certificate Signing Requests	<input type="checkbox"/>	CN=ise32-01.ad.rem-sj...1 m.com#rootCACCommonName#0004	Portal	ise32-01.ad.rem-sj...	em.com	rootCACCommonName	Tue, 4 Jun 2024	Wed, 4 Jun 2025	<input checked="" type="checkbox"/>	Active
	Certificate Periodic Check Se...	<input type="checkbox"/>	ise-server-cert-friendly-name	Admin, EAP Authentication, RADIUS DTLS, perGrid, Portal	ise32-01.ad.rem-sj...	m.com	ocsp-ca-common-name	Tue, 4 Jun 2024	Wed, 4 Jun 2025	<input checked="" type="checkbox"/>	Active

Server Certificate

Navigate to **Administration > Certificates > OCSP Client Profile**, click Add button to add a new OCSP

client profile.

- Name: ojsp\_test\_profile
- Configure OCSP Responder URL: <http://winserver.ad.rem-xxx.com/ocsp>

The screenshot shows the 'Edit OCSP Profile' configuration page in Cisco ISE. The 'Name' field is highlighted with a red box and contains 'ocsp\_test\_profile'. The 'Primary Server' section is expanded, showing the URL 'http://r.ad.rem-t\_s'm.com/ocsp' also highlighted with a red box. Below the URL, there are checkboxes for 'Enable Nonce Extension Support' and 'Validate Response Signature', both of which are checked. The 'Response Cache' section is also expanded, showing 'Cache Entry Time To Live' set to '1440 Minutes', which is highlighted with a red box. A 'Clear Cache' button is located to the right of the cache settings.

OCSP Client Profile

Navigate to **Administration > Certificates > Trusted Certificates**, confirm the trusted CA is imported to ISE.

The screenshot shows the 'Trusted Certificates' list in Cisco ISE. The entry 'ocsp-ca-friendly-name' is highlighted with a red box. The table below shows the details of the certificates.

Certificate Name	Issuer	Expiration Date	Status
Cisco Manufacturing CA SHA2	Cisco Manufacturing CA SH...	Mon, 12 Nov 2012	Enabled
Cisco Root CA 2048	Cisco Root CA 2048	Sat, 15 May 2004	Disabled
Cisco Root CA 2099	Cisco Root CA 2099	Wed, 10 Aug 2016	Enabled
Cisco Root CA M1	Cisco Root CA M1	Wed, 19 Nov 2008	Enabled
Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Enabled
Cisco RXC-R2	Cisco RXC-R2	Thu, 10 Jul 2014	Enabled
CN=root_ca_common_name, OU=cisc...	root_ca_common_name	Thu, 16 May 2024	Enabled
CN=rootCACCommonName#rootCACom...	rootCACCommonName	Tue, 4 Jun 2024	Enabled
Default self-signed server certificate	ise32-01.ad.rem-system.com	Thu, 2 May 2024	Enabled
DigiCert Global Root CA	DigiCert Global Root CA	Fri, 10 Nov 2006	Enabled
DigiCert Global Root G2 CA	DigiCert Global Root G2	Thu, 1 Aug 2013	Enabled
DigiCert root CA	DigiCert High Assurance EV ...	Fri, 10 Nov 2006	Enabled
DigiCert SHA2 High Assurance Server ...	DigiCert High Assurance EV...	Tue, 22 Oct 2013	Enabled
IdenTrust Commercial Root CA 1	IdenTrust Commercial Root ...	Fri, 17 Jan 2014	Enabled
ocsp-ca-friendly-name	ocsp-ca-common-name	Tue, 4 Jun 2024	Enabled

Trusted CA

Check the CA and click **Edit** button, input the detail of OCSP configuration for **Certificate Status Validation**.

- Validate against OCSP Service: oosp\_test\_profile
- Reject the request if OCSP returns UNKNOWN status: check
- Reject the request if OCSP Responder is unreachable: check

Cisco ISE Administration - System

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings

**Issuer**

\* Friendly Name

Status  Enabled

Description

Subject CN=oosp-ca-common-name

Issuer CN=oosp-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
- 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.

Certificate Status Validation

## Step 6. Add Allowed Protocols

Navigate to **Policy > Results > Authentication > Allowed Protocols**, edit the **Default Network Access** service list and then check **Allow EAP-TLS**.

Dictionary 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

Allow EAP-TLS

## Step 7. Add Policy Set

Navigate to **Policy > Policy Sets**, click + to add a policy set.

- Policy Set Name: EAP-TLS-Test
- Conditions: Network Access Protocol **EQUALS** RADIUS
- Allowed Protocols / Server Sequence: Default Network Access

Cisco ISE Policy - Policy Sets Evaluation Mode : 1 Days

Policy Sets

Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
<span style="color: green;">●</span>	EAP-TLS-Test		Network Access Protocol EQUALS RADIUS	Default Network Access	75		

Add Policy Set

## Step 8. Add Authentication Policy

Navigate to **Policy Sets**, click **EAP-TLS-Test** to add an authentication policy.

- Rule Name: EAP-TLS-Authentication
- Conditions: Network Access EapAuthentication **EQUALS** EAP-TLS **AND** Wired\_802.1 X
- Use: Identity\_AD

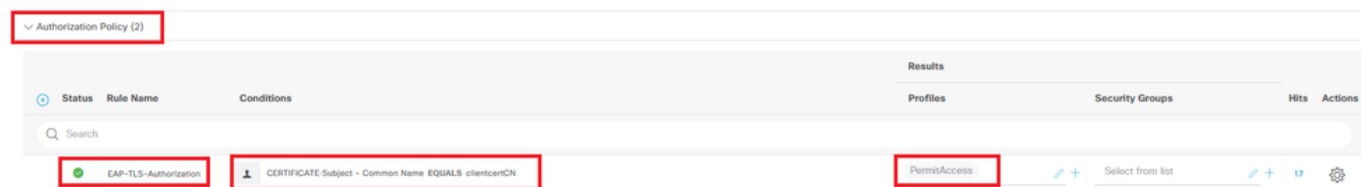


*Add Authentication Policy*

## Step 9. Add Authorization Policy

Navigate to **Policy Sets**, click **EAP-TLS-Test** to add an authorization policy.

- Rule Name: EAP-TLS-Authorization
- Conditions: CERTIFICATE Subject - Common Name **EQUALS** clientcertCN
- Results: PermitAccess



*Add Authorization Policy*

# Verify

## Step 1. Confirm Authentication Session

Runshow authentication sessions interface GigabitEthernet1/0/3 details command to confirm authentication session in C1000.

```
<#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: 01C2006500000933E4E87D9
```

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

## Step 2. Confirm Radius Live Log

Navigate to **Operations > RADIUS > Live Logs** in ISE GUI, confirm the live log for authentication.

The screenshot displays the Cisco ISE GUI for Operations - RADIUS. At the top, there are navigation tabs for 'Live Logs' and 'Live Sessions'. Below this, there are five summary cards: 'Misconfigured Supplicants' (0), 'Misconfigured Network Devices' (0), 'RADIUS Drops' (0), 'Client Stopped Responding' (0), and 'Repeat Counter' (0). Below the cards, there are controls for 'Refresh' (Never), 'Show Latest 50 records', and 'Within Last 24 hours'. There are also buttons for 'Reset Repeat Counts' and 'Export To'. The main part of the screenshot is a table with the following columns: Time, Status, Details, Repeats, Identity, Endpoint ID, Endpoint Name, Authentication Policy, Authorization Policy, Authorization Policy Name, and IP Address. The table contains two rows of data. The second row is highlighted with a red border and shows a successful authentication event for clientcertCN on Jun 05, 2024 at 09:43:33.2.

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authentication Policy	Authorization Policy	Authorizatio...	IP Address
Jun 05, 2024 09:43:36.3...	<span style="color: blue;">●</span>		0	clientcertCN	B4-98-91:14:3...	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...	<span style="color: green;">■</span>			clientcertCN	B4-98-91:14:3...	Intel-Device	EAP-TLS-Test >> EAP-TLS-Authentication	EAP-TLS-Test >> EAP-TLS-Authorization	PermitAccess	

*Radius Live Log*

Confirm the detailed live log of authentication.



## 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	01C2006500000933E4E87D9

## Other Attributes

ConfigVersionId	167
DestinationPort	1645
Protocol	Radius
NAS-Port	50103
Framed-MTU	1500
State	37CPMSessionID=01C2006500000933E4E87D9;31SessionID=ise32-01/506864164/73;
AD-User-Resolved-Identities	clientcertCN@ad.rem-s;:rem.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;:rem, DC=com
AD-User-DNS-Domain	ad.rem-s;:rem.com
AD-User-NetBios-Name	AD
IsMachineIdentity	false
AD-User-SamAccount-Name	clientcertCN
AD-User-Qualified-Name	clientcertCN@ad.rem-sy;:em.com
AD-User-SamAccount-Name	clientcertCN
AD-User-Qualified-Name	clientcertCN@ad.rem-sy;:em.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;:em.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

```
Crypto,2024-06-05 09:43:33,064,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, CryptoLib.CSSL.OCSP C
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
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=01C20065000000933E4E87D9;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,CPMSession

Code=5(AccountingResponse)

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

## 2. TCP Dump

In the TCP dump in ISE, you expect to find information about the OCSPP response and Radius session.

OCSP request and response :

No.	Time	Identification	Source	S.Port	Destination	D.Port	Time to Live	Protocol	Length	TCP.Se	Next seq	TCP.Ac	Info
140	2024-06-05 00:43:33.093523	0x0295 (661)	1.1.1.181	25844	1.1.1.157	80		64 OCSP	262	1	197	1	Request
141	2024-06-05 00:43:33.104108	0x0117 (279)	1.1.1.157	80	1.1.1.181	25844		128 OCSP	1671	1	1607	197	Response

Packet Capture of OCSP Request and Response

```

> 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: 1.1.1.157, Dst: 1.1.1.181
> Transmission Control Protocol, Src Port: 80, Dst Port: 25844, Seq: 1, Ack: 197, Len: 1605
> Hypertext Transfer Protocol
  Online Certificate Status Protocol
    responseStatus: successful (0)
  responseBytes
    ResponseType Id: 1.3.6.1.5.5.7.48.1.1 (id-pkix-ocsp-basic)
  BasicOCSPResponse
    tbsResponseData
      responderID: byKey (2)
      producedAt: Jun 5, 2024 09:43:33.000000000
      responses: 1 item
        SingleResponse
          certID
            certStatus: good (0)
            thisUpdate: Jun 4, 2024 16:05:00.000000000
            nextUpdate: Jul 4, 2024 16:05:00.000000000
          responseExtensions: 1 item

```

Capture Detail of OCSP Response

Radius session :

146	2024-06-05 00:43:33.118175	0x9bc6 (39878)	1.1.1.181	67181	1.1.1.181	1645		255 RADIUS	366				Access-Request id=238
185	2024-06-05 00:43:33.270244	0x033d (829)	1.1.1.181	67181	1.1.1.181	1645		64 RADIUS	336				Access-Accept id=238
187	2024-06-05 00:43:33.341233	0x9bc7 (39879)	1.1.1.181	1646	1.1.1.181	1646		255 RADIUS	328				Accounting-Request id=10
188	2024-06-05 00:43:33.350936	0x037a (890)	1.1.1.181	1646	1.1.1.181	1646		64 RADIUS	62				Accounting-Response id=10
267	2024-06-05 00:43:36.359621	0x9bc8 (39880)	1.1.1.181	1646	1.1.1.181	1646		255 RADIUS	334				Accounting-Request id=11
268	2024-06-05 00:43:36.369035	0x0489 (1161)	1.1.1.181	1646	1.1.1.181	1646		64 RADIUS	62				Accounting-Response id=11

Packet Capture of Radius Session

## **Related Information**

[Configure EAP-TLS Authentication with ISE](#)

[Configure TLS/SSL Certificates in ISE](#)