

Konfigurieren der EAP-TLS-Authentifizierung mit OCSP in der ISE

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Netzwerkdiagramm](#)

[Hintergrundinformationen](#)

[Konfigurationen](#)

[Konfiguration in C1000](#)

[Konfiguration auf Windows-PCs](#)

[Schritt 1: Benutzerauthentifizierung konfigurieren](#)

[Schritt 2: Clientzertifikat bestätigen](#)

[Konfiguration in Windows Server](#)

[Schritt 1: Benutzer hinzufügen](#)

[Schritt 2: OCSP-Dienst bestätigen](#)

[Konfiguration in der ISE](#)

[Schritt 1: Gerät hinzufügen](#)

[Schritt 2: Active Directory hinzufügen](#)

[Schritt 3: Zertifikatauthentifizierungsprofil hinzufügen](#)

[Schritt 4: Identitätsquelltext hinzufügen](#)

[Schritt 5: Zertifikat in ISE bestätigen](#)

[Schritt 6: Zulässige Protokolle hinzufügen](#)

[Schritt 7: Policy Set hinzufügen](#)

[Schritt 8: Authentifizierungsrichtlinie hinzufügen](#)

[Schritt 9: Autorisierungsrichtlinie hinzufügen](#)

[Überprüfung](#)

[Schritt 1: Authentifizierungssitzung bestätigen](#)

[Schritt 2: RADIUS-Live-Protokoll bestätigen](#)

[Fehlerbehebung](#)

[1. Debug-Protokoll](#)

[2. TCP-Dump](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument werden die erforderlichen Schritte zum Einrichten der EAP-TLS-Authentifizierung mit OCSP für Echtzeit-Clientzertifikatwiderrufsprüfungen beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Konfiguration der Cisco Identity Services Engine
- Konfiguration des Cisco Catalyst
- Online-Zertifikatstatusprotokoll

Verwendete Komponenten

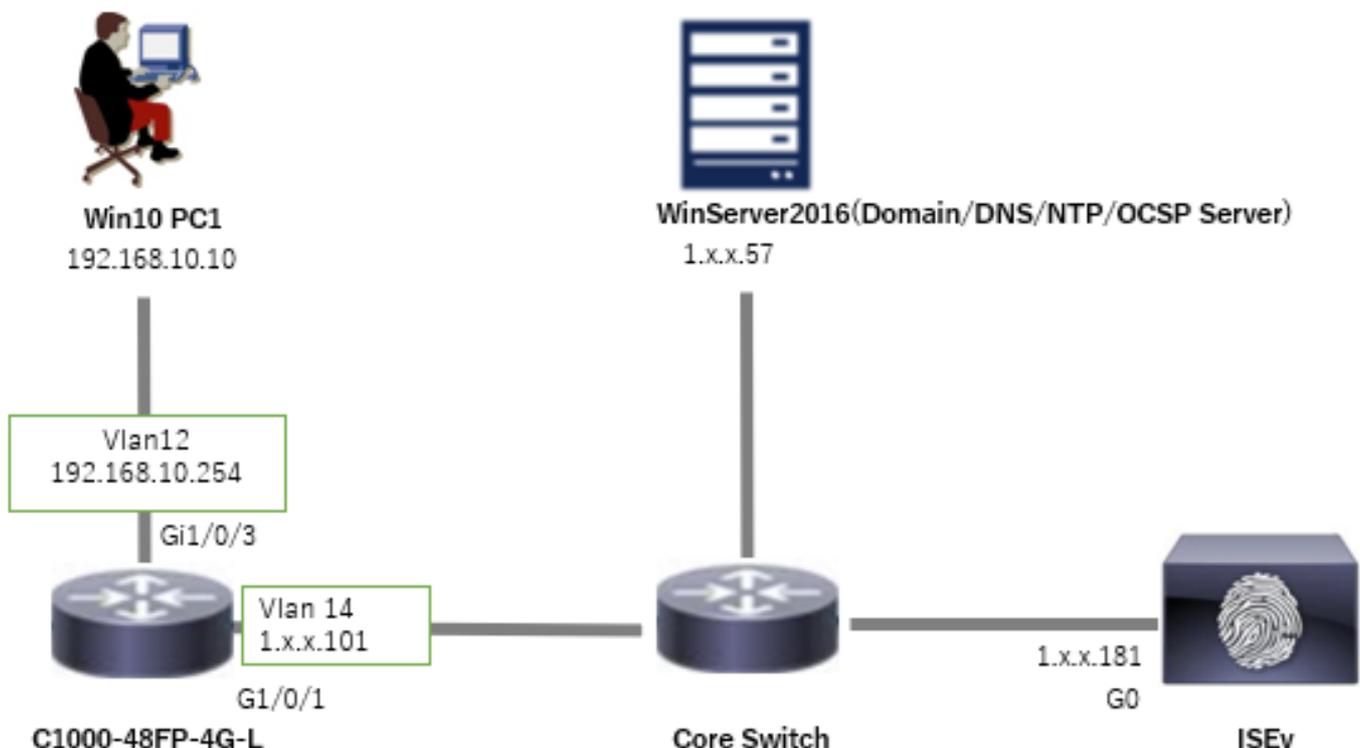
Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Identity Services Engine Virtual 3.2 Patch 6
- C1000-48FP-4G-L 15,2(7)E9
- Windows Server 2016
- Windows 10

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Netzwerkdiagramm

Dieses Bild zeigt die Topologie, die für das Beispiel dieses Dokuments verwendet wird.



Hintergrundinformationen

In EAP-TLS stellt ein Client dem Server sein digitales Zertifikat als Teil des Authentifizierungsprozesses dar. In diesem Dokument wird beschrieben, wie die ISE das Client-Zertifikat validiert, indem der Common Name (CN) des Zertifikats mit dem AD-Server abgeglichen wird und bestätigt wird, ob das Zertifikat mithilfe des OCSP (Online Certificate Status Protocol) widerrufen wurde, das den Echtzeit-Protokollstatus bereitstellt.

Der unter Windows Server 2016 konfigurierte Domänenname ist ad.rem-xxx.com. Dies wird in diesem Dokument als Beispiel verwendet.

Die in diesem Dokument erwähnten OCSP- (Online Certificate Status Protocol) und AD-Server (Active Directory) werden für die Zertifikatsvalidierung verwendet.

- Active Directory-FQDN: winserver.ad.rem-xxx.com
- URL der Zertifikatsperrlisten-Verteilung: <http://winserver.ad.rem-xxx.com/ocsp-ca.crl>
- URL der Behörde: <http://winserver.ad.rem-xxx.com/ocsp>

Dies ist die Zertifikatskette mit dem allgemeinen Namen jedes im Dokument verwendeten Zertifikats.

- CA: ocspp-ca-common-name
- Client-Zertifikat: clientcertCN
- Serverzertifikat: ise32-01.ad.rem-xxx.com
- OCSP-Signaturzertifikat: ocsppSignCommonName

Konfigurationen

Konfiguration in C1000

Dies ist die minimale Konfiguration in C1000 CLI.

```
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
```

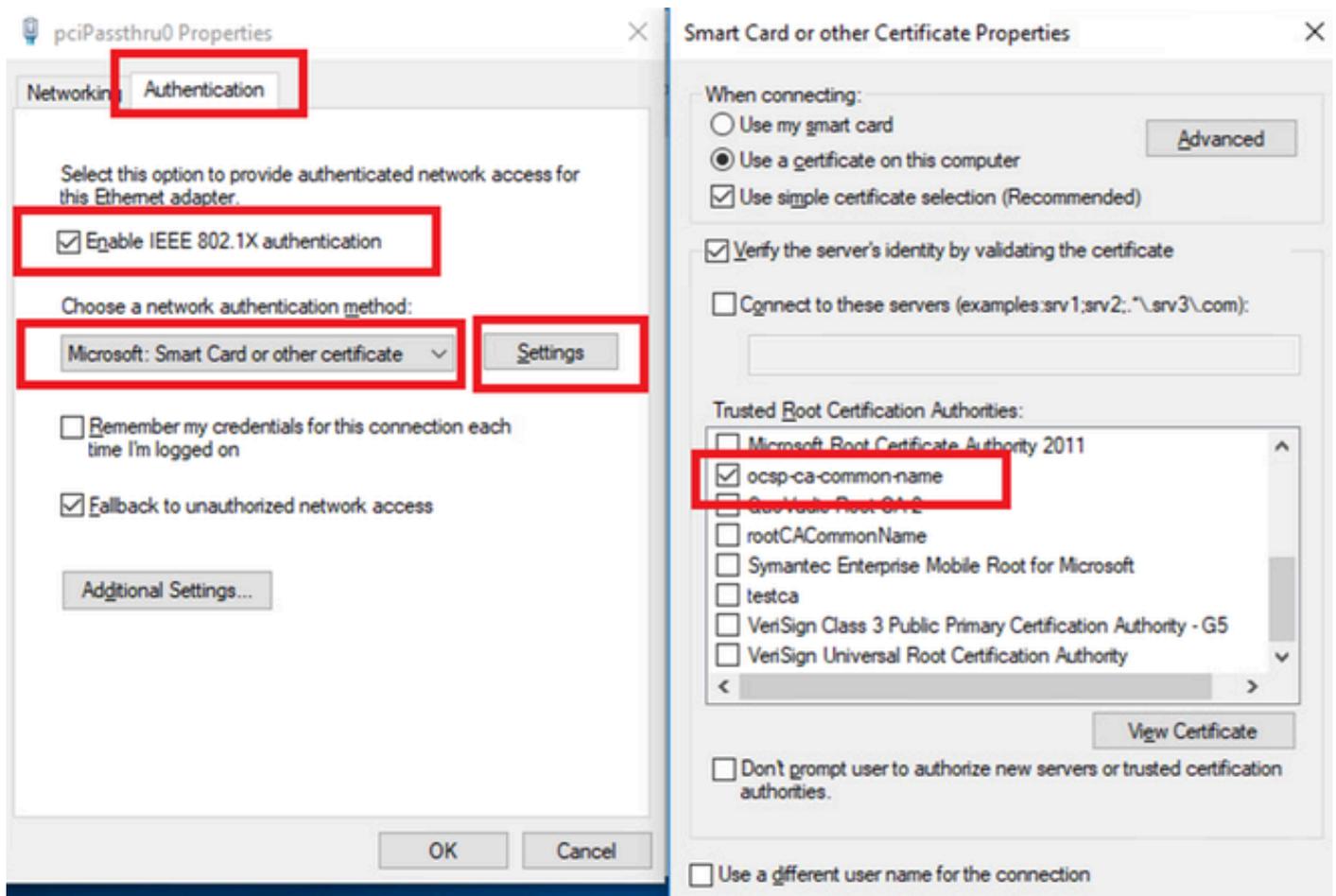
```
interface GigabitEthernet1/0/3
switchport access vlan 12
switchport mode access
authentication host-mode multi-auth
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge
```

Konfiguration auf Windows-PCs

Schritt 1: Benutzerauthentifizierung konfigurieren

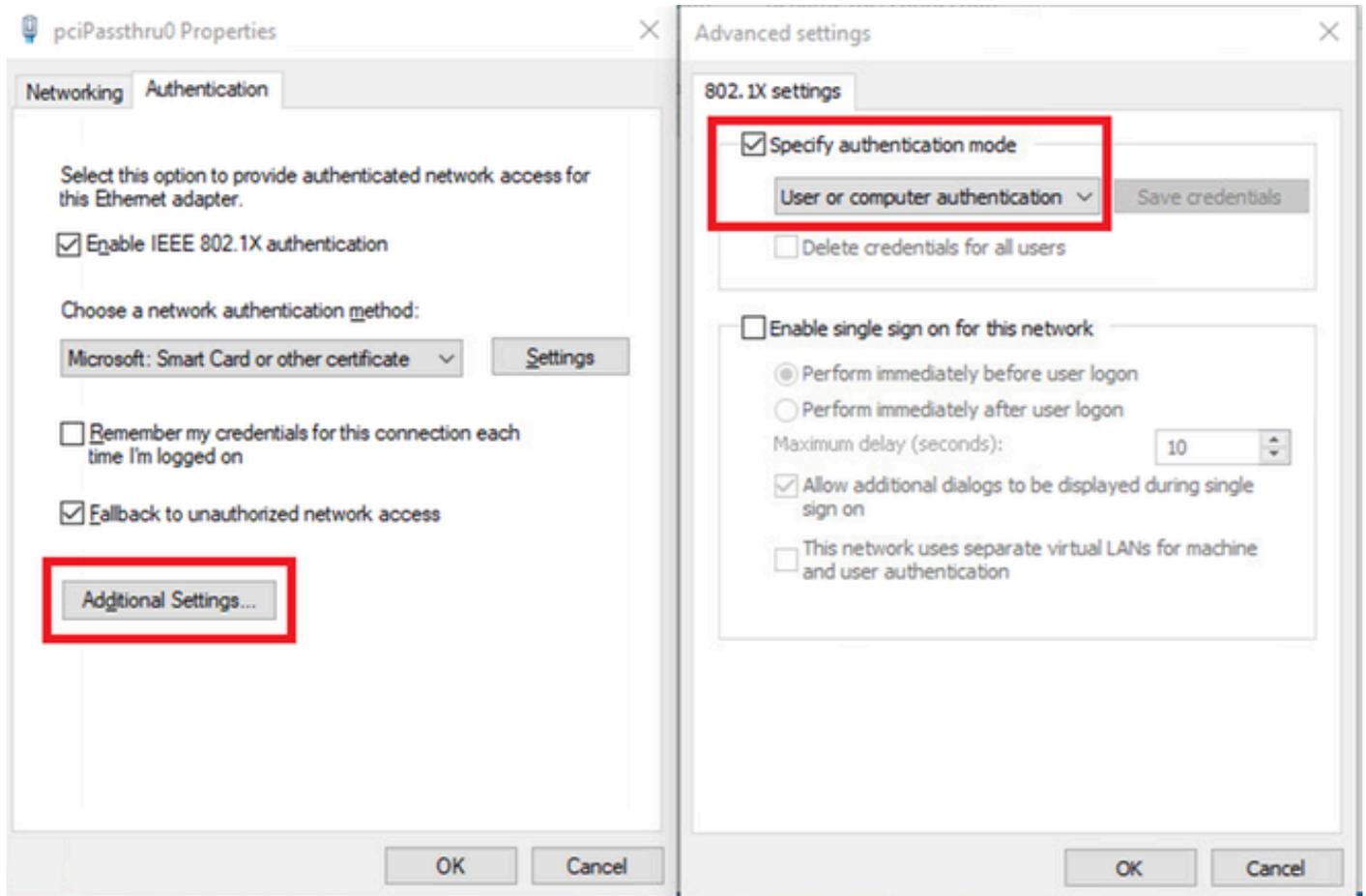
Navigieren Sie zu Authentication, aktivieren Sie Enable IEEE 802.1X authentication, und wählen Sie Microsoft: Smart Card oder sonstiges Zertifikat aus.

Klicken Sie auf die Schaltfläche Einstellungen, aktivieren Sie Zertifikat auf diesem Computer verwenden, und wählen Sie die vertrauenswürdige Zertifizierungsstelle von Windows PC aus.



Zertifikatsauthentifizierung aktivieren

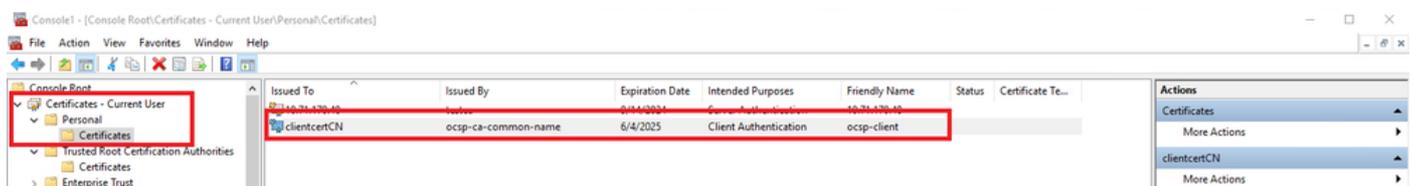
Navigieren Sie zu Authentifizierung, und aktivieren Sie Zusätzliche Einstellungen. Wählen Sie Benutzer- oder Computerauthentifizierung aus der Dropdown-Liste aus.



Authentifizierungsmodus angeben

Schritt 2: Clientzertifikat bestätigen

Navigieren Sie zu Certificates - Current User > Personal > Certificates, und überprüfen Sie das Client-Zertifikat, das für die Authentifizierung verwendet wird.

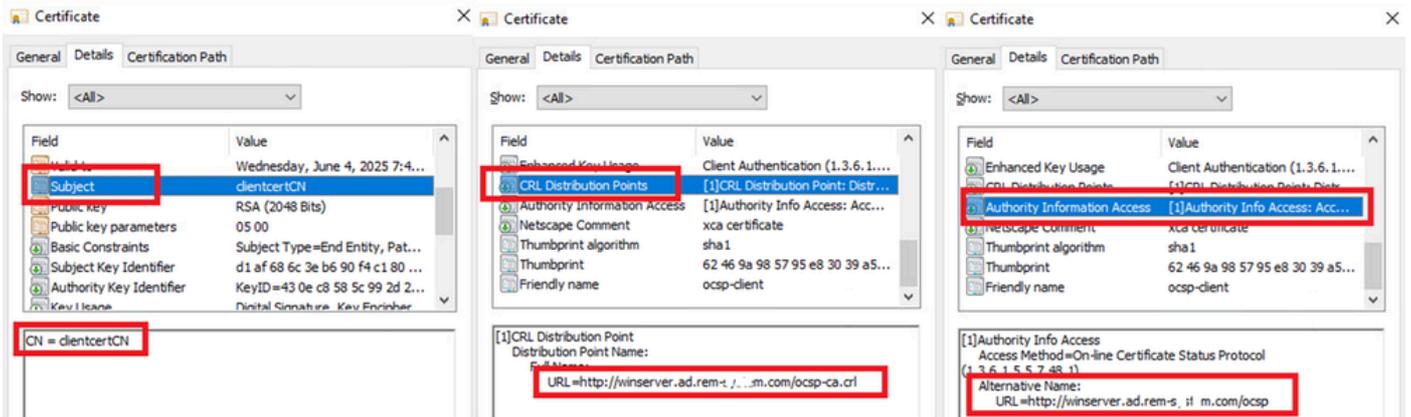


Clientzertifikat bestätigen

Doppelklicken Sie auf das Clientzertifikat, navigieren Sie zu Details, überprüfen Sie die Details zu Subject (Betreff), CRL Distribution Points (Zertifikatsperrlisten) und Authority Information Access (Zugriff auf Autoritätsinformationen).

- Betrifft: CN = clientcertCN
- CRL Distribution Points: <http://winserver.ad.rem-xxx.com/ocsp-ca.crl>

- Zugriff auf Behördeninformationen: <http://winserver.ad.rem-xxx.com/ocsp>

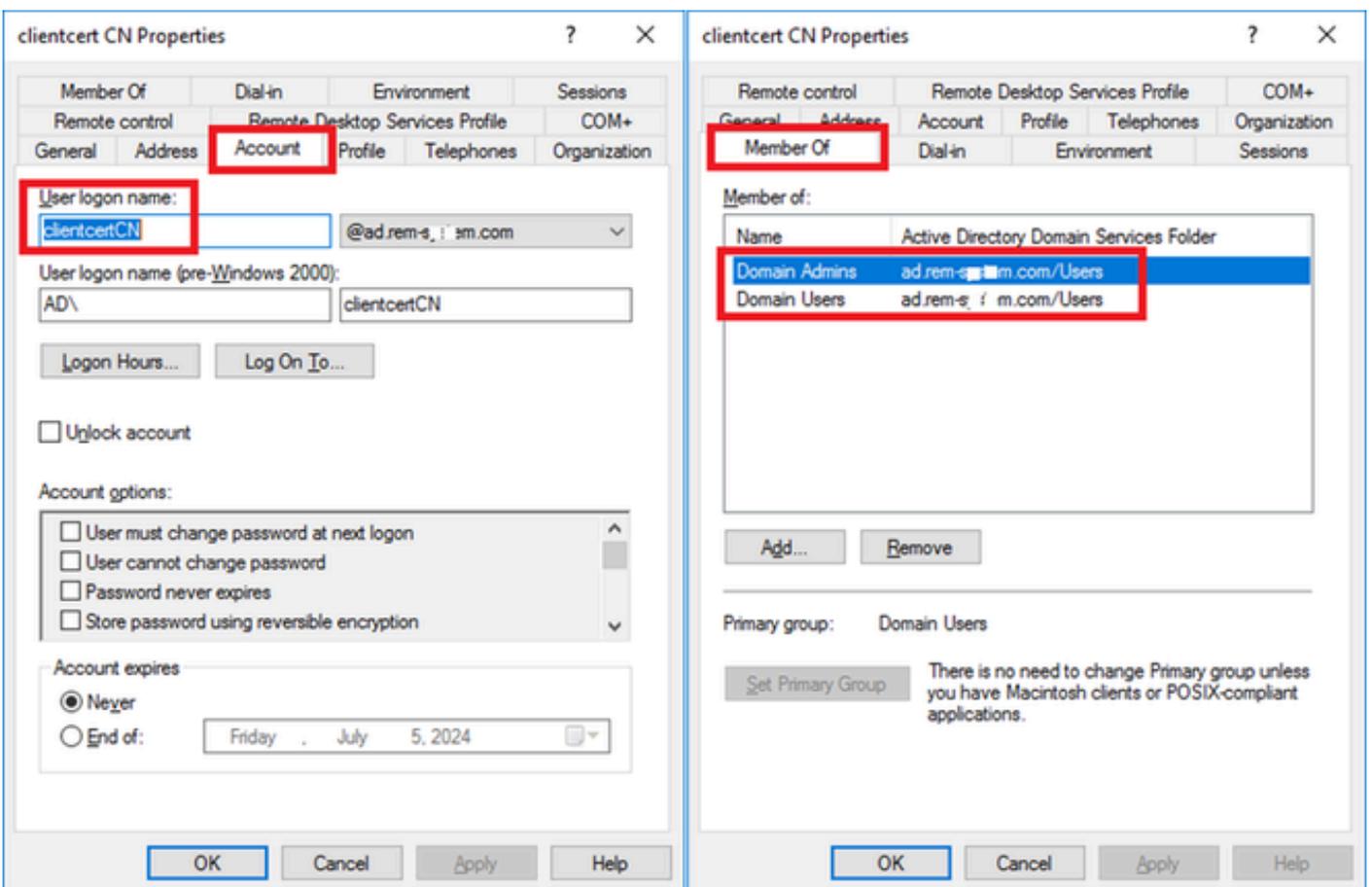


Details zum Client-Zertifikat

Konfiguration in Windows Server

Schritt 1: Benutzer hinzufügen

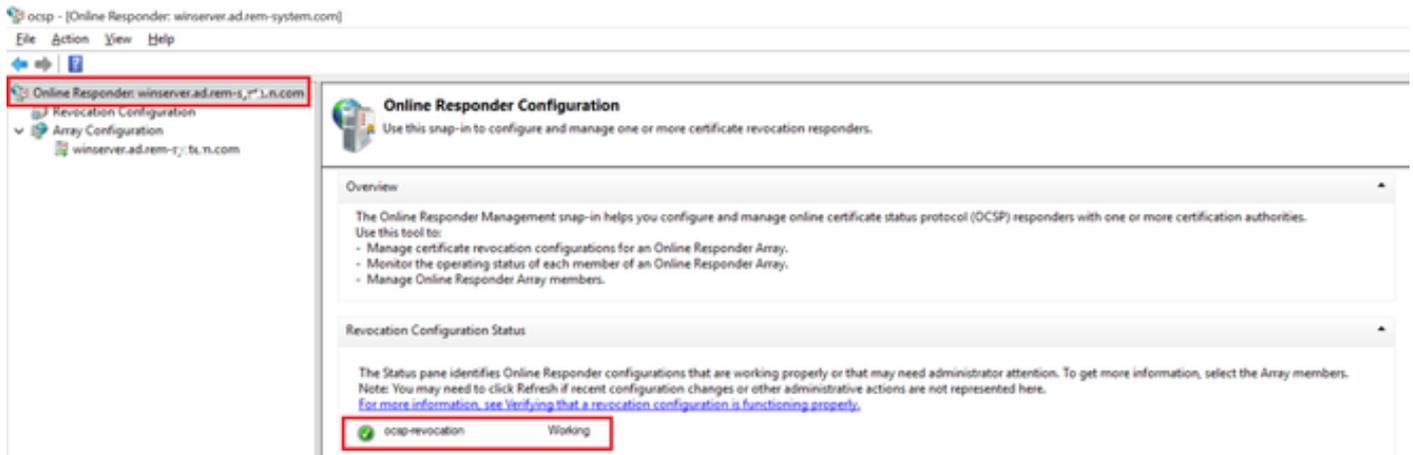
Navigieren Sie zu Active Directory-Benutzer und -Computer, und klicken Sie auf Benutzer. Fügen Sie clientcertCN als Benutzernamen hinzu.



Benutzername für Anmeldung

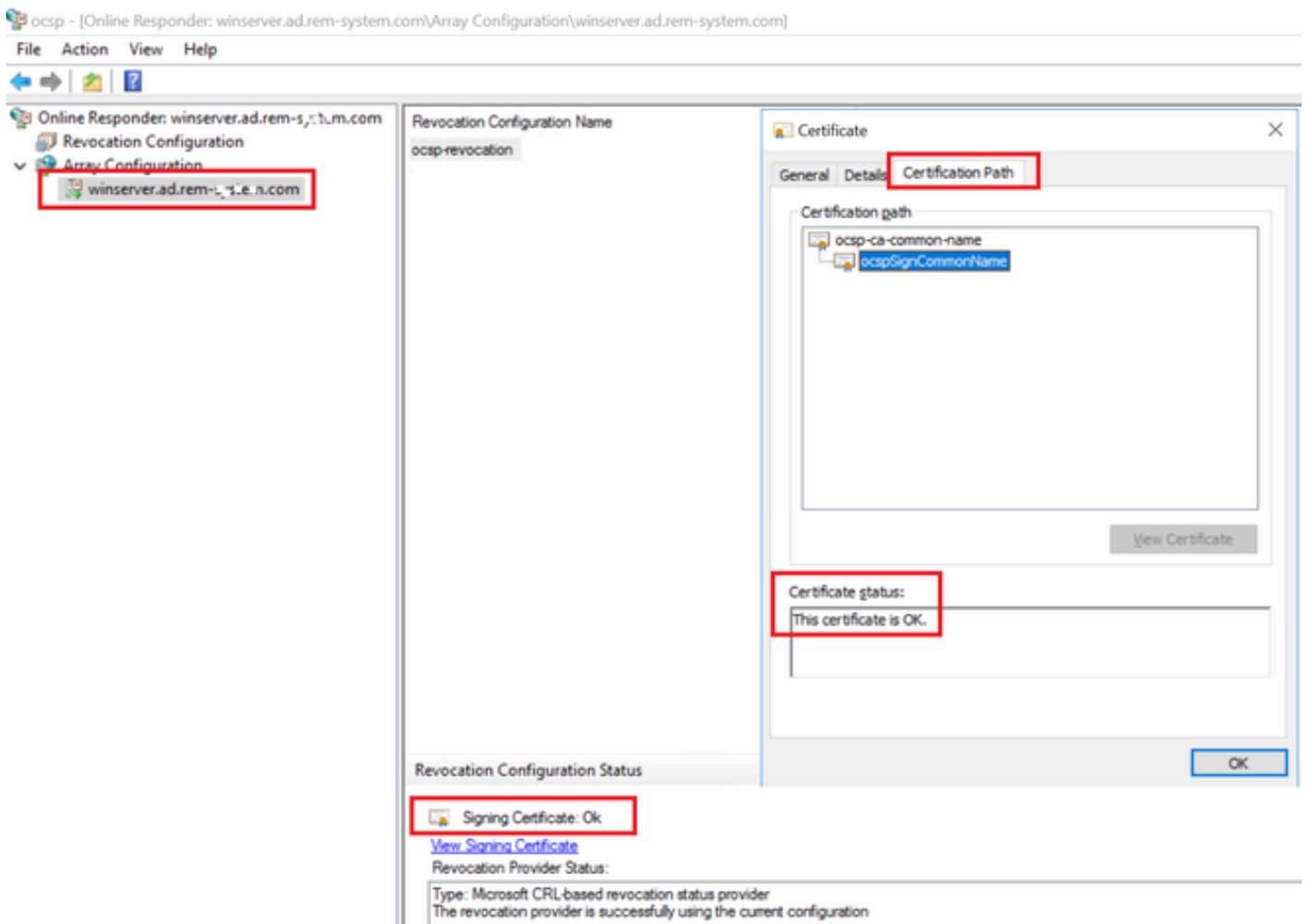
Schritt 2: OCSP-Dienst bestätigen

Navigieren Sie zu Windows, und klicken Sie auf Online-Responder-Verwaltung. Bestätigen Sie den Status des OCSP-Servers.



Status des OCSP-Servers

Klicken Sie auf winserver.ad.rem-xxx.com, und überprüfen Sie den Status des OCSP-Signaturzertifikats.



Status des OCSP-Signaturzertifikats

Konfiguration in der ISE

Schritt 1: Gerät hinzufügen

Navigieren Sie zu Administration > Network Devices, und klicken Sie auf Add (Hinzufügen), um ein C1000-Gerät hinzuzufügen.

The screenshot shows the Cisco ISE Administration console for configuring a C1000 network device. The interface includes a navigation menu on the left with 'Network Devices' highlighted. The main content area shows the configuration form for a device named 'C1000'. The IP address is set to 1.1.1.101/32. The device profile is set to 'Cisco'. The RADIUS Authentication Settings are expanded, showing the Shared Secret set to 'cisco123'. The 'Use Second Shared Secret' checkbox is unchecked.

Network Devices List > C1000

Network Devices

Name C1000

Description

IP Address * IP: 1.1.1.101 / 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

Gerät hinzufügen

Schritt 2: Active Directory hinzufügen

Navigieren Sie zu Administration > External Identity Sources > Active Directory, klicken Sie auf Registerkarte Connection, und fügen Sie Active Directory zur ISE hinzu.

- Verknüpfungspunkt-Name: AD_Join_Point
- Active Directory-Domäne: ad.rem-xxx.com

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

The screenshot shows the 'External Identity Sources' configuration page. The left sidebar lists various authentication methods, with 'Active Directory' selected. The main area shows the configuration for the 'AD_Join_Point' source. The 'Join Point Name' is set to 'AD_Join_Point' and the 'Active Directory Domain' is set to 'ad.rem-s...m.com'. Below the configuration, there is a table of ISE nodes and their status.

ISE Node	ISE Node R...	Status	Domain Controller	Site
<input type="checkbox"/>	ise32-01.ad.rem-sy...m.c...	STANDALONE	<input checked="" type="checkbox"/> Operational	winsrvr.ad.rem-s, ste... Default-First-Site-Na...

Active Directory hinzufügen

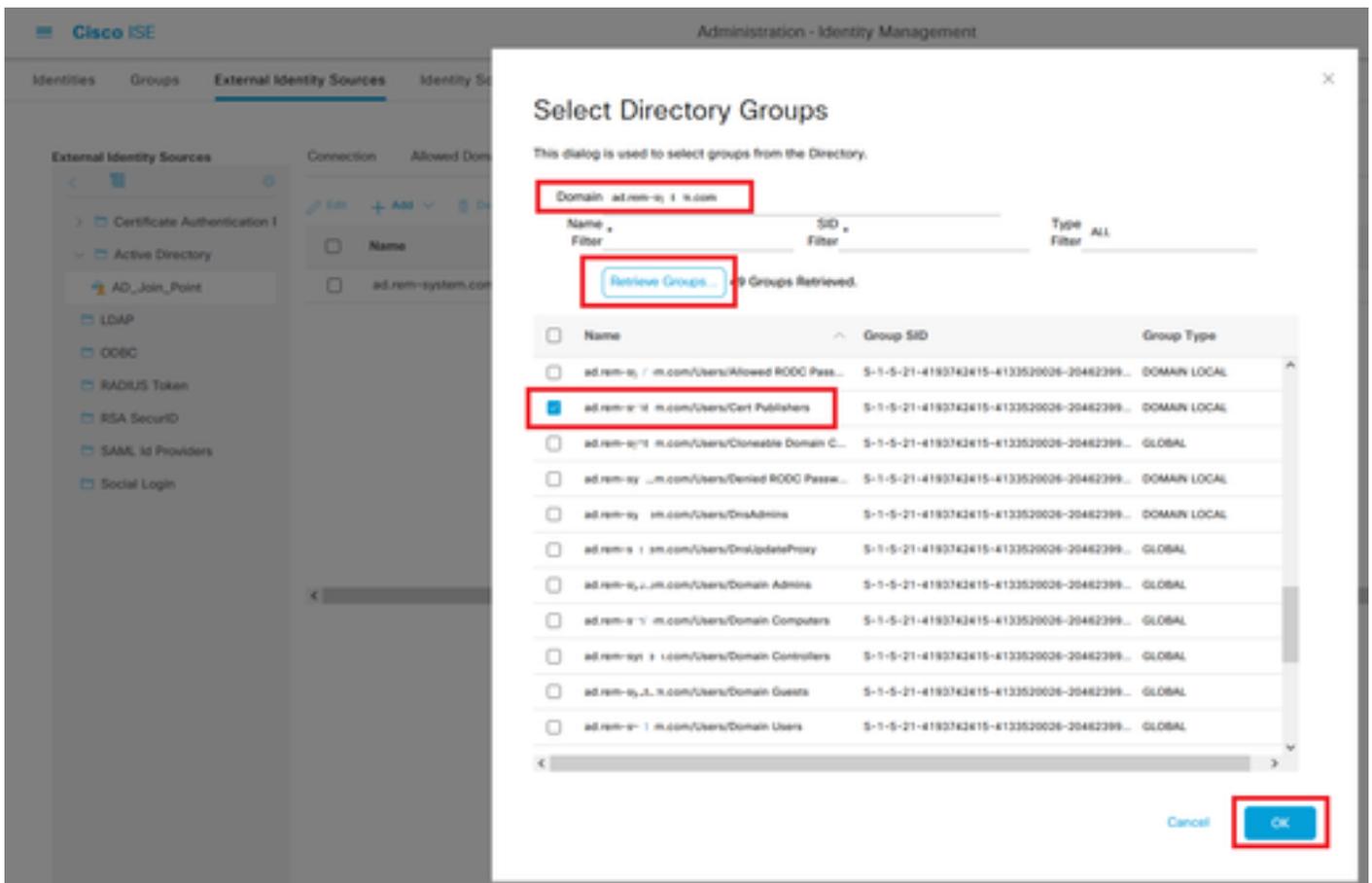
Navigieren Sie zur Registerkarte Gruppen, und wählen Sie in der Dropdown-Liste Gruppen aus Verzeichnis auswählen aus.

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

The screenshot shows the 'Groups' tab for the 'AD_Join_Point' external identity source. The 'Add' button is highlighted, and the 'Select Groups From Directory' dropdown menu is open, showing a list of groups from the directory.

Gruppen aus Verzeichnis auswählen

Klicken Sie auf Gruppen aus der Dropdown-Liste abrufen. Checkad.rem-xxx.com/Users/Cert Publisher und klicken Sie auf OK.



Zertifikatverleger überprüfen

Schritt 3: Zertifikatauthentifizierungsprofil hinzufügen

Navigieren Sie zu Administration > External Identity Sources > Certificate Authentication Profile, und klicken Sie auf die Schaltfläche Add, um ein neues Zertifikatauthentifizierungsprofil hinzuzufügen.

- Name: cert_authen_profile_test
- Identitätsspeicher: AD_Join_Point
- Identität aus Zertifikatattribut verwenden: Betreff - Allgemeiner Name.
- Zuordnen des Clientzertifikats zum Zertifikat im Identitätsspeicher: Nur zur Behebung von Identitätsmehrdeutigkeiten.

External Identity Sources

Certificate Authentication Profiles List > cert_authen_profile_test

Certificate Authentication Profile

* Name

Description

Identity Store

Use Identity From Certificate Attribute

Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only)

Match Client Certificate Against Certificate In Identity Store Only to resolve identity ambiguity

Never

Always perform binary comparison

Zertifikatauthentifizierungsprofil hinzufügen

Schritt 4: Identitätsquelltext hinzufügen

Navigieren Sie zu Administration > Identity Source Sequences, und fügen Sie eine Identity Source Sequence hinzu.

- Name: Identity_AD
- Wählen Sie Certificate Authentication Profile: cert_authen_profile_test
- Authentifizierungs-Suchliste: 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

Identitätsquellensequenzen hinzufügen

Schritt 5: Zertifikat in ISE bestätigen

Navigieren Sie zu Administration > Certificates > System Certificates, und bestätigen Sie, dass das Serverzertifikat von der vertrauenswürdigen Zertifizierungsstelle signiert wurde.

Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings
		<ul style="list-style-type: none"> <input type="checkbox"/> Default self-signed saml server cer... <input type="checkbox"/> CN=ise32-01.ad.rem-sj... em.com, ISE Messaging Service <input type="checkbox"/> CN=ise32-01.ad.rem-sj... em.com, Not in use <input type="checkbox"/> CN=ise32-01.ad.rem-sj... em.com, Portal <input type="checkbox"/> ise-server-cert-friendly-name Admin, EAP Authentication, RADIUS DTLS, perGrid, Portal 							

Serverzertifikat

Navigieren Sie zu Administration > Certificates > OCSP Client Profile, und klicken Sie auf Add

(Hinzufügen), um ein neues OCSP-Clientprofil hinzuzufügen.

- Name: ocsptestprofile
- URL des OCSP-Responders konfigurieren: <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 **ocsp_test_profile**

Description

Configure OCSP Responder

Server Connection

- Enable Secondary Server
- Always Access Primary Server First
- Failback 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

OCSP-Clientprofil

Navigieren Sie zu Administration > Certificates > Trusted Certificates, und bestätigen Sie, dass die vertrauenswürdige Zertifizierungsstelle in die ISE importiert wurde.

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

Certificate Name	Infrastructure	Expiration	Issued	Revoked	Status		
Cisco Manufacturing CA SHA2	Infrastructure	02	Cisco Manufacturing CA SH...	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 20...	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 20...	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 20...	Enabled
Cisco Root CA M2	Infrastructure Endpoints	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 20...	Enabled
Cisco RXC-R2	Cisco Services	01	Cisco RXC-R2	Cisco RXC-R2	Thu, 10 Jul 2014	Mon, 10 Jul 20...	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 20...	Enabled
CN=rootCACCommonName@rootCACom...	Infrastructure Cisco Services Endpoints AdminAuth	21 31 D3 DE ...	rootCACCommonName	rootCACCommonName	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 38 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

Vertrauenswürdige Zertifizierungsstelle

Überprüfen Sie die Zertifizierungsstelle, und klicken Sie auf die Schaltfläche Bearbeiten, und geben Sie die Details der OCSP-Konfiguration für die Zertifikatsstatusvalidierung ein.

- Validierung gegenüber OCSP-Service: ocsptestprofile
- Anfrage ablehnen, wenn OCSP den Status UNBEKANNT zurückgibt: prüfen
- Lehnen Sie die Anfrage ab, wenn der OCSP-Responder nicht erreichbar ist: Überprüfen

Cisco ISE Administration - System

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

Issuer

* Friendly Name ocsptestfriendlyname

Status Enabled

Description

Subject CN=ocsptestca-common-name

Issuer CN=ocsptestca-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 ocsptestprofile
- 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.

Validierung des Zertifikatsstatus

Schritt 6: Zulässige Protokolle hinzufügen

Navigieren Sie zu Policy > Results > Authentication > Allowed Protocols, bearbeiten Sie die Liste der Standard-Netzwerkzugriffsdienste, und aktivieren Sie dann Allow 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

EAP-TLS zulassen

Schritt 7. Policy Set hinzufügen

Navigieren Sie zu Policy > Policy Sets, und klicken Sie auf +, um einen Policy Set hinzuzufügen.

- Richtlinienatzname: EAP-TLS-Test
- Bedingungen: Network Access Protocol ENTSpricht RADIUS
- Zulässige Protokolle/Serversequenz: Standard-Netzwerkzugriff

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		

Policy Set hinzufügen

Schritt 8: Authentifizierungsrichtlinie hinzufügen

Navigieren Sie zu Policy Sets, und klicken Sie auf EAP-TLS-Test, um eine Authentifizierungsrichtlinie hinzuzufügen.

- Regelname: EAP-TLS-Authentifizierung
- Bedingungen: Network Access EapAuthentication EQUALS EAP-TLS UND Wired_802.1 X
- Verwenden: Identity_AD

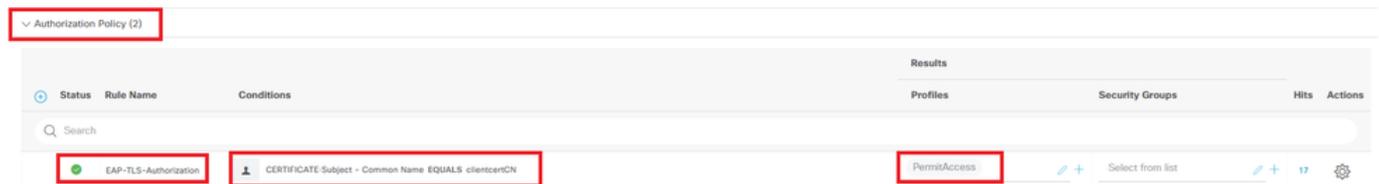


Authentifizierungsrichtlinie hinzufügen

Schritt 9. Autorisierungsrichtlinie hinzufügen

Navigieren Sie zu Policy Sets, und klicken Sie auf EAP-TLS-Test, um eine Autorisierungsrichtlinie hinzuzufügen.

- Regelname: EAP-TLS-Autorisierung
- Bedingungen: ZERTIFIKAT Betreff - Common Name EQUALS clientcertCN
- Ergebnisse: PermitAccess



Autorisierungsrichtlinie hinzufügen

Überprüfung

Schritt 1: Authentifizierungssitzung bestätigen

Führen `show authentication sessions interface GigabitEthernet1/0/3 details` Sie den Befehl aus, um die Authentifizierungssitzung in C1000 zu bestätigen.

<#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

Schritt 2: RADIUS-Live-Protokoll bestätigen

Navigieren Sie zu **Operations > RADIUS > Live Logs (Vorgänge > RADIUS > Live-Protokolle)** in der ISE-GUI, und bestätigen Sie das Live-Protokoll zur Authentifizierung.

Cisco ISE Operations - RADIUS

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

Refresh Never Show Latest 50 records 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-Authentication	PermitAccess	192.168.10.10
Jun 05, 2024 09:43:33.2...	●	🔒	0	clientcertCN	B4-96-91:14:3...	Intel-Device	EAP-TLS-Test >> EAP-TLS-Authentication	EAP-TLS-Test >> EAP-TLS-Authentication	PermitAccess	

Radius-Live-Protokoll

Bestätigen Sie das detaillierte Live-Protokoll der Authentifizierung.

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-sy;.em.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-sy;:em.com
AD-User-SamAccount-Name	clientcertCN
AD-User-Qualified-Name	clientcertCN@ad.rem-sy;:em.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;:em.com
24319	Single matching account found in forest - ad.rem-s;:em.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

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-Dump

Im TCP-Dump in der ISE erwarten Sie Informationen zur OCSP-Antwort und zur Radius-Sitzung.

OCSP-Anfrage und -Antwort:

No.	Time	Identification	Source	S.Port	Destination	D.Port	Time to Live	Protocol	Length	TCP.Se	Next sz	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

Paketerfassung von OCSP-Anfragen und -Antworten

```

> 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
  
```

Erfassen der Details der OCSP-Antwort

Radius-Sitzung:

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

Paketerfassung der RADIUS-Sitzung

Zugehörige Informationen

[Konfigurieren der EAP-TLS-Authentifizierung mit der ISE](#)

[Konfigurieren von TLS/SSL-Zertifikaten in der ISE](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.