在ISE中配置使用OCSP的EAP-TLS身份驗證

目錄

簡介

本文檔介紹為即時客戶端證書撤銷檢查設定使用OCSP的EAP-TLS身份驗證所需的步驟。

必要條件

需求

思科建議您瞭解以下主題：

- 思科身份服務引擎的配置
- Cisco Catalyst的配置
- 線上憑證狀態通訊協定

採用元件

本文中的資訊係根據以下軟體和硬體版本：

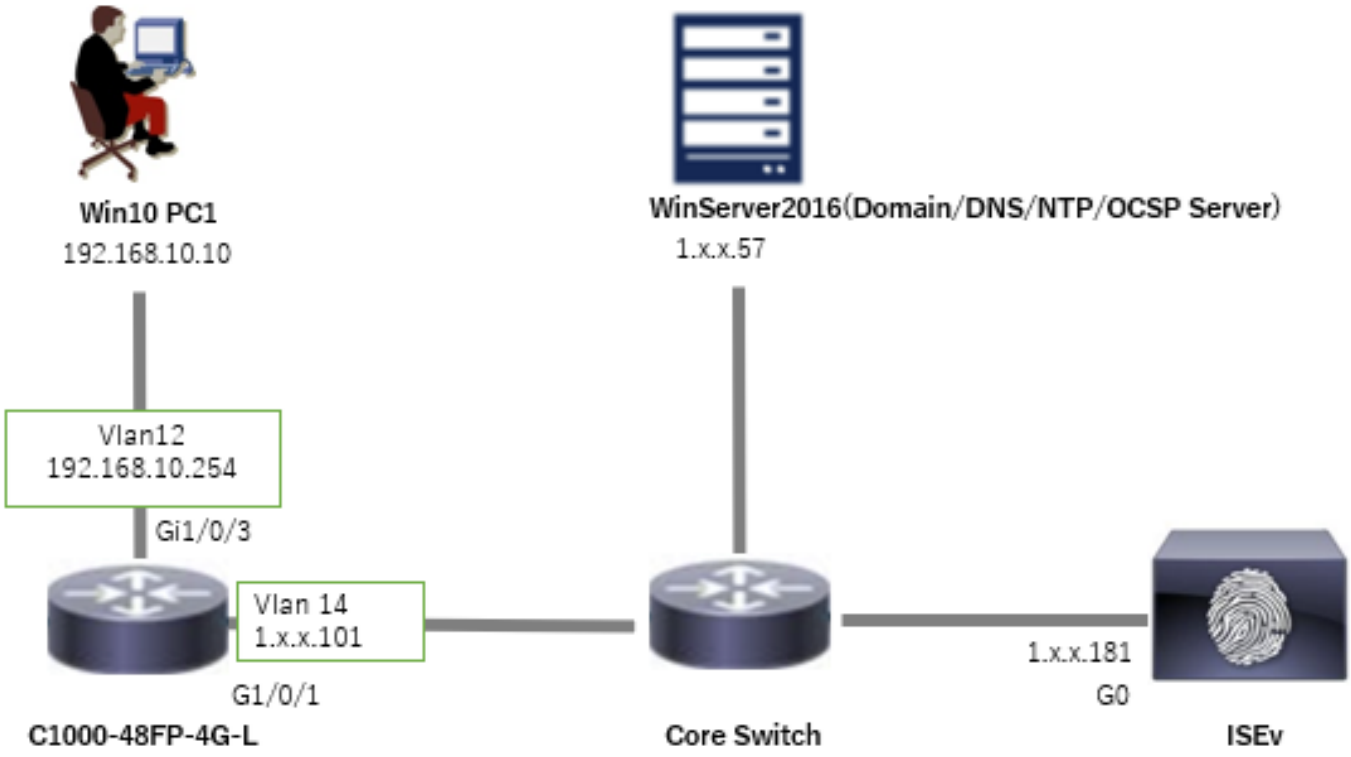
- 身分辨識服務引擎虛擬3.2修補程式6
- C1000-48FP-4G-L 15.2(7)E9

- Windows Server 2016
- Windows 10

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

網路圖表

下圖顯示本文檔示例中使用的拓撲。



網路圖表

背景資訊

在EAP-TLS中，使用者端將其數位憑證顯示給伺服器，作為驗證程式的一部分。 本文檔介紹ISE如

何透過根據AD伺服器檢查證書公用名(CN)並確認證書是否已使用OCSP（線上證書狀態協定）撤銷來驗證客戶端證書，OCSP提供即時協定狀態。

在Windows Server 2016上配置的域名是ad.rem-xxx.com，本文檔中用作示例。

本文檔中引用的OCSP（線上證書狀態協定）和AD(Active Directory)伺服器用於證書驗證。

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

這是憑證鏈結，其中包含檔案中使用的每個憑證的一般名稱。

- CA： ocsp-ca-common-name
- 客戶端證書：clientcertCN
- 伺服器憑證： ise32-01.ad.rem-xxx.com
- OCSP簽名證書：ocspSignCommonName

組態

C1000中的配置

這是C1000 CLI中的最小配置。

```
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
```

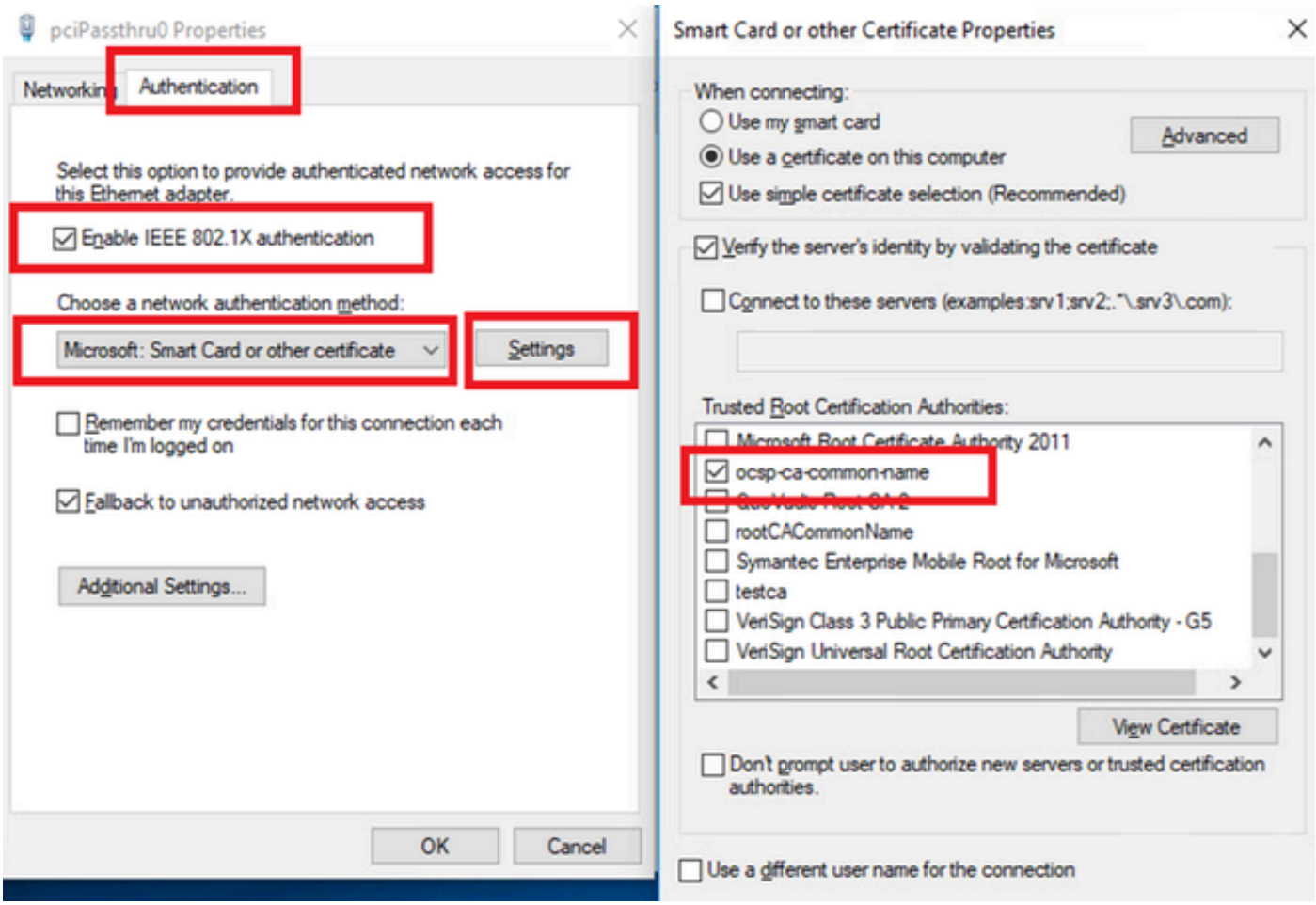
```
dot1x pae authenticator
spanning-tree portfast edge
```

Windows PC中的配置

步驟 1.配置使用者身份驗證

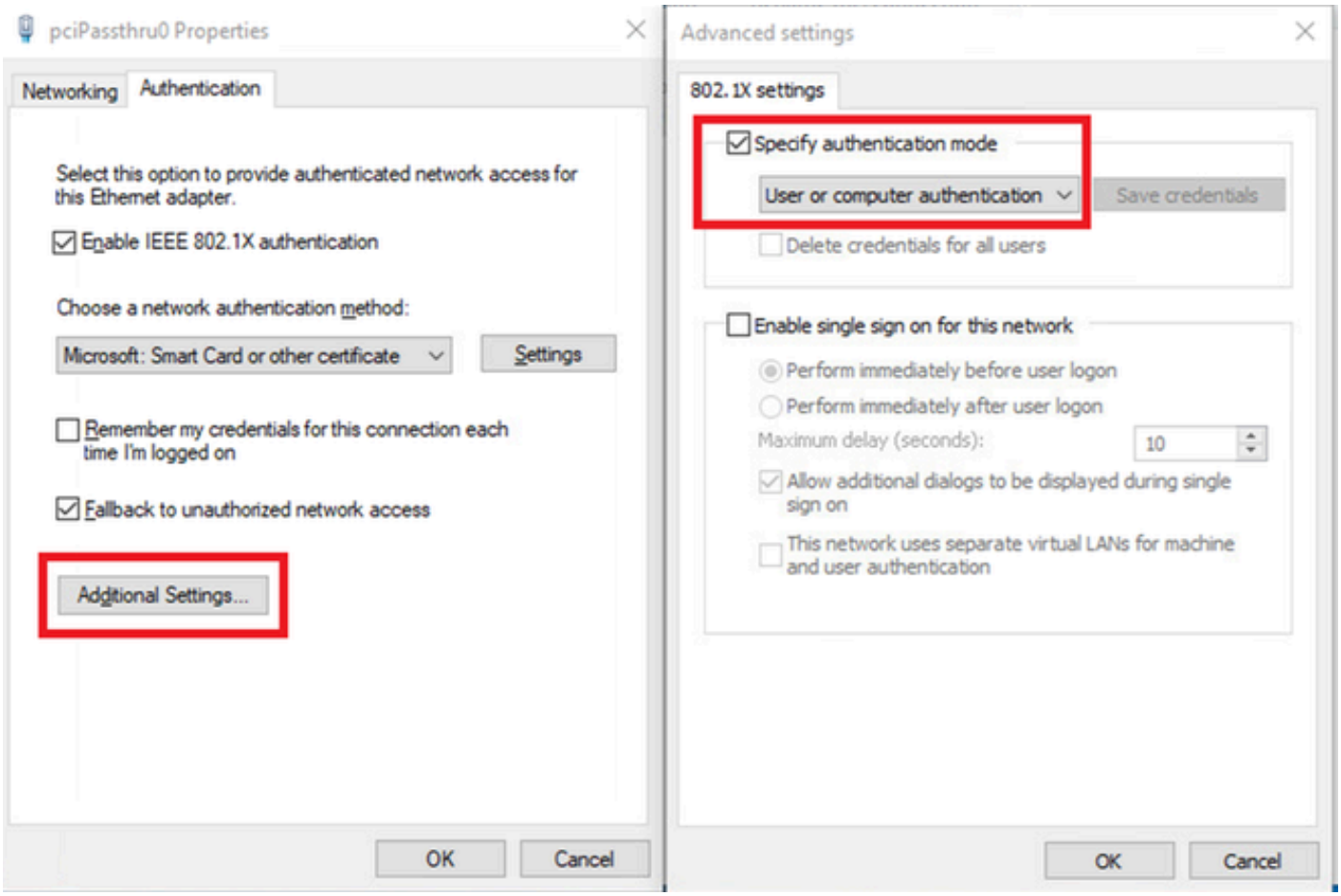
導覽至Authentication，checkEnable IEEE 802.1X authentication，然後選擇Microsoft：智慧卡或其他憑證。

按一下「設定」按鈕，選中「使用此電腦上的證書」，然後選擇Windows PC的受信任CA。



啟用憑證驗證

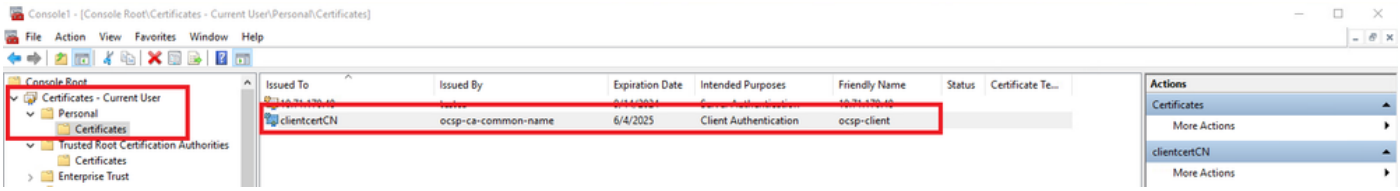
導覽至Authentication，checkAdditional Settings。從下拉清單中選擇使用者或電腦身份驗證。



指定驗證模式

步驟 2.確認使用者端憑證

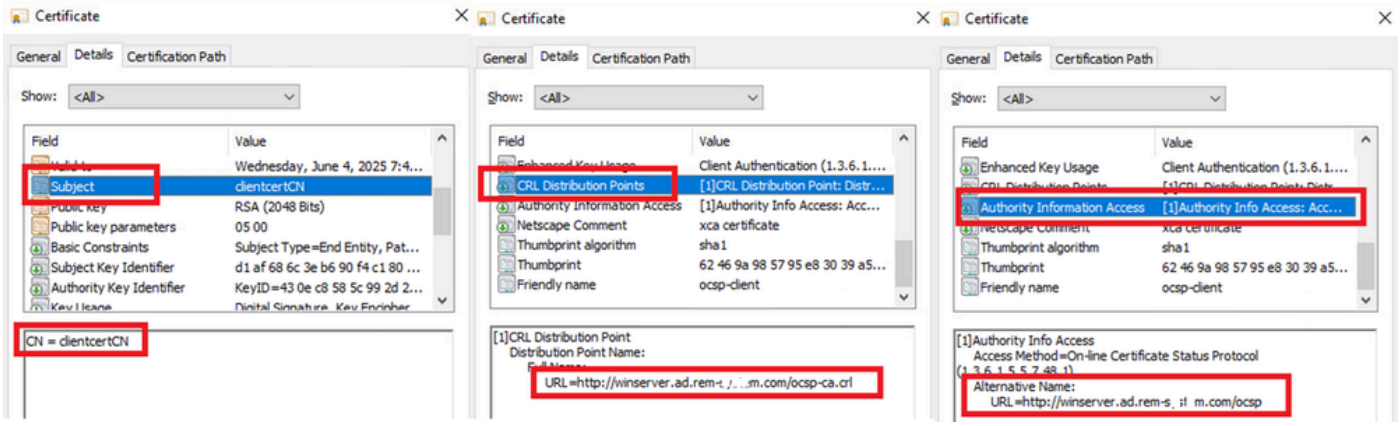
導航到證書- Current User > Personal > Certificates，然後檢查用於身份驗證的客戶端證書。



確認使用者端憑證

按兩下客戶端證書，導航到Details，檢查Subject、CRL分發點、Authority Information Access的詳細資訊。

- 主題：CN = clientcertCN
- CRL分發點：http://winserver.ad.rem-xxx.com/ocsp-ca.crl
- 授權資訊存取：http://winserver.ad.rem-xxx.com/ocsp

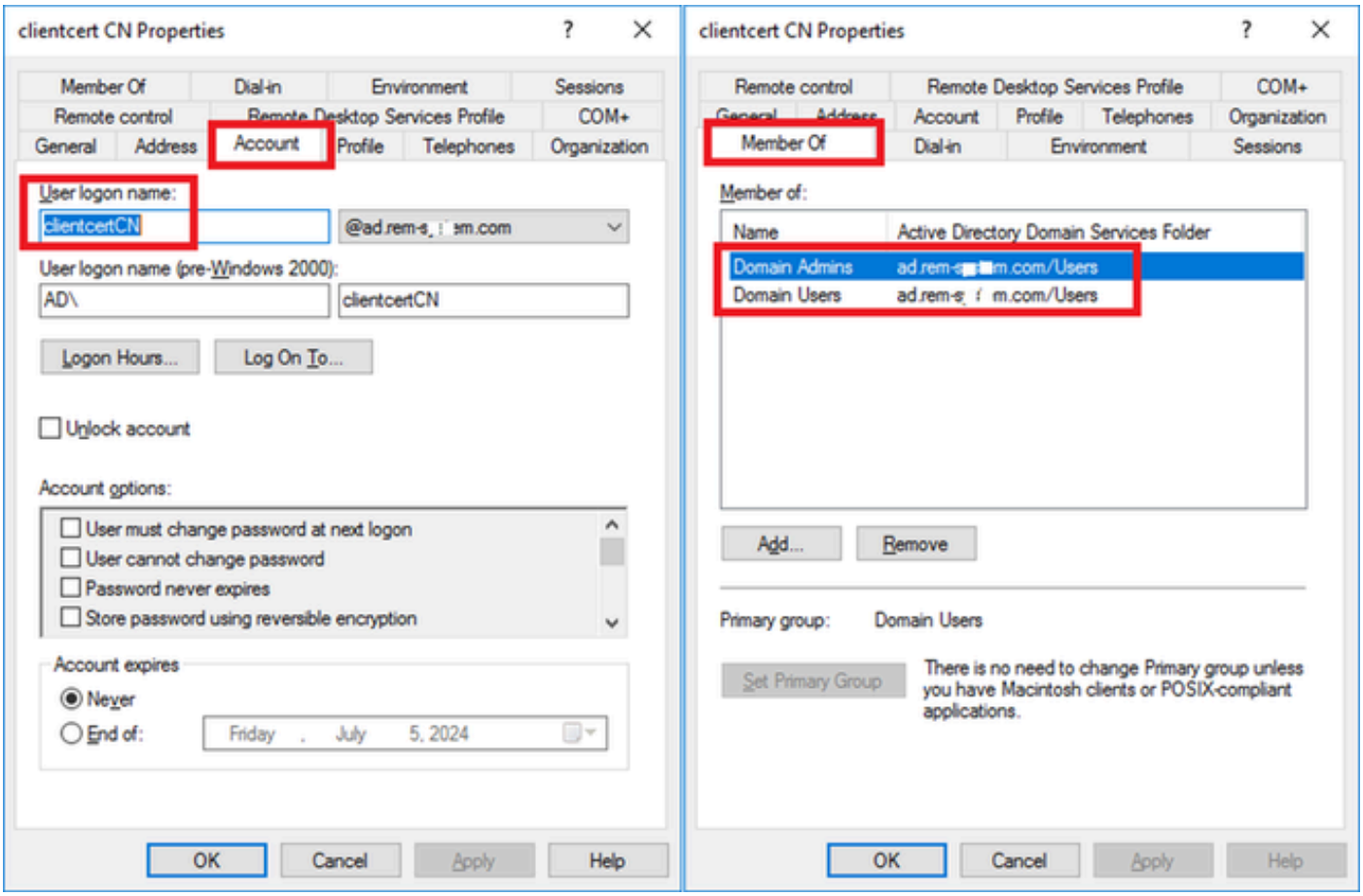


客戶端證書的詳細資訊

Windows Server中的配置

步驟 1.新增使用者

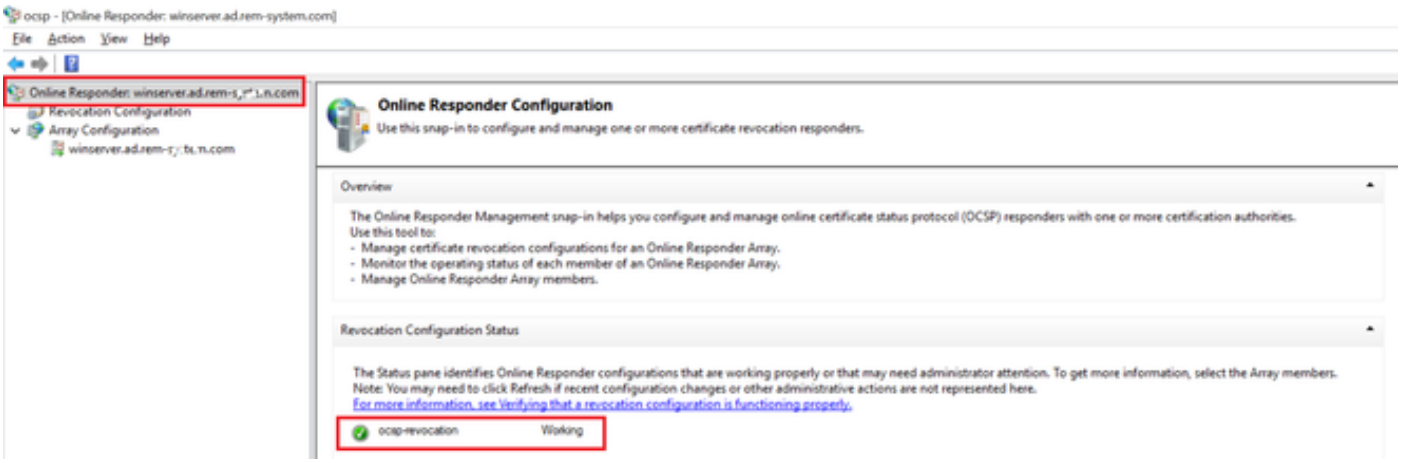
導覽至Active Directory Users and Computers，然後按一下Users。增加clientcertCN作為使用者登入名。



使用者登入名稱

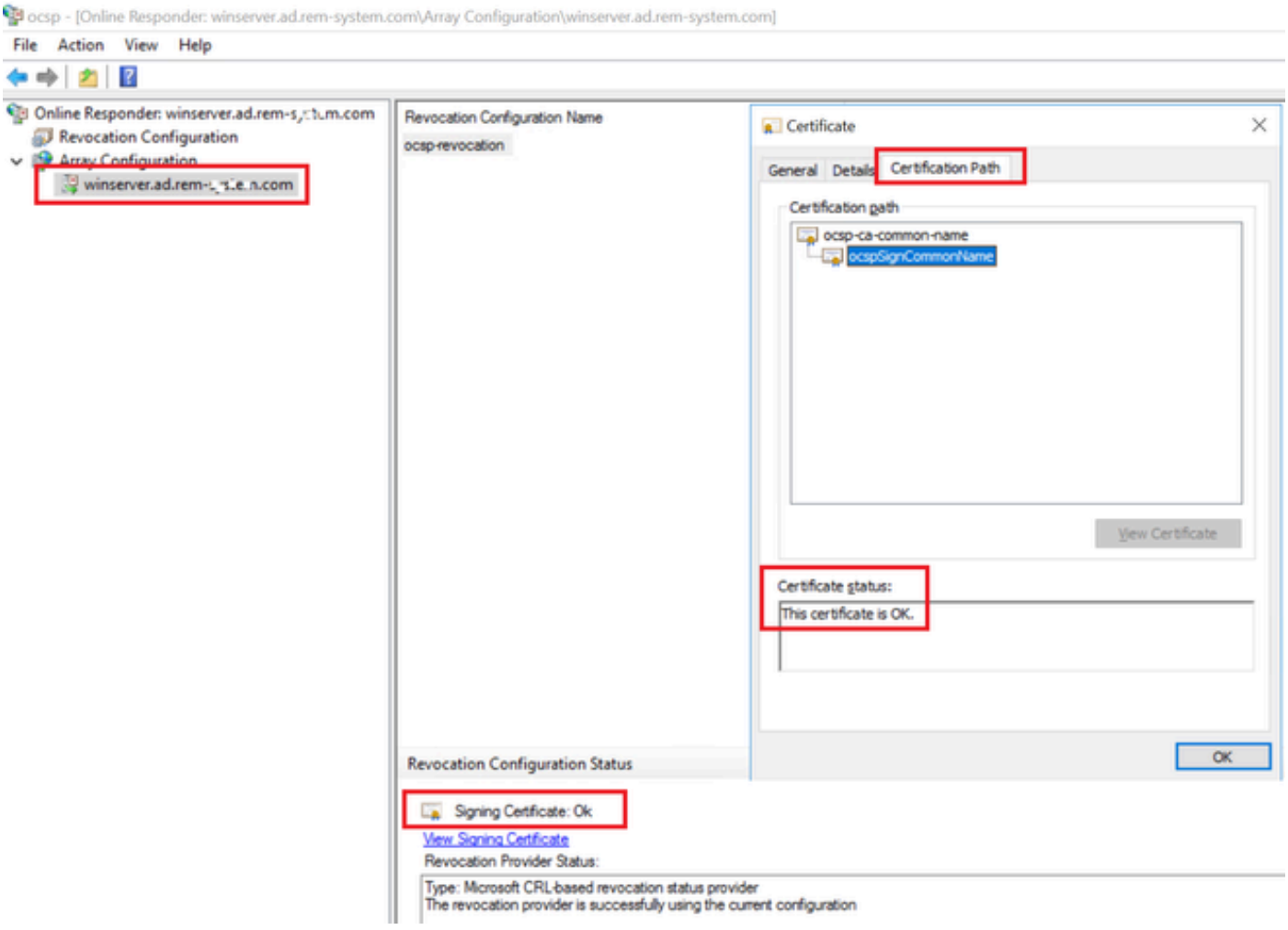
步驟 2.確認OCSP服務

導航到Windows，點選線上響應程式管理。確認OCSP伺服器的狀態。



OCSP伺服器的狀態

按一下winserver.ad.rem-xxx.com，檢查OCSP簽名證書的狀態。

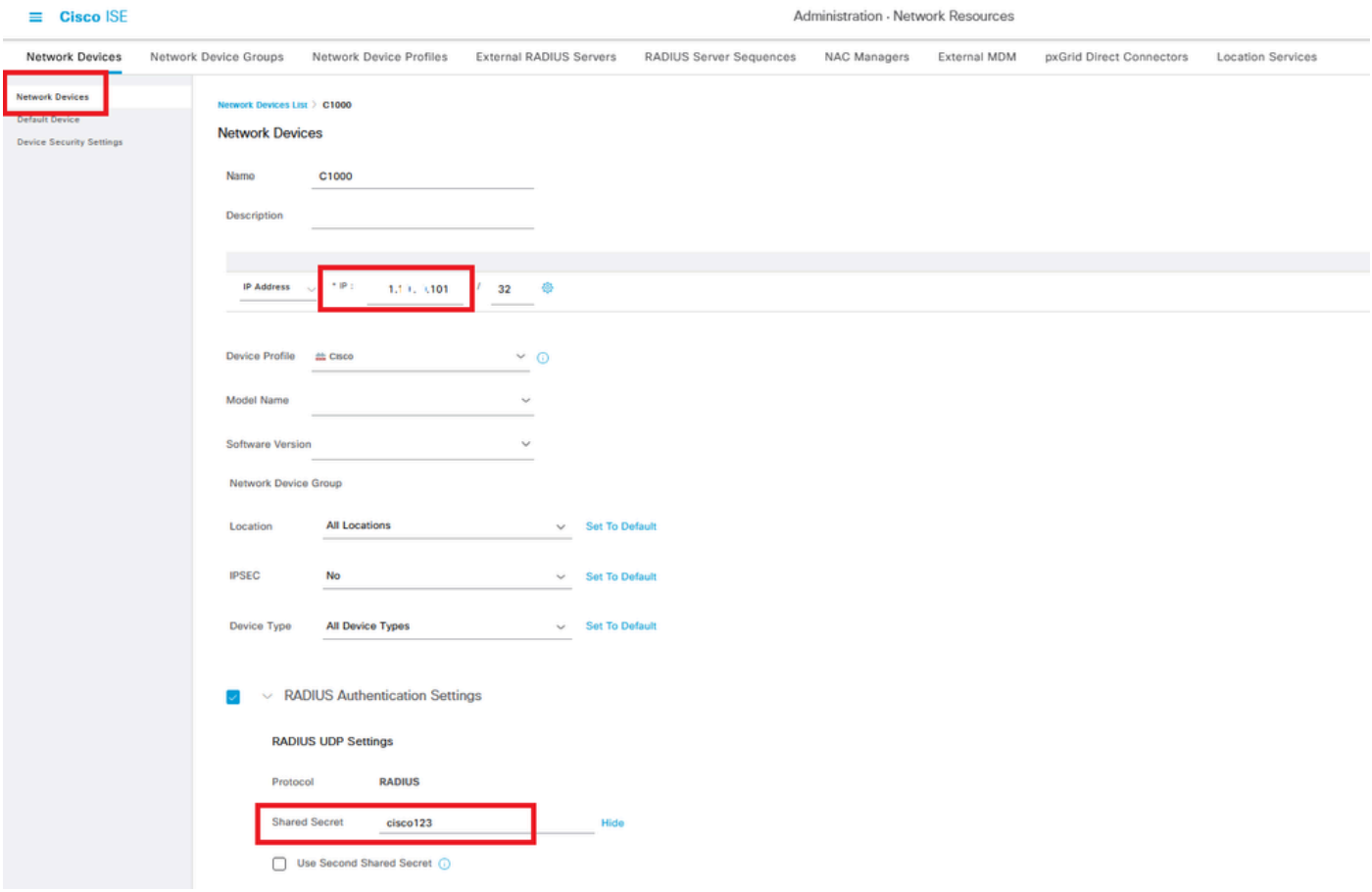


OCSP簽名證書的狀態

ISE中的配置

步驟 1.增加裝置

導航到管理>網路裝置，點選增加按鈕，增加C1000裝置。

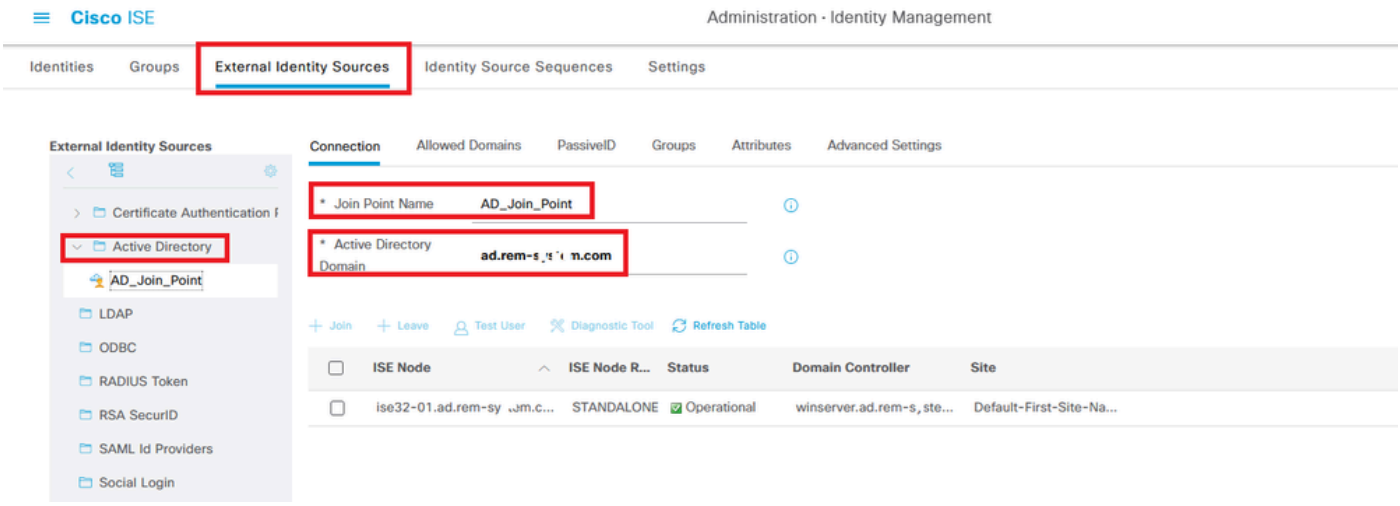


增加裝置

步驟 2.新增Active Directory

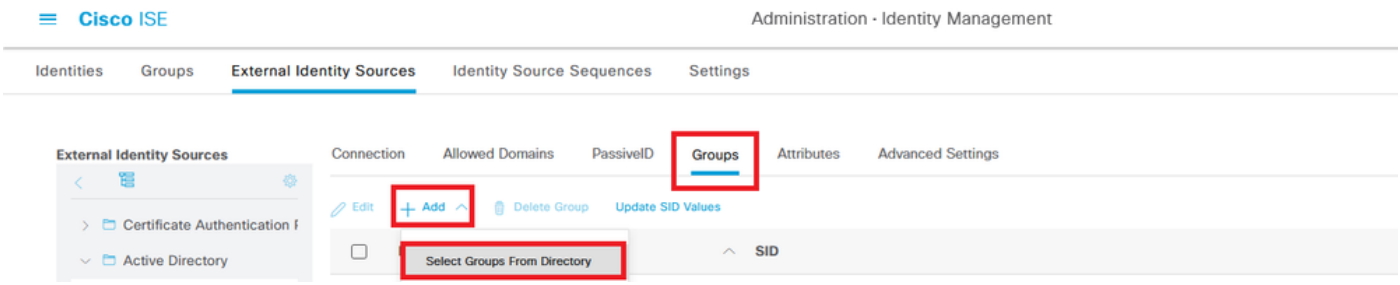
導航到管理>外部身份源> Active Directory，點選連線頁籤，將Active Directory增加到ISE。

- 連線點名稱：AD_Join_Point
- Active Directory域： ad.rem-xxx.com



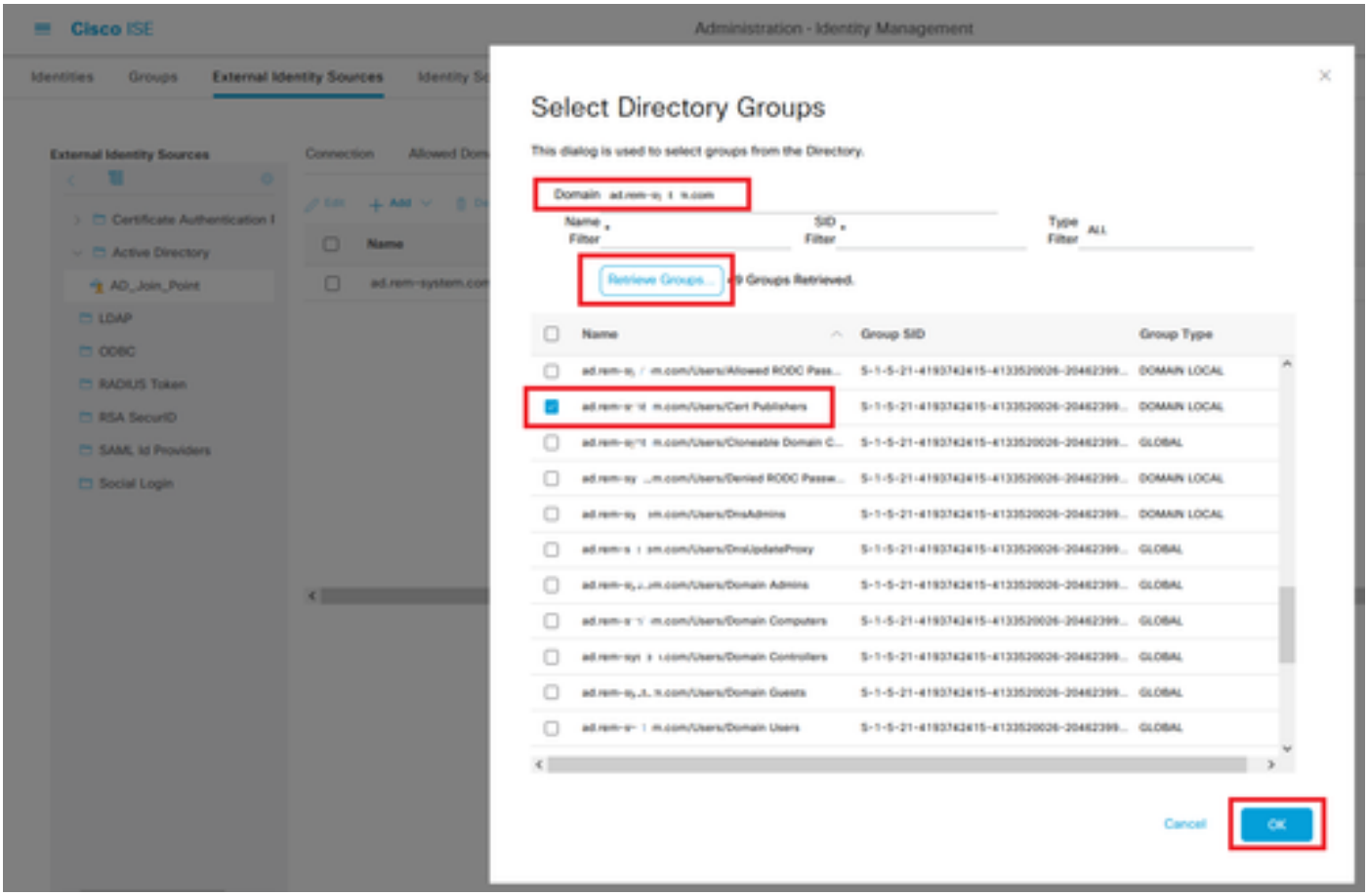
新增Active Directory

導航到組頁籤，從下拉選單中選擇從目錄選擇組。



從目錄選取群組

按一下「擷取群組」下拉式清單。Checkad.rem-xxx.com/Users/Cert Publishers 並按一下確定。

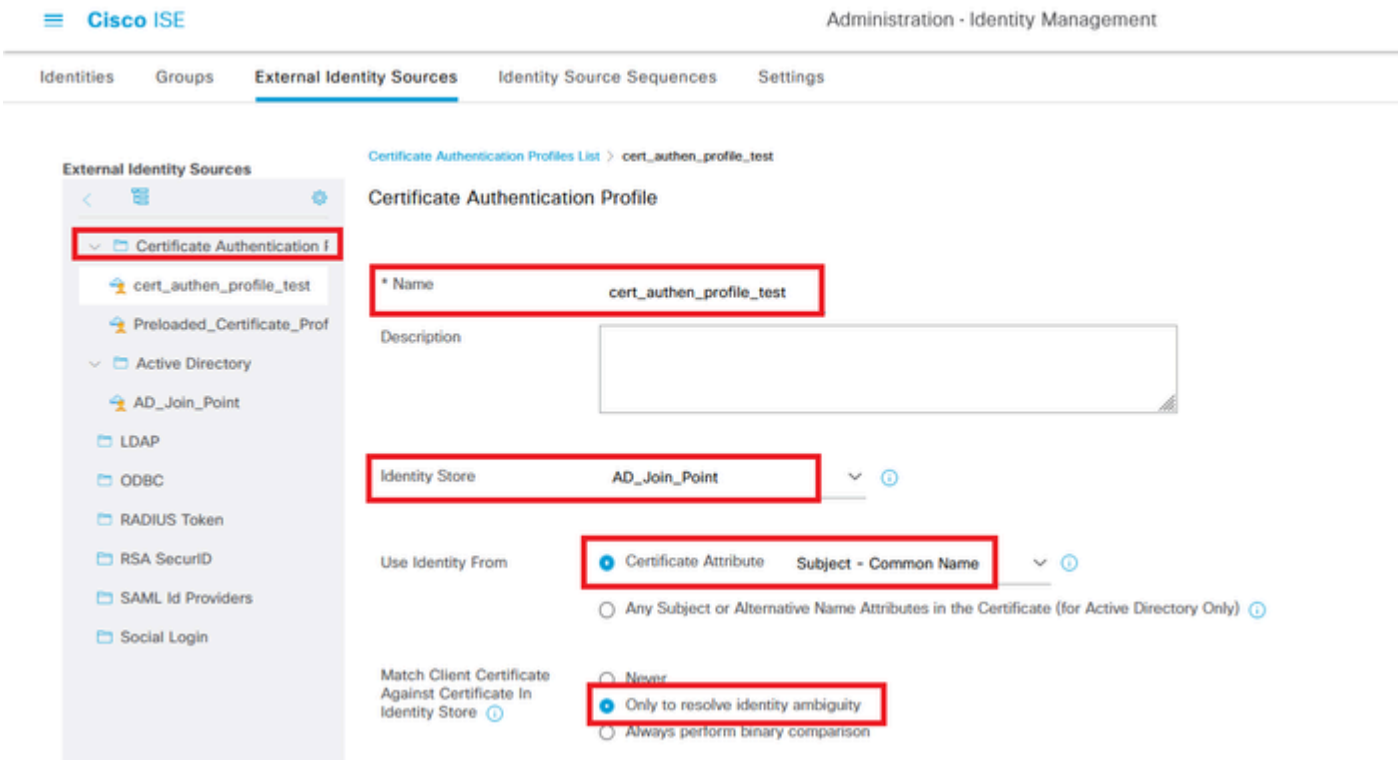


檢查憑證發行者

步驟 3.增加證書身份驗證配置檔案

導航到Administration > External Identity Sources > Certificate Authentication Profile，按一下Add按鈕以增加新的證書身份驗證配置檔案。

- 名稱：cert_authen_profile_test
- 身份庫：AD_Join_Point
- 使用Identity From Certificate屬性：使用者-一般名稱。
- 將使用者端憑證與辨識存放區中的憑證比對：僅用於解決辨識模糊問題。

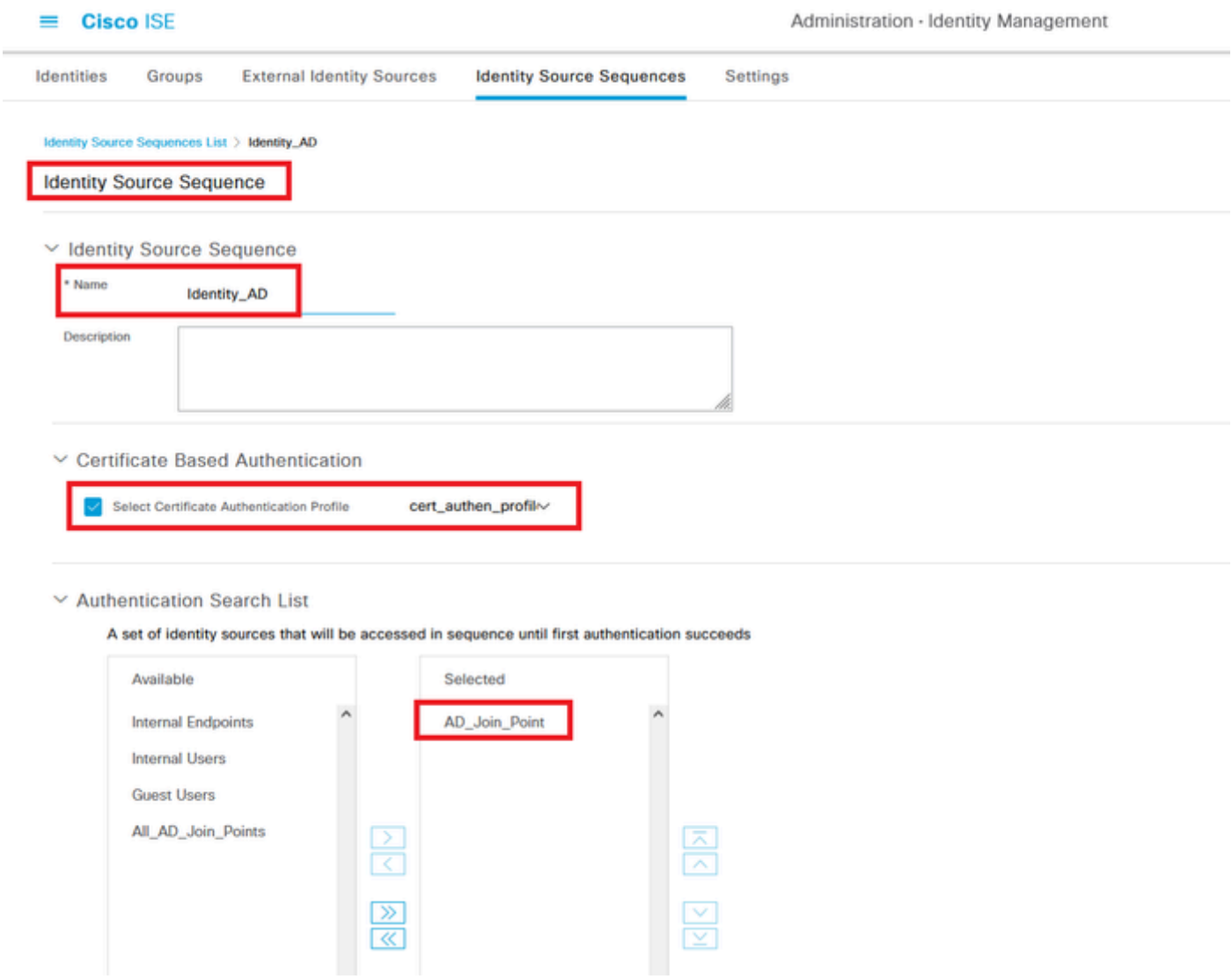


增加證書身份驗證配置檔案

步驟 4.增加身份源隔離

導航到管理>身份源序列，增加身份源序列。

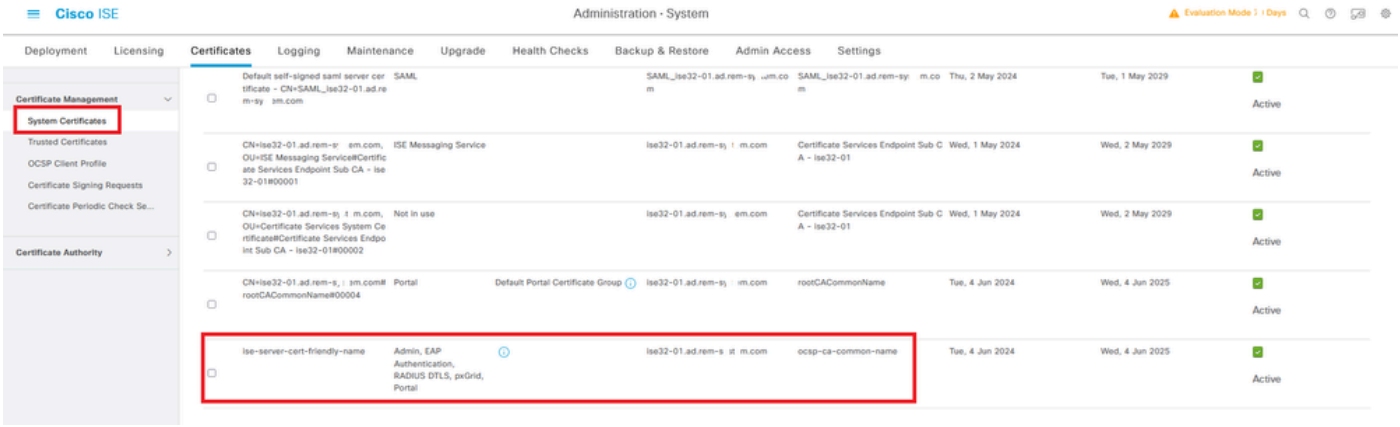
- 名稱：Identity_AD
- 選取「憑證驗證」 Profile: cert_authen_profile_test
- 身份驗證搜尋清單：AD_Join_Point



增加身份源序列

步驟 5.ISE中的確認證書

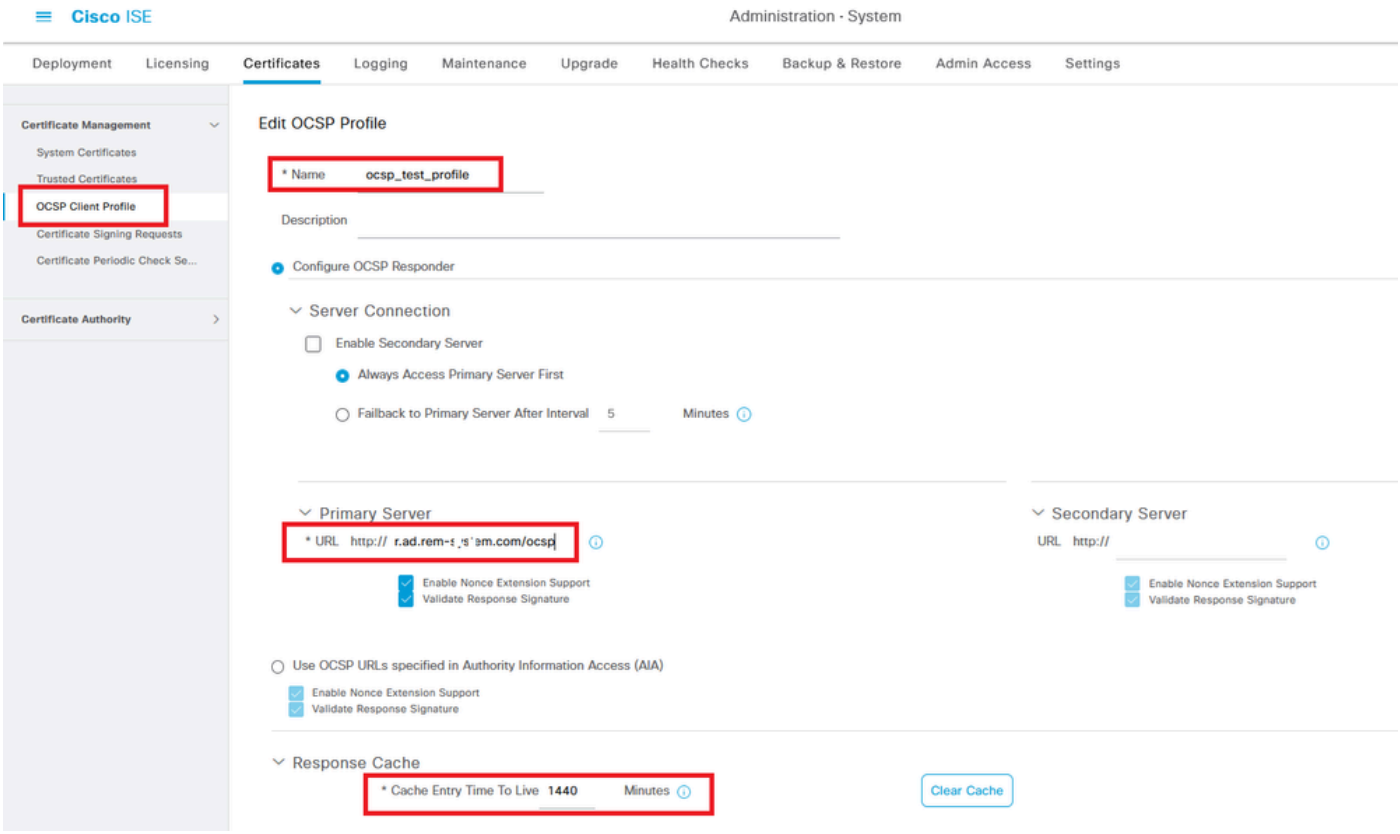
導航到管理>證書>系統證書，確認伺服器證書由受信任CA簽署。



伺服器憑證

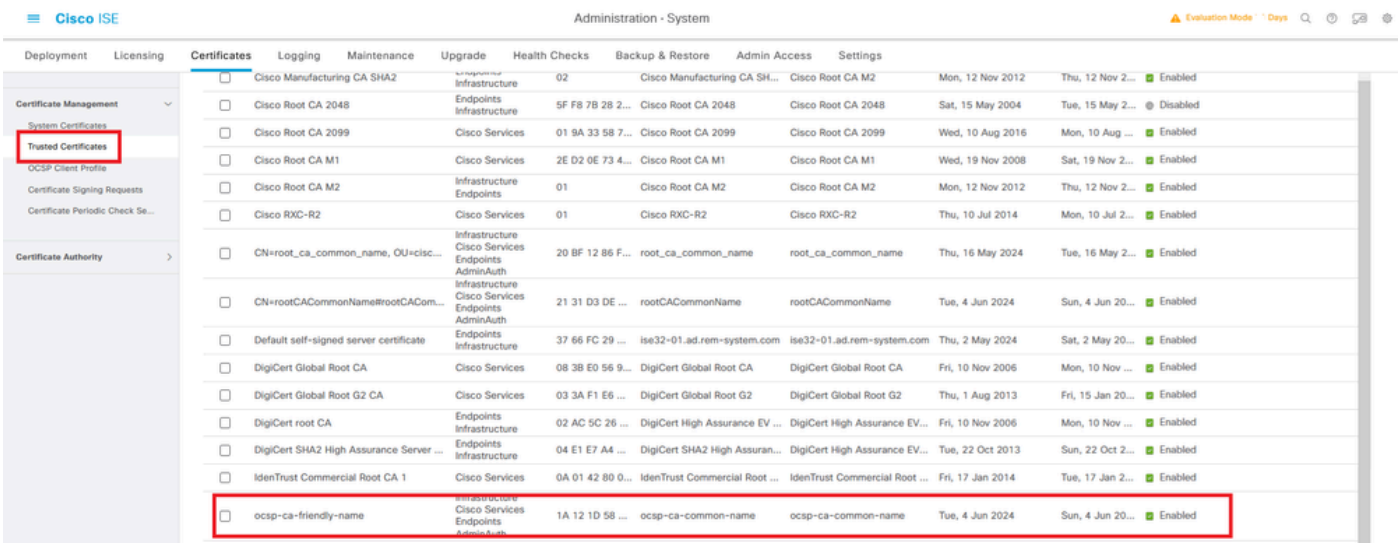
導航到管理>證書> OCSP客戶端配置檔案，按一下「增加」按鈕增加新的OCSP客戶端配置檔案。

- 名稱：ocsp_test_profile
- 配置OCSP響應程式URL：http://winserver.ad.rem-xxx.com/ocsp



OCSP客戶端配置檔案

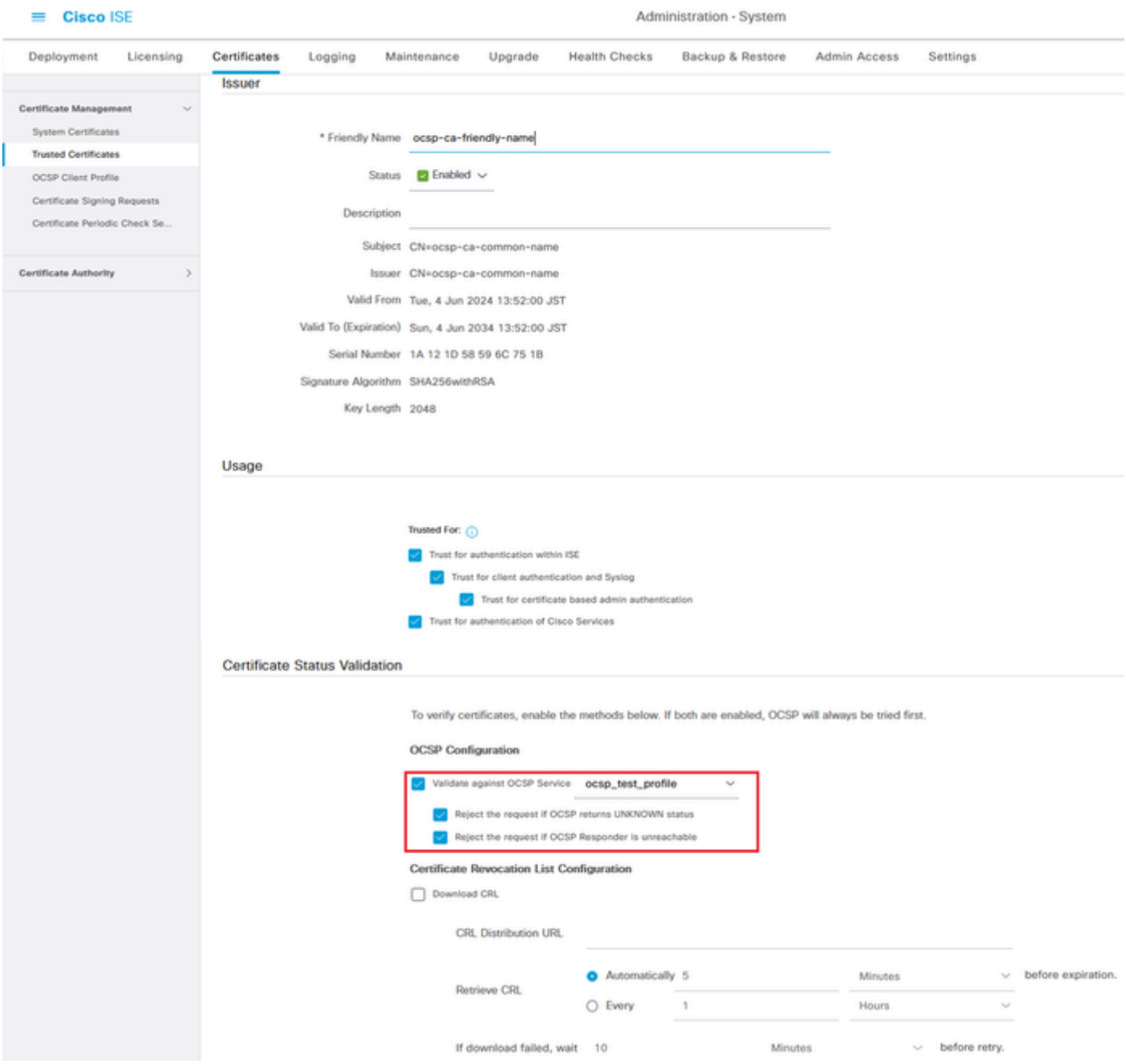
導航到管理>證書>受信任證書，確認受信任CA已導入到ISE。



受信任的CA

選中CA並按一下Edit按鈕，輸入OCSP配置的詳細資訊以進行證書狀態驗證。

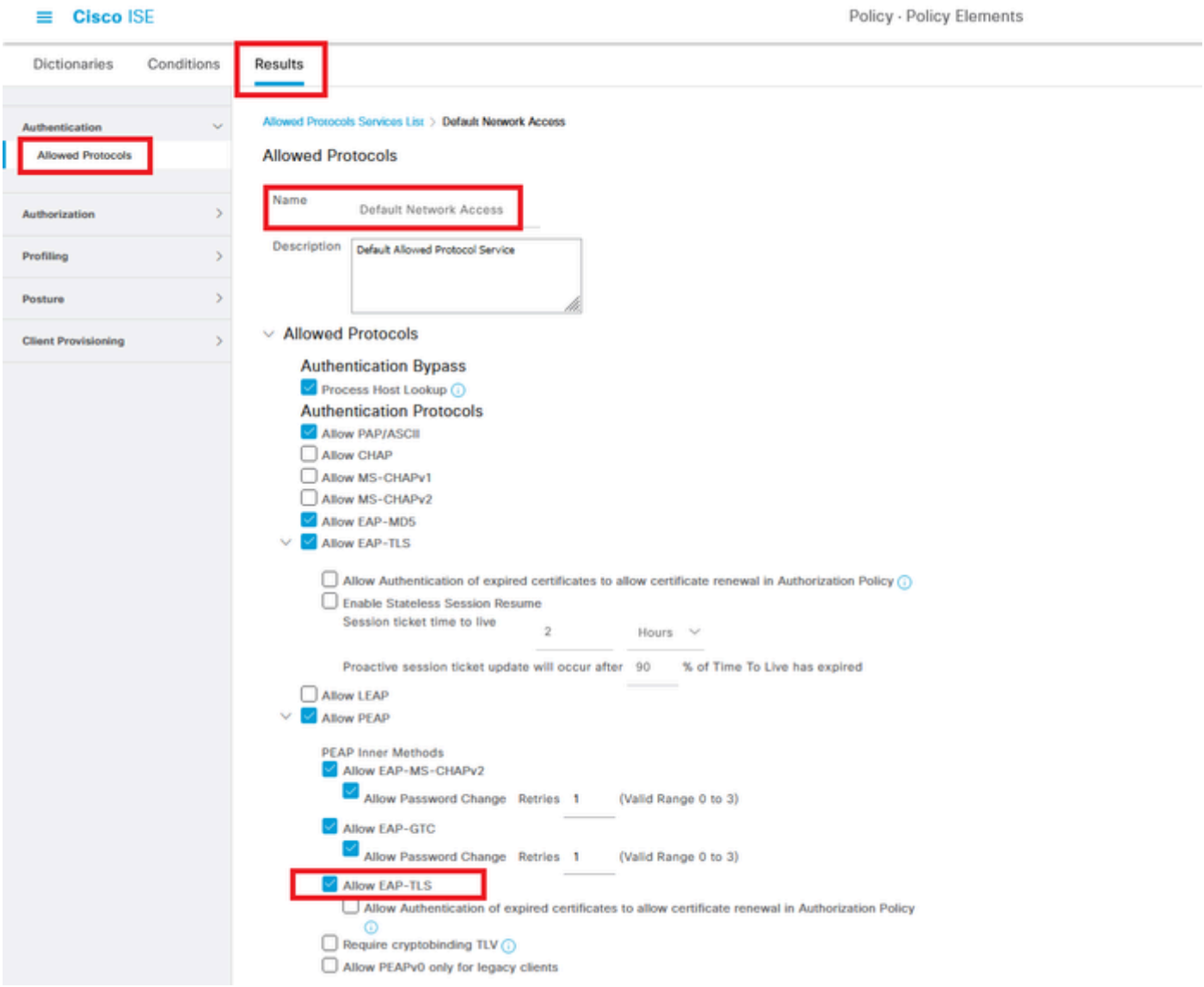
- 根據OCSP服務進行驗證：ocsp_test_profile
- 如果OCSP返回UNKNOWN狀態，則拒絕請求：檢查
- 如果OCSP響應程式無法訪問，則拒絕請求：檢查



憑證狀態驗證

步驟 6.增加允許的協定

導航到策略>結果>身份驗證>允許的協定，編輯預設網路訪問服務清單，然後選中允許EAP-TLS。

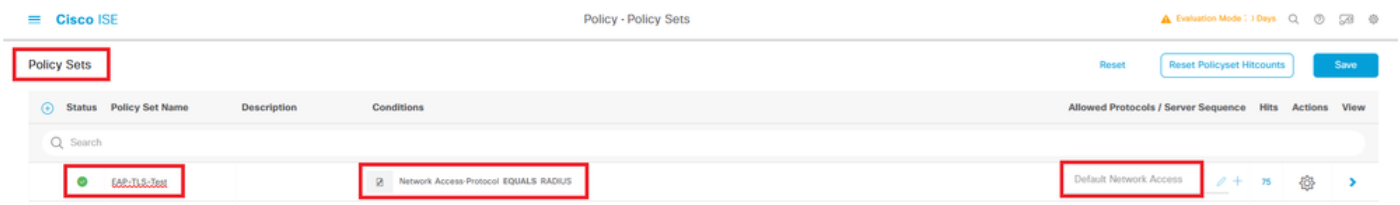


允許EAP-TLS

步驟 7.增加策略集

導航到策略>策略集，點選+ 增加策略集。

- 策略集名稱：EAP-TLS-Test
- 條件：網路訪問協定等於RADIUS
- 允許的協定/伺服器序列：預設網路訪問



增加策略集

步驟 8.增加身份驗證策略

導航到策略集，點選EAP-TLS-Testto增加身份驗證策略。

- 規則名稱：EAP-TLS-Authentication
- 條件：網路訪問EapAuthentication 等於EAP-TLS 和Wired_802.1 X
- 使用：Identity_AD

增加身份驗證策略

步驟 9.增加授權策略

導航到策略集，點選EAP-TLS-Test增加授權策略。

- 規則名稱：EAP-TLS-Authorization
- 條件：證書使用者-公用名等於clientcertCN
- 結果：PermitAccess

增加授權策略

驗證

步驟 1.確認身份驗證會話

運行show authentication sessions interface GigabitEthernet1/0/3 details命令，確認C1000中的身份驗證會話。

<#root>

Switch#

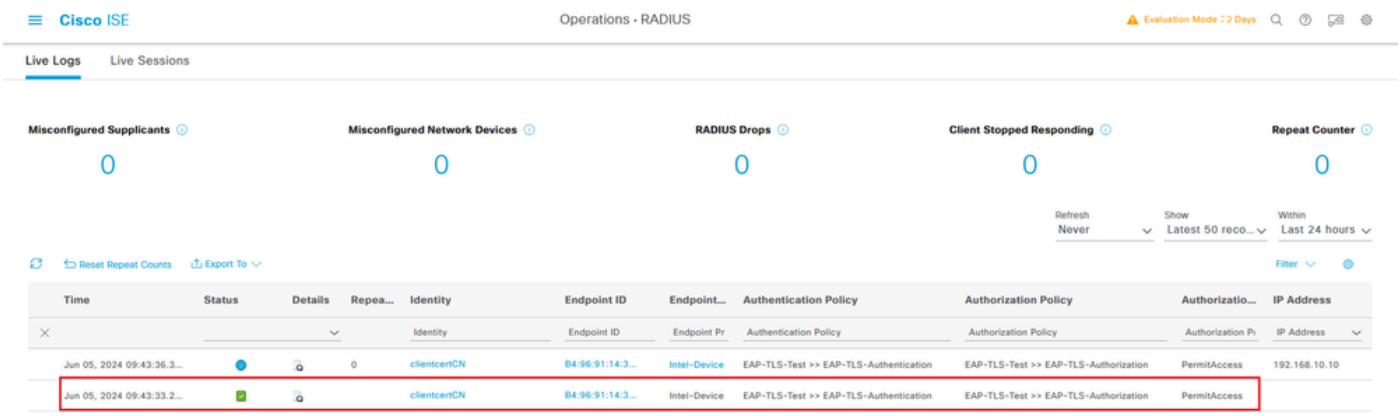
show authentication sessions interface GigabitEthernet1/0/3 details

```
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
```

步驟 2.確認Radius即時日誌

在ISE GUI中導航到**操作> RADIUS >即時**日誌，確認身份驗證的即時日誌。



*Radius*即時日誌

確認身份驗證的詳細即時日誌。

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	01C200650000000933E4E87D9

Other Attributes

ConfigVersionId	167
DestinationPort	1645
Protocol	Radius
NAS-Port	50103
Framed-MTU	1500
State	37CPMSessionID=01C200650000000933E4E87D9;31SessionID=ise32-01/506864164/73;
AD-User-Resolved-Identities	clientcertCN@ad.rem-s[illegible]em.com
AD-User-Candidate-Identities	clientcertCN@ad.rem-s[illegible]em.com
TotalAuthenLatency	324
ClientLatency	80
AD-User-Resolved-DNs	CN=clientcert CN,CN=Users,DC=ad,DC=rem-s[illegible]tem,DC=com
AD-User-DNS-Domain	ad.rem-s[illegible]tem.com
AD-User-NetBios-Name	AD
IsMachineIdentity	false
AD-User-SamAccount-Name	clientcertCN
AD-User-Qualified-Name	clientcertCN@ad.rem-s[illegible]m.com
AD-User-SamAccount-Name	clientcertCN
AD-User-Qualified-Name	clientcertCN@ad.rem-s[illegible]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[illegible]em.com
24319	Single matching account found in forest - ad.rem-s[illegible]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

身份驗證詳細資訊

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=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,CPMSessi
```

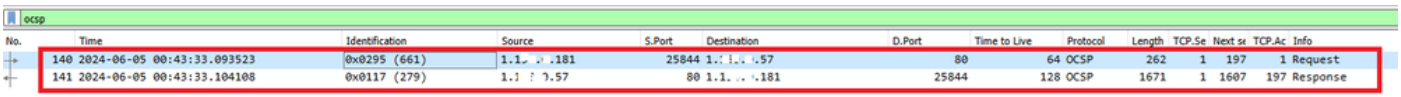
Code=5(AccountingResponse)

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

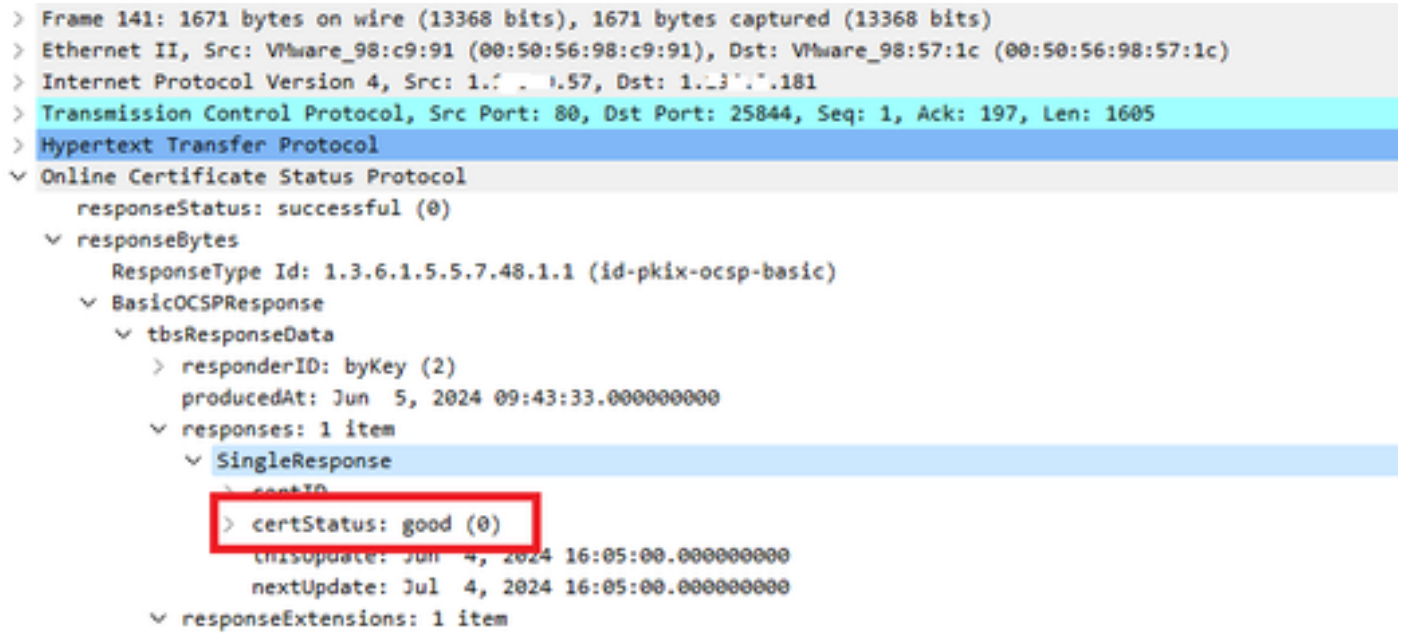
2. TCP轉儲

在ISE中的TCP轉儲中，您會發現有關OCSP響應和Radius會話的資訊。

OCSP請求和響應：

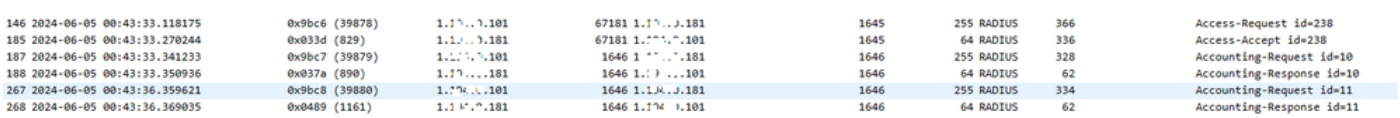


*OCSP*請求和響應的資料包捕獲



擷取*OCSP*回應的詳細資訊

Radius會話：



*Radius*會話的資料包捕獲

相關資訊

[配置使用ISE的EAP-TLS身份驗證]

[在ISE中配置TLS/SSL證書]

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。