

Configurazione dell'autenticazione EAP-TLS con OCSP in ISE

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Esempio di rete](#)

[Premesse](#)

[Configurazioni](#)

[Configurazione in C1000](#)

[Configurazione in un PC Windows](#)

[Passaggio 1. Configura autenticazione utente](#)

[Passaggio 2. Conferma certificato client](#)

[Configurazione in Windows Server](#)

[Passaggio 1. Aggiungi utenti](#)

[Passaggio 2. Conferma servizio OCSP](#)

[Configurazione in ISE](#)

[Passaggio 1. Aggiungi dispositivo](#)

[Passaggio 2. Aggiungi Active Directory](#)

[Passaggio 3. Aggiungi profilo di autenticazione certificato](#)

[Passaggio 4. Aggiungi sequenza di origine identità](#)

[Passaggio 5. Conferma certificato in ISE](#)

[Passaggio 6. Aggiungi protocolli consentiti](#)

[Passaggio 7. Aggiungi set di criteri](#)

[Passaggio 8. Aggiungi criterio di autenticazione](#)

[Passaggio 9. Aggiungi criterio di autorizzazione](#)

[Verifica](#)

[Passaggio 1. Conferma sessione di autenticazione](#)

[Passaggio 2. Conferma registro dinamico Radius](#)

[Risoluzione dei problemi](#)

[1. Registro di debug](#)

[2. Dump TCP](#)

[Informazioni correlate](#)

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

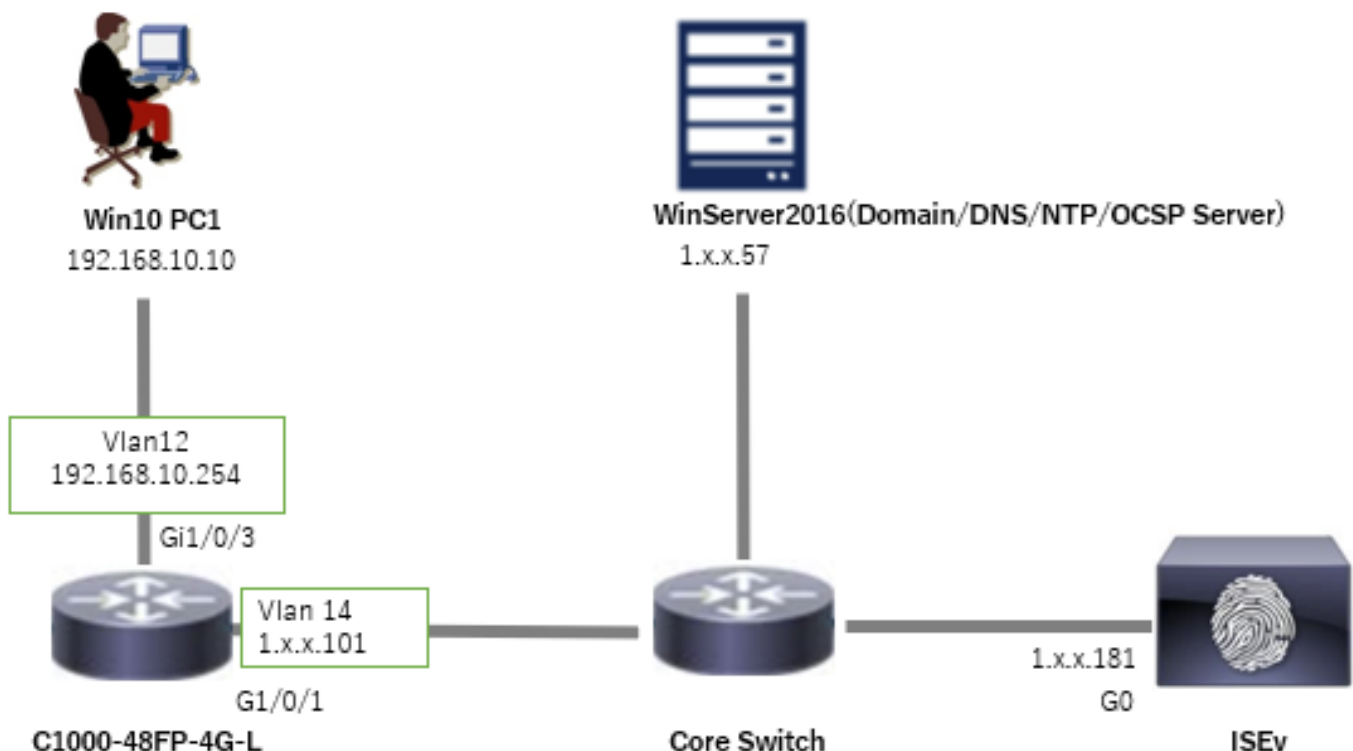
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- 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
```

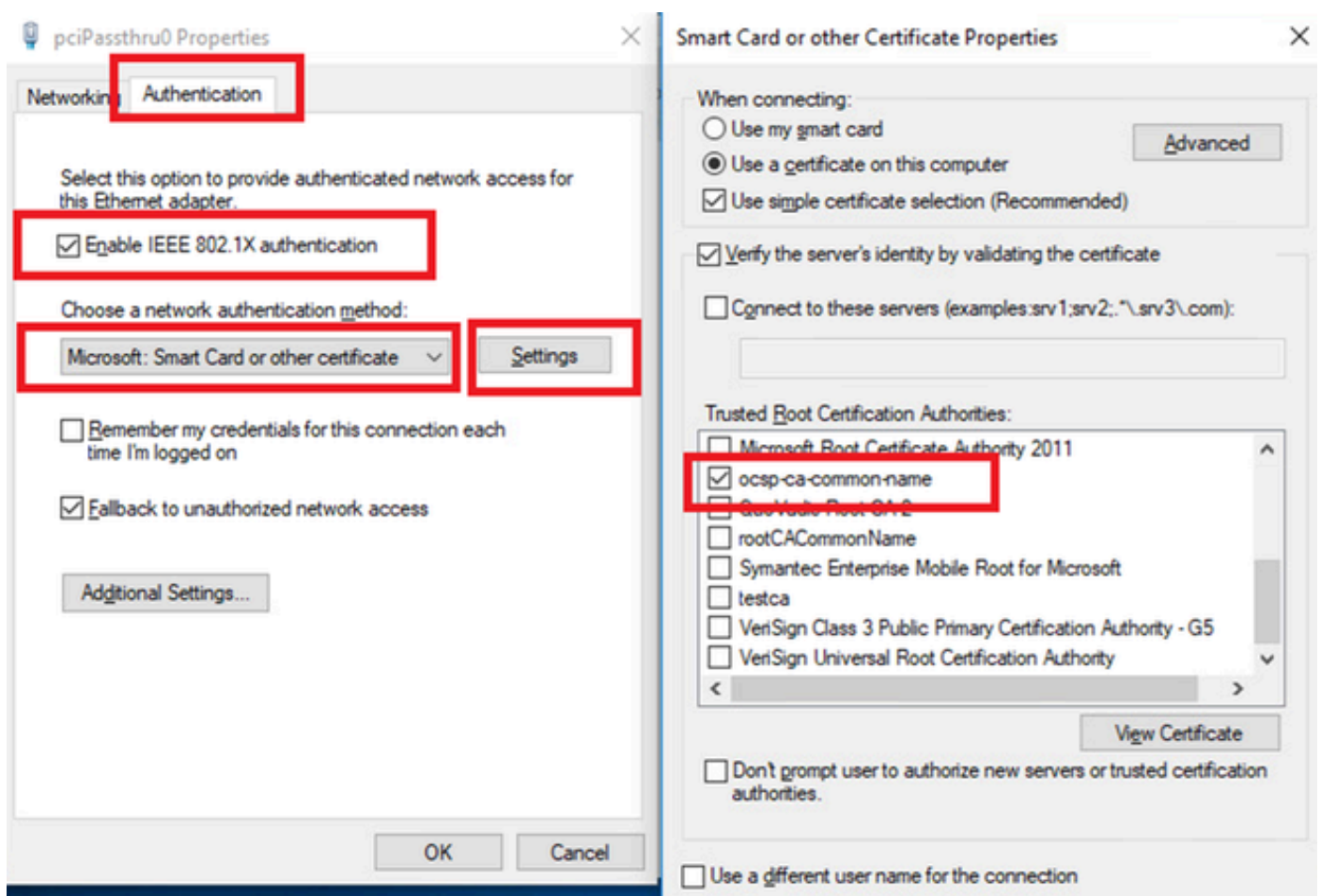
```
interface GigabitEthernet1/0/3
switchport access vlan 12
switchport mode access
authentication host-mode multi-auth
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge
```

Configurazione in un PC Windows

Passaggio 1. Configura autenticazione utente

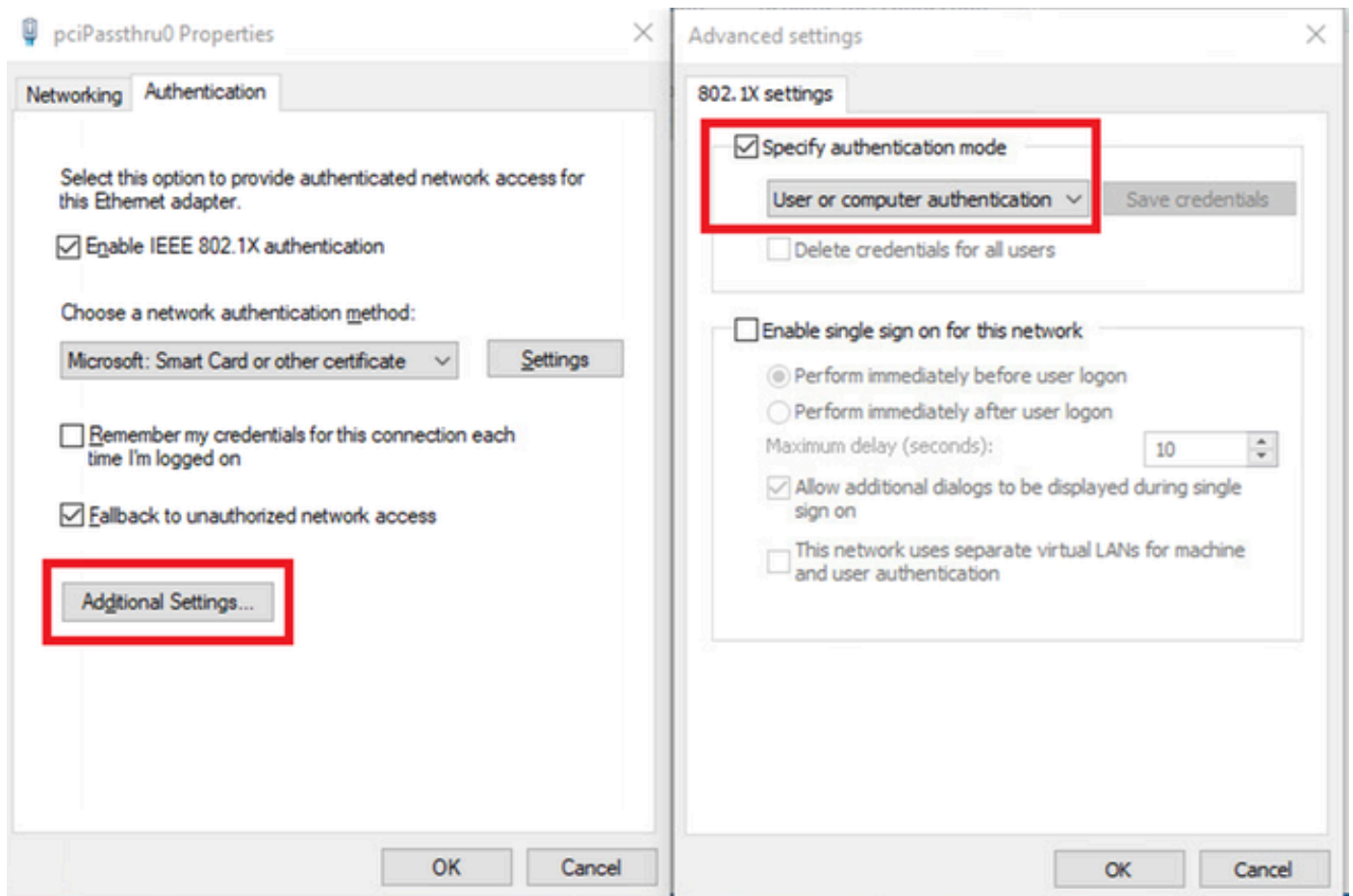
Passare a Autenticazione, selezionare Abilita autenticazione IEEE 802.1X e selezionare Microsoft: Smart Card o altro certificato.

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



Abilita autenticazione certificato

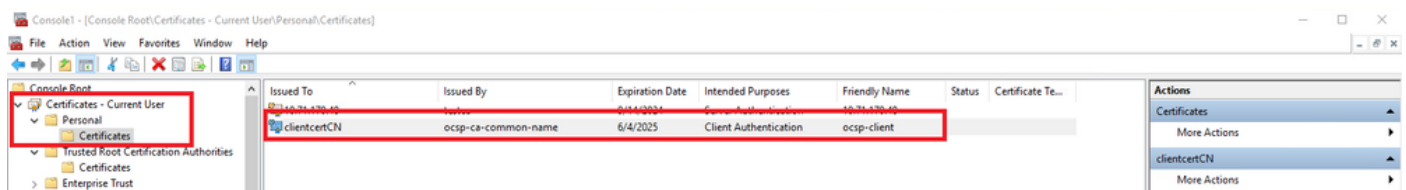
Passare a Autenticazione, selezionare Impostazioni aggiuntive. Selezionare Autenticazione utente o computer dall'elenco a discesa.



Specifica modalità di autenticazione

Passaggio 2. Conferma certificato client

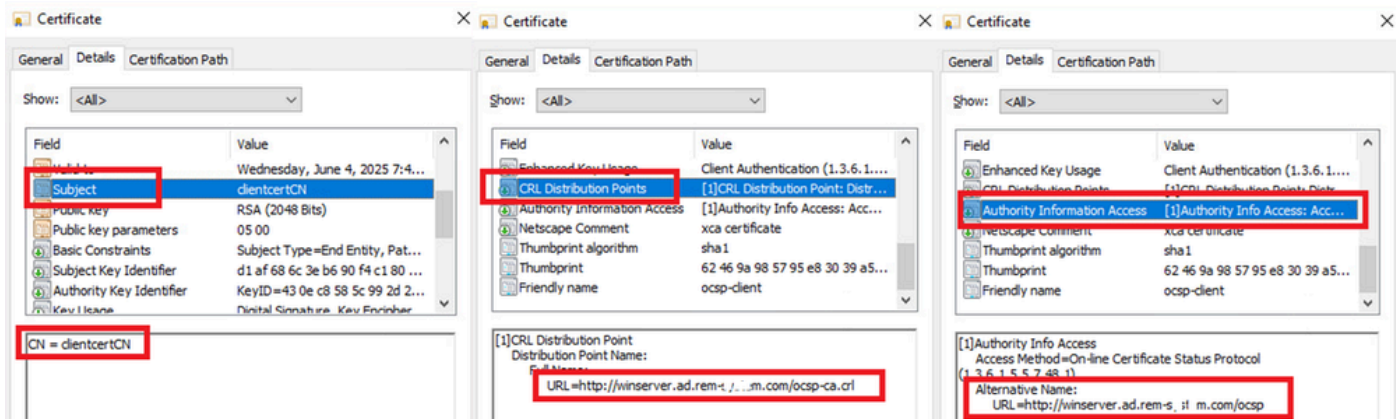
Passare a Certificati - Utente corrente > Personale > Certificati e verificare il certificato client utilizzato per l'autenticazione.



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>

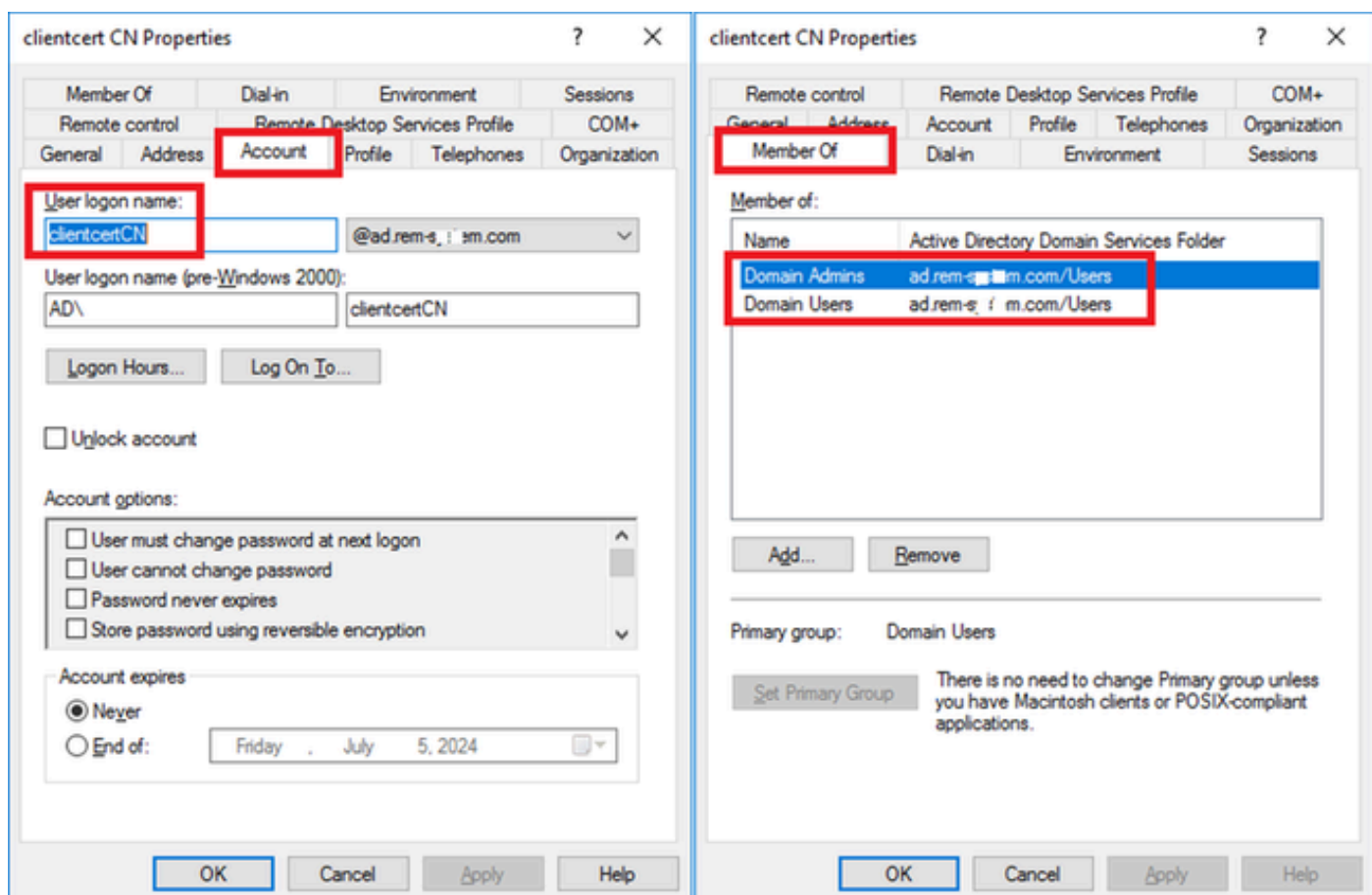


Dettagli del certificato client

Configurazione in Windows Server

Passaggio 1. Aggiungi utenti

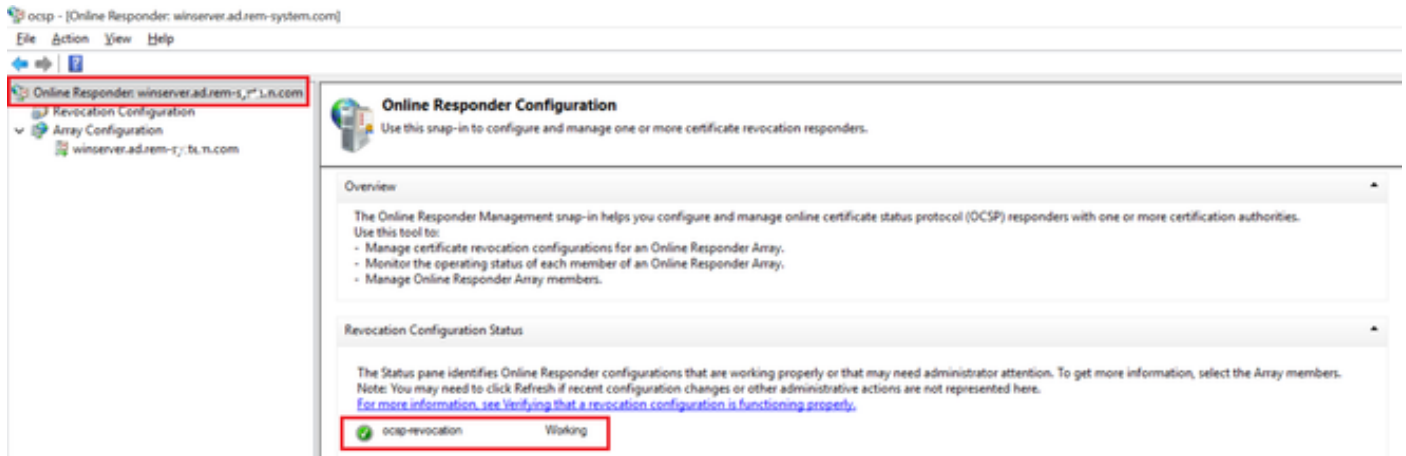
Passare a Utenti e computer di Active Directory, quindi fare clic su Utenti. Aggiungere clientcertCN come nome di accesso utente.



Nome di accesso utente

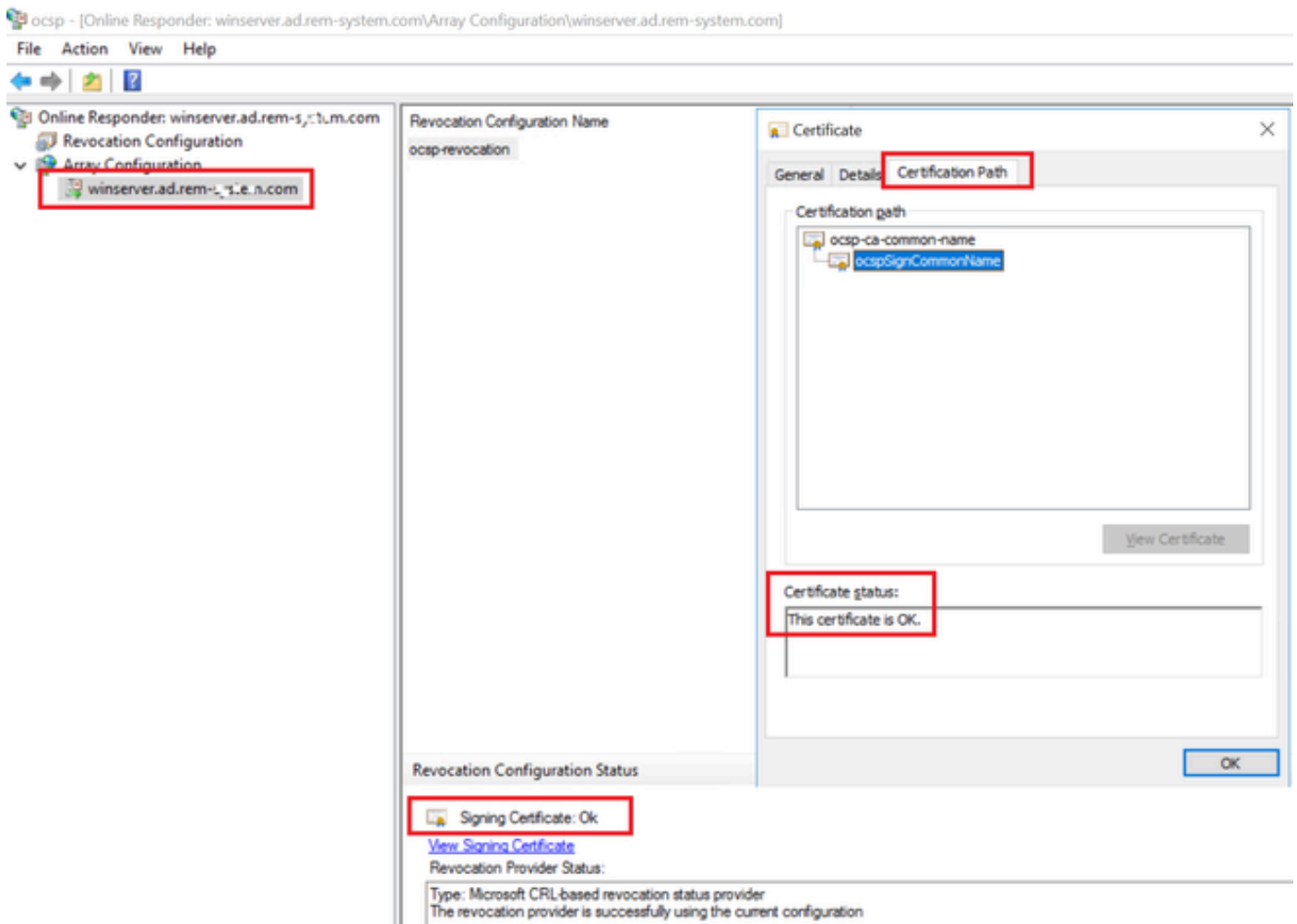
Passaggio 2. Conferma servizio OCSP

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.



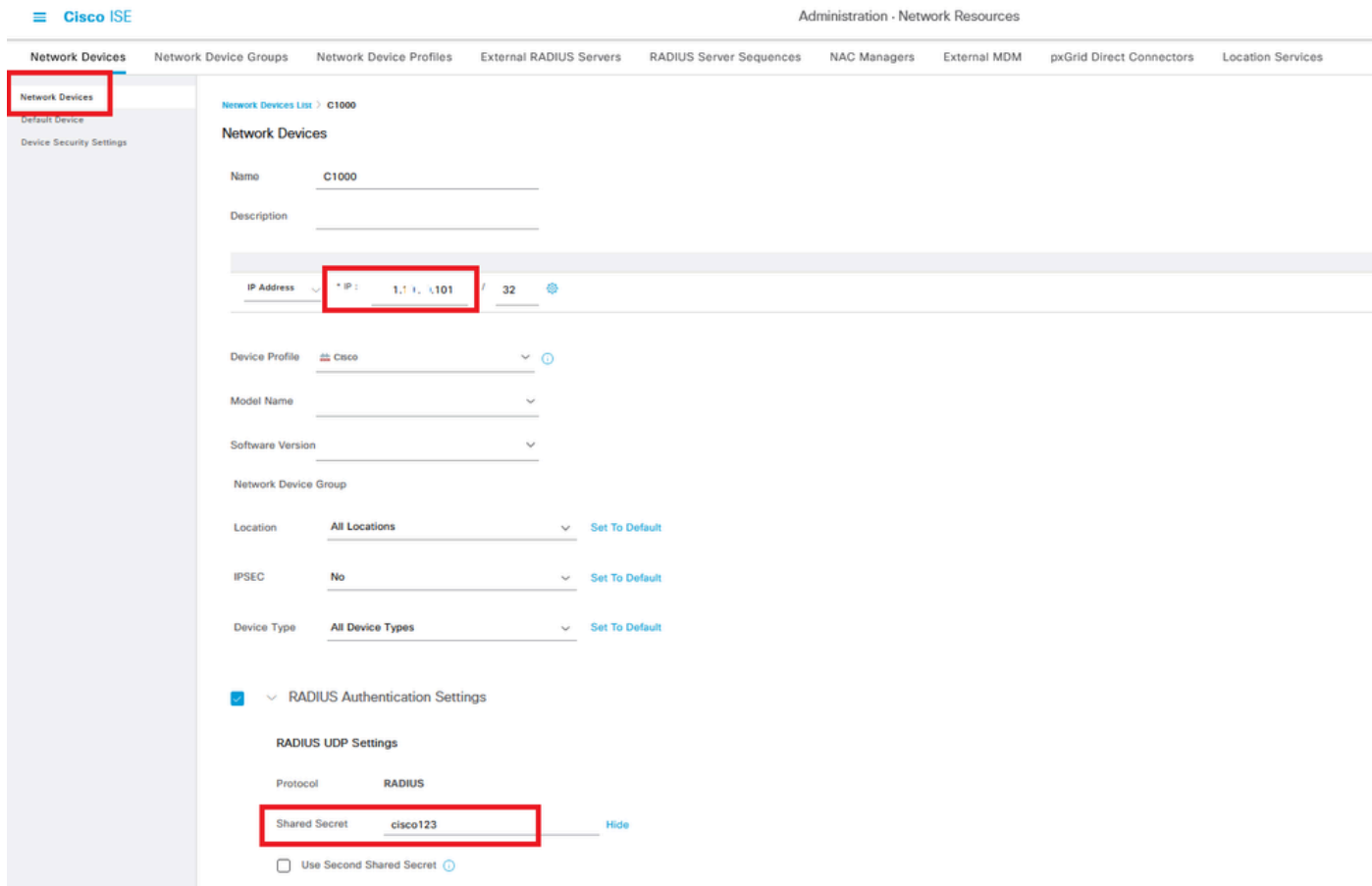
Stato del certificato di firma OCSP

Configurazione in ISE

Passaggio 1. Aggiungi dispositivo

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

dispositivo C1000.

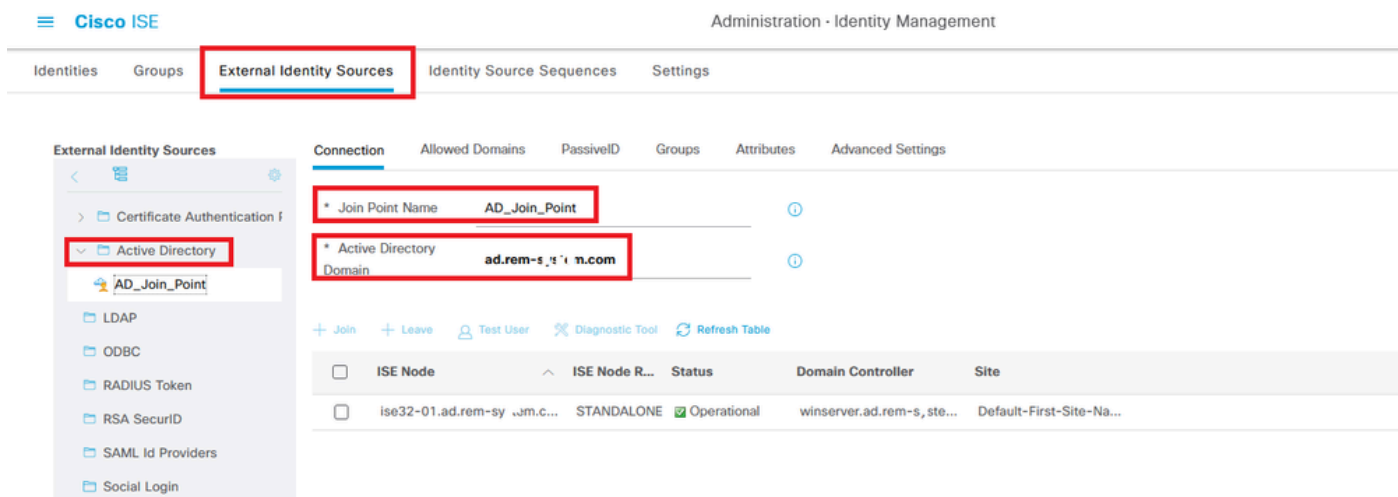


Aggiungi dispositivo

Passaggio 2. Aggiungi Active Directory

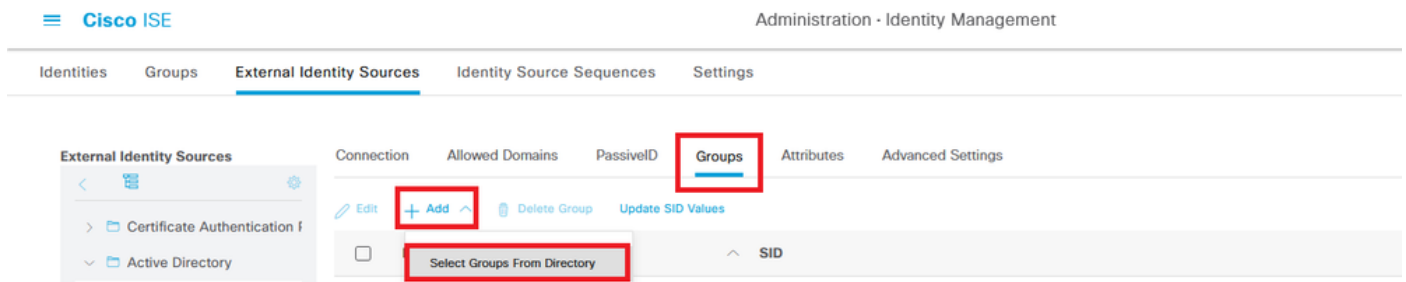
Selezionare Amministrazione > Origini identità esterne > Active Directory, fare clic sulla scheda Connessione, quindi aggiungere Active Directory ad ISE.

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



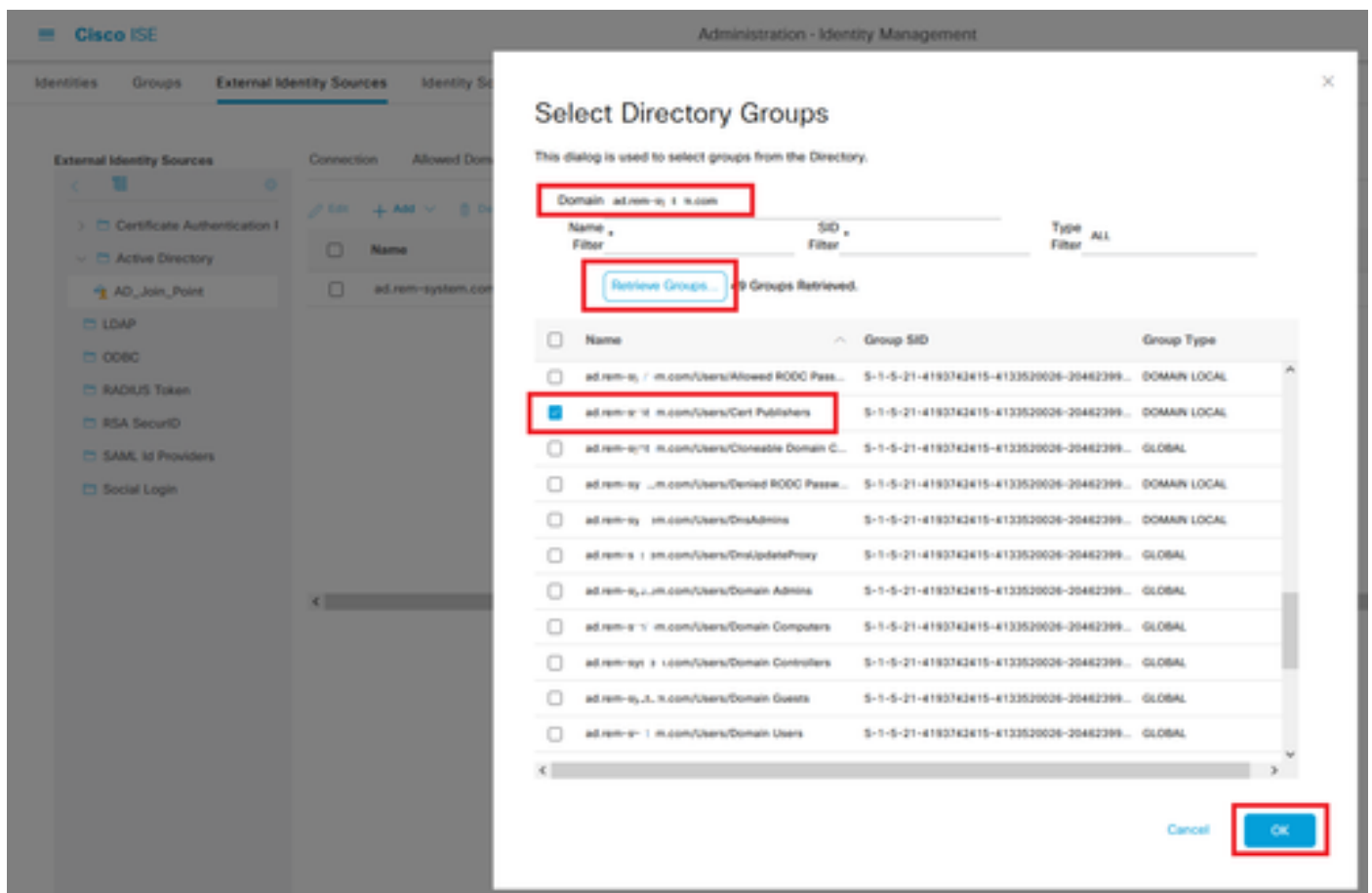
Aggiungi Active Directory

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.

The screenshot shows the Cisco ISE Administration interface for Identity Management. The breadcrumb trail is "Certificate Authentication Profiles List > cert_authen_profile_test". The main heading is "Certificate Authentication Profile".

On the left, the "External Identity Sources" sidebar is expanded to "Certificate Authentication f", with "cert_authen_profile_test" selected. Other sources include Preloaded_Certificate_Prof, Active Directory, AD_Join_Point, LDAP, ODBC, RADIUS Token, RSA SecurID, SAML Id Providers, and Social Login.

The configuration fields are:

- Name:** cert_authen_profile_test
- Description:** (empty text area)
- Identity Store:** AD_Join_Point
- Use Identity From:** Certificate Attribute (selected), Subject - Common Name
- Match Client Certificate Against Certificate In Identity Store:** Only to resolve identity ambiguity (selected)

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

Identity Source Sequences List > Identity_AD

Identity Source Sequence

Identity Source Sequence

* Name Identity_AD

Description

Empty text area for description.

Certificate Based Authentication

Select Certificate Authentication Profile cert_authen_profil

Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available

- Internal Endpoints
- Internal Users
- Guest Users
- All_AD_Join_Points

Selected

- 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.

Cisco ISE		Administration - System						Evaluation Mode 1 Days	
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings
Certificate Management		<input type="checkbox"/>	Default self-signed saml server cer...	SAML	SAML_Ise32-01.ad.rem-sj_ism.com	SAML_Ise32-01.ad.rem-sj_ism.com	Thu, 2 May 2024	Tue, 1 May 2029	Active
System Certificates		<input type="checkbox"/>	CN=Ise32-01.ad.rem-sj_ism.com, OU=ISE Messaging Service	ISE Messaging Service	Ise32-01.ad.rem-sj_ism.com	Certificate Services Endpoint Sub C A - Ise32-01	Wed, 1 May 2024	Wed, 2 May 2029	Active
Trusted Certificates		<input type="checkbox"/>	CN=Ise32-01.ad.rem-sj_ism.com, OU=Certificate Services System Ce...	Not in use	Ise32-01.ad.rem-sj_ism.com	Certificate Services Endpoint Sub C A - Ise32-01	Wed, 1 May 2024	Wed, 2 May 2029	Active
OCSP Client Profile		<input type="checkbox"/>	CN=Ise32-01.ad.rem-sj_ism.com, OU=Certificate Services Endpo...	Portal	Ise32-01.ad.rem-sj_ism.com	rootCACCommonName	Tue, 4 Jun 2024	Wed, 4 Jun 2025	Active
Certificate Signing Requests		<input type="checkbox"/>	Ise-server-cert-friendly-name	Admin, EAP Authentication, RADIUS DTLS, perGrid, Portal	Ise32-01.ad.rem-sj_ism.com	ocsp-ca-common-name	Tue, 4 Jun 2024	Wed, 4 Jun 2025	Active

Certificato server

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

Aggiungi per aggiungere un nuovo profilo client OCSP.

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

Cisco ISE Administration - System

Deployment Licensing **Certificates** Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings

Certificate Management

- System Certificates
- Trusted Certificates
- OCSP Client Profile**
- Certificate Signing Requests
- Certificate Periodic Check Se...

Certificate Authority

Edit OCSP Profile

* Name **ocsptestprofile**

Description

Configure OCSP Responder

Server Connection

- Enable Secondary Server
- Always Access Primary Server First
- Fallback to Primary Server After Interval Minutes

Primary Server

* URL **http://r.ad.rem-xxx.com/ocsp**

- Enable Nonce Extension Support
- Validate Response Signature

Secondary Server

URL **http://**

- Enable Nonce Extension Support
- Validate Response Signature

Use OCSP URLs specified in Authority Information Access (AIA)

- Enable Nonce Extension Support
- Validate Response Signature

Response Cache

* Cache Entry Time To Live **1440** Minutes

Clear Cache

Profilo client OCSP

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

Cisco ISE Administration - System

Deployment Licensing **Certificates** Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings

Certificate Management

- System Certificates
- Trusted Certificates**
- OCSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Se...

Certificate Authority

Trusted Certificate	Infrastructure	Endpoint	Expiration Date	Issued Date	Status		
<input type="checkbox"/> Cisco Manufacturing CA SHA2	Infrastructure	02	Cisco Manufacturing CA SH...	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 20...	Enabled
<input type="checkbox"/> Cisco Root CA 2048	Infrastructure	5F F8 7B 28 2...	Cisco Root CA 2048	Cisco Root CA 2048	Sat, 15 May 2004	Tue, 15 May 20...	Disabled
<input type="checkbox"/> Cisco Root CA 2099	Cisco Services	01 9A 33 58 7...	Cisco Root CA 2099	Cisco Root CA 2099	Wed, 10 Aug 2016	Mon, 10 Aug ...	Enabled
<input type="checkbox"/> Cisco Root CA M1	Cisco Services	2E D2 0E 73 4...	Cisco Root CA M1	Cisco Root CA M1	Wed, 19 Nov 2008	Sat, 19 Nov 20...	Enabled
<input type="checkbox"/> Cisco Root CA M2	Infrastructure	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 20...	Enabled
<input type="checkbox"/> Cisco RXC-R2	Cisco Services	01	Cisco RXC-R2	Cisco RXC-R2	Thu, 10 Jul 2014	Mon, 10 Jul 2...	Enabled
<input type="checkbox"/> CN=root_ca_common_name, OU=cisc...	Infrastructure	20 BF 12 86 F...	root_ca_common_name	root_ca_common_name	Thu, 16 May 2024	Tue, 16 May 2...	Enabled
<input type="checkbox"/> CN=rootCACCommonName@rootCACom...	Infrastructure	21 31 D3 DE ...	rootCACCommonName	rootCACCommonName	Tue, 4 Jun 2024	Sun, 4 Jun 20...	Enabled
<input type="checkbox"/> Default self-signed server certificate	Infrastructure	37 66 FC 29 ...	ise32-01.ad.rem-system.com	ise32-01.ad.rem-system.com	Thu, 2 May 2024	Sat, 2 May 20...	Enabled
<input type="checkbox"/> DigiCert Global Root CA	Cisco Services	08 38 E0 56 9...	DigiCert Global Root CA	DigiCert Global Root CA	Fri, 10 Nov 2006	Mon, 10 Nov ...	Enabled
<input type="checkbox"/> DigiCert Global Root G2 CA	Cisco Services	03 3A F1 E6 ...	DigiCert Global Root G2	DigiCert Global Root G2	Thu, 1 Aug 2013	Fri, 15 Jan 20...	Enabled
<input type="checkbox"/> DigiCert root CA	Infrastructure	02 AC 5C 26 ...	DigiCert High Assurance EV ...	DigiCert High Assurance EV...	Fri, 10 Nov 2006	Mon, 10 Nov ...	Enabled
<input type="checkbox"/> DigiCert SHA2 High Assurance Server ...	Infrastructure	04 E1 E7 A4 ...	DigiCert SHA2 High Assuran...	DigiCert High Assurance EV...	Tue, 22 Oct 2013	Sun, 22 Oct 2...	Enabled
<input type="checkbox"/> IdemTrust Commercial Root CA 1	Cisco Services	0A 01 42 80 0...	IdemTrust Commercial Root ...	IdemTrust Commercial Root ...	Fri, 17 Jan 2014	Tue, 17 Jan 2...	Enabled
<input type="checkbox"/> ocsptestfriendlyname	Infrastructure	1A 12 1D 58 ...	ocsp-ca-common-name	ocsp-ca-common-name	Tue, 4 Jun 2024	Sun, 4 Jun 20...	Enabled

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: oosp_test_profile
- Rifiuta la richiesta se OCSP restituisce lo stato UNKNOWN: check
- Rifiuta la richiesta se il risponditore OCSP non è raggiungibile: selezionare

Cisco ISE Administration - System

Deployment Licensing **Certificates** Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings

Issuer

* Friendly Name

Status Enabled

Description

Subject CN=oosp-ca-common-name

Issuer CN=oosp-ca-common-name

Valid From Tue, 4 Jun 2024 13:52:00 JST

Valid To (Expiration) Sun, 4 Jun 2034 13:52:00 JST

Serial Number 1A 12 1D 58 59 6C 75 1B

Signature Algorithm SHA256withRSA

Key Length 2048

Usage

Trusted For: ⓘ

- Trust for authentication within ISE
- Trust for client authentication and Syslog
- Trust for certificate based admin authentication
- Trust for authentication of Cisco Services

Certificate Status Validation

To verify certificates, enable the methods below. If both are enabled, OCSP will always be tried first.

OCSP Configuration

- Validate against OCSP Service
- Reject the request if OCSP returns UNKNOWN status
- Reject the request if OCSP Responder is unreachable

Certificate Revocation List Configuration

Download CRL

CRL Distribution URL

Retrieve CRL Automatically 5 Minutes before expiration.

Every 1 Hours

If download failed, wait 10 Minutes before retry.

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.

Dictionary Conditions **Results**

Authentication

Allowed Protocols

Authorization

Profiling

Posture

Client Provisioning

Allowed Protocols Services List > Default Network Access

Allowed Protocols

Name Default Network Access

Description Default Allowed Protocol Service

Allowed Protocols

Authentication Bypass

Process Host Lookup

Authentication Protocols

Allow PAP/ASCII

Allow CHAP

Allow MS-CHAPv1

Allow MS-CHAPv2

Allow EAP-MD5

Allow EAP-TLS

Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy

Enable Stateless Session Resume

Session ticket time to live 2 Hours

Proactive session ticket update will occur after 90 % of Time To Live has expired

Allow LEAP

Allow PEAP

PEAP Inner Methods

Allow EAP-MS-CHAPv2

Allow Password Change Retries 1 (Valid Range 0 to 3)

Allow EAP-GTC

Allow Password Change Retries 1 (Valid Range 0 to 3)

Allow EAP-TLS

Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy

Require cryptobinding TLV

Allow PEAPv0 only for legacy clients

Consenti EAP-TLS

Passaggio 7. Aggiungo 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

Cisco ISE Policy - Policy Sets Evaluation Mode : 1 Days

Policy Sets

Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	EAP-TLS-Test		Network Access-Protocol EQUALS RADIUS	Default Network Access	75		

Aggiungo set di criteri

Passaggio 8. Aggiungo 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

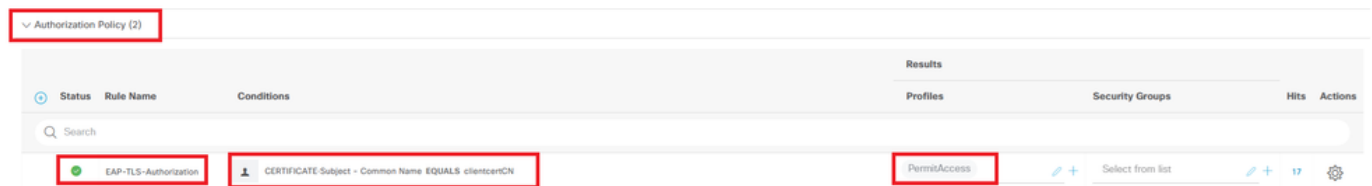


Aggiungi criterio di autenticazione

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

Esegui `show 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: 01C2006500000933E4E87D9
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.

The screenshot displays the Cisco ISE Operations - RADIUS Live Logs interface. At the top, there are five summary cards: Misconfigured Supplicants (0), Misconfigured Network Devices (0), RADIUS Drops (0), Client Stopped Responding (0), and Repeat Counter (0). Below these cards, there are options to 'Reset Repeat Counts' and 'Export To'. A table of live logs is shown with the following columns: Time, Status, Details, Repeats, Identity, Endpoint ID, Endpoint Name, Authentication Policy, Authorization Policy, Authorization Profile, and IP Address. Two log entries are visible, both with a status of 'Success' and a 'PermitAccess' authorization profile. The second entry is highlighted with a red box.

Time	Status	Details	Repeats	Identity	Endpoint ID	Endpoint Name	Authentication Policy	Authorization Policy	Authorization Profile	IP Address
Jun 05, 2024 09:43:36.3...	Success		0	clientcertCN	B4-96-91:14.3...	Intel-Device	EAP-TLS-Test >> EAP-TLS-Authentication	EAP-TLS-Test >> EAP-TLS-Authorization	PermitAccess	192.168.10.10
Jun 05, 2024 09:43:33.2...	Success		0	clientcertCN	B4-96-91:14.3...	Intel-Device	EAP-TLS-Test >> EAP-TLS-Authentication	EAP-TLS-Test >> EAP-TLS-Authorization	PermitAccess	

Registro Radius Live

Confermare il log dettagliato dell'autenticazione in tempo reale.

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	01C2006500000933E4E87D9

Other Attributes

ConfigVersionId	167
DestinationPort	1645
Protocol	Radius
NAS-Port	50103
Framed-MTU	1500
State	37CPMSessionID=01C2006500000933E4E87D9;31SessionID=ise32-01/506864164/73;
AD-User-Resolved-Identities	clientcertCN@ad.rem-s;:rem.com
AD-User-Candidate-Identities	clientcertCN@ad.rem-s;:rem.com
TotalAuthenLatency	324
ClientLatency	80
AD-User-Resolved-DNs	CN=clientcert CN, CN=Users, DC=ad, DC=rem-s;:rem, DC=com
AD-User-DNS-Domain	ad.rem-s;:rem.com
AD-User-NetBios-Name	AD
IsMachineIdentity	false
AD-User-SamAccount-Name	clientcertCN
AD-User-Qualified-Name	clientcertCN@ad.rem-s;:rem.com
AD-User-SamAccount-Name	clientcertCN
AD-User-Qualified-Name	clientcertCN@ad.rem-s;:rem.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;:rem.com
24319	Single matching account found in forest - ad.rem-s;:rem.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

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,CPMSession

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:

No.	Time	Identification	Source	S.Port	Destination	D.Port	Time to Live	Protocol	Length	TCP.Se	Next seq	TCP.Ac	Info
140	2024-06-05 00:43:33.093523	0x0295 (661)	1.1.1.181	25844	1.1.1.157	80		64 OCSP	262	1	197	1	Request
141	2024-06-05 00:43:33.104108	0x0117 (279)	1.1.1.157	80	1.1.1.181	25844		128 OCSP	1671	1	1607	197	Response

Acquisizione pacchetti di richiesta e risposta 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: 1.1.1.157, Dst: 1.1.1.181
> Transmission Control Protocol, Src Port: 80, Dst Port: 25844, Seq: 1, Ack: 197, Len: 1605
> Hypertext Transfer Protocol
  Online Certificate Status Protocol
    responseStatus: successful (0)
  responseBytes
    ResponseType Id: 1.3.6.1.5.5.7.48.1.1 (id-pkix-ocsp-basic)
  BasicOCSPResponse
    tbsResponseData
      responderID: byKey (2)
      producedAt: Jun 5, 2024 09:43:33.000000000
      responses: 1 item
        SingleResponse
          certID
            certStatus: good (0)
            thisUpdate: Jun 4, 2024 16:05:00.000000000
            nextUpdate: Jul 4, 2024 16:05:00.000000000
          responseExtensions: 1 item
  
```

Acquisisci dettagli risposta OCSP

Sessione Radius:

146	2024-06-05 00:43:33.118175	0x9bc6 (39878)	1.1.1.101	67181	1.1.1.181	1645		255 RADIUS	366				Access-Request id=238
185	2024-06-05 00:43:33.270244	0x033d (829)	1.1.1.181	67181	1.1.1.101	1645		64 RADIUS	336				Access-Accept id=238
187	2024-06-05 00:43:33.341233	0x9bc7 (39879)	1.1.1.101	1646	1.1.1.181	1646		255 RADIUS	328				Accounting-Request id=10
188	2024-06-05 00:43:33.350936	0x037a (890)	1.1.1.181	1646	1.1.1.101	1646		64 RADIUS	62				Accounting-Response id=10
267	2024-06-05 00:43:36.359621	0x9bc8 (39880)	1.1.1.101	1646	1.1.1.181	1646		255 RADIUS	334				Accounting-Request id=11
268	2024-06-05 00:43:36.369035	0x0489 (1161)	1.1.1.181	1646	1.1.1.101	1646		64 RADIUS	62				Accounting-Response id=11

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).