ISEでOCSPによるEAP-TLS認証を設定する

内容

はじめに

このドキュメントでは、リアルタイムのクライアント証明書失効チェックのためにOCSPでEAP-TLS認証を設定するために必要な手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Identity Services Engineの設定
- Cisco Catalyst設定
- オンライン証明書ステータスプロトコル

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

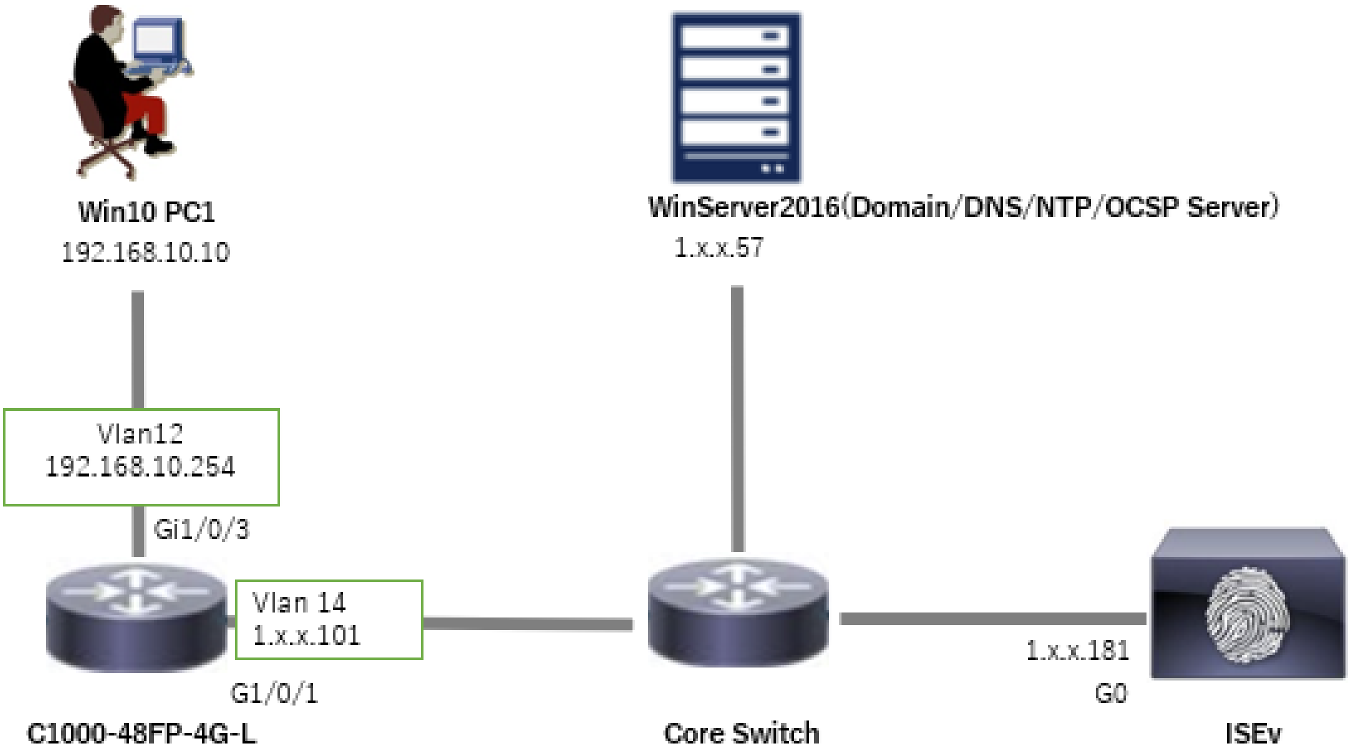
- Identity Services Engine仮想3.2パッチ6
- C1000-48FP-4G-L 15.2(7)E9

- Windows Server 2016
- Windows 10

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

ネットワーク図

次の図は、このドキュメントの例で使用するトポロジを示しています。



ネットワーク図

背景説明

EAP-TLSでは、認証プロセスの一部として、クライアントがサーバにデジタル証明書を提示します。 このドキュメントでは、ADサーバに対して証明書の共通名(CN)を確認し、リアルタイムのプロトコルステータスを提供するOCSP(Online Certificate Status Protocol)を使用して証明書が失効したかどうかを確認することによって、ISEがクライアント証明書を検証する方法について説明します。

Windows Server 2016で設定されるドメイン名は、このドキュメントの例で使用するad.rem-xxx.comです。

このドキュメントで参照されているOCSP(Online Certificate Status Protocol)およびAD(Active Directory)サーバは、証明書の検証に使用されます。

- Active DirectoryのFQDN:winserver.ad.rem-xxx.com
- CRLディストリビューションURL:http://winserver.ad.rem-xxx.com/ocsp-ca.crl
- 機関のURL:http://winserver.ad.rem-xxx.com/ocsp

これは、ドキュメントで使用される各証明書の共通名を持つ証明書チェーンです。

- CA: ocsp-ca-common-name
- クライアント証明書：clientcertCN
- サーバ証明書：ise32-01.ad.rem-xxx.com
- OCSP署名証明書： ocspSignCommonName

コンフィギュレーション

C1000での設定

これは、C1000 CLIでの最小限の設定です。

```
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
```

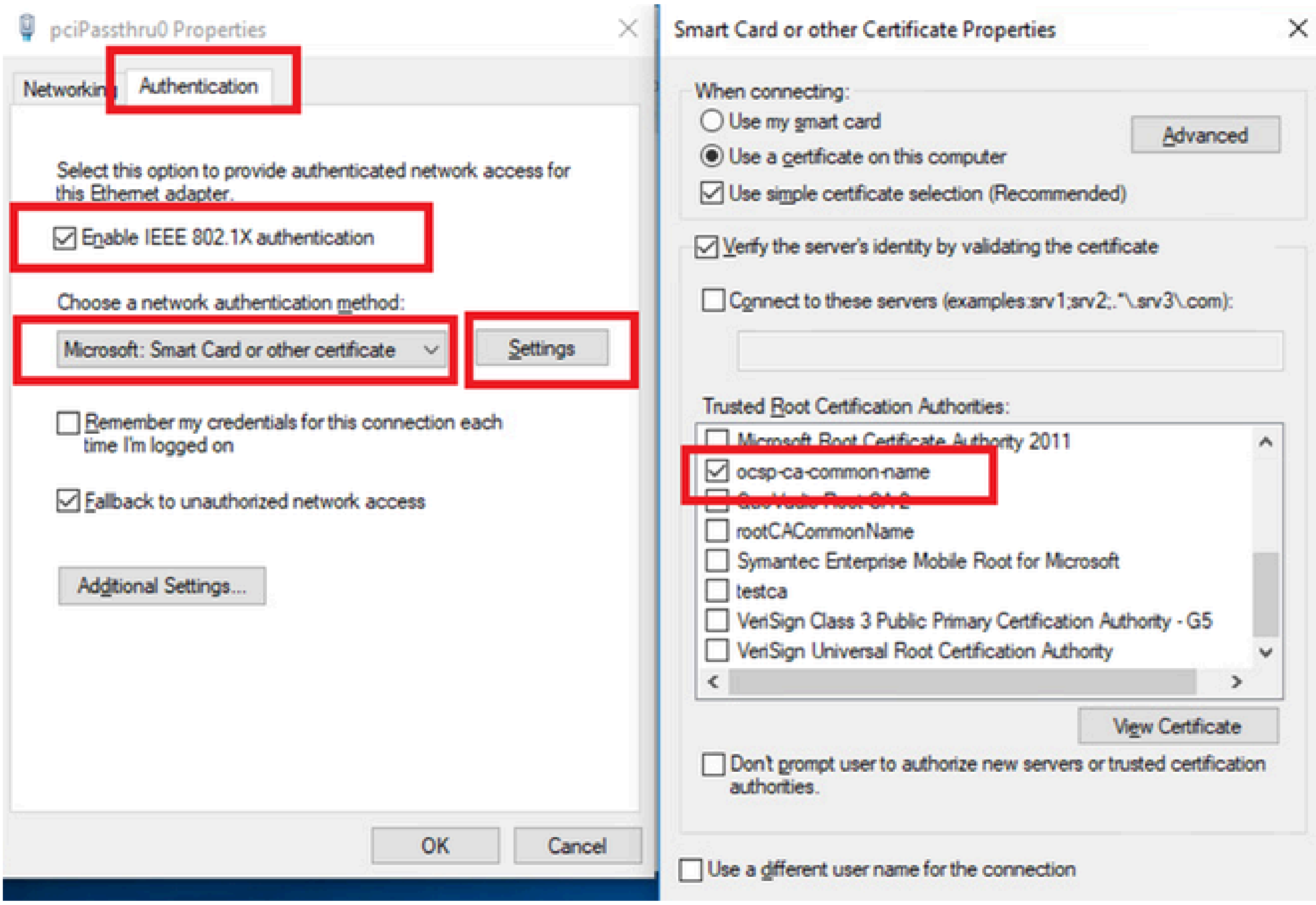
```
interface GigabitEthernet1/0/3
switchport access vlan 12
switchport mode access
authentication host-mode multi-auth
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge
```

Windows PCでの設定

ステップ 1：ユーザ認証の設定

Authenticationに移動し、checkEnable IEEE 802.1X authentication にチェックマークを付けて、Microsoft: Smart Card or other certificateを選択します。

Settingsボタンをクリックし、Use a certificate on this computerにチェックマークを入れて、Windows PCの信頼済みCAを選択します。



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 Settings

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

☑ Fallback to unauthorized network access

Additional Settings...

OK Cancel

Smart Card or other Certificate Properties

When connecting:

○ Use my smart card Advanced

● 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

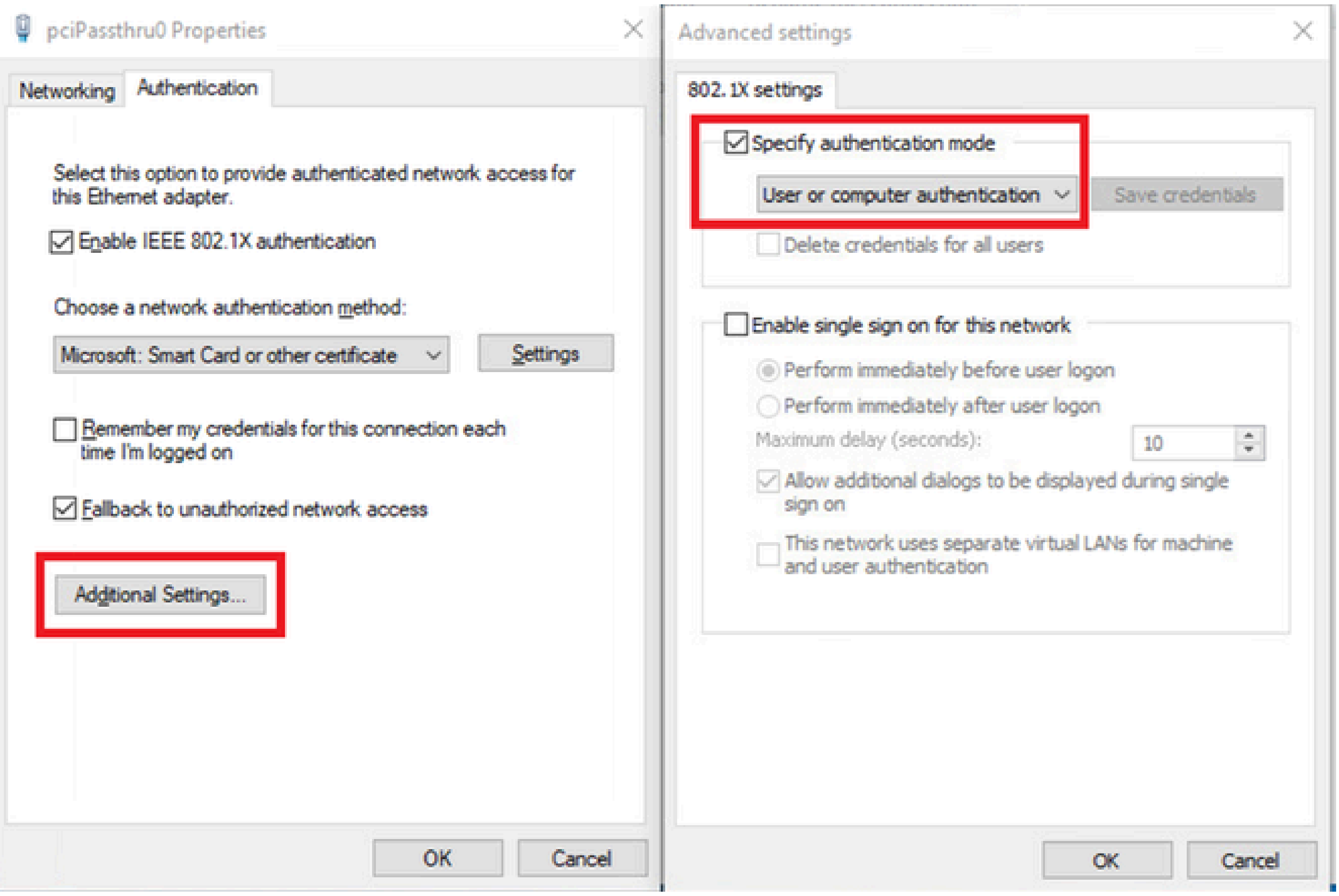
View Certificate

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

☐ Use a different user name for the connection

証明書認証の有効化

Authenticationに移動し、Additional Settingsをチェックします。ドロップダウンリストからUserまたはcomputer authenticationfromを選択します。



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

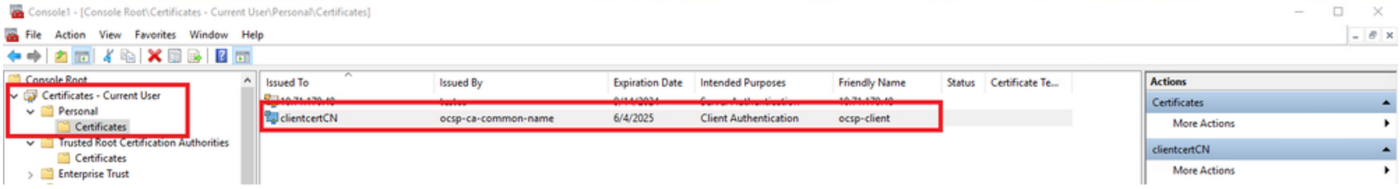
☑ Allow additional dialogs to be displayed during single sign on

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

認証モードの指定

ステップ２：クライアント証明書の確認

Certificates - Current User > Personal > Certificatesの順に移動し、認証に使用するクライアント証明書を確認します。



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

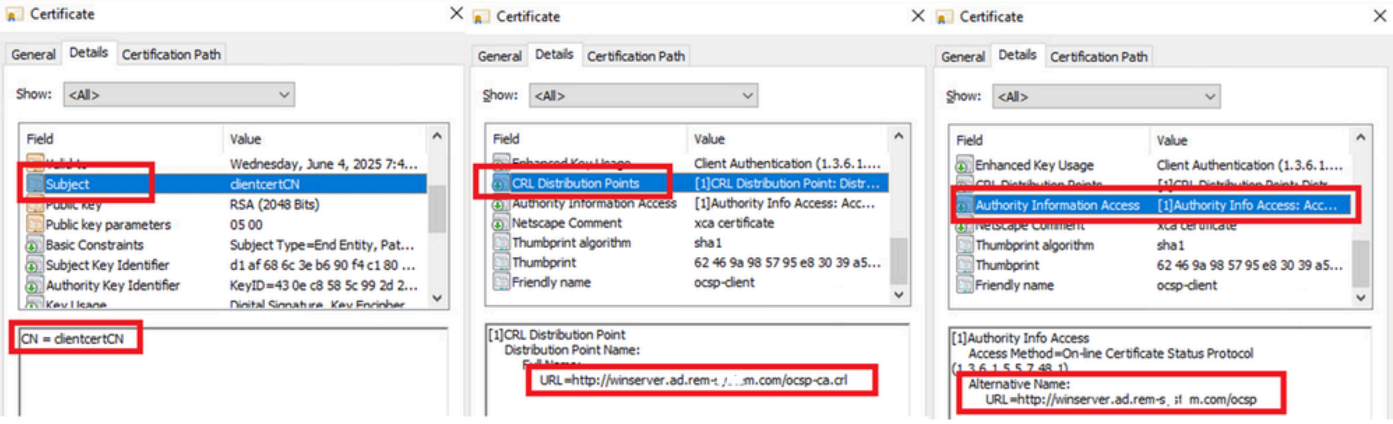
Console Root
- Certificates - Current User
  - Personal
    - Certificates
  - Trusted Root Certification Authorities
    - Certificates
  - Enterprise Trust

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		

クライアント証明書の確認

クライアント証明書をダブルクリックし、Detailsに移動して、Subject、CRL Distribution Points、Authority Information Accessの詳細をチェックします。

- 件名：CN = clientcertCN
- CRL分散ポイント:http://winserver.ad.rem-xxx.com/ocsp-ca.crl
- 機関情報アクセス:http://winserver.ad.rem-xxx.com/ocsp



Certificate

Show: <All>

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

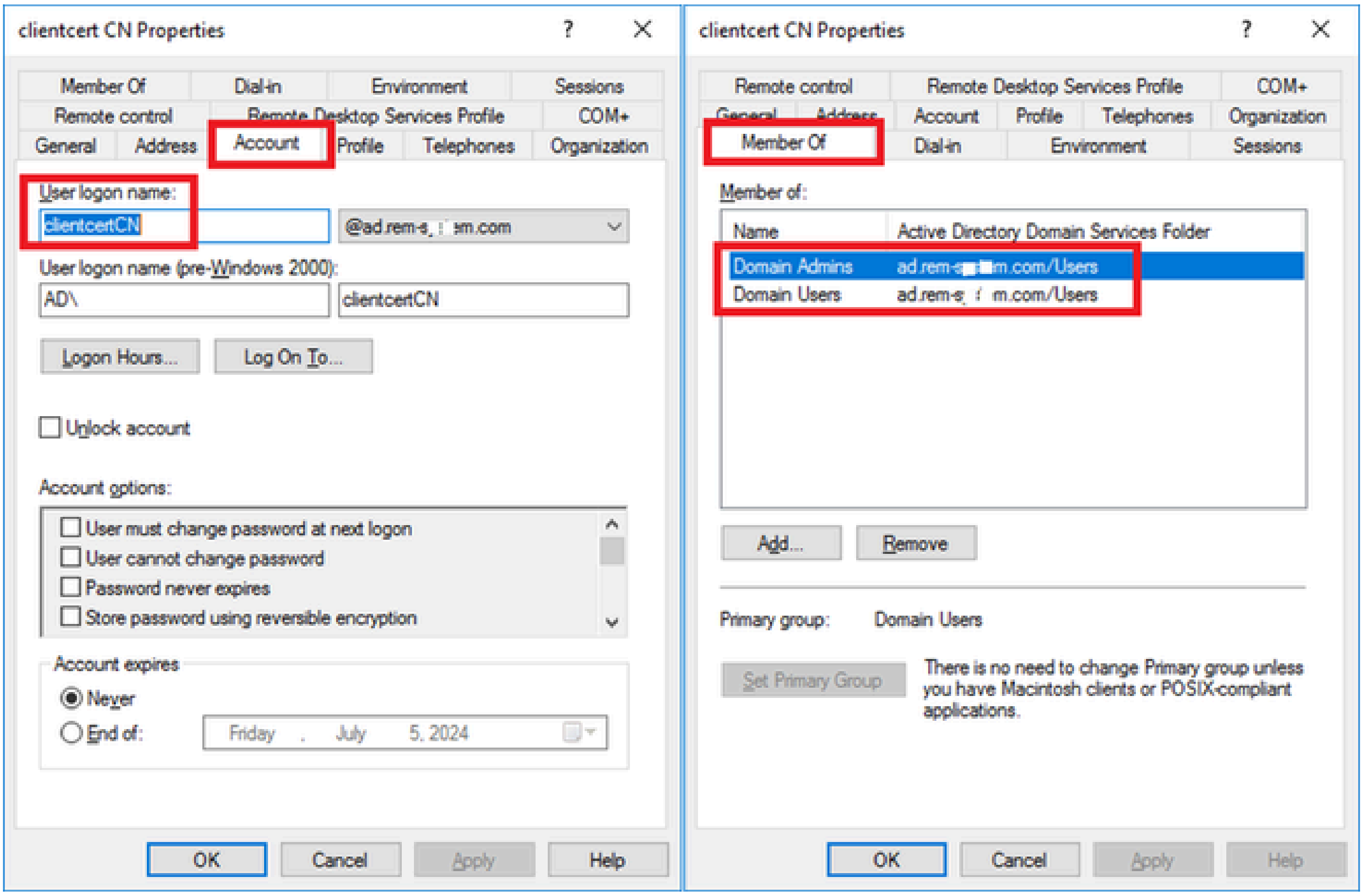
[1]Authority Info Access
Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)
Alternative Name:
URL=http://winserver.ad.rem-s[redacted]m.com/ocsp

クライアント証明書の詳細

Windows Serverでの設定

ステップ 1：ユーザの追加

Active Directory Users and Computersに移動し、Usersをクリックします。ユーザのログオン名としてclientcertCNを追加します。



clientcert CN Properties

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

clientcert CN Properties

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

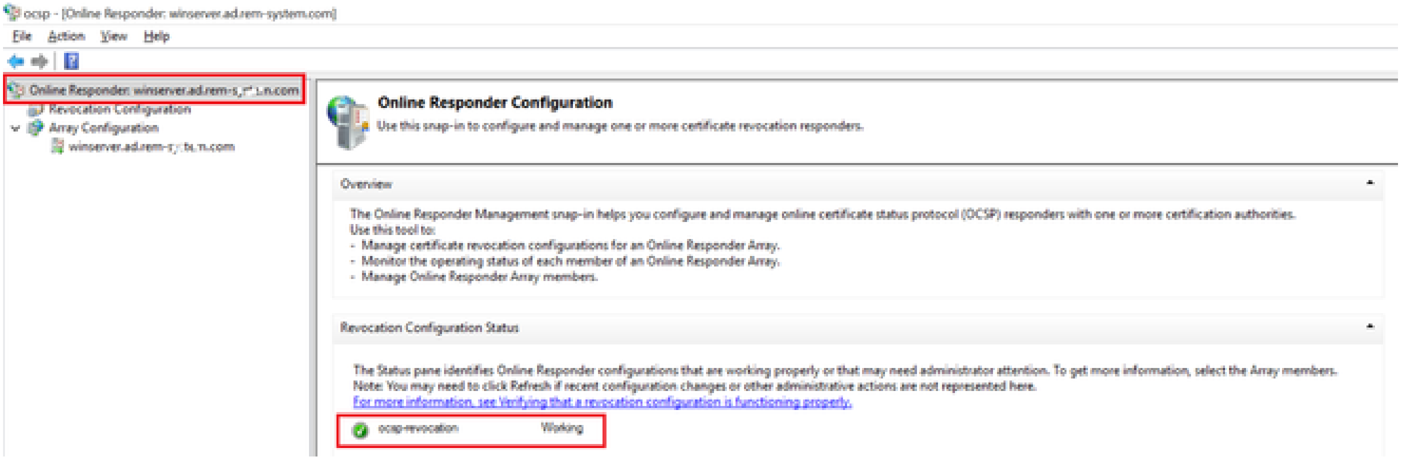
Primary group: Domain Users

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

ユーザーログオン名

ステップ 2：OCSPサービスの確認

Windowsに移動し、オンラインレスポンダー管理をクリックします。OCSPサーバのステータスを確認します。



ocsp - [Online Responder: winserver.ad.rem-system.com]

- Online Responder: winserver.ad.rem-s[illegible].com
  - Revocation Configuration
  - Array Configuration
    - winserver.ad.rem-s[illegible].com

Online Responder Configuration

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

Overview

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.

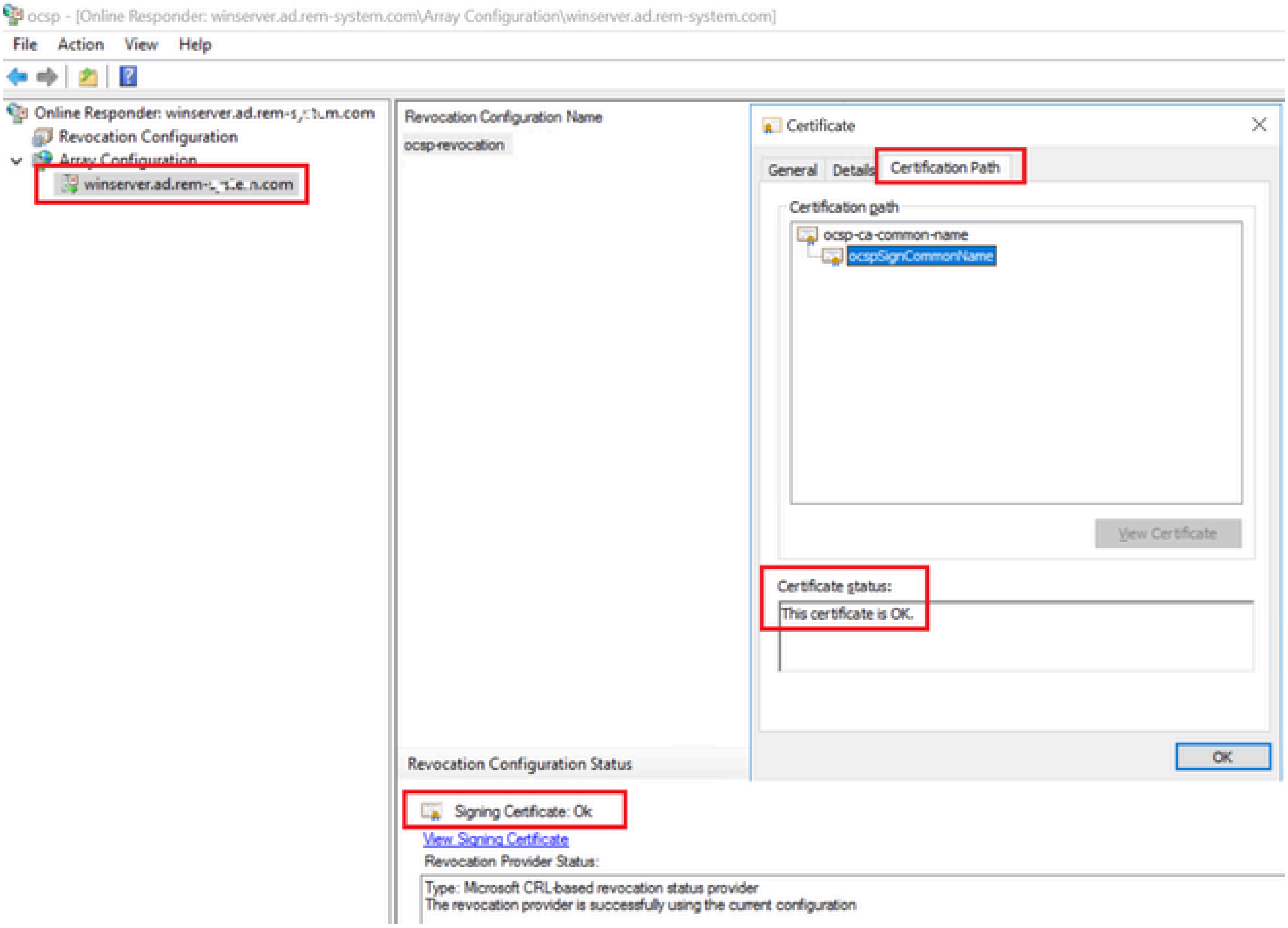
Revocation Configuration Status

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

OCSPサーバのステータス

winserver.ad.rem-xxx.comをクリックし、OCSP署名証明書のステータスを確認します。



ocsp - [Online Responder: winserver.ad.rem-system.com\Array Configuration\winserver.ad.rem-system.com]

- Online Responder: winserver.ad.rem-s[illegible]m.com
  - Revocation Configuration
  - Array Configuration
    - winserver.ad.rem-[illegible].com

Revocation Configuration Name

ocsp-revocation

Certificate

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

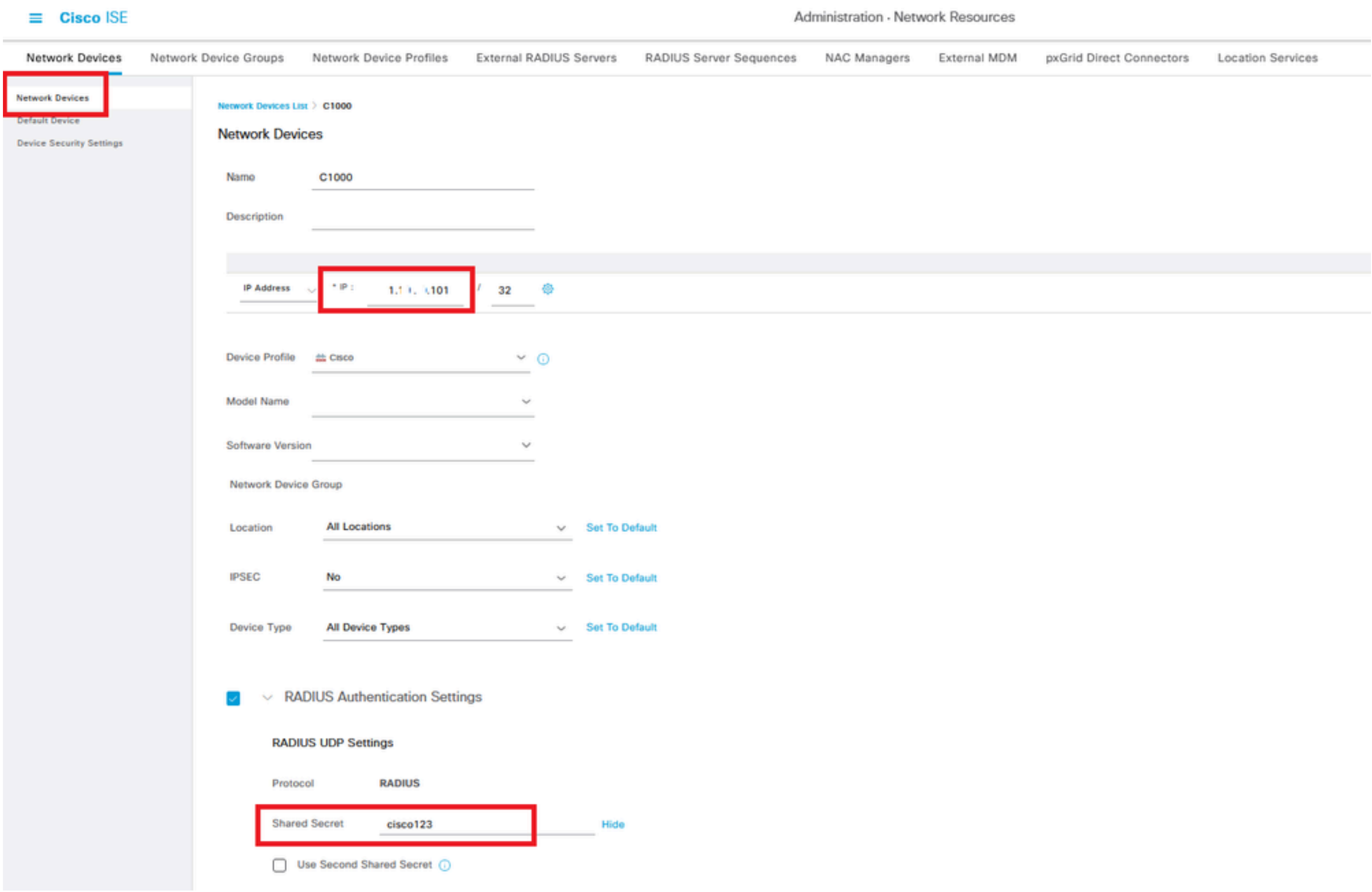
OCSP署名証明書のステータス

ISEでの設定

ステップ 1：デバイスの追加

Administration > Network Devicesの順に移動し、Addbuttonをクリックして C1000デバイスを追加

します。



Network Devices

Name C1000

Description

IP Address * IP : 1.[redacted].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

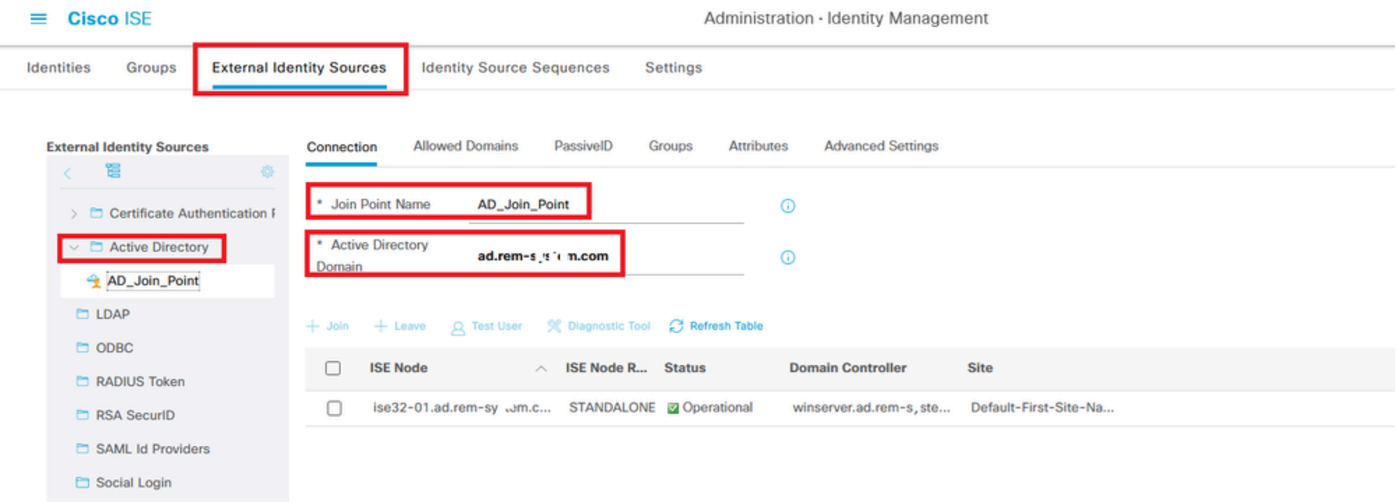
□ Use Second Shared Secret

デバイスの追加

ステップ２：Active Directoryの追加

Administration > External Identity Sources > Active Directoryの順に移動し、Connectiontabをクリックし、Active DirectoryをISEに追加します。

- [結合ポイント名]: AD_Join_Point
- Active Directoryドメイン：ad.rem-xxx.com



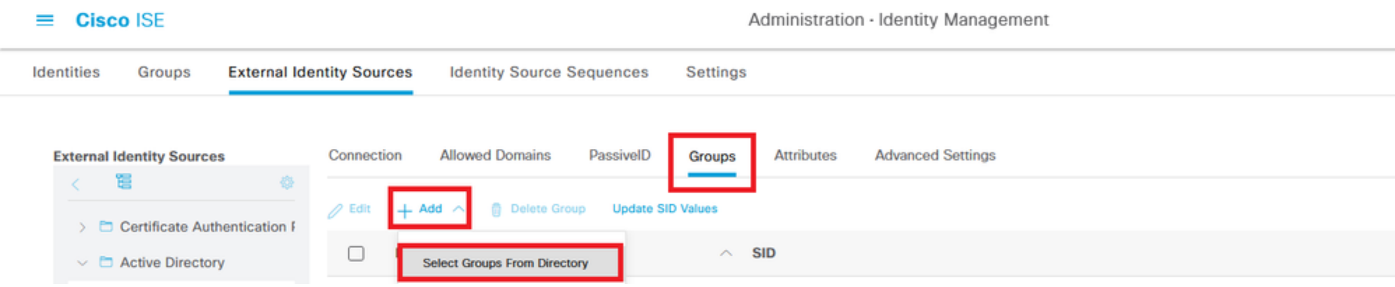
* Join Point Name AD_Join_Point

* Active Directory Domain ad.rem-s[redacted]n.com

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

Active Directoryの追加

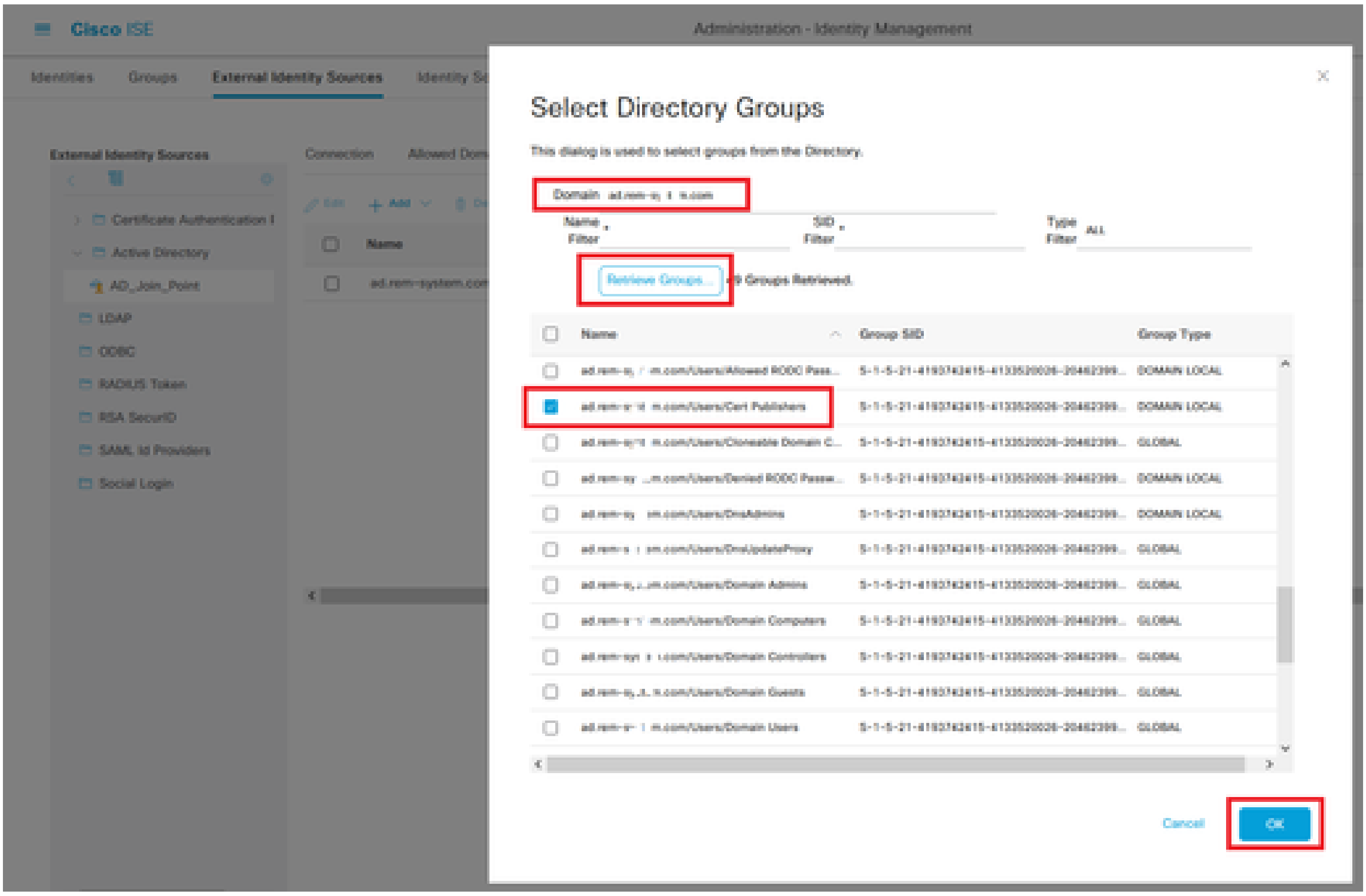
Groupsタブに移動し、select Groups From Directoryfromドロップダウンリストを選択します。



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

ディレクトリからグループを選択

[グループの取り出し]ドロップダウンリストをクリックします。Checkad.rem-xxx.com/Users/Cert Publishers と入力して、OKをクリックします。



Select Directory Groups

This dialog is used to select groups from the Directory.

Domain ad.rem-sy t m.com

Name Filter

SID Filter

Type Filter ALL

Retrieve Groups... 49 Groups Retrieved.

□	Name	Group SID	Group Type
□	ad.rem-sy / m.com/Users/Allowed RODC Pass...	S-1-5-21-4193742415-4133520026-20462399...	DOMAIN LOCAL
☑	ad.rem-s· d 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 em.com/Users/DnsAdmins	S-1-5-21-4193742415-4133520026-20462399...	DOMAIN LOCAL
□	ad.rem-s t em.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· t m.com/Users/Domain Computers	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
□	ad.rem-syt t i.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· t m.com/Users/Domain Users	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL

Cancel OK

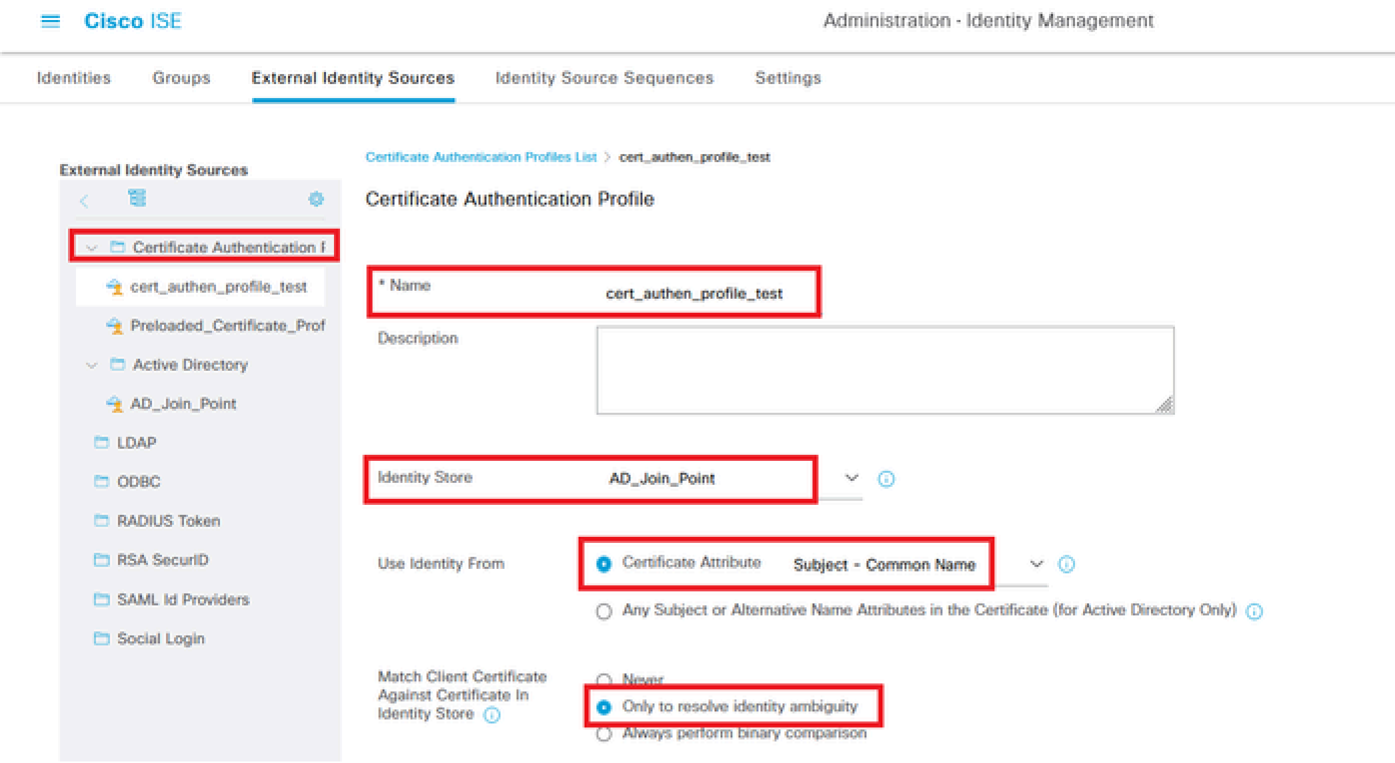
証明書の発行元の確認

ステップ 3：証明書認証プロファイルの追加

Administration > External Identity Sources > Certificate Authentication Profileの順に移動し、Addボタンをクリックして、新しい証明書認証プロファイルを追加します。

- 名前：cert_authen_profile_test
- IDストア： AD_Join_Point
- 証明書属性のIdを使用：件名 – 共通名。
- Match Client Certificate With Certificate In Identity Store:IDのあいまいさを解決するためだけ

に使用します。


Cisco ISE
Administration · Identity Management
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
External Identity Sources
Certificate Authentication I
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)

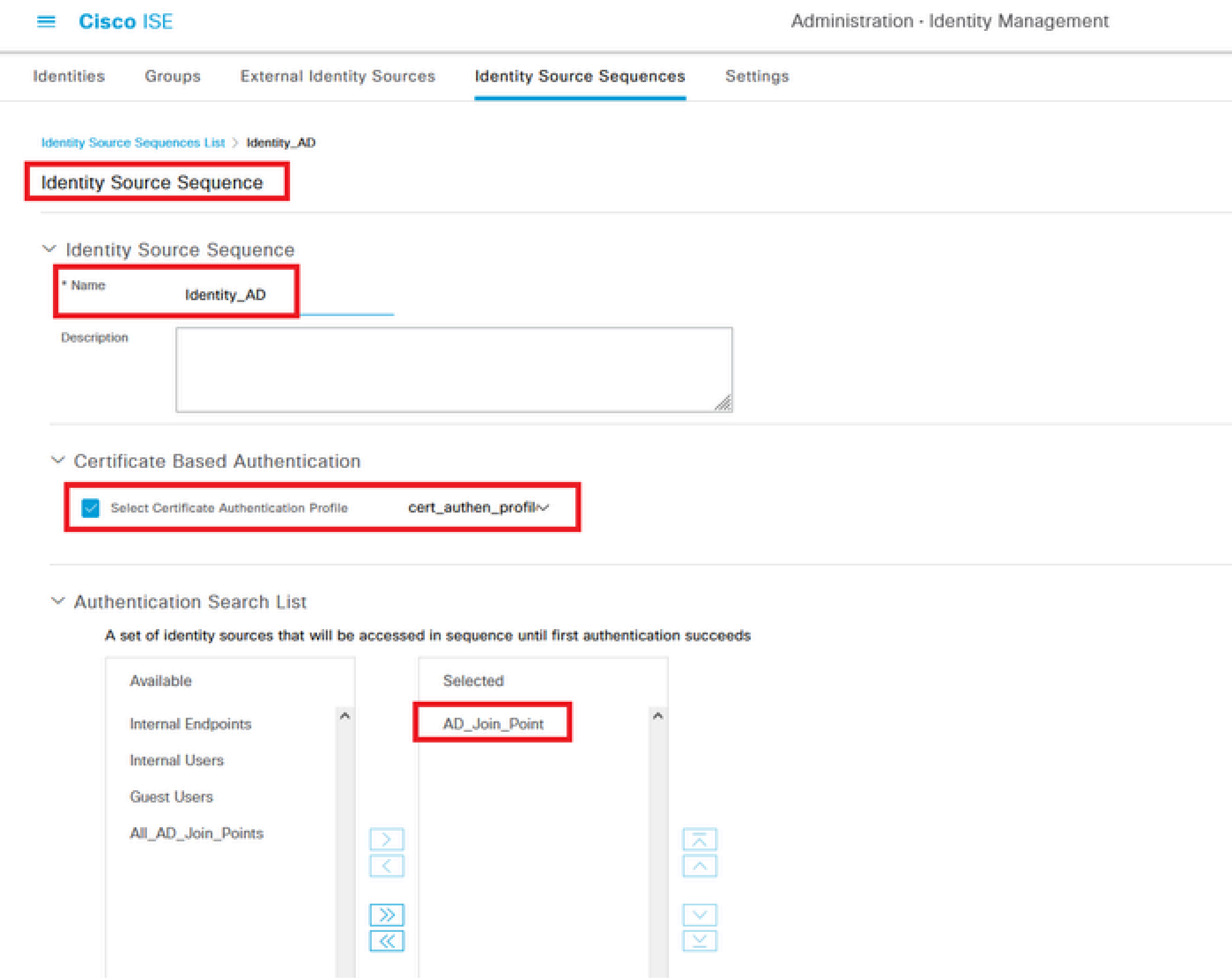
Match Client Certificate Against Certificate In Identity Store:
○ Never
● Only to resolve identity ambiguity
○ Always perform binary comparison

証明書認証プロファイルの追加

ステップ 4：アイデンティティソースシーケンスの追加

Administration > Identity Source Sequencesの順に移動し、Identity Source Sequenceを追加します。

- 名前：Identity_AD
- Certificate Authentication Proを選択します。file: cert_authen_profile_test
- 認証検索リスト：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

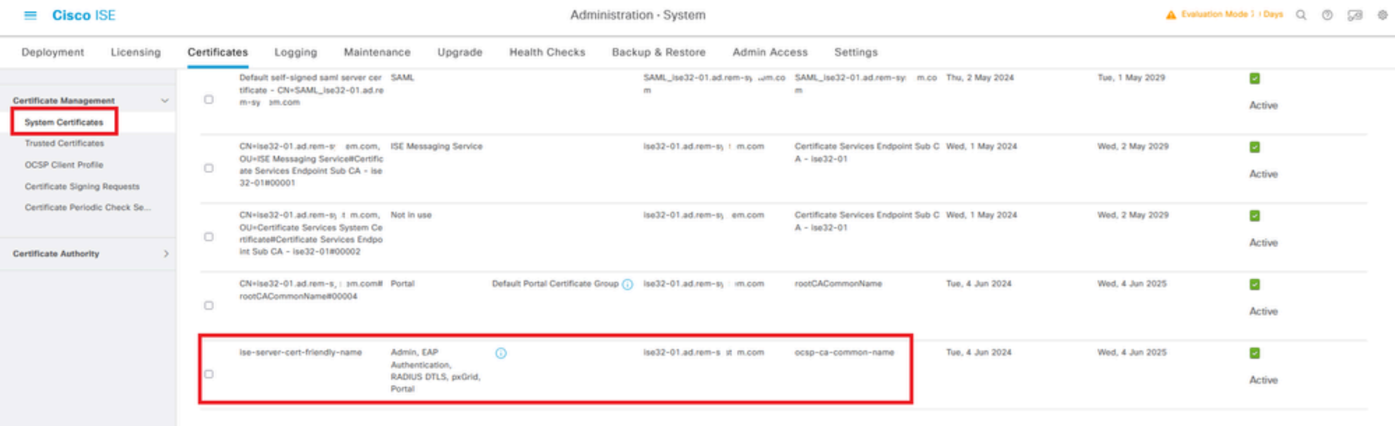
A set of identity sources that will be accessed in sequence until first authentication succeeds

Available	Selected
Internal Endpoints	AD_Join_Point
Internal Users	
Guest Users	
All_AD_Join_Points	

アイデンティティソースシーケンスの追加

ステップ 5：ISEでのconfrim証明書

Administration > Certificates > System Certificatesの順に移動し、サーバ証明書が信頼できるCAによって署名されていることを確認します。



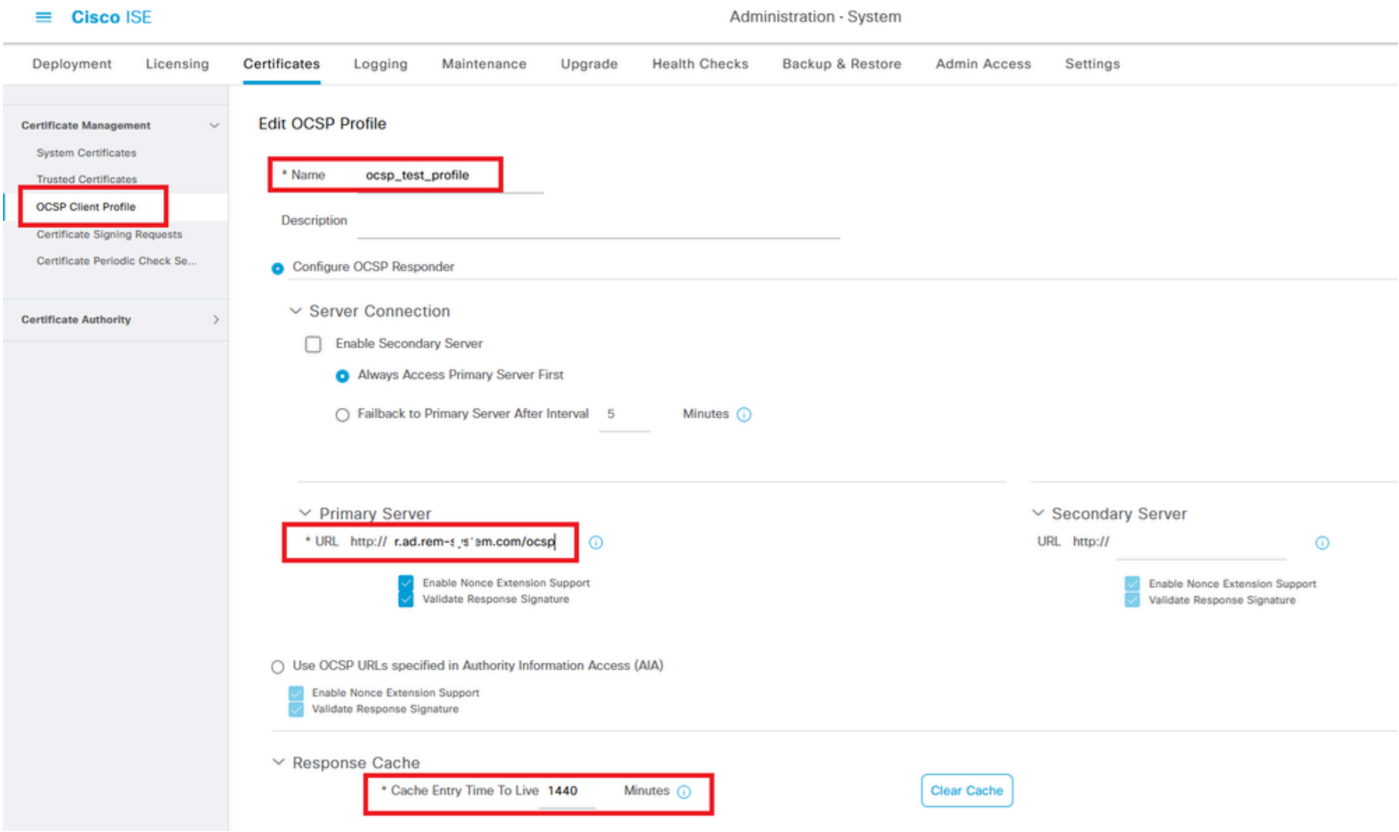
□	Default self-signed saml server certificate - CN=SAML_ise32-01.ad.rem-sy m.com	SAML		SAML_ise32-01.ad.rem-sy m.com	SAML_ise32-01.ad.rem-sy m.com	Thu, 2 May 2024	Tue, 1 May 2029	✓ Active
□	CN=ise32-01.ad.rem-s em.com, OU=ISE Messaging Service#Certificate Services Endpoint Sub CA - ise32-01#00001	ISE 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

サーバ証明書

Administration > Certificates > OCSP Client Profileの順に移動し、Addボタンをクリックして新し

いOCSPクライアントプロファイルを追加します。

- 名前： ocsp_test_profile
- OCSPレスポンダURLの設定：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_s 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)

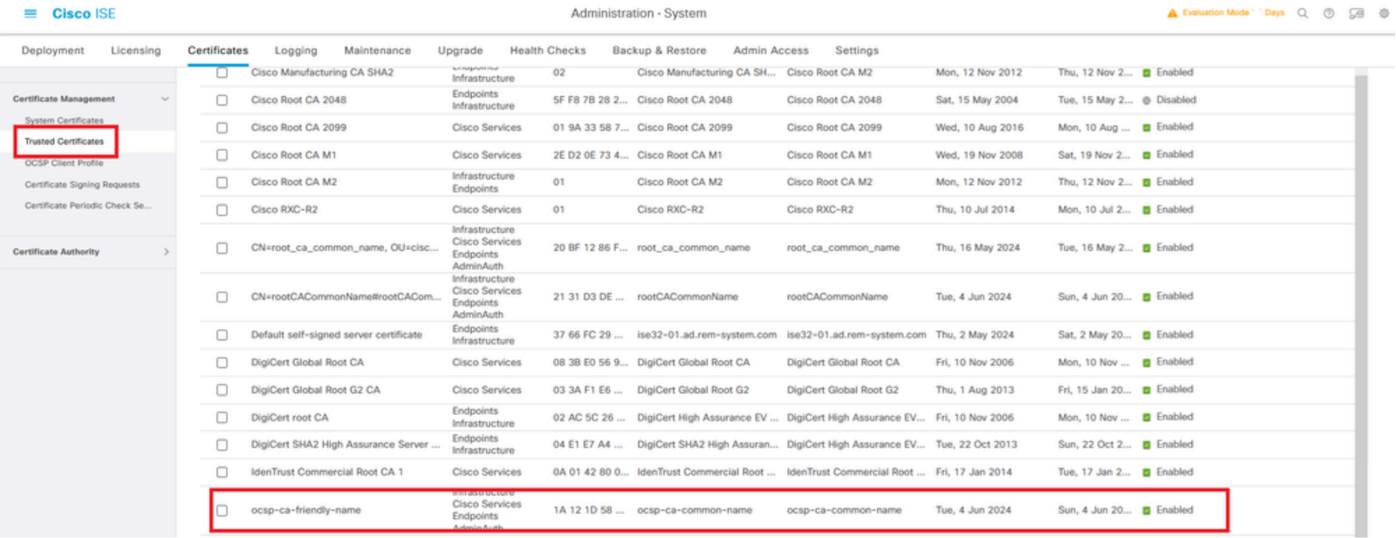
☑ Enable Nonce Extension Support
☑ Validate Response Signature

Response Cache

* Cache Entry Time To Live 1440 Minutes

OCSPクライアントプロファイル

Administration > Certificates > Trusted Certificatesの順に移動し、信頼できるCAがISEにインポートされていることを確認します。

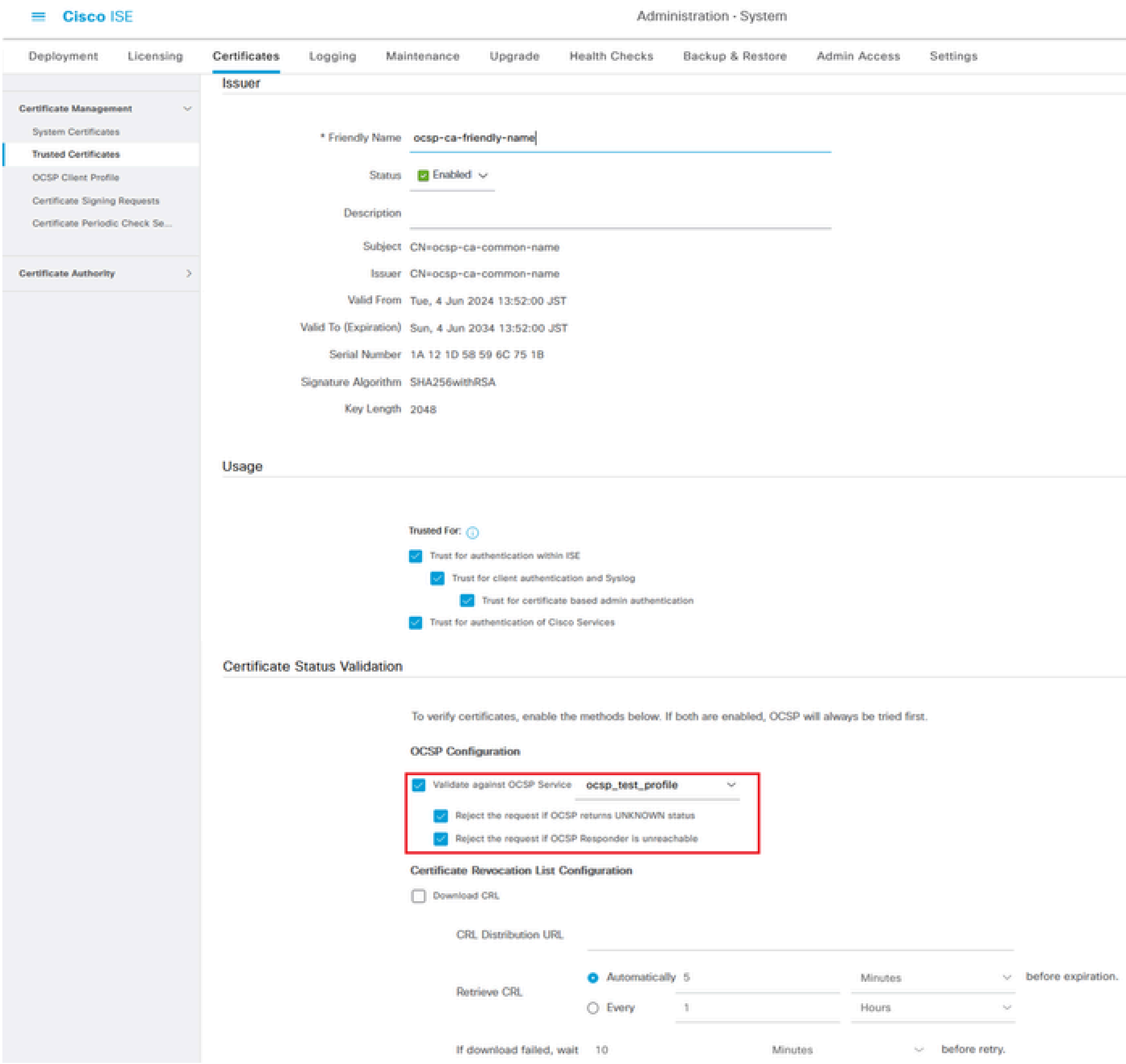


□	Cisco Manufacturing CA SHA2	Endpoints Infrastructure	02	Cisco Manufacturing CA SH...	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2...	Enabled
□	Cisco Root CA 2048	Endpoints Infrastructure	5F F8 7B 28 2...	Cisco Root CA 2048	Cisco Root CA 2048	Sat, 15 May 2004	Tue, 15 May 2...	Disabled
□	Cisco Root 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

信頼済みCA

CAをチェックしてEditボタンをクリックし、Certificate Status Validation用にOCSP設定の詳細を入力します。

- OCSPサービスに対する検証：ocsp_test_profile
- OCSPがUNKNOWNステータスを返す場合は、要求を拒否します。
- OCSPレスポンダが到達不能な場合は要求を拒否します。確認してください。



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

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

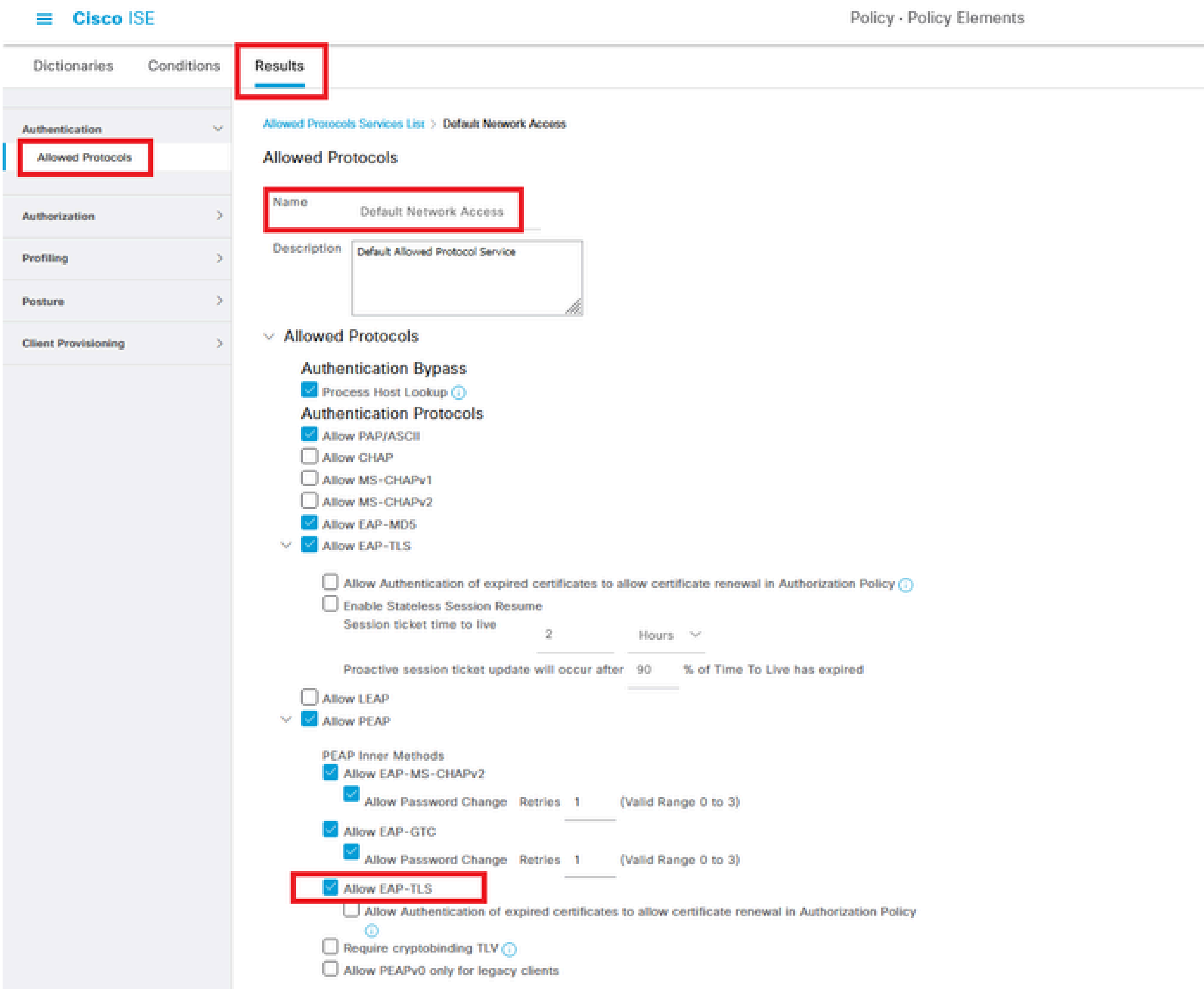
Retrieve CRL ● Automatically 5 Minutes before expiration.
○ Every 1 Hours

If download failed, wait 10 Minutes before retry.

証明書ステータスの検証

手順 6：許可されたプロトコルの追加

Policy > Results > Authentication > Allowed Protocolsの順に移動し、Default Network Accessサービスリストを編集して、Allow EAP-TLSにチェックマークを付けます。



Allowed Protocols

Name: Default Network Access

Description: Default Allowed Protocol Service

Allowed Protocols

Authentication Bypass

☑ Process Host Lookup

Authentication Protocols

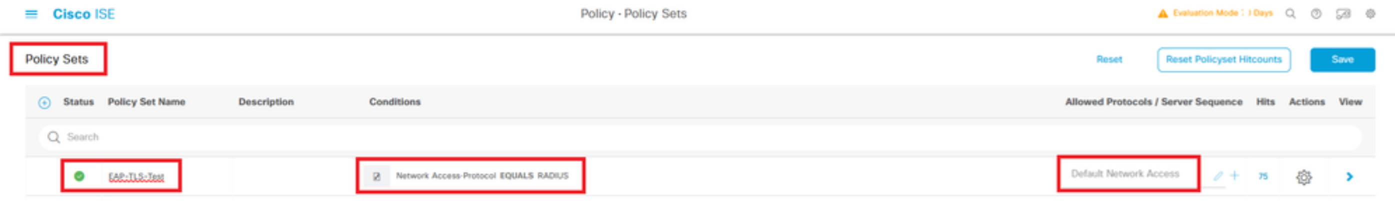
☑ Allow PAP/ASCII
□ Allow CHAP
□ Allow MS-CHAPv1
□ Allow MS-CHAPv2
☑ Allow EAP-MD5
☑ Allow EAP-TLS
  □ Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy
  □ Enable Stateless Session Resume
  Session ticket time to live: 2 Hours
  Proactive session ticket 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

EAP-TLSを許可する

手順 7：ポリシーセットの追加

Policy > Policy Setsの順に移動し、+ をクリックしてポリシーセットを追加します。

- ポリシーセット名：EAP-TLS-Test
- 条件：ネットワークアクセスプロトコルがRADIUSと等しい
- 許可されるプロトコル/サーバシーケンス：デフォルトのネットワークアクセス



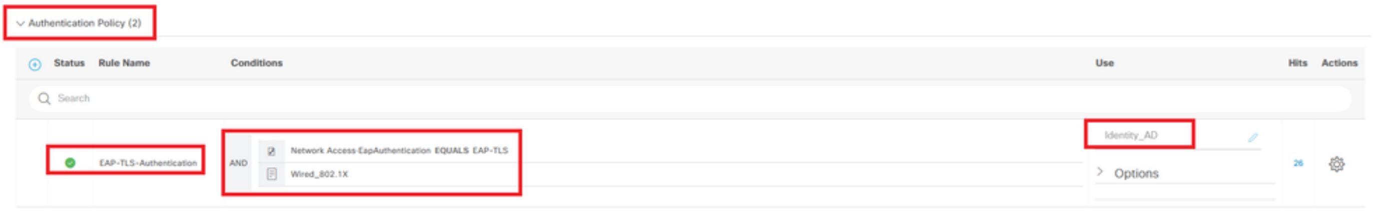
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	EAP-TLS-Test		Network Access·Protocol EQUALS RADIUS	Default Network Access	75	⚙	>

ポリシーセットの追加

ステップ 8：認証ポリシーの追加

Policy Setsに移動し、EAP-TLS-Testingをクリックして認証ポリシーを追加します。

- ルール名：EAP-TLS-Authentication
- 条件：ネットワークアクセスEapAuthentication がEAP-TLS およびWired_802.1 Xと等しい
- 使用：Identity_AD



Authentication Policy (2)

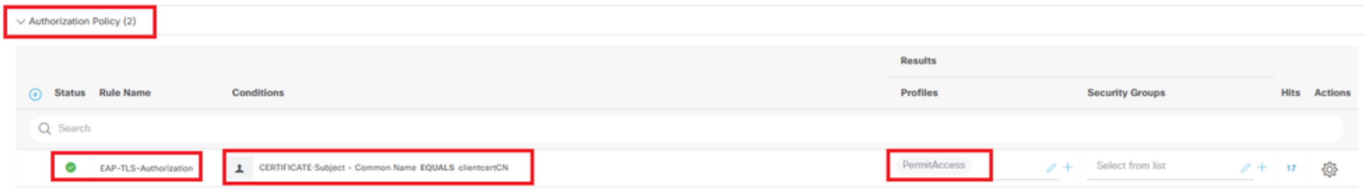
Status	Rule Name	Conditions	Use	Hits	Actions
●	EAP-TLS-Authentication	AND Network Access·EapAuthentication EQUALS EAP-TLS Wired_802.1X	Identity_AD Options	26	⚙

認証ポリシーの追加

ステップ 9：許可ポリシーの追加

Policy Setsに移動し、EAP-TLS-Testをクリックして認可ポリシーを追加します。

- ルール名：EAP-TLS-Authorization
- 条件：CERTIFICATE Subject - Common Name EQUALS clientcertCN
- 結果：PermitAccess



Authorization Policy (2)

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

許可ポリシーの追加

確認

ステップ 1：認証セッションの確認

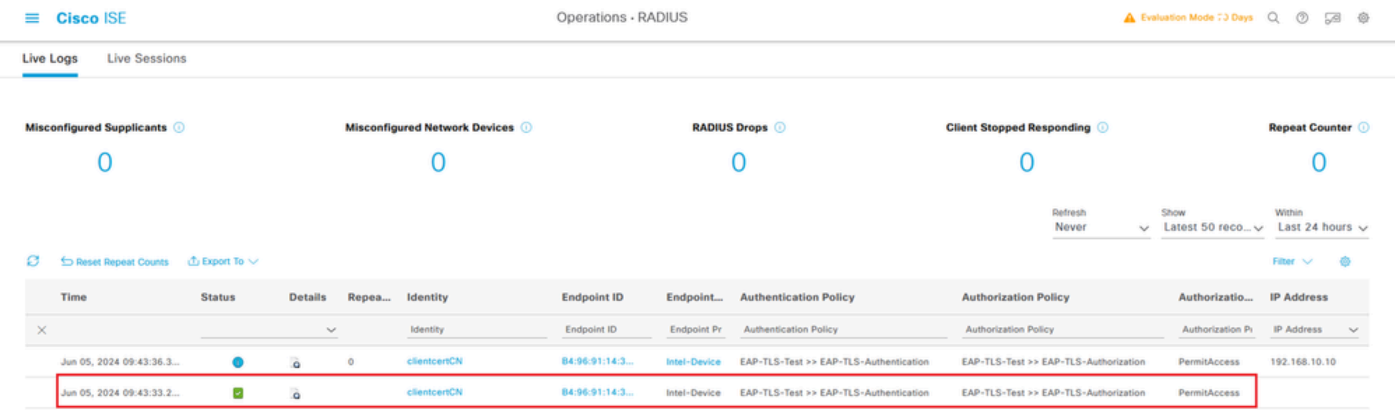
C1000で認証セッションを確認するには、show authentication sessions interface GigabitEthernet1/0/3 detailsコマンドを実行します。

```
<#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
```

ステップ２：Radiusライブログの確認

ISE GUIで**Operations** > **RADIUS** > **Live**の順に移動し、認証のライブログを確認します。



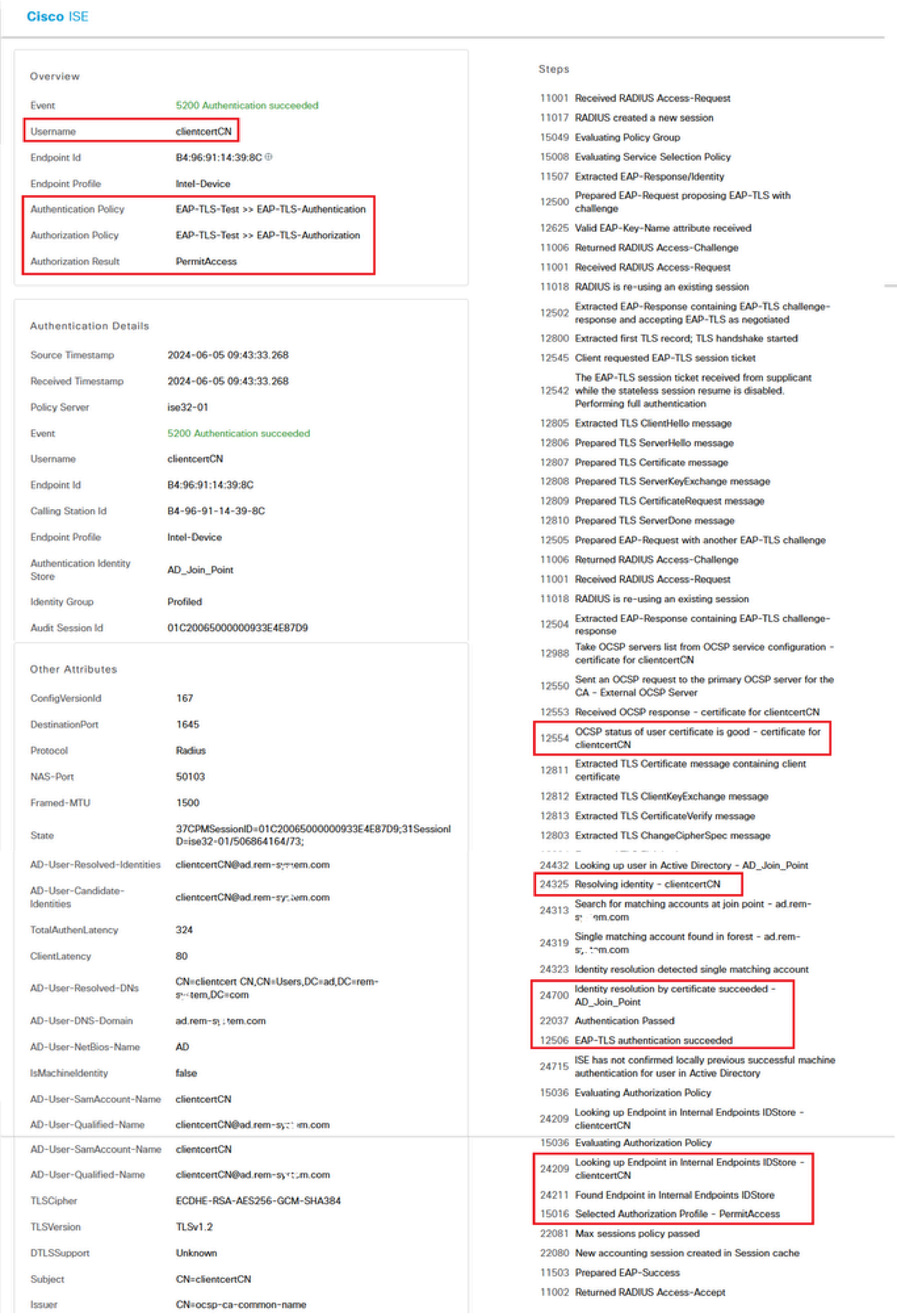
Misconfigured Supplicants 0 | Misconfigured Network Devices 0 | RADIUS Drops 0 | Client Stopped Responding 0 | Repeat Counter 0

Refresh: Never | Show: Latest 50 reco... | Within: Last 24 hours

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	

*Radius*ライブログ

認証の詳細なライブログを確認します。



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]m.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
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

認証の詳細

```
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
```

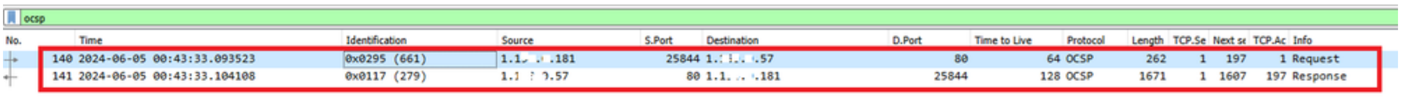
`Code=5(AccountingResponse)`

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

2. TCPダンプ

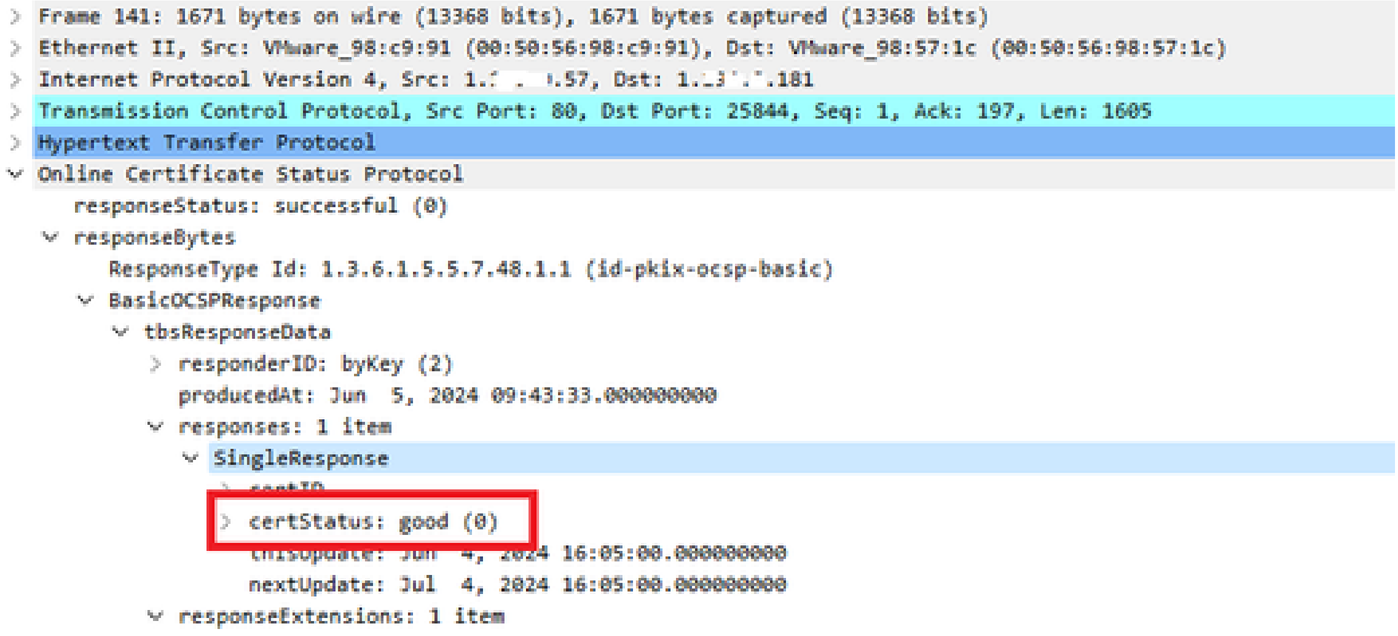
ISEのTCPダンプには、OCSP応答とRadiusセッションに関する情報が含まれています。

OCSP要求および応答：



```
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
```

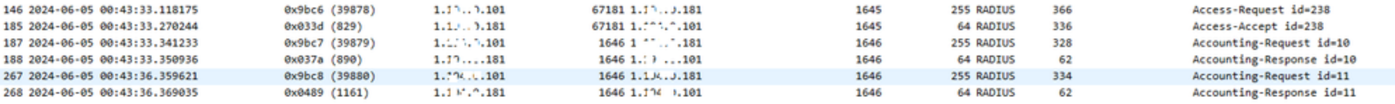
OCSP要求および応答のパケットキャプチャ



```
> 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
```

OCSP応答の詳細の取得

RADIUSセッション：



```
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 1.1[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
```

RADIUSセッションのパケットキャプチャ

関連情報

ISEでのEAP-TLS認証の設定

ISEでのTLS/SSL証明書の設定

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。