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

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Diagramme du réseau
- Informations générales
- Configurations
  - Configuration dans C1000
  - Configuration dans le PC Windows
    - Étape 1 : configuration de l'authentification utilisateur
    - Étape 2 : confirmation du certificat client
  - Configuration dans Windows Server
    - Étape 1. Ajout d'utilisateurs
    - Étape 2 : confirmation du service OCSP
  - Configuration dans ISE
    - Étape 1. Ajout d'un périphérique
    - Étape 2 : ajout d'Active Directory
    - Étape 3. Ajouter un profil d'authentification de certificat
    - Étape 4. Ajout de la séquence source d'identité
    - Étape 5. Confirmer le certificat dans ISE
    - Étape 6. Ajout de protocoles autorisés
    - Étape 7. Ajouter un ensemble de stratégies
    - Étape 8. Ajouter une stratégie d'authentification
    - Étape 9. Ajouter une stratégie d'autorisation
- Vérifier
  - Étape 1 : confirmation de la session d'authentification
  - Étape 2 : confirmation du journal Radius Live
- Dépannage
  - 1. Journal de débogage
  - 2. Dépôt TCP
- Informations connexes

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 (ISE)
- 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.

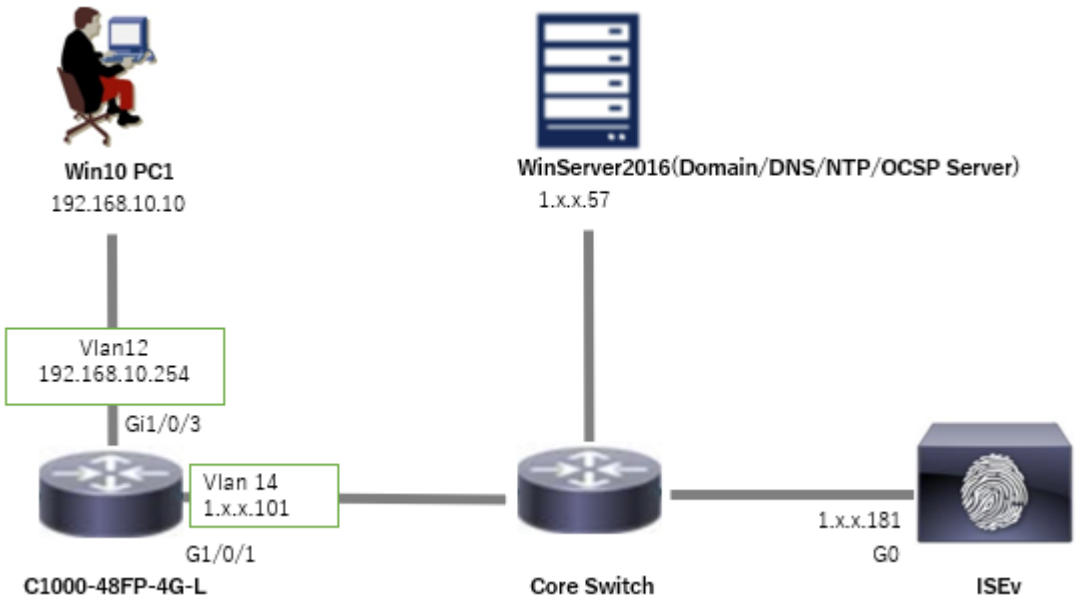


Diagramme du réseau

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 d'état de certificat en ligne, 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.

Le protocole OCSP (Online Certificate Status Protocol) et le serveur Active Directory (AD) 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-nom-commun
- 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

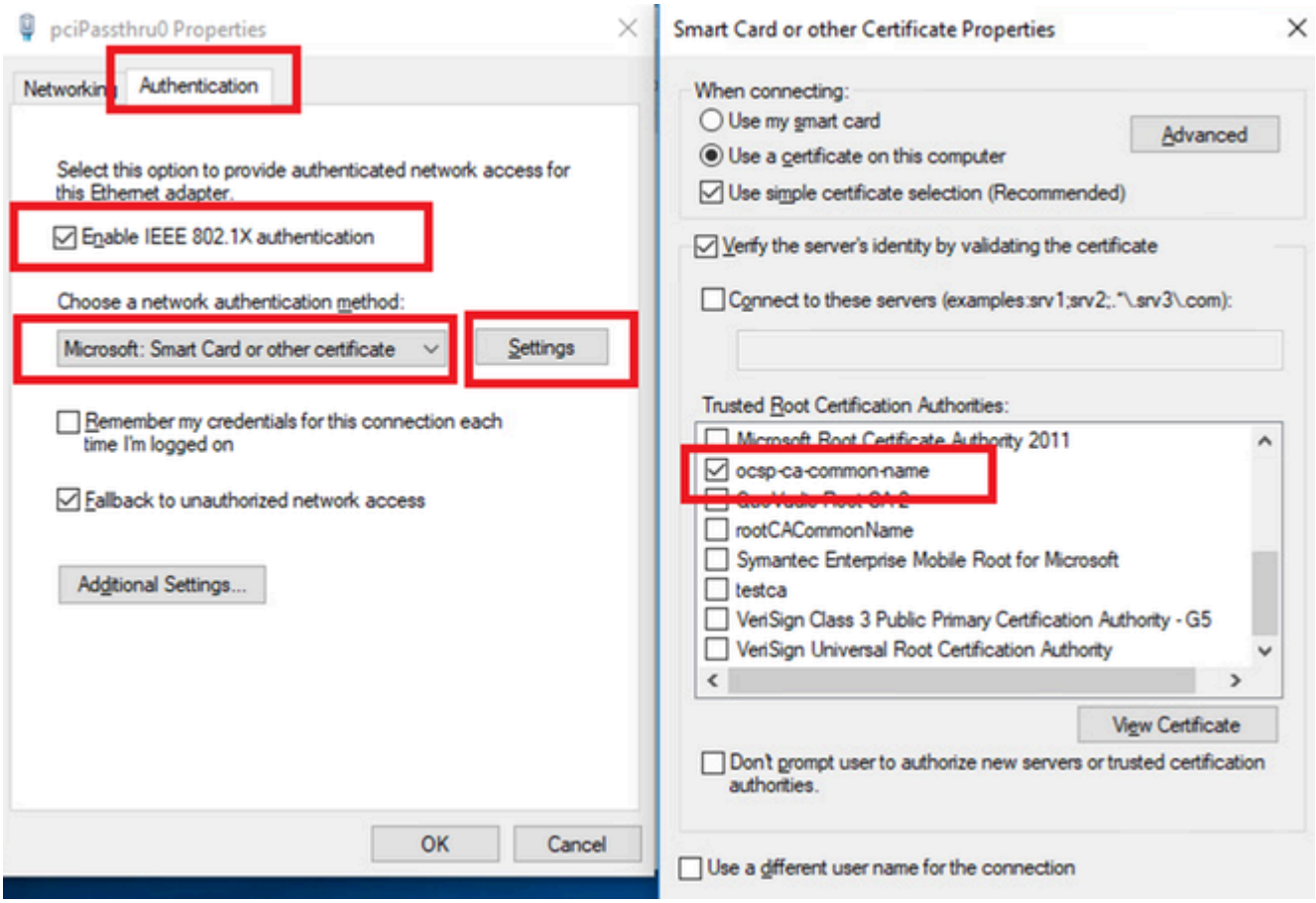
interface GigabitEthernet1/0/3
switchport access vlan 12
switchport mode access
authentication host-mode multi-auth
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge
```

Configuration dans le PC Windows

Étape 1 : configuration de l'authentification utilisateur

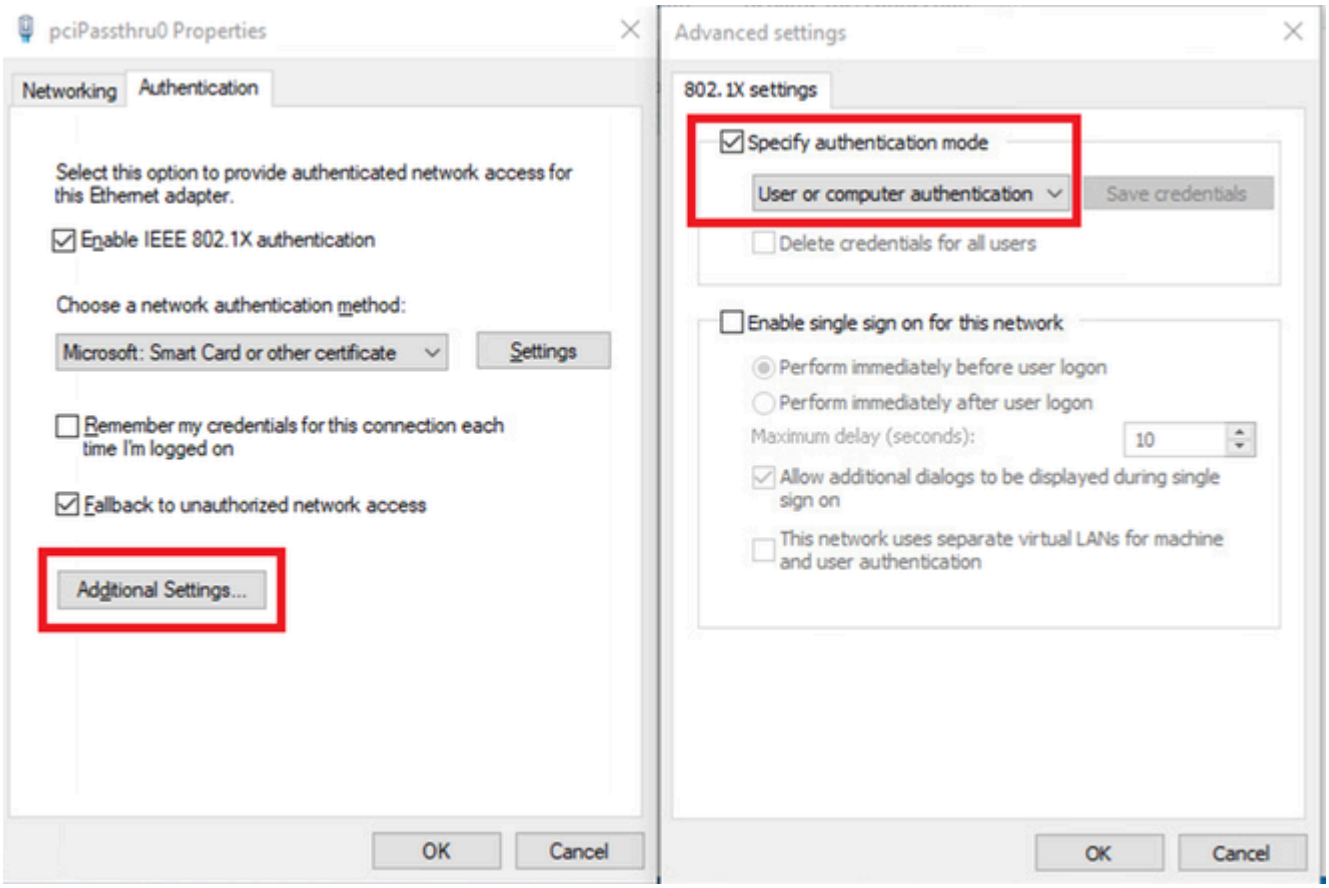
Accédez à Authentication, cochez Enable IEEE 802.1X authentication et sélectionnez Microsoft : Carte à puce ou autre certificat.

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

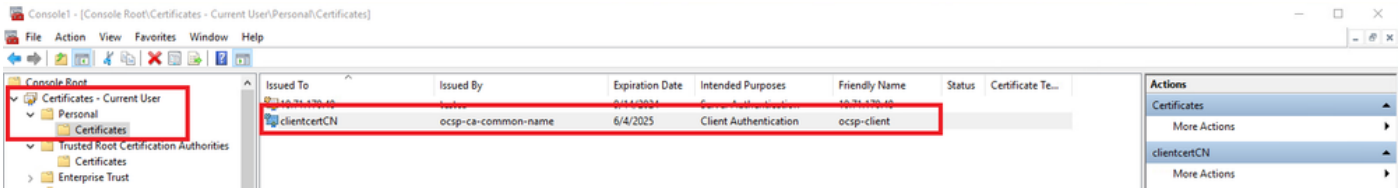
Accédez àAuthentification, cochezParamètres supplémentaires. Sélectionnez Authentification utilisateur ou ordinateur dans la liste déroulante.



Spécifier le mode d'authentification

Étape 2 : confirmation du certificat client

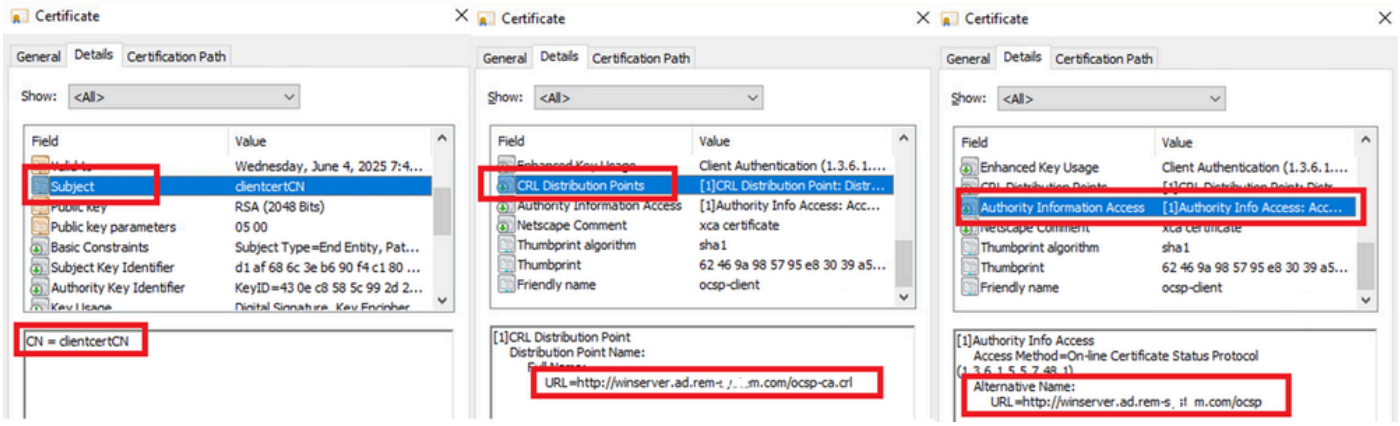
Accédez à Certificates - Current User > Personal > Certificates, et vérifiez le certificat client utilisé pour l'authentification.



Confirmer le certificat client

Double-cliquez sur le certificat client, accédez à Détails, vérifiez les détails de Objet, Points de distribution CRL, Accès aux informations d'autorité.

- 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

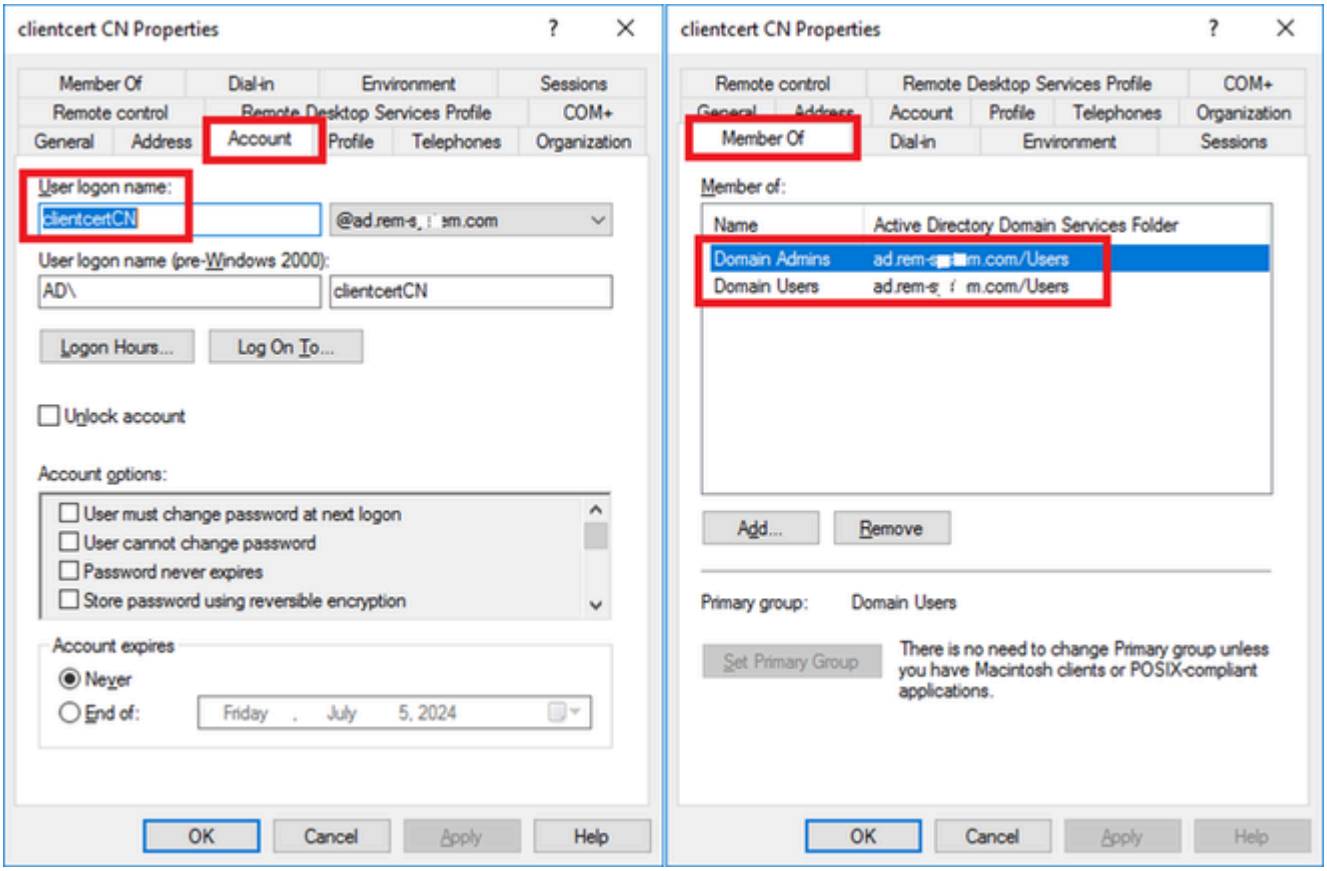


Détail du certificat client

Configuration dans Windows Server

Étape 1. Ajout d'utilisateurs

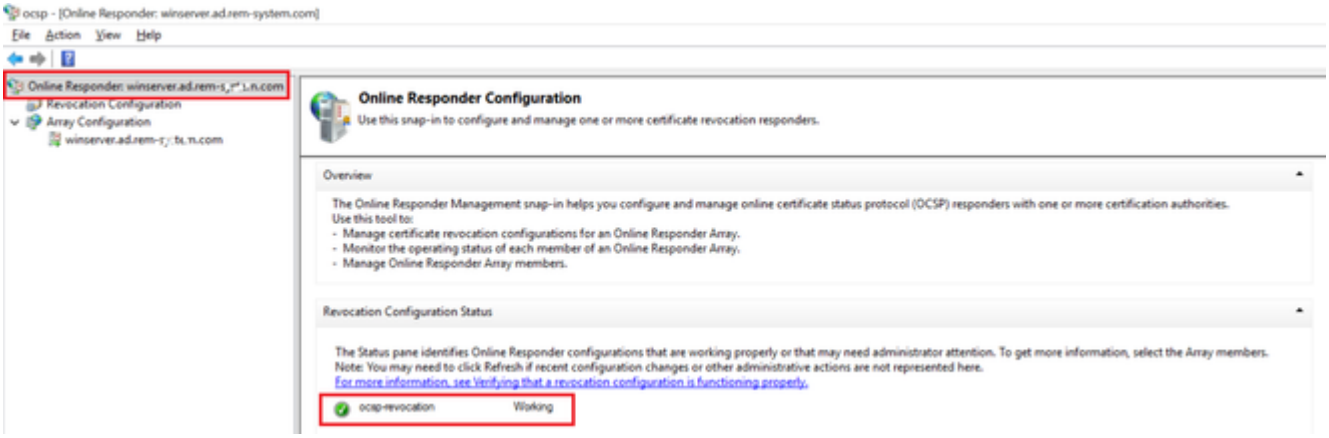
Accédez à Utilisateurs et ordinateurs Active Directory, puis cliquez surUtilisateurs. Ajoutez clientcertCN comme nom de connexion utilisateur.



Nom de connexion utilisateur

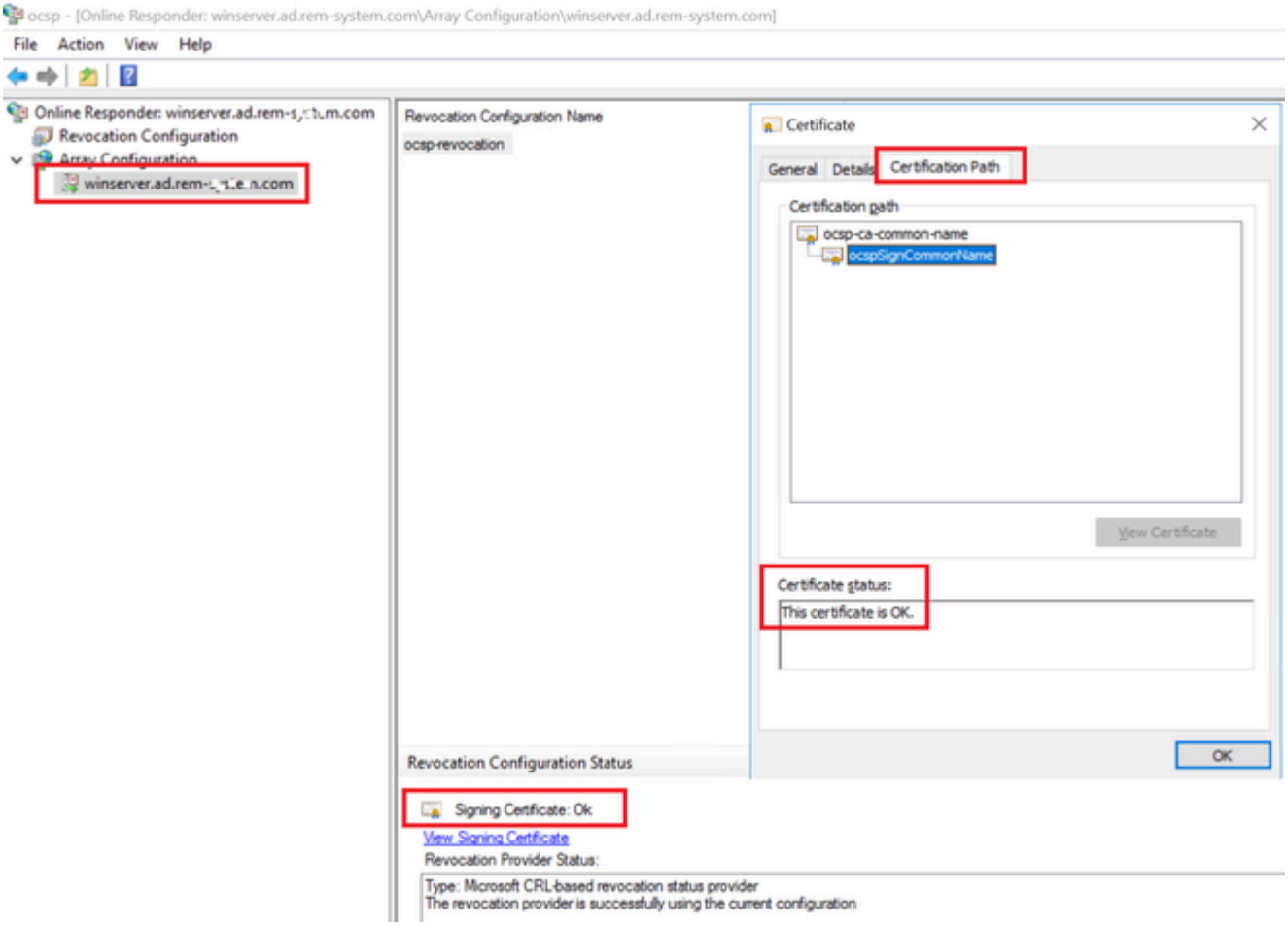
Étape 2 : confirmation du service OCSP

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.

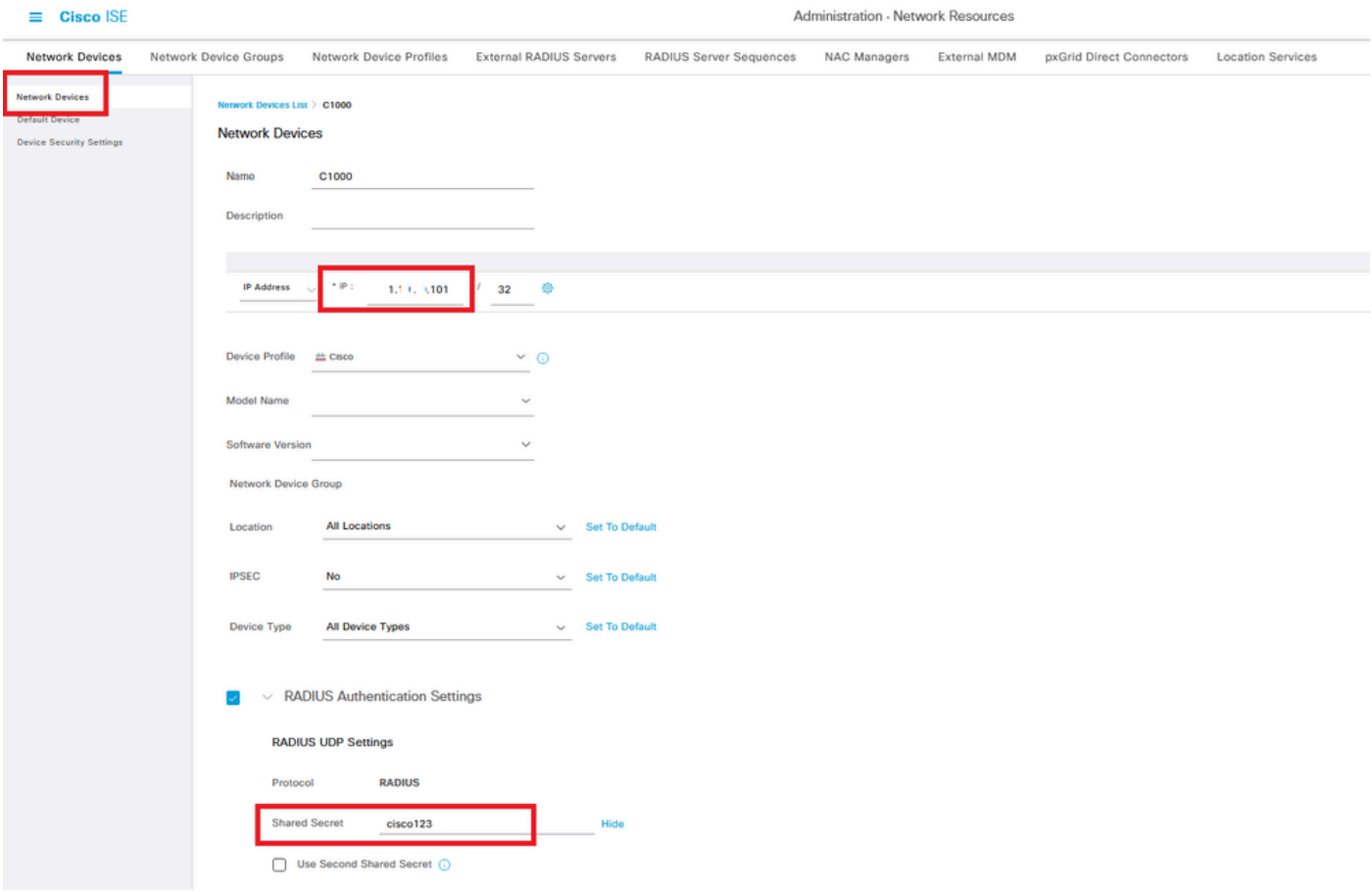


État du certificat de signature OCSP

Configuration dans ISE

Étape 1. Ajout d'un périphérique

Accédez à Administration > Network Devices, cliquez sur Addbutton pour ajouter un périphérique C1000.

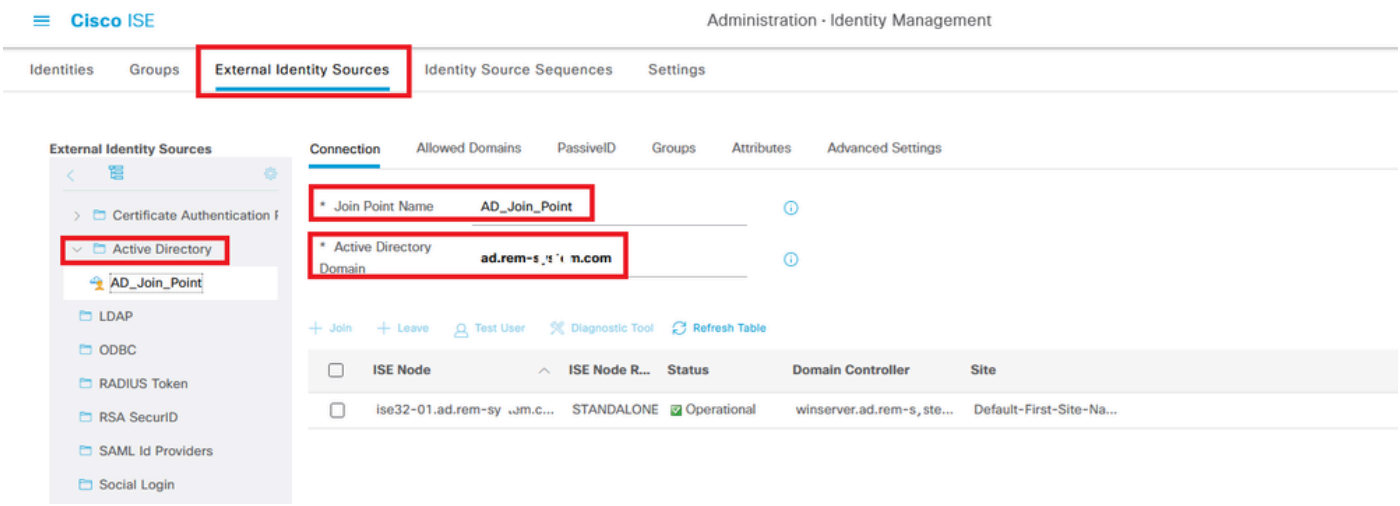


Ajouter un périphérique

Étape 2 : ajout d'Active Directory

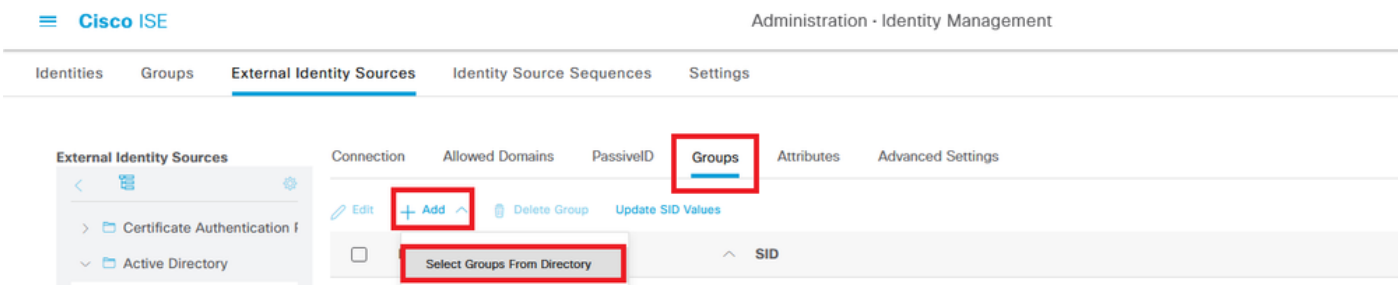
Accédez à Administration > Sources d'identité externes > Active Directory, cliquez sur l'onglet Connexion, ajoutez Active Directory à ISE.

- Nom du point de jonction : Point_Jointure_AD
- Domaine Active Directory : ad.rem-xxx.com



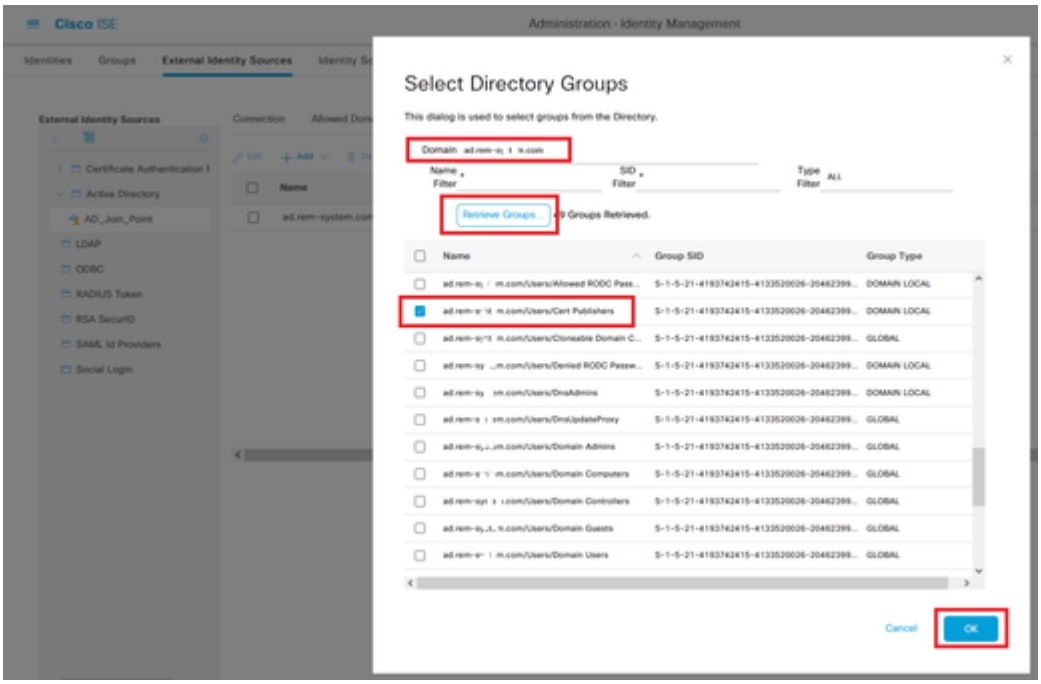
Ajouter Active Directory

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.

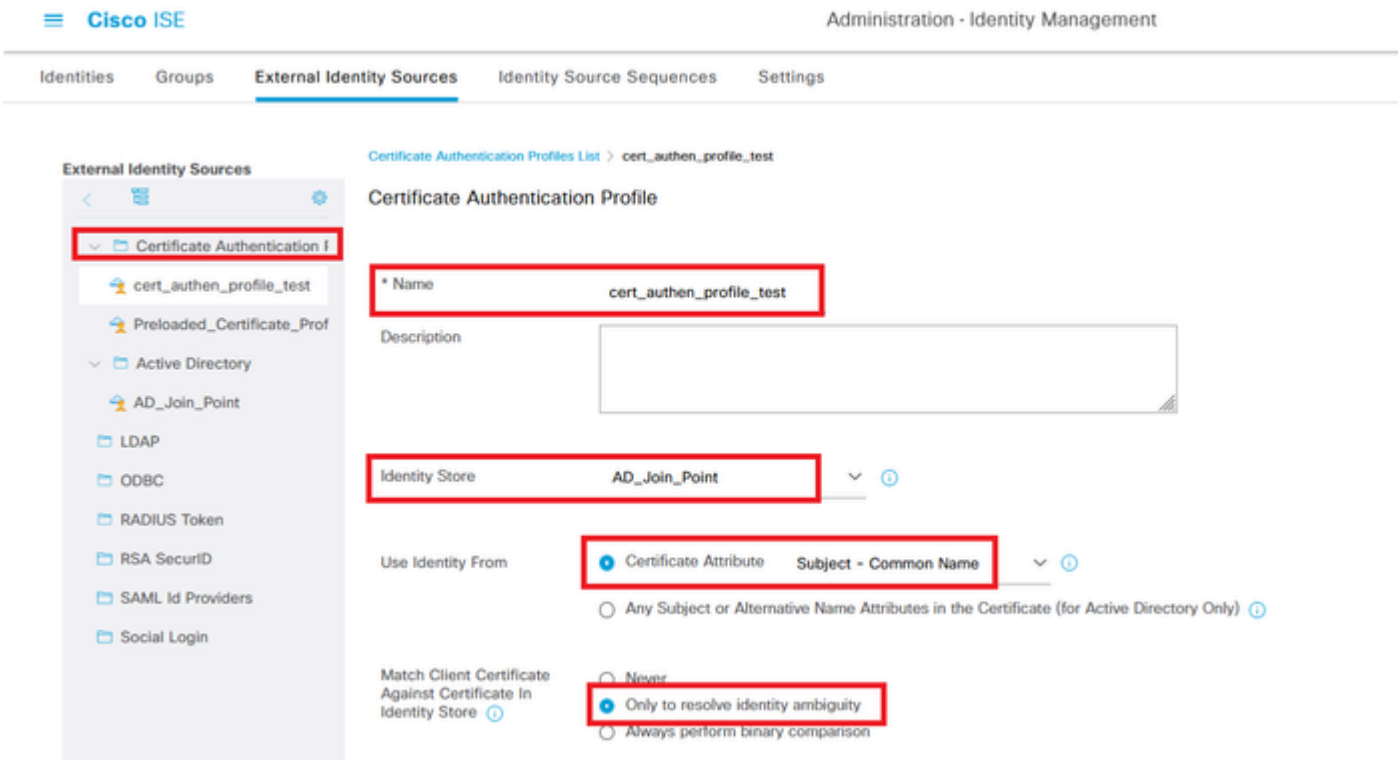


Vérifier les éditeurs de certificats

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.

- Name : cert_authen_profile_test
- Banque d'identités : Point_Jointure_AD
- Utiliser l'identité de l'attribut de certificat : Objet - Nom commun.
- Faire Correspondre Le Certificat Client Au Certificat Dans Le Magasin D'Identités : Uniquement pour résoudre l'ambiguïté d'identité.

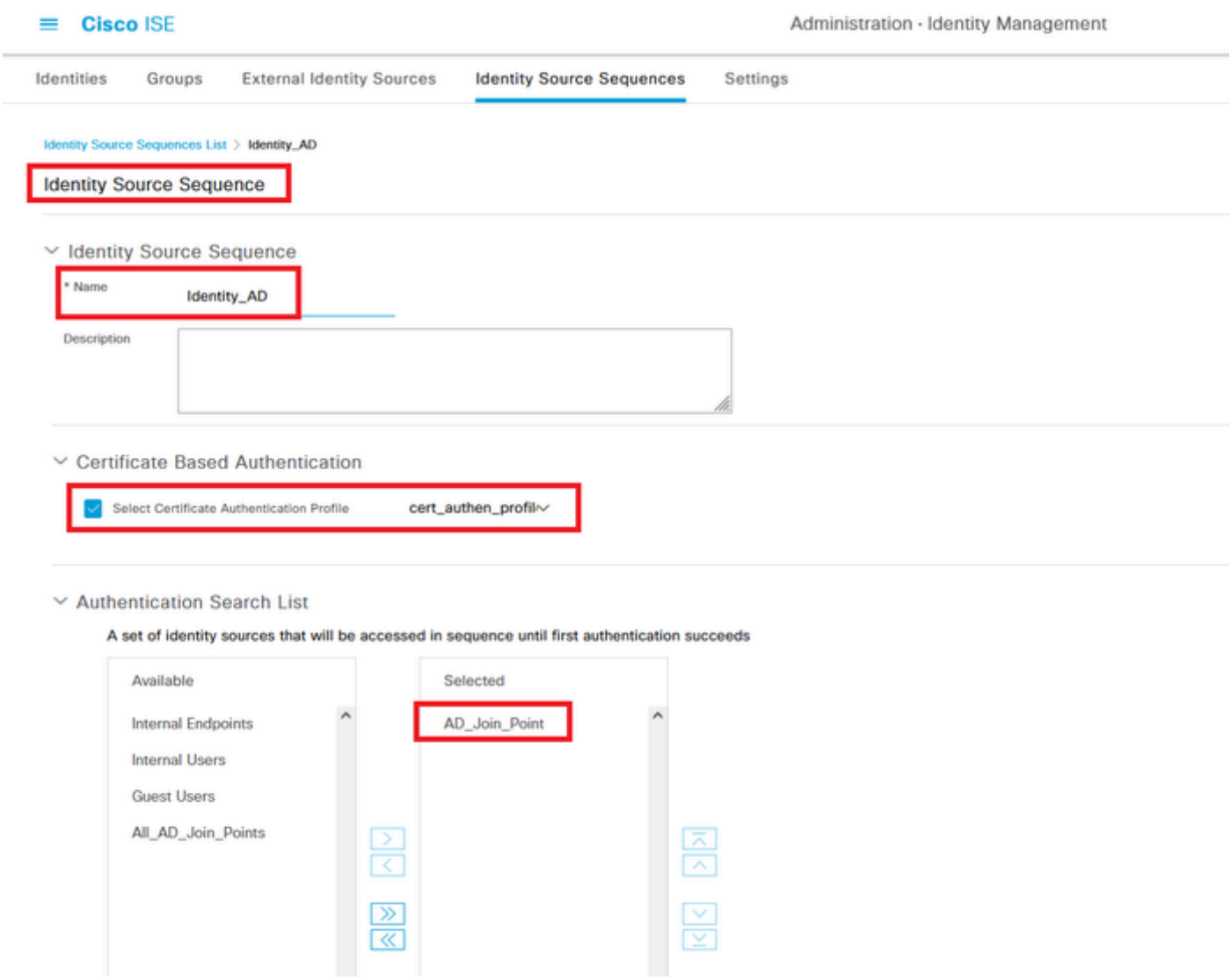


Ajouter un profil d'authentification de certificat

Étape 4. Ajout de la séquence source d’identité

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

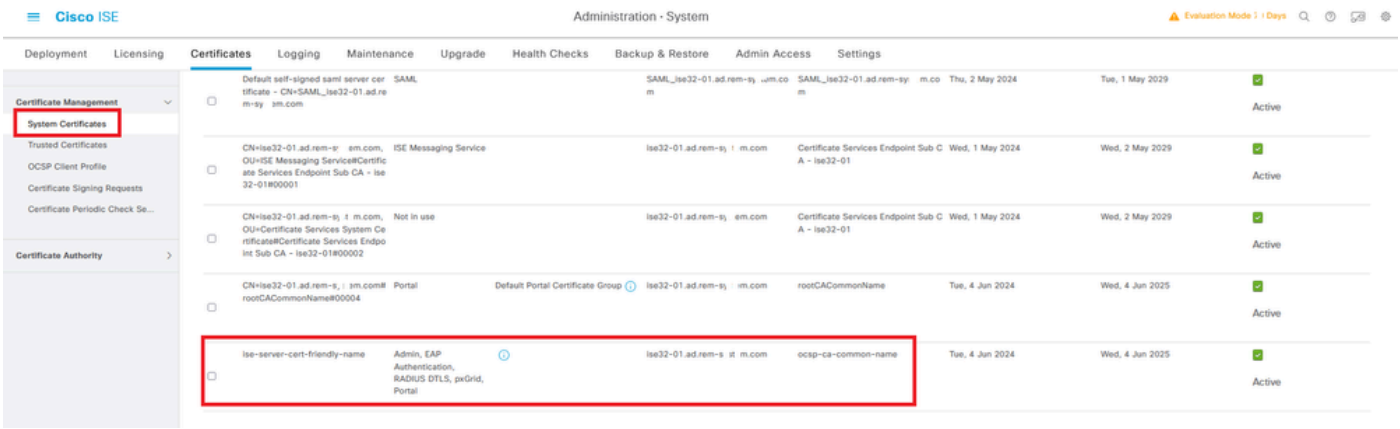
- Name : Identité_AD
- Sélectionnez Certificate Authentication Profile: cert_authen_profile_test
- Liste de recherche d'authentification : Point_Jointure_AD



Ajouter des séquences source d'identité

Étape 5. Confirmation du certificat dans ISE

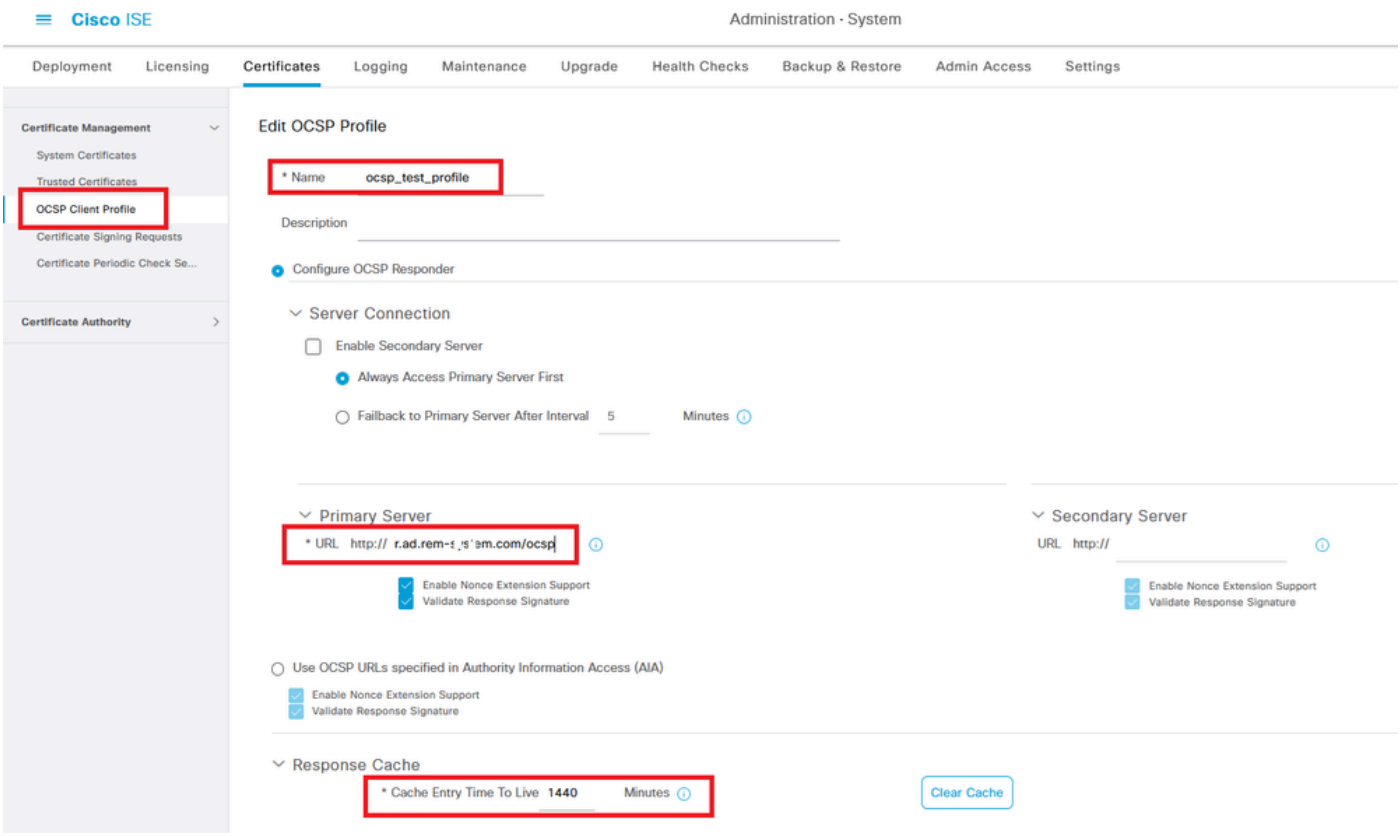
Accédez à Administration > Certificates > System Certificates, confirmez que le certificat du serveur est signé par l'autorité de certification approuvée.



certificat du serveur

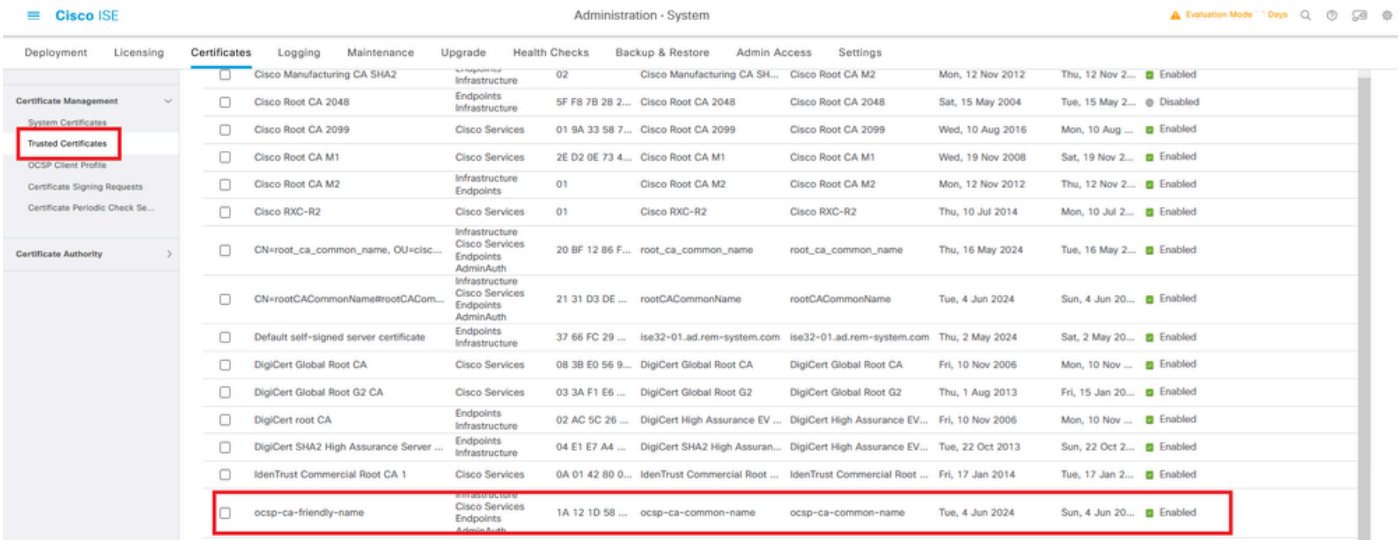
Accédez à Administration > Certificates > OCSP Client Profile, cliquez sur Add button to add a new OCSP client profile.

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



Profil du client OCSP

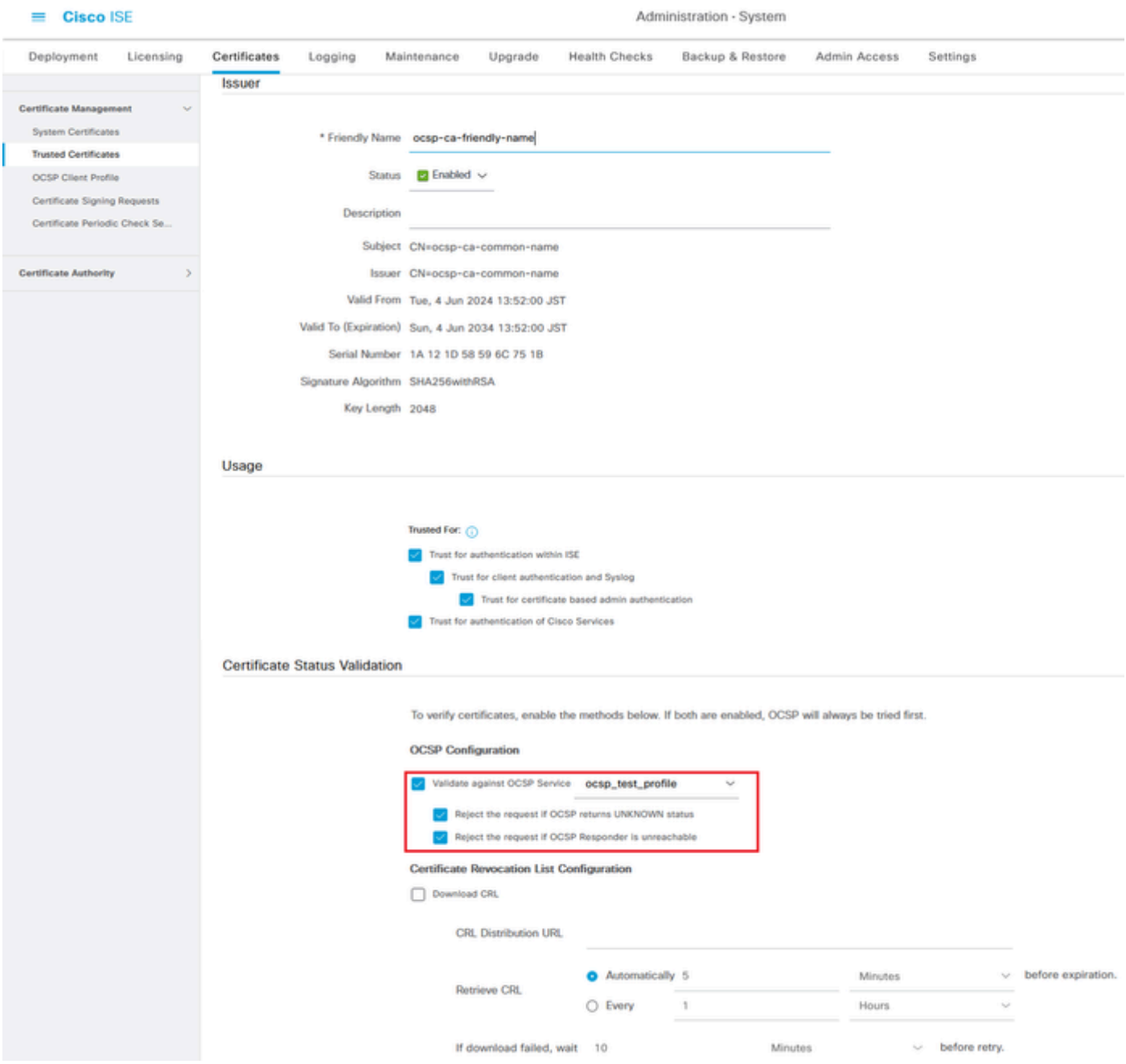
Accédez à Administration > Certificates > Trusted Certificates, confirmez que l'autorité de certification approuvée est importée vers ISE.



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.

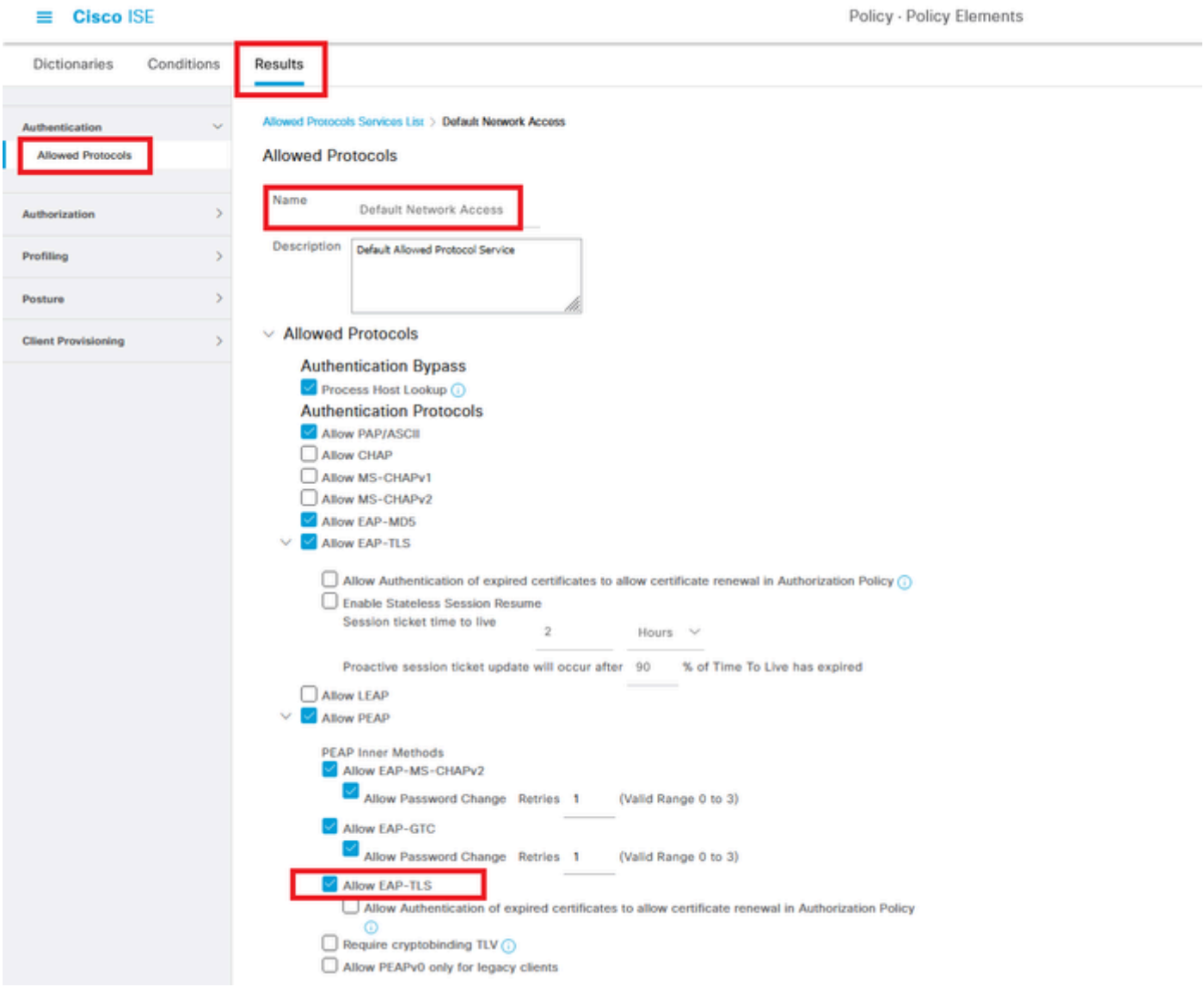
- Valider par rapport au service OCSP : ocsp_test_profile
- Rejeter la demande si OCSP renvoie l'état UNKNOWN : chèque
- Rejeter la demande si le répondeur OCSP est inaccessible : chèque



Validation du statut du certificat

Étape 6. Ajout de protocoles autorisés

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

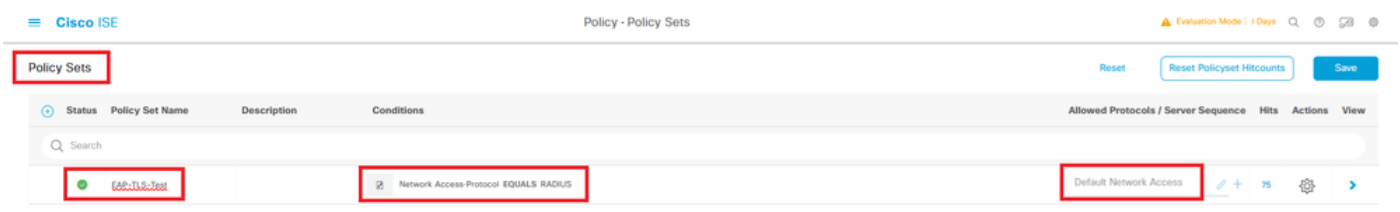


Autoriser EAP-TLS

Étape 7. Ajouter un ensemble de stratégies

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

- Nom du jeu de stratégies : EAP-TLS-Test
- Modalités: Protocole d'accès réseau EQUALS 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 : Authentification EAP-TLS
- Modalités: 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 : AutoriserAccès



Ajouter une stratégie d'autorisation

Vérifier

Étape 1 : confirmation de la session d’authentification

Exécutez`show 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)

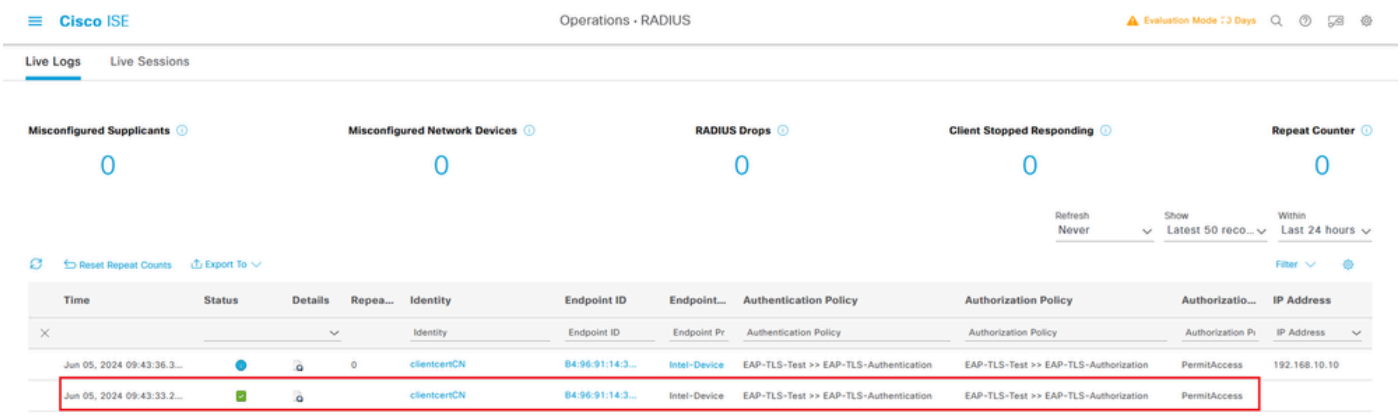
Server Policies:


Method status list:
Method State

dot1x Authc Success
```

Étape 2 : confirmation du journal Radius Live

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



Confirmez le journal en direct détaillé de l'authentification.

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

Dépannage

1. Journal de débogage

Ce journal de débogage (prrt-server.log) vous aide à confirmer le comportement détaillé de l'authentification dans ISE.

- runtime-AAA

<#root>

```
// OCSP request and response
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

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

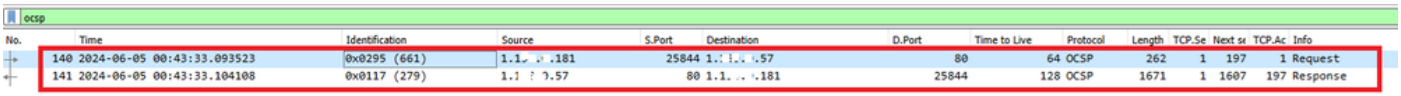
Code=5(AccountingResponse)

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

2. Dépôt TCP

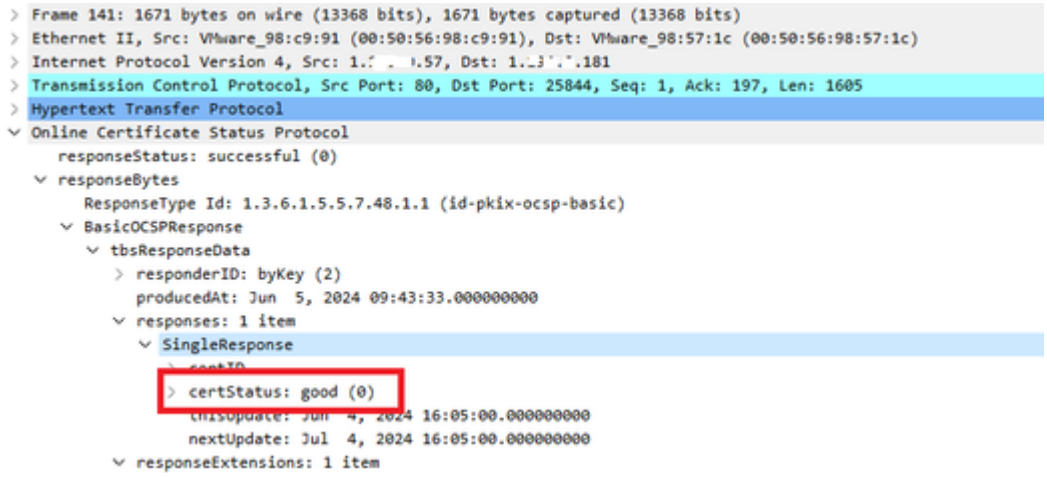
Dans le dump TCP dans ISE, vous vous attendez à trouver des informations sur la réponse OCSP et la session Radius.

Requête et réponse OCSP :



No.	Time	Identification	Source	S.Port	Destination	D.Port	Time to Live	Protocol	Length	TCP.Se	Next se	TCP.Ac	Info
140	2024-06-05 00:43:33.093523	0x0295 (661)	1.1[illegible].181	25844	1.[illegible].57	80	64	OCSP	262	1	197	1	Request
141	2024-06-05 00:43:33.104108	0x0117 (279)	1.1[illegible].57	80	1.1[illegible].181	25844	128	OCSP	1671	1	1607	197	Response

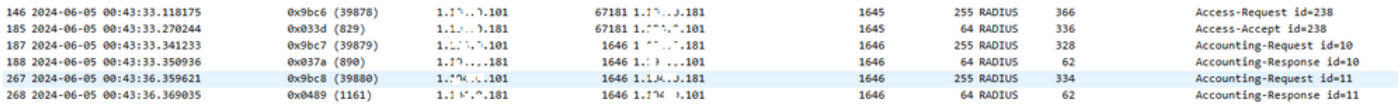
Capture de paquets de requête et de réponse OCSP



```
> 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.[illegible].57, Dst: 1.[illegible].181
> Transmission Control Protocol, Src Port: 80, Dst Port: 25844, Seq: 1, Ack: 197, Len: 1605
> Hypertext Transfer Protocol
v Online Certificate Status Protocol
    responseStatus: successful (0)
  v responseBytes
      ResponseType Id: 1.3.6.1.5.5.7.48.1.1 (id-pkix-ocsp-basic)
    v BasicOCSPResponse
      v tbsResponseData
        > responderID: byKey (2)
          producedAt: Jun  5, 2024 09:43:33.000000000
        v responses: 1 item
          v SingleResponse
            > certID
            > certStatus: good (0)
              thisUpdate: Jun  4, 2024 16:05:00.000000000
              nextUpdate: Jul  4, 2024 16:05:00.000000000
        v responseExtensions: 1 item
```

Capturer les détails de la réponse OCSP

Session Radius :



146	2024-06-05 00:43:33.118175	0x9bc6 (39878)	1.[illegible].101	67181	1.[illegible].181	1645	255	RADIUS	366	Access-Request id=238
185	2024-06-05 00:43:33.270244	0x033d (829)	1.1[illegible].181	67181	1.[illegible].101	1645	64	RADIUS	336	Access-Accept id=238
187	2024-06-05 00:43:33.341233	0x9bc7 (39879)	1.[illegible].101	1646	1.[illegible].181	1646	255	RADIUS	328	Accounting-Request id=10
188	2024-06-05 00:43:33.350936	0x037a (890)	1.[illegible].181	1646	1.[illegible].101	1646	64	RADIUS	62	Accounting-Response id=10
267	2024-06-05 00:43:36.359621	0x9bc8 (39880)	1.[illegible].101	1646	1.[illegible].181	1646	255	RADIUS	334	Accounting-Request id=11
268	2024-06-05 00:43:36.369035	0x0489 (1161)	1.1[illegible].181	1646	1.[illegible].101	1646	64	RADIUS	62	Accounting-Response id=11

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.