

# ةيوهلا تامدخ كرحم ىلع RADIUS DTLS نيوكت

## تايوتحمل

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[نيوكتلا](#)

[تاننيوكتلا](#)

[1. DTLS لوكوتورب نيوكمتو ISE ىلع ةكبش زاوج ةفاضا.](#)

[2. لومخلا ةلهمو DTLS ذفنم نيوكت.](#)

[3. ةقثلل ISE نزم نم DTLS RADIUS ةداهش رصم ريصت.](#)

[4. ق.دصملا ىلا ةداهشلا داريستساو ةقثلا ةطقن نيوكت.](#)

[5. لومخلا ةداهش ريصت.](#)

[6. ISE Trust Store نزم ىلا لومخلا ةداهش داريستسا.](#)

[7. لومخلا ىلع RADIUS نيوكتب مق.](#)

[8. ISE ىلع تاسايسلا نيوكت.](#)

[ةحصلا نم ق.قحتلا](#)

[اهحالص او ءاطخألا فاشكتسا](#)

[1. تابلط ي ISE ىقلى تي ال.](#)

[2. DTLS لاصلتا ديكأت لشف.](#)

## ةمدقملا

طاطخم ربع RADIUS ربع (DTLS) لقنلا ةقبط نام لوكوتورب نيوكت دنتسملا اذه حضوي RADIUS ل ريفشت تامدخ DTLS رفوت. اهحالص او لوكوتوربلا اذه ءاطخأ فاشكتساو تانايابل، نم آق فن ربع هلقن متي يذلاو.

## ةيساسألا تابلطتملا

### تابلطتملا

ةيلالل عيضاوملاب ةفرعم كيديل نوكت نأب Cisco ي صوت:

- Cisco (ISE) نم ةيوهلا تامدخ كرحم
- RADIUS لوكوتورب
- Cisco نم IOS

### ةمدختسملا تانوكملا

ةيلالل ةيداملا تانوكملا او جماربلا تارادصا ىلا دنتسملا اذه ي ف ةدراولا تامولعمل دنتست:

- Cisco Identity Services Engine، رادصلإل 2.2
- Catalyst 3650 عم IOS 16.6.1

ةصاخ ةي لم عم ةئيب ي ف ةدوجوملا ةزهجالا نم دنتسمل اذ ه ي ف ةدراول ا تامول عملا ءاشن ا مت تناك اذا .(يضا رتفا) حوسمم نيوك ت ب دنتسمل اذ ه ي ف ةمدختسمل ا ةزهجالا عيمج ت ادب رما يال لم تحملا ري ثاتلل كم ه ف نم دكات ف ، ةرشابم كتك ب ش

## نيوك تال

### تان نيوك تال

1. DTLS لوكوتورب نيكم متو ISE يل ع ةكبش زاه ةفاضا .

يل ع ةيمازل ا الوقح رف و ا ةفاضا قوف رونا . ةكبشلا ةزهجا > ةكبشلا دراوم > ةرادا يل ل لقتنا لقال :

- زاهجلل فولأم مسا ةفاضا متت - مسالا .
  - ةعومجم نيوك ت نكمملا نم . ISE ب لاصتال ق دصملا هم دختسي يذلا ، IP ناو نع - IP ناو نع (32 نم رغصأ) بسانملا عانقلا نييعت ب مق ، كلذ لمعل . ةزهجالا نم
  - متت ي تال الوكوتوربلا ديدحت ب حمسي وهو . زاهجلل ةماع تاداعا - زاهجالا في صوت نم ديزمل . RADIUS تامس نيوك ت و (CoA) لي وختلا تاداعا لصفم ريغت و اهتجال عم ةكبشلا ةزهجا تافي صوت > ةكبشلا دراوم > ةرادا يل ل لقتنا ، لي صافاتلا
  - ريغ دادعإل اذ ه . زاهجالا ع قوم و تاردقلا IPSec و ، زاهجالا عون نييعت - ةكبشلا ةزهجا ةعومجم . ةيضا رتفال ا تاداعال نوكت نأ ضررت في ، ةصصخم مي ق دحت مل اذا . يمازل ا
- DTLS رايتخال ا ةناخ دح RADIUS DTLS تاداعا تحت و RADIUS ةق داصم تاداعا رايتخال ا ةناخ دح ع برم نأ ظحال . نم آل ا DTLS ق فن ربع طقف ق دصملا عم RADIUS لاصتاب حمسي اذ ه و . ةبولطم متي و ةتبات RADIUS DTLS ةلاح ي ف ةميقل ا هذ ه نوكت . بترم كرتشملا يرسل ا ص نلا ق دصملا بناج يل ع ةلسلسلا س فن نيوك ت

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Ce

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Mana

Network devices

Default Device

Device Security Settings

Network Devices List > WLC\_3650

### Network Devices

\* Name

Description

\* IP Address:  /

\* Device Profile

Model Name

Software Version

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM

Network devices

Default Device

Device Security Settings

\* Network Device Group

Device Type

IPSEC

Location

RADIUS Authentication Settings

#### RADIUS UDP Settings

Protocol **RADIUS**

\* Shared Secret

CoA Port

#### RADIUS DTLS Settings

DTLS Required

Shared Secret

CoA Port

Issuer CA of ISE Certificates for CoA

#### General Settings

Enable KeyWrap

\* Key Encryption Key

\* Message Authenticator Code Key

Key Input Format  ASCII  HEXADECIMAL

## 2. لومخالا ةلهمو DTLS ذفنم نيوكت .

يف ةلهم لم اخولاصت DTLS ل تلمعتسا نوكي نأ ءانيملا تلكش عي طتسي تنأ

## RADIUS > RADIUS DTLS. > تالوكوتورب > دادع | ةيلمع > ماظن > ةراد

The screenshot shows the RADIUS DTLS configuration page in the Cisco ISE Administration console. The left sidebar contains navigation options like Client Provisioning, FIPS Mode, Alarm Settings, Posture, Profiling, Protocols (EAP-FAST, EAP-TLS, PEAP, EAP-TTLS, RADIUS), IPsec, Security Settings, Proxy, SMTP Server, and SMS Gateway. The main content area displays the following settings:

- Detection Interval: 5 (in minutes)
- Reporting Interval: 15 (in minutes)
- Reject RADIUS Requests:
- Failures prior to Rejection: 5 (valid range 2 to 100)
- Request Rejection Interval: 60 (in minutes)
- Suppress Repeated Successful Authentications:
- Accounting Suppression Interval: 5 (in seconds)
- Long Processing Step Threshold Interval: 1,000 (in milliseconds)
- Radius UDP ports**
  - \*Authentication Ports: 1812,1645
  - \*Accounting Ports: 1813,1646
- Radius DTLS**
  - \*Authentication & Accounting Ports: 2083
  - Idle Timeout: 60 (in second, valid range 60 to 600)

Buttons for Save, Reset, and Reset To Defaults are located at the bottom of the settings area.

اجوزاً RADIUS مدختسي، يضارتفا لكشبو. RADIUS ذفانم نع فلتخم DTLS ذفنم نأ طحال ليوختلاو ةقداصم ليل يضارتفا لكشبو DTLS مدختسي. 1812 و 1813 و 1645 و 1646 نم قداصم لاول ISE اهيف ظفاحي يتلا ةدملا لومخلا ةلهم ددحت. 2083 ذفنم ل CoA و ةب ساجم لاول ي ناوثلاب ةلهم ل هذه سايق متي. هلالخ نم رمي يلعل لاصتا ي نودب قفنلا يلعل ةيناث 600 لىإ 60 نم تاقاطن لاول.

### 3. ةقثلل ISE نزخم نم DTLS RADIUS ةداهش ردصم ريصدت.

ققحتلاو تاداهش لادابت لىل نيناكلا لكجاتحي، ةقداصم لاول ISE نيب قفنلا عاشن ل نوكي نأ بجي هرصدم نأ ينعي امم، ISE RADIUS DTLS ةداهش يف قداصم لاقثي نأ بجي. اهنم، تاداهش > ماظن > ةراد | لىل لقتنا، ISE ةداهش عقوم ريصدت. قداصم لاقثي نزخم يف ادوجوم ةروصل يف حضوم وه امك:

The screenshot shows the System Certificates page in the Cisco ISE Administration console. The left sidebar contains navigation options like Certificate Management, System Certificates, Trusted Certificates, OCSP Client Profile, Certificate Signing Requests, Certificate Periodic Check Sett..., and Certificate Authority. The main content area displays a table of system certificates:

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date
ISE22-1ek.example.com#Certificate Services Endpoint Sub CA - ISE22-1ek#00001	pxGrid		ISE22-1ek.example.com	Certificate Services Endpoint Sub CA - ISE22-1ek	Wed, 19 Oct 2016	Wed, 20 Oct 2021
ISE22-1ek.example.com,ISE22-1ek.example.com,*example.com#LAB CA#00002	EAP Authentication, Admin, Portal, RADIUS DTLS	Default Portal Certificate Group	ISE22-1ek.example.com	LAB CA	Mon, 31 Oct 2016	Wed, 31 Oct 2018
Default self-signed saml server certificate - CN=SAML_ISE22-1ek.example.com	SAML		SAML_ISE22-1ek.example.com	SAML_ISE22-1ek.example.com	Thu, 20 Oct 2016	Fri, 20 Oct 2017

هذه لىل قح لادصا نم ققحتو نيعم لاول RADIUS DTLS رود اهل يتلا ةداهش لاناك مدح مايقولل. ةقثلل ISE نزخم نم اهريصدت بجي يتلا ةداهش لىل ةداهش لىل مسالا وه اذه. ةداهش لىل

راجع رايته | ةناخ دح .اهب قووم تاداهش تاداهش تاداهش > ماظن > ةراد | ل لقتنا ،كلذب  
ريصت قوف رقتناو ةبسانملا ةداهشلا

#### 4. قوصملا ل ةداهشلا داريتساو ةقثلا ةطقن نيوكت .

لرم اوالا ذيفنتو لوجملا ل لوخدلا ليجستب مق ،TrustPoint نيوكتل

```
configure terminal
crypto pki trustpoint isetp
enrollment terminal
revocation-check none
exit
```

لوبق كنم بلطي ام دنع .crypto pki authentication isetp رمالا مادختساب ةداهش داريتسا  
م.معن بتكا ،ةداهشلا

```
Switch3650(config)#crypto pki authenticate isetp
```

```
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
```

```
-----BEGIN CERTIFICATE-----
MIIDWTCCAkGgAwIBAgIQI9s4RrhtWLPjJBYB5v0dtTANBgkqhkiG9w0BAQUFADA/
MRMwEQYKCZImiZPyLGBGRYDY29tMRcwFQYKCCZImiZPyLGBGRYHZZhhbXBsZTEP
MA0GA1UEAxMGTEFCIEBMB4XDTE1MDIxMjA3MzgxM1oXDTI1MDIxMjA3NDgxMlow
PzETMBEGCgmSJomT8ixkARkWA2NvbTEXMBUGCgmSJomT8ixkARkWB2V4Yw1wbGUx
DzANBgNVBAMTBkxkQjBDQTECCASIdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMDSfJwvbjLHHJf4vDTalGjKrDI73c/y269IMZV48xpCruNhg1cU8CW/T9Ysj6xk
Oogtx2vpG4XJt7KeBDZ/aclYmjg7sPBPCnyDZCd2a1b39XakD2puE81Vi4RVkjBH
pss2fTWeuor9dzb/kWb0YqIsgw1sRKQ2Veh1IXmuhX+wDqELHPIzgXn/DOBF0qN
vWlevrAlmBTxc04t1aPwyRk6b6ptjMeaIv2nqy8tOrldMVYKsPDj8aOrFEQ2d/wg
HDvd6C6LKRbpmAvtrqyDtineI/CraEFH7dZpvUSJBNUh7st3JIG8gVFstweoMmTE
zxUONQw8QrZmXDGTkgqvisECAwEAANRME8wCwYDVR0PBAQDAGGMA8GA1UdEwEB
/wQFMAMBAf8wHQYDVR0OBBYEF0TzYQ4kQ3fN6x6JzCit3/l0qoHMBAGCSsGAQQB
gjcVAQQDAGEAMA0GCSqGSIb3DQEBBQUAA4IBAQAwbWGBeqE2u6IGdKEPhv+t/rVi
xhn7KrEyWxLkWalSbU2ixsfTeJDCM8pxQItsj6B0Ey6A05c3YNcvW1iNpupGgc7v
9lmt4/TB6aRLVLi jBPB9/p2/3SjadCe/YBaOn/vpmfBPPPhUQVPiBM9fy/Al+zsh
t66bc03WcD8ZaKaER0oT8Pt/4GHZA0Unx+UxpcNuRRz4COArINXE0ULRfBxpIkkF
pWNjH0r1V55edOga0/r60Cg1/J9VAHh3qK2/3zXJE53N+A0h9whpG4LYgIFLB9ep
ZDim7KGsf+P3zk7SsKioGB4kqidHnm34XjlkWFnrCMQH4HC1oEymakV3Kq24
-----END CERTIFICATE-----
```

Certificate has the following attributes:

```
Fingerprint MD5: B33EAD49 87F18924 590616B9 C8880D9D
Fingerprint SHA1: FD729A3B B533726F F8450358 A2F7EB27 EC8A1178
```

```
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

#### 5. لوجملا ةداهش ريصت .

هريصتو لوجملا ل ةداهشلا DTLS ل امادختسا ل بولطملا ةداهشلاو TrustPoint دح

```
Switch3650(config)#crypto pki export TP-self-signed-721943660 pem terminal
% Self-signed CA certificate:
-----BEGIN CERTIFICATE-----
MIICKTCCAZKgwAwIBAgIBATANBgkqhkiG9w0BAQUFADAwMS4wLAYDVQQDEyVJTF1Mt
```

```

U2VsZi1TaWduZWQtQ2VydGhmaWNhdGUtNzIxOTQzNjYwMB4XDTE2MDQyNzExNDYw
Nl0XDTEwMDEwMTAwMDAwMFowMDEuMCwGA1UEAxM1SU9TLVNiYU21nbnVkbUN1
cnRpZmljYXR1LTcyMTk0MzY2MDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
xRybTGD526rPYuD2puMJU8ANcdQqNwunIERgvIWoLwBovuAu7WcRmzw1IDTDryOH
PXt1n5GcQSAOgn+9QdvKl1Z43ZkRWK5E7EGmjM/aL1287mg4/NlrWr4KMSwDQBJI
noJ52CABXUoApuiiJ8Ya4gOYeP0TmsZtxP1N+s+wqjMCAwEAaANTMFEwDwYDVR0T
AQH/BAUwAwEB/zAfBgNVHSMEGDAwGtBSEOKlAPAHBPedwichXL+qUM+lrITAdBgNV
HQ4EFgQUhDipQDwBwT3ncInIVy/q1DPta4kwdQYJKoZIhvcNAQEFBQADgYEA1BNN
wKSS8yBuOH0/jUV7sy3Y9/oV7Z9bW8WfV9QiTQ11ZelvwMTbewozwX2LJvxobGcj
Pi+n99RIH8dBhWwoY19GTN2LVI22GIPX12jNLqps+Mq/u2qxVm0964SaJs501KjQ
69XFfCVot1NA6z2eEP/69oL9x0uaJDZa+6ileh0=
-----END CERTIFICATE-----

```

يُظهر `show crypto pki trustPoints` رموز الأمان التي تم تثبيتها في جهازك، وهي موزعة على عدة مستويات. يمكنك رؤية هذه المستويات في قائمة `show crypto pki trustPoints`.  
 يُلحظ أن هذه المستويات هي `TrustPoint`، وهي موزعة على عدة مستويات. يمكنك رؤية هذه المستويات في قائمة `show crypto pki trustPoints`.

## 6. إعداد ISE Trust Store لإدارة الشهادات.

يُعد إعداد Trust Store في ISE خطوة هامة في إعداد النظام. يمكنك رؤية الخطوات في الفيديو التالي.

تُعد إعداد Trust Store في ISE خطوة هامة في إعداد النظام. يمكنك رؤية الخطوات في الفيديو التالي. يُعد إعداد Trust Store في ISE خطوة هامة في إعداد النظام. يمكنك رؤية الخطوات في الفيديو التالي.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The main navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The left sidebar shows 'Certificate Management' with options like 'System Certificates', 'Trusted Certificates', 'OCSP Client Profile', 'Certificate Signing Requests', and 'Certificate Periodic Check Settings'. The main content area is titled 'Import a new Certificate into the Certificate Store'. It includes a 'Certificate File' field with a 'Browse...' button and the value 'sw.pem'. The 'Friendly Name' field contains 'Switch3650'. Under 'Trusted For', there are four checkboxes: 'Trust for authentication within ISE' (checked), 'Trust for client authentication and Syslog' (checked), 'Trust for authentication of Cisco Services' (unchecked), and 'Validate Certificate Extensions' (unchecked). There is also a 'Description' field and 'Submit' and 'Cancel' buttons at the bottom.

## 7. إعداد RADIUS في ISE.

يُعد إعداد RADIUS في ISE خطوة هامة في إعداد النظام. يمكنك رؤية الخطوات في الفيديو التالي. يُعد إعداد RADIUS في ISE خطوة هامة في إعداد النظام. يمكنك رؤية الخطوات في الفيديو التالي.

```

radius server ISE22
address ipv4 10.48.23.86
key radius/dtls
dtls port 2083

```

```
dtls trustpoint client TP-self-signed-721943660
dtls trustpoint server isetp
```

كتابلطتم ىل ع (AAA) ةبساحملاو ضيوفتلاو ةقداصملا ةصاخلا ةئيهتلا ةيقب دمتعت  
لاثمك نيوكتلا اذ عم لماعت .كميمصتو

```
aaa group server radius ISE
server name ISE22
```

```
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
```

```
aaa authentication dot1x default group ISE
aaa authorization network default group ISE
```

## 8. ISE ىل ع تاسايسلا نيوكت .

كميمصت ىل ع ةوطخلال هذه دمتعت . ISE ىل ع ضيوفتلاو ةقداصملا تاسايس نيوكت ب مق  
اضيا كتابلطتمو .

## ةحصلا نم ققحتلا

لوحمل ىل ع **test aaa** رمأل مدختسأ ، ني مدختسملا ةقداصم ةئيناك نم ققحتلل

```
Switch3650#test aaa group ISE alice Krakow123 new-code
User successfully authenticated
```

USER ATTRIBUTES

```
username 0 "alice"
Switch3650#
```

ISE > RADIUS > LiveLog تاي لمع ىل لقتنا . حاجنب ةلاسرلا مدختسم ةقداصم ىرت نأ بجي  
(ةربكم ةسدع ىل ع رقنا) بسانملا لجسلل ليصافتلا دحو:

Time	Status	Details	Repeat ...	Identity	Endpoint ID
Jan 25, 2017 07:55:49.801 PM	Success			alice	00:50:56:A5:13:0D

**Overview**

Event	5200 Authentication succeeded
Username	alice
Endpoint Id	
Endpoint Profile	
Authentication Policy	Default >> Default >> Default
Authorization Policy	Default >> Basic_Authenticated_Access
Authorization Result	PermitAccess

**Authentication Details**

Source Timestamp	2017-01-25 18:19:24.672
Received Timestamp	2017-01-25 18:19:24.673
Policy Server	ISE22-1ek
Event	5200 Authentication succeeded
Username	alice
User Type	User
Authentication Identity Store	Internal Users

**Steps**

- 91055 RADIUS packet is encrypted
- 11001 Received RADIUS Access-Request
- 11017 RADIUS created a new session
- 11117 Generated a new session ID
- 15049 Evaluating Policy Group
- 15008 Evaluating Service Selection Policy
- 15048 Queried PIP - Normalised Radius.RadiusFlowType (4 times)
- 15006 Matched Default Rule
- 15041 Evaluating Identity Policy
- 15006 Matched Default Rule
- 15013 Selected Identity Source - Internal Users
- 24210 Looking up User in Internal Users IDStore - alice
- 24212 Found User in Internal Users IDStore
- 22037 Authentication Passed
- 15036 Evaluating Authorization Policy
- 15048 Queried PIP - DEVICE.IPSEC
- 15048 Queried PIP - Threat.Rapid7 Nexpose-CVSS\_Base\_Score
- 15048 Queried PIP - Network Access.UseCase
- 15048 Queried PIP - Normalised Radius.RadiusFlowType (2 times)
- 15048 Queried PIP - Network Access.AuthenticationStatus
- 15004 Matched rule - Basic\_Authenticated\_Access
- 15016 Selected Authorization Profile - PermitAccess
- 22080 New accounting session created in Session cache
- 11002 Returned RADIUS Access-Accept

في الواجهة ووسطها نأ ن م ق قحت . تاوطلاب ةمئاق دجوت ، ريرقت ال ن م ن م ي ال بناجل ال عو RADIUS ةم زح ريفشت يه ةمئاق ال

يرخأ ةرم aaa رابتلخال رما ذيفنتو ISE ال ةمزحل طاقتل ادب كنكمي ، كلذ ال ةفاضل ابو > صيخشتل تاودأ > اهالصل او اطلخال فاشكتسا > تايلمعل ال ال لقتنا ، طاقتل ال ادبل : ادب قوف رقناو ةقداصل لل ةمدختس مل جهنل ال ةمدخ ةدقع دح . TCP غيرفت > ةماع تاودأ



General Tools

- RADIUS Authentication Trouble...
- Execute Network Device Comm...
- Evaluate Configuration Validator
- Posture Troubleshooting
- EndPoint Debug
- TCP Dump
- Session Trace Test Cases

TrustSec Tools

## TCP Dump

Monitor the packet headers on the network and save to a file (up to 5 Minutes)

Status ■ Stopped

Host Name

Network Interface

Promiscuous Mode  On  Off

Filter

Example: 'ip host helios and not iceberg'

Format

**Dump File** Last created on Wed Jan 25 18:25:43 CET 2017  
 File size: 212,627 bytes  
 Format: Raw Packet Data  
 Host Name: ISE22-1ek  
 Network Interface: GigabitEthernet 0  
 Promiscuous Mode: On

أرداق نوكت نأ بجي ،مزلحلا طاقتلا حتف دنع .لليزنتو فاقلي| لىل رقنا ،ةقداصملا ءاهتنا دنع  
 DTLS: مادختساب ةرفشم رورملا ةكرح ةيؤر لىل

813	2017-01-25	18:19:20.699601	10.229.20.241	10.48.23.86	DTLSv1.2	180 Client Hello
815	2017-01-25	18:19:20.702006	10.48.23.86	10.229.20.241	DTLSv1.2	1311 Server Hello, Certificate (Fragment), Certificate (...)
816	2017-01-25	18:19:20.750480	10.229.20.241	10.48.23.86	DTLSv1.2	270 Certificate (Fragment)
817	2017-01-25	18:19:20.750604	10.229.20.241	10.48.23.86	DTLSv1.2	270 Certificate (Fragment)
818	2017-01-25	18:19:20.755830	10.229.20.241	10.48.23.86	DTLSv1.2	270 Certificate (Reassembled), Client Key Exchange (Fra...
819	2017-01-25	18:19:20.756049	10.229.20.241	10.48.23.86	DTLSv1.2	270 Client Key Exchange (Fragment)
820	2017-01-25	18:19:20.777474	10.229.20.241	10.48.23.86	DTLSv1.2	258 Client Key Exchange (Reassembled), Certificate Veri...
821	2017-01-25	18:19:20.779217	10.229.20.241	10.48.23.86	DTLSv1.2	133 Change Cipher Spec, Encrypted Handshake Message
822	2017-01-25	18:19:20.794575	10.48.23.86	10.229.20.241	DTLSv1.2	133 Change Cipher Spec, Encrypted Handshake Message
823	2017-01-25	18:19:20.830404	10.229.20.241	10.48.23.86	DTLSv1.2	151 Application Data
824	2017-01-25	18:19:20.880231	10.48.23.86	10.229.20.241	DTLSv1.2	279 Application Data
832	2017-01-25	18:19:23.646428	10.229.20.241	10.48.23.86	DTLSv1.2	151 Application Data
833	2017-01-25	18:19:23.693076	10.48.23.86	10.229.20.241	DTLSv1.2	279 Application Data
834	2017-01-25	18:19:24.622672	10.229.20.241	10.48.23.86	DTLSv1.2	151 Application Data
835	2017-01-25	18:19:24.674113	10.48.23.86	10.229.20.241	DTLSv1.2	279 Application Data

ةحفاصملا لوح ضوافتلا متي ام دنع . DTLS لاصتلا ديكتأ نم عزج يه 822 مقر - #813 مزلحلا  
 لىل بس لىل فقوتيو فلتخي دق مزلحلا ددع نأ طحلال . قىبطتلا تانايب لقن متي ،حاجناب  
 ريفشت متي . (X، |، EAP-TLS، EAP-PEAP، PAP) ةمدختسمل ةقداصملا ةقيرط لىل لاثمل  
 ةمزلح لك تايوتحم:

822	2017-01-25	18:19:20.794575	10.48.23.86	10.229.20.241	DTLSv1.2	133 Change Cipher Spec, Encrypted Handshake Message
823	2017-01-25	18:19:20.830404	10.229.20.241	10.48.23.86	DTLSv1.2	151 Application Data

▶ Frame 823: 151 bytes on wire (1208 bits), 151 bytes captured (1208 bits)  
 ▶ Ethernet II, Src: CiscoInc\_1c:e8:00 (00:07:4f:1c:e8:00), Dst: Vmware\_99:64:0c (00:50:56:99:64:0c)  
 ▶ Internet Protocol Version 4, Src: 10.229.20.241, Dst: 10.48.23.86  
 ▶ User Datagram Protocol, Src Port: 51598 (51598), Dst Port: 2083 (2083)  
 ▼ Datagram Transport Layer Security  
 ▼ DTLSv1.2 Record Layer: Application Data Protocol: Application Data  
 Content Type: Application Data (23)  
 Version: DTLS 1.2 (0xfefd)  
 Epoch: 1  
 Sequence Number: 1  
 Length: 96  
 Encrypted Application Data: 8d83ddac8b027b5a5f9e355243b0f9155680d2a933c09635...

لىل ءهنيوكت متي يتلا IdleTimeout ددحت .اروف قفنلا عطقني ال ،تانايبلا لك لقنت ام دنعو  
 تقوؤملا ةيجالصة تهتنا اذا .هلخال رمي لاصتلا نود قفن ءاشنإ هلخال نكمي يتلا ءدملا ISE  
 قفنلا ءاشنإ ءداعو DTLS ءحفاصم ءارج متي ،ISE لىل ديدجلا لوصول بلط لاسررا نيغتو

# اهحال صإو ءاطخأل فاشكسا

## 1. تابلط يإ ISE ىقلتي ال

و 1645،1646 يه ءيضا رت فالإ RADIUS ذفانم 2083. وه يضا رت فالإ DTLS ذفنم نأ طحال UDP/2083 رورم ءكرح عنمي ال ءيماحلل راج نأ نم دكأت 1812،1813.

## 2. DTLS لاصتا ديكأت لشف

تلشف DTLS ءحفاصم نأ ىرت دق ISE نع يلي صفتللا ريرقتللا ي:

Overview	
Event	5450 RADIUS DTLS handshake failed
Username	
Endpoint Id	
Endpoint Profile	
Authorization Result	

### Steps

91030	RADIUS DTLS handshake started
91031	RADIUS DTLS: received client hello message
91032	RADIUS DTLS: sent server hello message
91033	RADIUS DTLS: sent server certificate
91034	RADIUS DTLS: sent client certificate request
91035	RADIUS DTLS: sent server done message
91036	RADIUS DTLS: received client certificate

Authentication Details	
Source Timestamp	2017-01-25 16:15:36.092
Received Timestamp	2017-01-25 16:15:36.094
Policy Server	ISE22-1ek
Event	5450 RADIUS DTLS handshake failed
NAS IPv4 Address	10.229.20.241

ققحت ءحفاصملا ءانثأ ءلسررملا ءداهشلا ي قثي ال ISE وأ لوحملا نأ وه لم تحملا ببسلا ISE ىل ءحفاصملا RADIUS DTLS روجل ءبسانملا ءداهشلا نبيعت نم ققحت. ءداهشلا نبيكت نم لوحملا ىل ءحفاصملا ءداهشلا نبيعت نم ققحت. ءداهشلا نبيكت نم ققحت. ءداهشلا نبيكت نم ققحت.

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 لاعل او  
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco  
Systems (رفوتم طبارل) ةل صأل ةل ءل ءن إل دن تسمل