Configurazione dell'autenticazione EAP-TLS con OCSP in ISE

Sommario

Introduzione

In questo documento viene descritto come configurare l'autenticazione EAP-TLS con OCSP per i controlli in tempo reale delle revoche di certificati dei client.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione di Cisco Identity Services Engine
- Configurazione di Cisco Catalyst
- Protocollo di stato del certificato in linea

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

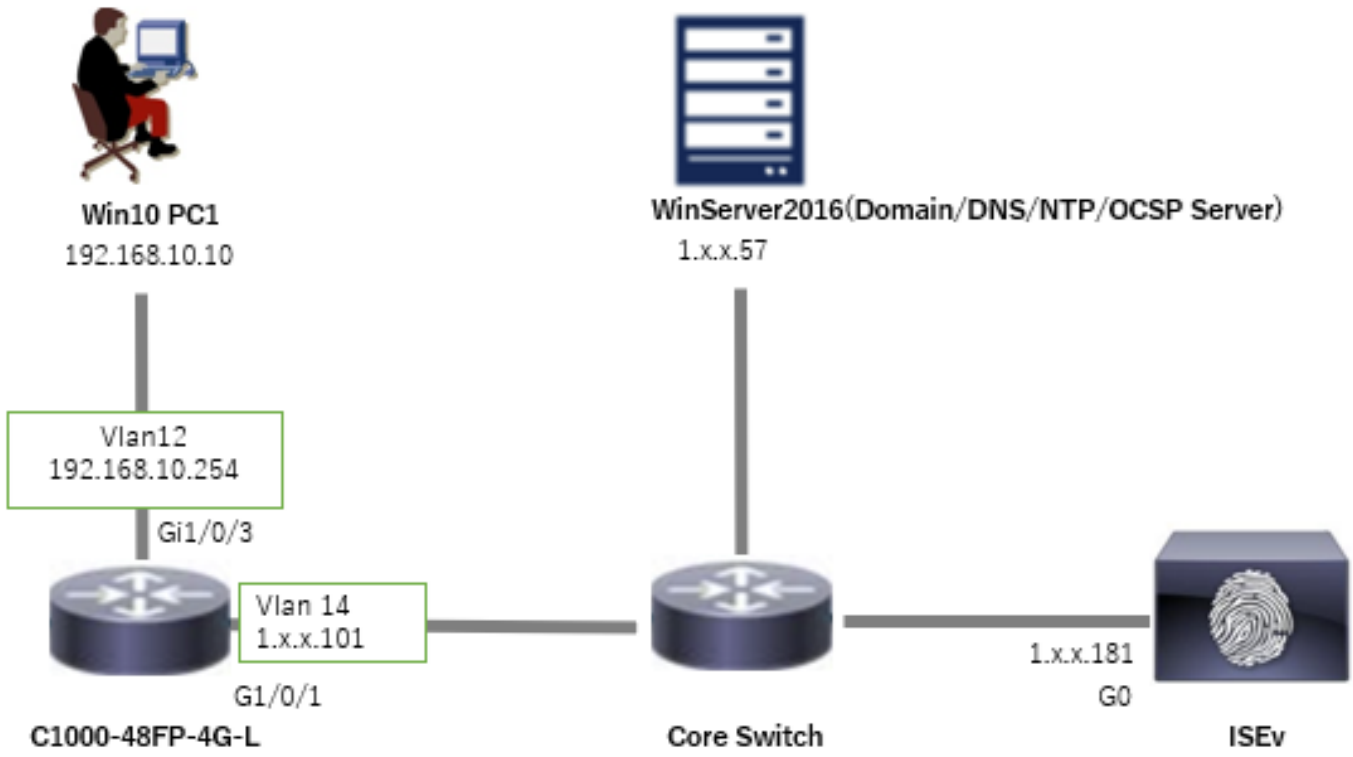
- Patch 6 Identity Services Engine Virtual 3.2
- C1000-48FP-4G-L 15.2(7)E9

- Windows Server 2016
- Windows 10

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Esempio di rete

Nell'immagine è illustrata la topologia utilizzata per l'esempio del documento.



Premesse

In EAP-TLS, un client presenta il proprio certificato digitale al server come parte del processo di autenticazione. In questo documento viene descritto come ISE convalida il certificato client verificando il nome comune del certificato (CN) sul server AD e confermando se il certificato è stato revocato utilizzando OCSP (Online Certificate Status Protocol), che fornisce lo stato del protocollo in tempo reale.

Il nome di dominio configurato in Windows Server 2016 è ad.rem-xxx.com, utilizzato come esempio in questo documento.

Per la convalida del certificato vengono utilizzati i server OCSP (Online Certificate Status Protocol) e AD (Active Directory) a cui si fa riferimento in questo documento.

- FQDN di Active Directory: winserver.ad.rem-xxx.com
- URL di distribuzione CRL: http://winserver.ad.rem-xxx.com/ocsp-ca.crl
- URL autorità: http://winserver.ad.rem-xxx.com/ocsp

Catena di certificati con il nome comune di ogni certificato utilizzato nel documento.

- CA: nome-comune-ocsp-ca
- Certificato client: clientcertCN
- Certificato server: ise32-01.ad.rem-xxx.com
- Certificato di firma OCSP: ocspSignCommonName

Configurazioni

Configurazione in C1000

Questa è la configurazione minima nella CLI di C1000.

```
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
```

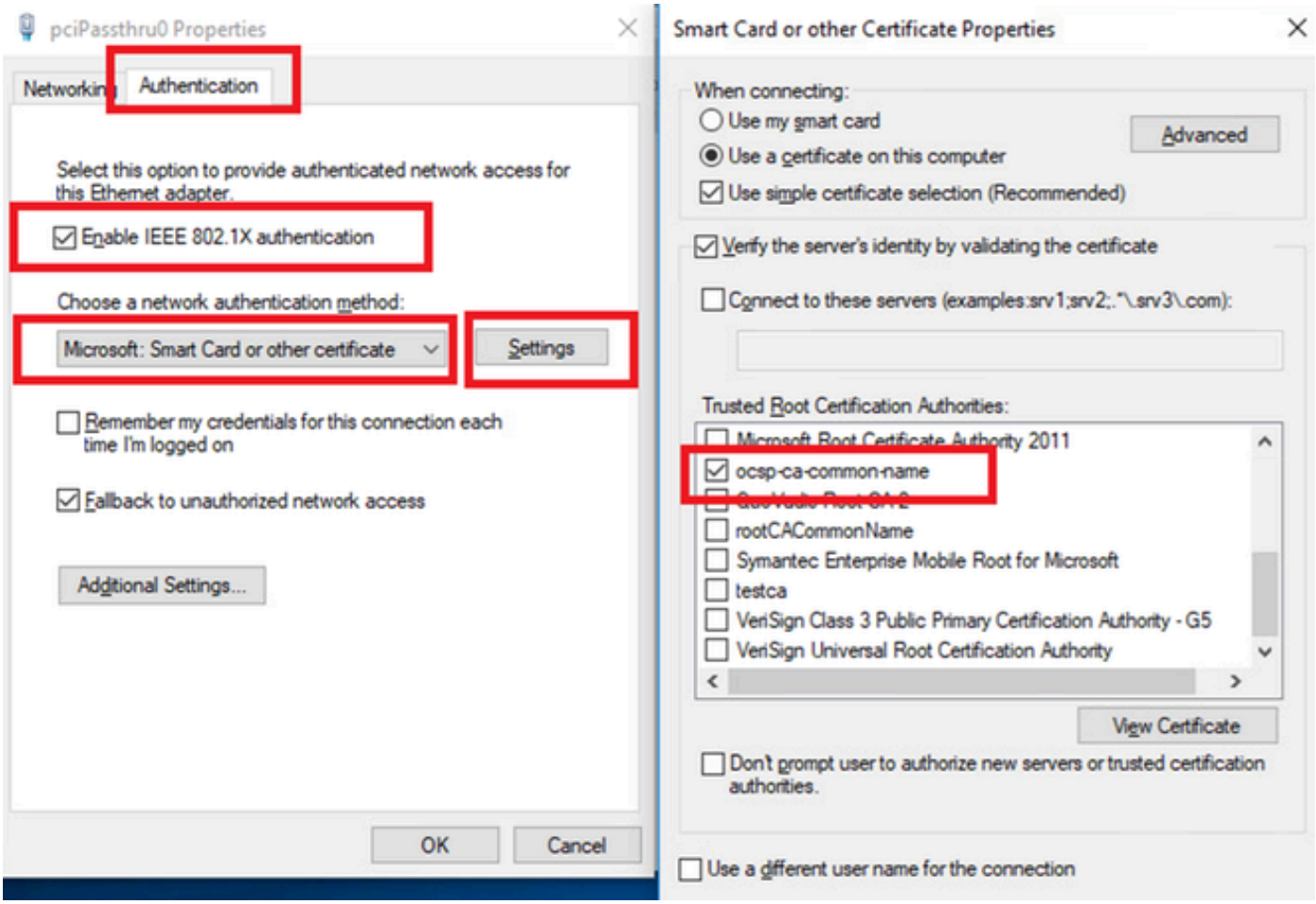
```
interface Vlan14
ip address 1.x.x.101 255.0.0.0

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
```

Configurazione in un PC Windows

Passaggio 1. Configura autenticazione utente

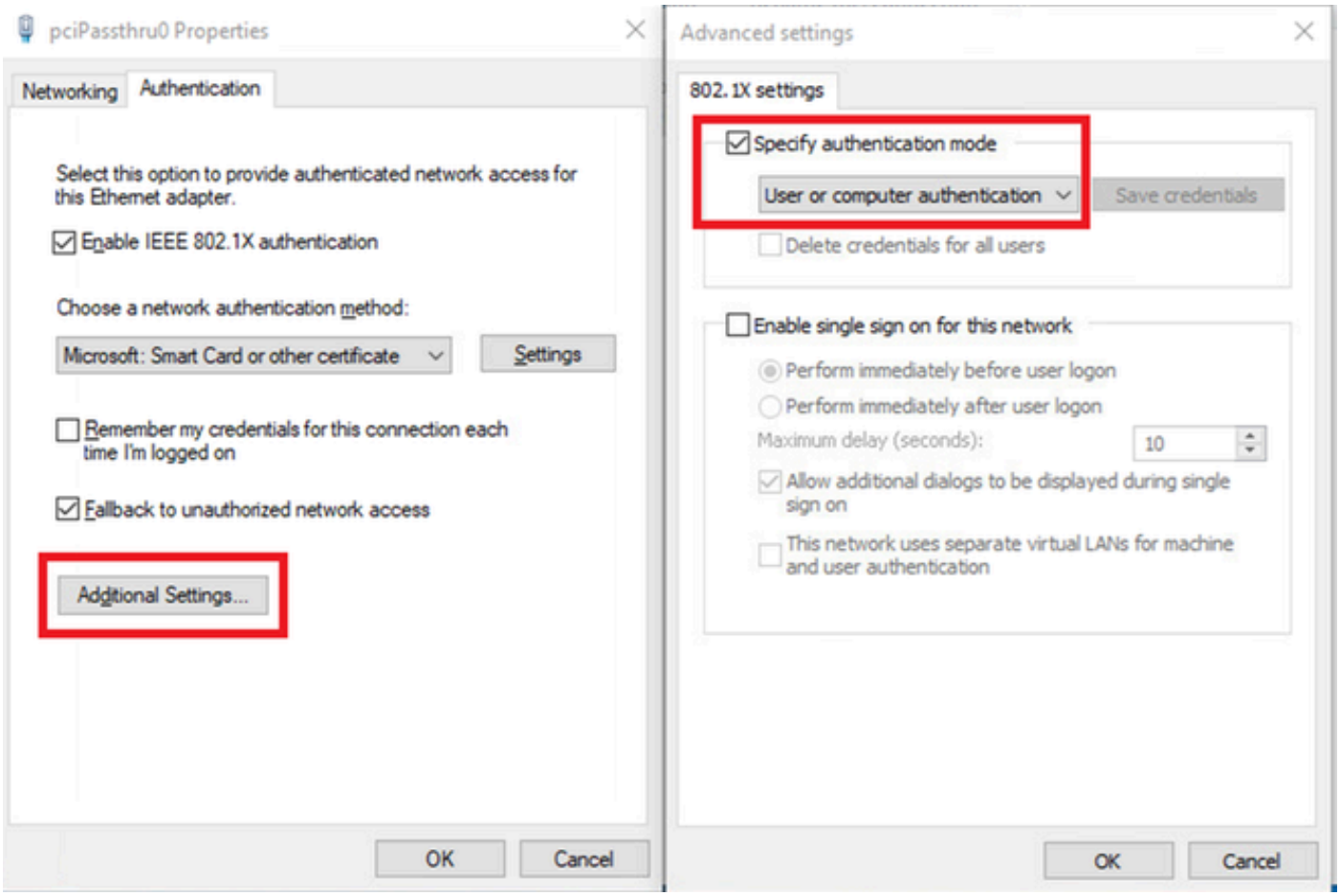
Passare a Autenticazione, selezionare Abilita autenticazione IEEE 802.1X e selezionare Microsoft: Smart Card o altro certificato.

Fare clic su ImpostazioniPulsante, selezionare Utilizza un certificato in questo computer, quindi selezionare l'autorità di certificazione attendibile del PC Windows.



Abilita autenticazione certificato

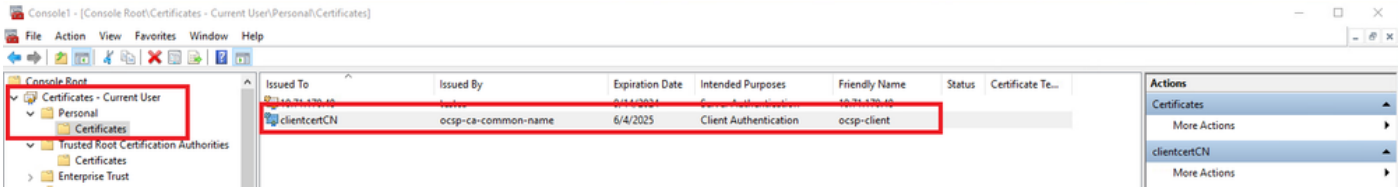
Passare a Autenticazione, selezionare Impostazioni aggiuntive. Selezionare Autenticazione utente o computer dall'elenco a discesa.



Specifica modalità di autenticazione

Passaggio 2. Conferma certificato client

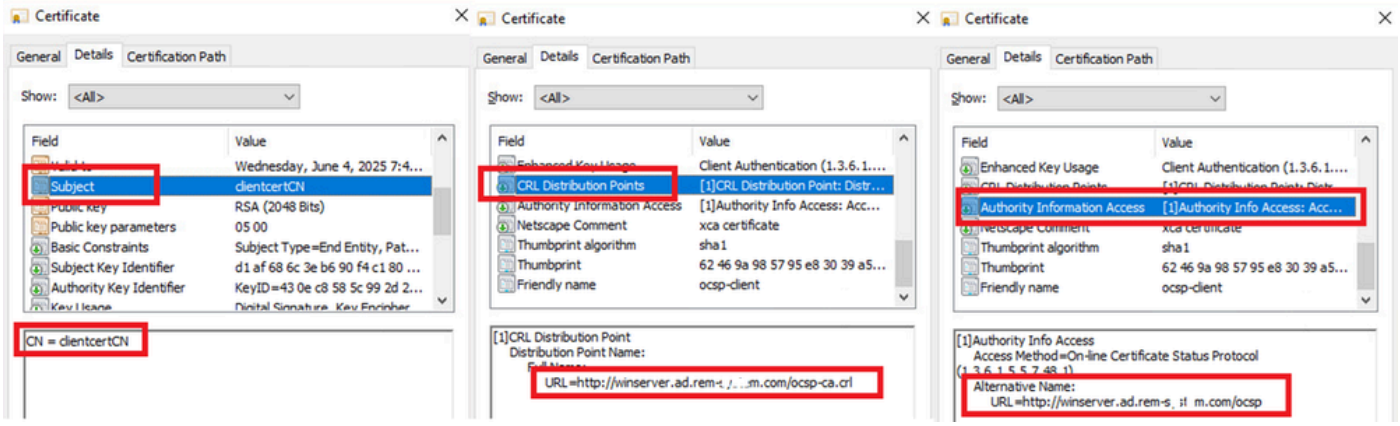
Passare a Certificati - Utente corrente > Personale > Certificati e verificare il certificato client utilizzato per l'autenticazione.



Conferma certificato client

Fare doppio clic sul certificato client, passare a Dettagli, controllare i dettagli di Oggetto, Punti di distribuzione CRL, Accesso alle informazioni dell'autorità.

- Oggetto: CN = clientCN
- Punti di distribuzione CRL: http://winserver.ad.rem-xxx.com/ocsp-ca.crl
- Accesso alle informazioni dell'autorità: http://winserver.ad.rem-xxx.com/ocsp

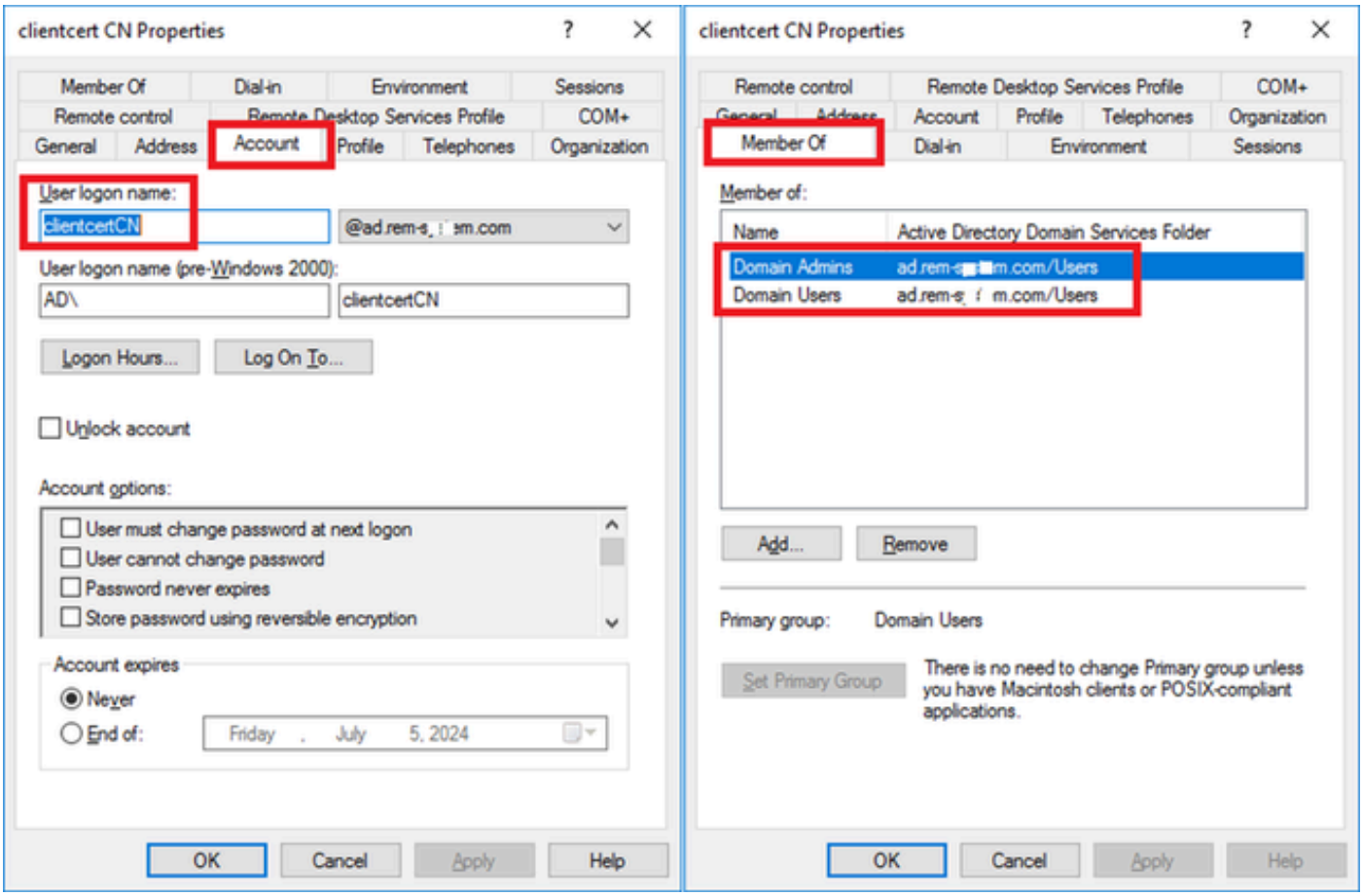


Dettagli del certificato client

Configurazione in Windows Server

Passaggio 1. Aggiungi utenti

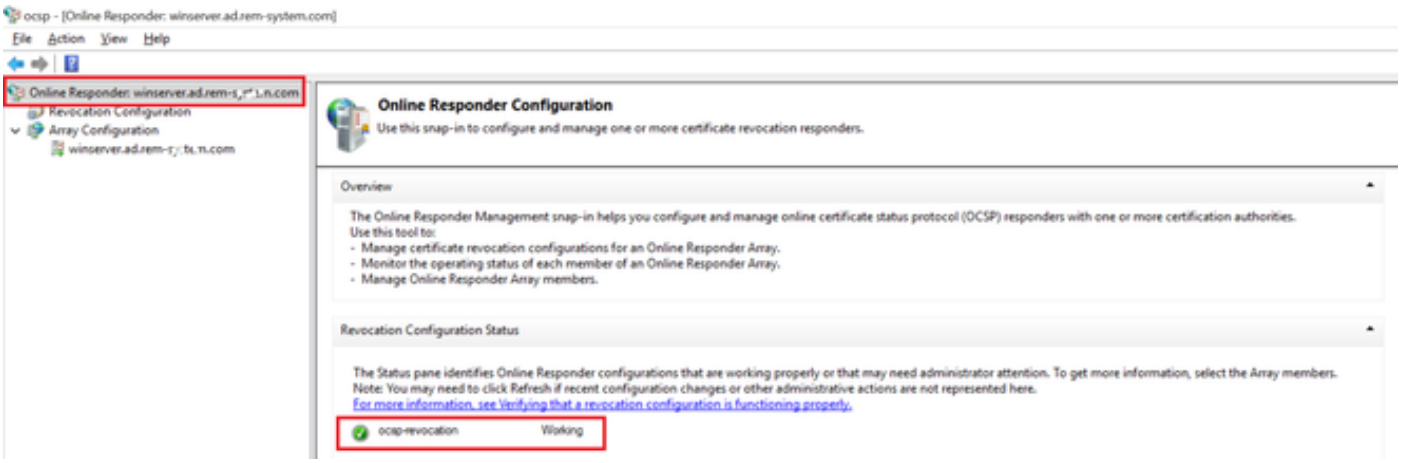
Passare a Utenti e computer di Active Directory, quindi fare clic su Utenti. Aggiungere clientcertCN come nome di accesso utente.



Nome di accesso utente

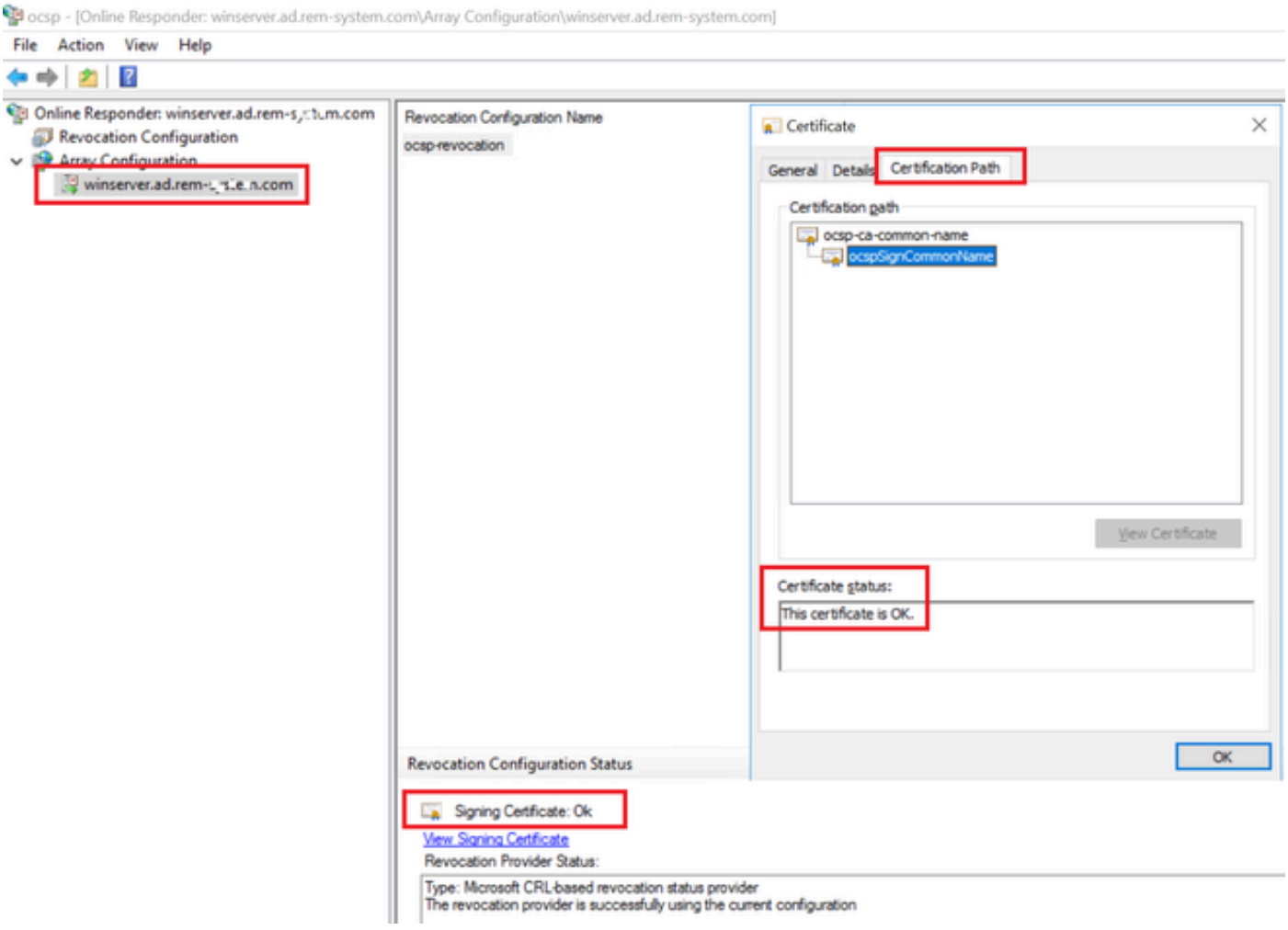
Passaggio 2. Conferma servizio OCSP

Passare a Windows e fare clic su Gestione risponditore in linea. Confermare lo stato del server OCSP.



Stato del server OCSP

Fare clic su winserver.ad.rem-xxx.com, verificare lo stato del certificato di firma OCSP.



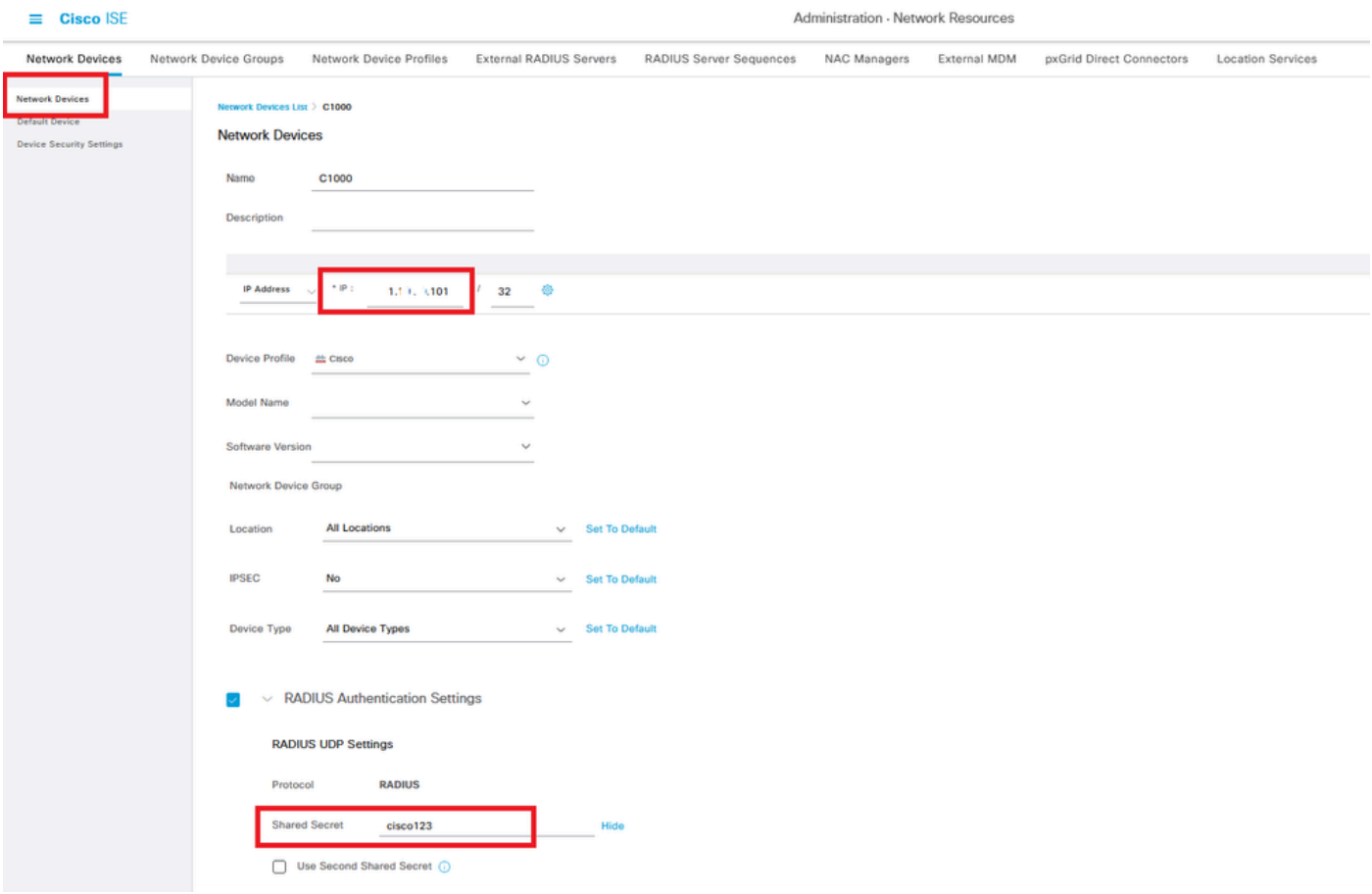
Stato del certificato di firma OCSP

Configurazione in ISE

Passaggio 1. Aggiungi dispositivo

Selezionare Amministrazione > Dispositivi di rete, quindi fare clic su Aggiungi per aggiungere un

dispositivo C1000.

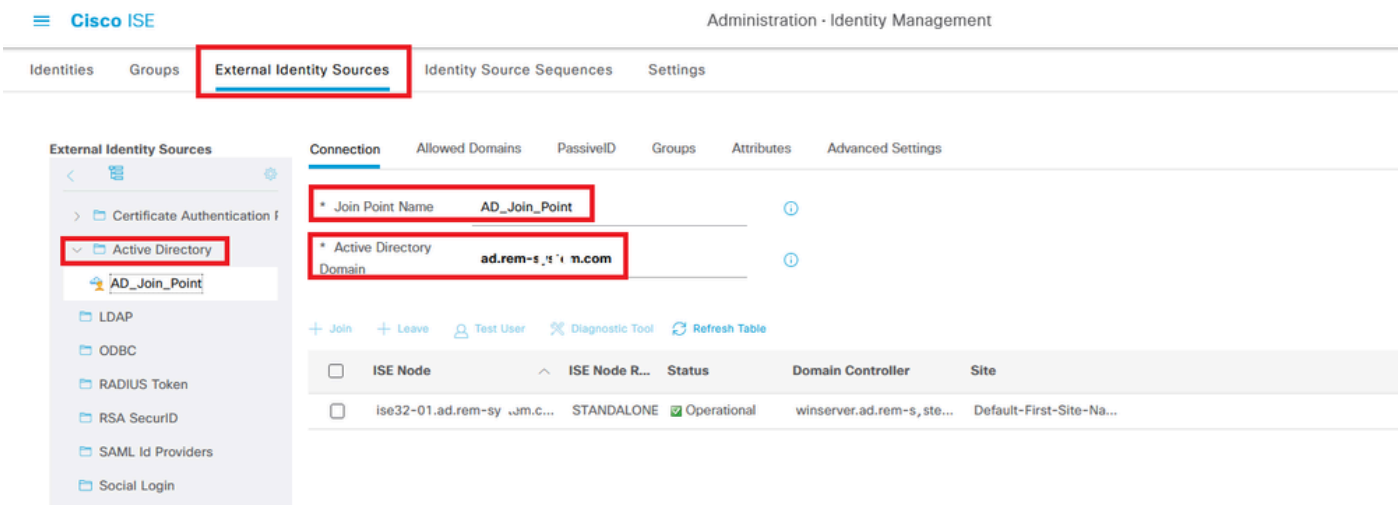


Aggiungi dispositivo

Passaggio 2. Aggiungi Active Directory

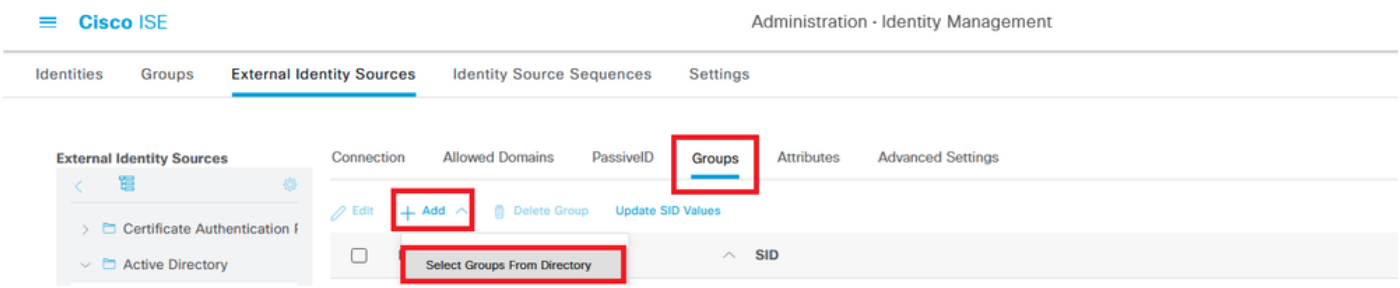
Selezionare Amministrazione > Origini identità esterne > Active Directory, fare clic sulla scheda Connessione, quindi aggiungere Active Directory ad ISE.

- Nome punto di join: AD_Join_Point
- Dominio Active Directory: ad.rem-xxx.com



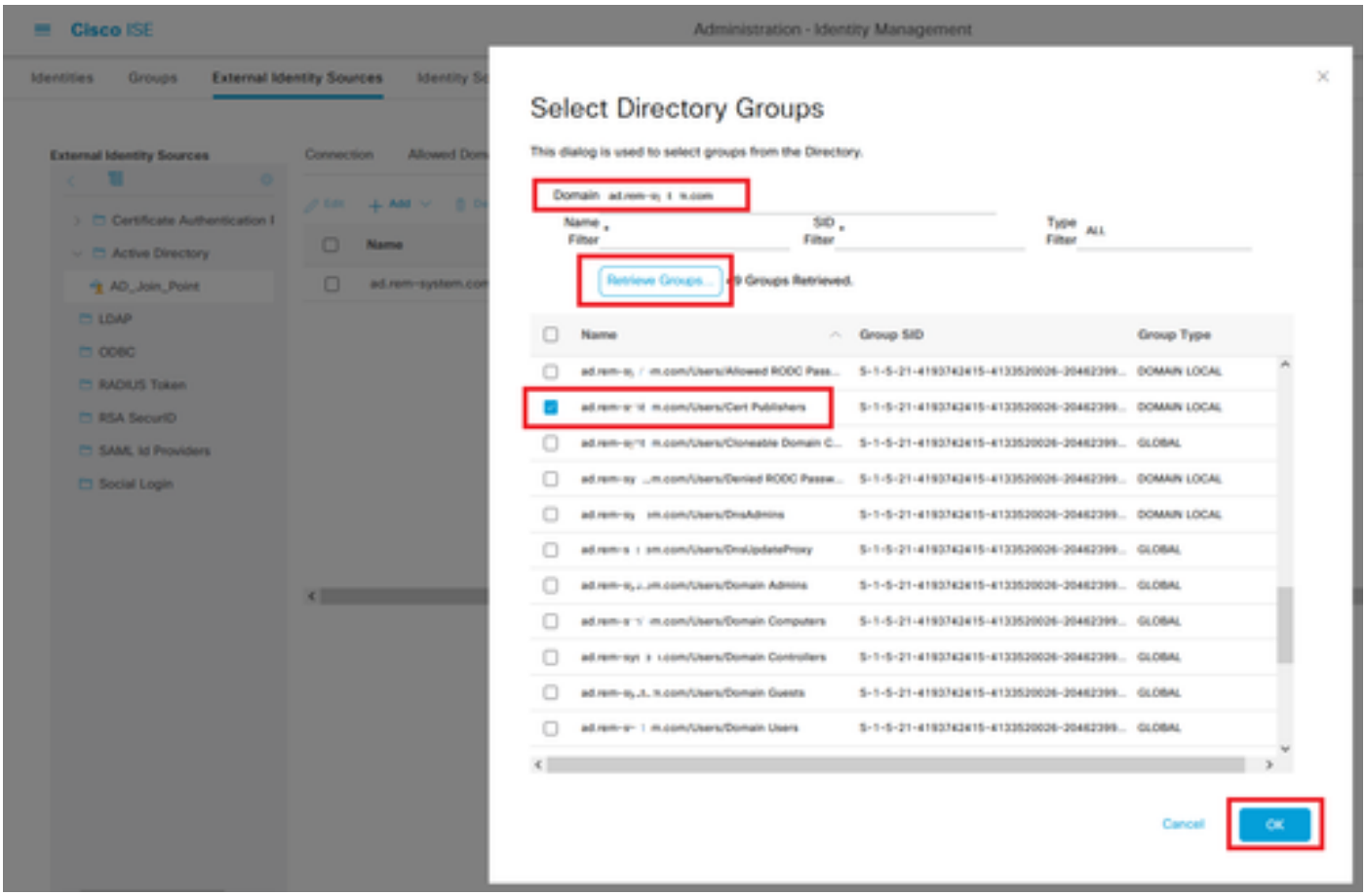
Aggiungi Active Directory

Passare alla scheda Gruppi, selezionare Seleziona gruppi dalla directory dall'elenco a discesa.



Seleziona gruppi dalla directory

Selezionate Recupera gruppi (Retrieve Groups) dall'elenco a discesa. Checkad.rem-xxx.com/Users/Cert Publisher e fare clic su OK.



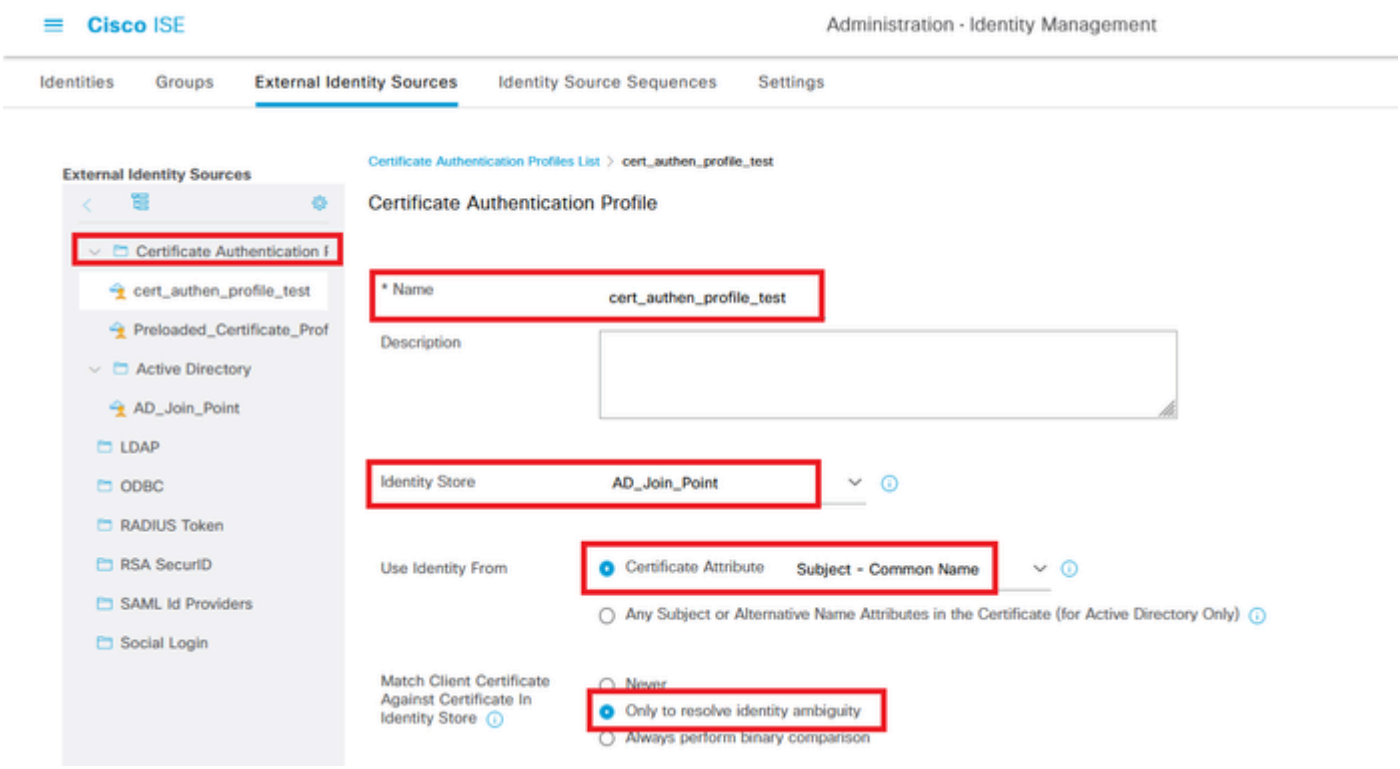
Controlla autori certificati

Passaggio 3. Aggiungi profilo di autenticazione certificato

Passare a Amministrazione > Origini identità esterne > Profilo di autenticazione certificato, fare clic sul pulsante Aggiungi per aggiungere un nuovo profilo di autenticazione certificato.

- Nome: cert_auto_profile_test
- Archivio identità: AD_Join_Point
- Usa identità da attributo certificato: Oggetto - Nome comune.
- Confronta certificato client con certificato nell'archivio identità: solo per risolvere l'ambiguità

dell'identità.

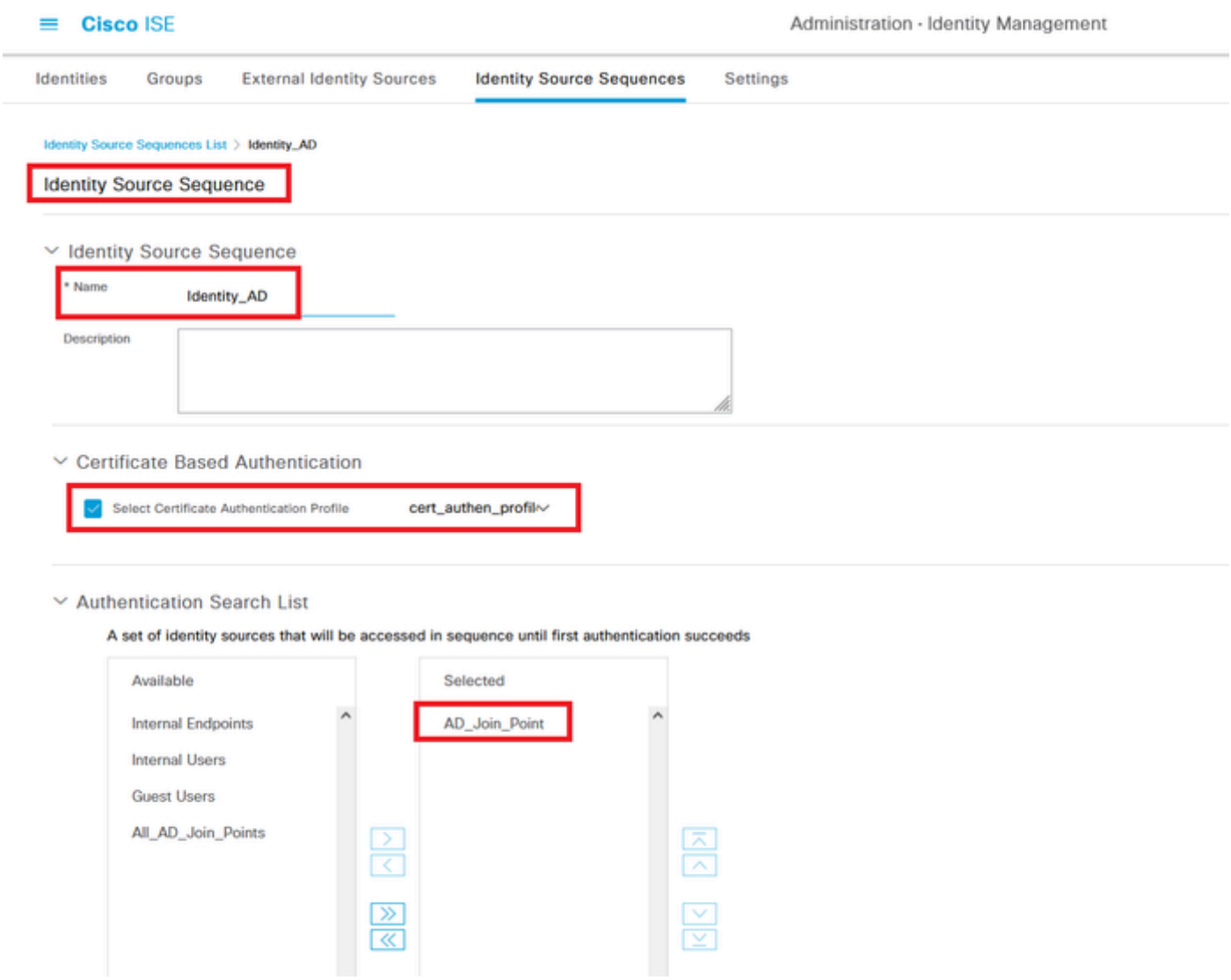


Aggiungi profilo di autenticazione certificato

Passaggio 4. Aggiungi sequenza di origine identità

Passare ad Amministrazione > Sequenze origine identità, quindi aggiungere una sequenza origine identità.

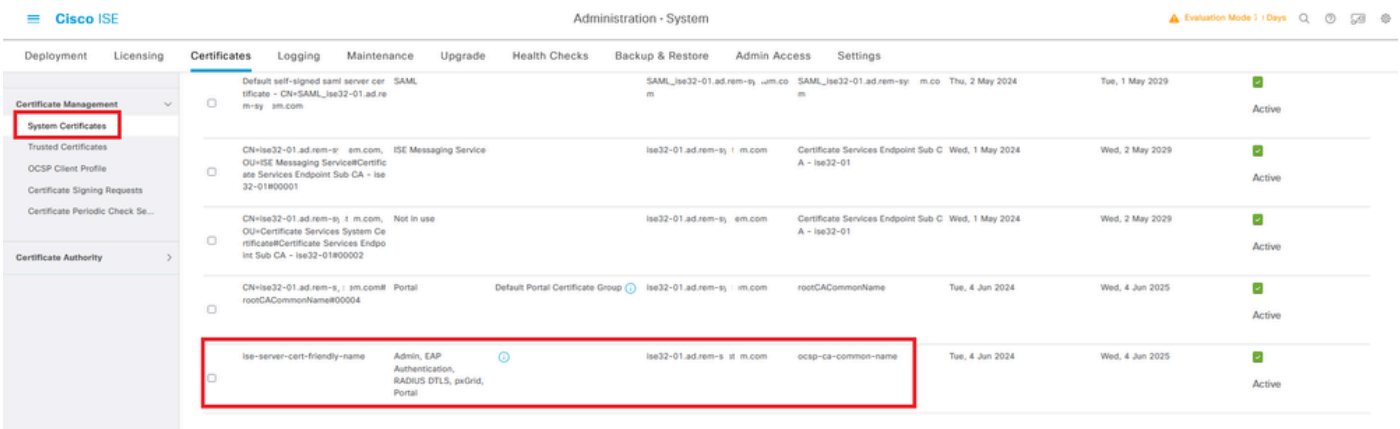
- Nome: Identity_AD
- Selezionare Certificate Authentication Profile: cert_authen_profile_test
- Elenco di ricerca autenticazione: AD_Join_Point



Aggiungi sequenze origine identità

Passaggio 5. Conferma certificato in ISE

Passare a Amministrazione > Certificati > Certificati di sistema, quindi verificare che il certificato del server sia firmato dalla CA attendibile.

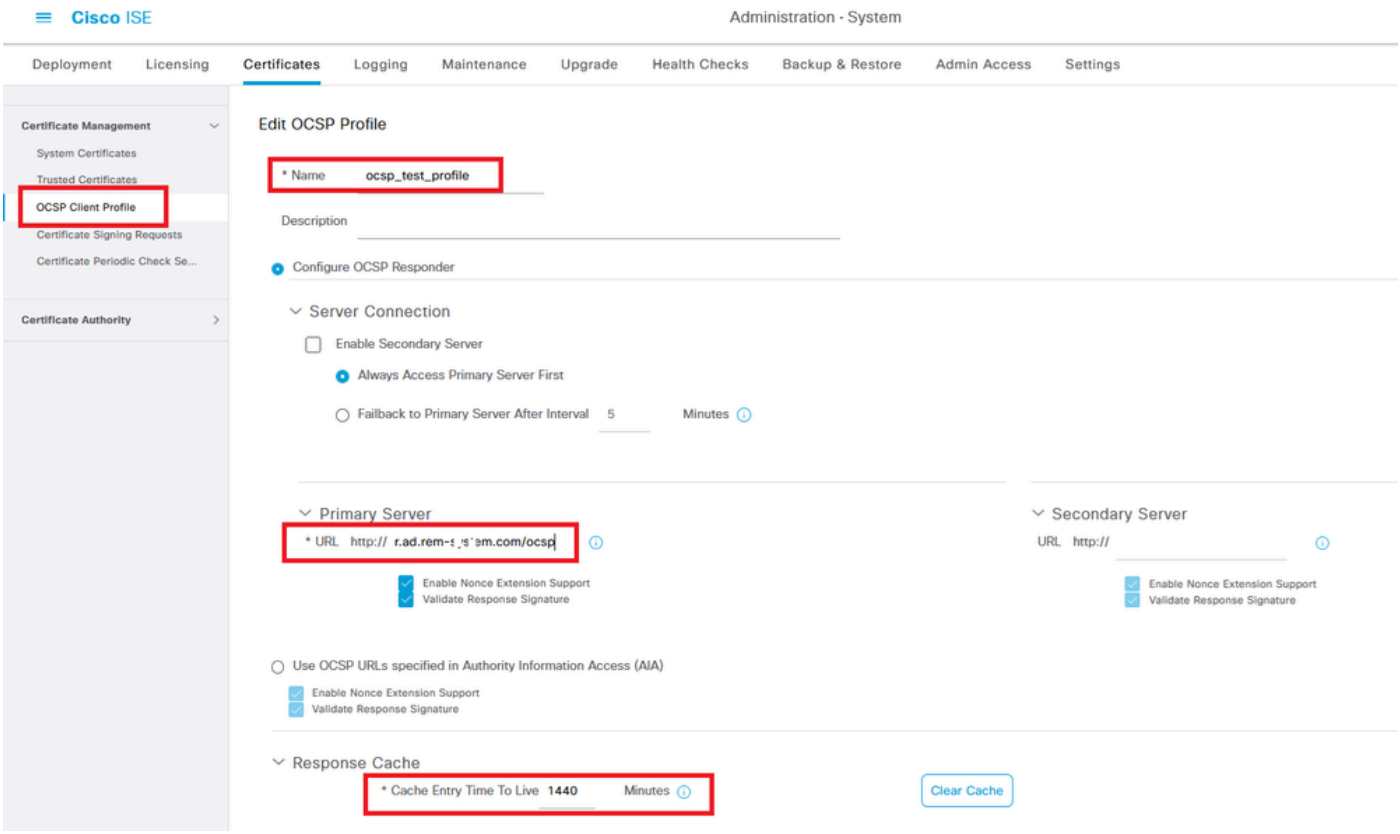


Certificato server

Passare a Amministrazione > Certificati > Profilo client OCSP, quindi fare clic su Pulsante

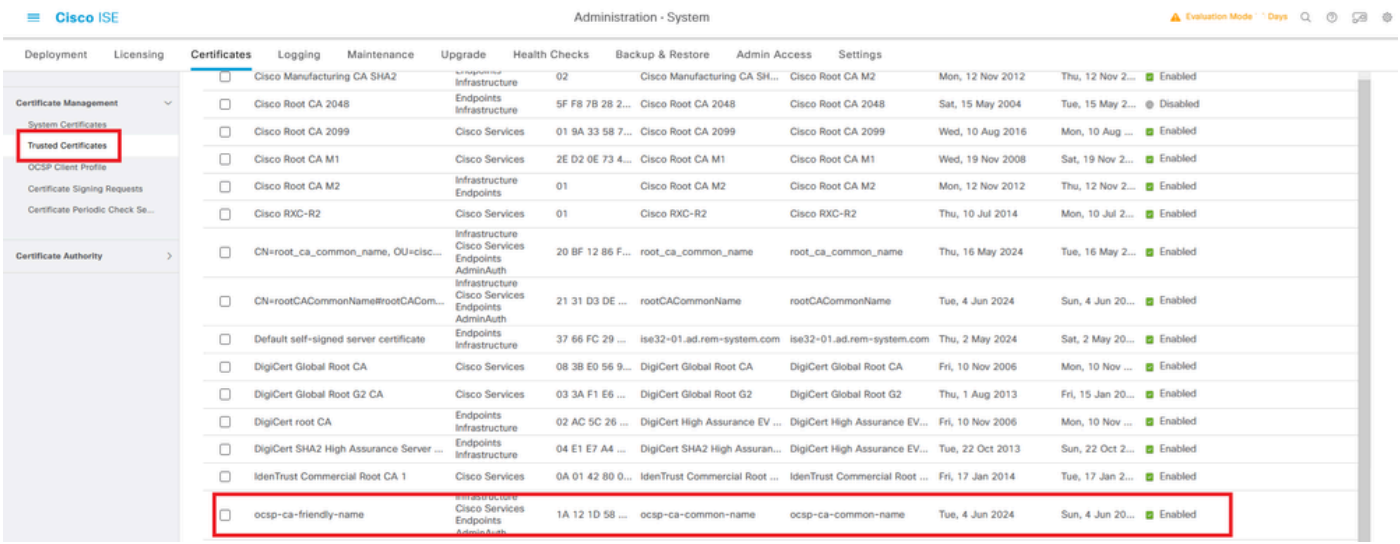
Aggiungi per aggiungere un nuovo profilo client OCSP.

- Nome: ocsp_test_profile
- Configura URL risponditore OCSP: http://winserver.ad.rem-xxx.com/ocsp



Profilo client OCSP

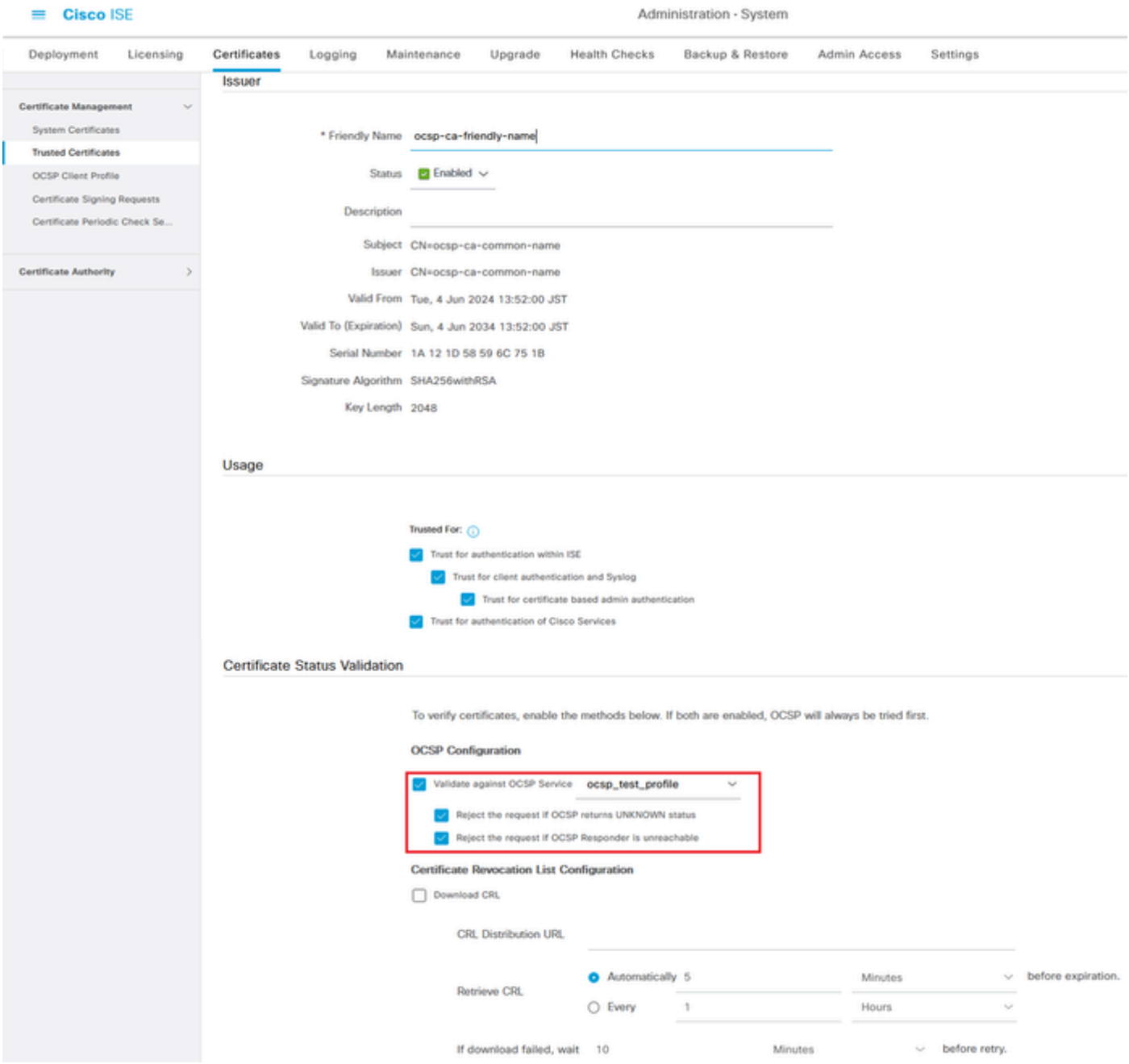
Selezionare Amministrazione > Certificati > Certificati attendibili, quindi confermare che l'autorità di certificazione attendibile sia stata importata in ISE.



CA attendibile

Controllare la CA e fare clic sul pulsante Modifica, immettere i dettagli della configurazione OCSP per la convalida dello stato del certificato.

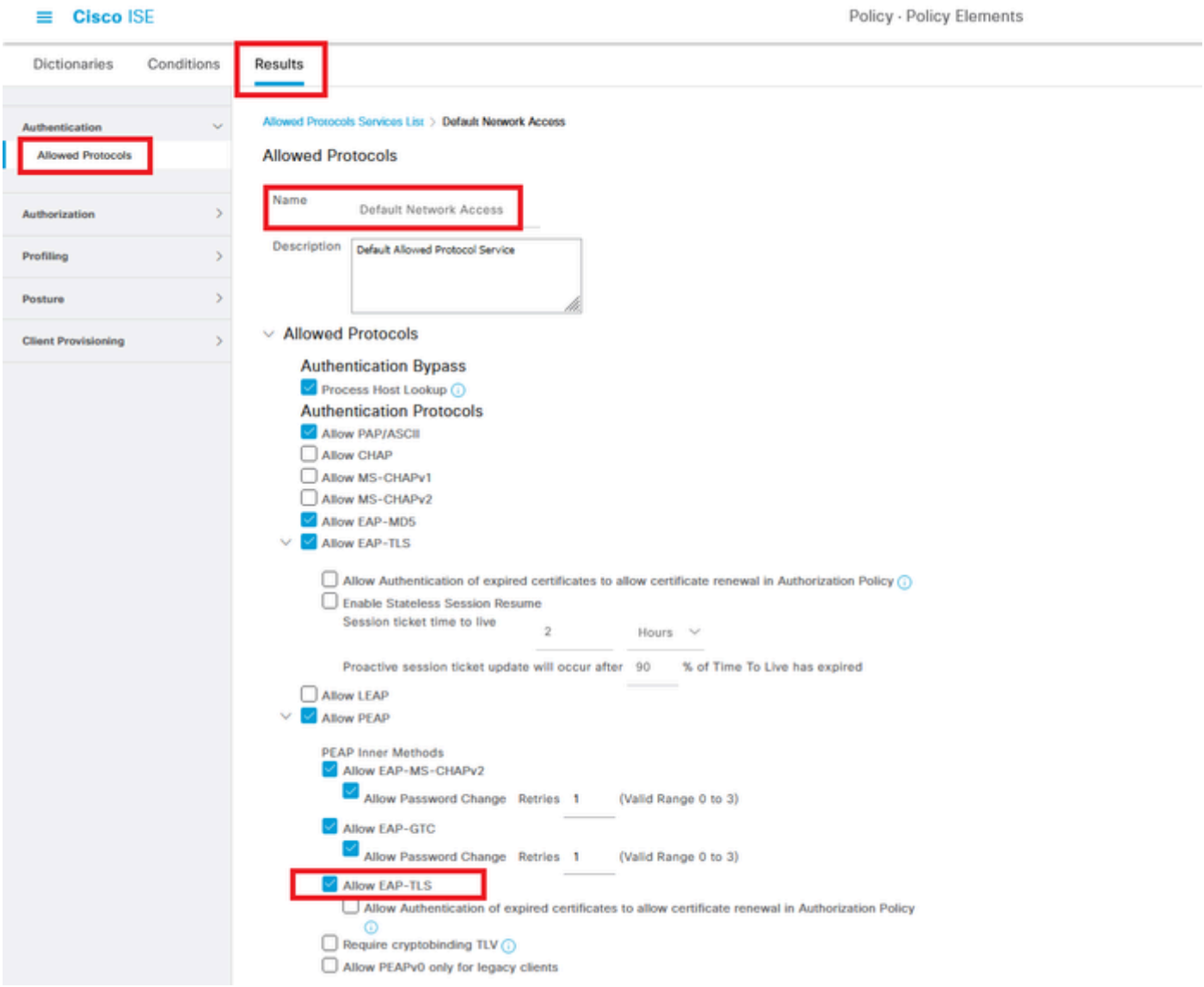
- Convalida rispetto al servizio OCSP: ocsp_test_profile
- Rifiuta la richiesta se OCSP restituisce lo stato UNKNOWN: check
- Rifiuta la richiesta se il risponditore OCSP non è raggiungibile: selezionare



Convalida stato certificato

Passaggio 6. Aggiungi protocolli consentiti

Passare a Criterio > Risultati > Autenticazione > Protocolli consentiti, modificare l'elenco dei servizi di accesso alla rete predefiniti e quindi selezionare Consenti EAP-TLS.

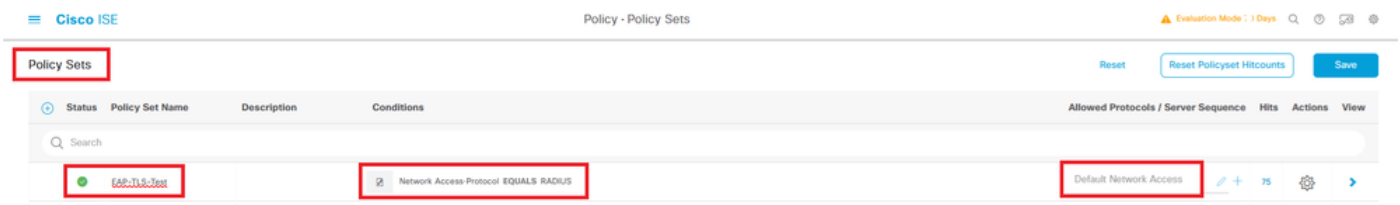


Consenti EAP-TLS

Passaggio 7. Aggiungi set di criteri

Passare a Criterio > Set di criteri, fare clic su + per aggiungere un set di criteri.

- Nome set di criteri: EAP-TLS-Test
- Condizioni: il protocollo di accesso alla rete è RADIUS
- Protocolli consentiti/sequenza server: accesso alla rete predefinito



Aggiungi set di criteri

Passaggio 8. Aggiungi criterio di autenticazione

Passare a Set di criteri, quindi fare clic su EAP-TLS-Test per aggiungere un criterio di autenticazione.

- Nome regola: autenticazione EAP-TLS
- Condizioni: Autenticazione Eap di accesso alla rete UGUALE A EAP-TLS E Wired_802.1 X
- Uso: Identity_AD

Aggiungi criterio di autenticazione

Passaggio 9. Aggiungi criterio di autorizzazione

Passare a Set di criteri e fare clic su EAP-TLS-Test per aggiungere un criterio di autorizzazione.

- Nome regola: EAP-TLS-Authorization
- Condizioni: Soggetto CERTIFICATO - Nome comune EQUALS clientcertCN
- Risultati: PermitAccess

Aggiungi criterio di autorizzazione

Verifica

Passaggio 1. Conferma sessione di autenticazione

Eseguireshow authentication sessions interface GigabitEthernet1/0/3 details il comando per confermare la sessione di autenticazione in C1000.

<#root>

Switch#

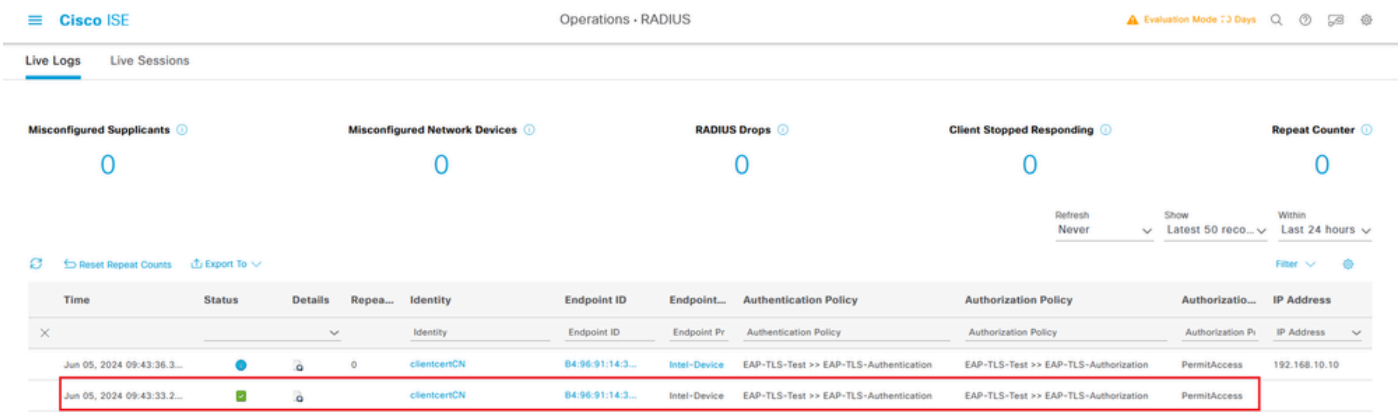
show authentication sessions interface GigabitEthernet1/0/3 details

```
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: 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
```

Passaggio 2. Conferma registro dinamico Radius

Selezionare **Operations > RADIUS > Live** Login nella GUI di ISE, quindi confermare il log attivo per l'autenticazione.



Registro Radius Live

Confermare il log dettagliato dell'autenticazione in tempo reale.

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

Dettagli di autenticazione

```
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
```

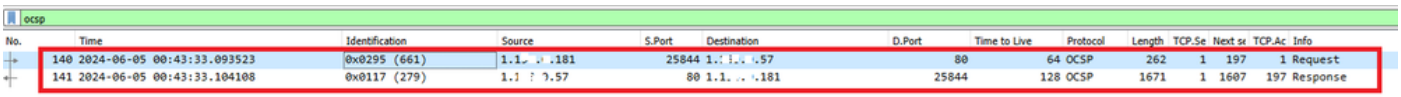
Code=5(AccountingResponse)

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

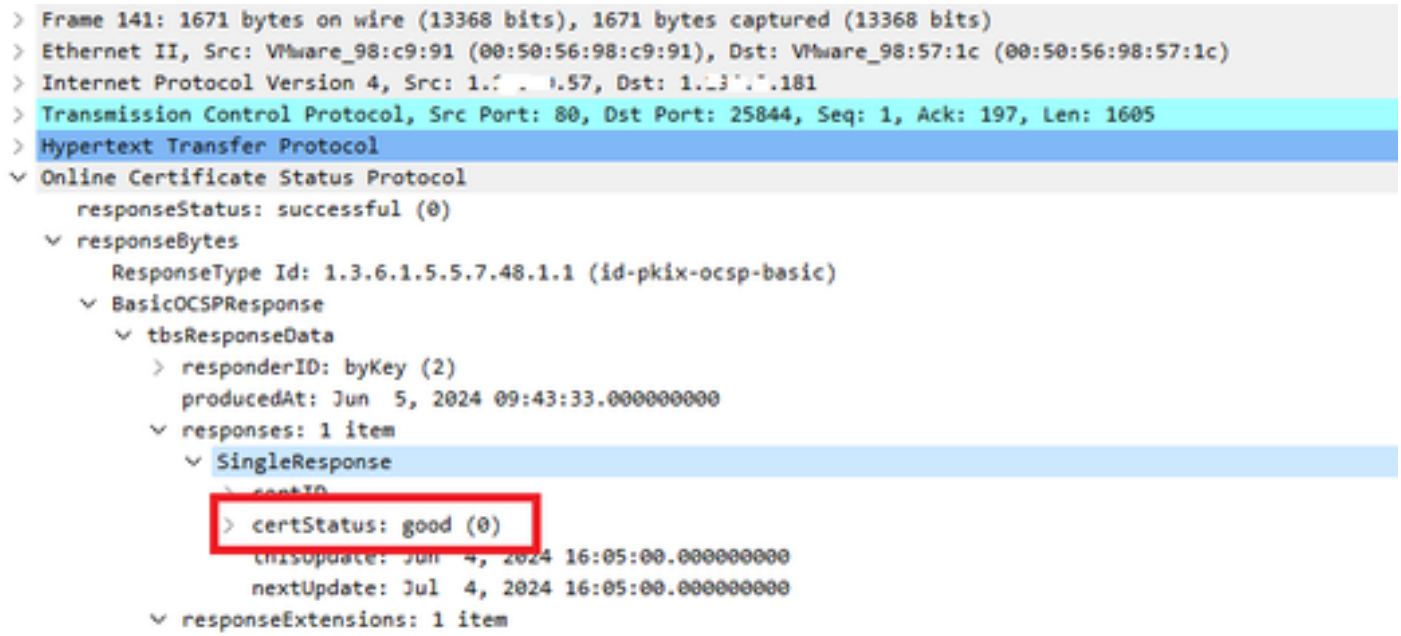
2. Dump TCP

Nel dump TCP ad ISE, ci si aspetta di trovare informazioni sulla risposta OCSP e sulla sessione Radius.

Richiesta e risposta OCSP:

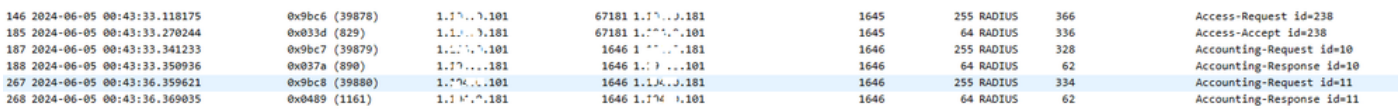


Acquisizione pacchetti di richiesta e risposta OCSP



Acquisisci dettagli risposta OCSP

Sessione Radius:



Acquisizione pacchetto sessione Radius

Informazioni correlate

Configurazione dell'autenticazione EAP-TLS con ISE

Configurazione dei certificati TLS/SSL in ISE

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).