

# Configurare DTLS RADIUS su Identity Services Engine

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Configurazioni](#)

[1. Aggiungere un dispositivo di rete ad ISE e abilitare il protocollo DTLS.](#)

[2. Configurare la porta DTLS e il timeout di inattività.](#)

[3. Esportare l'autorità emittente del certificato RADIUS DTLS dall'archivio certificati ISE.](#)

[4. Configurare il trust point e importare il certificato nell'autenticatore.](#)

[5. Esportare il certificato dello switch.](#)

[6. Importare il certificato dello switch nell'archivio di attendibilità ISE.](#)

[7. Configurare RADIUS sullo switch.](#)

[8. Configurare le policy su ISE.](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[1. ISE non riceve richieste.](#)

[2. Handshake DTLS non riuscito.](#)

## Introduzione

In questo documento viene descritta la configurazione e la risoluzione dei problemi di RADIUS su DTLS (Datagram Transport Layer Security Protocol). DTLS fornisce servizi di crittografia per RADIUS, che viene trasportato su un tunnel sicuro.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Identity Services Engine (ISE)
- protocollo RADIUS
- Cisco IOS

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e

hardware:

- Cisco Identity Services Engine 2.2
- Catalyst 3650 con IOS 16.6.1

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Configurazione

### Configurazioni

#### 1. Aggiungere un dispositivo di rete ad ISE e abilitare il protocollo DTLS.

Selezionare **Amministrazione > Risorse di rete > Dispositivi di rete**. Fare clic su **Add (Aggiungi)** e fornire almeno i campi obbligatori:

- **Name** - Viene aggiunto un nome descrittivo del dispositivo.
- **Indirizzo IP** - Indirizzo IP utilizzato dall'autenticatore per contattare ISE. È possibile configurare una serie di dispositivi. A tal fine, specificare la maschera corretta (inferiore a 32).
- **Profilo dispositivo** - Impostazioni generali del dispositivo. Consente di specificare i protocolli da gestire, le impostazioni CoA (Change of Authorization) dettagliate e la configurazione degli attributi Radius. Per ulteriori informazioni, selezionare **Amministrazione > Risorse di rete > Profili dispositivi di rete**.
- **Gruppo dispositivi di rete** - Impostare il tipo di dispositivo, IPsec le funzionalità e il percorso del dispositivo. Questa impostazione non è obbligatoria. Se non si selezionano valori personalizzati, vengono utilizzate le impostazioni predefinite.

Selezionare la casella di controllo **RADIUS Authentication Settings** e in **RADIUS DTLS Settings** selezionare la casella di controllo **DTLS Required**. Ciò consente la comunicazione RADIUS con l'autenticatore solo tramite il tunnel protetto DTLS. Si noti che la casella di testo **Segreto condiviso** è disattivata. Questo valore in caso di DTLS RADIUS è fisso e la stessa stringa è configurata sul lato autenticatore.

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  Cisco

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. Configurare la porta DTLS e il timeout di inattività.

È possibile configurare la porta utilizzata per la comunicazione DTLS e il timeout di inattività in

## Amministrazione > Sistema > Impostazioni > Protocolli > RADIUS > DTLS RADIUS.

The screenshot shows the configuration page for RADIUS DTLS in the Cisco Identity Services Engine. 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 is divided into sections: Detection Interval (5 minutes), Reporting Interval (15 minutes), Reject RADIUS Requests (checked), Failures prior to Rejection (5, valid range 2 to 100), Request Rejection Interval (60 minutes), Suppress Repeated Successful Authentications (unchecked), Accounting Suppression Interval (5 seconds), Long Processing Step Threshold Interval (1,000 milliseconds), Radius UDP ports (\*Authentication Ports: 1812,1645; \*Accounting Ports: 1813,1646), and Radius DTLS (\*Authentication & Accounting Ports: 2083; Idle Timeout: 60 seconds, valid range 60 to 600). At the bottom, there are buttons for Save, Reset, and Reset To Defaults.

Si noti che la porta DTLS è diversa dalle porte RADIUS. Per default, un raggio utilizza le coppie 1645, 1646 e 1812, 1813. Per impostazione predefinita, DTLS per autenticazione, autorizzazione, accounting e CoA utilizza la porta 2083. **Idle Timeout** specifica per quanto tempo ISE e l'autenticatore mantengono il tunnel senza che vi sia alcuna comunicazione effettiva. Questo timeout è misurato in secondi e varia da 60 a 600 secondi.

### 3. Esportare l'autorità emittente del certificato RADIUS DTLS dall'archivio certificati ISE.

Per stabilire il tunnel tra ISE e l'autenticatore, entrambe le entità devono scambiarsi e verificare i certificati. L'autenticatore deve considerare attendibile il certificato DTLS ISE RADIUS, pertanto l'autorità emittente deve essere presente nell'archivio di attendibilità dell'autenticatore. Per esportare il firmatario del certificato ISE, selezionare **Amministrazione > Sistema > Certificati**, come mostrato nell'immagine:

The screenshot shows the Certificate Management page in the Cisco Identity Services Engine. The left sidebar contains navigation options like Certificate Management, System Certificates, Trusted Certificates, OSCP Client Profile, Certificate Signing Requests, Certificate Periodic Check Setti..., and Certificate Authority. The main content area shows a table of System Certificates. The table has columns for Friendly Name, Used By, Portal group tag, Issued To, Issued By, Valid From, and Expiration Date. The table contains three rows of certificates, each with a checkbox for selection and a green checkmark in the Expiration Date column.

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 (i)	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

Individuare il certificato a cui è assegnato il ruolo DTLS RADIUS e controllare il campo **Rilasciato**

da per questo certificato. Questo è il nome comune del certificato che deve essere esportato dall'ISE Trust Store. A tale scopo, selezionare **Amministrazione > Sistema > Certificati**. Selezionare la casella di controllo accanto al certificato appropriato e fare clic su **Esporta**.

#### 4. Configurare il trust point e importare il certificato nell'autenticatore.

Per configurare un trustpoint, accedere allo switch ed eseguire i comandi:

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

Importare il certificato con il comando **crypto pki authentication isetp**. Quando viene richiesto di accettare il certificato, digitare **yes**.

```
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-----
MIIDWTCCAkgAwIBAgIQ9s4RrhtWlpJjBYB5v0dtTANBgkqhkiG9w0BAQUFADA/
MRMwEQYKZCIImiZPyLGQBGRYDY29tMRcwFQYKZCIImiZPyLGQBGRYHZAjEjMjE1
MA0GA1UEAxMGTGF1eWVhbnR1eWVhbnR1eWVhbnR1eWVhbnR1eWVhbnR1eWVhbnR1
PzETMBEGCgmSJomT8ixkARkWA2NvbWVhbnR1eWVhbnR1eWVhbnR1eWVhbnR1eWVh
DzANBgNVBAMTBkx1eWVhbnR1eWVhbnR1eWVhbnR1eWVhbnR1eWVhbnR1eWVhbnR1
AMDSfJwvbjLHhJf4vDTalGjKrdI73c/y269IMZV48xpCruNhglcU8CW/T9Ysj6xk
Oogtx2vpG4XJt7KebDZ/ac1Ymjg7sPBPCnyDZCd2a1b39XakD2puE81Vi4RVkjBH
pss2fTWeuor9dzgb/kWb0YqIsgw1sRKQ2Veh1IXmuhX+wDqELHPIzgXn/DOBF0qN
vWlevrAlmBTxC04t1aPwyRk6b6ptjMeaIv2nqy8tOrldMVYKsPDj8aOrFEQ2d/wg
HDvd6C6LKRbpmAvtrqyDtInEl/CRAEFH7dZpVUSJBnuh7st3JIG8gVFstweoMmTE
zxUONQw8QrZmXDGTGqgqvisECAAEEAAaNRME8wCwYDVR0PBAQDAgGMA8GA1UdEwEB
/wQFMAMBAf8wHQYDVR0OBBYEF00TzYQ4kQ3fN6x6JzCit3/l0qoHMBAGCSsGAQQB
gjcVAQQDAgEAMA0GCSqSIB3DQEBBQUAA4IBAQAwbWGBeqE2u6IGdKEPhv+t/rVi
xhn7KrEyWxLkWaLsbU2ixsfTeJDCM8pxQIItsj6B0Ey6A05c3YNcvWlinPupGgc7v
91Mt4/TB6aRLVLIjBPB9/p2/3SJadCe/YBaOn/vpmfBPPPhxUQVPIBM9fy/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. Esportare il certificato dello switch.

Selezionare il trust point e il certificato da utilizzare per DTLS sullo switch ed esportarlo:

```
Switch3650(config)#crypto pki export TP-self-signed-721943660 pem terminal
```

```
% Self-signed CA certificate:
-----BEGIN CERTIFICATE-----
MIICKTCCAZKgAwIBAgIBATANBgkqhkiG9w0BAQUFADAwMS4wLAYDVQQDEyVJT1Mt
U2VsZi1TaWduZWQtQ2VydGlmYWVhdGUtNzIxOTQzNjYwMB4XDTE2MDQyNzExNDYw
Nl0XDTIwMDEwMTAwMDAwMFowMDEuMCA1UEAxM1SU9TLVNlbG9tU2lnbmVklUNl
cnRpZmljYXR1LTcyMTk0MzY2MDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwYkCgYEA
xRybTGD526rPYuDu2puMJU8ANcDqQnwnIERgvIWOLwBovuAu7WcRmzw1IDTDryOH
PXtln5GcQSAOgn+9QdvKl1Z43ZkRWK5E7EGmjM/aL1287mg4/NlrWr4KMSwDQBJI
noJ52CABXUoApuiiJ8Ya4gOYeP0TmsZtxP1N+s+wqjMCAwEAaNTMFEwDwYDVR0T
AQH/BAUwAwEB/zAfBgNVHSMEGDAWgBSEOKlAPAHBPedwichXL+qUM+lrITAdBgNV
HQ4EFgQUhDipQDwBwT3ncInIVy/qLDpta4kwdQYJKoZIhvcNAQEFBQADgYEA1BNN
wKSS8yBuOH0/jUV7sy3Y9/oV7Z9bW8WfV9QitQ11ZelvWMTbewozwX2LJvxobGcj
Pi+n99RIH8dBhWwoYl9GTN2LVI22GIPX12jNLqps+Mq/u2qxVm0964Sajs501KjQ
69XFfCVot1NA6z2eEP/69oL9x0uaJDZa+6ileh0=
-----END CERTIFICATE-----
```

Per elencare tutti i trust point configurati, eseguire il comando **show crypto pki trustpoints**. Una volta stampato il certificato sulla console, copiarlo su un file e salvarlo sul PC.

## 6. Importare il certificato dello switch nell'archivio di attendibilità ISE.

Su ISE, selezionare **Amministrazione > Certificati > Certificati attendibili**, quindi fare clic su **Importa**.

Fare clic su **Sfoggia** e selezionare il certificato dello switch. Fornire (facoltativamente) un nome descrittivo e selezionare le caselle di controllo **Trust for authentication within ISE** and **Trust for client authentication and Syslog**. Quindi fare clic su **Submit** (Invia), come mostrato nell'immagine:

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu includes System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, and Threat Centric NAC. The 'Certificates' section is selected, and the 'Import a new Certificate into the Certificate Store' form is displayed. The form includes the following fields and options:

- \* Certificate File:** Browse... sw.pem
- Friendly Name:** Switch3650
- Trusted For:**
  - Trust for authentication within ISE
  - Trust for client authentication and Syslog
  - Trust for authentication of Cisco Services
  - Validate Certificate Extensions
- Description:** (empty text field)
- Buttons:** Submit, Cancel

## 7. Configurare RADIUS sullo switch.

Aggiungere la configurazione RADIUS sullo switch. Per configurare lo switch in modo che comunichi con ISE su DTLS, utilizzare i comandi:

```
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
```

Il resto della configurazione specifica del server AAA dipende dai requisiti e dal progetto. Considerare questa configurazione come un esempio:

```
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. Configurare le policy su ISE.

Configurare i criteri di autenticazione e autorizzazione su ISE. Questo passaggio dipende anche dal progetto e dai requisiti.

## Verifica

Per verificare che gli utenti possano autenticarsi, usare il comando **test aaa** sullo switch:

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

USER ATTRIBUTES

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

Verrà visualizzato il messaggio **Autenticazione utente completata**. Selezionare **ISE Operations > RADIUS > LiveLog**, quindi selezionare i dettagli del log desiderato (fare clic sulla lente di ingrandimento):

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

Nella parte destra del rapporto è riportato un elenco di **passaggi**. Verificare che il primo passaggio dell'elenco sia un **pacchetto RADIUS crittografato**.

Inoltre, è possibile avviare l'acquisizione dei pacchetti su ISE ed eseguire nuovamente il comando **test aaa**. Per avviare l'acquisizione, selezionare **Operazioni > Risoluzione dei problemi > Strumenti diagnostici > Strumenti generali > Dump TCP**. Selezionare Policy Service Node utilizzato per l'autenticazione e fare clic su **Start**:



**Identity Services Engine** Home Context Visibility Operations Policy Administration Work Centers

RADIUS Threat-Centric NAC Live Logs TACACS Troubleshoot Adaptive Network Control Reports

Diagnostic Tools Download Logs

**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

Al termine dell'autenticazione, fare clic su **Stop and Download** (Interrompi e scarica). Quando si apre l'acquisizione dei pacchetti, dovrebbe essere possibile visualizzare il traffico crittografato con DTLS:

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

I pacchetti 813 - 822 fanno parte dell'handshake DTLS. Quando l'handshake viene negoziato correttamente, i dati dell'applicazione vengono trasferiti. Il numero di pacchetti può variare e dipende, ad esempio, dal metodo di autenticazione utilizzato (PAP, EAP-PEAP, EAP-TLS, ecc.). Il contenuto di ciascun pacchetto viene crittografato:

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...

Quando vengono trasmessi tutti i dati, il tunnel non viene demolito immediatamente. Il valore di **IdleTimeout** configurato su ISE determina per quanto tempo è possibile stabilire il tunnel senza

passare attraverso la comunicazione. Se il timer scade e occorre inviare una nuova richiesta di accesso all'ISE, viene eseguito l'handshake DTLS e il tunnel viene ricompilato.

## Risoluzione dei problemi

### 1. ISE non riceve richieste.

Notare che la porta DTLS predefinita è 2083. Le porte RADIUS predefinite sono 1645,1646 e 1812,1813. Verificare che il firewall non blocchi il traffico UDP/2083.

### 2. Handshake DTLS non riuscito.

Nel report dettagliato su ISE è possibile notare un errore dell'handshake DTLS:

#### 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

Il motivo possibile è che lo switch o ISE non considerano attendibile il certificato inviato durante l'handshake. Verificare la configurazione del certificato. Verificare che il certificato appropriato sia assegnato al ruolo DTLS RADIUS su ISE e ai trust point sullo switch.