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

Inhalt

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:

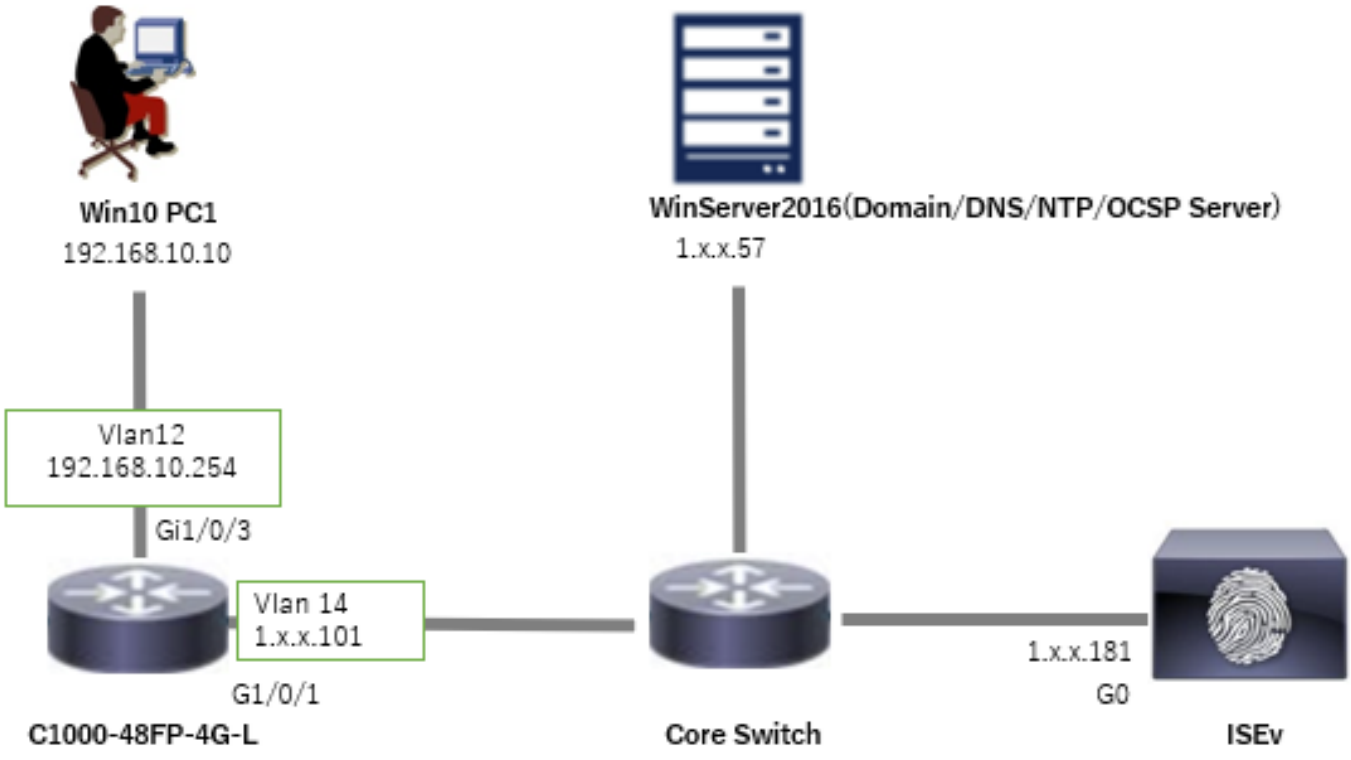
- Identity Services Engine Virtual 3.2 Patch 6
- C1000-48FP-4G-L 15,2(7)E9

- 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: ocsp-ca-common-name
- Client-Zertifikat: clientcertCN
- Serverzertifikat: ise32-01.ad.rem-xxx.com
- OCSP-Signaturzertifikat: ocspSignCommonName

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
```

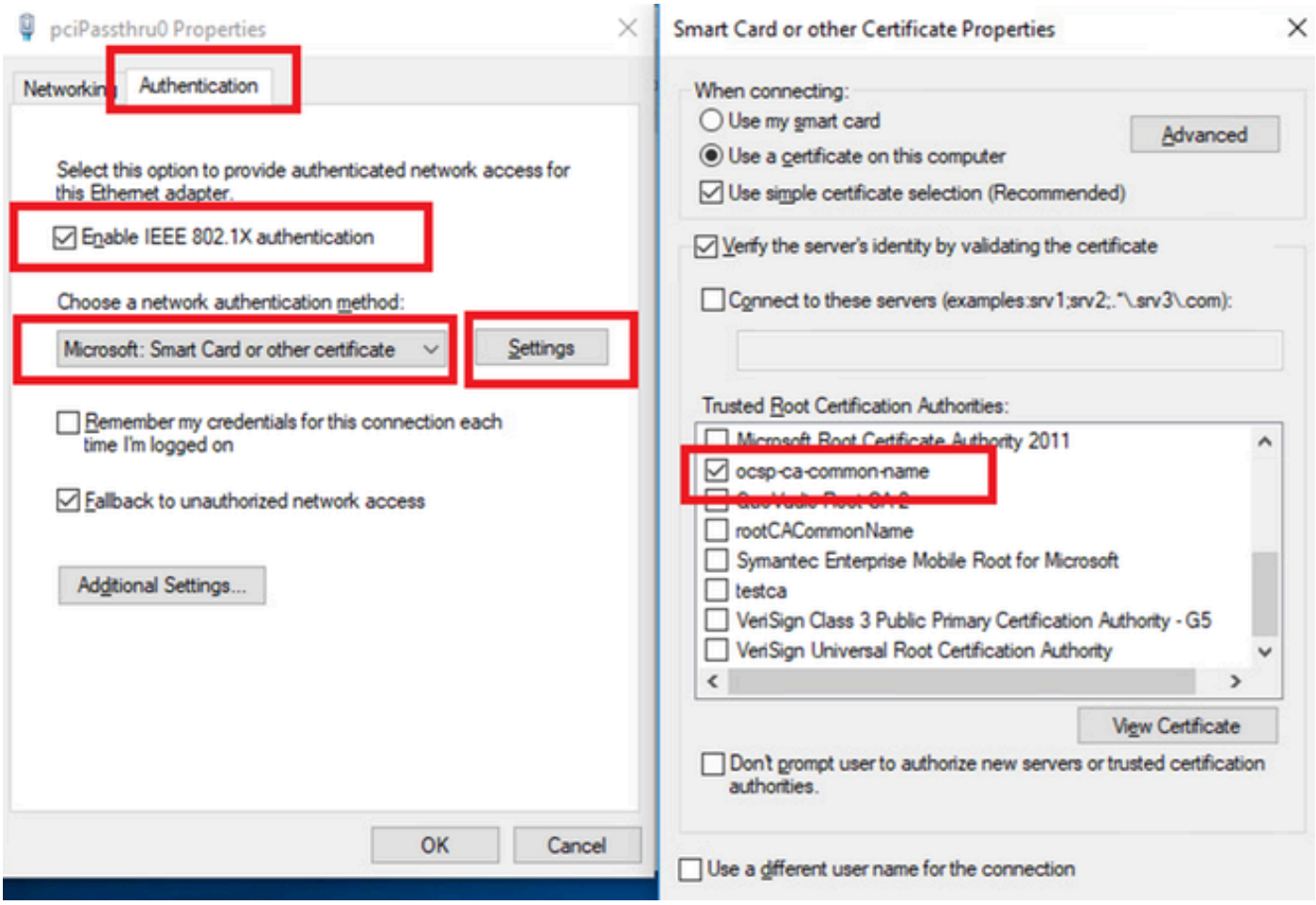
```
interface Vlan14
ip address 1.x.x.101 255.0.0.0

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

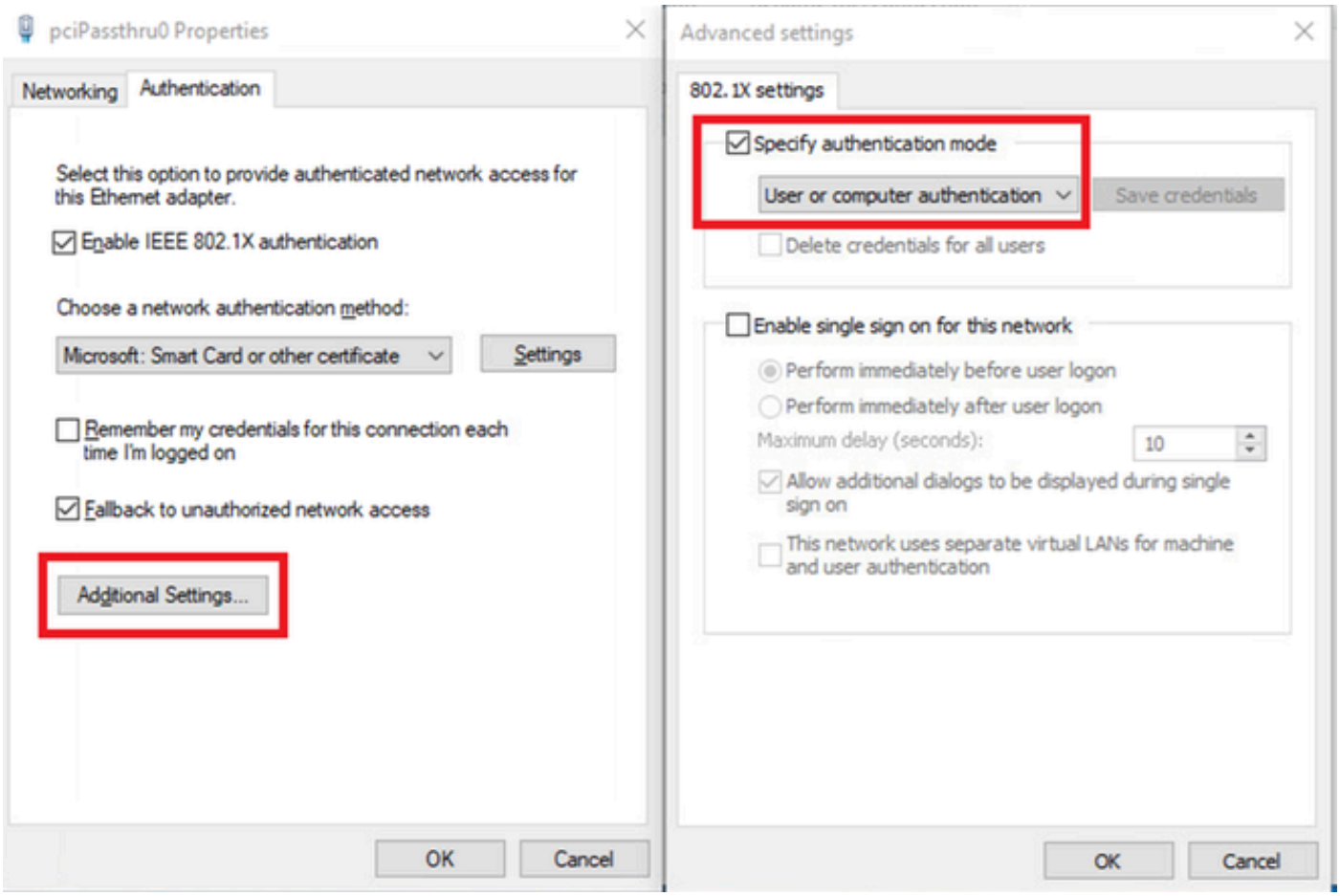
Navigieren Sie zuAuthentication, aktivieren SieEnable IEEE 802.1X authentication, und wählen Sie Microsoft: Smart Card oder sonstiges Zertifikat aus.

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



Zertifikatsauthentifizierung aktivieren

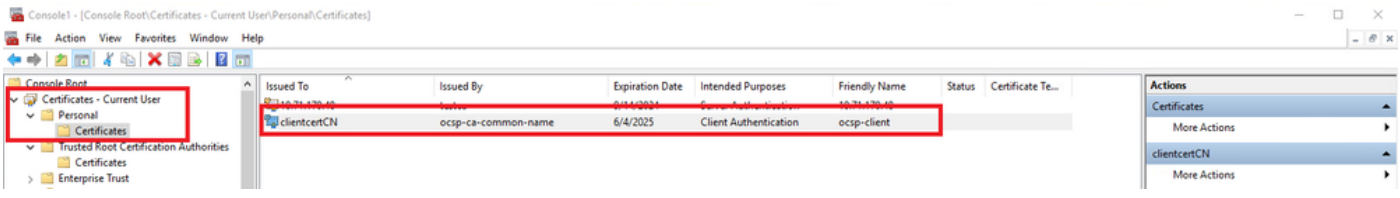
Navigieren Sie zuAuthentifizierung, und aktivieren SieZusätzliche Einstellungen. Wählen SieBenutzer- oder Computerauthentifizierung aus der Dropdown-Liste aus.



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.

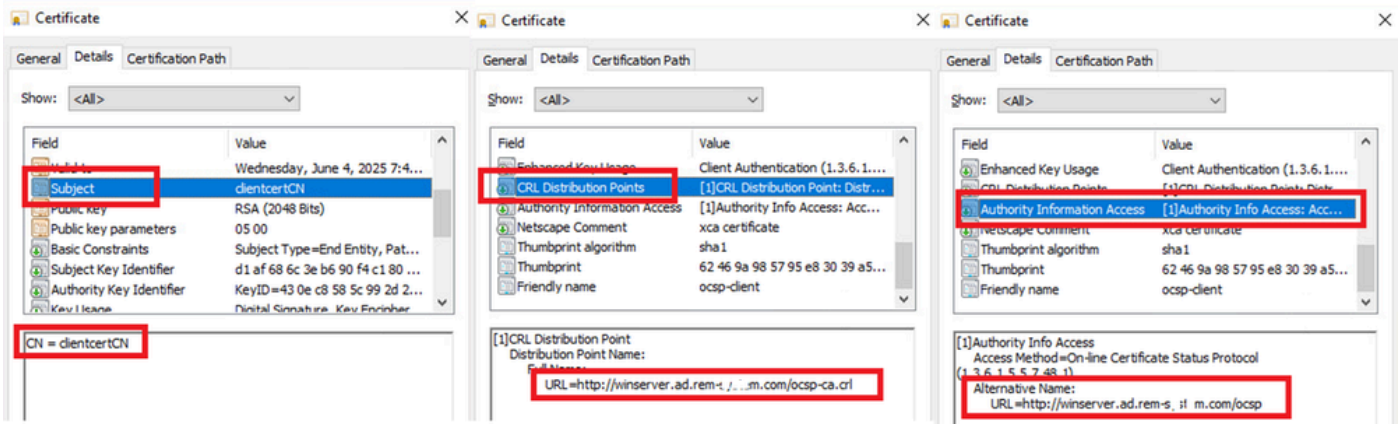


Clientzertifikat bestätigen

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

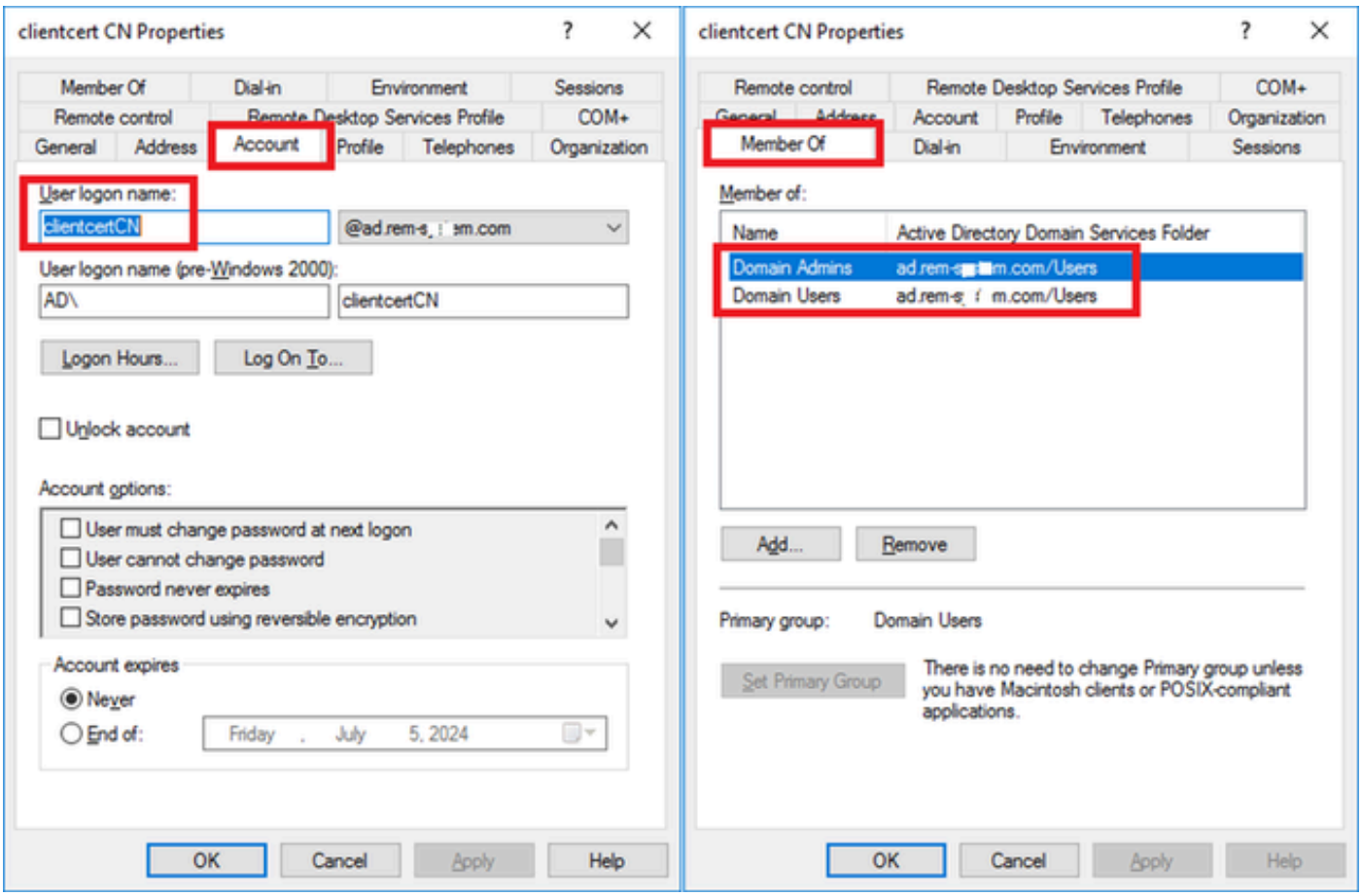


Details zum Client-Zertifikat

Konfiguration in Windows Server

Schritt 1: Benutzer hinzufügen

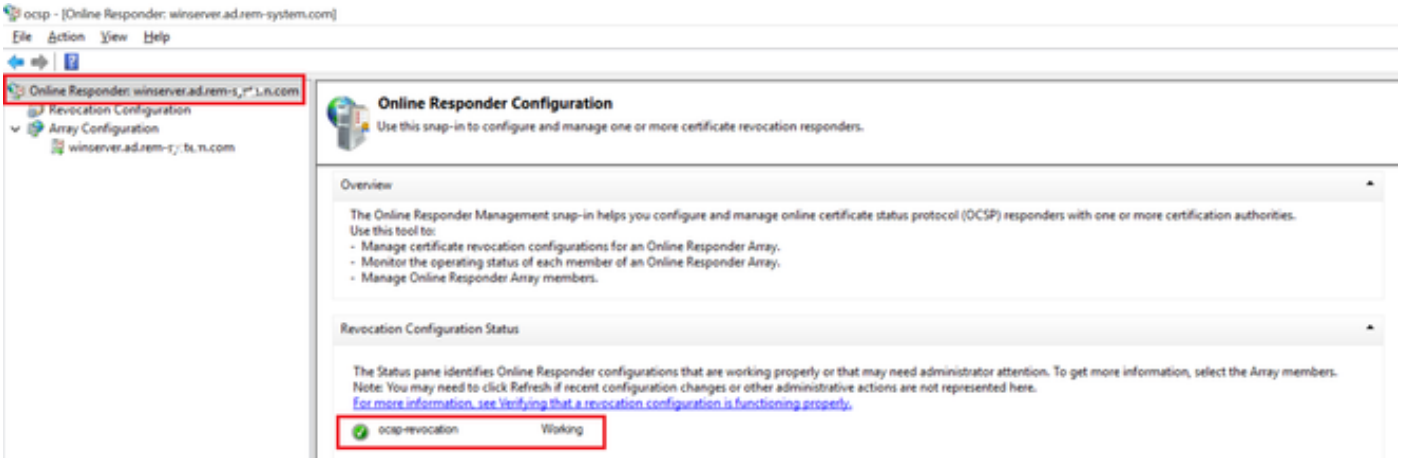
Navigieren Sie zu Active Directory-Benutzer und -Computer, und klicken Sie auf Benutzer. Fügen Sie clientcertCN als Benutzernamen hinzu.



Benutzername für Anmeldung

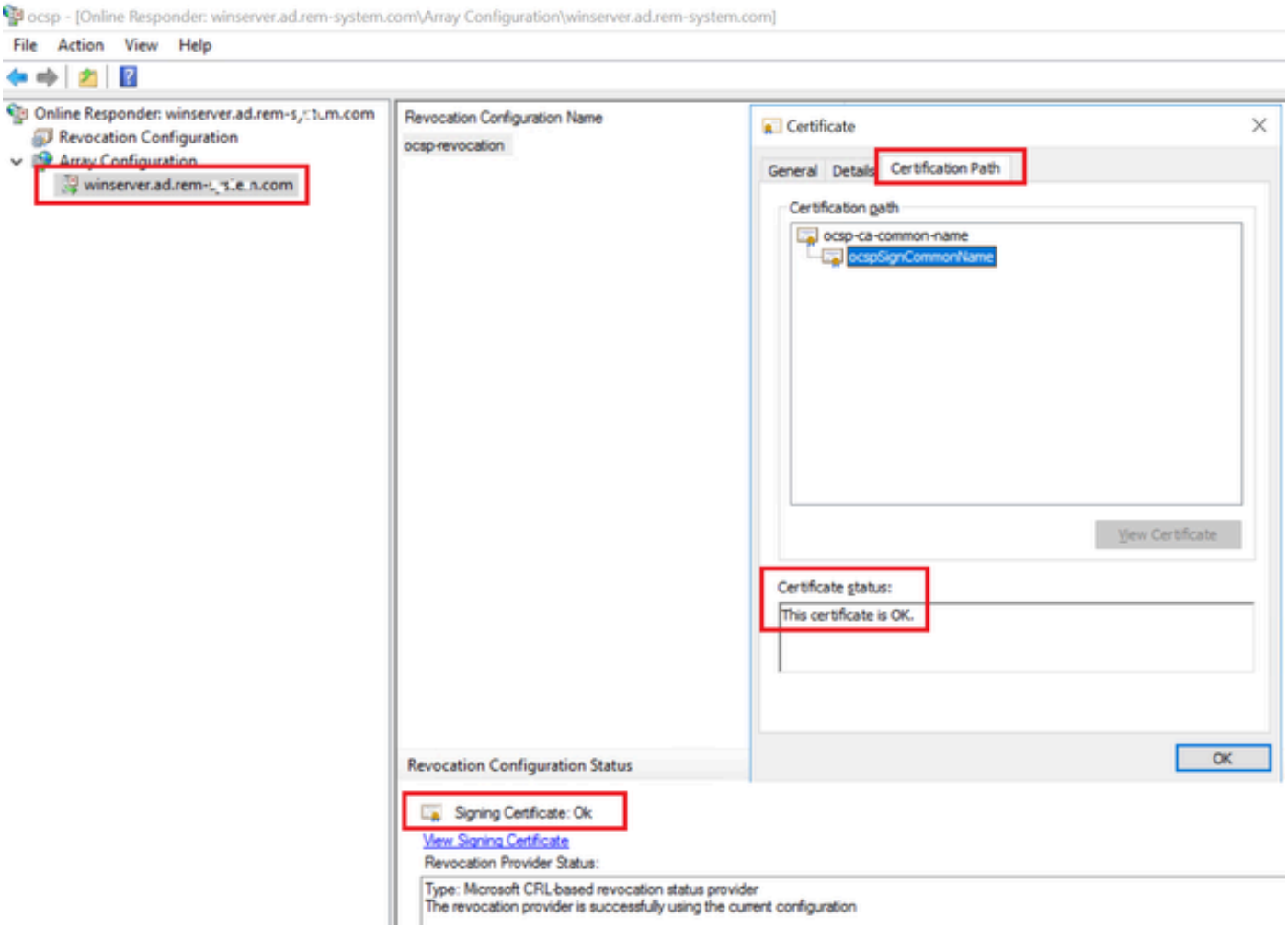
Schritt 2: OCSP-Dienst bestätigen

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.

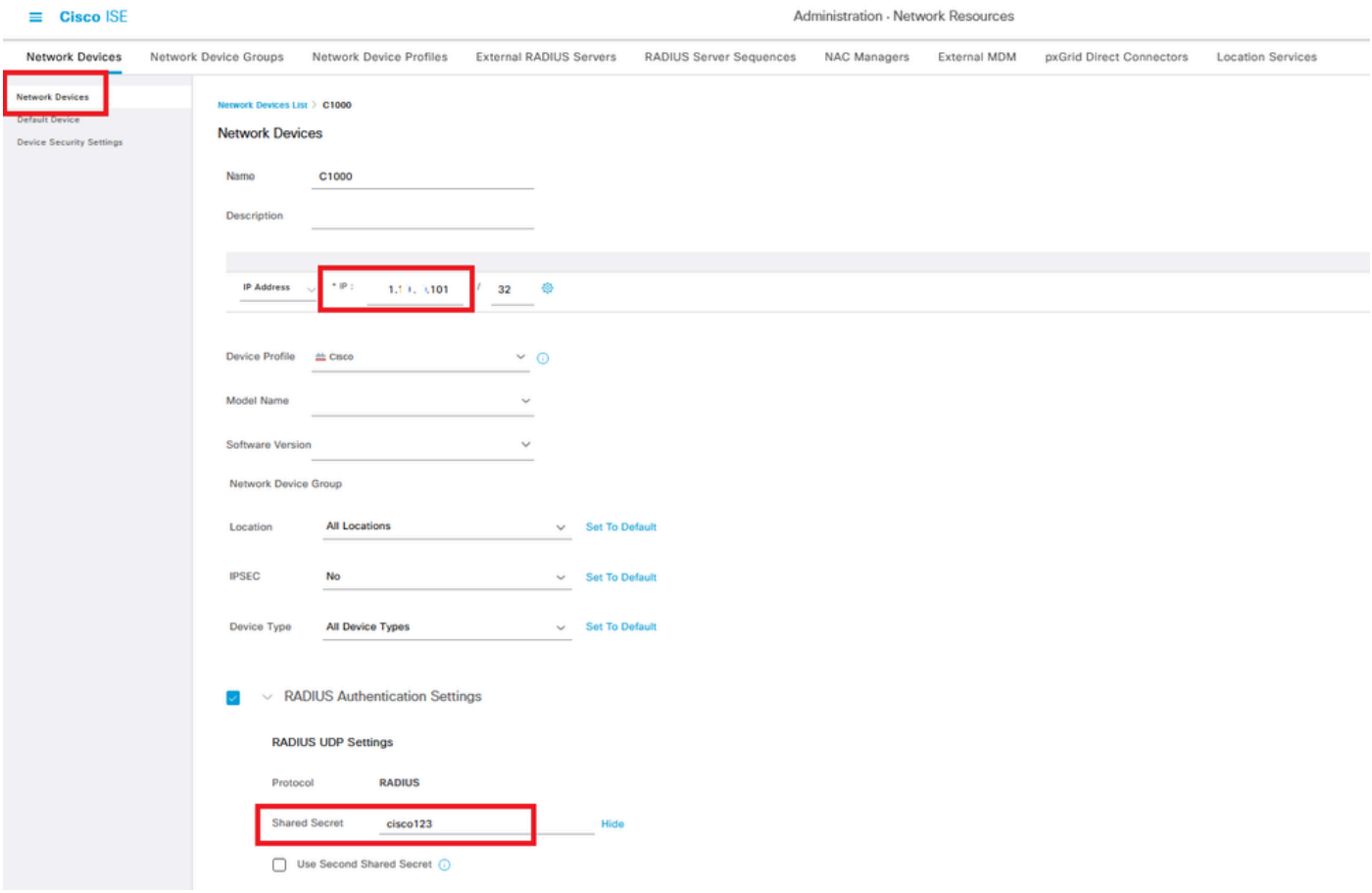


Status des OCSP-Signaturzertifikats

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.

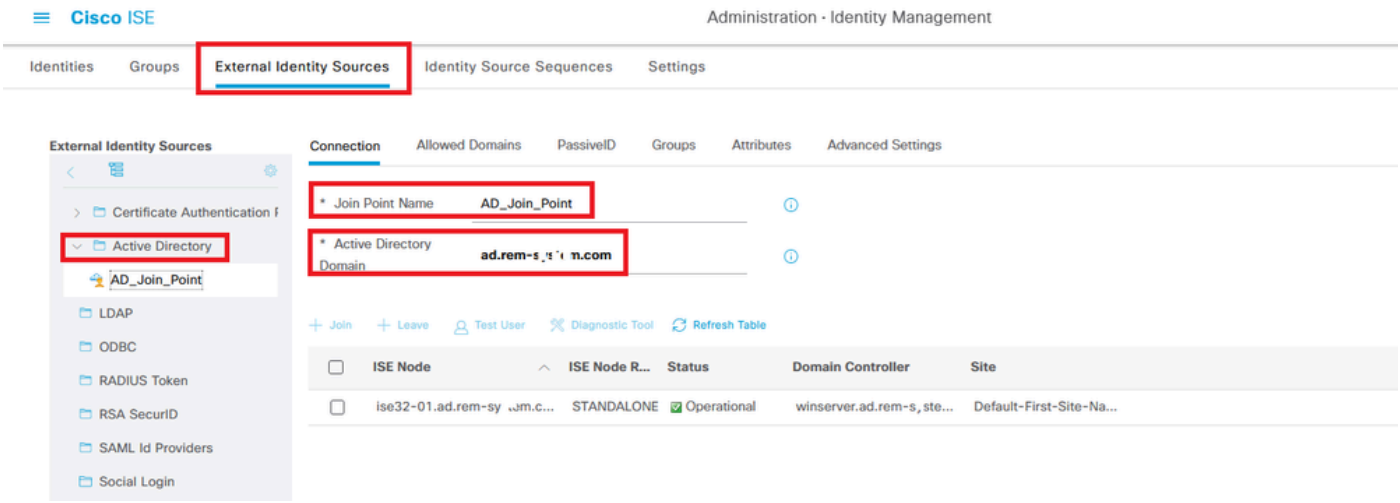


Gerät hinzufügen

Schritt 2: Active Directory hinzufügen

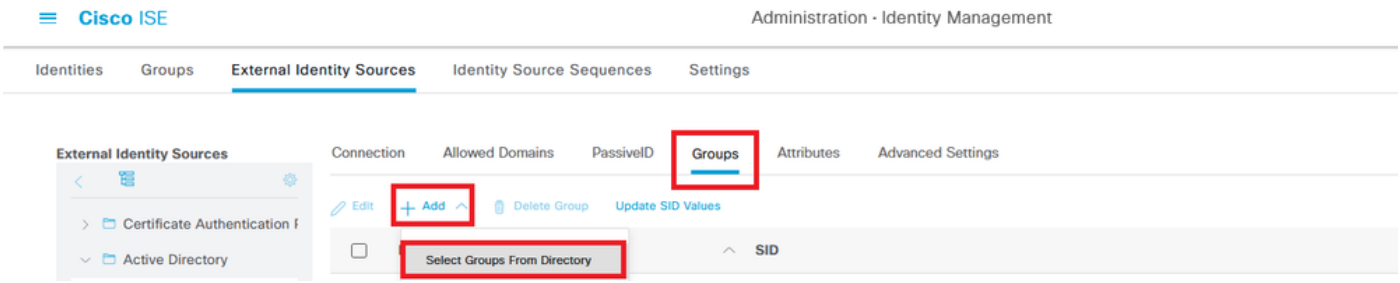
Navigieren Sie zu Administration > External Identity Sources > Active Directory, klicken Sie aufRegisterkarte Connection, und fügen Sie Active Directory zur ISE hinzu.

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



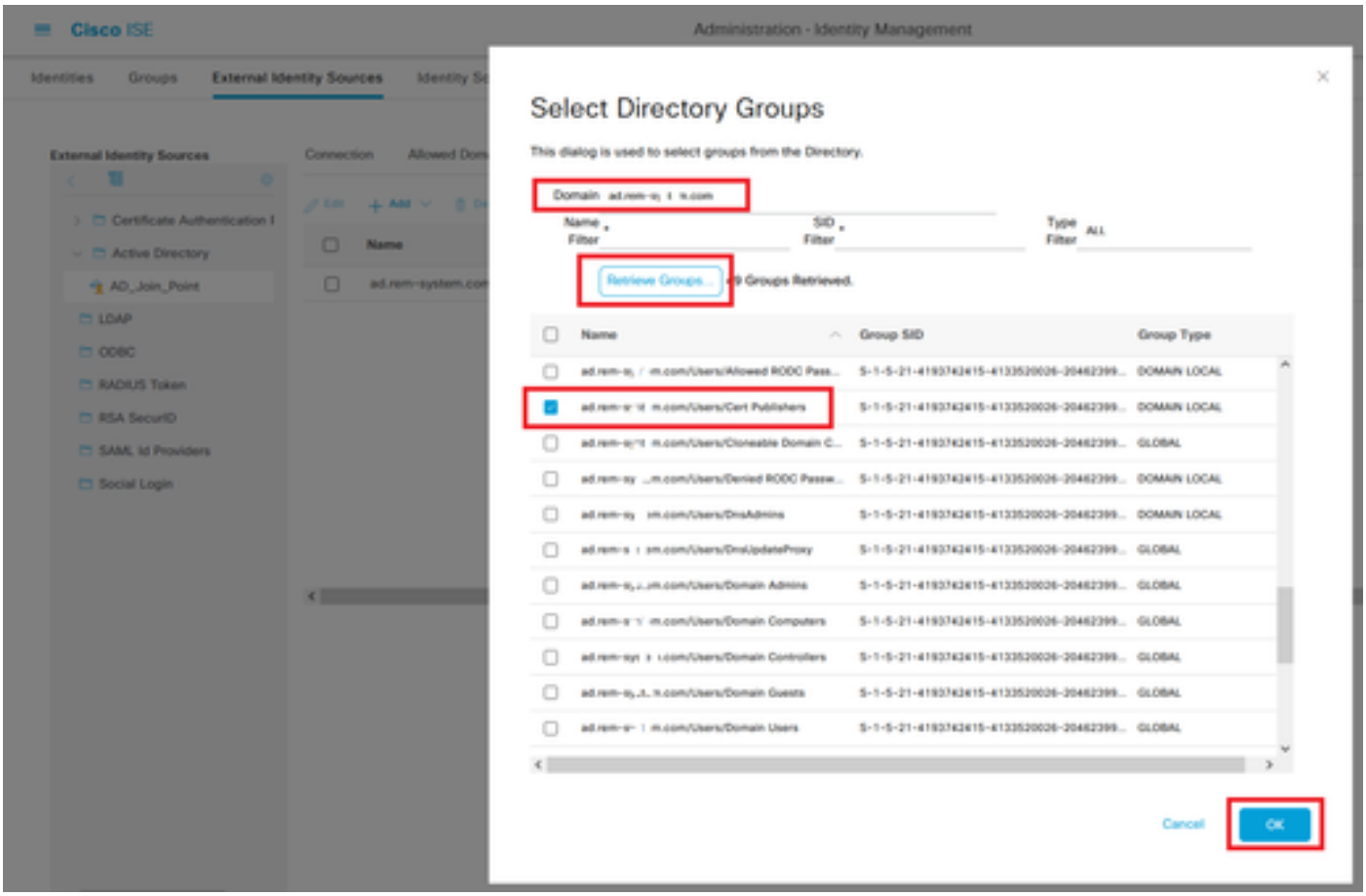
Active Directory hinzufügen

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



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.

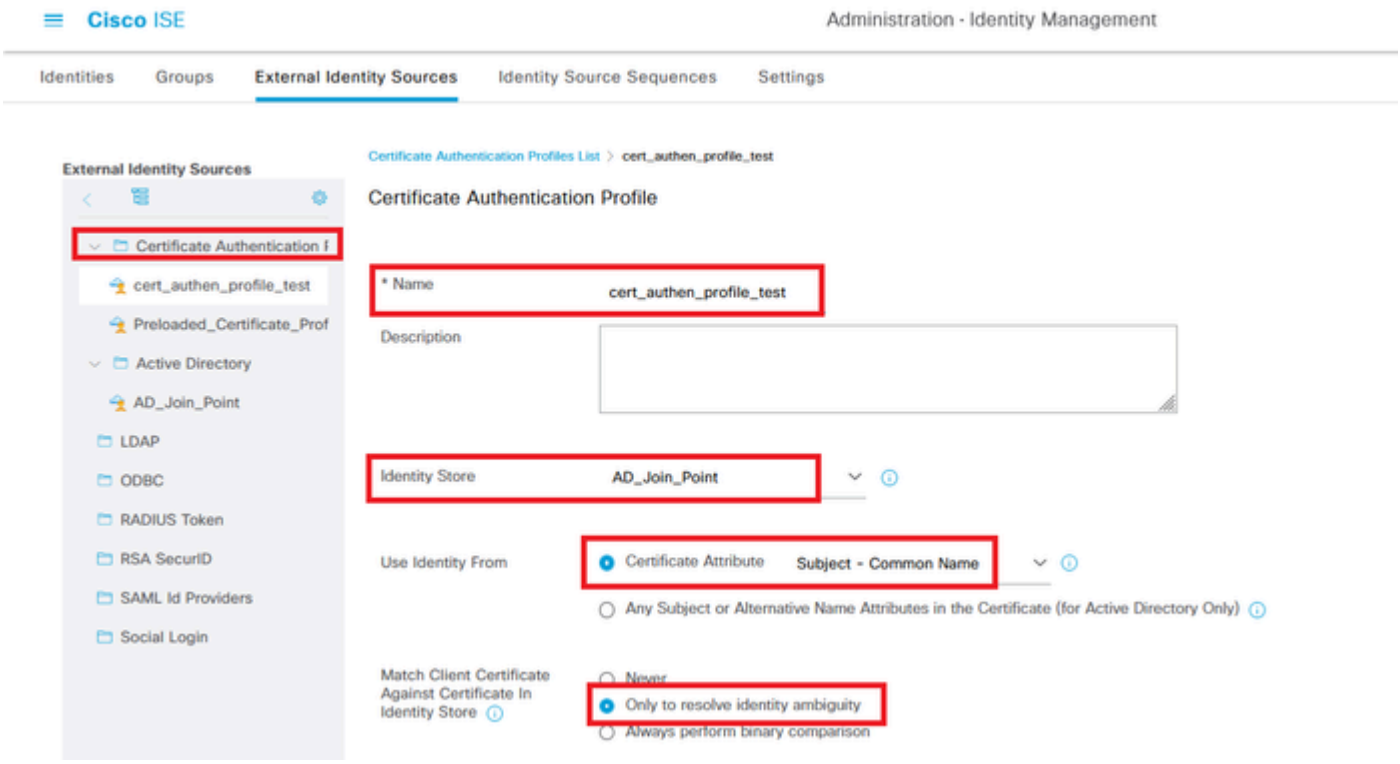


Zertifikatverleger überprüfen

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.

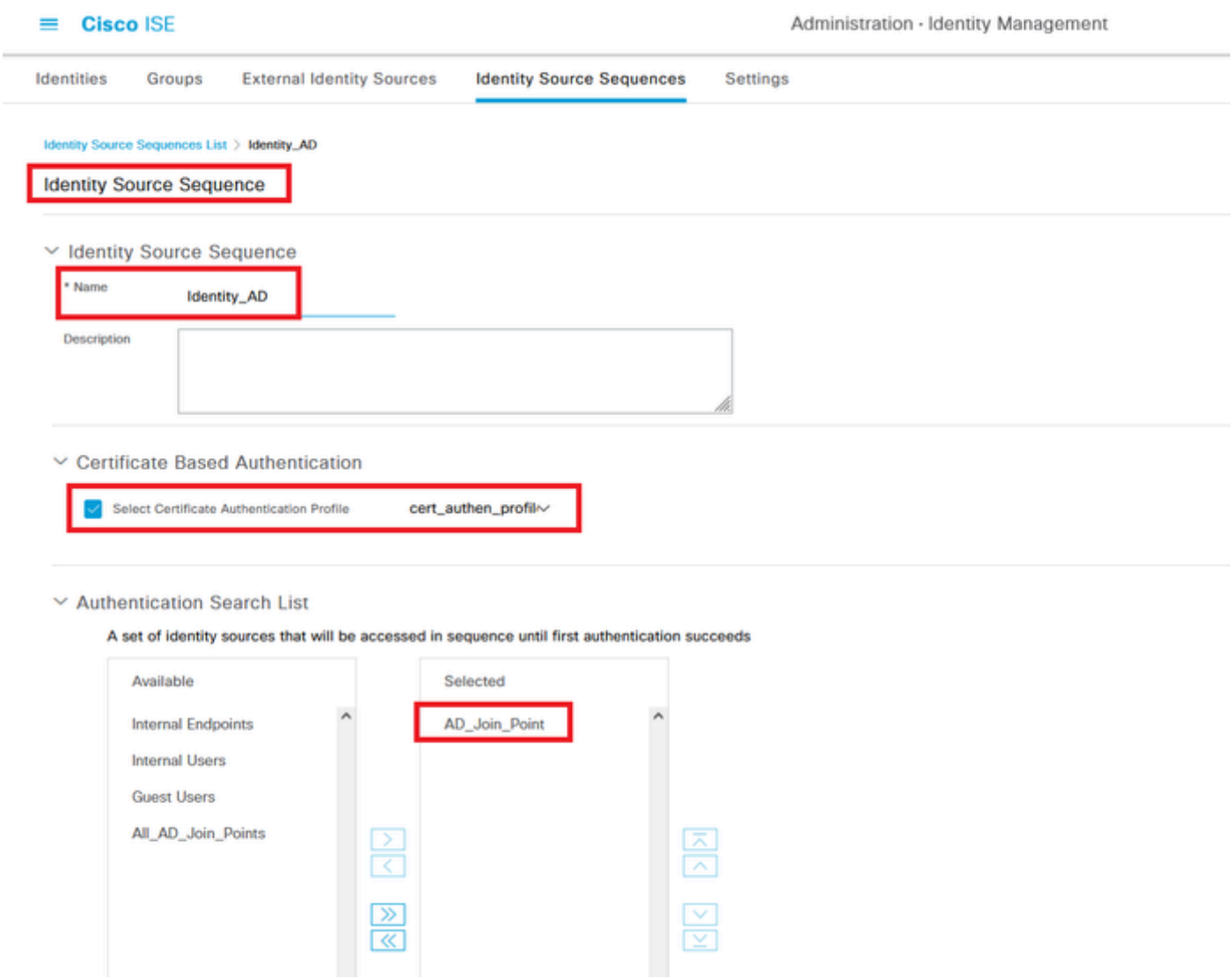


Zertifikatauthentifizierungsprofil hinzufügen

Schritt 4: Identitätsquelltext hinzufügen

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

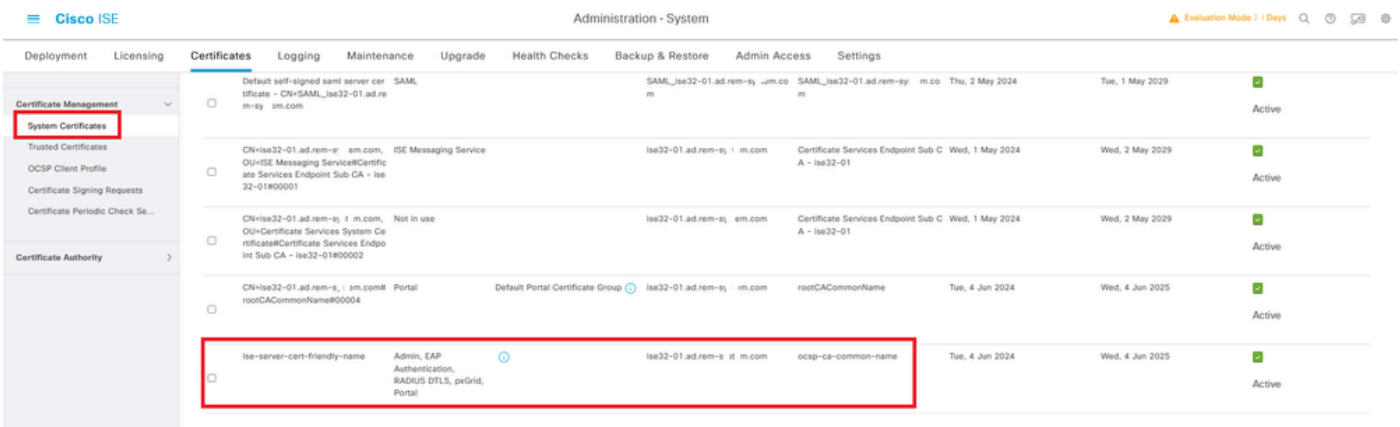
- Name: Identity_AD
- Wählen Sie Certificate Authentication Profile: cert_authen_profile_test
- Authentifizierungs-Suchliste: AD_Join_Point



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.

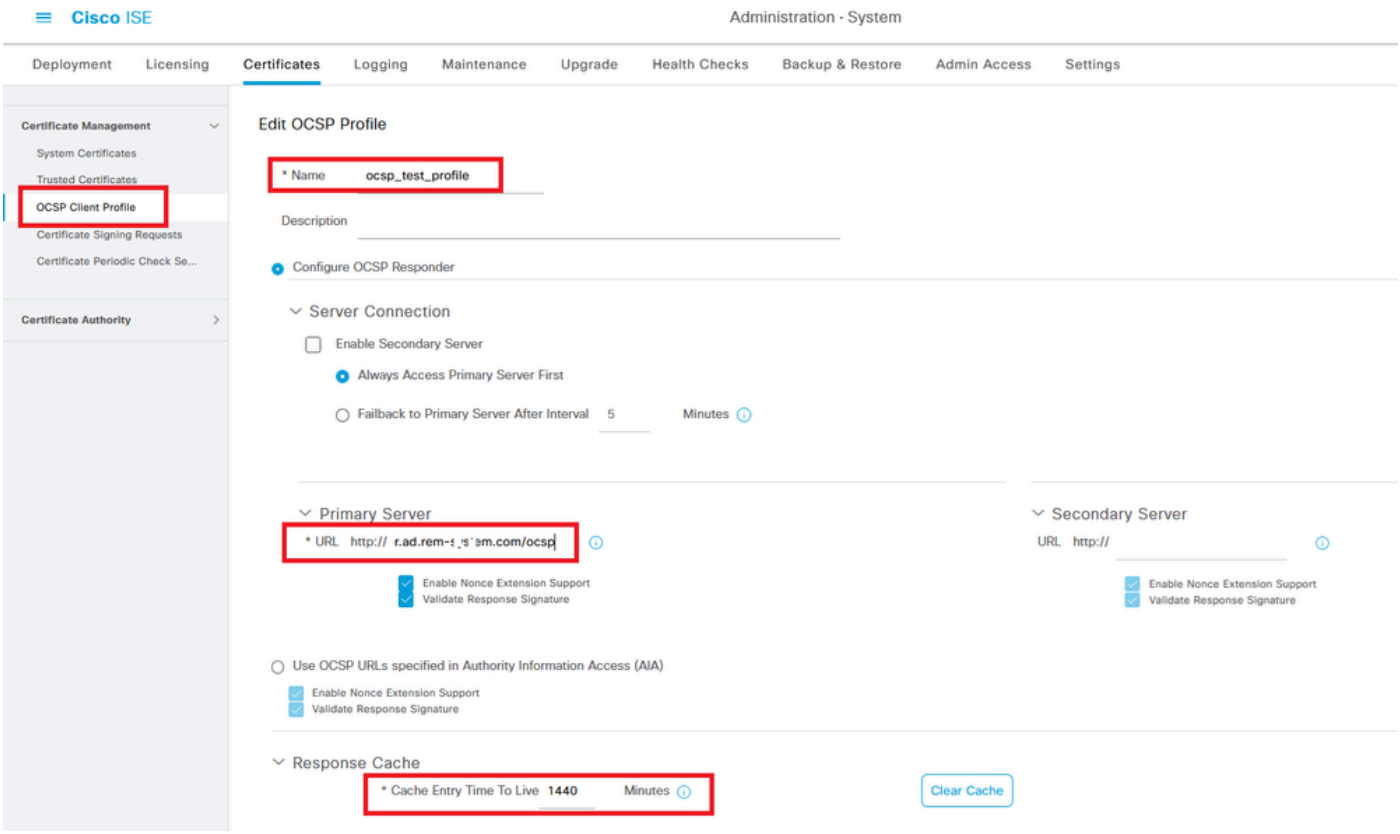


Serverzertifikat

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

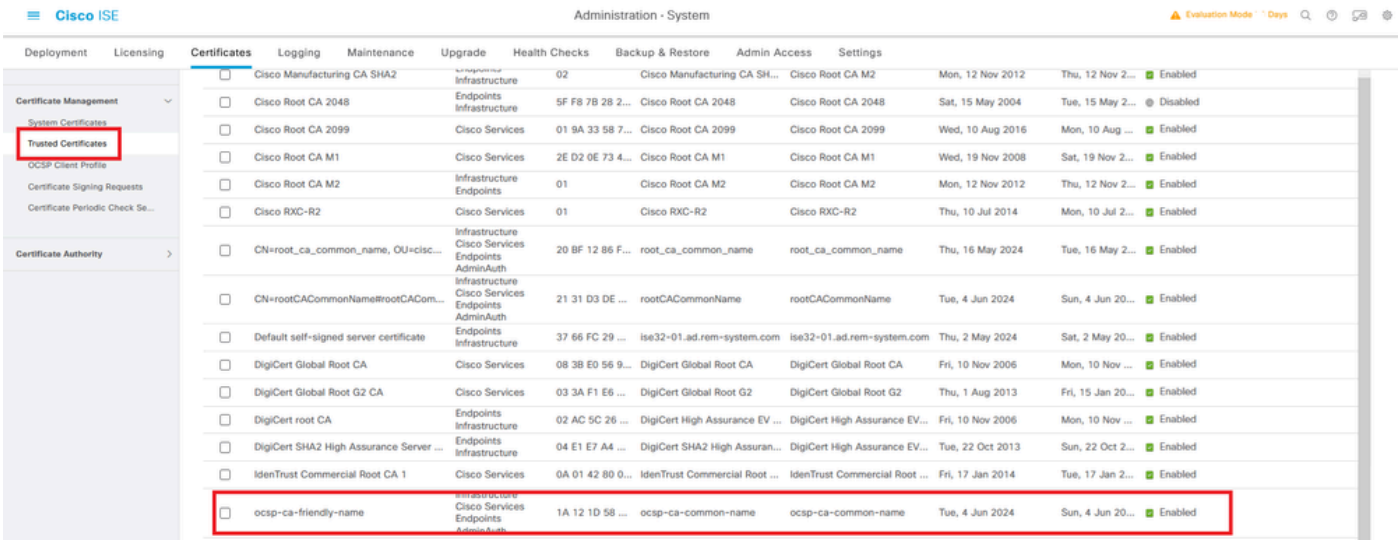
(Hinzufügen), um ein neues OCSP-Clientprofil hinzuzufügen.

- Name: ocsp_test_profile
- URL des OCSP-Responders konfigurieren: http://winserver.ad.rem-xxx.com/ocsp



OCSP-Clientprofil

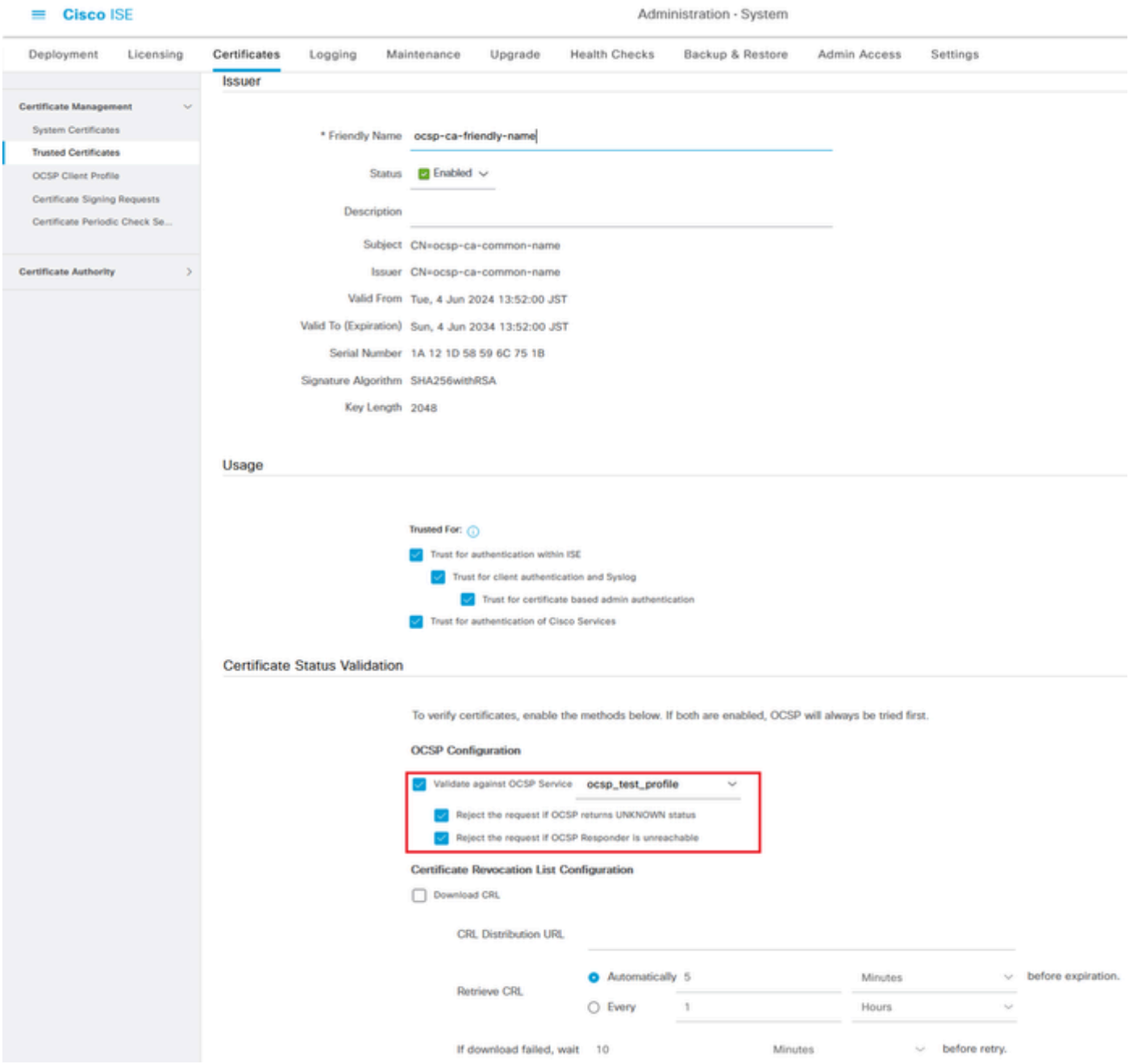
Navigieren Sie zu Administration > Certificates > Trusted Certificates, und bestätigen Sie, dass die vertrauenswürdige Zertifizierungsstelle in die ISE importiert wurde.



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.

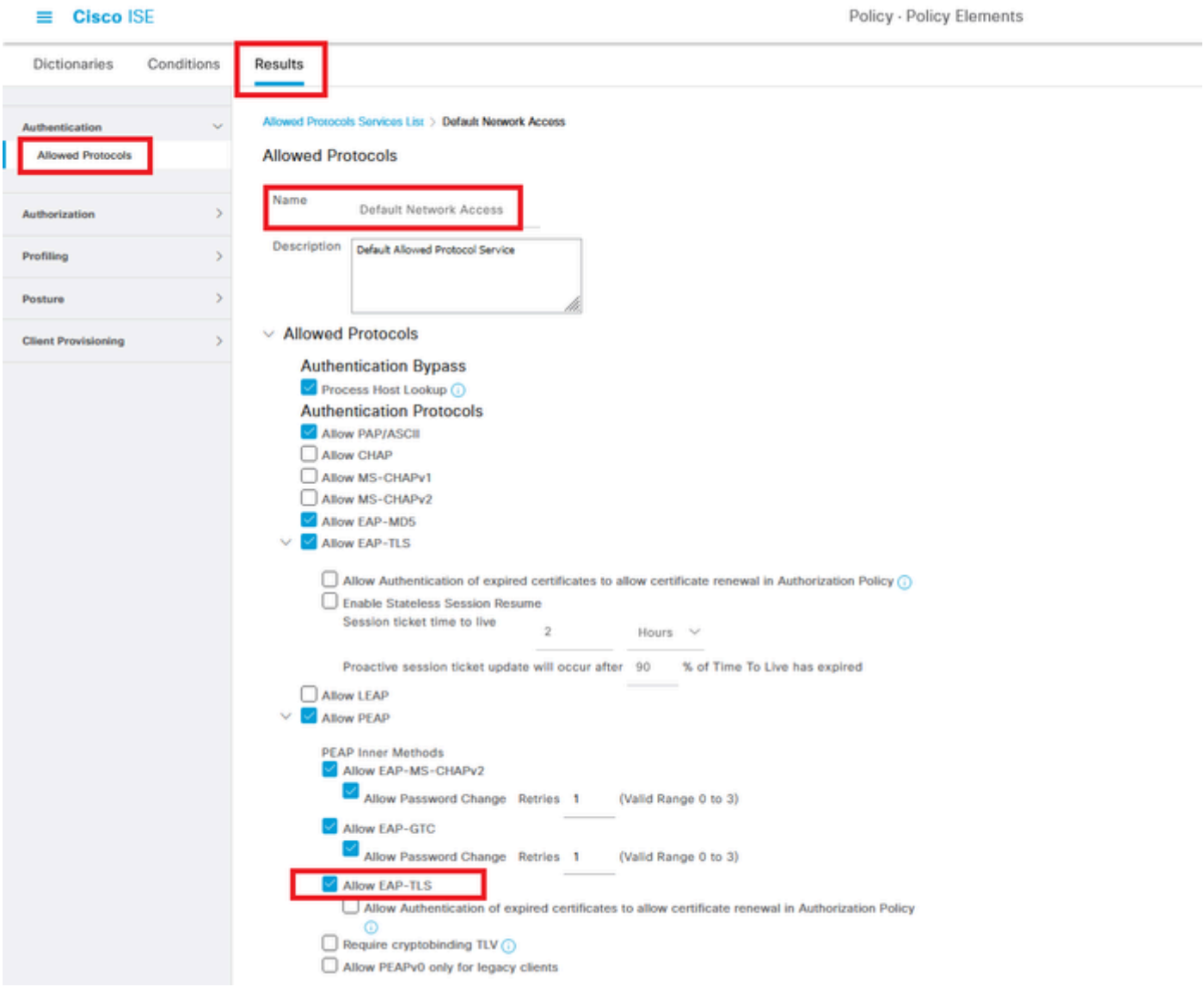
- Validierung gegenüber OCSP-Service: ocsp_test_profile
- Anfrage ablehnen, wenn OCSP den Status UNBEKANNT zurückgibt: prüfen
- Lehnen Sie die Anfrage ab, wenn der OCSP-Responder nicht erreichbar ist: Überprüfen



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.

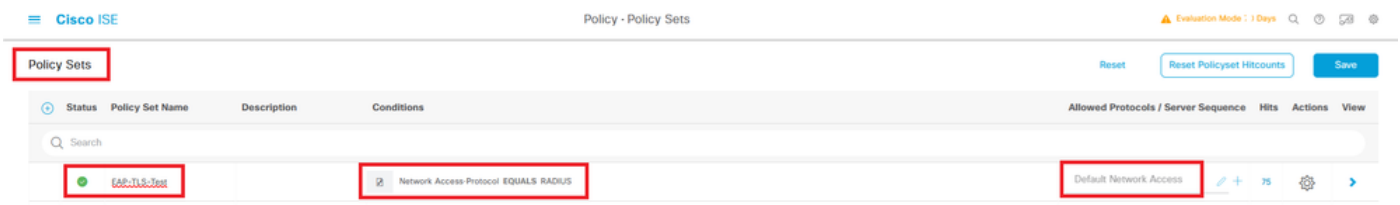


EAP-TLS zulassen

Schritt 7. Policy Set hinzufügen

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

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



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 ENTSPRICHT 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#

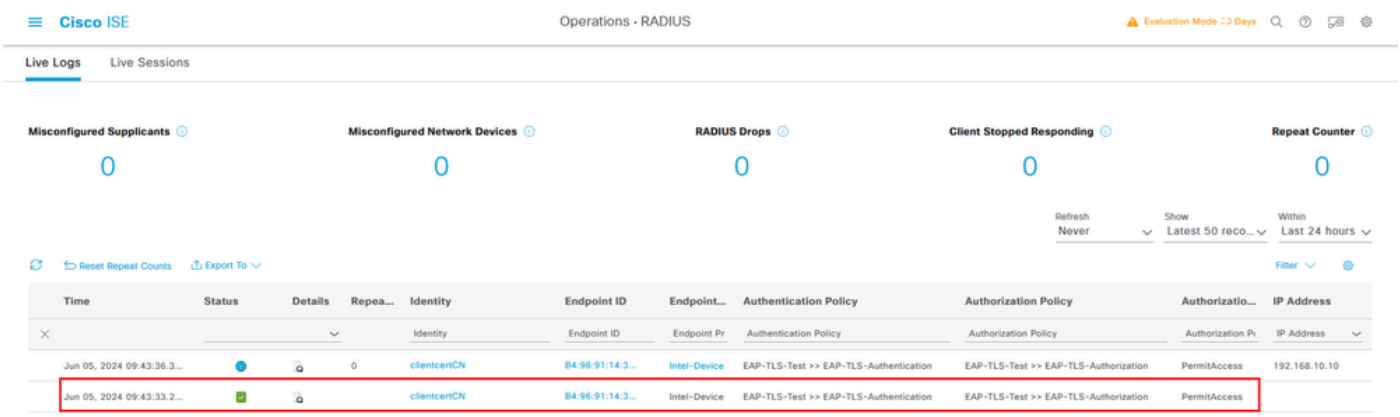
show authentication sessions interface GigabitEthernet1/0/3 details

```
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: 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
```

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.



Radius-Live-Protokoll

Bestätigen Sie das detaillierte Live-Protokoll der Authentifizierung.

Cisco ISE

Overview

Event	5200 Authentication succeeded
Username	clientcertCN
Endpoint Id	B4:96:91:14:39:8C
Endpoint Profile	Intel-Device
Authentication Policy	EAP-TLS-Test >> EAP-TLS-Authentication
Authorization Policy	EAP-TLS-Test >> EAP-TLS-Authorization
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2024-06-05 09:43:33.268
Received Timestamp	2024-06-05 09:43:33.268
Policy Server	ise32-01
Event	5200 Authentication succeeded
Username	clientcertCN
Endpoint Id	B4:96:91:14:39:8C
Calling Station Id	B4-96-91-14-39-8C
Endpoint Profile	Intel-Device
Authentication Identity Store	AD_Join_Point
Identity Group	Profiled
Audit Session Id	01C200650000000933E4E87D9

Other Attributes

ConfigVersionId	167
DestinationPort	1645
Protocol	Radius
NAS-Port	50103
Framed-MTU	1500
State	37CPMSessionID=01C200650000000933E4E87D9;31SessionID=ise32-01/506864164/73;
AD-User-Resolved-Identities	clientcertCN@ad.rem-s[illegible]em.com
AD-User-Candidate-Identities	clientcertCN@ad.rem-s[illegible]em.com
TotalAuthenLatency	324
ClientLatency	80
AD-User-Resolved-DNs	CN=clientcert CN,CN=Users,DC=ad,DC=rem-s[illegible]tem,DC=com
AD-User-DNS-Domain	ad.rem-s[illegible]tem.com
AD-User-NetBios-Name	AD
IsMachineIdentity	false
AD-User-SamAccount-Name	clientcertCN
AD-User-Qualified-Name	clientcertCN@ad.rem-s[illegible]m.com
AD-User-SamAccount-Name	clientcertCN
AD-User-Qualified-Name	clientcertCN@ad.rem-s[illegible]m.com
TLSCipher	ECDHE-RSA-AES256-GCM-SHA384
TLSVersion	TLSv1.2
DTLSSupport	Unknown
Subject	CN=clientcertCN
Issuer	CN=ocsp-ca-common-name

Steps

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
11507	Extracted EAP-Response/Identity
12500	Prepared EAP-Request proposing EAP-TLS with challenge
12625	Valid EAP-Key-Name attribute received
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12502	Extracted EAP-Response containing EAP-TLS challenge-response and accepting EAP-TLS as negotiated
12800	Extracted first TLS record; TLS handshake started
12545	Client requested EAP-TLS session ticket
12542	The EAP-TLS session ticket received from supplicant while the stateless session resume is disabled. Performing full authentication
12805	Extracted TLS ClientHello message
12806	Prepared TLS ServerHello message
12807	Prepared TLS Certificate message
12808	Prepared TLS ServerKeyExchange message
12809	Prepared TLS CertificateRequest message
12810	Prepared TLS ServerDone message
12505	Prepared EAP-Request with another EAP-TLS challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12504	Extracted EAP-Response containing EAP-TLS challenge-response
12988	Take OCSP servers list from OCSP service configuration - certificate for clientcertCN
12550	Sent an OCSP request to the primary OCSP server for the CA - External OCSP Server
12553	Received OCSP response - certificate for clientcertCN
12554	OCSP status of user certificate is good - certificate for clientcertCN
12811	Extracted TLS Certificate message containing client certificate
12812	Extracted TLS ClientKeyExchange message
12813	Extracted TLS CertificateVerify message
12803	Extracted TLS ChangeCipherSpec message
24432	Looking up user in Active Directory - AD_Join_Point
24325	Resolving identity - clientcertCN
24313	Search for matching accounts at join point - ad.rem-s[illegible]m.com
24319	Single matching account found in forest - ad.rem-s[illegible]m.com
24323	Identity resolution detected single matching account
24700	Identity resolution by certificate succeeded - AD_Join_Point
22037	Authentication Passed
12506	EAP-TLS authentication succeeded
24715	ISE has not confirmed locally previous successful machine authentication for user in Active Directory
15036	Evaluating Authorization Policy
24209	Looking up Endpoint in Internal Endpoints IDStore - clientcertCN
15036	Evaluating Authorization Policy
24209	Looking up Endpoint in Internal Endpoints IDStore - clientcertCN
24211	Found Endpoint in Internal Endpoints IDStore
15016	Selected Authorization Profile - PermitAccess
22081	Max sessions policy passed
22080	New accounting session created in Session cache
11503	Prepared EAP-Success
11002	Returned RADIUS Access-Accept

Authentifizierungsdetails

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
```

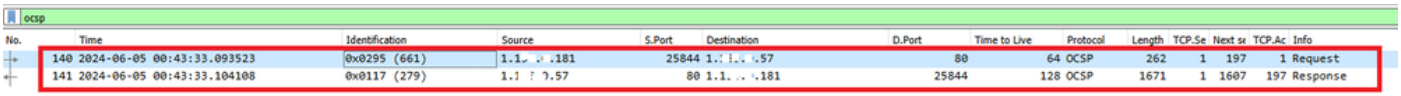
Code=4(AccountingRequest)

```
 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
```

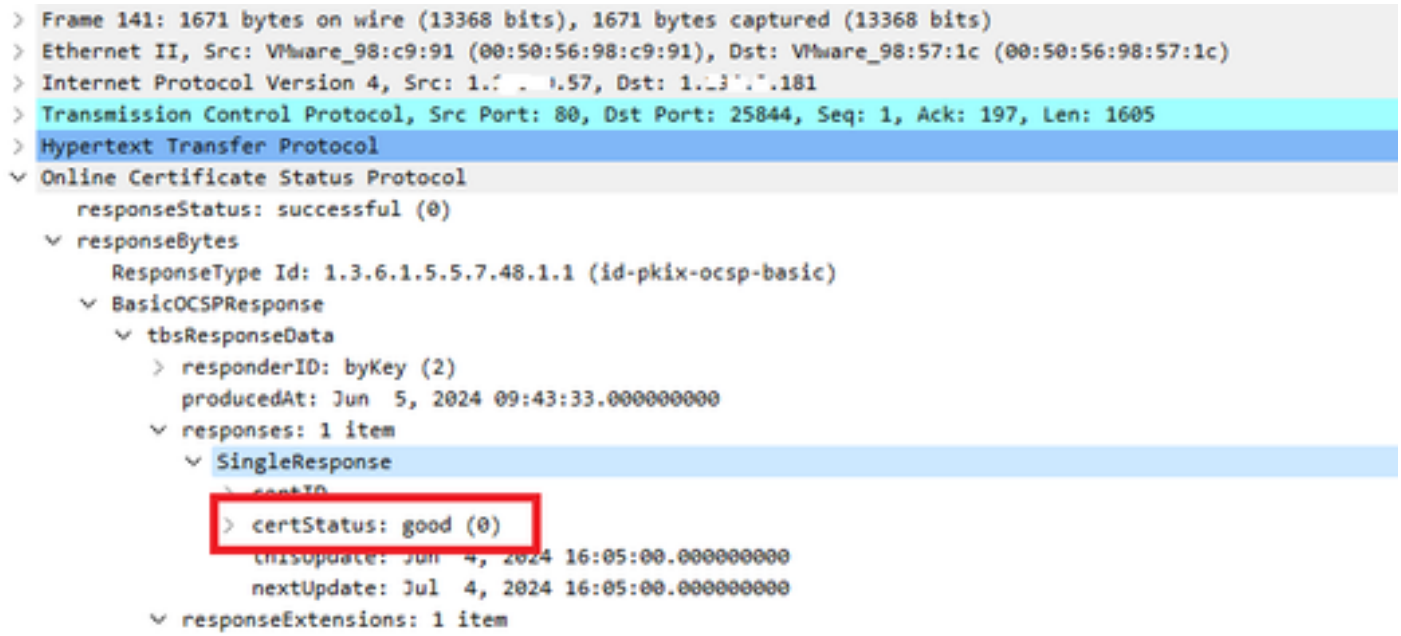
2. TCP-Dump

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

OCSP-Anfrage und -Antwort:

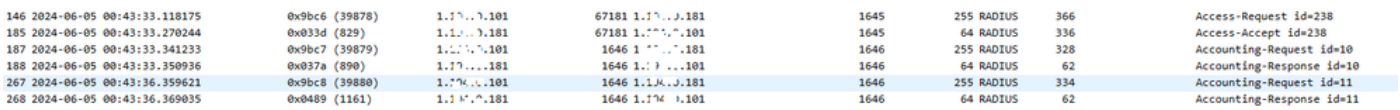


Paketerfassung von OCSP-Anfragen und -Antworten



Erfassen der Details der OCSP-Antwort

Radius-Sitzung:



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.