Configuring RadSec

This chapter describes how to configure RadSec over Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) servers.

Restrictions for Configuring RadSec

Following restrictions apply to the RadSec feature:

- RADIUS client uses an ephemeral port as source port, and this source port should not be used for UDP, Datagram Transport Layer Security (DTLS), and Transport Layer Security (TLS) at the same time.
- Although there is no configuration restriction, it is recommended to use the same type, either only TLS or only DTLS, for a server under a Authentication, Authorization, and Accounting (AAA) server group.
- RadSec is supported on IPv4 connections only.

Information About RadSec

RadSec Overview

RadSec provides encryption services over RADIUS, which is transported over a secure tunnel. RadSec over TLS and DTLS is implemented in both client and device servers. Client side controls radius Authentication, Authorization, and Accounting (AAA) and device server side controls Change of Authorization (CoA).

You can configure the following parameters:

- Per client specific idletimeout, client trustpoint, and server trustpoint.
- Global CoA-specific TLS/DTLS listening port and list of source interfaces.

You can disable TLS or DTLS for a specific server by using the **no tls** or **no dtls** command in radius server configuration mode.

How to Configure RadSec

Configuring RadSec over TLS

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius server** *radius-server-name*
4. **tls** [**connectiontimeout** *connection-timeout-value*] [**idletimeout** *idle-timeout-value*] [**ip** {**radius source-interface** *interface-name* |**vrf forwarding** *forwarding-table-name*}] [**port** *port-number*] [**retries** *number-of-connection-retries*] [**trustpoint** {**client** *trustpoint name*|**server** *trustpoint name*}]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius server** *radius-server-name* **Example:** `Device(config)# radius server R1`	Enters radius server configuration mode.

Step 4	**tls** [**connectiontimeout** *connection-timeout-value*] [**idletimeout** *idle-timeout-value*] [**ip** {**radius source-interface** *interface-name* |**vrf forwarding** *forwarding-table-name*}] [**port** *port-number*] [**retries** *number-of-connection-retries*] [**trustpoint** {**client** *trustpoint name*|**server** *trustpoint name*}]
	Example:
	`Device(config-radius-server)# tls connectiontimeout 10`
	`Device(config-radius-server)# tls idletimeout 5`
	`Device(config-radius-server)# tls retries 15`
	`Device(config-radius-server)# tls ip radius source-interface GigabitEthernet 1/0/1`
		Configures TLS parameters. You can configure the following parameters:
		• **connectiontimeout**—Configures TLS connection timeout value. The default is 5 seconds.
		• **idletimeout**—Configures TLS idle timeout value. The default is 60 seconds.
		• **ip**—Configures IP source parameters.
		• **port**—Configures TLS port number. The default is 2083.
		• **retries**—Configures number of TLS connection retries. The default is 5.

	Command or Action	Purpose

	`Device(config-radius-server)# tls ip vrf forwarding table-1`
	`Device(config-radius-server)# tls port 10`
	`Device(config-radius-server)# tls trustpoint`
	`Device(config-radius-server)# tls trustpoint client TP-self-signed-721943660`
	`Device(config-radius-server)# tls trustpoint server isetp`
		• **trustpoint**—Configures TLS trustpoint for client and server. If TLS trustpoint for client and server are the same, the trustpoint name should also be the same for both.

Step 5	**end**
	Example:
	`Device(config-radius-server)# end`
		Returns from radius server configuration mode to privileged EXEC mode.

Configuring Dynamic Authorization for TLS CoA

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa server radius dynamic-author**
4. **client** {**ip-addr** \| **hostname**} [**tls** [**client-tp** *client-tp-name*] [**idletimeout** *idletimeout-interval*] [**server-tp** *server-tp-name*] \| **vrf** *vrf-id*]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa server radius dynamic-author** **Example:** `Device(config)# aaa server radius dynamic-author`	Enters dynamic authorization local server configuration mode and specifies a RADIUS client from which a device accepts Change of Authorization (CoA) and disconnect requests. Configures the device as a AAA server to facilitate interaction with an external policy server.
Step 4	**client** {**ip-addr** | **hostname**} [**tls** [**client-tp** *client-tp-name*] [**idletimeout** *idletimeout-interval*] [**server-tp** *server-tp-name*] | **vrf** *vrf-id*] **Example:**	Configures the IP address or hostname of the AAA server client. You can configure the following optional parameters: • **tls**—Enables TLS for the client. • **client-tp**—Configures client trustpoint.

	Command or Action	Purpose
	`Device(config-locsvr-da-radius)# client 10.104.49.14 tls idletimeout 100 client-tp tls_ise server-tp tls_client`	• **idletimeout**—Configures TLS idle timeout value. • **server-tp**—Configures server trustpoint. • **vrf**—Virtual routing and forwarding (VRF) ID of the client.

Step 5	**end**
	Example:
	`Device(config-radius-server)# end`
		Returns from dynamic authorization local server configuration mode to privileged EXEC mode.

Configuring RadSec over DTLS

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius server** *radius-server-name*
4. **dtls** [**connectiontimeout** *connection-timeout-value*] [**idletimeout** *idle-timeout-value*] [**ip** {**radius source-interface** *interface-name* |**vrf forwarding** *forwarding-table-name*}] [**port** *port-number*] [**retries** *number-of-connection-retries*] [**trustpoint** {**client** *trustpoint name*|**server** *trustpoint name*}]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius server** *radius-server-name* **Example:** `Device(config)# radius server R1`	Enters radius server configuration mode.
Step 4	**dtls** [**connectiontimeout** *connection-timeout-value*] [**idletimeout** *idle-timeout-value*] [**ip** {**radius source-interface** *interface-name* |**vrf forwarding** *forwarding-table-name*}] [**port** *port-number*] [**retries** *number-of-connection-retries*] [**trustpoint** {**client** *trustpoint name*|**server** *trustpoint name*}] **Example:**	Configures DTLS parameters. You can configure the following parameters: • **connectiontimeout**—Configures DTLS connection timeout value. The default is 5 seconds. • **idletimeout**—Configures DTLS idle timeout value. The default is 60 seconds.

	Command or Action	Purpose

	`Device(config-radius-server)# dtls connectiontimeout 10`
	`Device(config-radius-server)# dtls idletimeout 5`
	`Device(config-radius-server)# dtls retries 15`
	`Device(config-radius-server)# dtls ip radius source-interface GigabitEthernet 1/0/1`
	`Device(config-radius-server)# dtls ip vrf forwarding table-1`
	`Device(config-radius-server)# dtls port 10`
	`Device(config-radius-server)# dtls trustpoint`
	`Device(config-radius-server)# dtls trustpoint client TP-self-signed-721943660`
	`Device(config-radius-server)# dtls trustpoint server isetp`
		• **ip**—Configures IP source parameters.
		• **port**—Configures DTLS port number. The default is 2083.
		• **retries**—Configures number of DTLS connection retries. The default is 5.
		• **trustpoint**—Configures DTLS trustpoint for client and server. If DTLS trustpoint for client and server are the same, the trustpoint name should also be the same for both.

Step 5	**end**
	Example:
	`Device(config-radius-server)# end`
		Returns from radius server configuration mode to privileged EXEC mode.

Configuring Dynamic Authorization for DTLS CoA

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa server radius dynamic-author**
4. **client {ip-addr | hostname}** [**dtls** [**client-tp** *client-tp-name*] [**idletimeout** *idletimeout-interval*] [**server-tp** *server-tp-name*] | **vrf** *vrf-id*]
5. **dtls** {**ip radius source-interface** *interface-name* | **port** *radius-dtls-server-port-number*}
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa server radius dynamic-author** **Example:**	Enters dynamic authorization local server configuration mode and specifies a RADIUS client from which a device

	Command or Action	Purpose
	`Device(config)# aaa server radius dynamic-author`	accepts Change of Authorization (CoA) and disconnect requests. Configures the device as a AAA server to facilitate interaction with an external policy server.
Step 4	**client {ip-addr | hostname}** [**dtls** [**client-tp** *client-tp-name*] [**idletimeout** *idletimeout-interval*] [**server-tp** *server-tp-name*] | **vrf** *vrf-id*] **Example:** `Device(config-locsvr-da-radius)# client 10.104.49.14 dtls idletimeout 100 client-tp dtls_ise server-tp dtls_client`	Configures the IP address or hostname of the AAA server client. You can configure the following optional parameters: • **dtls**—Enables DTLS for the client. • **client-tp**—Configures client trustpoint. • **idletimeout**—Configures DTLS idle timeout value. • **server-tp**—Configures server trustpoint. • **vrf**—Virtual routing and forwarding (VRF) ID of the client.

Step 5	**dtls** {**ip radius source-interface** *interface-name* | **port** *radius-dtls-server-port-number*}
	Example:
	`Device(config-locsvr-da-radius)# dtls ip radius source-interface  GigabitEthernet 1/0/24`
	`Device(config-locsvr-da-radius)# dtls port 100`
		Configures RADIUS CoA server. You can configure the following parameters:
		• **ip radius source-interface** *interface-name*—Specifies the interface for source address in RADIUS CoA Server.
		• **port** *radius-dtls-server-port-number*—Specifies port on which local DTLS RADIUS server listens.

Step 6	**end**
	Example:
	`Device(config-radius-server)# end`
		Returns from dynamic authorization local server configuration mode to privileged EXEC mode.

Monitoring RadSec

The following commands can be used to monitor TLS and DTLS server statistics:

Table 1: Monitoring TLS and DTLS Server Statistics Commands

Command	Purpose
show aaa servers	Displays information related to TLS and DTLS servers.
clear aaa counters servers radius {*server id* | **all**}	Clears the RADIUS TLS/DTLS specific statistics.
debug radius tls	Enables RADIUS TLS specific debugs.
debug radius dtls	Enables RADIUS DTLS specific debugs.

Configuration Examples for RadSec

Example: Configuring RadSec over TLS

```
Device> enable
Device# configure terminal
Device(config)# radius server R1
Device(config-radius-server)# tls connectiontimeout 10
Device(config-radius-server)# tls idletimeout 5
Device(config-radius-server)# tls retries 15
Device(config-radius-server)# tls ip radius source-interface GigabitEthernet 1/0/1
Device(config-radius-server)# tls ip vrf forwarding table-1
Device(config-radius-server)# tls port 10
Device(config-radius-server)# tls trustpoint
Device(config-radius-server)# tls trustpoint client TP-self-signed-721943660
Device(config-radius-server)# tls trustpoint server isetp
Device(config-radius-server)# end
```

Example: Configuring Dynamic Authorization for TLS CoA

```
Device> enable
Device# configure terminal
Device(config)# aaa server radius dynamic-author
Device(config-locsvr-da-radius)# client 10.104.49.14 tls idletimeout 100 client-tp tls_ise
 server-tp tls_client
Device(config-locsvr-da-radius)# dtls port 100
Device(config-radius-server)# end
```

Example: Configuring RadSec over DTLS

```
Device> enable
Device# configure terminal
Device(config)# radius server R1
Device(config-radius-server)# dtls connectiontimeout 10
Device(config-radius-server)# dtls idletimeout 5
Device(config-radius-server)# dtls retries 15
Device(config-radius-server)# dtls ip radius source-interface GigabitEthernet 1/0/1
Device(config-radius-server)# dtls ip vrf forwarding table-1
Device(config-radius-server)# dtls port 10
Device(config-radius-server)# dtls trustpoint
Device(config-radius-server)# dtls trustpoint client TP-self-signed-721943660
Device(config-radius-server)# dtls trustpoint server isetp
Device(config-radius-server)# end
```

Example: Configuring Dynamic Authorization for DTLS CoA

```
Device> enable
Device# configure terminal
Device(config)# aaa server radius dynamic-author
Device(config-locsvr-da-radius)# client 10.104.49.14 dtls idletimeout 100 client-tp dtls_ise
 server-tp dtls_client
```

```
Device(config-locsvr-da-radius)# dtls ip radius source-interface GigabitEthernet 1/0/24
Device(config-locsvr-da-radius)# dtls port 100
Device(config-radius-server)# end
```

Feature Information for Configuring RadSec

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 2: Feature Information for Configuring RadSec

Feature Name	Releases	Feature Information
Configuring RadSec over DTLS	Cisco IOS XE Everest 16.6.1	RadSec over DTLS provides encryption services over RADIUS, which is transported over a secure tunnel.
Configuring RadSec over TLS	Cisco IOS XE Fuji 16.9.1	RadSec over TLS provides encryption services over RADIUS, which is transported over a secure tunnel.