تكوين مصادقة EAP-TLS باستخدام OCSP في ISE

المحتويات

المقدمة

يصف هذا المستند الخطوات المطلوبة لإعداد مصادقة EAP-TLS باستخدام OCSP للتحقق من إبطال شهادة العميل في الوقت الفعلي.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تكوين محرك خدمات الهوية من Cisco
- تكوين Cisco Catalyst
- بروتوكول حالة الشهادة عبر الإنترنت

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

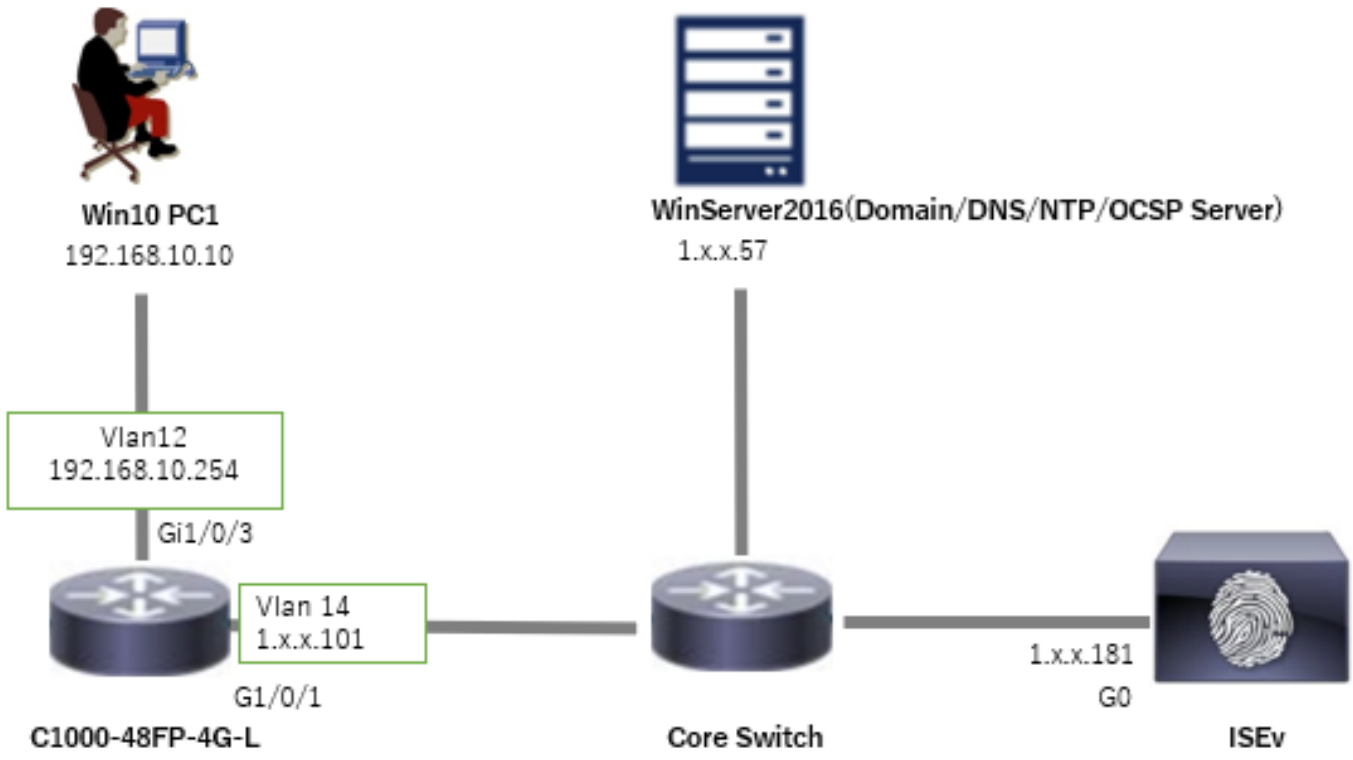
- البرنامج Identity Services Engine Virtual 3.2 Patch 6
- C1000-48FP-4G-L 15.2(7)E9

- نظام التشغيل Windows Server 2016
- نظام التشغيل Windows 10

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الرسم التخطيطي للشبكة

تعرض هذه الصورة المخطط الذي يتم إستخدامه لمثال هذا المستند.



الرسم التخطيطي للشبكة

معلومات أساسية

في EAP-TLS، يقدم العميل شهادته الرقمية إلى الخادم كجزء من عملية المصادقة. يوضح هذا المستند كيفية قيام ISE بالتحقق من صحة شهادة العميل عن طريق التحقق من صحة اسم الشهادة الشائع (CN) مقابل خادم AD وتأكيد ما إذا كان قد تم إبطال الشهادة باستخدام OCSP (بروتوكول حالة الشهادة عبر الإنترنت)، والذي يوفر حالة البروتوكول في الوقت الفعلي.

اسم المجال الذي تم تكوينه على Windows Server 2016 هو ad.rem-xxx.com، والذي يتم إستخدامه كمثال في هذا المستند.

يتم إستخدام خادم OCSP (بروتوكول حالة الشهادة على الإنترنت) و AD (Active Directory) المشار إليهما في هذا المستند للتحقق من الشهادة.

- Active Directory FQDN: winserver.ad.rem-xxx.com
- عنوان URL الخاص بتوزيع CRL: http://winserver.ad.rem-xxx.com/ocsp-ca.crl
- عنوان URL للمرجع: http://winserver.ad.rem-xxx.com/ocsp

هذه هي سلسلة الشهادات التي لها الاسم الشائع لكل شهادة مستخدمة في المستند.

- أ ك: OCSP-CA-الاسم الشائع
- شهادة العميل: clientcertCN
- شهادة الخادم: ise32-01.ad.rem-xxx.com
- شهادة توقيع OCSP: ocspSignCommonName

التكوينات

التكوين في C1000

هذا هو الحد الأدنى للتكوين في 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
```

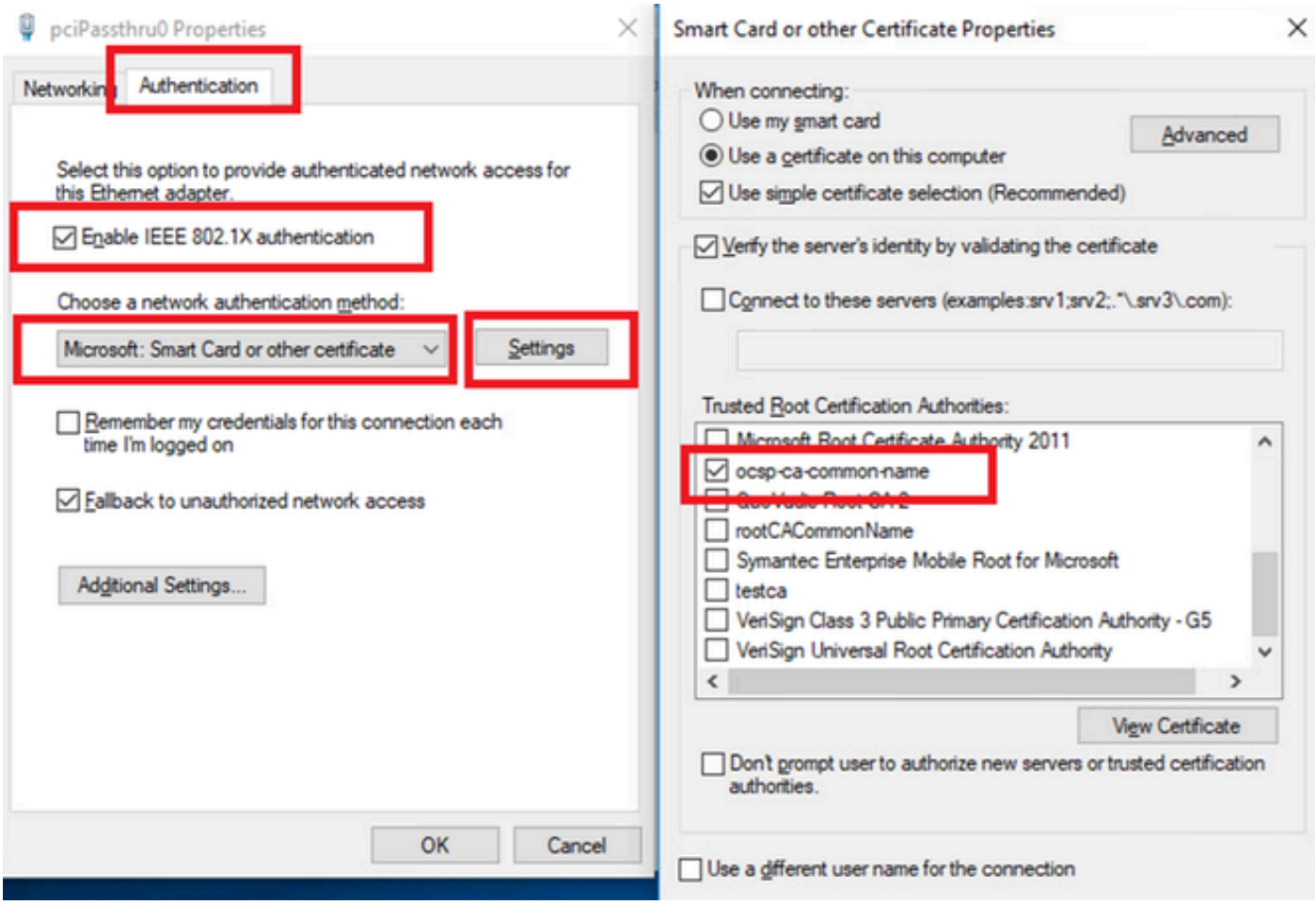
```
interface GigabitEthernet1/0/1
Switch port access vlan 14
Switch port mode access

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
```

التكوين في كمبيوتر Windows

الخطوة 1. تكوين مصادقة المستخدم

انتقل إلى المصادقة، تحقق من تمكين مصادقة IEEE 802.1X وحدد Microsoft: البطاقة الذكية أو شهادة أخرى.

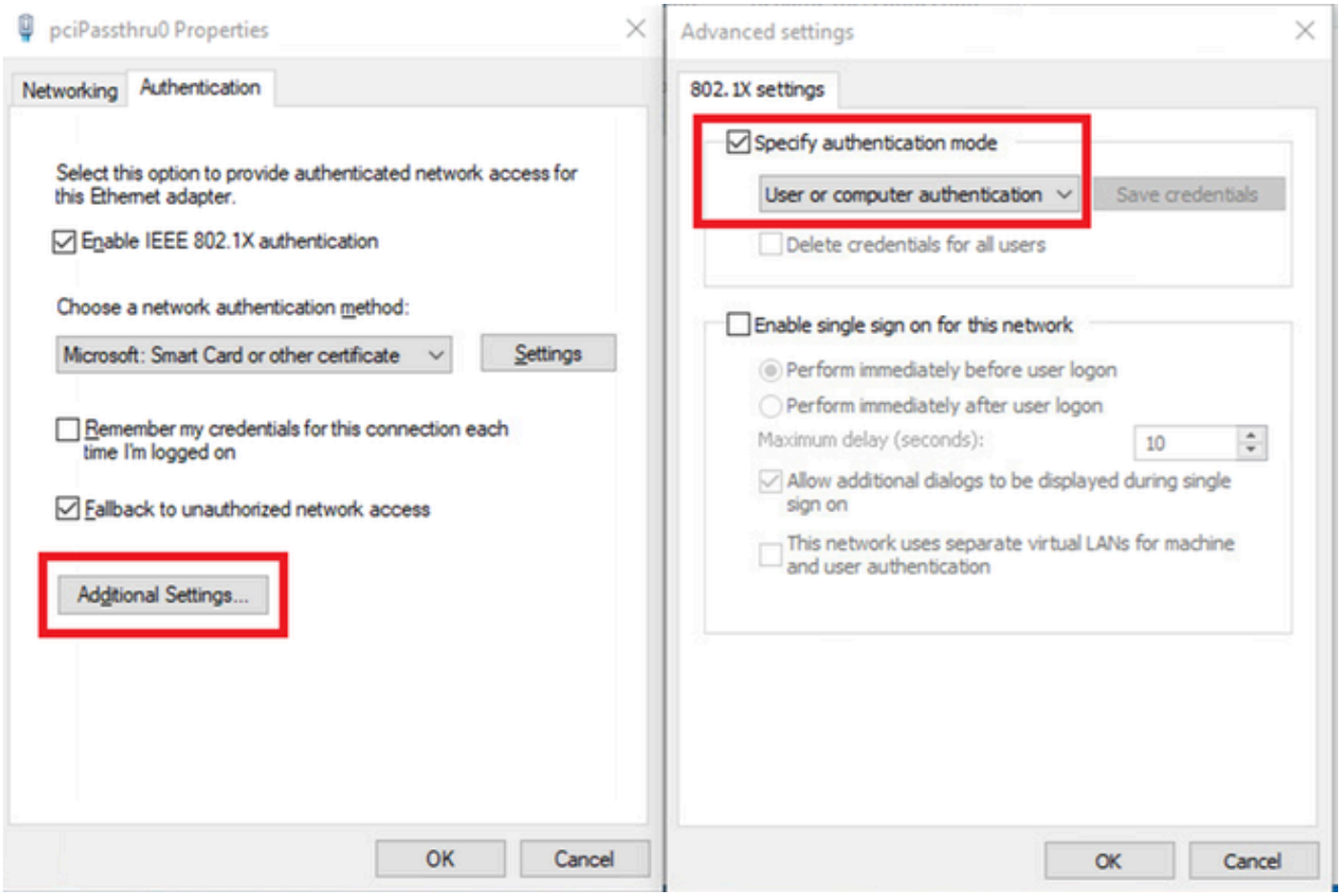
انقر فوق Settingsbutton، ثم حدد إستخدام شهادة على هذا الكمبيوتر، ثم حدد المرجع المصدق الموثوق به لجهاز كمبيوتر Windows.



تمكين مصادقة الشهادة

انتقل إلى المصادقة، تحقق من الإعدادات الإضافية. مصادقة المستخدم أو الكمبيوتر من

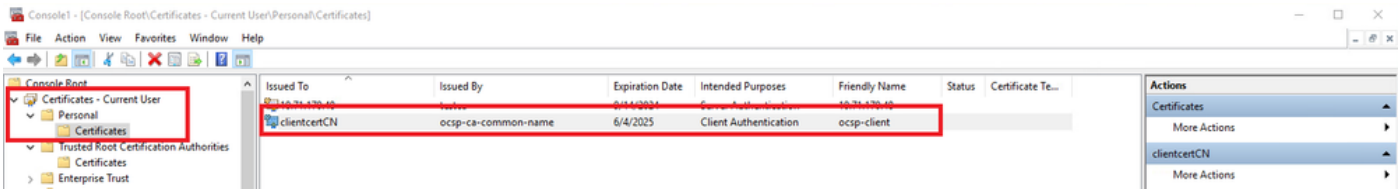
القائمة المنسدلة.



تحديد وضع المصادقة

الخطوة 2. تأكيد شهادة العميل

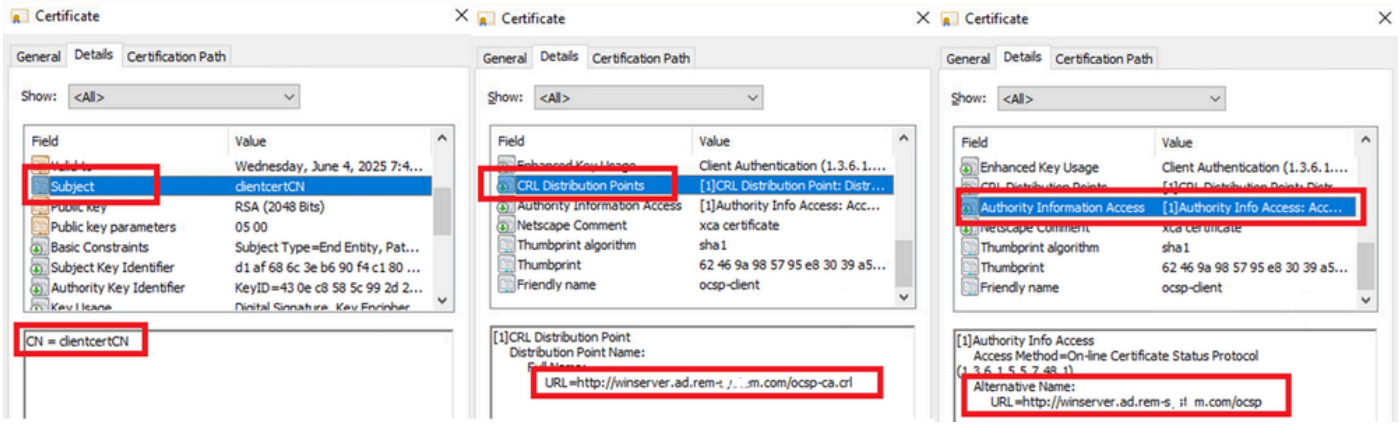
انتقل إلى الشهادات - المستخدم الحالي > شخصي > شهادات، وفحص شهادة العميل المستخدمة للمصادقة.



تأكيد شهادة العميل

انقر نقرا مزدوجا فوق شهادة العميل، وانتقل إلى التفاصيل، ثم تحقق من تفاصيل الموضوع، نقاط توزيع CRL، والوصول إلى معلومات المرجع.

- الموضوع: CN = clientcertCN
- نقاط توزيع CRL: http://winserver.ad.rem-xxx.com/ocsp-ca.crl
- الوصول إلى معلومات السلطة: http://winserver.ad.rem-xxx.com/ocsp

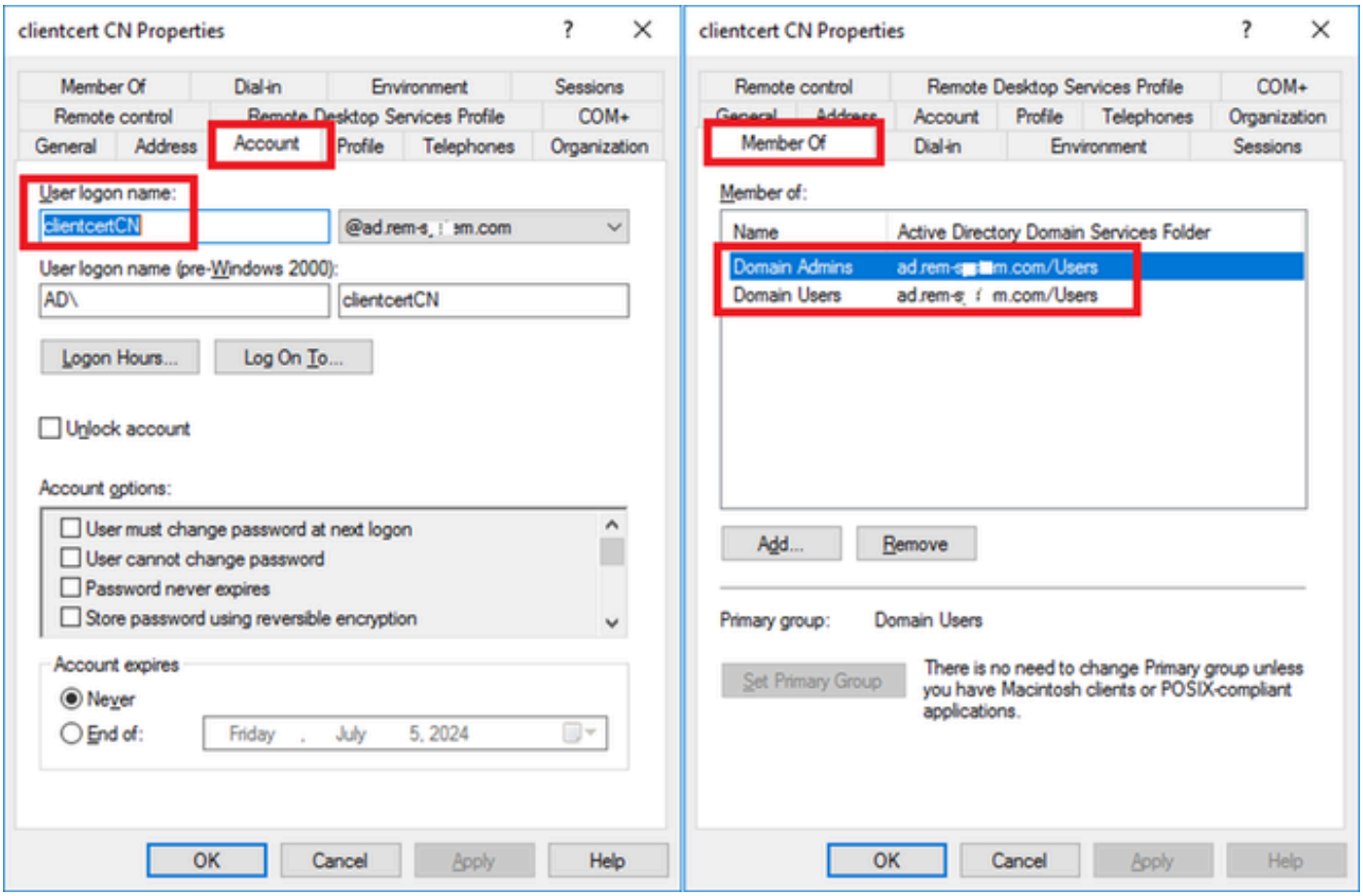


تفاصيل شهادة العميل

التكوين في خادم Windows

الخطوة 1. إضافة مستخدمين

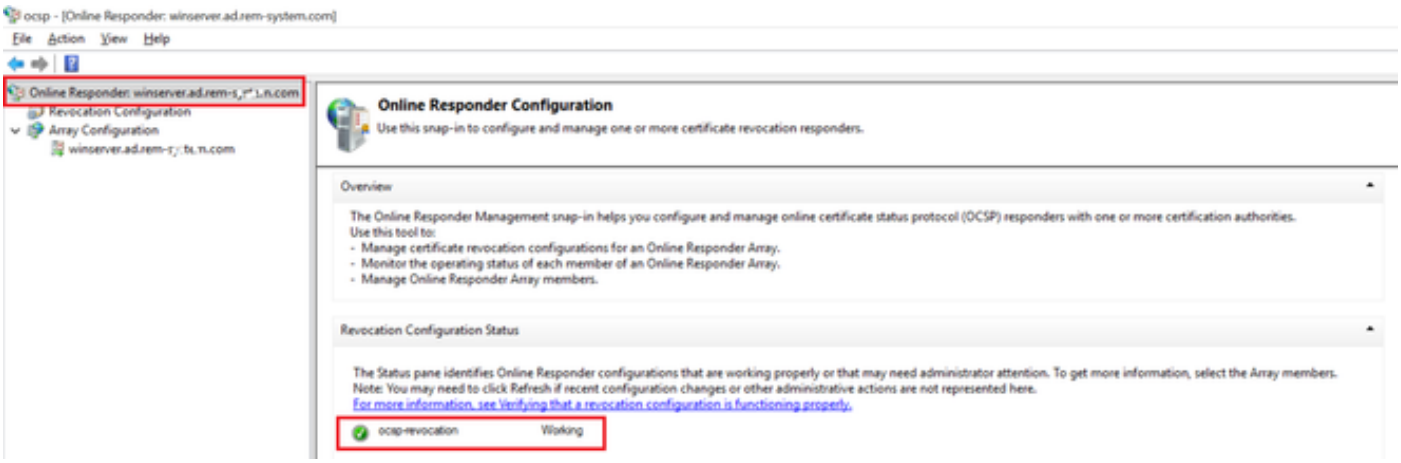
انتقل إلى Active Directory Users and Computers، انقر فوق Users. إضافة clientCERTcn كاسم تسجيل دخول المستخدم.



اسم تسجيل دخول المستخدم

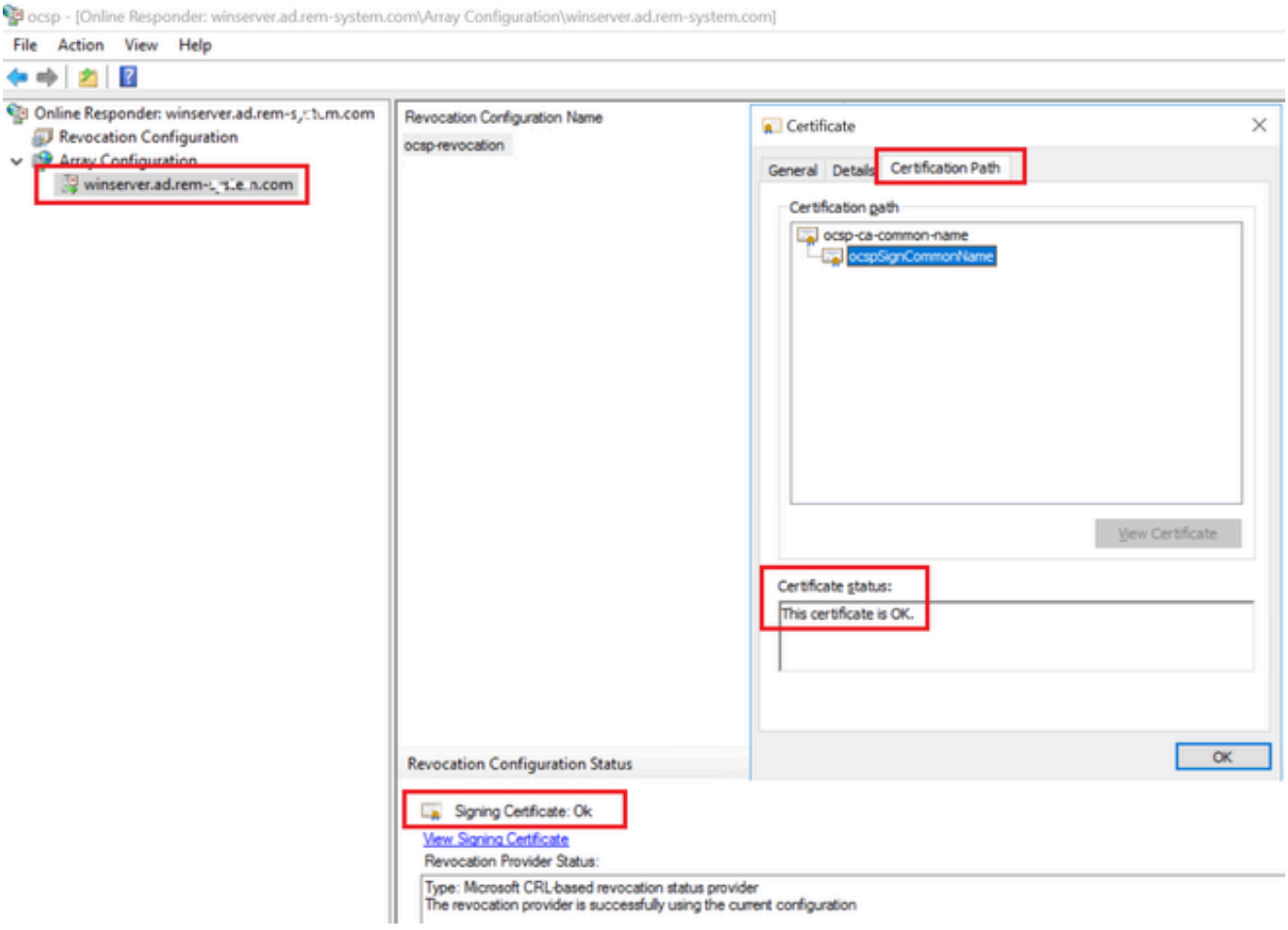
الخطوة 2. تأكيد خدمة OCSP

انتقل إلى Windows، وانقر فوق إدارة المستجيب عبر الإنترنت. تأكيد حالة خادم OCSP.



حالة خادم OCSP

انقر winserver.ad.rem-xxx.com، تحقق من حالة شهادة توقيع OCSP.

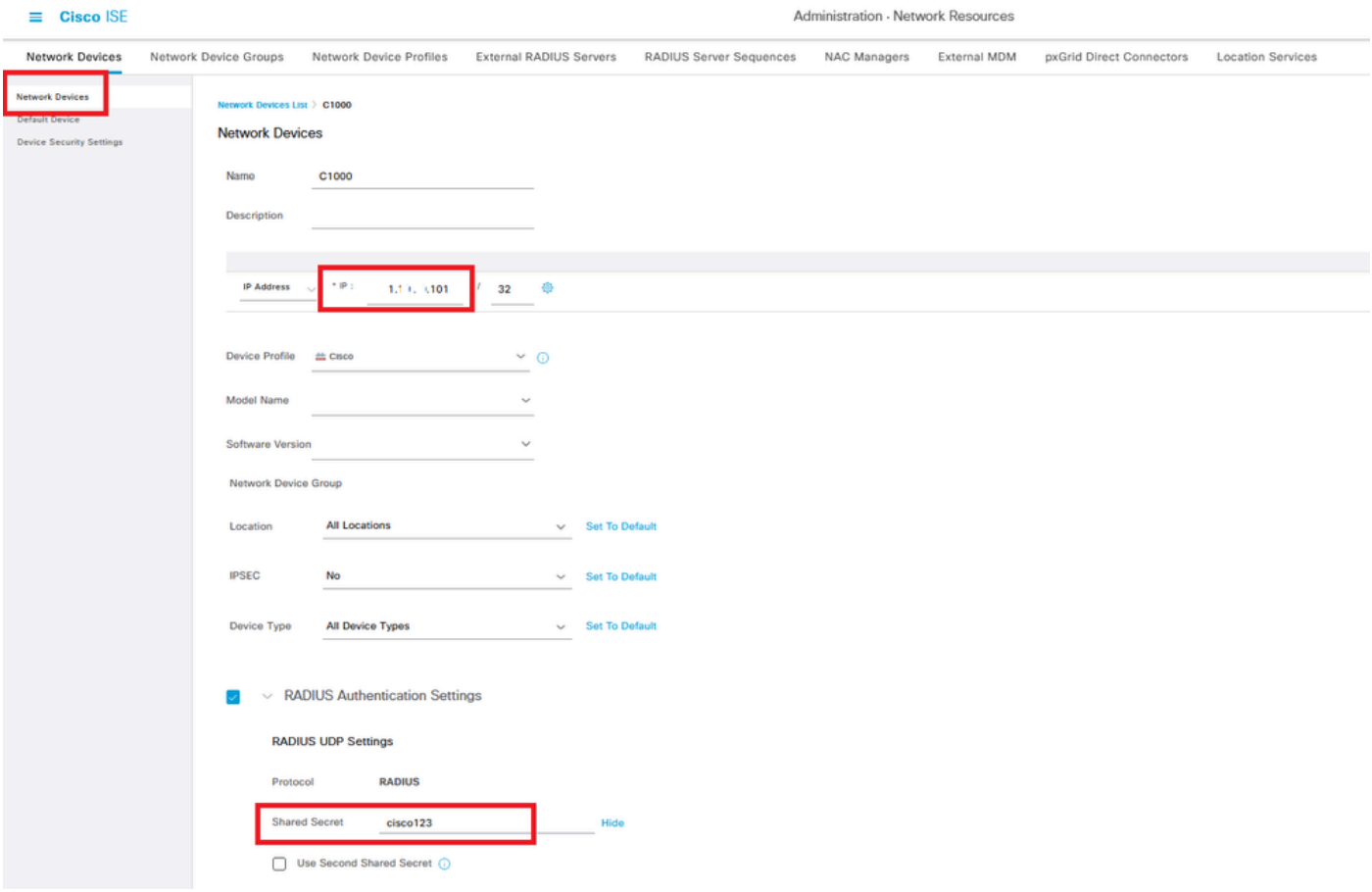


حالة شهادة توقيع OCSP

التكوين في ISE

الخطوة 1. إضافة جهاز

انتقل إلى الإدارة > أجهزة الشبكة، انقر فوق إضافة زر لإضافة جهاز C1000.

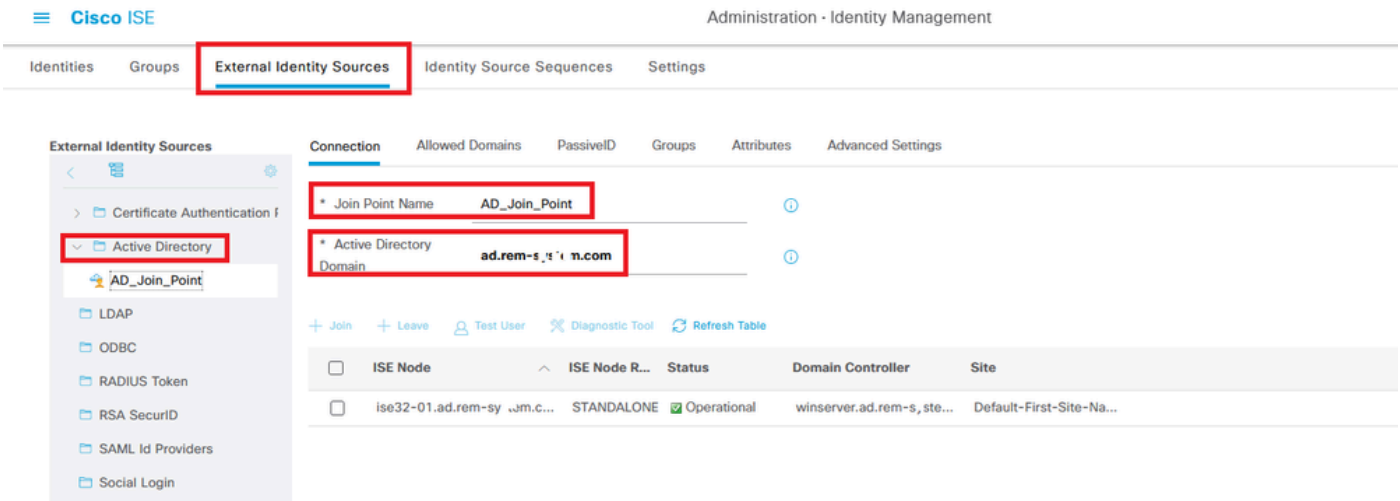


إضافة جهاز

الخطوة 2. إضافة Active Directory

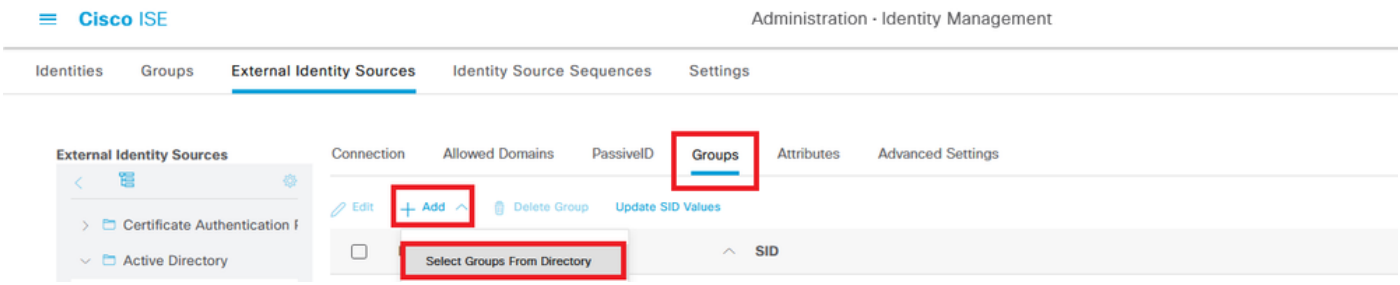
انتقل إلى Administration > مصادر الهوية الخارجية > Active Directory، انقر فوق ConnectTab، وقم بإضافة Active Directory إلى ISE.

- اسم نقطة الربط: AD_JOIN_POINT
- مجال خدمة Active Directory: ad.rem-xxx.com



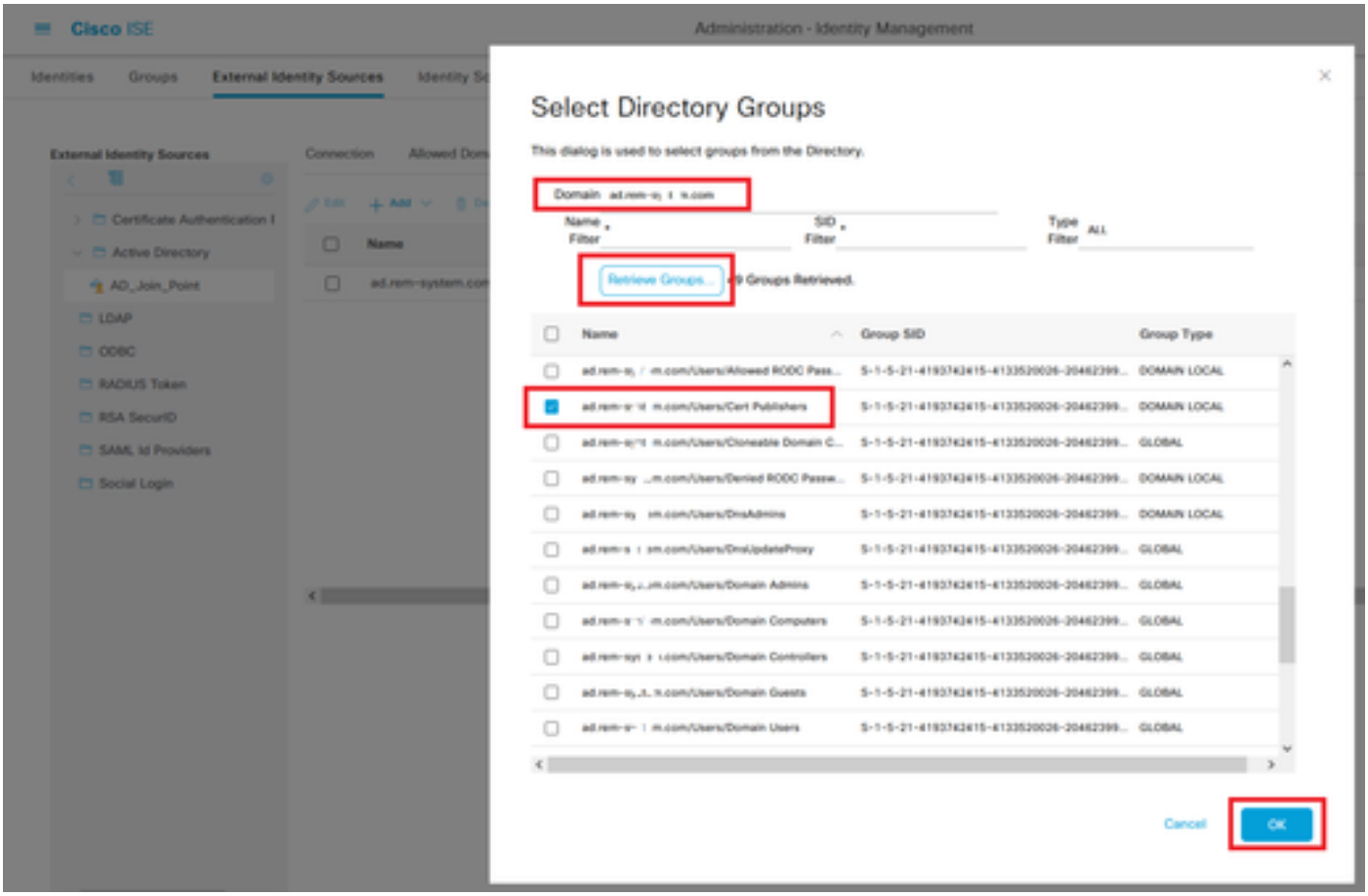
إضافة Active Directory

انتقل إلى علامة التبويب مجموعات، حدد مجموعات من القائمة المنسدلة DirectFrom.



تحديد مجموعات من الدليل

انقر فوق إستيراد المجموعات من القائمة المنسدلة. Checkad.rem-xxx.com/Users/Cert النارين وانقر فوق موافق.

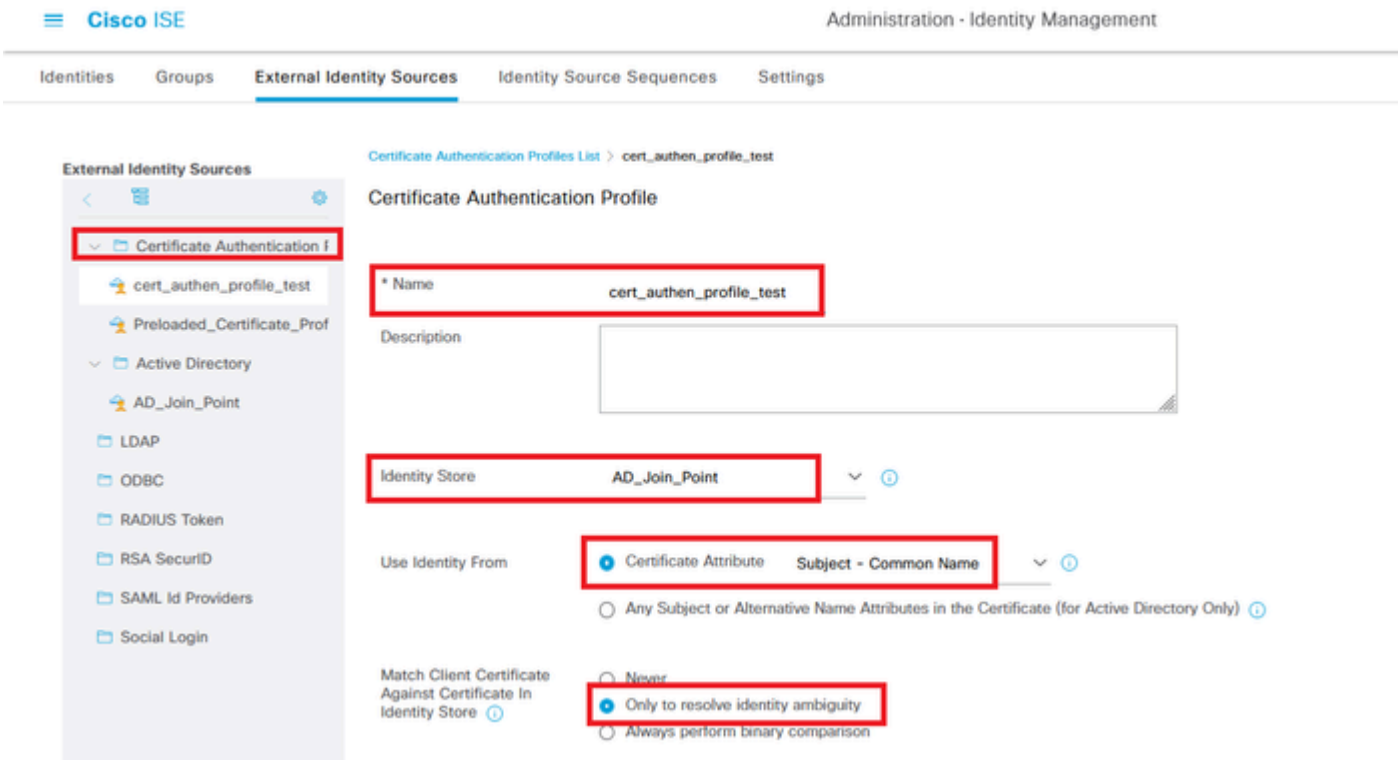


التحقق من ناشري CERT

الخطوة 3. إضافة ملف تعريف مصادقة الشهادة

انتقل إلى إدارة > مصادر هوية خارجية > ملف تعريف مصادقة الشهادة، انقر على إضافة زر لإضافة ملف تعريف مصادقة شهادة جديد.

- الاسم: cert_authen_profile_test
- Identity Store: AD_JOIN_POINT
- أستخدم الهوية من سمة الشهادة: الموضوع - الاسم الشائع.
- مطابقة شهادة العميل مقابل الشهادة في مخزن الهويات: فقط لحل غموض الهوية.

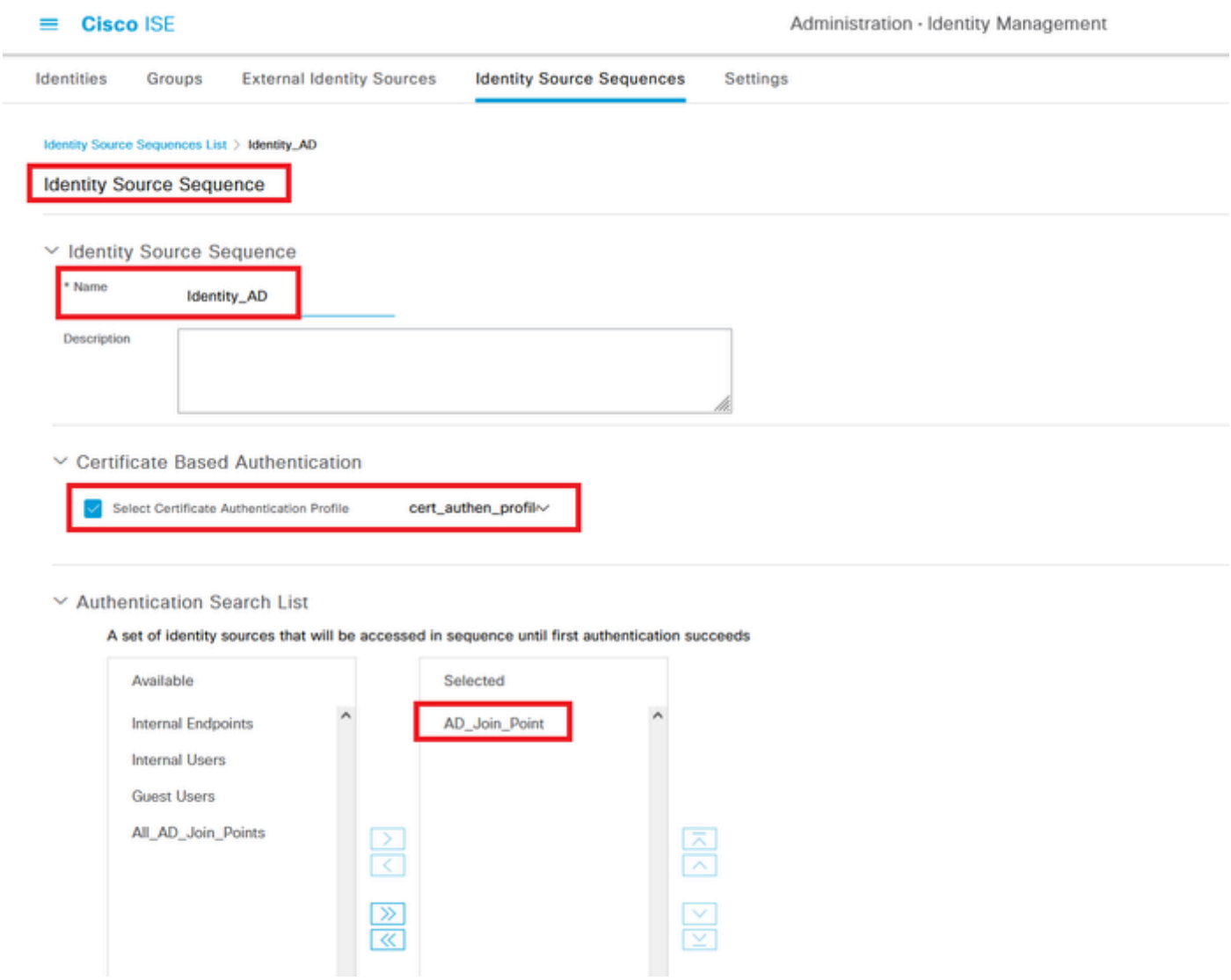


إضافة ملف تعريف مصادقة الشهادة

الخطوة 4. إضافة سلسلة مصدر الهوية

انتقل إلى إدارة > تسلسلات مصدر الهوية، وقم بإضافة تسلسل مصدر هوية.

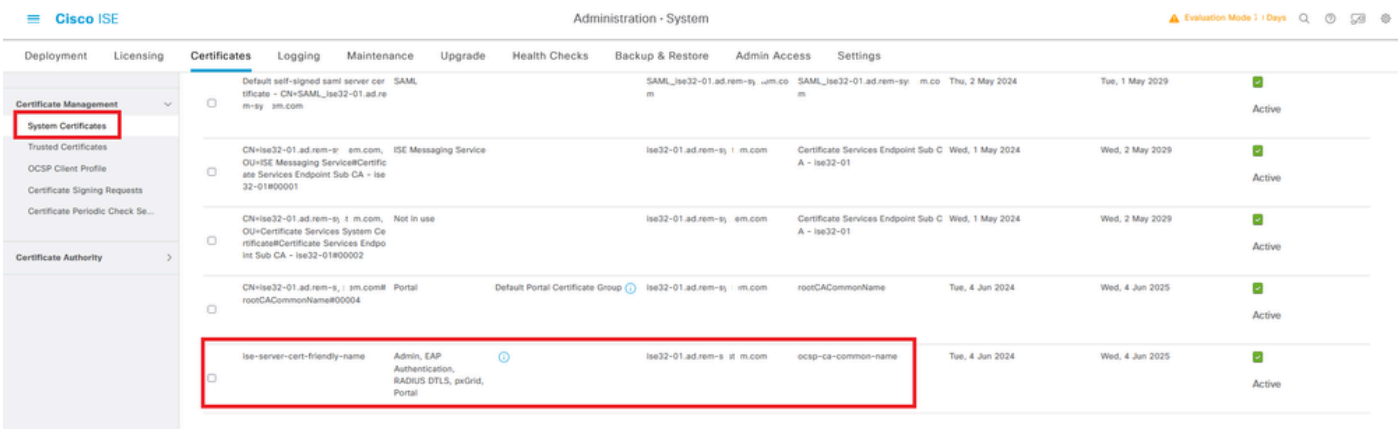
- الاسم: Identity_AD
- حدد مصادقة الشهادة Profile: cert_authen_profile_test
- قائمة البحث عن المصادقة: AD_JOIN_POINT



إضافة تسلسلات مصدر الهوية

الخطوة 5. شهادة Confrim في ISE

انتقل إلى إدارة > شهادات > شهادات النظام، تأكد من توقيع شهادة الخادم من قبل المرجع المصدق الثقة.

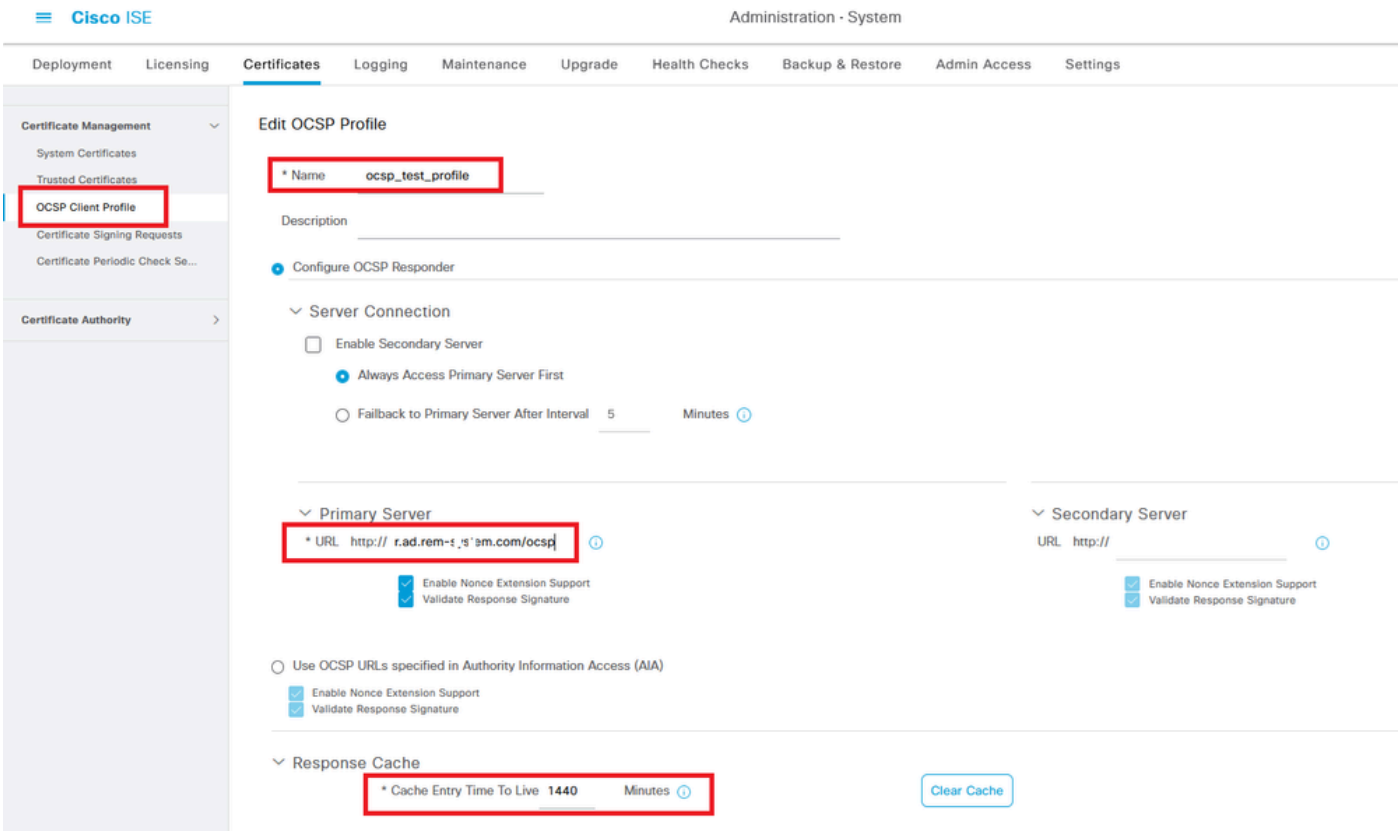


شهادة الخادم

انتقل إلى إدارة > شهادات > ملف تعريف عميل OCSP، انقر فوق زر إضافة لإضافة ملف

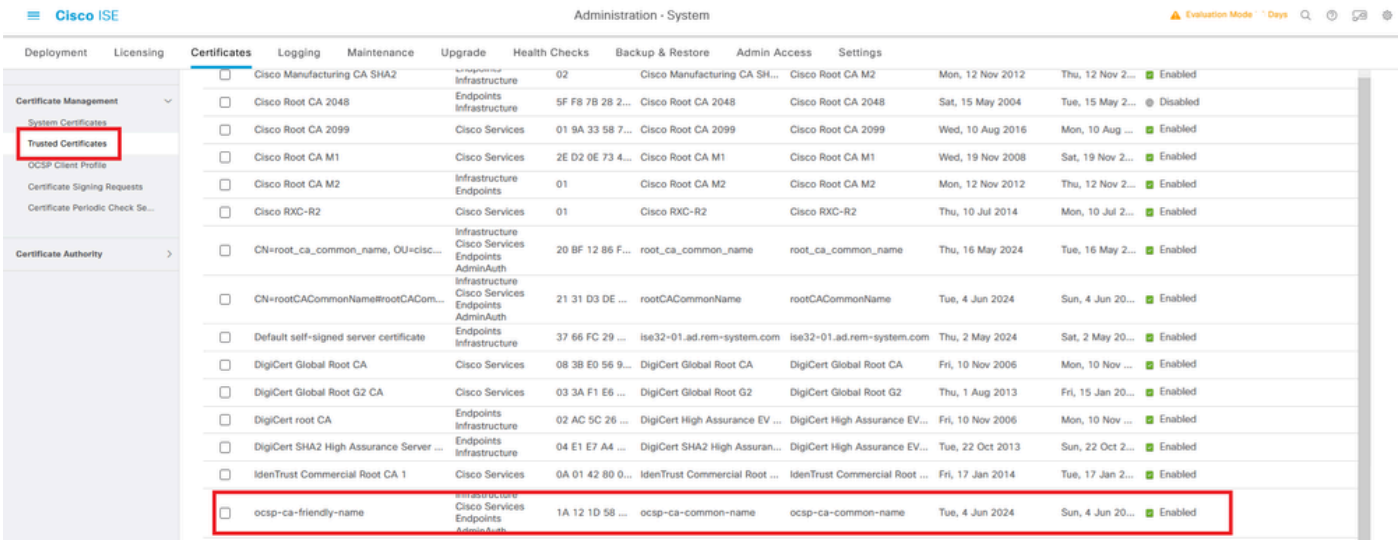
تعريف عميل OCSP جديد.

- الاسم: ocsp_test_profile
- تكوين عنوان URL لمستجيب OCSP: http://winserver.ad.rem-xxx.com/ocsp



ملف تعريف عميل OCSP

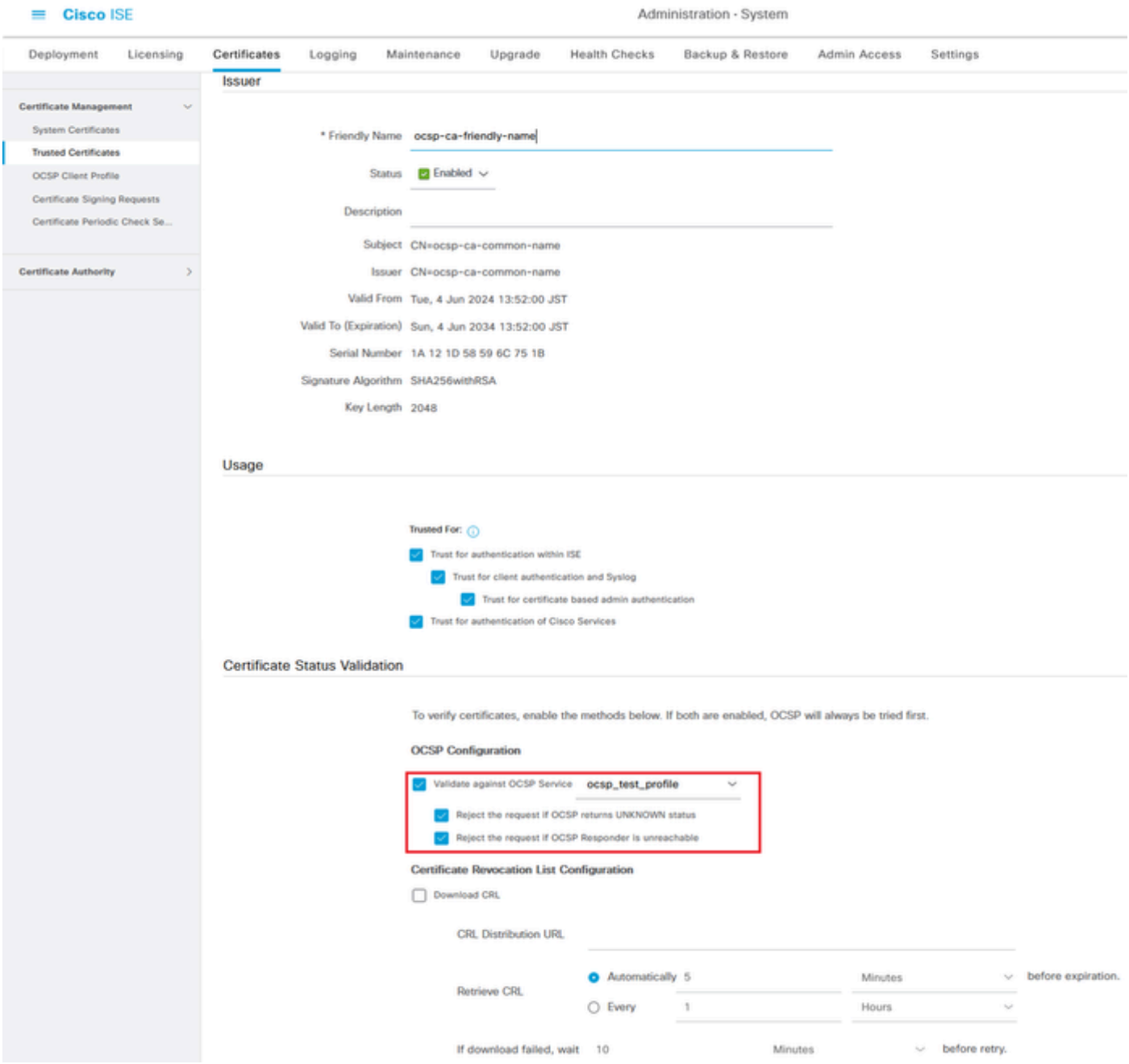
انتقل إلى إدارة > شهادات > شهادات موثوق بها، تأكد من أن CA موثوق به تم إستيراده إلى ISE.



مرجع مصدق ثقة

تحقق من المرجع المصدق وانقر فوق زر تحرير، وأدخل تفاصيل تكوين OCSP للتحقق من حالة الشهادة.

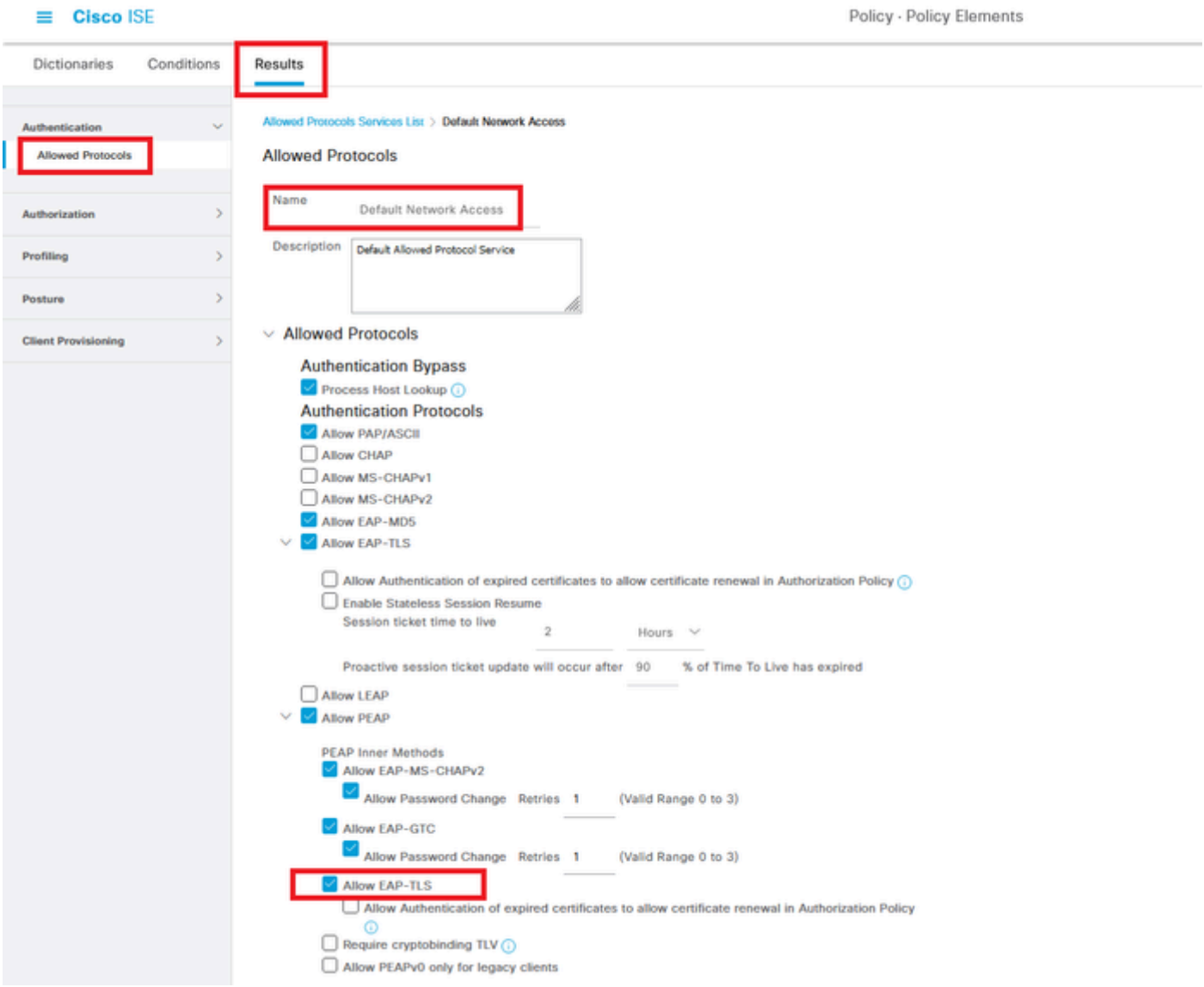
- التحقق من الصحة مقابل خدمة OCSP: ocsp_test_profile
- رفض الطلب إذا قام OCSP بإرجاع حالة غير معروفة: تحقق
- رفض الطلب إذا كان مستجيب OCSP غير قابل للوصول: تحقق



التحقق من حالة الشهادة

الخطوة 6. إضافة البروتوكولات المسموح بها

انتقل إلى سياسة > نتائج > مصادقة > بروتوكولات مسموح بها، وحرر قائمة خدمة الوصول إلى الشبكة الافتراضية، ثم حدد السماح ب EAP-TLS.

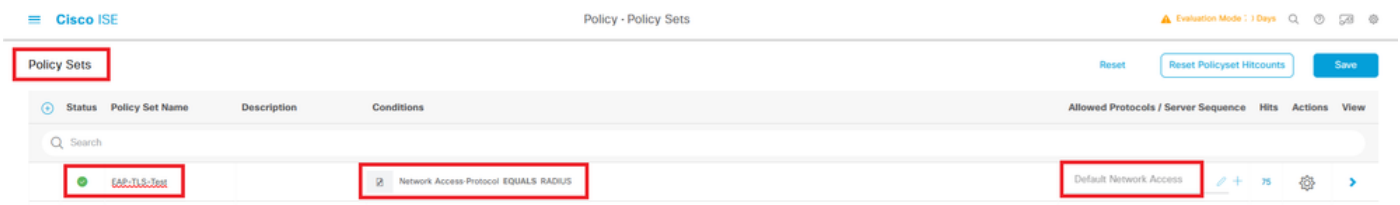


السماح ب EAP-TLS

الخطوة 7. إضافة مجموعة نهج

انتقل إلى نهج > مجموعات نهج، انقر فوق + لإضافة مجموعة نهج.

- اسم مجموعة النهج: EAP-TLS-Test
- الشروط: بروتوكول الوصول إلى الشبكة يساوي RADIUS
- البروتوكولات المسموح بها / تسلسل الخادم: الوصول الافتراضي إلى الشبكة



إضافة مجموعة نهج

الخطوة 8. إضافة نهج المصادقة

انتقل إلى مجموعات النهج، انقر على EAP-TLS-Testلإضافة سياسة مصادقة.

- اسم القاعدة: مصادقة EAP-TLS
- الشروط: تساوي مصادقة EAP للوصول إلى الشبكة EAP-TLS وWIRED_802.1 X
- الاستخدام: Identity_AD

إضافة نهج المصادقة

الخطوة 9. إضافة نهج التخويل

انتقل إلى مجموعات النهج، وانقر فوق EAP-TLS-Test لإضافة نهج تخويل.

- اسم القاعدة: تفويض EAP-TLS
- الشروط: موضوع الشهادة - الاسم الشائع يساوي clientCN
- النتائج: PermitAccess

إضافة نهج التخويل

التحقق من الصحة

الخطوة 1. تأكيد جلسة عمل المصادقة

قم بتشغيلshow authentication sessions interface GigabitEthernet1/0/3 details الأمر لتأكيد جلسة عمل المصادقة في C1000.

<#root>

Switch#

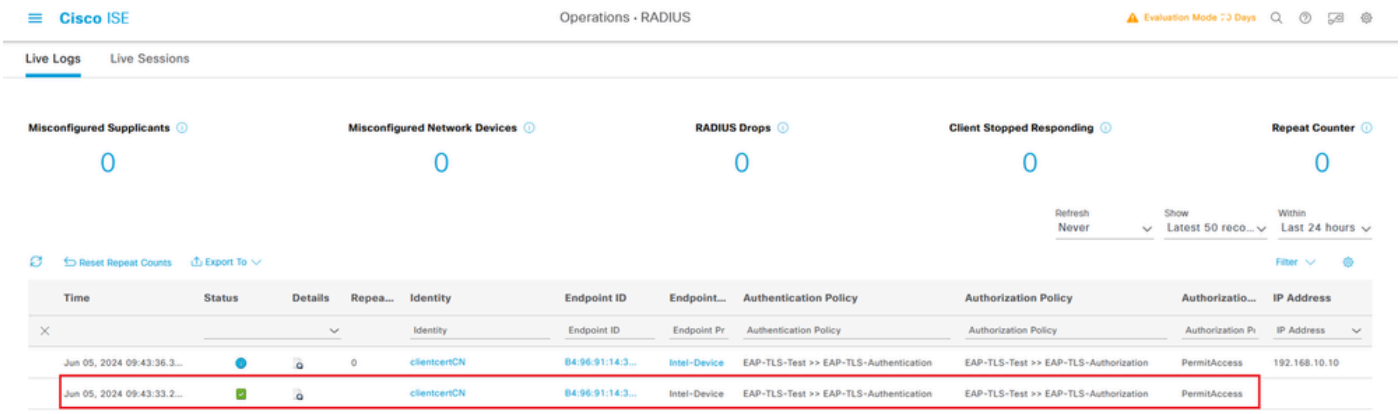
show authentication sessions interface GigabitEthernet1/0/3 details

```
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: 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
```

الخطوة 2. تأكيد سجل Radius Live

انتقل إلى العمليات > **RADIUS** > تسجيل الدخول المباشر في واجهة المستخدم الرسومية (GUI) ل ISE، قم بتأكيد السجل النشط للمصادقة.



سجل Radius Live

قم بتأكيد سجل المصادقة المباشر المفصل.

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

تفاصيل المصادقة

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
```

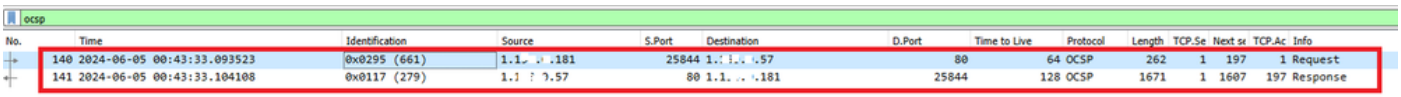
Code=4(AccountingRequest)

```
 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
```

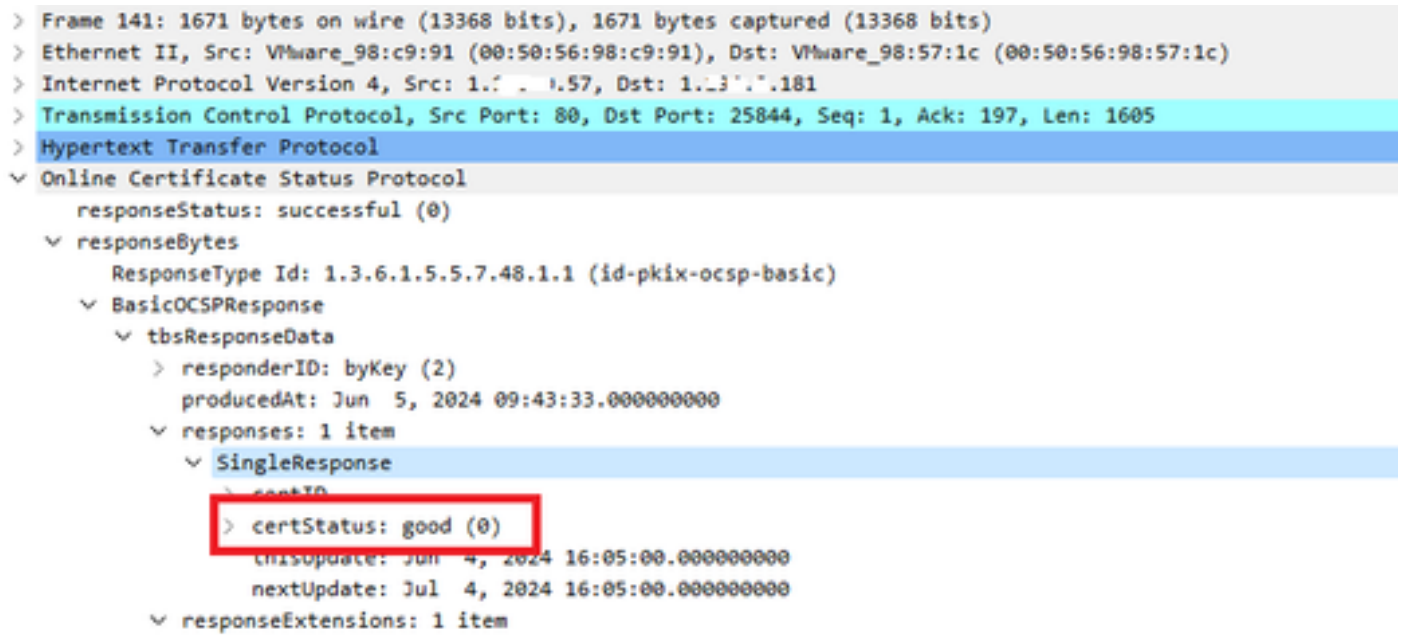
2. تفريغ TCP

في عملية تفريغ TCP في ISE، تتوقع العثور على معلومات حول إستجابة OCSP وجلسة عمل RADIUS.

طلب OCSP والرد عليه :

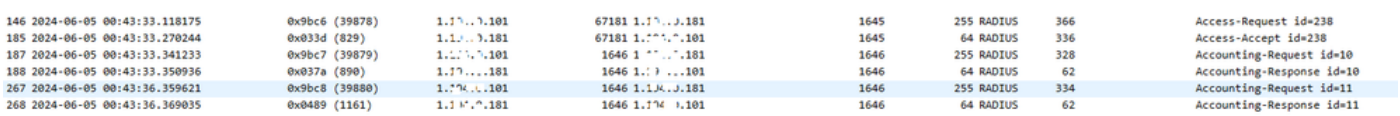


التقاط حزمة طلب *OCSP* والاستجابة



تفاصيل التقاط إستجابة *OCSP*

جلسة عمل RADIUS :



التقاط حزمة من جلسة *RADIUS*

معلومات ذات صلة

[تكوين مصادقة EAP-TLS باستخدام ISE](#)

[تكوين شهادات TLS/SSL في ISE](#)

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).