Configuration de l'authentification EAP-TLS avec OCSP dans ISE

Table des matières

Introduction

Ce document décrit les étapes requises pour configurer l'authentification EAP-TLS avec OCSP pour les contrôles de révocation de certificat client en temps réel.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration de Cisco Identity Services Engine
- Configuration de Cisco Catalyst
- Protocole d'état de certificat en ligne

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Correctif 6 d'Identity Services Engine Virtual 3.2
- 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Diagramme du réseau

Cette image présente la topologie utilisée pour l'exemple de ce document.

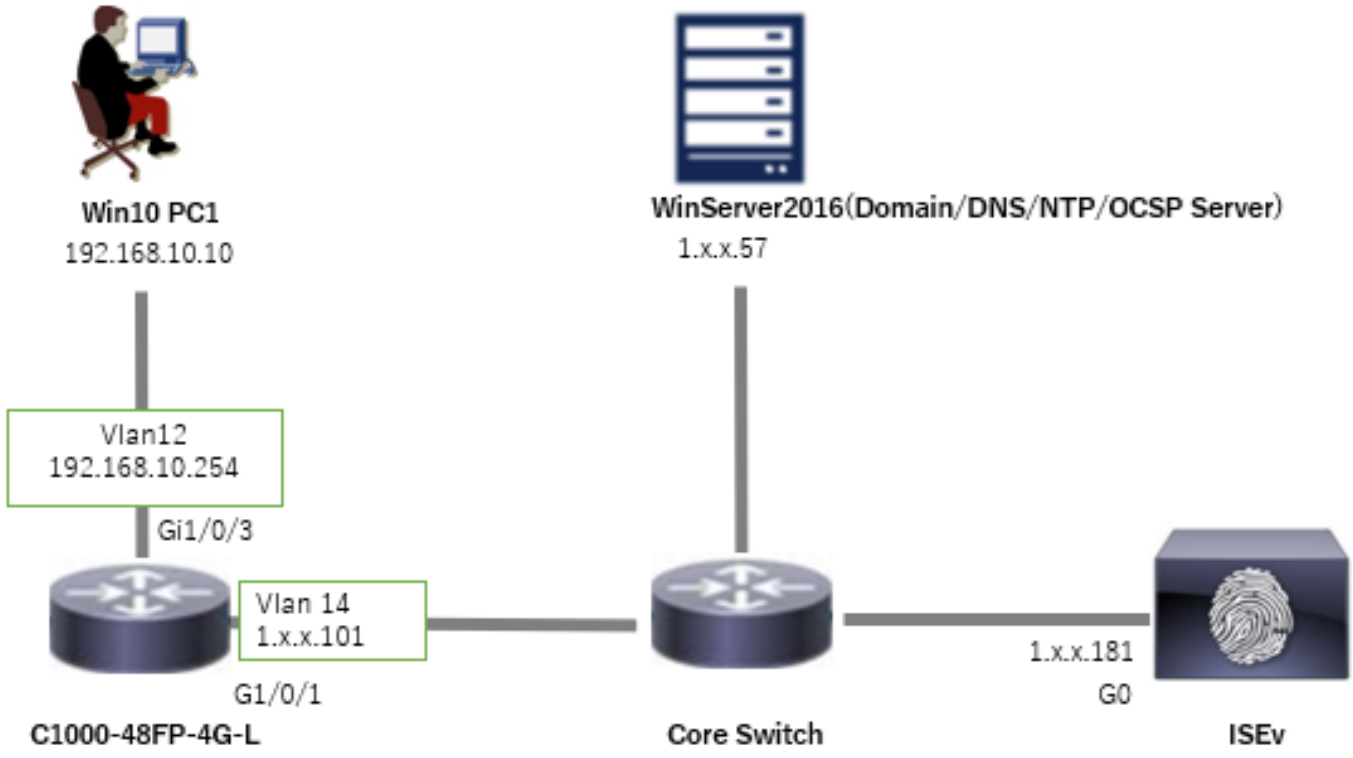


Diagramme du réseau

Informations générales

Dans EAP-TLS, un client présente son certificat numérique au serveur dans le cadre du processus d'authentification. Ce document décrit comment l'ISE valide le certificat client en vérifiant le nom commun (CN) du certificat par rapport au serveur AD et en confirmant si le certificat a été révoqué à l'aide du protocole OCSP (Online Certificate Status Protocol), qui fournit l'état du protocole en temps réel.

Le nom de domaine configuré sur Windows Server 2016 est ad.rem-xxx.com, qui est utilisé comme exemple dans ce document.

Les serveurs OCSP (Online Certificate Status Protocol) et AD (Active Directory) référencés dans ce document sont utilisés pour la validation des certificats.

- Nom de domaine complet Active Directory : winserver.ad.rem-xxx.com
- URL de distribution CRL : http://winserver.ad.rem-xxx.com/ocsp-ca.crl
- URL de l'autorité : http://winserver.ad.rem-xxx.com/ocsp

Il s'agit de la chaîne de certificats avec le nom commun de chaque certificat utilisé dans le document.

- CA : ocsp-ca-common-name
- Certificat client : clientcertCN
- Certificat du serveur : ise32-01.ad.rem-xxx.com
- Certificat de signature OCSP : ocspSignCommonName

Configurations

Configuration dans C1000

Il s'agit de la configuration minimale de l'interface de ligne de commande 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
```

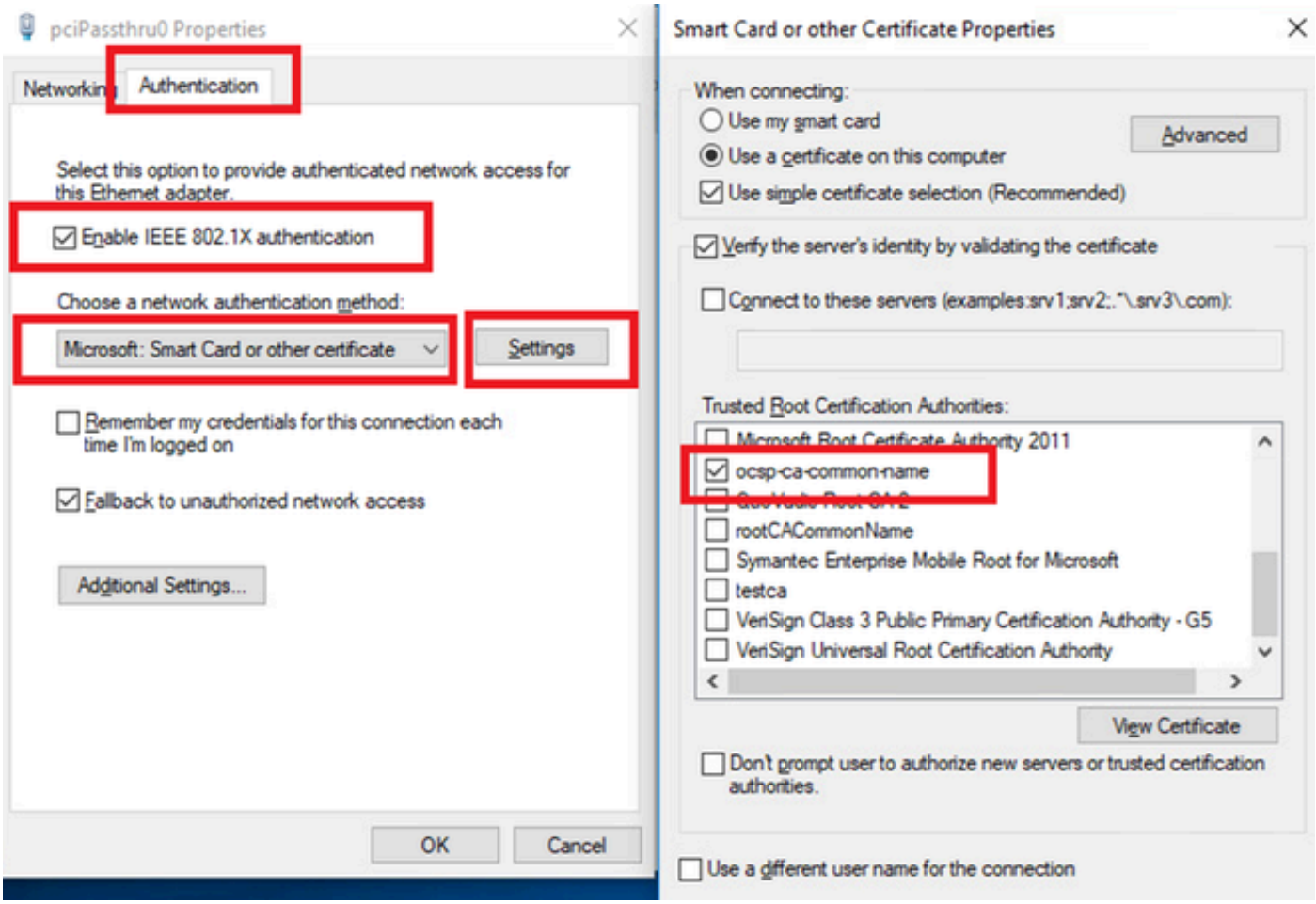
```
ip address 1.x.x.101 255.0.0.0

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
```

Configuration dans le PC Windows

Étape 1. Configurer l'authentification utilisateur

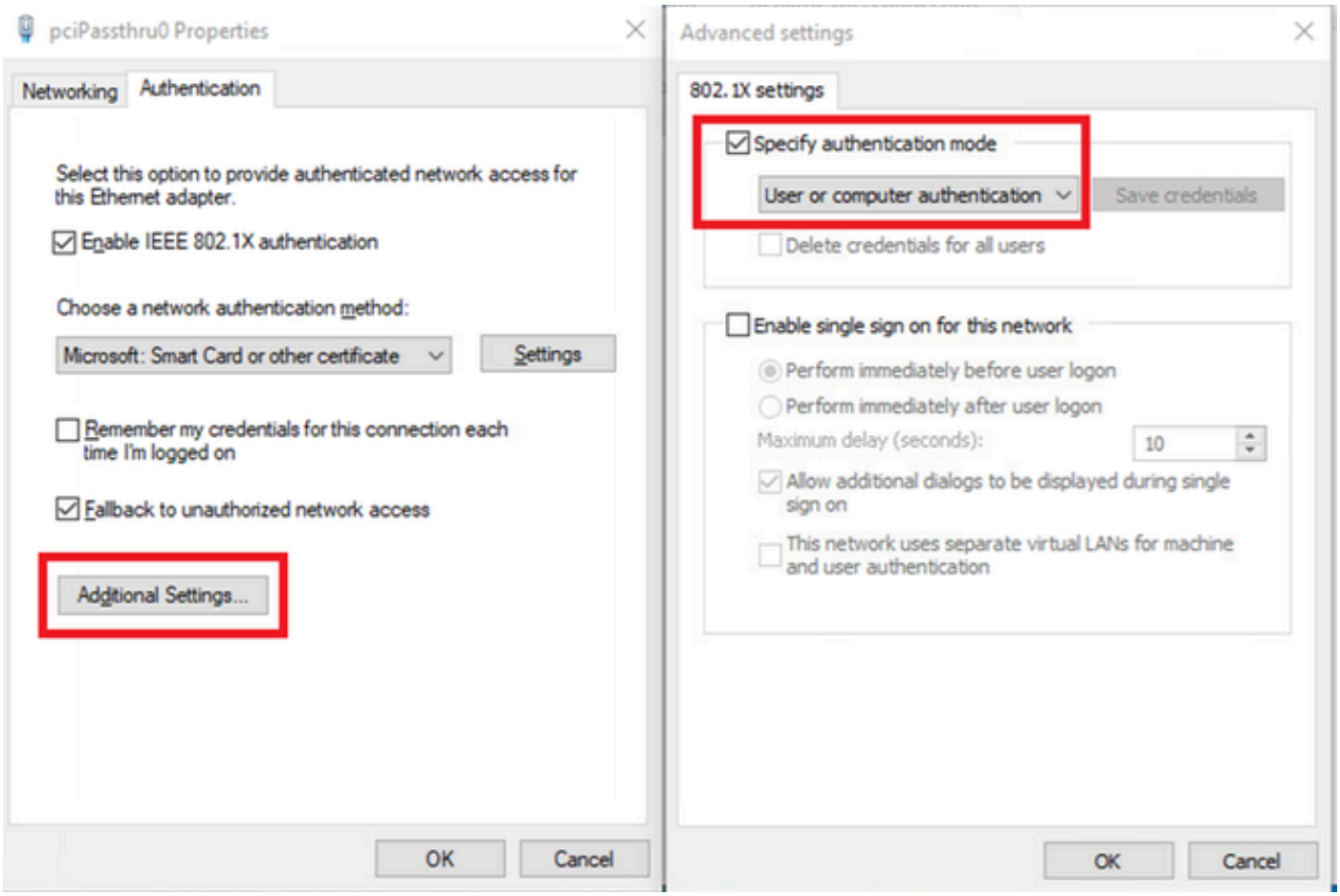
Accédez àAuthentication, cochezEnable IEEE 802.1X authentication et sélectionnez Microsoft : Smart Card or other certificate.

Cliquez sur le bouton Paramètres, cochez la case Utiliser un certificat sur cet ordinateur, puis sélectionnez l'autorité de certification approuvée du PC Windows.



Activer l'authentification du certificat

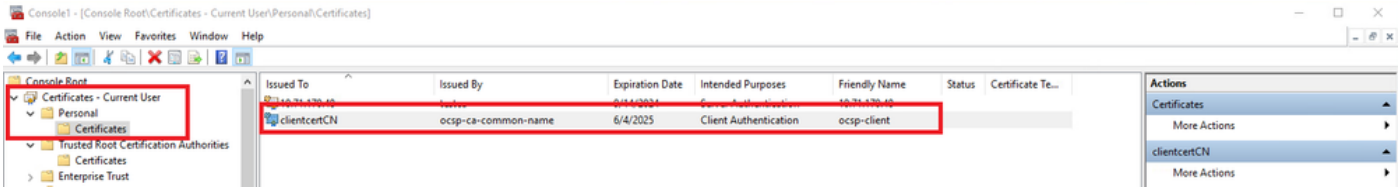
Accédez àAuthentification, cochezParamètres supplémentaires. Sélectionnez Authentification utilisateur ou ordinateur dans la liste déroulante.



Spécifier le mode d'authentification

Étape 2. Confirmer le certificat client

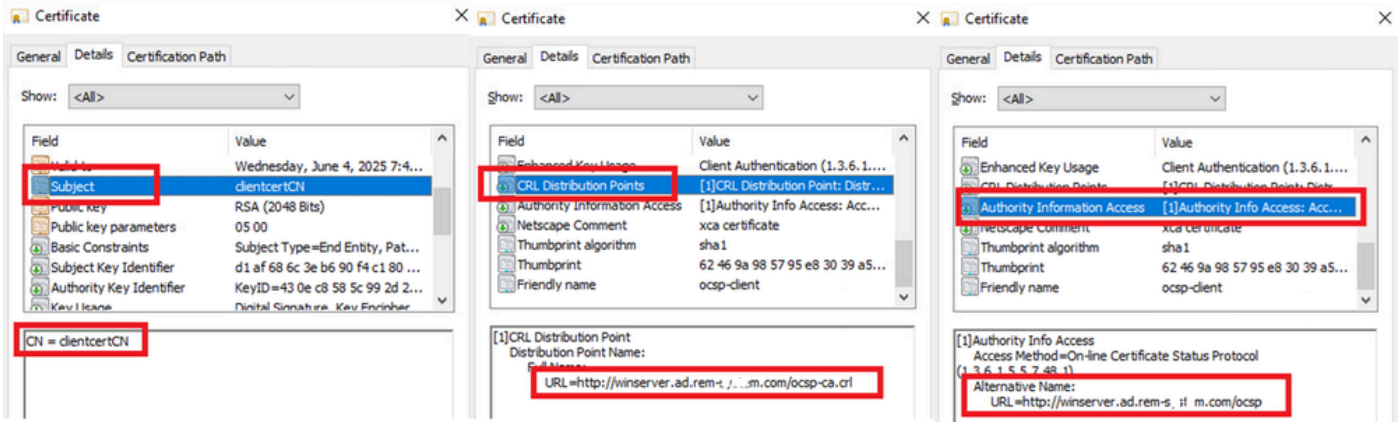
Accédez à Certificates - Current User > Personal > Certificates, et vérifiez le certificat client utilisé pour l'authentification.



Confirmer le certificat client

Double-cliquez sur le certificat client, accédez à Details, vérifiez les détails de Subject, CRL Distribution Points, Authority Information Access.

- Objet : CN = clientcertCN
- Points de distribution CRL : http://winserver.ad.rem-xxx.com/ocsp-ca.crl
- Accès aux informations d'autorité : http://winserver.ad.rem-xxx.com/ocsp

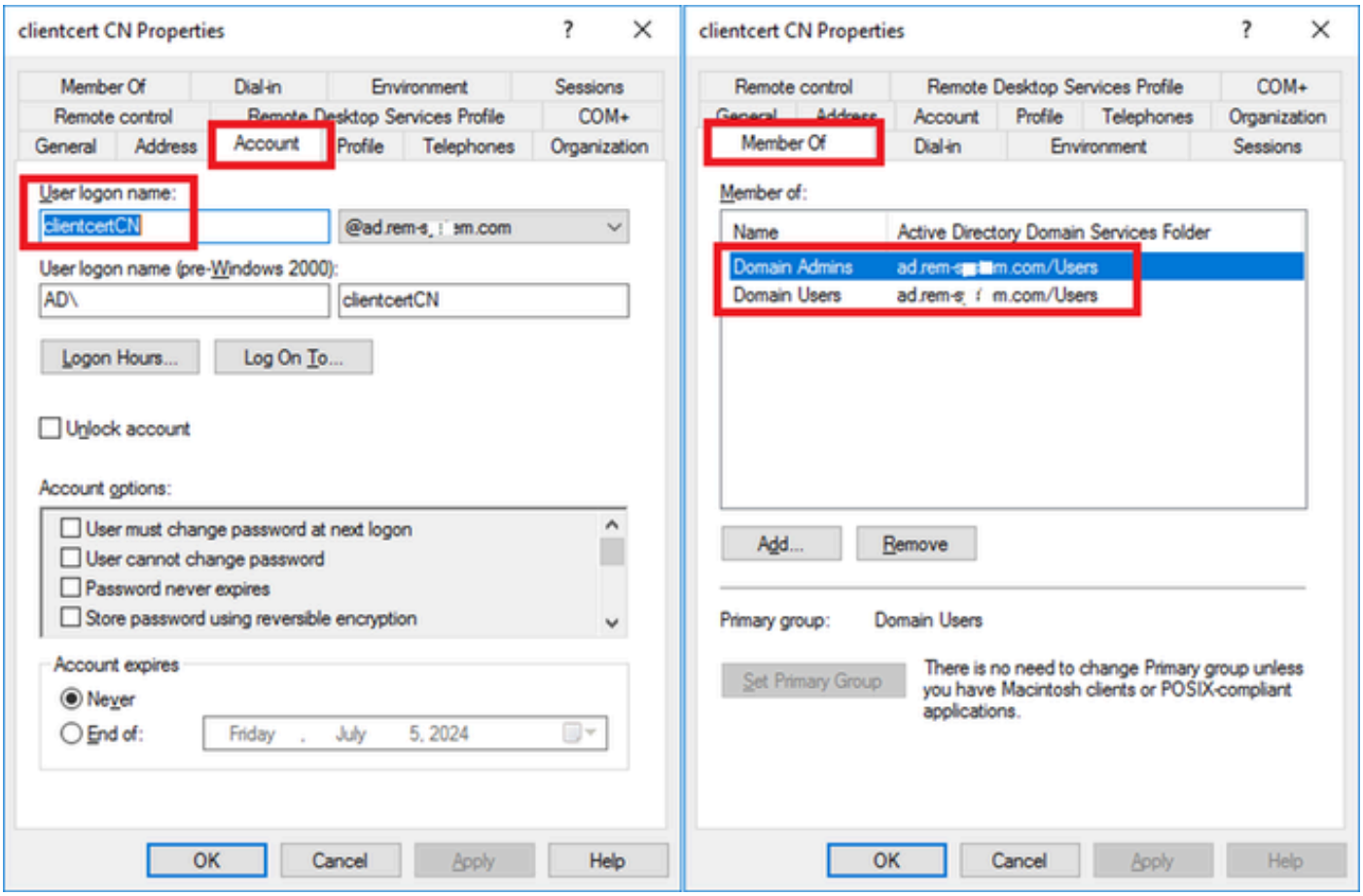


Détail du certificat client

Configuration dans Windows Server

Étape 1. Ajouter des utilisateurs

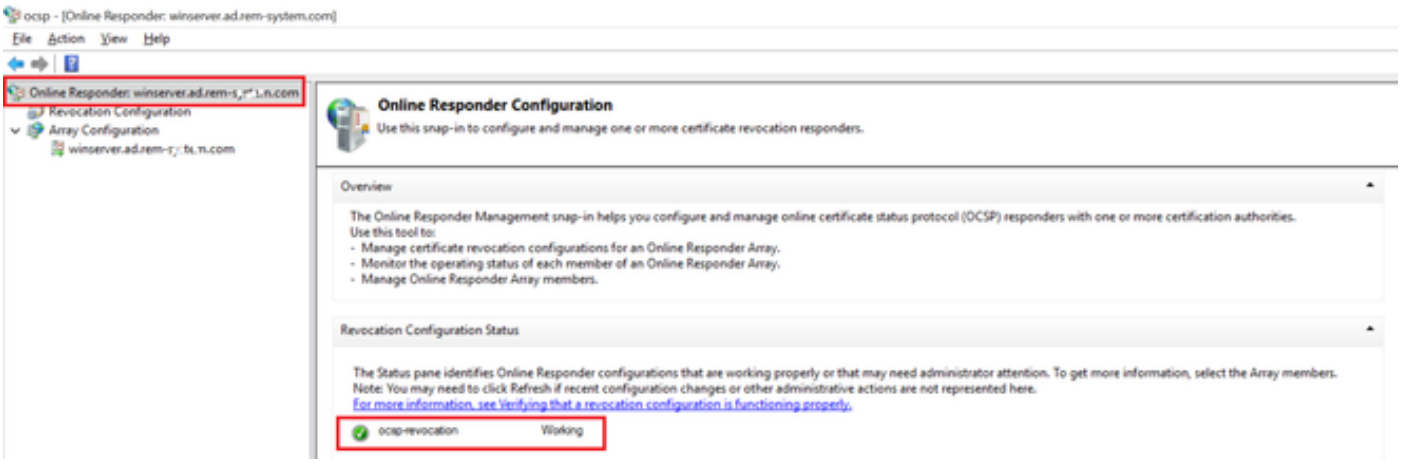
Accédez à Utilisateurs et ordinateurs Active Directory, puis cliquez surUtilisateurs. Ajoutez clientcertCN en tant que nom de connexion utilisateur.



Nom de connexion utilisateur

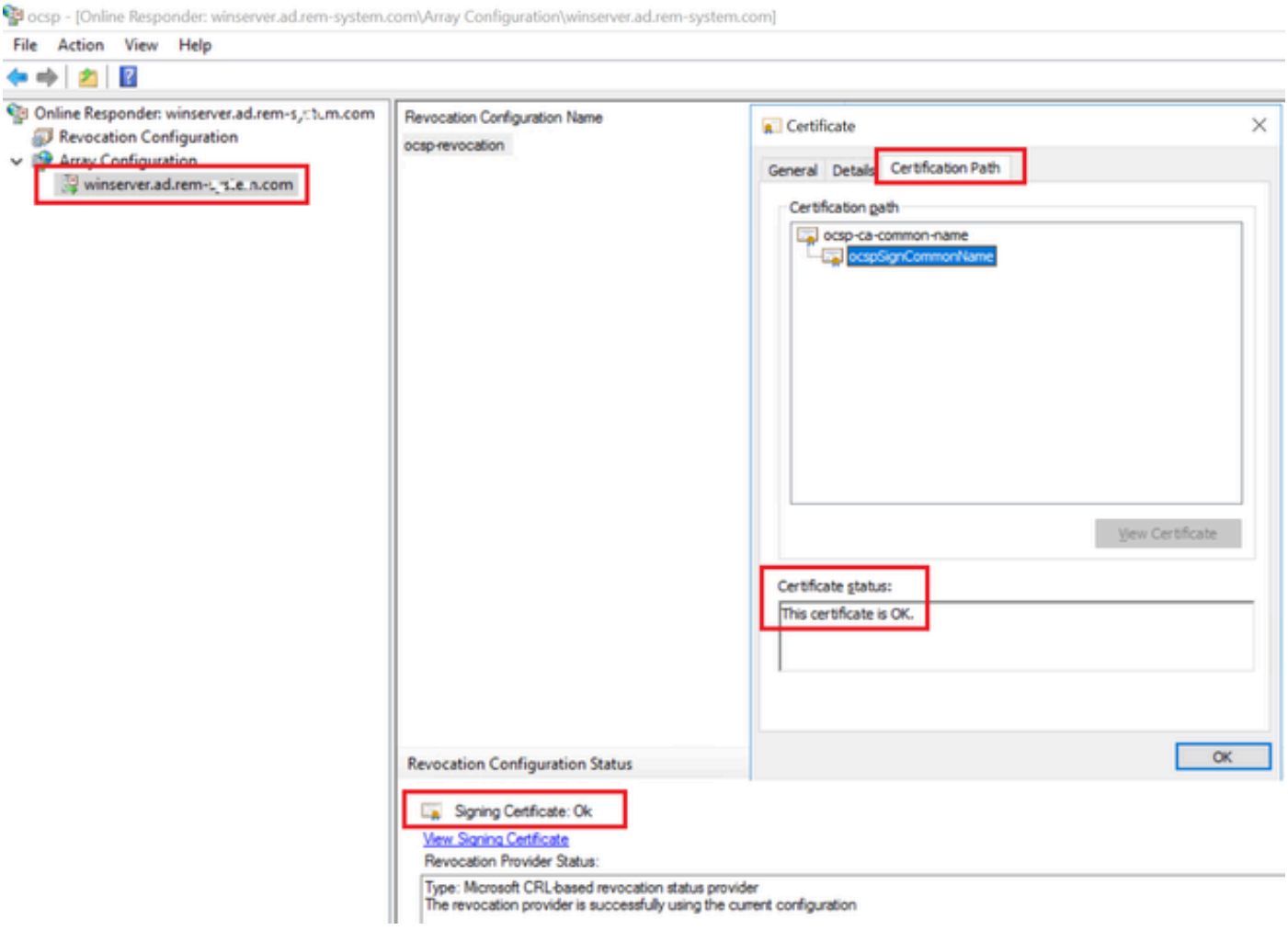
Étape 2. Confirmer le service OCSP

Accédez à Windows, cliquez sur Gestion des répondeurs en ligne. Confirmez l'état du serveur OCSP.



État du serveur OCSP

Cliquez sur winserver.ad.rem-xxx.com, vérifiez l'état du certificat de signature OCSP.



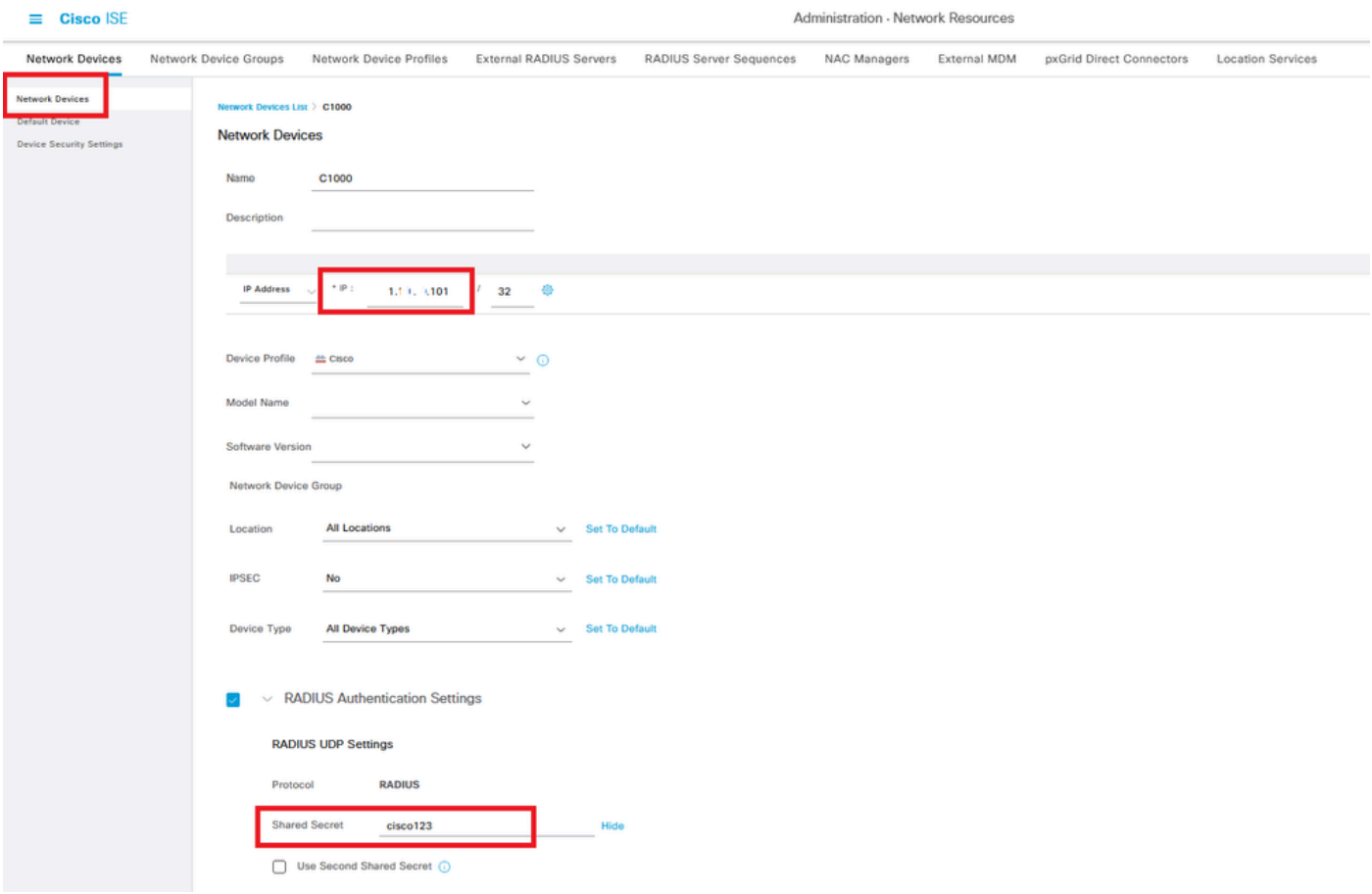
État du certificat de signature OCSP

Configuration dans ISE

Étape 1. Ajouter un périphérique

Accédez à Administration > Network Devices, cliquez sur Addbutton pour ajouter un périphérique

C1000.

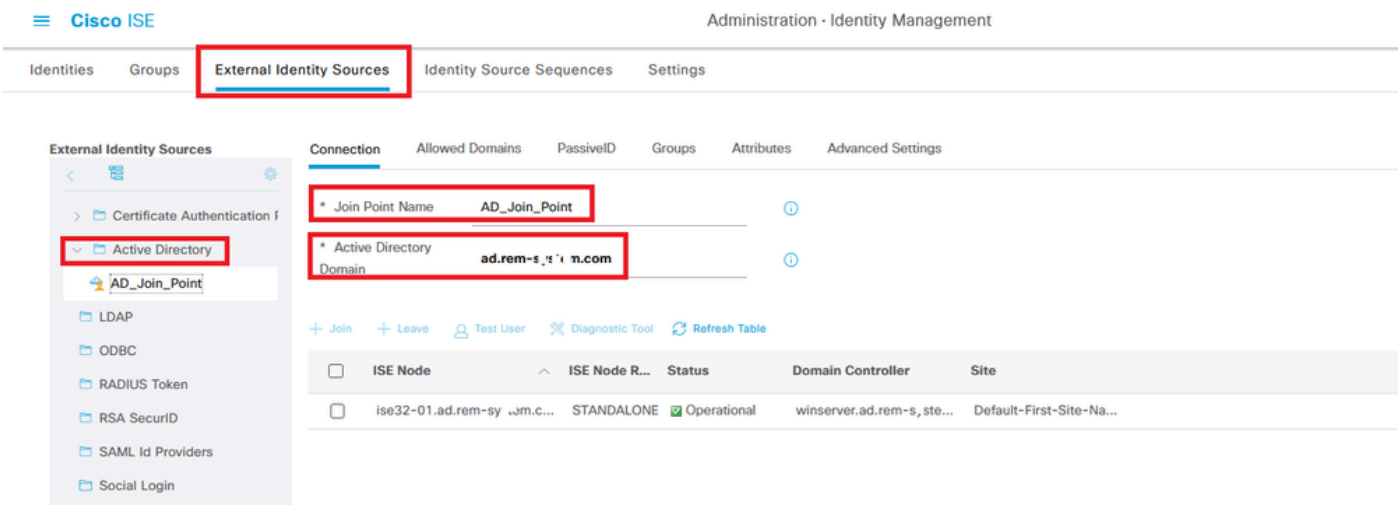


Ajouter un périphérique

Étape 2. Ajouter Active Directory

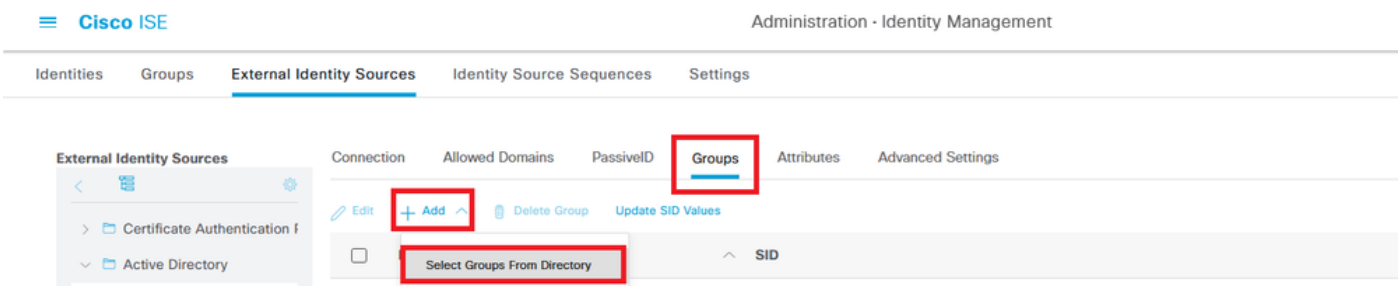
Accédez à Administration > Sources d'identité externes > Active Directory, cliquez sur l'onglet Connexion, ajoutez Active Directory à ISE.

- Nom du point de jointure : AD_Join_Point
- Domaine Active Directory : ad.rem-xxx.com



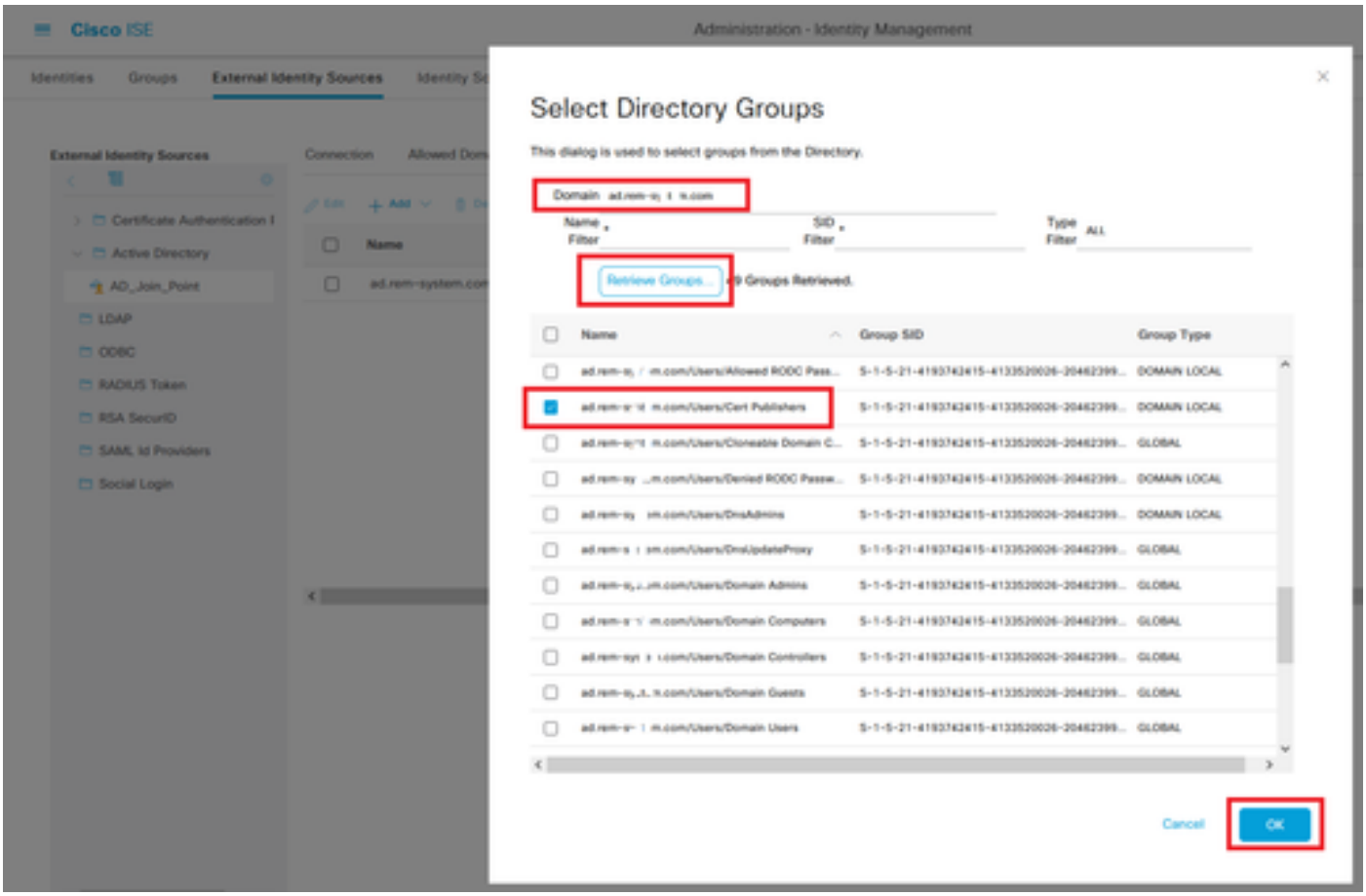
Ajouter Active Directory

Accédez à l'onglet Groups, sélectionnez Select Groups From Directory dans la liste déroulante.



Sélectionner des groupes dans le répertoire

Cliquez sur la liste déroulante Récupérer des groupes. Checkad.rem-xxx.com/Users/Cert Publishers et cliquez sur OK.



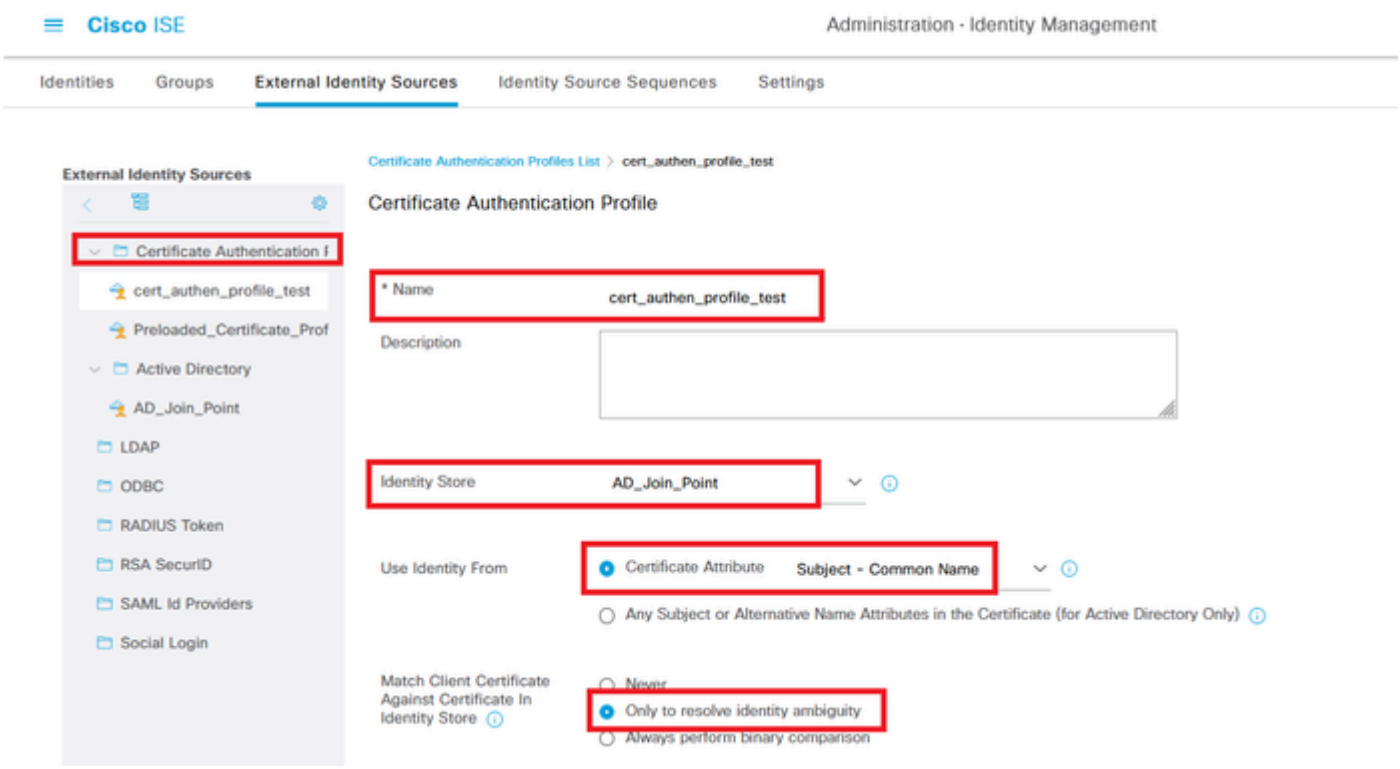
Vérifier les éditeurs de certificats

Étape 3. Ajouter un profil d'authentification de certificat

Accédez à Administration > External Identity Sources > Certificate Authentication Profile, cliquez sur le bouton Add pour ajouter un nouveau profil d'authentification de certificat.

- Nom : cert_authen_profile_test
- Magasin d'identités : AD_Join_Point
- Utiliser L'Identité De L'Attribut De Certificat : Objet - Nom Commun.
- Faire correspondre le certificat client avec le certificat dans le magasin d'identités :

uniquement pour résoudre l'ambiguïté d'identité.

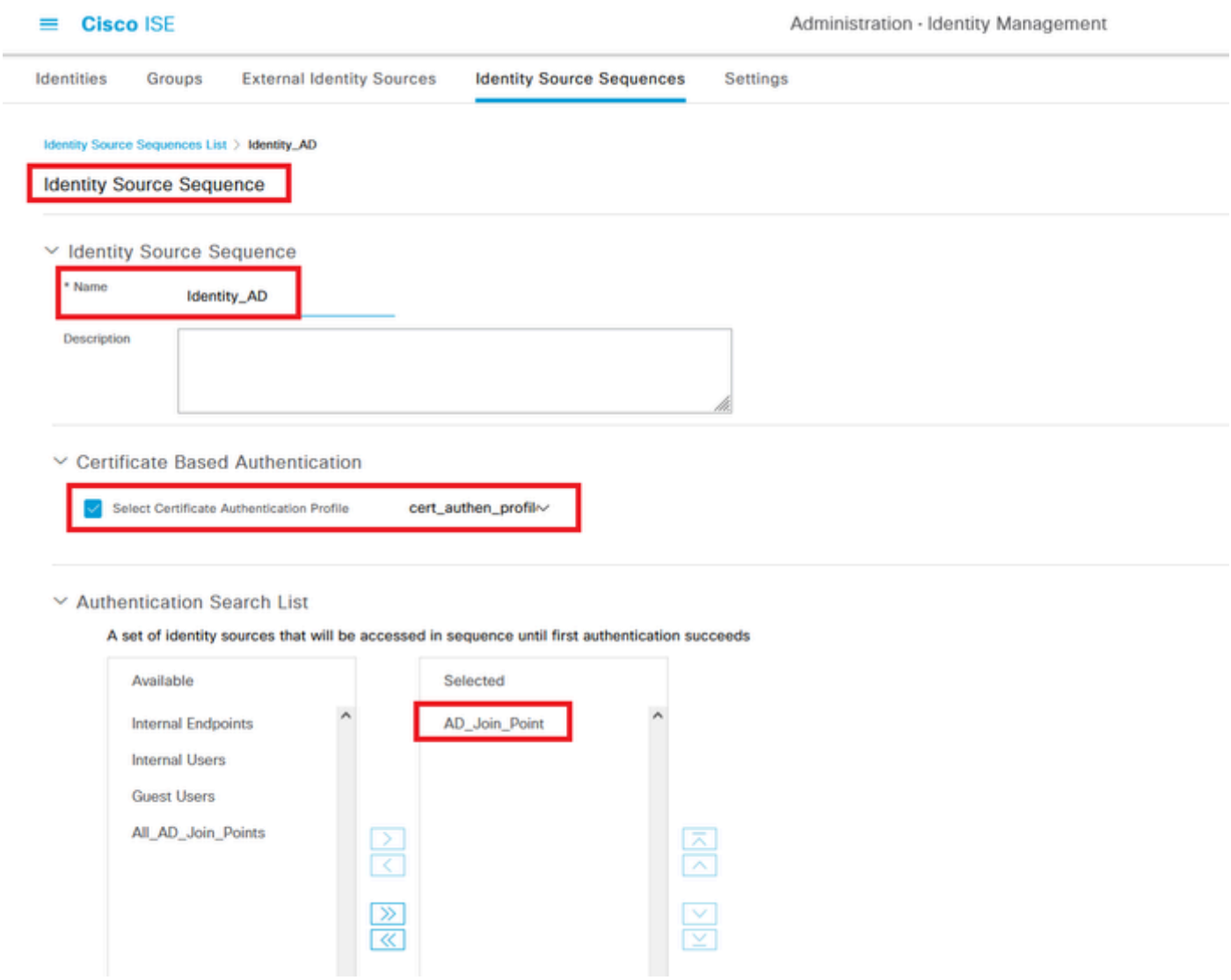


Ajouter un profil d'authentification de certificat

Étape 4. Ajouter une séquence source d'identité

Accédez à Administration > Identity Source Sequences, ajoutez une Identity Source Sequence.

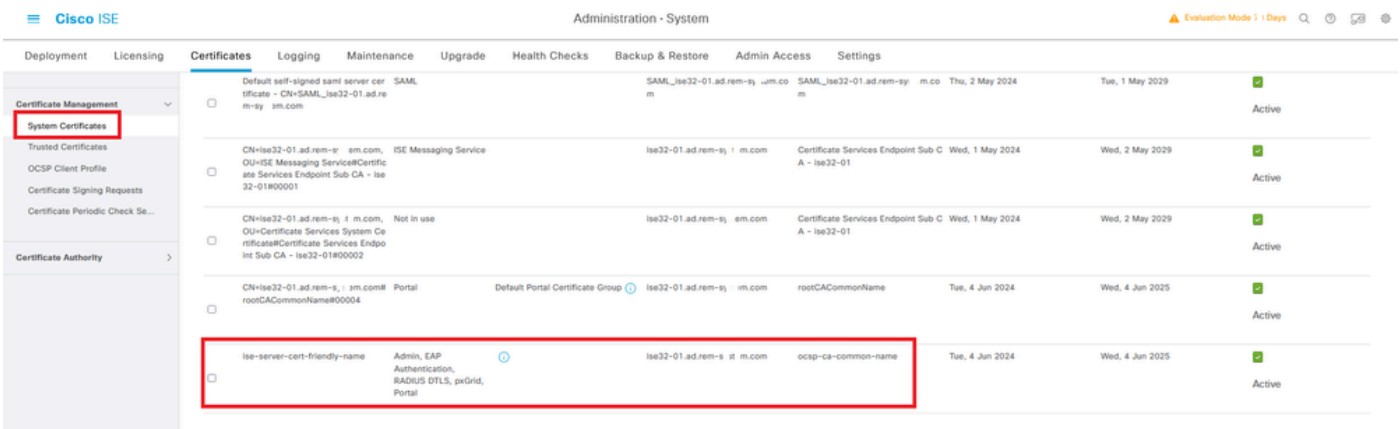
- Nom : Identity_AD
- Sélectionnez Certificate Authentication Profile: cert_authen_profile_test
- Liste de recherche d'authentification : AD_Join_Point



Ajouter des séquences source d'identité

Étape 5. Confirmer le certificat dans ISE

Accédez à Administration > Certificates > System Certificates, confirmez que le certificat du serveur est signé par l'autorité de certification approuvée.

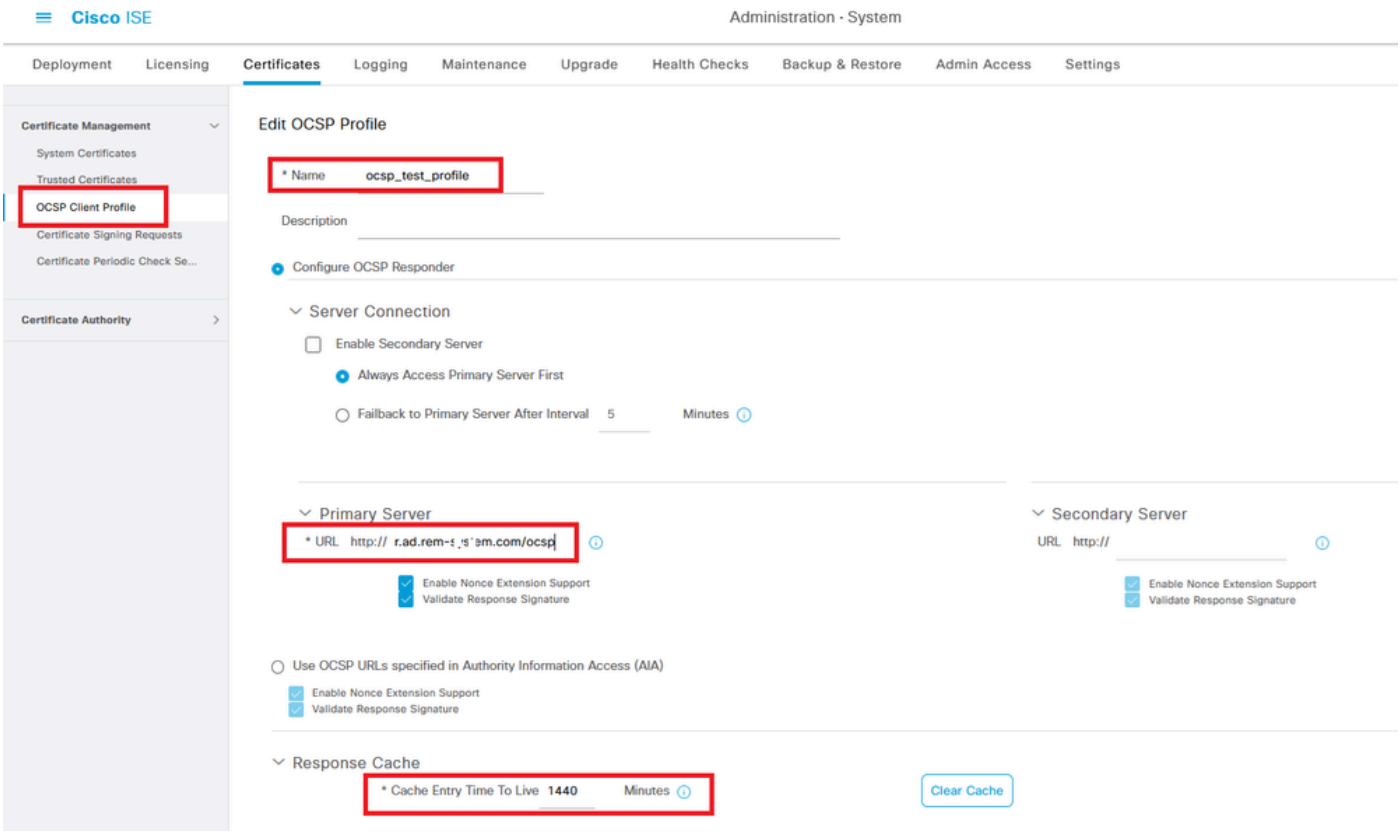


certificat du serveur

Accédez à Administration > Certificates > OCSP Client Profile, cliquez sur Add button to add a

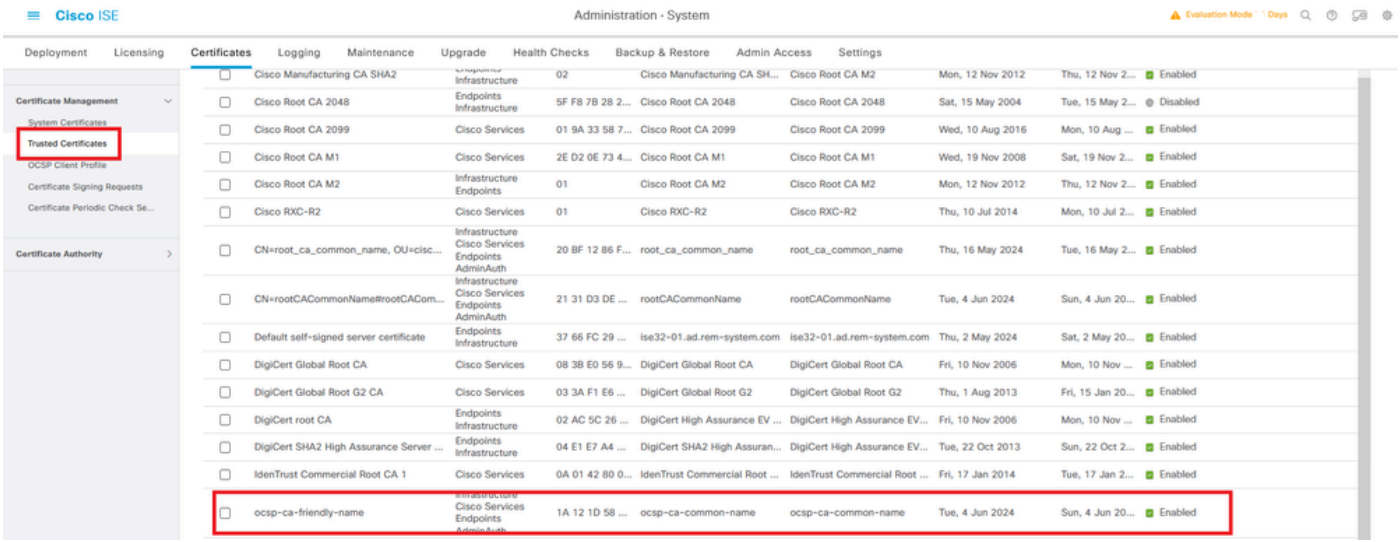
new OCSP client profile.

- Nom : ocsp_test_profile
- Configurer l'URL du répondeur OCSP : http://winserver.ad.rem-xxx.com/ocsp



Profil du client OCSP

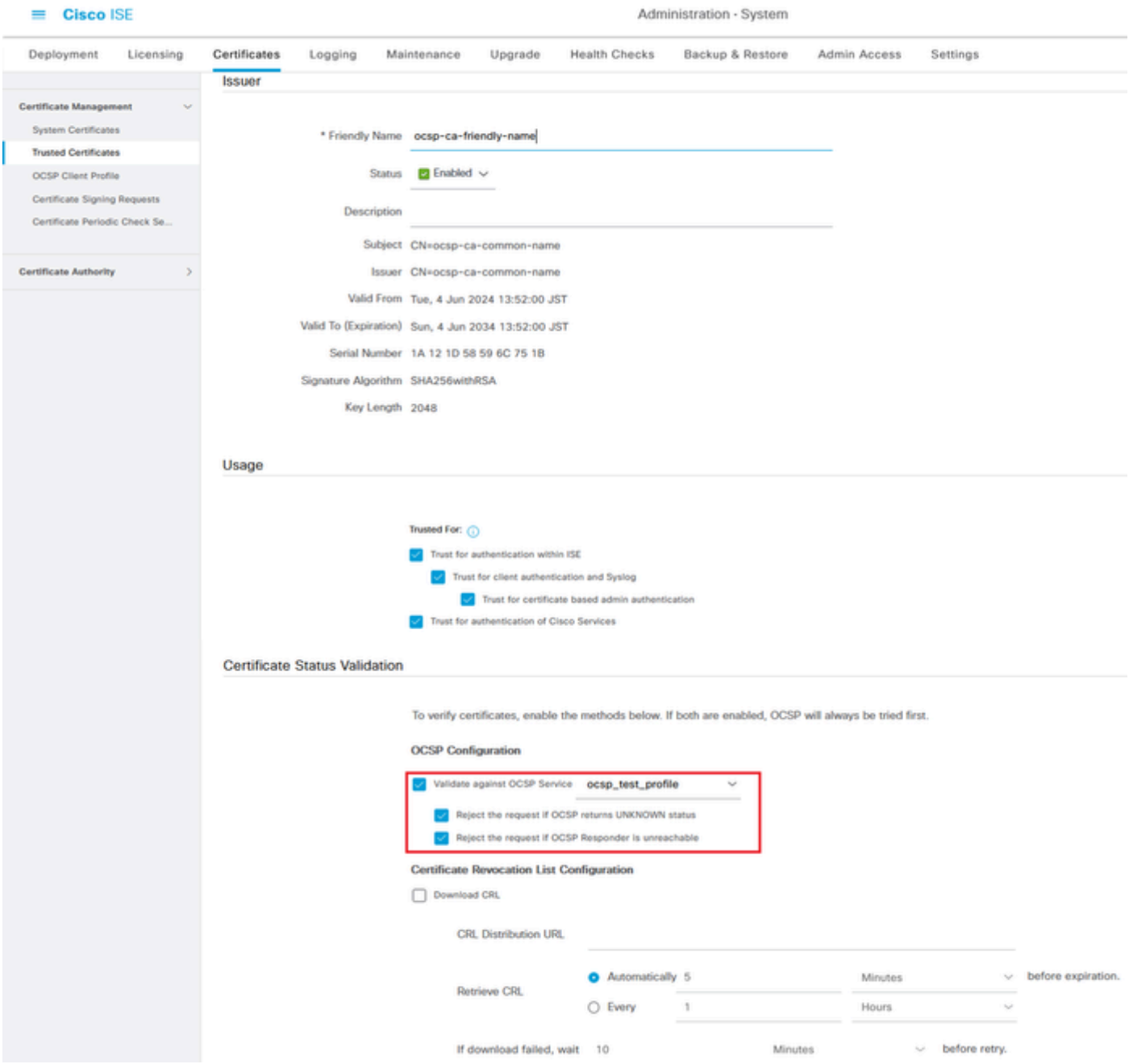
Accédez à Administration > Certificates > Trusted Certificates, confirmez que l'autorité de certification approuvée est importée vers ISE.



Autorité de certification approuvée

Vérifiez l'autorité de certification et cliquez sur le bouton Edit, entrez les détails de la configuration OCSP pour la validation de l'état du certificat.

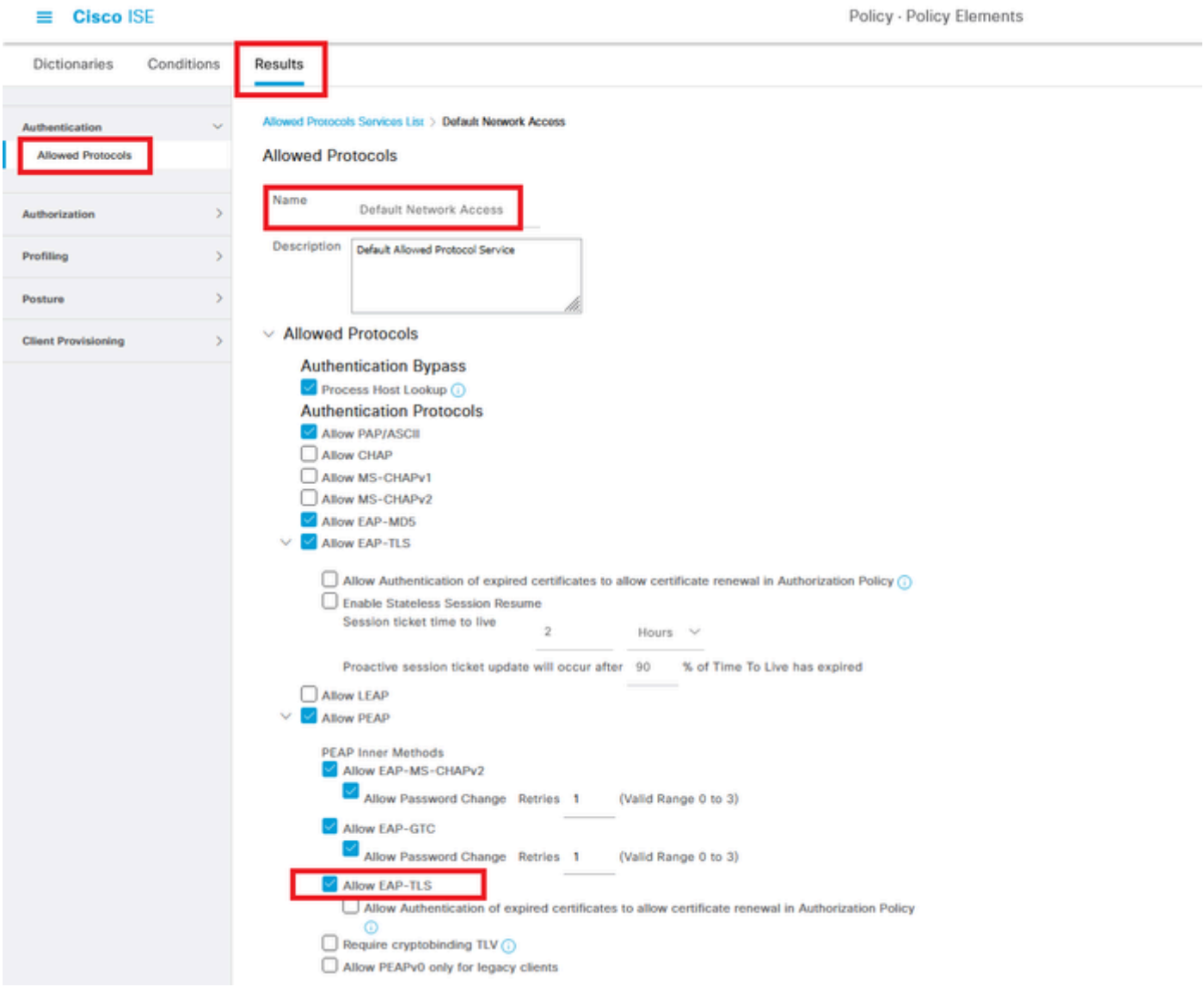
- Validation par rapport au service OCSP : ocsp_test_profile
- Rejeter la demande si OCSP renvoie l'état UNKNOWN : vérifier
- Rejeter la demande si le répondeur OCSP est inaccessible : vérifier



Validation du statut du certificat

Étape 6. Ajouter des protocoles autorisés

Accédez à Policy > Results > Authentication > Allowed Protocols, modifiez la liste de services Default Network Access et cochez la case Allow EAP-TLS.

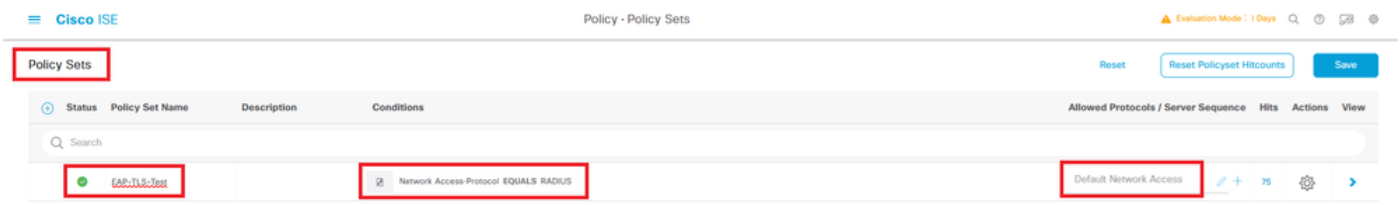


Autoriser EAP-TLS

Étape 7. Ajouter un jeu de stratégies

Accédez à Policy > Policy Sets, cliquez sur + pour ajouter un jeu de stratégies.

- Nom du jeu de stratégies : EAP-TLS-Test
- Conditions : Le protocole d'accès au réseau ÉGALE RADIUS
- Protocoles autorisés / Séquence de serveurs : Accès réseau par défaut



Ajouter un jeu de stratégies

Étape 8. Ajouter une stratégie d'authentification

Accédez à Jeux de stratégies, cliquez sur EAP-TLS-Test pour ajouter une stratégie d'authentification.

- Nom de la règle : EAP-TLS-Authentication
- Conditions : Accès réseau EAPauthentication ÉGALE EAP-TLS ET Wired_802.1 X
- Utiliser : Identity_AD

Ajouter une stratégie d'authentification

Étape 9. Ajouter une stratégie d'autorisation

Accédez à Jeux de stratégies, cliquez sur EAP-TLS-Test pour ajouter une stratégie d'autorisation.

- Nom de la règle : EAP-TLS-Authorization
- Conditions : CERTIFICAT Objet - Nom commun EQUALS clientcertCN
- Résultats : PermitAccess

Ajouter une stratégie d'autorisation

Vérifier

Étape 1. Confirmer la session d'authentification

Exécutezshow authentication sessions interface GigabitEthernet1/0/3 details la commande pour confirmer la session d'authentification dans C1000.

<#root>

Switch#

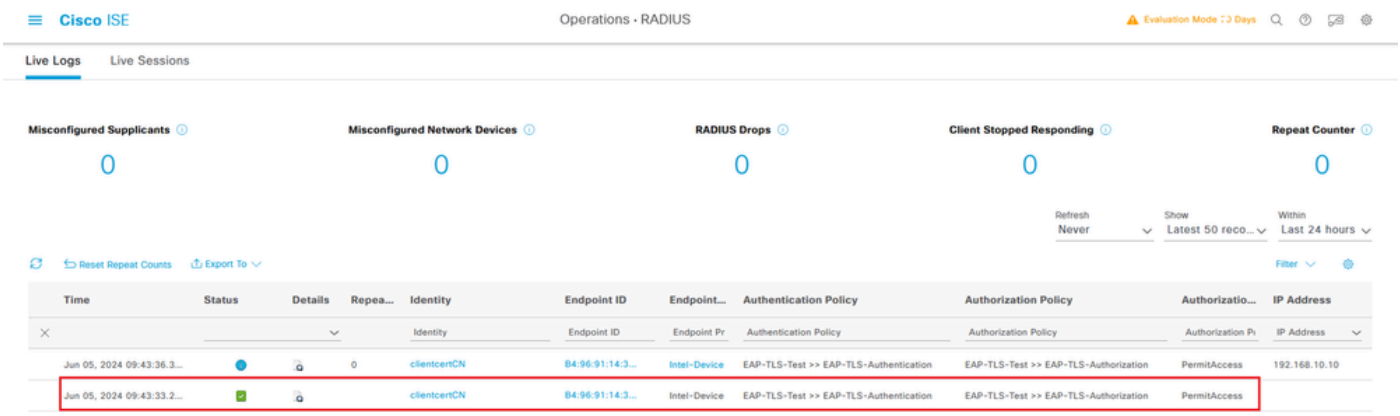
show authentication sessions interface GigabitEthernet1/0/3 details

```
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
```

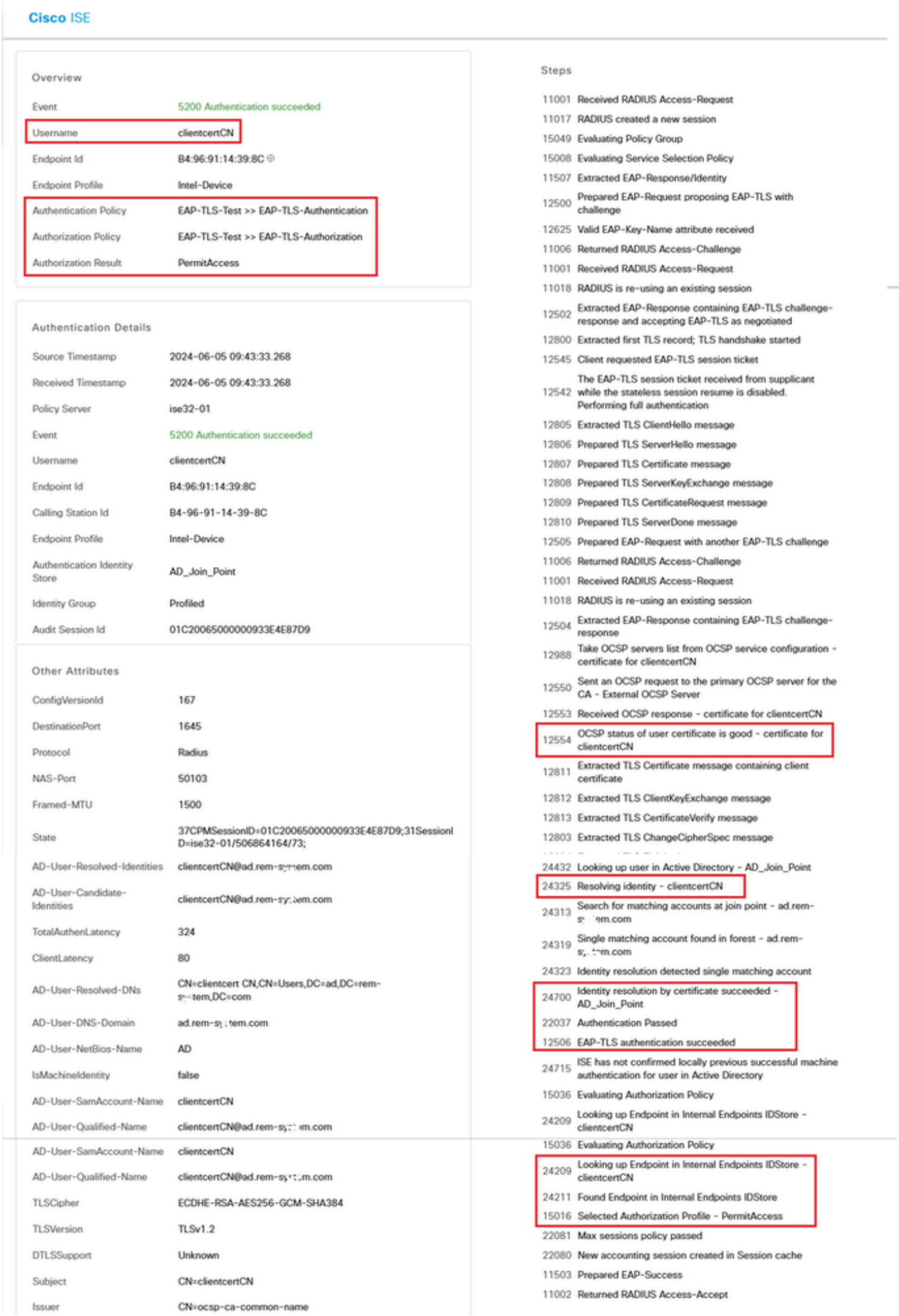
Étape 2. Confirmer le journal Radius en direct

Accédez à **Operations > RADIUS > Live Login** ISE GUI, confirmez le journal en direct pour l'authentification.



Journal Radius Live

Confirmez le journal en direct détaillé de l'authentification.



Détail de l'authentification

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
```

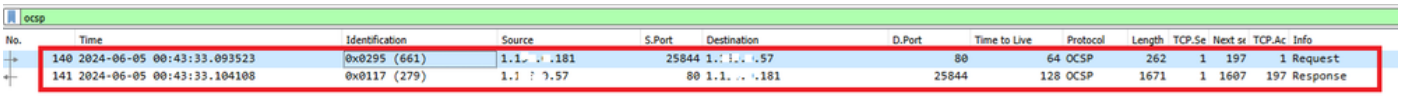
Code=5(AccountingResponse)

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

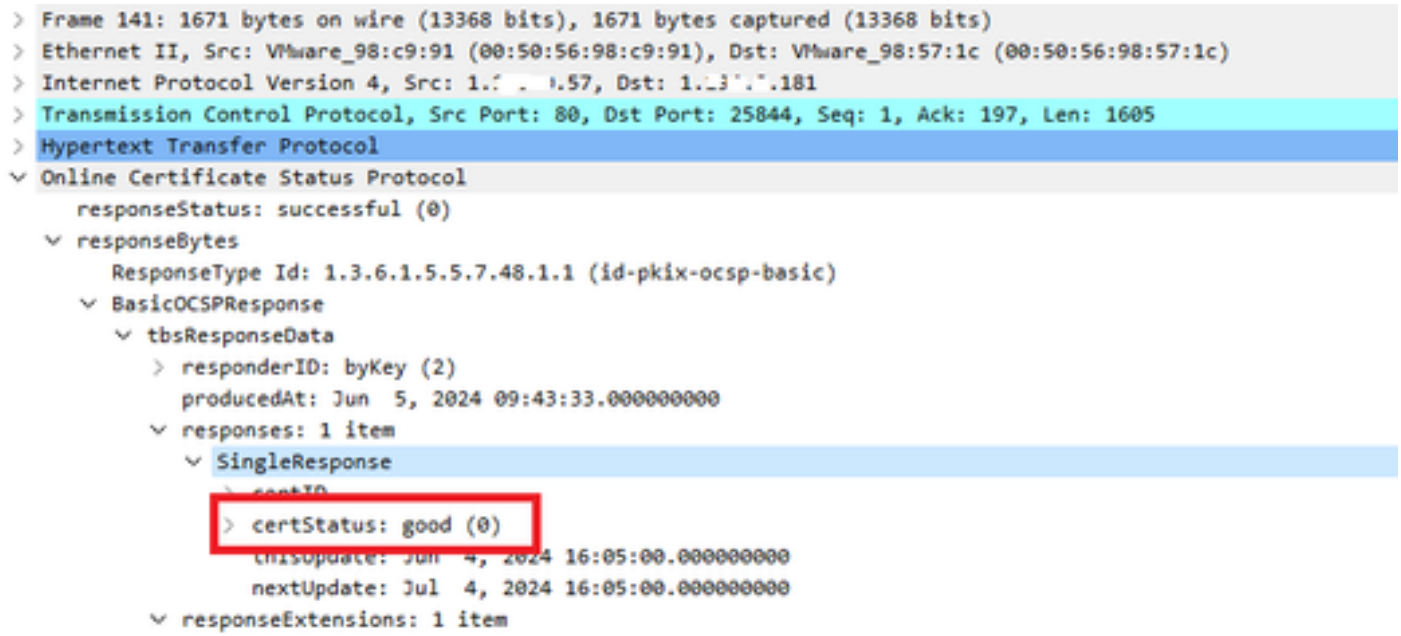
2. Dépôt TCP

Dans le dump TCP dans ISE, vous vous attendez à trouver des informations sur la réponse OCSP et la session Radius.

Requête et réponse OCSP :

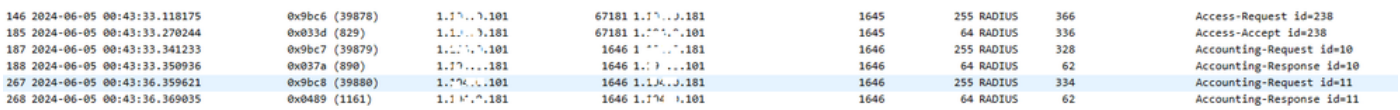


Capture de paquets de requête et réponse OCSP



Capturer les détails de la réponse OCSP

Session Radius :



Capture de paquets de session Radius

Informations connexes

Configuration de l'authentification EAP-TLS avec ISE

Configuration des certificats TLS/SSL dans ISE

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.