

Secure Logging Commands

This module describes the Cisco IOS XR software commands used to configure secure logging on the Cisco 8000 Series Routers over Transport Layer Security (TLS). TLS, the successor of Secure Socket Layer (SSL), is an encryption protocol designed for data security over networks.

For detailed information about secure logging concepts, configuration tasks, and examples, see the *Implementing Secure Logging* module in the *System Security Configuration Guide for Cisco 8000 Series Routers*.

- address, on page 2
- enable tls 1.3 legacy kdf, on page 3
- logging tls-server, on page 4
- tls-hostname , on page 5
- tlsv1-disable, on page 6
- trustpoint , on page 7
- vrf, on page 8

address

To configure the syslog server settings with IP address, use the **address** command in logging TLS peer configuration mode. To remove the configuration, use the **no** form of this command.

address { **IPv4** *ipv4-address* | **IPv6** *ipv6-address* **}**

Syntax Description

ipv4-address	IPv4 address in A:B:C:D format.
ipv6-address	IPv6 address in X:X::X format.

Command Default

None

Command Modes

Logging TLS peer configuration mode

Command History

Release	Modification
Release 6.2.1	This command was introduced.

Usage Guidelines

You can use the IPv4 or IPv6 address of the server to access the remote syslog server.

Task ID

Task ID	Operations
logging	Read, Write

Examples

The following example shows how to configure syslog server settings with IPv4 address:

```
Router(config)# logging tls-server TEST
Router(config-logging-tls-peer)# severity debugging
Router(config-logging-tls-peer)# trustpoint tp
Router(config-logging-tls-peer)# address ipv4 10.105.230.83
```

Related Commands

Command	Description
logging tls-server, on page 4	Configures syslog over TLS server.
trustpoint , on page 7	Configures the trustpoint for the TLS server.

enable tls 1.3 legacy kdf

To support backward compatibility for local EAP authentication, use **enable-tls1.3-legacy-kdf** command in CONFIG mode.

enable-tls1.3-legacy-kdf

Syntax Description

enable-tls1.3-legacy-kdf	Enables legacy key derivation for MACsec EAP with TLS 1.3.

Command Default

No default behavior or values

Command Modes

CONFIG mode

Command History

Release	Modification
Release 25.4.1	The command was introduced.

Usage Guidelines

This command must be configured when using EAP based MACsec with Local EAP Authentication to ensure interoperability with XR releases earlier than 25.4.1.

Task ID

Task ID	Operation
eap	read

This example shows how to configure and enable legacy key derivation for MACsec EAP with TLS 1.3 on the router:

```
Router#configure
Router#(config)#eap profile tls
Router#(config-eap-tls)#method tls
Router#(config-profile-tls-tls)#enable-tls1.3-legacy-kdf
Router#(config-profile-tls-tls)#commit
Router#(config-profile-tls-tls)#end
```

logging tls-server

To configure System Logging over Transport Layer Security (TLS) server, use the **logging tls-server** command in Global Configuration mode. To remove the configuration, use the **no** form of this command.

logging tls-server *tls-name*

Syntax Description

tls-name	User-defined name for the TLS server.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 6.2.1	This command was introduced.

Usage Guidelines

This command enters the logging TLS peer configuration mode, where you can configure the settings to access the remote syslog server.

Starting with Cisco IOS XR Software Release 25.4.1, a one-time syslog warning is generated if TLS 1.0 or TLS 1.1 is used, and a continuous warning once in a month occurs if the syslog minimum TLS version is configured as TLS 1.0 or 1.1. The default minimum syslog TLS version is now TLS 1.2 to enhance security.

Task ID

Task ID	Operation
logging	read, write

This example shows how to configure a TLS server that enters the logging TLS peer configuration mode:

```
Router#Configure
Router(config)#logging tls-server TEST
Router(config-logging-tls-peer)#commit
```

tls-hostname

To configure the syslog server settings with hostname or FQDN of the secure log server, use the **tls-hostname** command in logging TLS peer configuration mode. To remove the configuration, use the **no** form of this command.

tls-hostname *hostname*

Syntax Description

hostname	Name of the logging host.

Command Default

None

Command Modes

Logging TLS peer configuration mode

Command History

Release	Modification
Release 6.2.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
logging	Read, Write

Examples

The following example shows how to configure syslog server settings with server hostname:

```
Router(config)# logging tls-server TEST
Router(config-logging-tls-peer)# severity debugging
Router(config-logging-tls-peer)# trustpoint tp
Router(config-logging-tls-peer)# tls-hostname xyz.cisco.com
```

Related Commands

Command	Description
logging tls-server, on page 4	Configures syslog over TLS server.
trustpoint , on page 7	Configures the trustpoint for the TLS server.

tlsv1-disable

To disable Transport Layer Security (TLS) version 1.0, use the **tlsv1-disable** command in Global Configuration modeXR Config mode.

tlsv1-disable

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global Configuration modeXR Config mode

Command History

Release	Modification
Release 7.9.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
system	Read, Write

Examples

The following example shows how to disable TLS version 1.0:

```
Router(config)# grpc tlsv1-disable
```

trustpoint

To configure syslog server settings with a trustpoint for the TLS server, use the **trustpoint** command in logging TLS peer configuration mode. To remove the configuration, use the **no** form of this command.

trustpoint *trustpoint-name*

Syntax Description

trustpoint-name	Name of the configured trustpoint .

Command Default

None

Command Modes

Logging TLS peer configuration mode

Command History

Release	Modification
Release 6.2.1	This command was introduced.

Usage Guidelines

Ensure that you have already configured the trustpoint name, using the **crypto ca trustpoint** command.

Task ID

Task ID	Operations
logging	Read, Write

Examples

The following example shows how to configure syslog server settings with trustpoint:

```
Router(config)# logging tls-server TEST
Router(config-logging-tls-peer)# severity debugging
Router(config-logging-tls-peer)# trustpoint tp
```

Related Commands

Command	Description
logging tls-server, on page 4	Configures syslog over TLS server.

vrf

To configure the VRF option for the TLS server, use the **vrf** command in logging TLS peer configuration mode. To remove the configuration, use the **no** form of this command.

vrf *vrf-name*

Syntax Description

vrf-name	VPN Routing/Forwarding instance name.

Command Default

None

Command Modes

Logging TLS peer configuration mode

Command History

Release	Modification
Release 6.2.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
logging	Read, Write

Examples

The following example shows how to configure a VRF instance:

```
Router(config)# logging tls-server TEST
Router(config-logging-tls-peer)# vrf vrftest
```

Related Commands

Command	Description
logging tls-server, on page 4	Configures syslog over TLS server.