Configurar a autenticação EAP-TLS com OCSP no ISE

Contents

Introdução

Este documento descreve as etapas necessárias para configurar a autenticação EAP-TLS com OCSP para verificações de revogação de certificados de clientes em tempo real.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração do Cisco Identity Services Engine
- Configuração do Cisco Catalyst
- Protocolo de Status de Certificado Online

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

- Windows Server 2016
- Windows 10

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Diagrama de Rede

Esta imagem mostra a topologia usada para o exemplo deste documento.

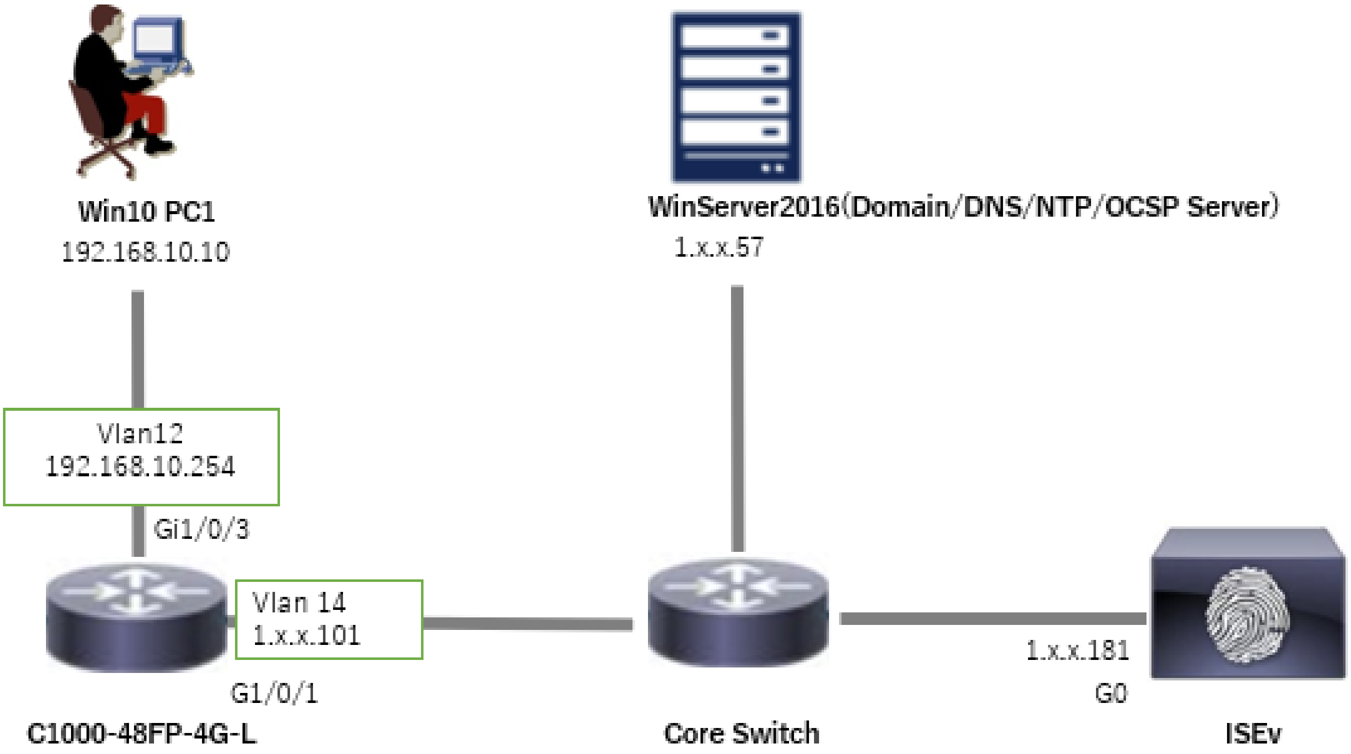


Diagrama de Rede

Informações de Apoio

No EAP-TLS, um cliente apresenta seu certificado digital ao servidor como parte do processo de autenticação. Este documento descreve como o ISE valida o certificado do cliente verificando o CN (nome comum) do certificado em relação ao servidor do AD e confirmando se o certificado foi revogado usando o OCSP (Online Certificate Status Protocol), que fornece o status do protocolo em tempo real.

O nome de domínio configurado no Windows Server 2016 é ad.rem-xxx.com, usado como exemplo neste documento.

Os servidores OCSP (Online Certificate Status Protocol) e AD (Ative Diretory) mencionados neste documento são usados para validação de certificado.

- FQDN do Ative Diretory: winserver.ad.rem-xxx.com
- URL de Distribuição de CRL: http://winserver.ad.rem-xxx.com/ocsp-ca.crl
- URL da autoridade: http://winserver.ad.rem-xxx.com/ocsp

Esta é a cadeia de certificados com o nome comum de cada certificado usado no documento.

- CA: ocsp-ca-common-name
- Certificado do cliente: clientcertCN
- Certificado do servidor: ise32-01.ad.rem-xxx.com
- Certificado de Autenticação OCSP: ocspSignCommonName

Configurações

Configuração no C1000

Essa é a configuração mínima na CLI do 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
```

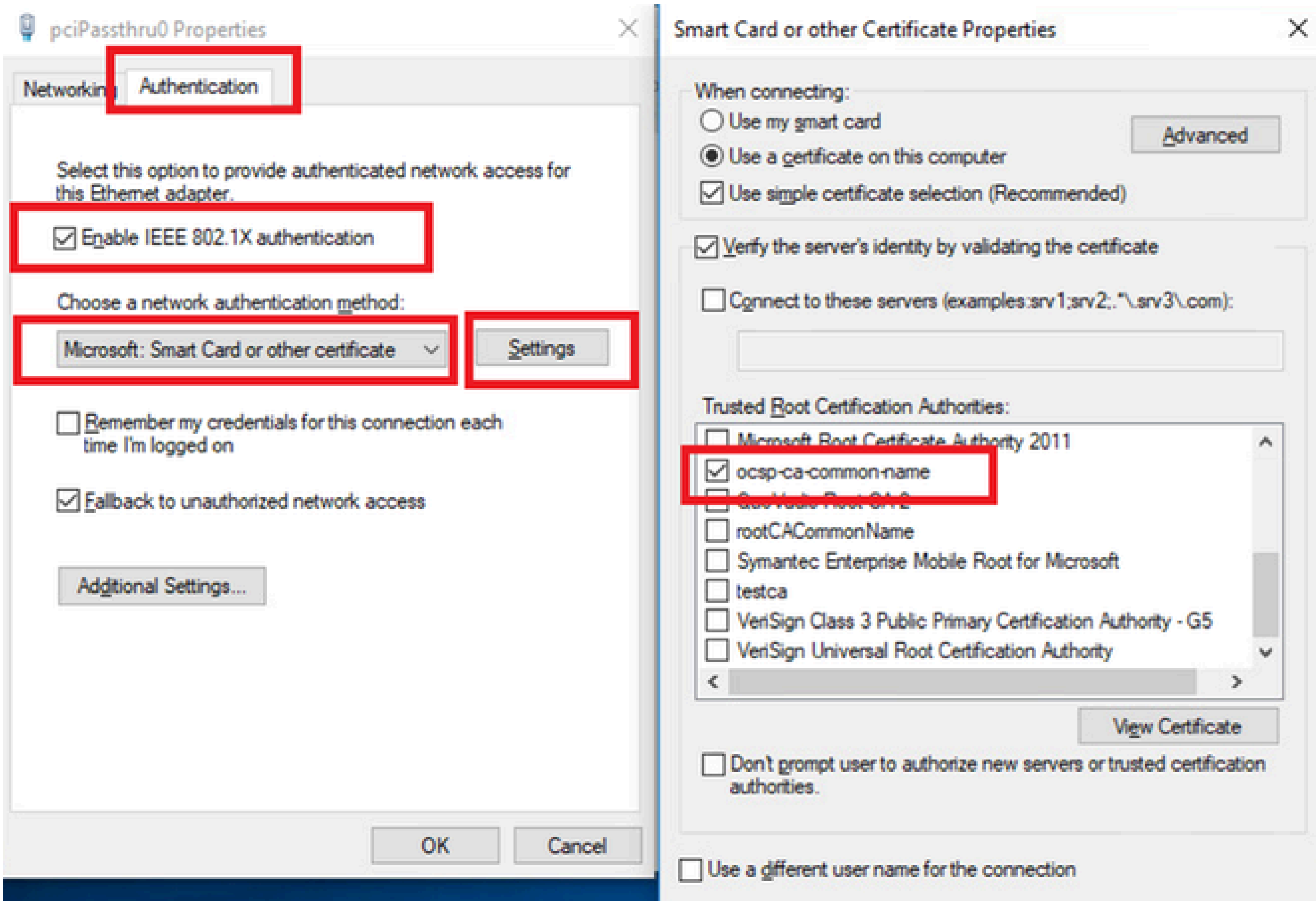
```
interface GigabitEthernet1/0/1
Switch port access vlan 14
Switch port mode access

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
```

Configuração no PC com Windows

Etapa 1. Configurar autenticação de usuário

Navegue até Authentication, marque Enable IEEE 802.1X authentication e selecione Microsoft: Smart Card ou outro certificado.

Clique no botão Configurações, marque Usar um certificado neste computador e selecione a CA confiável do Windows PC.



pciPassthru0 Properties

Networking | Authentication

Select this option to provide authenticated network access for this Ethernet adapter.

☑ Enable IEEE 802.1X authentication

Choose a network authentication method:

Microsoft: Smart Card or other certificate

□ Remember my credentials for this connection each time I'm logged on

☑ Fallback to unauthorized network access

Smart Card or other Certificate Properties

When connecting:

○ Use my smart card

● Use a certificate on this computer

☑ Use simple certificate selection (Recommended)

☑ Verify the server's identity by validating the certificate

□ Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):

Trusted Root Certification Authorities:

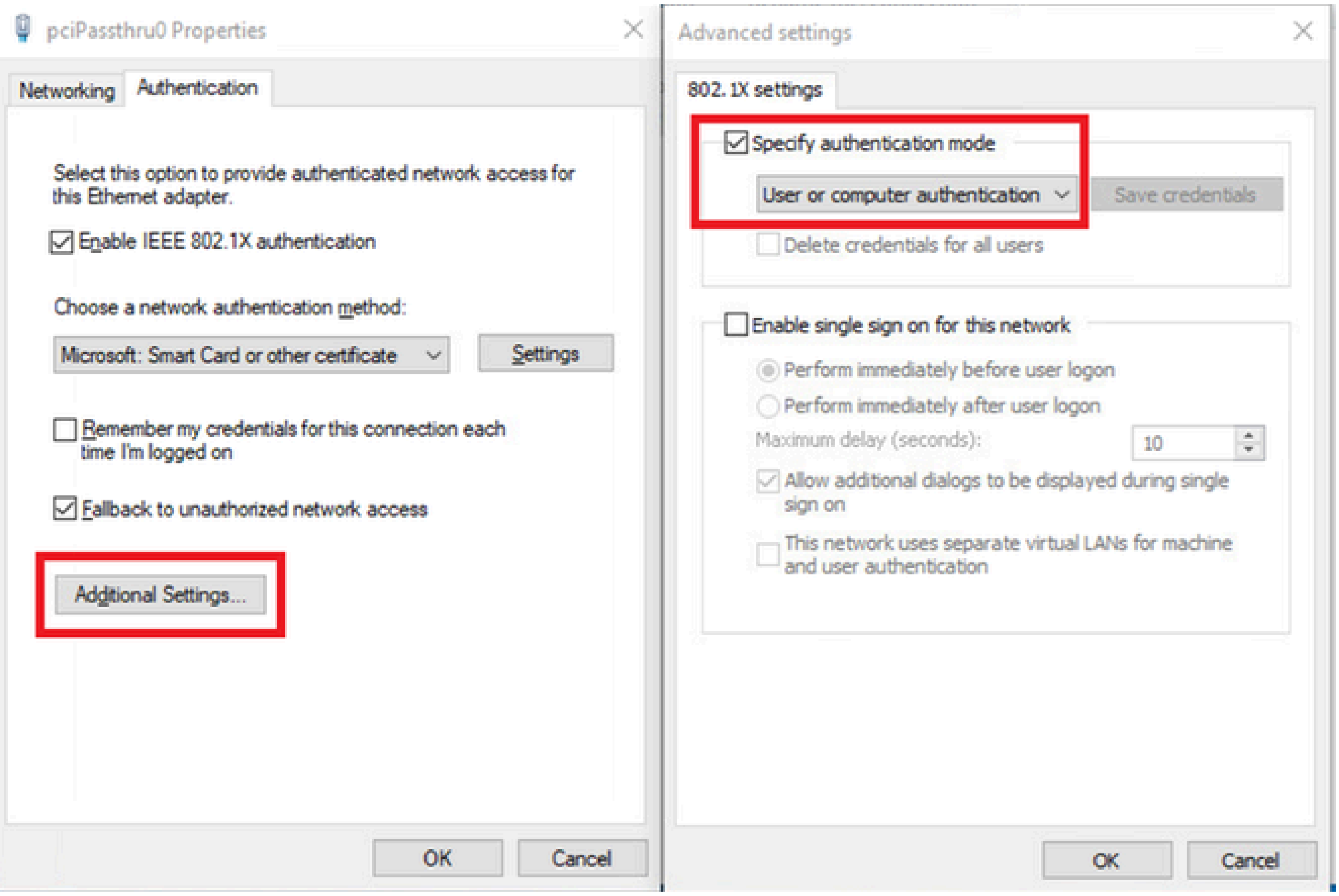
□ Microsoft Root Certificate Authority 2011
☑ ocsp-ca-common-name
□ QuoVadis Root CA 2
□ rootCACommonName
□ Symantec Enterprise Mobile Root for Microsoft
□ testca
□ VeriSign Class 3 Public Primary Certification Authority - G5
□ VeriSign Universal Root Certification Authority

□ Don't prompt user to authorize new servers or trusted certification authorities.

□ Use a different user name for the connection

Habilitar Autenticação de Certificado

Navegue atéAuthentication, checkAdditional Settings. SelecioneAutenticação do usuário ou do computador na lista suspensa.



pciPassthru0 Properties

Networking | Authentication

Select this option to provide authenticated network access for this Ethernet adapter.

☑ Enable IEEE 802.1X authentication

Choose a network authentication method:

Microsoft: Smart Card or other certificate

☐ Remember my credentials for this connection each time I'm logged on

☑ Fallback to unauthorized network access

Advanced settings

802.1X settings

☑ Specify authentication mode

User or computer authentication

☐ Delete credentials for all users

☐ Enable single sign on for this network

● Perform immediately before user logon

○ Perform immediately after user logon

Maximum delay (seconds): 10

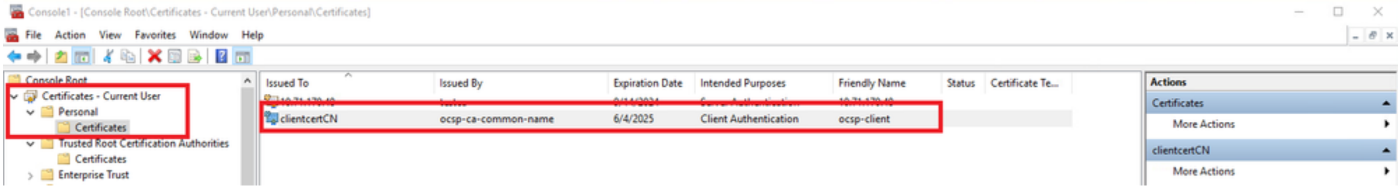
☑ Allow additional dialogs to be displayed during single sign on

☐ This network uses separate virtual LANs for machine and user authentication

Especificar Modo de Autenticação

Etapa 2. Confirmar certificado do cliente

Navegue até Certificates - Current User > Personal > Certificates e verifique o certificado do cliente usado para autenticação.



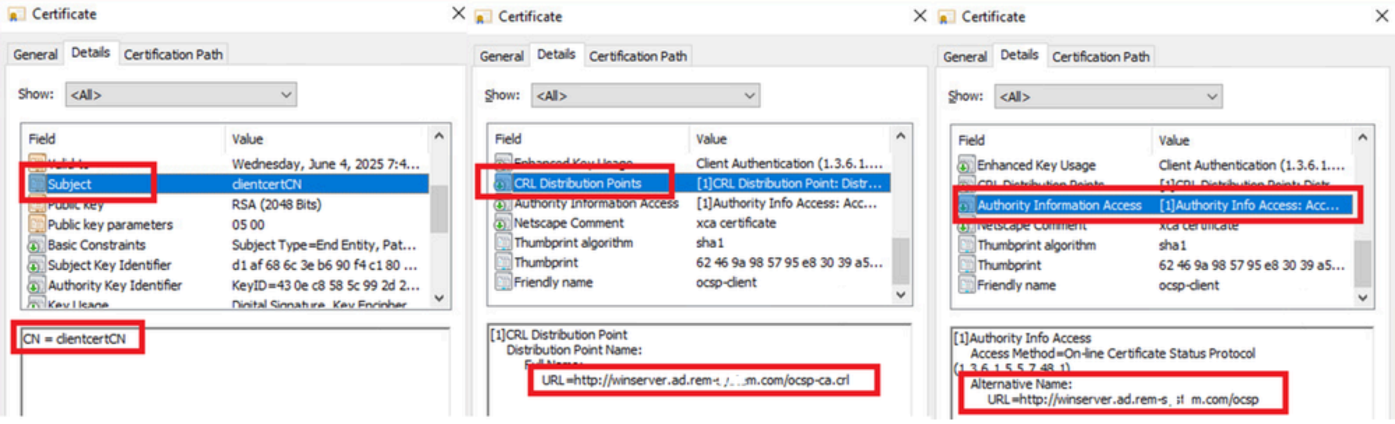
Console1 - [Console Root\Certificates - Current User\Personal\Certificates]

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Te...
clientcertCN	ocsp-ca-common-name	6/4/2025	Client Authentication	ocsp-client		

Confirmar certificado do cliente

Clique duas vezes no certificado do cliente, navegue até Details, verifique os detalhes de Subject, CRL Distribution Points, Authority Information Access.

- Assunto: CN = clientcertCN
- Pontos de Distribuição de CRL: http://winserver.ad.rem-xxx.com/ocsp-ca.crl
- Acesso às informações da autoridade: http://winserver.ad.rem-xxx.com/ocsp



Field	Value
Valid to	Wednesday, June 4, 2025 7:4...
Subject	clientcertCN
Public key	RSA (2048 Bits)
Public key parameters	05 00
Basic Constraints	Subject Type=End Entity, Pat...
Subject Key Identifier	d1 af 68 6c 3e b6 90 f4 c1 80 ...
Authority Key Identifier	KeyID=43 0e c8 58 5c 99 2d 2...
Key Usage	Digital Signature, Key Encipher...

CN = clientcertCN

Field	Value
Enhanced Key Usage	Client Authentication (1.3.6.1....
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Netscape Comment	xca certificate
Thumbprint algorithm	sha1
Thumbprint	62 46 9a 98 57 95 e8 30 39 a5...
Friendly name	ocsp-client

[1]CRL Distribution Point
Distribution Point Name:
Full Name:
URL=http://winserver.ad.rem-[redacted]m.com/ocsp-ca.crl

Field	Value
Enhanced Key Usage	Client Authentication (1.3.6.1....
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Netscape Comment	xca certificate
Thumbprint algorithm	sha1
Thumbprint	62 46 9a 98 57 95 e8 30 39 a5...
Friendly name	ocsp-client

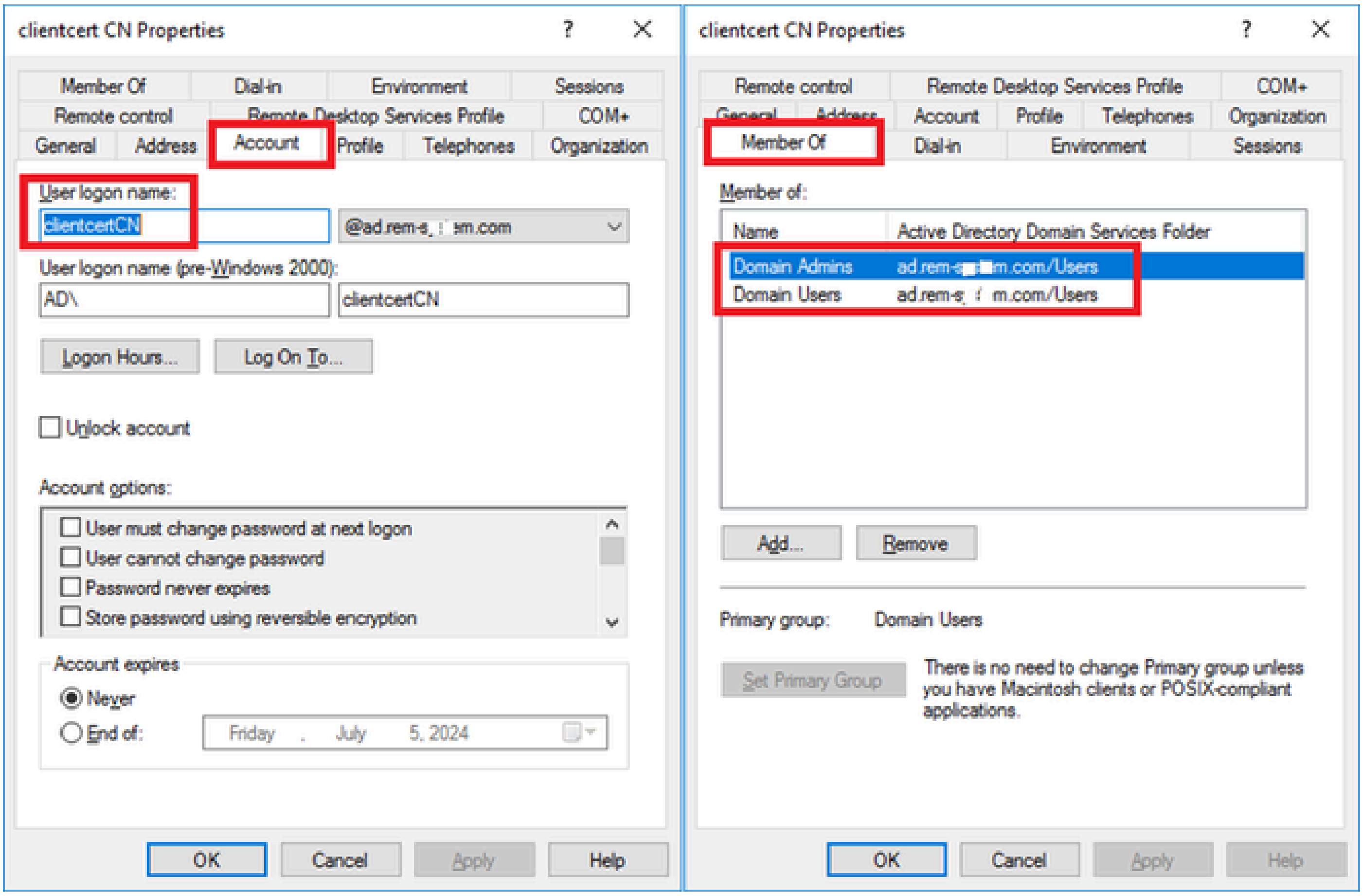
[1]Authority Info Access
Access Method=On-line Certificate Status Protocol
(1.3.6.1.5.5.7.48.1)
Alternative Name:
URL=http://winserver.ad.rem-s[redacted]m.com/ocsp

Detalhe do Certificado do Cliente

Configuração no Windows Server

Etapa 1. Adicionar usuários

Navegue atéUsuários e computadores do Ative Diretory, clique emUsuários. Adicione clientcertCN como nome de logon de usuário.



User logon name: clientcertCN @ad.rem-s[redacted]m.com

User logon name (pre-Windows 2000): AD\ clientcertCN

□ Unlock account

Account options:

- □ User must change password at next logon
- □ User cannot change password
- □ Password never expires
- □ Store password using reversible encryption

Account expires

- ● Never
- ○ End of: Friday , July 5, 2024

Member of:

Name	Active Directory Domain Services Folder
Domain Admins	ad.rem-s[redacted]m.com/Users
Domain Users	ad.rem-s[redacted]m.com/Users

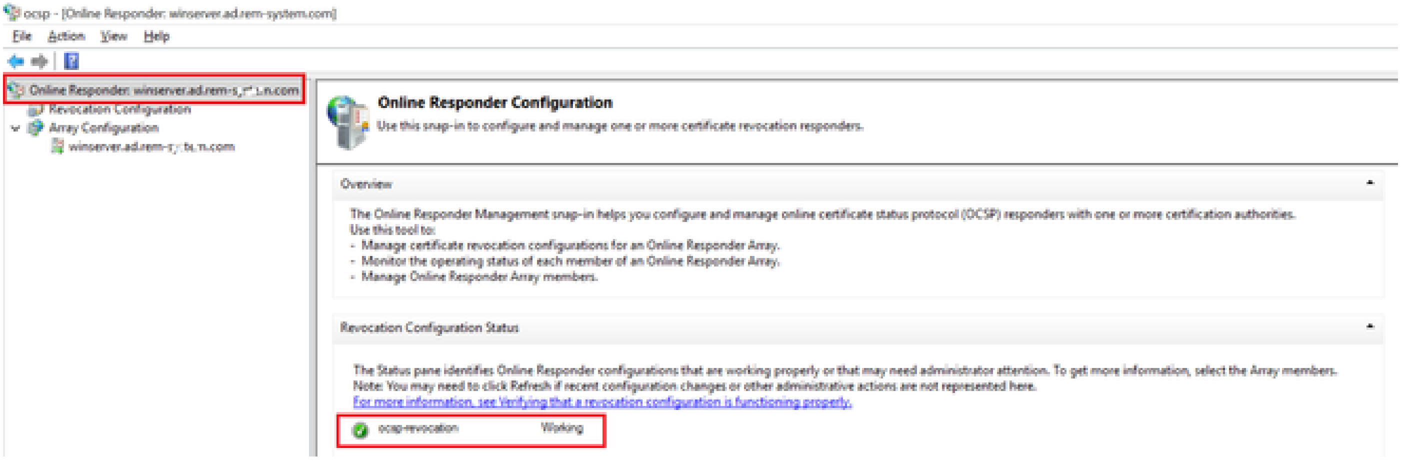
Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

Nome de Logon do Usuário

Etapa 2. Confirmar serviço OCSP

Navegue até Windows, clique em Online Responder Management. Confirme o status do servidor OCSP.


ocsp - [Online Responder: winserver.ad.rem-system.com]
File Action View Help
Online Responder: winserver.ad.rem-s,[illegible].n.com
Revocation Configuration
Array Configuration
winserver.ad.rem-s[illegible].n.com
Overview
Revocation Configuration Status

Online Responder Configuration

Use this snap-in to configure and manage one or more certificate revocation responders.

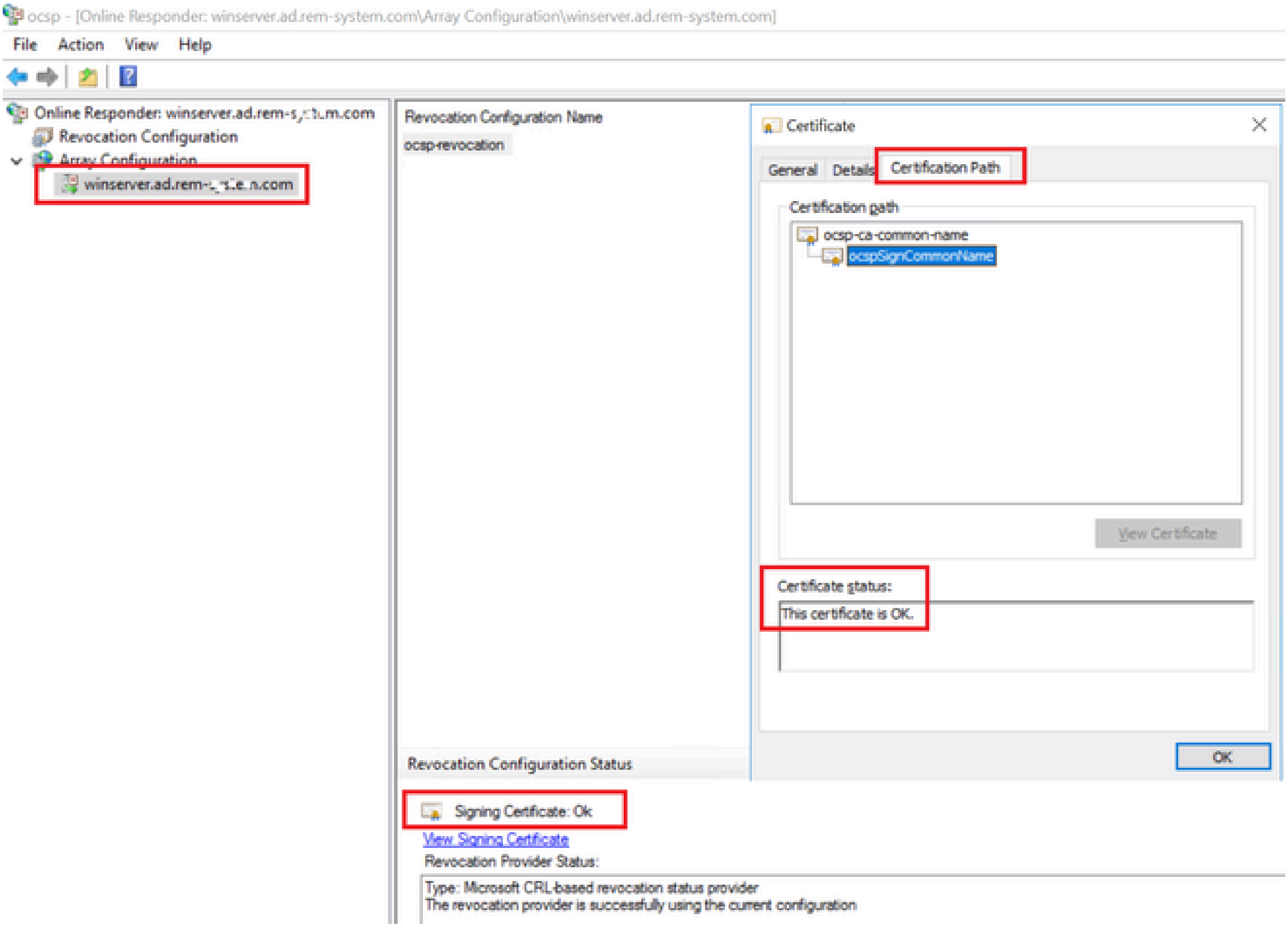
The Online Responder Management snap-in helps you configure and manage online certificate status protocol (OCSP) responders with one or more certification authorities.
Use this tool to:
- Manage certificate revocation configurations for an Online Responder Array.
- Monitor the operating status of each member of an Online Responder Array.
- Manage Online Responder Array members.

The Status pane identifies Online Responder configurations that are working properly or that may need administrator attention. To get more information, select the Array members.
Note: You may need to click Refresh if recent configuration changes or other administrative actions are not represented here.
For more information, see Verifying that a revocation configuration is functioning properly.

ocsp-revocation	Working

Status do servidor OCSP

Clique em winserver.ad.rem-xxx.com, verifique o status do certificado de assinatura OCSP.


ocsp - [Online Responder: winserver.ad.rem-system.com\Array Configuration\winserver.ad.rem-system.com]
File Action View Help
Online Responder: winserver.ad.rem-s[illegible]m.com
Revocation Configuration
Array Configuration
winserver.ad.rem-[illegible]e.n.com
Certificate
General
Details
Certification Path
View Certificate
OK

Revocation Configuration Name
ocsp-revocation

Certification path
ocsp-ca-common-name
ocspSignCommonName

Certificate status:
This certificate is OK.

Revocation Configuration Status

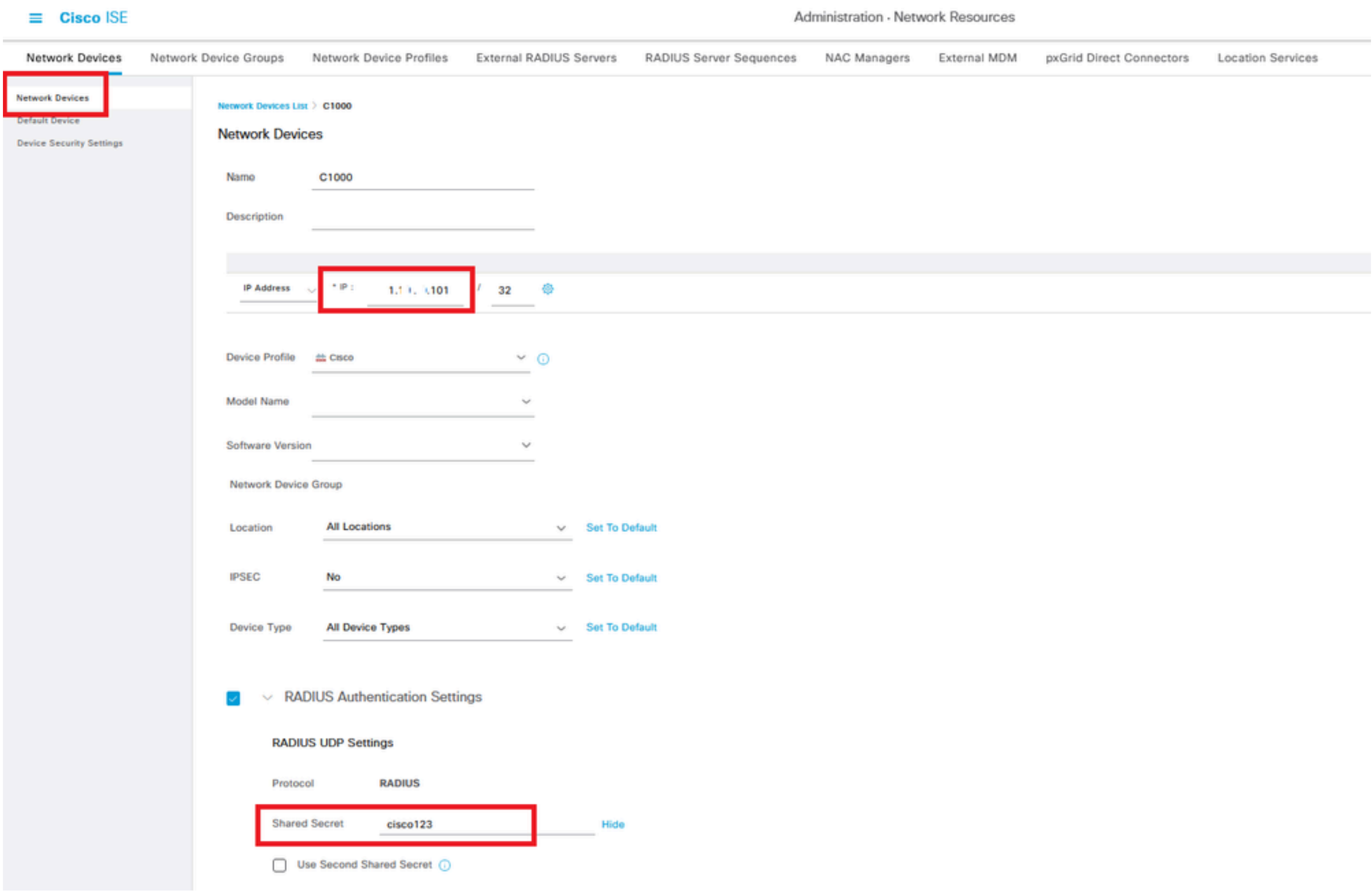
Signing Certificate: Ok
View Signing Certificate
Revocation Provider Status:
Type: Microsoft CRL-based revocation status provider
The revocation provider is successfully using the current configuration

Status do Certificado de Autenticação OCSP

Configuração no ISE

Etapa 1. Adicionar dispositivo

Navegue até Administração > Dispositivos de rede, clique no botão Adicionar para adicionar o dispositivo C1000.



Network Devices

Name: C1000

Description:

IP Address * IP : 1.[illegible].101 / 32

Device Profile: Cisco

Model Name:

Software Version:

Network Device Group

Location: All Locations — Set To Default

IPSEC: No — Set To Default

Device Type: All Device Types — Set To Default

☑ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

Shared Secret: cisco123 — Hide

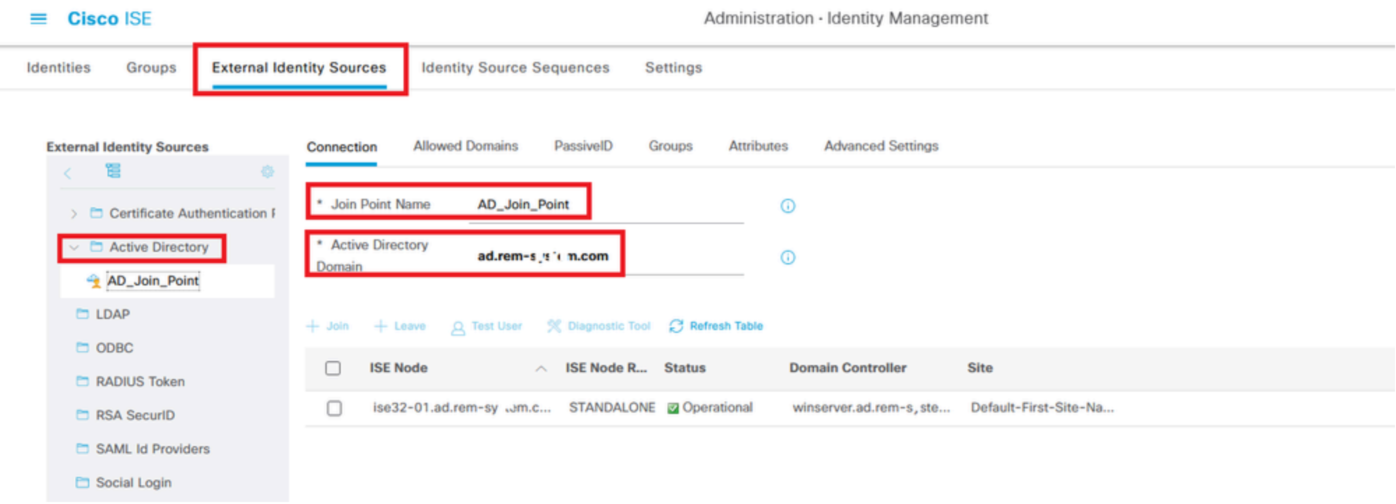
□ Use Second Shared Secret

Adicionar dispositivo

Etapa 2. Adicionar Ative Diretory

Navegue até Administração > Fontes de identidade externas > Ative Diretory, clique na guiaConexão e adicione o Ative Diretory ao ISE.

- Nome do ponto de junção: AD_Join_Point
- Domínio do Ative Diretory: ad.rem-xxx.com



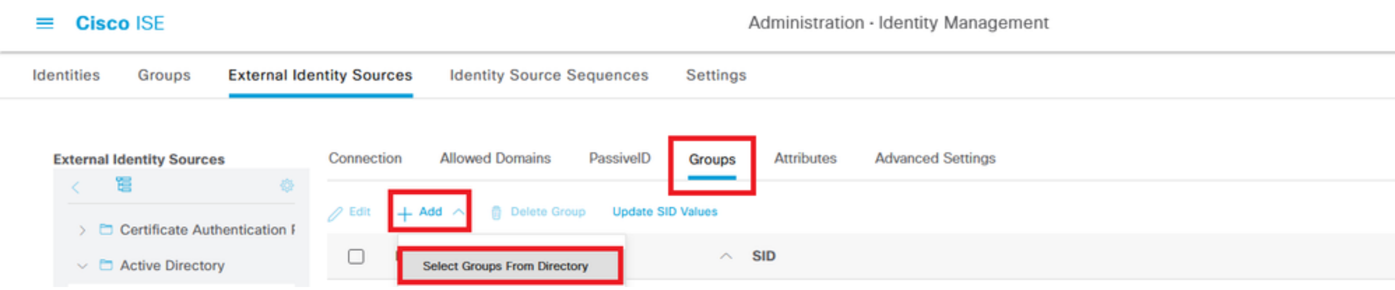
* Join Point Name: AD_Join_Point

* Active Directory Domain: ad.rem-[illegible]n.com

□	ISE Node	ISE Node R...	Status	Domain Controller	Site
□	ise32-01.ad.rem-sy[illegible]m.c...	STANDALONE	☑ Operational	winserver.ad.rem-s[illegible]ste...	Default-First-Site-Na...

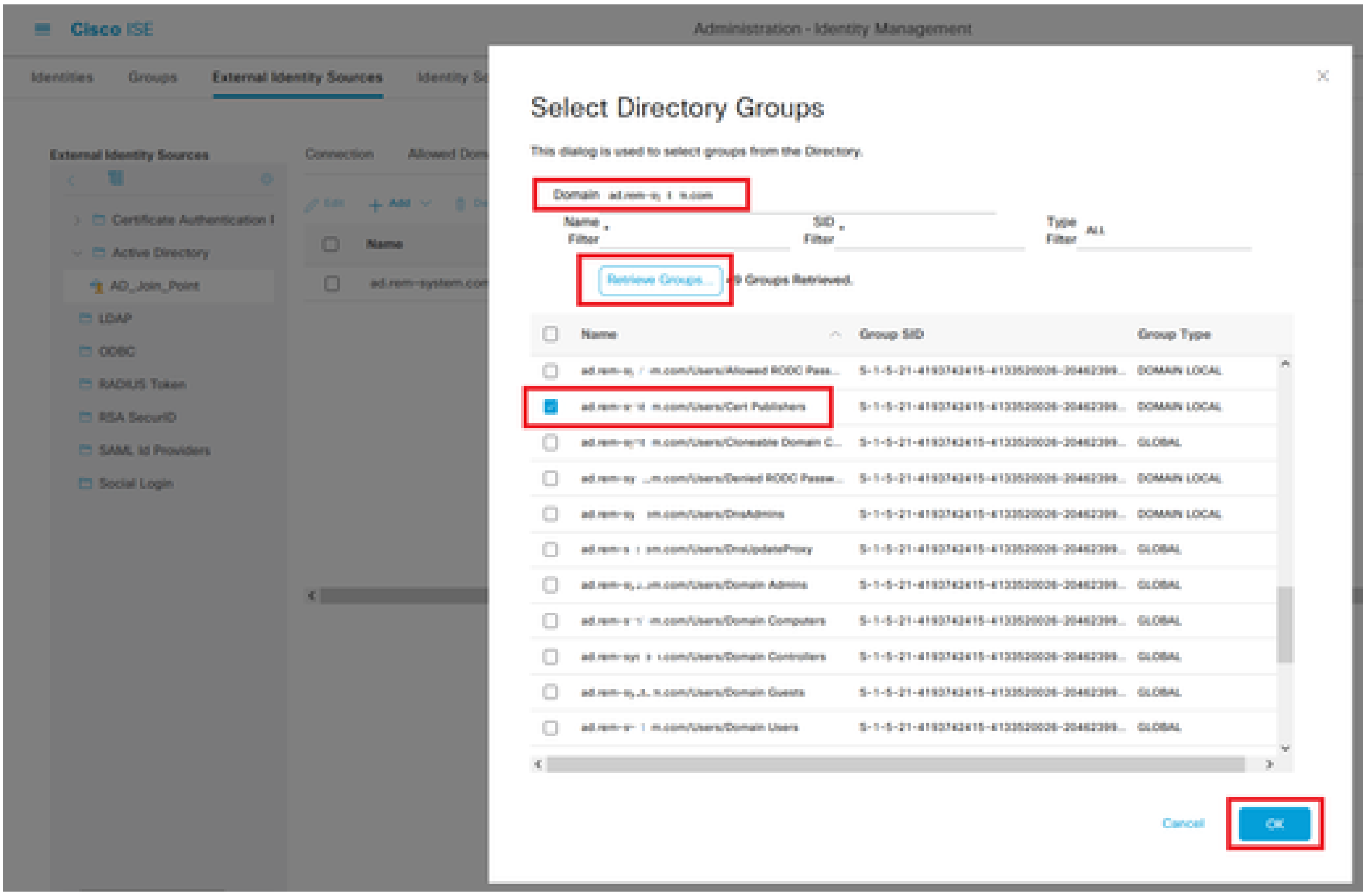
Adicionar Ative Diretory

Navegue até a guia Grupos e selecione Selecionar grupos do diretório na lista suspensa.


Cisco ISE
Administration · Identity Management
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
External Identity Sources
Certificate Authentication I
Active Directory
Connection
Allowed Domains
PassiveID
Groups
Attributes
Advanced Settings
Edit
Add
Delete Group
Update SID Values
Select Groups From Directory
SID

Selecionar grupos do diretório

Clique em Recuperar grupos na lista suspensa. Checkad.rem-xxx.com/Users/Cert Publishers e clique em OK.



☐	Name	Group SID	Group Type
☐	ad.rem-s, / m.com/Users/Allowed RODC Pass...	S-1-5-21-4193742415-4133520026-20462399...	DOMAIN LOCAL
☑	ad.rem-s/ it m.com/Users/Cert Publishers	S-1-5-21-4193742415-4133520026-20462399...	DOMAIN LOCAL
☐	ad.rem-sy't m.com/Users/Cloneable Domain C...	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
☐	ad.rem-sy ...m.com/Users/Denied RODC Passw...	S-1-5-21-4193742415-4133520026-20462399...	DOMAIN LOCAL
☐	ad.rem-sy sm.com/Users/DnsAdmins	S-1-5-21-4193742415-4133520026-20462399...	DOMAIN LOCAL
☐	ad.rem-s i sm.com/Users/DnsUpdateProxy	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
☐	ad.rem-sy,...m.com/Users/Domain Admins	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
☐	ad.rem-s' ' m.com/Users/Domain Computers	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
☐	ad.rem-sys ɪ ı.com/Users/Domain Controllers	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
☐	ad.rem-sy,.t. n.com/Users/Domain Guests	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
☐	ad.rem-s· ı m.com/Users/Domain Users	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL

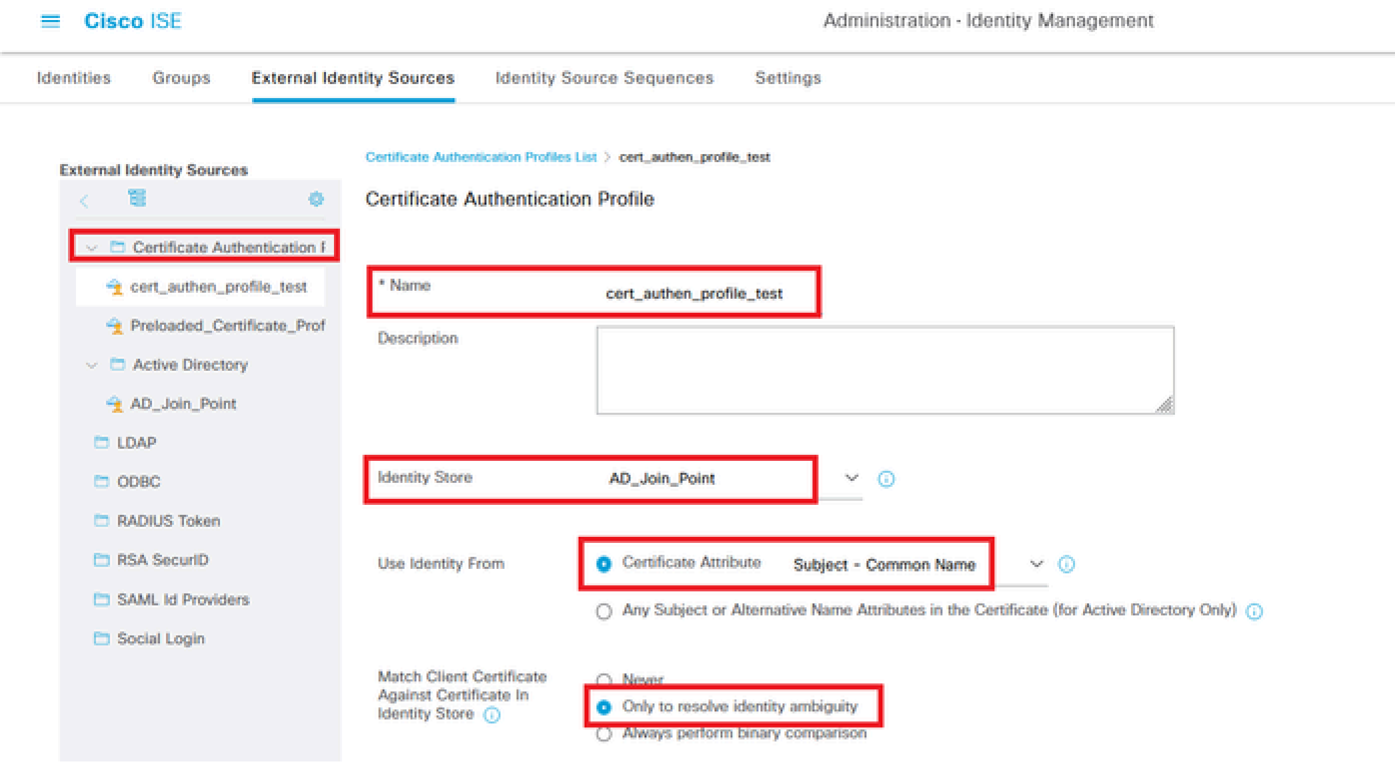
Verificar Publicadores de Certificados

Etapa 3. Adicionar perfil de autenticação de certificado

Navegue para Administração > Fontes de identidade externas > Perfil de autenticação de certificado, clique no botão Adicionar para adicionar um novo perfil de autenticação de certificado.

- Nome: cert_authen_profile_test
- Repositório de Identidades: AD_Join_Point
- Usar identidade do atributo do certificado: assunto - nome comum.
- Corresponder Certificado de Cliente ao Certificado no Repositório de Identidades: Somente

para resolver a ambiguidade de identidade.



Cisco ISE — Administration · Identity Management

External Identity Sources

- Certificate Authentication P
  - cert_authen_profile_test
  - Preloaded_Certificate_Prof
- Active Directory
  - AD_Join_Point
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- SAML Id Providers
- Social Login

Certificate Authentication Profiles List > cert_authen_profile_test

Certificate Authentication Profile

* Name: cert_authen_profile_test

Description:

Identity Store: AD_Join_Point

Use Identity From:
● Certificate Attribute: Subject - Common Name
○ Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only)

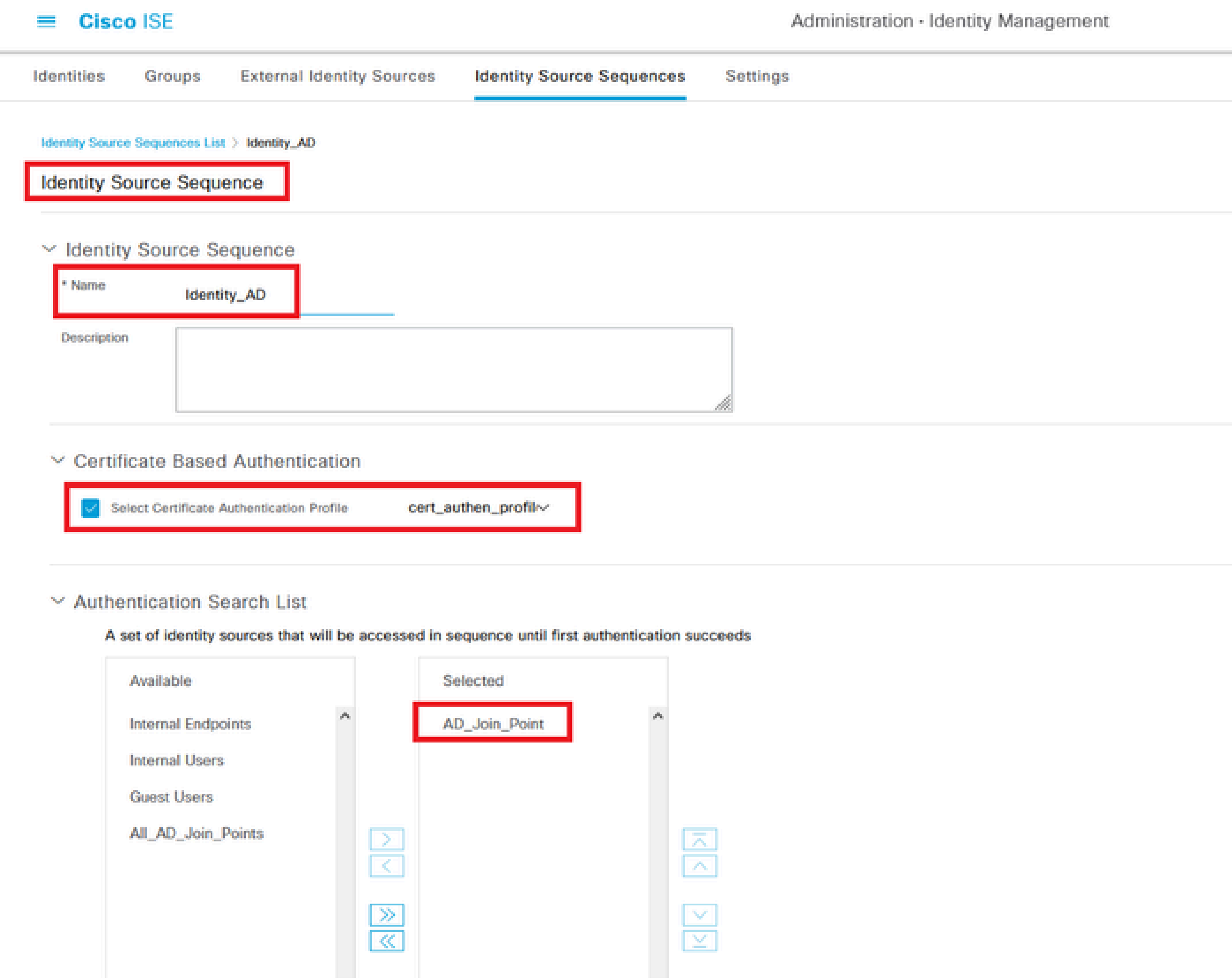
Match Client Certificate Against Certificate In Identity Store:
○ Never
● Only to resolve identity ambiguity
○ Always perform binary comparison

Adicionar perfil de autenticação de certificado

Etapa 4. Adicionar sequência de origem de identidade

Navegue até Administração > Sequências de origem de identidade, adicione uma Sequência de origem de identidade.

- Nome: Identity_AD
- Selecione Certificar Autenticação Profile: cert_authen_profile_test
- Lista de pesquisa de autenticação: AD_Join_Point



Cisco ISE — Administration · Identity Management

Identities | Groups | External Identity Sources | Identity Source Sequences | Settings

Identity Source Sequences List > Identity_AD

Identity Source Sequence

Identity Source Sequence

* Name: Identity_AD

Description:

Certificate Based Authentication

☑ Select Certificate Authentication Profile: cert_authen_profil

Authentication Search List

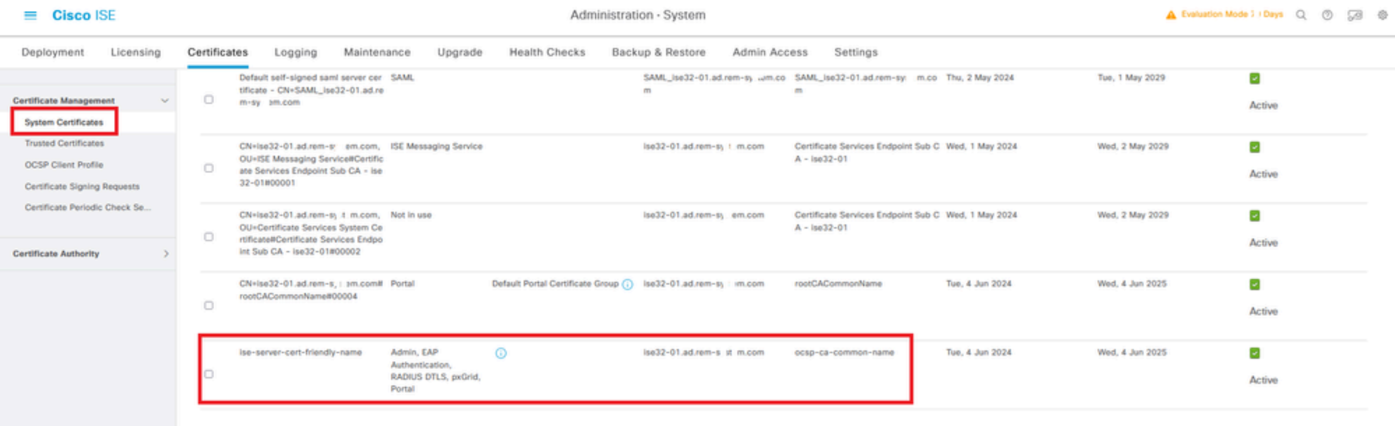
A set of identity sources that will be accessed in sequence until first authentication succeeds

Available	Selected
Internal Endpoints	AD_Join_Point
Internal Users	
Guest Users	
All_AD_Join_Points	

Adicionar Sequências de Origem de Identidade

Etapa 5. Confirmar certificado no ISE

Navegue até Administration > Certificates > System Certificates, confirme se o certificado do servidor está assinado pela CA confiável.



Cisco ISE — Administration · System

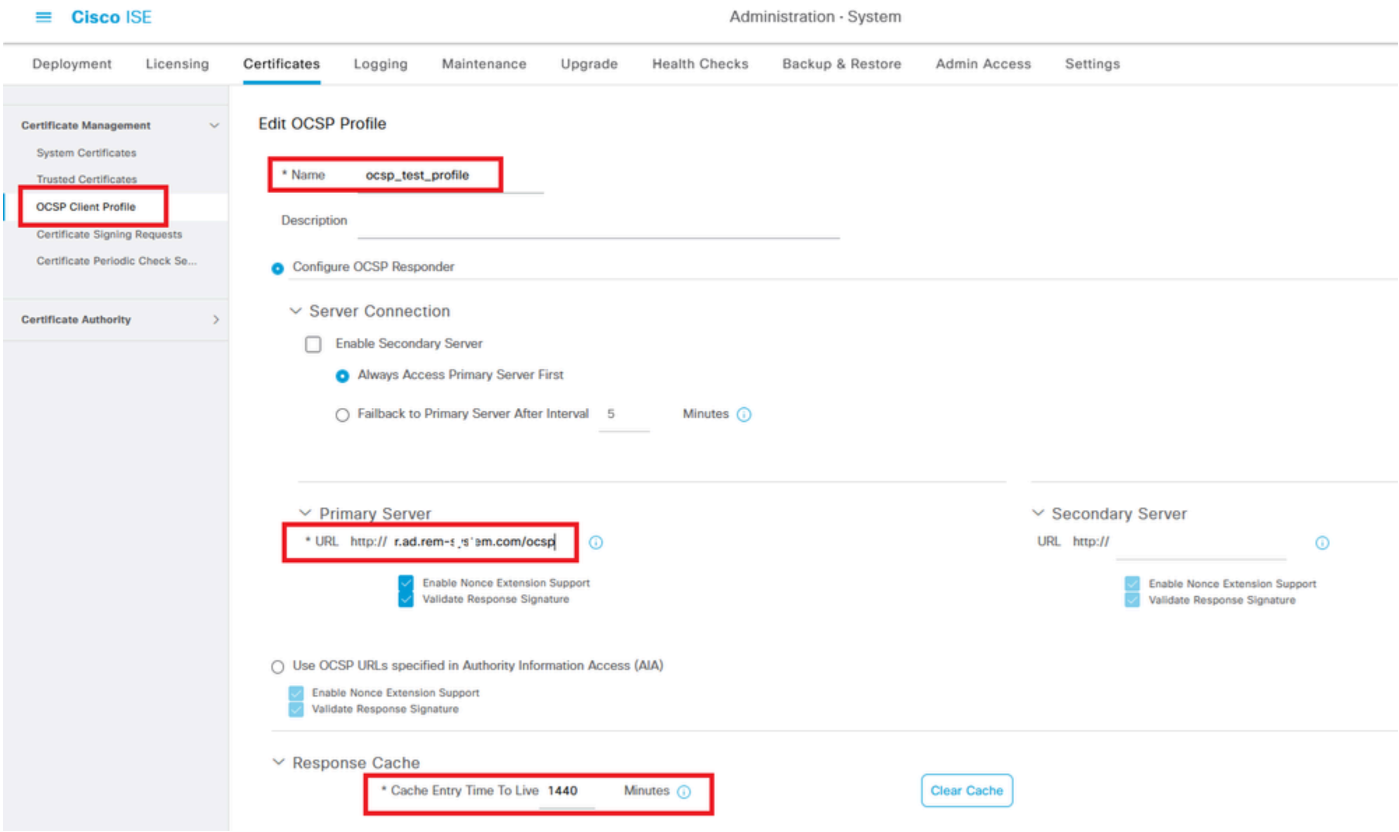
Deployment | Licensing | Certificates | Logging | Maintenance | Upgrade | Health Checks | Backup & Restore | Admin Access | Settings

□	Default self-signed saml server certificate - CN=SAML_ise32-01.ad.rem-sy m.com	SAML		SAML_ise32-01.ad.rem-sy m.com	SAML_ise32-01.ad.rem-sy m.com	Thu, 2 May 2024	Tue, 1 May 2029	✓ Active
□	CN=ise32-01.ad.rem-s em.com, OU=ISE Messaging Service#Certificate Services Endpoint Sub CA - ise32-01#00001	ISE Messaging Service		ise32-01.ad.rem-sy m.com	Certificate Services Endpoint Sub CA - ise32-01	Wed, 1 May 2024	Wed, 2 May 2029	✓ Active
□	CN=ise32-01.ad.rem-sy m.com, OU=Certificate Services System Certificate#Certificate Services Endpoint Sub CA - ise32-01#00002	Not in use		ise32-01.ad.rem-sy em.com	Certificate Services Endpoint Sub CA - ise32-01	Wed, 1 May 2024	Wed, 2 May 2029	✓ Active
□	CN=ise32-01.ad.rem-s m.com#rootCACommonName#00004	Portal	Default Portal Certificate Group ⓘ	ise32-01.ad.rem-sy m.com	rootCACommonName	Tue, 4 Jun 2024	Wed, 4 Jun 2025	✓ Active
□	ise-server-cert-friendly-name	Admin, EAP Authentication, RADIUS DTLS, pxGrid, Portal	ⓘ	ise32-01.ad.rem-s m.com	ocsp-ca-common-name	Tue, 4 Jun 2024	Wed, 4 Jun 2025	✓ Active

Server Certificate

Navegue até Administration > Certificates > OCSP Client Profile, clique no botão Add para adicionar um novo perfil de cliente OCSP.

- Nome: ocsp_test_profile
- Configurar URL do Respondente OCSP: http://winserver.ad.rem-xxx.com/ocsp



Edit OCSP Profile

* Name ocsp_test_profile

Description

● Configure OCSP Responder

Server Connection

□ Enable Secondary Server

● Always Access Primary Server First

○ Failback to Primary Server After Interval 5 Minutes

Primary Server

* URL http:// r.ad.rem-s ys em.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)

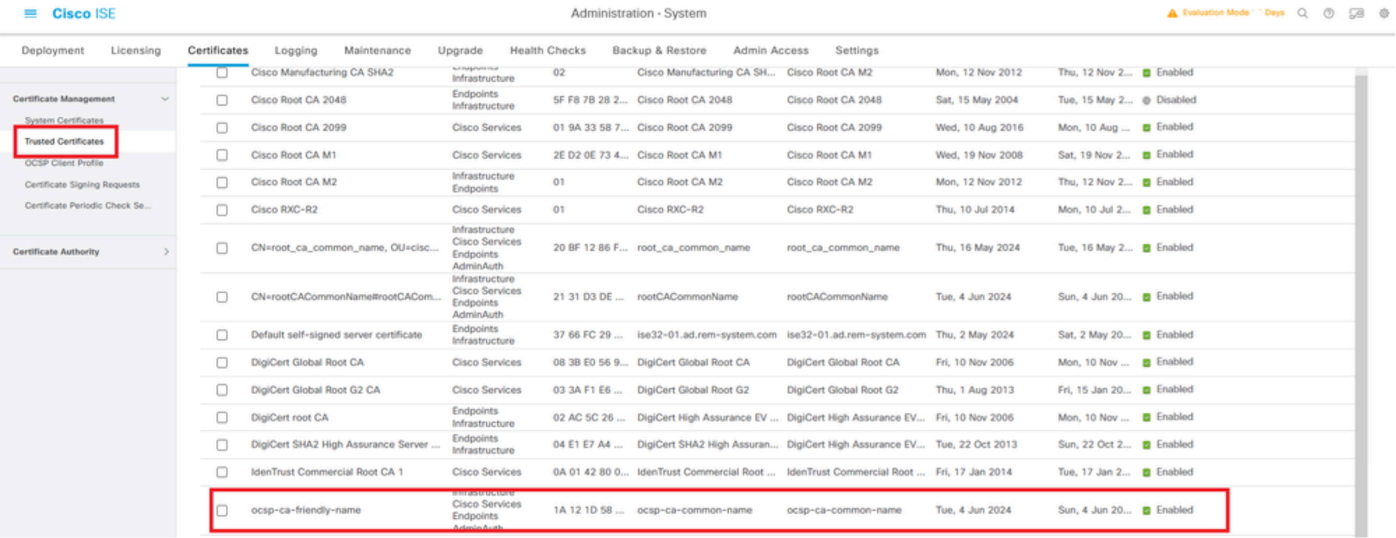
☑ Enable Nonce Extension Support
☑ Validate Response Signature

Response Cache

* Cache Entry Time To Live 1440 Minutes

Perfil do cliente OCSP

Navegue até Administration > Certificates > Trusted Certificates, confirme se a CA confiável foi importada para o ISE.

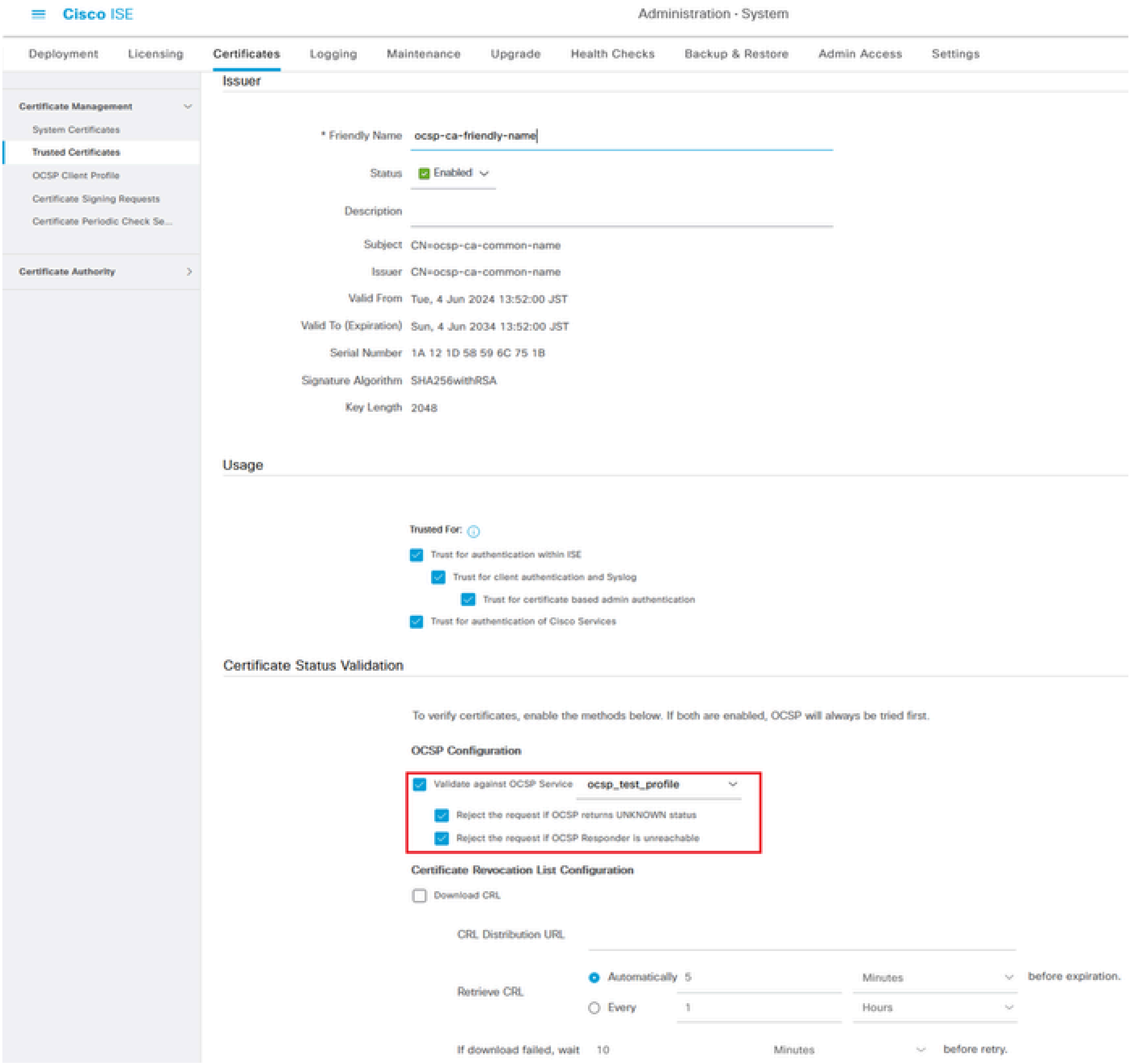


□	Cisco Manufacturing CA SHA2	Endpoints Infrastructure	02	Cisco Manufacturing CA SH...	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2...	Enabled
□	Cisco Root CA 2048	Endpoints Infrastructure	5F F8 7B 28 2...	Cisco Root CA 2048	Cisco Root CA 2048	Sat, 15 May 2004	Tue, 15 May 2...	Disabled
□	Cisco Root 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
□	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 2...	Enabled
□	Cisco Root CA M2	Infrastructure Endpoints	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2...	Enabled
□	Cisco RXC-R2	Cisco Services	01	Cisco RXC-R2	Cisco RXC-R2	Thu, 10 Jul 2014	Mon, 10 Jul 2...	Enabled
□	CN=root_ca_common_name, OU=cisc...	Infrastructure Cisco Services Endpoints AdminAuth	20 BF 12 86 F...	root_ca_common_name	root_ca_common_name	Thu, 16 May 2024	Tue, 16 May 2...	Enabled
□	CN=rootCACommonName#rootCACom...	Infrastructure Cisco Services Endpoints AdminAuth	21 31 D3 DE ...	rootCACommonName	rootCACommonName	Tue, 4 Jun 2024	Sun, 4 Jun 20...	Enabled
□	Default self-signed server certificate	Endpoints 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
□	DigiCert Global Root CA	Cisco Services	08 3B E0 56 9...	DigiCert Global Root CA	DigiCert Global Root CA	Fri, 10 Nov 2006	Mon, 10 Nov ...	Enabled
□	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
□	DigiCert root CA	Endpoints Infrastructure	02 AC 5C 26 ...	DigiCert High Assurance EV ...	DigiCert High Assurance EV...	Fri, 10 Nov 2006	Mon, 10 Nov ...	Enabled
□	DigiCert SHA2 High Assurance Server ...	Endpoints Infrastructure	04 E1 E7 A4 ...	DigiCert SHA2 High Assuran...	DigiCert High Assurance EV...	Tue, 22 Oct 2013	Sun, 22 Oct 2...	Enabled
□	IdenTrust Commercial Root CA 1	Cisco Services	0A 01 42 80 0...	IdenTrust Commercial Root ...	IdenTrust Commercial Root ...	Fri, 17 Jan 2014	Tue, 17 Jan 2...	Enabled
□	ocsp-ca-friendly-name	Infrastructure Cisco Services Endpoints AdminAuth	1A 12 1D 58 ...	ocsp-ca-common-name	ocsp-ca-common-name	Tue, 4 Jun 2024	Sun, 4 Jun 20...	Enabled

CA confiável

Verifique a CA e clique no botão Edit, insira os detalhes da configuração OCSP para Certificate Status Validation.

- Validar com base no Serviço OCSP: ocsp_test_profile
- Rejeitar a solicitação se o OCSP retornar o status DESCONHECIDO: marque
- Rejeitar a solicitação se o Respondente OCSP estiver inacessível: marque



Issuer

* Friendly Name: ocsp-ca-friendly-name

Status: ☑ Enabled

Description:

Subject: CN=ocsp-ca-common-name

Issuer: CN=ocsp-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: ocsp_test_profile

☑ 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:

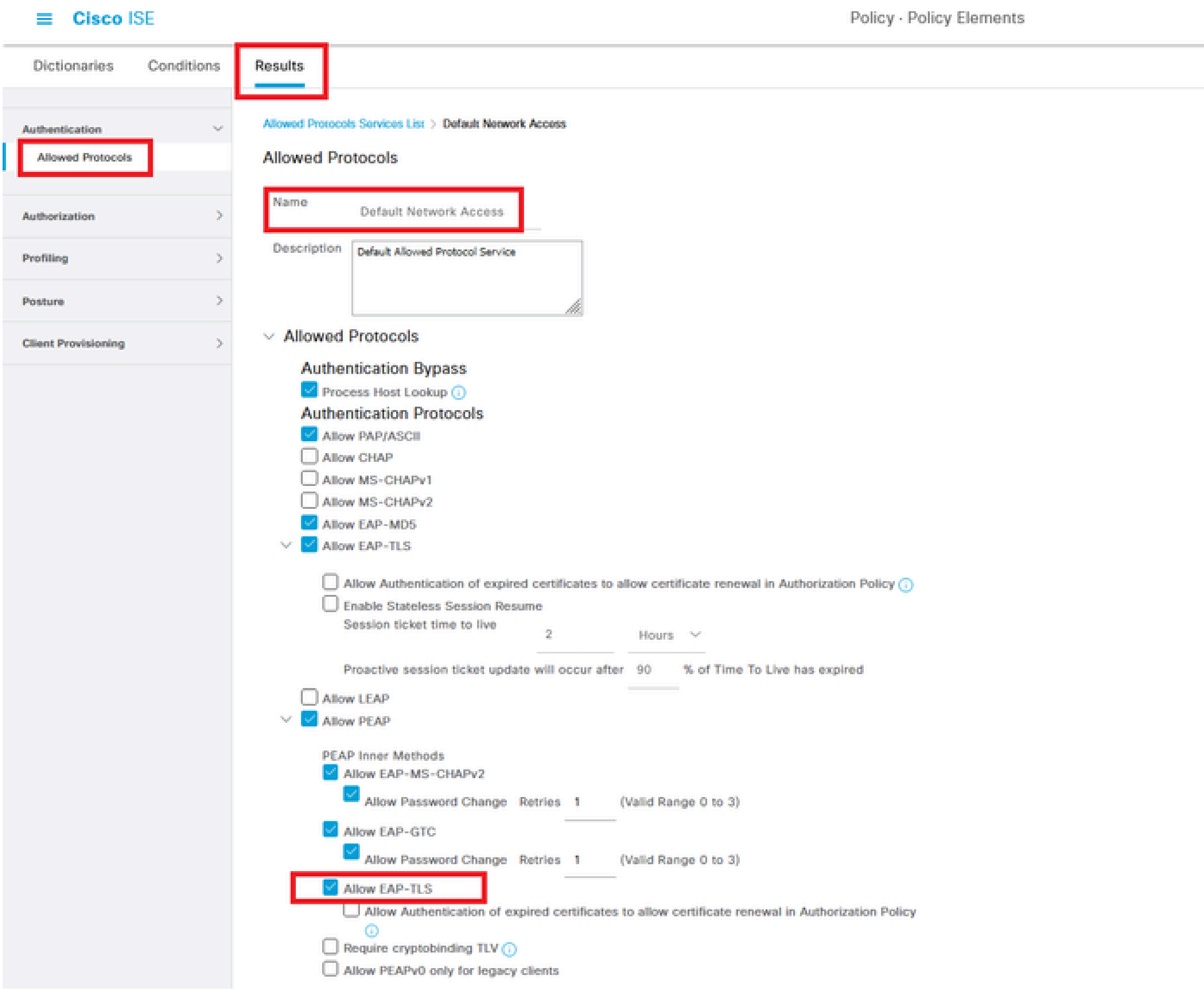
Retrieve CRL: ● Automatically 5 Minutes before expiration. ○ Every 1 Hours

If download failed, wait 10 Minutes before retry.

Validação do status do certificado

Etapa 6. Adicionar protocolos permitidos

Navegue para Policy > Results > Authentication > Allowed Protocols, edite a lista de serviços Default Network Access e marque Allow EAP-TLS.



Cisco ISE — Policy · Policy Elements

Dictionaries | 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

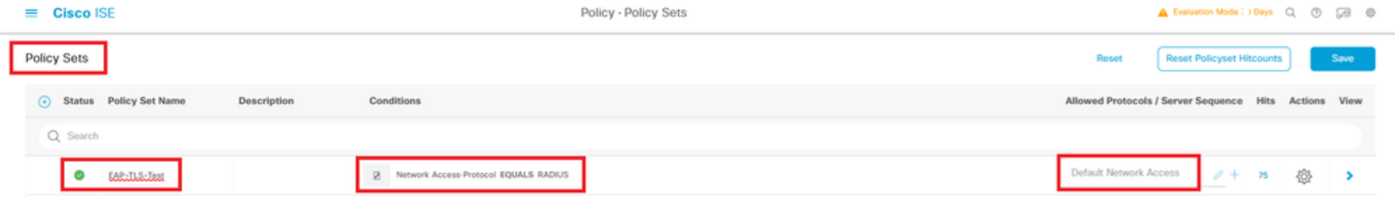
- PEAP Inner Methods
- ☑ Allow EAP-MS-CHAPv2
  - ☑ Allow Password Change Retries 1 (Valid Range 0 to 3)
- ☑ Allow EAP-GTC
  - ☑ Allow Password Change Retries 1 (Valid Range 0 to 3)
- ☑ Allow EAP-TLS
  - □ Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy
- □ Require cryptobinding TLV
- □ Allow PEAPv0 only for legacy clients

Permitir EAP-TLS

Passo 7. Adicionar conjunto de políticas

Navegue para Política > Conjuntos de políticas, clique em + para adicionar um conjunto de políticas.

- Nome do conjunto de políticas: EAP-TLS-Test
- Condições: Network Access Protocol EQUALS RADIUS
- Protocolos Permitidos/Sequência de Servidores: Acesso Padrão à Rede



Cisco ISE — Policy · Policy Sets

Policy Sets

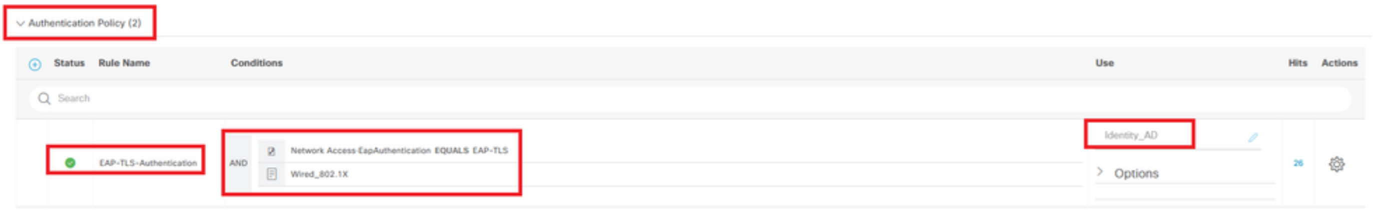
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	EAP-TLS-Test		Network Access Protocol EQUALS RADIUS	Default Network Access	75		

Adicionar conjunto de políticas

Etapa 8. Adicionar política de autenticação

Navegue até Policy Sets, clique em EAP-TLS-Test para adicionar uma política de autenticação.

- Nome da regra: Autenticação EAP-TLS
- Condições: Network Access EapAuthentication EQUALS EAP-TLS AND Wired_802.1 X
- Uso: Identity_AD



Authentication Policy (2)

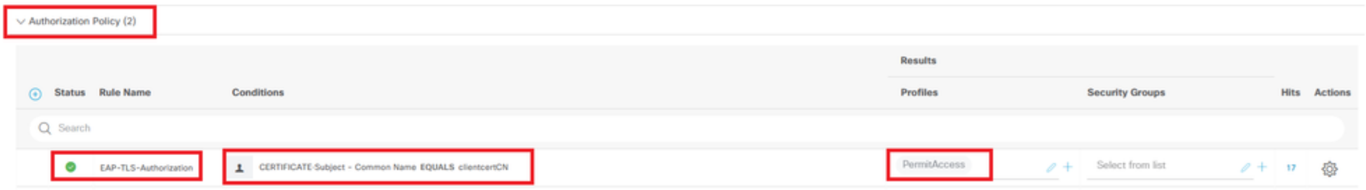
Status	Rule Name	Conditions	Use	Hits	Actions
●	EAP-TLS-Authentication	AND Network Access·EapAuthentication EQUALS EAP-TLS Wired_802.1X	Identity_AD Options	26	⚙

Adicionar política de autenticação

Etapa 9. Adicionar Política de Autorização

Navegue até Policy Sets, clique em EAP-TLS-Test para adicionar uma política de autorização.

- Nome da regra: EAP-TLS-Authorization
- Condições: CERTIFICATE Subject - Common Name EQUALS clientcertCN
- Resultados: PermitAccess



Authorization Policy (2)

Status	Rule Name	Conditions	Results Profiles	Security Groups	Hits	Actions
●	EAP-TLS-Authorization	CERTIFICATE·Subject - Common Name EQUALS clientcertCN	PermitAccess	Select from list	17	⚙

Adicionar Política de Autorização

Verificar

Etapa 1. Confirmar sessão de autenticação

Executeshow authentication sessions interface GigabitEthernet1/0/3 details o comando para confirmar a sessão de autenticação no C1000.

<#root>

Switch#

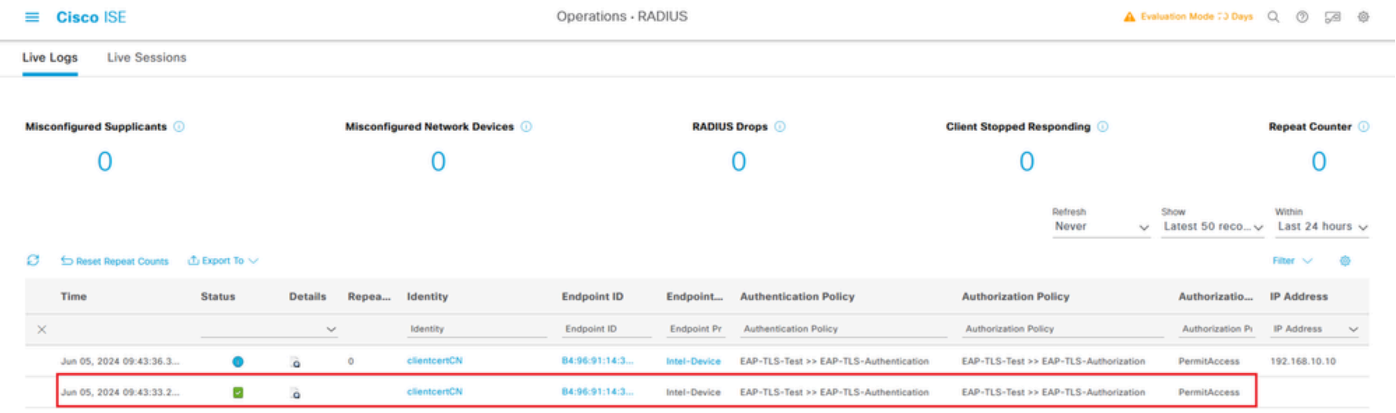
show authentication sessions interface GigabitEthernet1/0/3 details

```
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
```

Etapa 2. Confirmar registro ao vivo do Radius

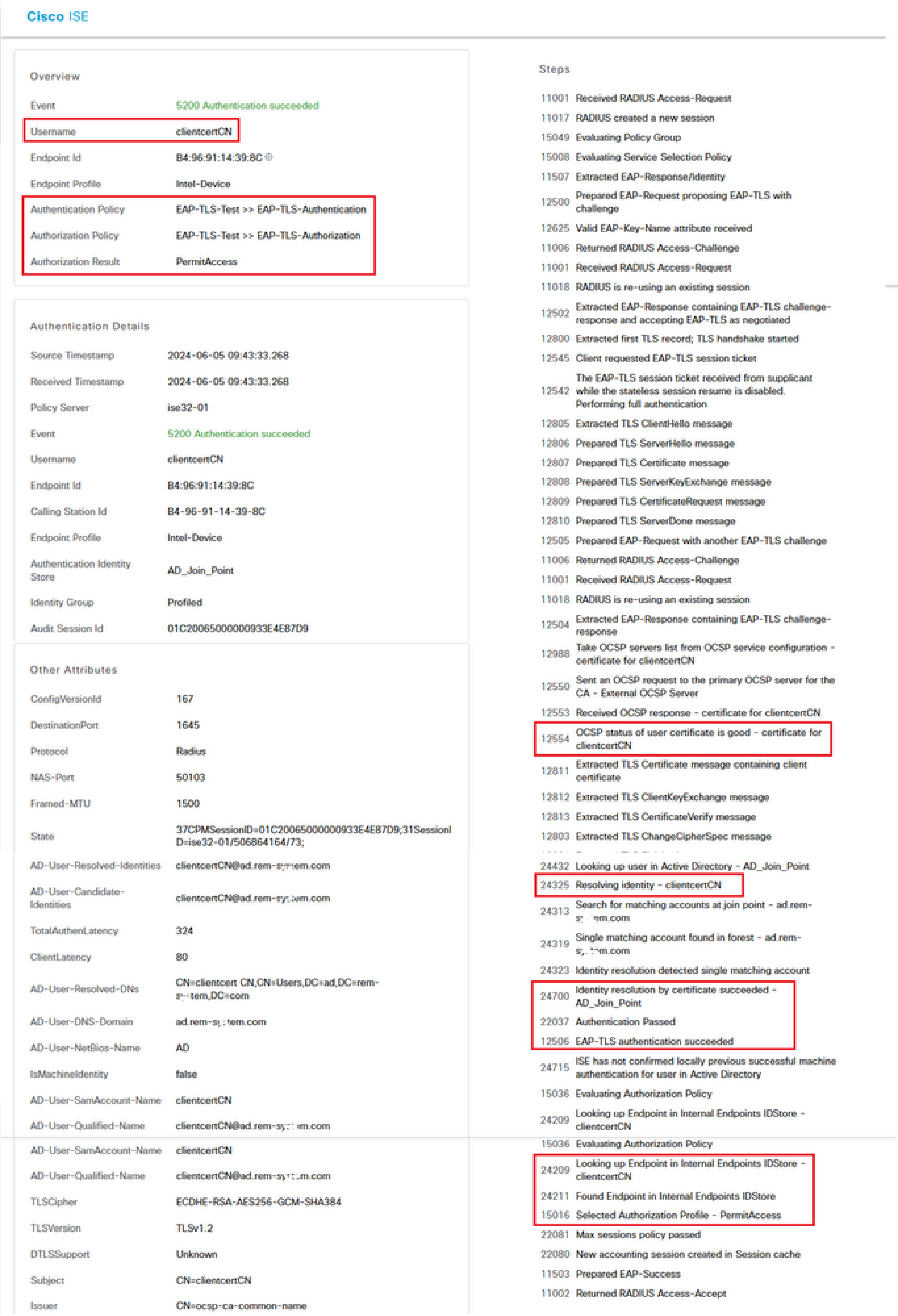
Navegue até **Operations** > **RADIUS** > **Live** Logons na GUI do ISE e confirme o registro em tempo real para autenticação.



Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authentication Policy	Authorization Policy	Authorizatio...	IP Address
Jun 05, 2024 09:43:36.3...	●		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...	✓			clientcertCN	B4:96:91:14:3...	Intel-Device	EAP-TLS-Test >> EAP-TLS-Authentication	EAP-TLS-Test >> EAP-TLS-Authorization	PermitAccess	

Log ao vivo do Radius

Confirme o registro ao vivo detalhado da autenticação.



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	01C20065000000933E4E87D9

Other Attributes

ConfigVersionId	167
DestinationPort	1645
Protocol	Radius
NAS-Port	50103
Framed-MTU	1500
State	37CPMSessionID=01C20065000000933E4E87D9;31SessionID=ise32-01/506864164/73;
AD-User-Resolved-Identities	clientcertCN@ad.rem-s[redacted]em.com
AD-User-Candidate-Identities	clientcertCN@ad.rem-sy[redacted]em.com
TotalAuthenLatency	324
ClientLatency	80
AD-User-Resolved-DNs	CN=clientcert CN,CN=Users,DC=ad,DC=rem-s[redacted]tem,DC=com
AD-User-DNS-Domain	ad.rem-s[redacted]tem.com
AD-User-NetBios-Name	AD
IsMachineIdentity	false
AD-User-SamAccount-Name	clientcertCN
AD-User-Qualified-Name	clientcertCN@ad.rem-sy[redacted]em.com
AD-User-SamAccount-Name	clientcertCN
AD-User-Qualified-Name	clientcertCN@ad.rem-sy[redacted]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
[illegible]	[illegible]
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[redacted]em.com
24319	Single matching account found in forest - ad.rem-s[redacted]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

Detalhes da autenticação

```
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
```

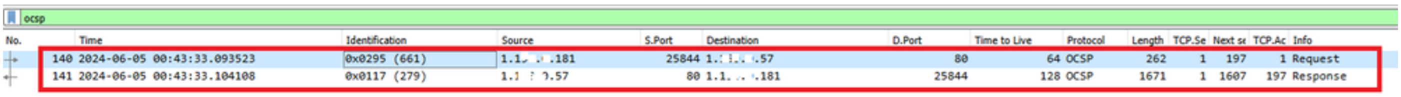
`Code=5(AccountingResponse)`

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

2. Despejo TCP

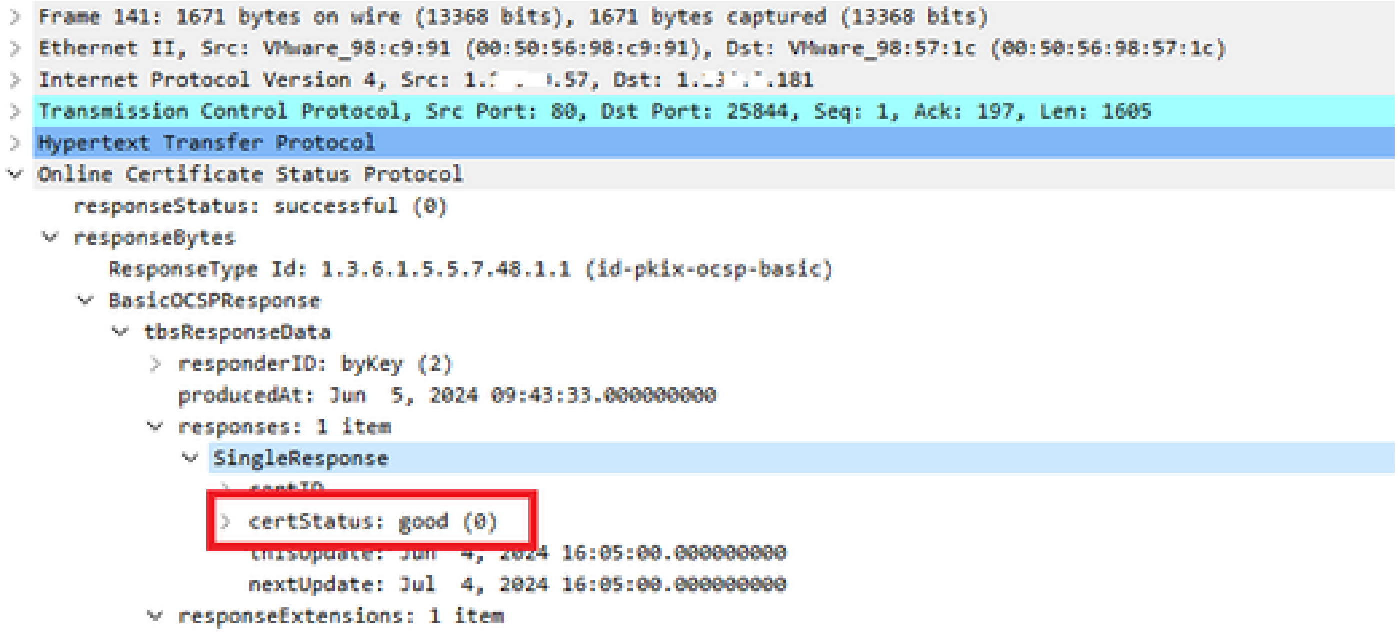
No dump TCP no ISE, você espera encontrar informações sobre a resposta OCSP e a sessão Radius.

Solicitação e resposta OCSP:



```
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.[redacted].181  25844  1.[redacted].57     80       64  OCSP       262       1      197       1  Request
141  2024-06-05 00:43:33.104108  0x0117 (279)    1.[redacted].57        80  1.1.[redacted].181  25844   128  OCSP      1671       1     1607     197  Response
```

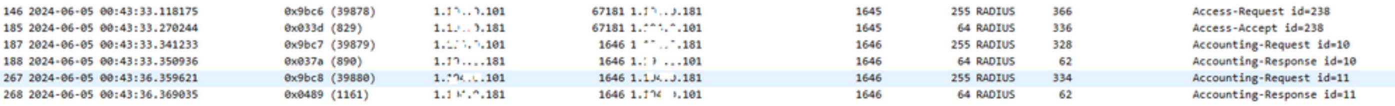
Captura de pacotes de solicitação e resposta OCSP



```
> 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.[redacted].57, Dst: 1.[redacted].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
```

Capturar Detalhes da Resposta OCSP

Sessão Radius:



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

Captura de pacote de sessão Radius

Informações Relacionadas

Configurar a autenticação EAP-TLS com ISE

Configurar certificados TLS/SSL no ISE