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, on page 1
- Information About RadSec, on page 2
- How to Configure RadSec, on page 2
- Monitoring RadSec, on page 7
- Configuration Examples for RadSec, on page 7
- Feature History for Configuring RadSec, on page 9

Restrictions for Configuring RadSec

The following restrictions apply to the RadSec feature:

- A RADIUS client uses an ephemeral port as the source port. 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, we recommend that you use the same type—either only TLS or only DTLS—for a server under an AAA server group.
- RadSec is not supported on the DTLS port range 1 to 1024.

Note DTLS ports must be configured to work with the RADIUS server.

- RadSec is not supported with high availability.
- RADIUS Change of Authorization (CoA) reception of request and transmission of response over the same authentication channel is supported with RadSec over TLS only. It is not supported over DTLS or plain RADIUS.
- The **tls watchdoginterval** command is not applicable for Packet of Disconnect (PoD) use cases.
- FQDN configuration for CoA is not supported.
- VRF-aware DNS resolution is not supported if configured with FQDNs.

Information About RadSec

RadSec provides encryption services over the RADIUS server transported over a secure tunnel. RadSec over TLS and DTLS is implemented in both client and device servers. While the client side controls RADIUS AAA, the device side controls CoA.

You can configure the following parameters:

- Individual client-specific idle timeout, client trustpoint, and server trustpoint.
- Global CoA-specific TLS or DTLS listening port and the corresponding list of source interfaces.

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

RadSec CoA request reception and CoA response transmission over the same authentication channel can be enabled by configuring the **tls watchdoginterval** command. The TLS watchdog timer must be lesser than the TLS idle timer so that the established tunnel remains active if RADIUS test authentication packets are seen before the idle timer expires. If the tunnel is torn down and **tls watchdoginterval** command is enabled, the tunnel gets re-established immediately. If **tls watchdoginterval** command is disabled, CoA requests on the same authentication channel are discarded.

How to Configure RadSec

The following sections provide information about the various tasks that comprise RadSec configuration.

Configuring RadSec over TLS

Procedure

	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`	Specifies the name for the RADIUS server configuration for Protected Access Credential (PAC) provisioning, and enters RADIUS server configuration mode.

	Command or Action	Purpose

Step 4	**tls** [**connectiontimeout** *connection-timeout-value*] [**idletimeout** *idle-timeout-value*] [[**ip** | **ipv6**] {**radius source-interface** *interface-name* |**vrf forwarding** *forwarding-table-name*}] [**match-server-identity** {**email-address** *email-address* | **hostname** *host-name* | **ip-address** *ip-address*}] [**port** *port-number*] [**retries** *number-of-connection-retries*] [**trustpoint** {**client** *trustpoint name* | **server** *trustpoint name*}] [**watchdoginterval** *interval*]
	Example:
	`Device(config-radius-server)# tls connectiontimeout 10`
	`Device(config-radius-server)# tls idletimeout 75`
	`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 ipv6 vrf forwarding table-1`
	`Device(config-radius-server)# tls match-server-identity ip-address 10.1.1.10`
	`Device(config-radius-server)# tls port 10`
	`Device(config-radius-server)# tls trustpoint client TP-self-signed-721943660`
	`Device(config-radius-server)# tls trustpoint server isetp`
	`Device(config-radius-server)# tls watchdoginterval 10`
		Configures the TLS parameters. You can configure the following parameters:
		• **connectiontimeout**: Configures TLS connection timeout value. The default is 5 seconds.
		• **idletimeout**: Configures the TLS idle timeout value. The default is 60 seconds.
		• **ip**: Configures IP source parameters.
		• **ipv6**: Configures IPv6 source parameters.
		• **match-server-identity**: Configures RadSec certification validation parameters.
		Note This is a mandatory configuration.
		• **port**: Configures the TLS port number. The default is 2083.
		• **retries**: Configures the number of TLS connection retries. The default is 5.
		• **trustpoint**: Configures the TLS trustpoint for a client and a server. If the TLS trustpoint for the client and server are the same, the trustpoint name should also be the same for both.
		• **watchdoginterval**: Configures the watchdog interval. This enables CoA requests to be received on the same authentication channel. It also serves as a keepalive to keep the TLS tunnel up, and re-establishes the tunnel if it is torn down.
		Note **watchdoginterval** value must be lesser than **idletimeout**, for the established tunnel to remain up.

Step 5	**end** **Example:** `Device(config-radius-server)# end`	Exits RADIUS server configuration mode and returns to privileged EXEC mode.

Configuring Dynamic Authorization for TLS CoA

Note When the **tls watchdoginterval** command is enabled, the client IP configuration under **aaa server radius dynamic-author** command is not used. Instead, the key configured under **radius server** command is used for CoA transactions.

Procedure

	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 the RADIUS client from which a device accepts CoA and disconnect requests. Configures the device as an 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-key** *server-key*] [**server-tp** *server-tp-name*]] **Example:** `Device(config-locsvr-da-radius)# client 10.104.49.14 tls idletimeout 100 client-tp tls_ise server-tp tls_client server-key key1`	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 the client trustpoint. • **idletimeout**: Configures the TLS idle timeout value. • **server-key**: Configures a RADIUS client server key. • **server-tp**: Configures the server trustpoint.
Step 5	**end** **Example:** `Device(config-locsvr-da-radius)# end`	Exits dynamic authorization local server configuration mode and returns to privileged EXEC mode.

Configuring RadSec over DTLS

Procedure

	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`	Specifies the name for the RADIUS server configuration for Protected Access Credential (PAC) provisioning, and enters RADIUS server configuration mode.

Step 4	**dtls** [**connectiontimeout** *connection-timeout-value*] [**idletimeout** *idle-timeout-value*] [[**ip | ipv6**] {**radius source-interface** *interface-name* |**vrf forwarding** *forwarding-table-name*}] [**match-server-identity** {**email-address** *email-address* | **hostname** *host-name* | **ip-address** *ip-address*}] [**port** *port-number*] [**retries** *number-of-connection-retries*] [**trustpoint** {**client** *trustpoint name* | **server** *trustpoint name*}]
	Example:
	`Device(config-radius-server)# dtls connectiontimeout 10`
	`Device(config-radius-server)# dtls idletimeout 75`
	`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 ipv6 vrf forwarding table-1`
	`Device(config-radius-server)# tls match-server-identity ip-address 10.1.1.10`
	`Device(config-radius-server)# dtls port 10`
	`Device(config-radius-server)# dtls trustpoint client TP-self-signed-721943660`
	`Device(config-radius-server)# dtls trustpoint server isetp`
		Configures DTLS parameters. You can configure the following parameters:
		• **connectiontimeout**: Configures the DTLS connection timeout value. The default is 5 seconds.
		• **idletimeout**: Configures the DTLS idle timeout value. The default is 60 seconds.
		Note When the idle timeout expires, and there are no transactions after the last idle timeout, the DTLS session is closed. When the session is re-established, restart the idle timer for the session to work.
		If the configured idle timeout is 30 seconds, when the timeout expires, the number of RADIUS DTLS transactions are checked. If the RADIUS DTLS packets are more than 0, the transaction counter is reset and the timer is started again.
		• **ip**: Configures IP source parameters.
		• **ipv6**: Configures IPv6 source parameters.
		• **match-server-identity**: Configures RadSec certification validation parameters.
		Note This is a mandatory configuration.

	Command or Action	Purpose
		• **port**: Configures the DTLS port number. The default is 2083. • **retries**: Configures the number of DTLS connection retries. The default is 5. • **trustpoint**: Configures the DTLS trustpoint for the client and the server. If the DTLS trustpoint for the 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`	Exits RADIUS server configuration mode and returns to privileged EXEC mode.

Configuring Dynamic Authorization for DTLS CoA

Procedure

	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 the device accepts CoA and disconnect requests. Configures the device as an 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-key** *server-key*] [**server-tp** *server-tp-name*]] **Example:** `Device(config-locsvr-da-radius)# client 10.104.49.14 dtls idletimeout 100 client-tp tls_ise server-tp tls_client server-key key1`	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 the client trustpoint. • **idletimeout**: Configures the TLS idle timeout value.

	Command or Action	Purpose
		• **server-key**: Configures a RADIUS client server key. • **server-tp**: Configures the server trustpoint.

Step 5	**dtls** {{**ip** | **ipv6**} **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 the RADIUS CoA server. You can configure the following parameters:
		• {**ip** | **ipv6**} **radius source-interface** *interface-name*: Specifies the interface for the source address in the RADIUS CoA server.
		• **port** *radius-dtls-server-port-number*: Specifies the port on which the local DTLS RADIUS server listens.

Step 6	**end** **Example:** `Device(config-locsvr-da-radius)# end`	Exits dynamic authorization local server configuration mode and returns to privileged EXEC mode.

Monitoring RadSec

Use the following commands to monitor TLS and DTLS server statistics.

Table 1: Monitoring TLS and DTLS Server Statistics

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-specific or DTLS-specific statistics.
debug radius radsec	Enables RADIUS RadSec debugs.

Configuration Examples for RadSec

The following examples help you understand the RadSec configuration better.

Example: Configuring RadSec over TLS

The following example shows how to configure 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 75
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 client TP-self-signed-721943660
Device(config-radius-server)# tls trustpoint server isetp
Device(config-radius-server)# tls watchdoginterval 10
Device(config-radius-server)# end
```

Example: Configuring Dynamic Authorization for TLS CoA

The following example shows how to configure 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)# end
```

Example: Configuring RadSec over DTLS

The following example shows how to configure 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 75
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 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

The following example shows how to configure 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-locsvr-da-radius)# end
```

Feature History for Configuring RadSec

This table provides release and related information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE Bengaluru 17.4.1	Configuring RadSec	RadSec provides encryption services over the RADIUS server, which is transported over a secure tunnel.
Cisco IOS XE Bengaluru 17.6.1	Radsec CoA over Same Tunnel	RadSec CoA request reception and CoA response transmission can be done over the same authentication channel.
Cisco IOS XE Cupertino 17.9.1	Configuring RadSec	This feature was implemented on C9200CX-12P-2X2G, C9200CX-8P-2X2G, and C9200CX-12T-2X2G models of the Cisco Catalyst 9200CX Series Switches, which were introduced in this release.

Use the Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to Cisco Feature Navigator.