

OCSP مادختساب EAP-TLS ةقداصم نيوكت يف ISE

تايوتحمل

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةكبشلال يطيختملا مسرلا](#)

[ةيساسأ تامولعم](#)

[تان نيوكتلا](#)

[C1000 يف نيوكتلا](#)

[Windows رتوي بمك يف نيوكتلا](#)

[مدختسملا ةقداصم نيوكت 1. ةوطخل](#)

[ليعمل ةداهش ديكأت 2. ةوطخل](#)

[Windows مداخ يف نيوكتلا](#)

[نيمدختسم ةفاضلا 1. ةوطخل](#)

[OCSP ةمدخ ديكأت 2. ةوطخل](#)

[ISE يف نيوكتلا](#)

[زاهج ةفاضلا 1. ةوطخل](#)

[Active Directory ةفاضلا 2. ةوطخل](#)

[ةداهشلا ةقداصم فيرعت فلم ةفاضلا 3. ةوطخل](#)

[ةيوهلا رصم ةلسلس ةفاضلا 4. ةوطخل](#)

[ISE يف Confrim ةداهش 5. ةوطخل](#)

[اهب حومسمل تالوكوتوربلا ةفاضلا 6. ةوطخل](#)

[جهن ةعومجم ةفاضلا 7. ةوطخل](#)

[ةقداصملا جهن ةفاضلا 8. ةوطخل](#)

[ليوختلا جهن ةفاضلا 9. ةوطخل](#)

[ةحصللا نم ققحتلا](#)

[ةقداصملا لمع ةسلس ديكأت 1. ةوطخل](#)

[Radius Live لچس ديكأت 2. ةوطخل](#)

[اهجالص او عاخذالا فاشكتسا](#)

[عاخذالا جيحصت لچس 1.](#)

[TCP غيرفت 2.](#)

[ةلص تاذا تامولعم](#)

ةمدقملا

ققحتلل OCSP مادختساب EAP-TLS ةقداصم دادعال ةبولطملا تاوطخللا دنتسملا اذه فصي
يلعفللا تقولا يف لي عمل ةداهش لاطبإ نم

ةيساسألا تابلطتملا

تابلطتملا

ةيلتال عيضاوملاب ةفرعم كيديل نوكت نأب Cisco ي صوت

- Cisco نم ةيوهلا تامدخ كرحم نيوكت
- Cisco Catalyst نيوكت
- تنرتنإل ربق ةداهشلا ةلاح لوكتورب

ةمدختسملا تانوكملا

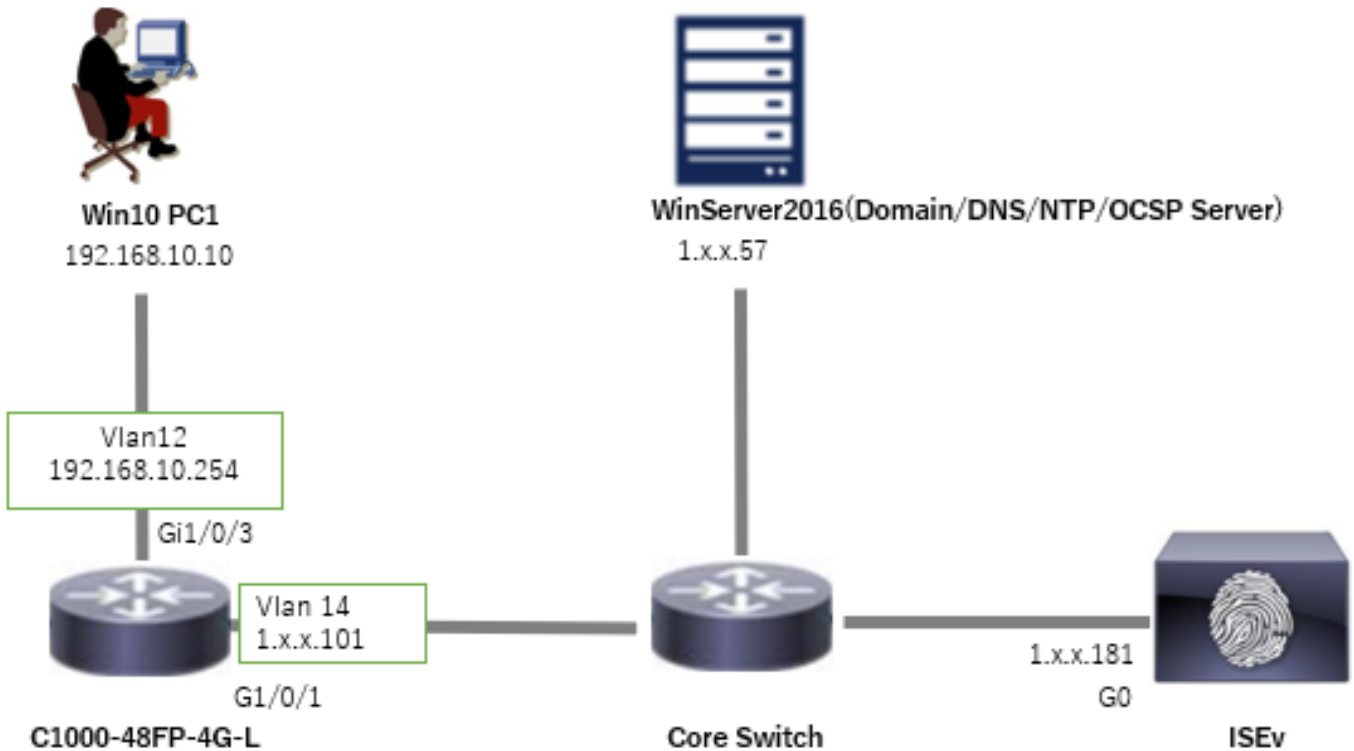
ةيلتال ةيداملا تانوكملا وجماربل تارادصإ يل دنن تسملا اذه يف ةدراولا تامولعمل دنن تست

- Identity Services Engine Virtual 3.2 Patch 6 جمانربلا
- C1000-48FP-4G-L 15.2(7)E9
- Windows Server 2016 ليغشتلا ماظن
- Windows 10 ليغشتلا ماظن

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجال نم دنن تسملا اذه يف ةدراولا تامولعمل عاشنإ مت تناك اذإ. (يضايرتفا) حوسمم نيوكتب دنن تسملا اذه يف ةمدختسملا ةزهجال عيمج تادب رمأ يال لمحتحمل ريثأتلل كمهف نم دكأتف، ليغشتلا ديقتك ككبش

ةكبشلل يطيختلا مسرلا

دنن تسملا اذه لاثمل همادختسا متي يذلا طاطخمل ةروصل اذه ضرعت



ةكبشلل يطيختلا مسرلا

ةيساسأ تامولعم

حضوي .ةقداصملا ةيلعم نم عزجك مداخللا ىلإ ةيمقرلا هتداهش ليمعلا مدقي ،EAP-TLS في ةحص نم ققحتلا قيرط نع ليمعلا ةداهش ةحص نم ققحتلاب ISE مايق ةيفيك دنتسمل اذه مادختساب ةداهشلا لاطبإ مت دق ناك اذا ام ديكأتو AD مداخل لباقم (CN) ةئاشلا ةداهشلا مسا تقولا في لوكوتوربلا ةلاح رفوي يذلاو ،(تنرتنإل ربع ةداهشلا ةلاح لوكوتورب) OCSP يلعفل.

م تي يذلاو ،ad.rem-xxx.com وه Windows Server 2016 ىلع هنوكت مت يذلا لاجملا مسا دنتسمل اذه في لاثمك همادختسإ.

AD (Active Directory) و (تنرتنإل ىلع ةداهشلا ةلاح لوكوتورب) OCSP مداخل مادختسإ متي ةداهشلا نم ققحتلل دنتسمل اذه في امهيا لراشملا.

- Active Directory FQDN: winserver.ad.rem-xxx.com
- CRL عيزوتب صاخلا URL ناو نع : <http://winserver.ad.rem-xxx.com/ocsp-ca.crl>
- عجرملا URL ناو نع : <http://winserver.ad.rem-xxx.com/ocsp>

دنتسمل في ةمدختسم ةداهش لك ةئاشلا مسالا اهل يتلا تاداهشلا ةلسلس يه هذو.

- ةئاشلا مسالا-OCSP-CA: أ ك
- ليمعلا ةداهش : clientcertCN
- مداخل ةداهش : ise32-01.ad.rem-xxx.com
- عيقوت ةداهش OCSP: ocspsigncommonname

تانويكتلا

C1000 في نيوكتلا

C1000 CLI في نيوكتلل ىندألا دحلا وه اذه.

```
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
```

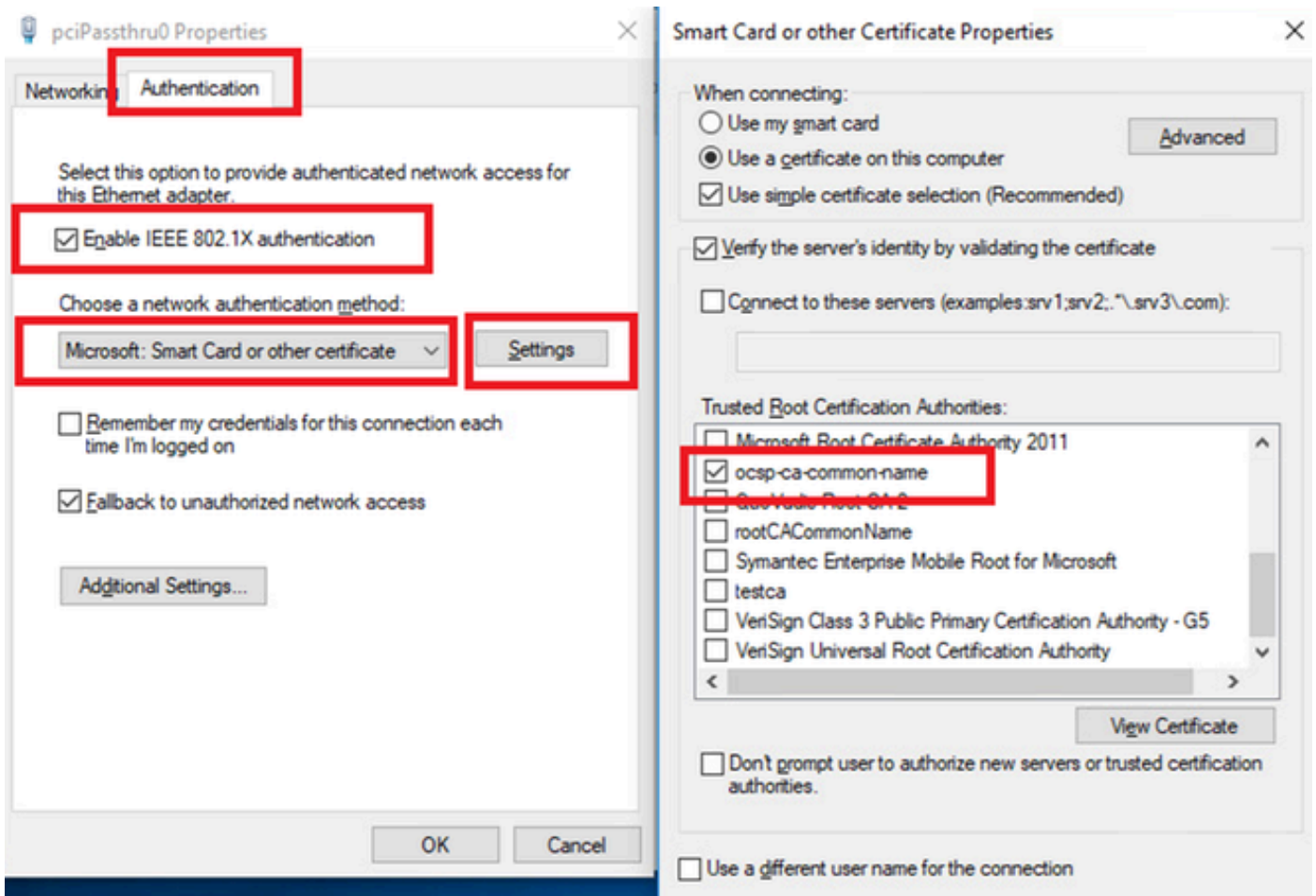
```
interface GigabitEthernet1/0/3
switchport access vlan 12
switchport mode access
authentication host-mode multi-auth
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge
```

Windows رتويبمك في نيوكتل

مدختسمل ةقداصم نيوكت 1. ةوطخل

ةقاطبلا Microsoft: ددحو IEEE 802.1X ةقداصم نيوكمت نم ققحت، ةقداصملا ىلى لقتنا ىرخأ ةداهش وأ ةيكذلا.

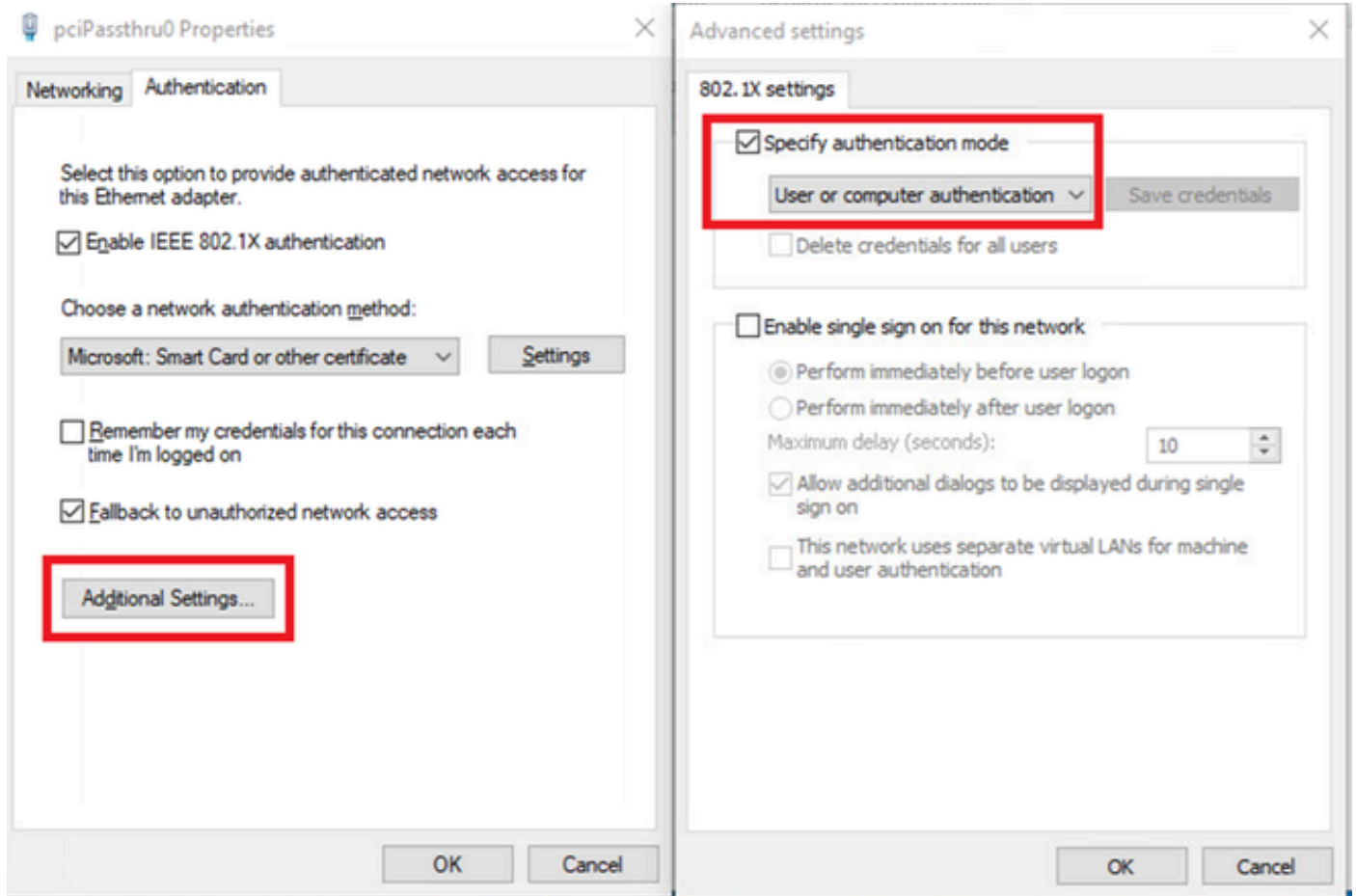
قدصملا عجرملا ددح م، رتويبمكلا اذه ىلع ةداهش مادختسا ددح م، Settingsbutton قوف رقتنا Windows رتويبمك زاهج هب قوئوملا.



ةداهشلا ةقداصم نيوكمت

نم رتويبمكلا وأ مدختسمل ةقداصم. ةيفاضلا تاداعلا نم ققحت، ةقداصملا ىلى لقتنا

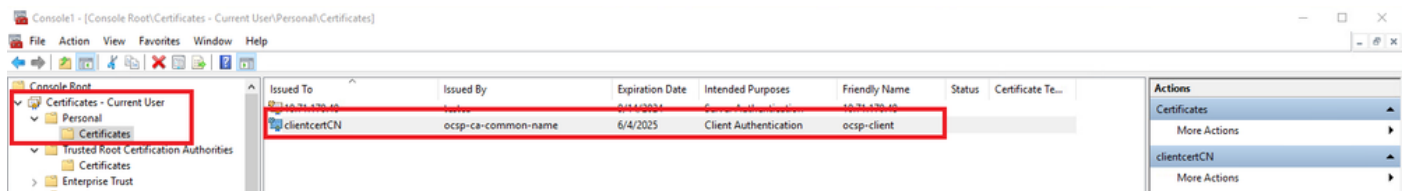
ةلدسنملا ةمئاقلا



ةقداصملا عضو دي دحت

لېمعل ةداهش ديكأت 2. ةوطخل

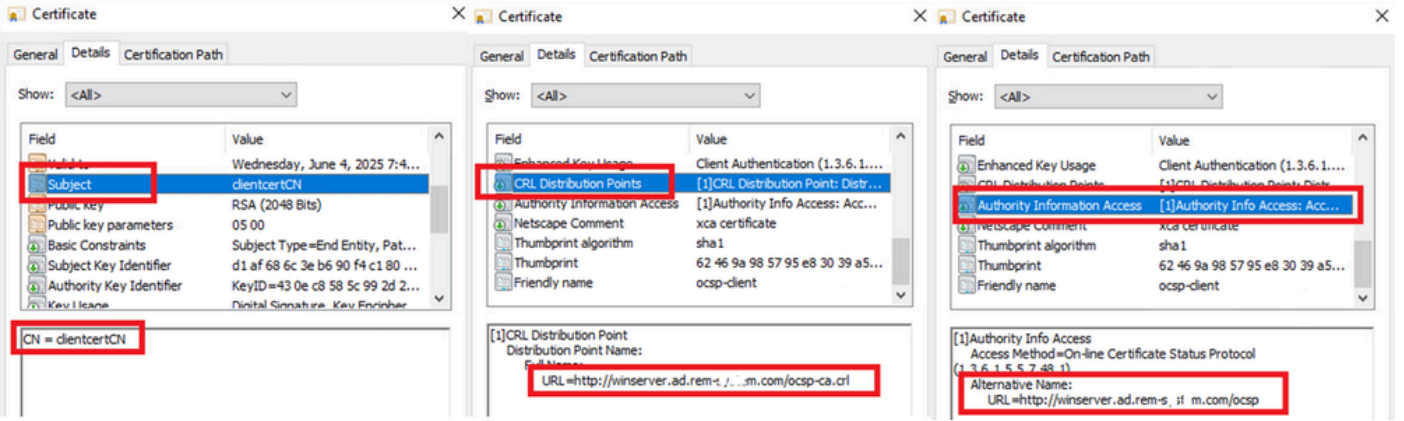
لېمعل ةداهش صحفو، تاداهش > يصخش > يلالحا مدختسملا - تاداهشلا ىل لقتنا ةقداصملا ةمدختسملا



لېمعل ةداهش ديكأت

لېصافات نم ققحت م، لېصافاتلا ىل لقتناو، لېمعل ةداهش قوف اجوزم ارقن رقن اعرجرملا تامولعم ىل لوصولاو، CRL عيزوت طاقن، عوضوملا

- عوضوملا: CN = clientcertCN
- عيزوت طاقن CRL: <http://winserver.ad.rem-xxx.com/ocsp-ca.crl>
- ةطالسلا تامولعم ىل لوصولو: <http://winserver.ad.rem-xxx.com/ocsp>

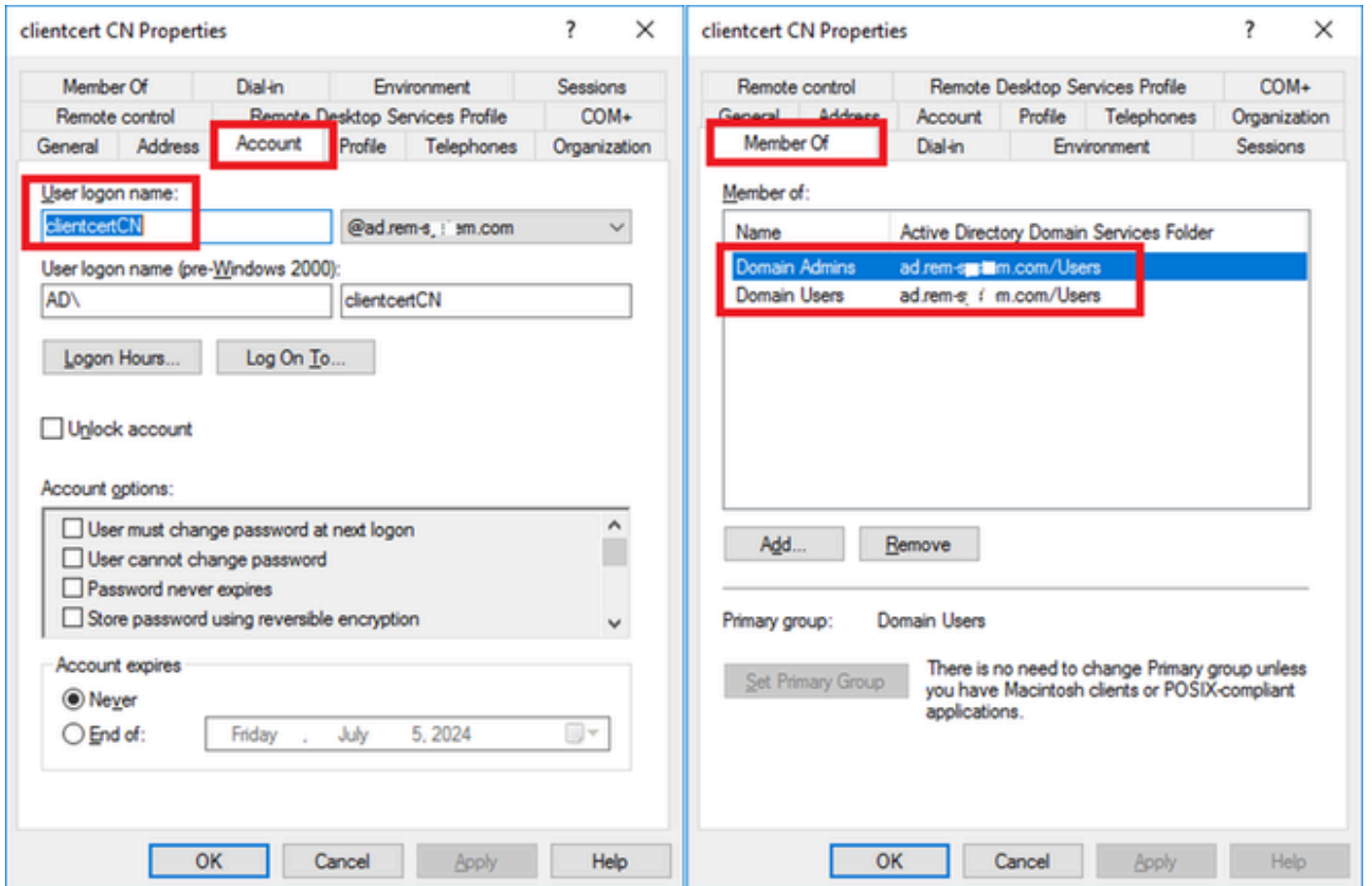


لي مدهاش لى صافات

Windows مداخل في نيوكتال

ني مدهاش لى صافات 1. ةوطخلا

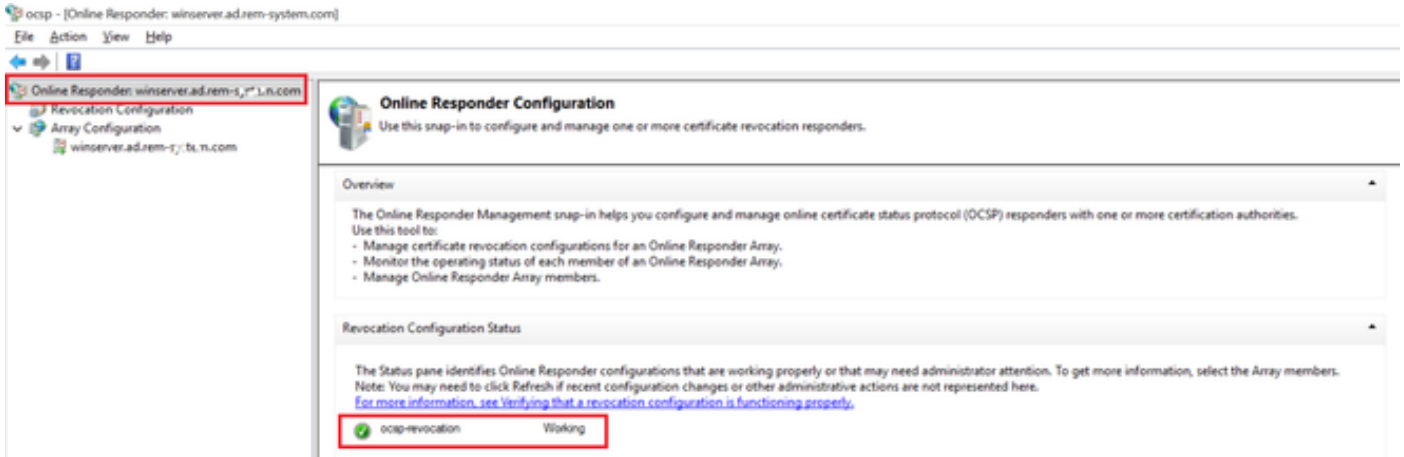
مدهاش لى صافات clientCERTcn ةفاضلا. Users قوف رونا، Active Directory Users and Computers لى لقتنا مدهاش لى صافات لى صافات مدهاش لى صافات.



مدهاش لى صافات لى صافات مدهاش لى صافات

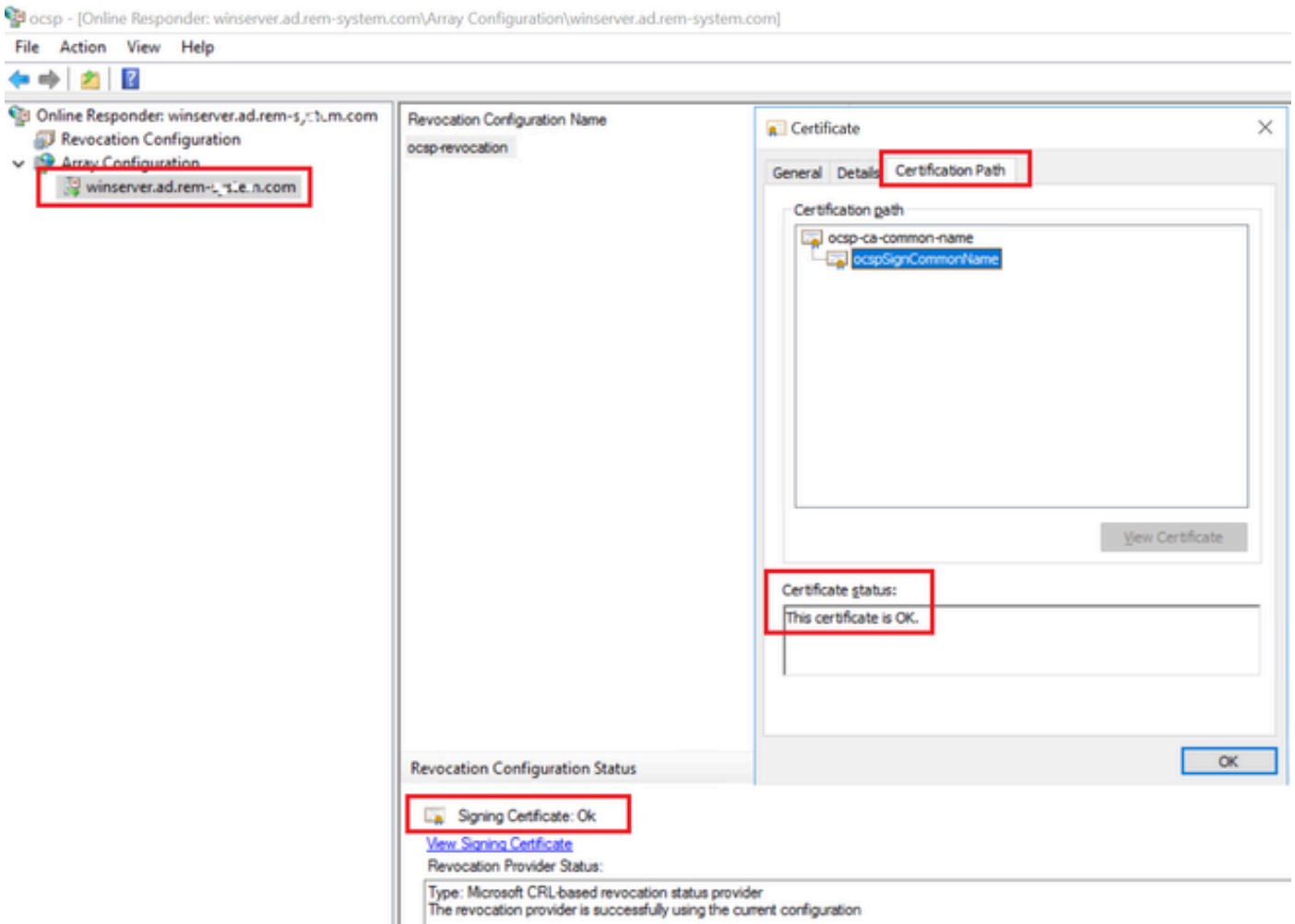
OCSP مدهاش لى صافات 2. ةوطخلا

OCSP مدهاش لى صافات ربع بي مدهاش لى صافات ةرادلا قوف رونا، Windows لى لقتنا



مداخ OCSP

OCSP عي قوت ةداهش ةلاح نم ققحت ، winserver.ad.rem-xxx.com رقن



OCSP عي قوت ةداهش ةلاح

ISE يف نيوكتلا

زاهج ةفاضلا 1 ةوطخلا

C1000 زاهج ةفاضلا رز ةفاضلا قوف رقن ، ةكبشلا ةزهج > ةرادلا ىلا لقتنا

Cisco ISE Administration - Network Resources

Network Devices | Network Device Groups | Network Device Profiles | External RADIUS Servers | RADIUS Server Sequences | NAC Managers | External MDM | pxGrid Direct Connectors | Location Services

Network Devices

Network Devices List > C1000

Network Devices

Name: C1000

Description:

IP Address: * IP: 1,1,1,1,101 / 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

زاهج ةفاضل

2. ةوطخلل Active Directory ةفاضل

Administration > Active Directory > ةيخراخلل ةيولل رءاصم > ConnectTab قوف رقنا، ISE ةفاضل مقو

- AD_JOIN_POINT ةطبرلل ةطقن مسا
- Active Directory ةمدخ لءام: ad.rem-xxx.com

Cisco ISE Administration - Identity Management

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

External Identity Sources

Active Directory

AD_Join_Point

LDAP

ODBC

RADIUS Token

RSA SecurID

SAML Id Providers

Social Login

Connection

* Join Point Name: AD_Join_Point

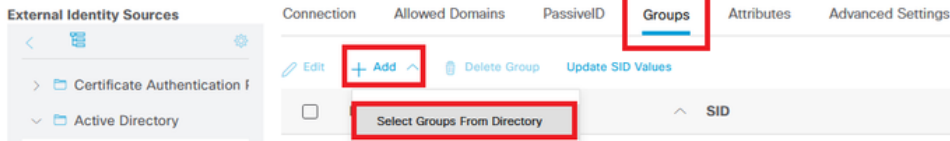
* Active Directory Domain: ad.rem-xxx.com

+ Join + Leave Test User Diagnostic Tool Refresh Table

<input type="checkbox"/>	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	winserv.ad.rem-s,ste...	Default-First-Site-Na...

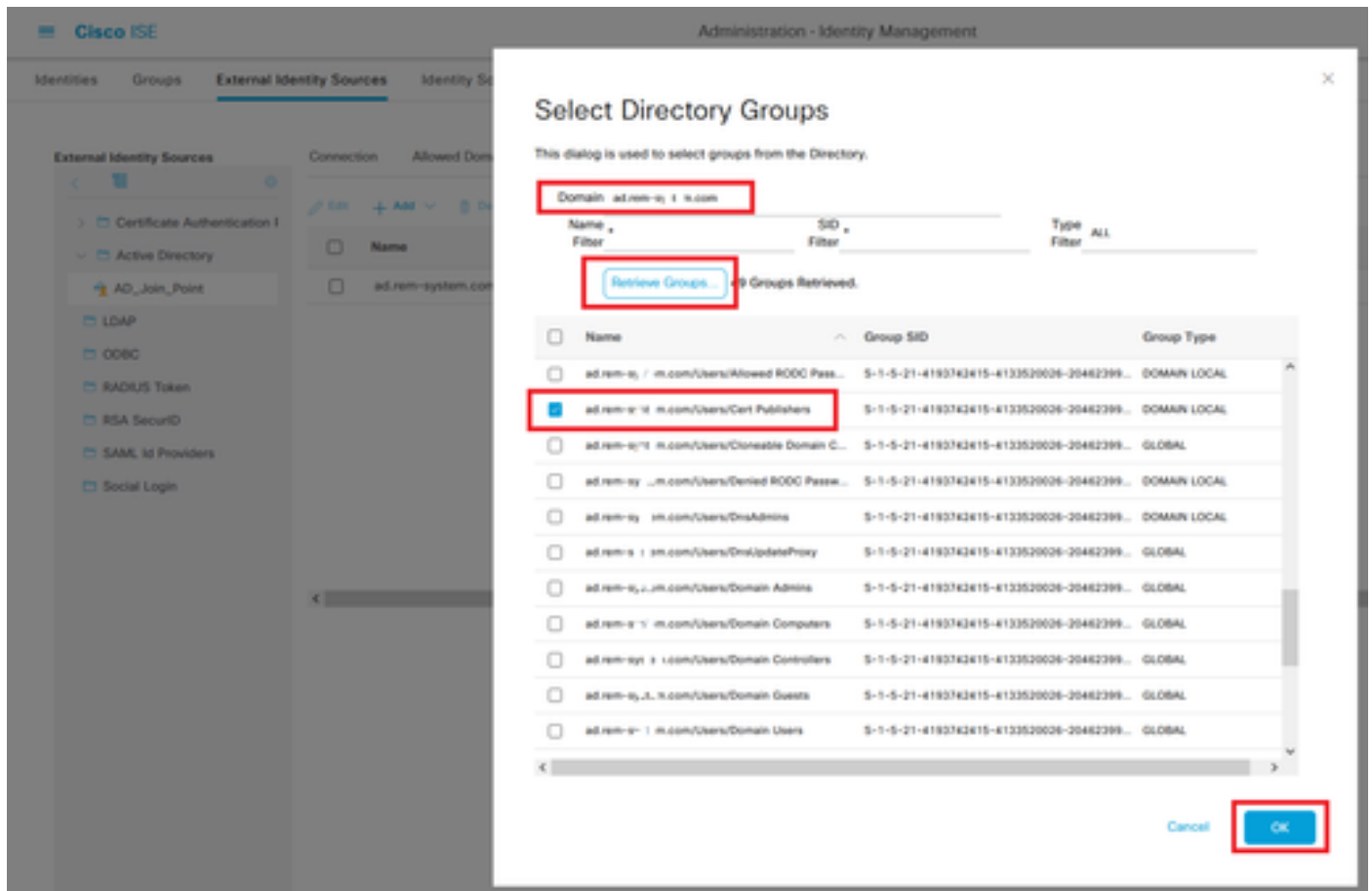
ةفاضل Active Directory

DirectFrom. ةلءسنملا ةمئائلل نم ةاعوومء دء، ةاعوومء بيوبتلل ةمءلل ةلءتن



ليدل نم تاعومجم ديدحت

ق ف ا و م ج م ل ا د ا ر ت س ا ق و ف ر ق ن ا . Checkad.rem-xxx.com/Users/Cert
ق ف ا و م ج م ل ا د ا ر ت س ا ق و ف ر ق ن ا و ن ي ر ش ا ن ل ل



CERT يرشان نم ققحتلا

ةداهشلا ققداصم فيرعت فلم ةفاضلا 3. ةوطخل

رزة ةفاضلا يلع رقنا، ةداهشلا ققداصم فيرعت فلم > ةيجراخ ةيوه رداصم > ةرادا يلا لقتنا
ديدج ةداهش ققداصم فيرعت فلم ةفاضلا

- مرسال: cert_authen_profile_test
- Identity Store: AD_JOIN_POINT
- عئاشلا مرسال - عوضوملا: ةداهشلا ةمس نم ةيوهلا مدختسا
- ةيوهلا ضومغ لحل طوق: تايوهلا نزخم يف ةداهشلا لباقم ليمعلا ةداهش ققباطم

External Identity Sources

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

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

Other options: Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only), Never, Always perform binary comparison

داهشلا ةقداصم فيرعت فلم ةفاض

ةيوهلا ردصم ةلسلس ةفاض. 4 ةوطخلا

ةيوه ردصم لسلس ةفاضاب مقو، ةيوهلا ردصم تالسلس ت > ةرادإ يلا لقتنا

- مسالا: Identity_AD
- Profile: cert_authen_profile_test داهشلا ةقداصم ددح
- ةقداصملا نع ثحبلا ةمئاق: 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

وهو ال ردصم تالسلست ةفاضل

ISE يف Confirم ةداهش 5. ةوطخلال

عجرمل لبق نم مداخل ةداهش عيقوت نم دكأت ،مظنل تاداهش > تاداهش > ةرادل لىل لقتنا ةقثال قدصم ل.

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 certificate - CN=SAML_Ise32-01.ad.rem-sy <input type="checkbox"/> CN=Ise32-01.ad.rem-sy <input type="checkbox"/> CN=Ise32-01.ad.rem-sy <input type="checkbox"/> CN=Ise32-01.ad.rem-sy <input type="checkbox"/> CN=Ise32-01.ad.rem-sy <input type="checkbox"/> Ise-server-cert-friendly-name 							

مداخل ةداهش

فلم ةفاضل ةفاضل رزقوف رقنا ، OCSP ليمع فيرعت فلم > تاداهش > ةرادل لىل لقتنا

ديج OCSP لي مع في رعت

- مسال: oosp_test_profile
- OCSP: <http://winserver.ad.rem-xxx.com/ocsp> بيجت سمل URL ناوع ني وكت

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 **oosp_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-1.s'am.com/ocsp**

Enable Nonce Extension Support
 Validate Response Signature

Secondary Server

URL **http://**

Enable Nonce Extension Support
 Validate Response Signature

Use OCSP URLs specified in Authority Information Access (AIA)

Enable Nonce Extension Support
 Validate Response Signature

Response Cache

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

Clear Cache

OCSP لي مع في رعت فلم

لي اداريت سا مت هب قو ووم CA نأ نم دكات ، اهب قو ووم تاداهش > تاداهش > قراد لي لقتنا ISE.

Cisco ISE Administration - System

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

Certificate Management

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

Certificate Authority

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

قوت قدصم عجم

نم ققحت لل OCSP ني وكت لي صافات لخدأو ، ريرت رز قوف رقناو قدصم لا عجم لا نم ققحت تاداهش لا ح.

- ققحت: لوصول ل لباق ريغ OCSP: oosp_test_profile
- ققحت: ةفورعم ريغ ةلأح اعجاراب OCSP ماق اذبا لطلالض فر
- ققحت: لوصول ل لباق ريغ OCSP بيحتسم ناك اذبا لطلالض فر

Cisco ISE Administration - System

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

Issuer

* Friendly Name oosp-ca-friendly-name

Status Enabled

Description

Subject CN=oosp-ca-common-name

Issuer CN=oosp-ca-common-name

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

Valid To (Expiration) Sun, 4 Jun 2024 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 oosp_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.

ةداهشلا ةلأح نم ققحتلا

اهب حومسملا تالوكوتوربلا ةفاضلا 6 ةوطخلا

لوصول ل ةمدخ ةمئاق ررحو، اهب حومسم تالوكوتورب > ةقداصم > جئاتن > ةسايس ل لقتنا
 EAP-TLS ب حامسلا ددح م، ةيضارتفالا ةكبشلا ل

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 ب ڄامس ل

ڄهن ٽو وڃي ٿو ٽي 7. ٽو وڃي ٿو

ڄهن ٽو وڃي ٿو ٽي 8. ٽو وڃي ٿو

- EAP-TLS-Test: ڄهن ٽو وڃي ٿو ٽي 9
- RADIUS واسي ٽي ٽو وڃي ٿو ٽي 10: ٽو وڃي ٿو
- ٽي ٽو وڃي ٿو ٽي 11: ٽو وڃي ٿو / ٽو وڃي ٿو ٽي 12

Cisco ISE Policy - Policy Sets

Policy Sets

Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
<input checked="" type="checkbox"/>	EAP-TLS-Test		Network Access-Protocol EQUALS RADIUS	Default Network Access	75		

ڄهن ٽو وڃي ٿو ٽي 13

ٽي ٽو وڃي ٿو ٽي 14. ٽو وڃي ٿو

ةقداصم ةسايس ةفاضلEAP-TLS-Testىلع رقنا ،جهنل اتاعومجم ىلإ لقتنا

- EAP-TLS ةقداصم :ةدعاقلا مسا
- EAP-TLS وWIRED_802.1 X ةكبشللا ىلإ لوصولل ةقداصم يواسن :طورشللا
- Identity_AD :مادختساللا



ةقداصملا جهن ةفاضلا

ليوختلا جهن ةفاضلا 9. ةوطخللا

ليوخت جهن ةفاضلEAP-TLS-Testقوف رقناو ،جهنل اتاعومجم ىلإ لقتنا

- EAP-TLS ضيوفت :ةدعاقلا مسا
- clientCN يواسي عئاشللا مسالا - ةداهشلا عوضوم :طورشللا
- PermitAccess :جئاتنللا



ليوختلا جهن ةفاضلا

ةحصللا نم ققحتلا

ةقداصملا لمع ةسلج ديكأت 1. ةوطخللا

C1000 ي ةقداصملا لمع ةسلج ديكأتل رمأل show authentication sessions interface GigabitEthernet1/0/3 details ليغش تب مق

<#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

Radius Live لجس دي كأت 2. ةوطخلال

لجس ل دي كأت ب مق ل ISE، ل (GUI) ةيموسر ل مدخت سمل ةه جاو يف رشابم ل لوخلال لجس ت > RADIUS > تاي لم عل ل ل لقتنا
ةق داصم ل طشن ل.

The screenshot shows the Cisco ISE Operations - RADIUS interface. At the top, there are several status indicators: Misconfigured Supplicants (0), Misconfigured Network Devices (0), RADIUS Drops (0), Client Stopped Responding (0), and Repeat Counter (0). Below these are controls for Refresh (Never), Show Latest 50 records, and Within Last 24 hours. A table of live logs is displayed below, with the following columns: Time, Status, Details, Repeats, Identity, Endpoint ID, Endpoint Pr, Authentication Policy, Authorization Policy, Authorizatio..., and IP Address. The table contains two rows of data, with the second row highlighted in red. The second row shows a successful session for clientcertCN on Jun 05, 2024 at 09:43:33.2, with endpoint ID B4:96:91:14:3... and IP address 192.168.10.10.

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint Pr	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...	●	🔒	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

لجس Radius Live

لص فم ل رشابم ل ةق داصم ل لجس دي كأت ب مق.

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-sy;.rem.com
AD-User-Candidate-Identities	clientcertCN@ad.rem-sy;.rem.com
TotalAuthenLatency	324
ClientLatency	80
AD-User-Resolved-DNs	CN=clientcert CN, CN=Users, DC=ad, DC=rem-sy;.rem.com
AD-User-DNS-Domain	ad.rem-sy;.rem.com
AD-User-NetBios-Name	AD
IsMachineIdentity	false
AD-User-SamAccount-Name	clientcertCN
AD-User-Qualified-Name	clientcertCN@ad.rem-sy;.rem.com
AD-User-SamAccount-Name	clientcertCN
AD-User-Qualified-Name	clientcertCN@ad.rem-sy;.rem.com
TLSCipher	ECDHE-RSA-AES256-GCM-SHA384
TLSVersion	TLSv1.2
DTLSSupport	Unknown
Subject	CN=clientcertCN
Issuer	CN=ocsp-ca-common-name

Steps

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

Crypto,2024-06-05 09:43:33,064,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, CryptoLib.CSSL.OCSP Callback -

starting OCSP request to primary

,SSL.cpp:1444

Crypto,2024-06-05 09:43:33,064,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, Crypto.OcspClient::pe

Start processing OCSP request

,

URL=<http://winserver.ad.rem-xxx.com/ocsp>

, use nonce=1,OcspClient.cpp:144

Crypto,2024-06-05 09:43:33,104,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, Crypto.OcspClient::pe

Received OCSP server response

,OcspClient.cpp:411

Crypto,2024-06-05 09:43:33,104,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, Crypto.OcspClient::pe

Crypto,2024-06-05 09:43:33,104,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, Crypto.OcspClient::pe

Crypto,2024-06-05 09:43:33,104,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, Crypto.OcspClient::pe

Crypto,2024-06-05 09:43:33,104,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, Crypto.OcspClient::pe

Crypto,2024-06-05 09:43:33,104,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, Crypto.OcspClient::pe

Crypto,2024-06-05 09:43:33,104,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, Crypto.OcspClient::pe

User certificate status: Good

,OcspClient.cpp:598

Crypto,2024-06-05 09:43:33,104,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, CryptoLib.CSSL.OCSP C

perform OCSP request succeeded

, status: Good,SSL.cpp:1684

// Radius session

Radius,2024-06-05 09:43:33,120,DEBUG,0x7f982d7b9700,cntx=0000017387,sesn=ise32-01/506864164/73,CPMSessi

Code=1(AccessRequest)

Identifier=238 Length=324

[1] User-Name - value: [

clientcertCN

]

[4] NAS-IP-Address - value: [1.x.x.101]

[5] NAS-Port - value: [50103]

[24] State - value: [37CPMSessionID=01C2006500000933E4E87D9;31SessionID=ise32-01/506864164/73;]

[87] NAS-Port-Id - value: [GigabitEthernet1/0/3]

Radius,2024-06-05 09:43:33,270,DEBUG,0x7f982d9ba700,cntx=0000017387,sesn=ise32-01/506864164/73,CPMSessi

Code=2(AccessAccept)

Identifier=238 Length=294

[1] User-Name - value: [clientcertCN]

Radius,2024-06-05 09:43:33,342,DEBUG,0x7f982d1b6700,cntx=0000017401,sesn=ise32-01/506864164/74,CPMSessi

Code=4(AccountingRequest)

Identifier=10 Length=286
 [1] User-Name - value: [clientcertCN]
 [4] NAS-IP-Address - value: [1.x.x.101]
 [5] NAS-Port - value: [50103]
 [40] Acct-Status-Type - value: [Interim-Update]
 [87] NAS-Port-Id - value: [GigabitEthernet1/0/3]
 [26] cisco-av-pair - value: [audit-session-id=01C20065000000933E4E87D9]
 [26] cisco-av-pair - value: [method=dot1x] ,RADIUSHandler.cpp:2455

Radius,2024-06-05 09:43:33,350,DEBUG,0x7f982e1be700,cntx=0000017401,sesn=ise32-01/506864164/74,CPMSessio

Code=5(AccountingResponse)

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

2. غيّر TCP

RADIUS لمعّ و OCSPP باجستسا لوح تام ولعم ىلع روثعلا عقوتت، ISE في TCP غيّر في لمع ي

هيلي دلل او OCSPP بلط :

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

ة باجستسال او OCSPP بلط ةمّح طاقثلا

```
> 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
```

ة باجستسال طاقثلا لي صافت OCSPP

RADIUS لمعّ ةسّج :

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

RADIUS ةسّج نمّ ةمّح طاقثلا

قلمص تاذا تام ولعم

[ISE مادختساب EAP-TLS ققداصم نيوكت](#)

[ISE يف TLS/SSL تاداهش نيوكت](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةللخت. فرتمة مچرت مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعلاء و
ىل إلمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةل صأل ةزىل ءن إلال دن تسمل