System Security Command Reference for Cisco ASR 9000 Series Routers

First Published: 2020-06-08

Last Modified: 2024-03-01

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Preface

This guide describes the commands used to display and configure system security on Cisco IOS XR software. For System Security configuration information and examples, refer to the *System Security Configuration Guide for Cisco ASR 9000 Series Routers*.

The preface contains the following sections:

Changes to This Document

This table lists the technical changes made to this document since it was first printed.

Table 1: Changes to This Document

Date	Change Summary
August 2023	Republished for Release 7.10.1
November 2022	Republished for Release 7.8.1
July 2022	Republished for Release 7.7.1
November 2021	Republished for Release 7.5.1
October 2021	Republished for Release 7.3.2
July 2021	Republished for Release 7.4.1
July 2021	Republished for Release 6.8.1
February 2021	Republished for Release 7.3.1
August 2020	Republished for Release 7.1.2 and Release 6.7.2
May 2020	Initial release of the cumulative command reference document that covers all updates from Release 4.3.0 onwards

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Authentication, Authorization, and Accounting Commands

This module describes the commands used to configure authentication, authorization, and accounting (AAA) services.

To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

For detailed information about AAA concepts, configuration tasks, and examples, see the *Configuring AAA Services on Cisco IOS XR Software* chapter in the *System Security Configuration Guide for Cisco ASR 9000 Series Routers*.

aaa accounting

To create a method list for accounting, use the **aaa accounting** command in Global Configuration mode. To remove a list name from the system, use the **no** form of this command.

aaa accounting {**commands** | **exec** | **mobile** | **network** | **subscriber** | **system** } {**default** | **list-name**} {**start-stop** | **stop-only**} {**none** | **method**}

Syntax Description

commands	Enables accounting for EXEC shell commands.
exec	Enables accounting of an EXEC session.
mobile	Enables Mobile IP related accounting events.
network	Enables accounting for all network-related service requests, such as Internet Key Exchange (IKE) and Point-to-Point Protocol (PPP).
subscriber	Sets accounting lists for subscribers.
system	Enables accounting for all system-related events.
default	Uses the listed accounting methods that follow this keyword as the default list of methods for accounting services.
list-name	Character string used to name the accounting method list.
start-stop	Sends a "start accounting" notice at the beginning of a process and a "stop accounting" notice at the end of a process. The requested user process begins regardless of whether the "start accounting" notice was received by the accounting server.
stop-only	Sends a "stop accounting" notice at the end of the requested user process. Note: This is not supported with system accounting.
none	Uses no accounting.
method	Method used to enable AAA system accounting. The value is one of the following options: • **group tacacs+**—Uses the list of all TACACS+ servers for accounting. • **group radius**—Uses the list of all RADIUS servers for accounting. • **group** *named-group*—Uses a named subset of TACACS+ or RADIUS servers for accounting, as defined by the **aaa group server tacacs+** or **aaa group server radius** command.

Command Default

AAA accounting is disabled.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 5.3.0	The **mobile** keyword was added.

Usage Guidelines

Use the **aaa accounting** command to create default or named method lists defining specific accounting methods and that can be used on a per-line or per-interface basis. You can specify up to four methods in the method list. The list name can be applied to a line (console, aux, or vty template) to enable accounting on that particular line.

The Cisco IOS XR software supports both TACACS+ and RADIUS methods for accounting. The router reports user activity to the security server in the form of accounting records, which are stored on the security server.

Method lists for accounting define the way accounting is performed, enabling you to designate a particular security protocol that is used on specific lines or interfaces for particular types of accounting services.

For minimal accounting, include the **stop-only** keyword to send a "stop accounting" notice after the requested user process. For more accounting, you can include the **start-stop** keyword, so that TACACS+ sends a "start accounting" notice at the beginning of the requested process and a "stop accounting" notice after the process. The accounting record is stored only on the TACACS+ server.

The requested user process begins regardless of whether the "start accounting" notice was received by the accounting server.

Note This command cannot be used with TACACS or extended TACACS.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to define a default commands accounting method list, where accounting services are provided by a TACACS+ security server, with a stop-only restriction:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa accounting commands default stop-only group tacacs+
```

Related Commands

Command	Description
aaa authorization , on page 20	Creates a method list for authorization.

aaa accounting service

To create an accounting list for service accounting, use the **aaa accounting service** command in Global Configuration mode or Admin Configuration mode. To disable the service authentication method, use the **no** form of this command.

aaa accounting service {*list_name* | **default**} {**broadcast group** {*group_name* | **diameter** | **radius**} | **group** {*group_name* | **diameter** | **radius**}}

Syntax Description

default	Uses the listed authentication methods that follow this keyword as the default list of methods for authentication.
list-name	Represents the character string of the list name for AAA authentication.
broadcast	Specifies the broadcast accounting for the service.
group	Specifies the server-group.
group_name	Specifies the server group name.
diameter	Specifies the list of all DIAMETER peers.
radius	Specifies the list of all RADIUS hosts.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 4.3.1	This command was introduced.
Release 5.3.0	The **diameter** keyword was added for DIAMETER protocol support in BNG.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
aaa	read, write

This is an example of configuring the **aaa accounting service** command for the grpFR server group:

```
RP/0/RSP0/CPU0:router(config)# aaa accounting service default group grpFR
```

This example shows how to configure the **aaa accounting service** command with DIAMETER protocol to carry subscriber service accounting records to DIAMETER server using base accounting application:

aaa accounting system default

To enable authentication, authorization, and accounting (AAA) system accounting, use the **aaa accounting system default** command in Global Configuration mode. To disable system accounting, use the **no** form of this command.

aaa accounting system default {**start-stop** | **stop-only**} {**none** | **method**}

Syntax Description

start-stop	Sends a "start accounting" notice during system bootup and a "stop accounting" notice during system shutdown or reload.
stop-only	Sends a "stop accounting" notice during system shutdown or reload.
none	Uses no accounting.
method	Method used to enable AAA system accounting. The value is one of the following options: • **group tacacs+**—Uses the list of all TACACS+ servers for accounting. • **group radius**—Uses the list of all RADIUS servers for accounting. • **group** *named-group*—Uses a named subset of TACACS+ or RADIUS servers for accounting, as defined by the **aaa group server tacacs+** or **aaa group server radius** command.

Command Default

AAA accounting is disabled.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

System accounting does not use named accounting lists; you can define only the default list for system accounting.

The default method list is automatically applied to all interfaces or lines. If no default method list is defined, then no accounting takes place.

You can specify up to four methods in the method list.

Task ID

Task ID	Operations
aaa	read, write

Examples

This example shows how to cause a "start accounting" record to be sent to a TACACS+ server when a router initially boots. A "stop accounting" record is also sent when a router is shut down or reloaded.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa accounting system default start-stop group tacacs+
```

Related Commands

Command	Description
aaa authentication , on page 15	Creates a method list for authentication.
aaa authorization , on page 20	Creates a method list for authorization.

aaa accounting system rp-failover

To create an accounting list to send rp-failover or rp-switchover start or stop accounting messages, use the **aaa accounting system rp-failover** command in Global Configuration mode. To disable the system accounting for rp-failover, use the **no** form of this command.

aaa accounting system rp-failover {*list_name* {**start-stop** | **stop-only**} | **default** {**start-stop** | **stop-only**}}

Syntax Description

list_name	Specifies the accounting list name.
default	Specifies the default accounting list.
start-stop	Enables the start and stop records.
stop-only	Enables the stop records only.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
aaa	read, write

This is an example of configuring the **aaa accounting system rp-failover** command for default accounting list:

```
RP/0/RSP0/CPU0:router(config)# aaa accounting system rp-failover default start-stop none
```

Related Commands

Command	Description
aaa attribute format	Create an AAA attribute format name.

aaa accounting update

To enable periodic interim accounting records to be sent to the accounting server, use the **aaa accounting update** command in Global Configuration mode. To disable the interim accounting updates, use the **no** form of this command.

aaa accounting update {**periodic** *minutes*}

Syntax Description

periodic *minutes*	(Optional) Sends an interim accounting record to the accounting server periodically, as defined by the *minutes* argument, which is an integer that specifies the number of minutes. The range is from 1 to 35791394 minutes.

Command Default

AAA accounting update is disabled.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

When used with the **periodic** keyword, interim accounting records are sent periodically as defined by the *minutes* argument. The interim accounting record contains all the accounting information recorded for that user up to the time the accounting record is sent.

Caution Using the **aaa accounting update** command with the **periodic** keyword can cause heavy congestion when many users are logged into the network.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to send periodic interim accounting records to the RADIUS server at 30-minute intervals:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa accounting update periodic 30
```

Related Commands

Command	Description
aaa accounting, on page 4	Creates a method list for accounting.
aaa authorization , on page 20	Creates a method list for authorization.

aaa attribute format

To create an AAA attribute format name and to enter the configuration ID format sub mode, use the **aaa attribute format** command in Global Configuration mode. To disable this AAA attribute format, use the **no** form of this command.

aaa attribute format *format_name* [**circuit-id[plus][mac-address| remote-id]** [**separator** *separator*] | **format-string** [**length** *length*] {*string* [*Identity-Attribute*] } | **mac-address [plus][circuit-id | remote-id]** [**separator** *separator*] | **remote-id [plus][circuit-id | mac-address]** [**separator** *separator*] | **username-strip** {**prefix-delimiter** | **suffix-delimiter**} {*delimiter*}]

Syntax Description

format_name	Specifies the name of the format.
circuit-id	Specifies the construction of the AAA attribute format name for subscribers based on the circuit-ID.
format-string	Specifies the extended string format of the AAA attribute format name.
string	Specifies the regular ASCII characters that includes conversion specifiers. The value is enclosed in double quotes.
Identity-Attribute	Identifies a session. For more information about the syntax for the router, use the question mark (?) online help function.
length	Specifies the length of the formatted attribute string.
length	Length of the formatted string, in integer. The range is from 1 to 253.
mac-address	Specifies the construction of the AAA attribute format name for subscribers based on the mac-address. The MAC address must be in the form of three 4-digit values (12 digits in dotted decimal notation).
remote-id	Specifies the construction of the AAA attribute format name for subscribers based on the remote-ID.
plus	Specifies the use of additional identifiers.
separator	Specifies the separator to be used between keys.
separator	Separator to be used between keys, default is a semicolon.
username-strip	Configures a network access server (NAS) to strip both suffixes and/or prefixes from the username before forwarding the username to the remote RADIUS server.

prefix-delimiter	Enables prefix stripping and specifies the character that will be recognized as a prefix delimiter.
suffix-delimiter	Enables suffix stripping and specifies the character that will be recognized as a suffix delimiter.
Delimiter	Suffix or prefix delimiter.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.
Release 4.2.1	The support for **format-string** keyword was added.
Release 6.2.1	Introduced support for a new MAC address format, **client-mac-address-custom1**, which is in 01.23.45.67.89.AB format.
Release 6.4.1	Introduced support for **dhcpv6-client-id-enterprise-identifier**, **dhcpv6-vendor-class-spl**, **dhcpv4-client-id-spl** and **dhcpv4-vendor-class** as part of enabling AAA username formation using DHCP option 1 and option 16.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
aaa	read, write

This is an example of configuring the **aaa attribute format** command in the Global Configuration mode:

```
RP/0/RSP0/CPU0:router(config)# aaa attribute format form1
RP/0/RSP0/CPU0:router(config-id-format)# format-string "%s%s"
RP/0/RSP0/CPU0:router(config-id-format)# username-strip prefix-delimiter @
```

This is an example of configuring MAC address in "01.23.45.67.89.AB" format:

```
RP/0/RSP0/CPU0:router(config)# aaa attribute format form1
RP/0/RSP0/CPU0:router(config-id-format)# format-string length 253 "%s"
client-mac-address-custom1
```

This example shows how to enable AAA username formation using DHCP option 1 and option 16 in BNG:

```
RP/0/RSP0/CPU0:router(config)# aaa attribute format format_v6
RP/0/RSP0/CPU0:router(config-id-format)# format-string length 233 "%s@%s"
dhcpv6-client-id-enterprise-identifier dhcpv6-vendor-class-string
```

aaa authentication

To create a method list for authentication, use the **aaa authentication** command. To disable this authentication method, use the **no** form of this command.

aaa authentication {**login** | **ppp**} {**default***list-name* | **remote**} *method-list*

Syntax Description

login	Sets authentication for login.
ppp	Sets authentication for Point-to-Point Protocol.
default	Uses the listed authentication methods that follow this keyword as the default list of methods for authentication.
subscriber	Sets the authentication list for the subscriber.
list-name	Character string used to name the authentication method list.
remote	Uses the listed authentication methods that follow this keyword as the default list of methods for administrative authentication on a remote non-owner secure domain router. The **remote** keyword is used only with the **login** keyword and not with the **ppp** keyword. **Note** The **remote** keyword is available only on the administration plane.
method-list	Method used to enable AAA system accounting. The value is one of the following options: • **group tacacs+**—Specifies a method list that uses the list of all configured TACACS+ servers for authentication. • **group radius**—Specifies a method list that uses the list of all configured RADIUS servers for authentication. • **group** *named-group* —Specifies a method list that uses a named subset of TACACS+ or RADIUS servers for authentication, as defined by the **aaa group server tacacs+** or **aaa group server radius** command. • **local**—Specifies a method list that uses the local username database method for authentication. AAA method rollover happens beyond the local method if username is not defined in the local group. • **line**—Specifies a method list that uses the line password for authentication.

Command Default

Default behavior applies the local authentication on all ports.

Command Modes

Global Configuration mode

Admin Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **aaa authentication** command to create a series of authentication methods, or method list. You can specify up to four methods in the method list. A *method list* is a named list describing the authentication methods (such as TACACS+ or RADIUS) in sequence. The subsequent methods of authentication are used only if the initial method is not available, not if it fails.

The default method list is applied for all interfaces for authentication, except when a different named method list is explicitly specified—in which case the explicitly specified method list overrides the default list.

For console and vty access, if no authentication is configured, a default of local method is applied.

Note

- The **group tacacs+**, **group radius**, and **group** *group-name* forms of this command refer to a set of previously defined TACACS+ or RADIUS servers.
- Use the **tacacs-server host** or **radius-server host** command to configure the host servers.
- Use the **aaa group server tacacs+** or **aaa group server radius** command to create a named subset of servers.
- The **login** keyword, **remote** keyword, **local** option, and **group** option are available only in administration configuration mode.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to specify the default method list for authentication, and also enable authentication for console in global configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa authentication login default group tacacs+
```

The following example shows how to specify the remote method list for authentication, and also enable authentication for console in administration configuration mode:

```
RP/0/RSP0/CPU0:router# admin
RP/0/RSP0/CPU0:router (admin)# configure
RP/0/RSP0/CPU0:router(admin-config)# aaa authentication login remote local group tacacs+
```

Related Commands

Command	Description
aaa accounting, on page 4	Creates a method list for accounting.
aaa authorization , on page 20	Creates a method list for authorization.
aaa group server radius, on page 32	Groups different RADIUS server hosts into distinct lists and distinct methods.

Command	Description
aaa group server tacacs+, on page 34	Groups different TACACS+ server hosts into distinct lists and distinct methods.
login authentication, on page 70	Enables AAA authentication for logins.
tacacs-server host, on page 158	Specifies a TACACS+ host.

aaa authentication subscriber

To create a method list for subscriber authentication, use the **aaa authentication subscriber** command in Global Configuration mode. To disable this subscriber authentication method, use the **no** form of this command.

aaa authentication subscriber {*list_name* | **default**} **group** {*server_group_name* | **diameter** | **radius**}

Syntax Description

default	Uses the listed authentication methods that follow this keyword as the default list of methods for authentication.
list-name	Represents the character string for the list name for AAA authentication.
group	Specifies the server-group.
diameter	Specifies the list of all DIAMETER peers.
radius	Specifies the list of all RADIUS hosts.
server_group_name	Specifies the server group name.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.
Release 5.3.0	The **diameter** keyword was added for DIAMETER protocol support in BNG.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
aaa	read, write

This is an example of configuring the **aaa authentication subscriber** command in the Global Configuration mode:

```
RP/0/RSP0/CPU0:router(config)# aaa authentication subscriber sub1 group sg1 group sg2
```

This example shows how to configure the **aaa authentication subscriber** command with DIAMETER protocol to carry subscriber authentication with DIAMETER protocol using NASREQ application:

```
RP/0/RSP0/CPU0:router(config)# aaa authentication subscriber default group diameter
```

Related Commands

Command	Description
aaa authorization subscriber, on page 28	Creates authorization-related configurations

aaa authorization

To create a method list for authorization, use the **aaa authorization** command in Global Configuration mode. To disable authorization for a function, use the **no** form of this command.

aaa authorization { **commands** | **eventmanager** | **exec** | **network** | **subscriber** | **nacm** } { **default** *list-name* } { **none** | **local** | **prefer-external** | **only-external** | **group** { **tacacs** + | **radius** *group-name* } }

Syntax Description

commands	Configures authorization for all EXEC shell commands.
eventmanager	Applies an authorization method for authorizing an event manager (fault manager).
exec	Configures authorization for an interactive (EXEC) session.
network	Configures authorization for network services, such as PPP or Internet Key Exchange (IKE).
subscriber	Sets the authorization lists for the subscriber.
nacm	Enables the nacm functionality.
default	Uses the listed authorization methods that follow this keyword as the default list of methods for authorization.
list-name	Character string used to name the list of authorization methods.
none	Uses no authorization. If you specify **none**, no subsequent authorization methods is attempted. However, the task ID authorization is always required and cannot be disabled.
local	Uses local authorization. While this method of authorization is already supported, it is available for command authorization only from Cisco IOS XR Software Release 7.5.1 and later.
prefer-external	Adds the external group names to the list of local group names to determine the access control rules.
only-external	Uses the external group names to determine the access control rules.
group tacacs+	Uses the list of all configured TACACS+ servers for authorization.
group radius	Uses the list of all configured RADIUS servers for authorization. This method of authorization is not available for command authorization.
group *group-name*	Uses a named subset of TACACS+ or RADIUS servers for authorization as defined by the **aaa group server tacacs+** or **aaa group server radius** command.

Command Default

Authorization is disabled for all actions (equivalent to the method **none** keyword).

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 7.5.1	The command was modified to make the **local** option available for command authorization as well.
Release 7.4.1	NACM **prefer-external** and **only-external** keywords are introduced.
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **aaa authorization** command to create method lists defining specific authorization methods that can be used on a per line or a per interface basis. You can specify up to four methods in the method list.

Note NACM authorization cannot be configured on a per line or a per interface basis.

Note The NACM authorization mentioned here applies to the one performed by an external AAA server and *not* for task-based authorization.

Method lists for authorization define the ways authorization will be performed and the sequence in which these methods will be performed. A method list is a named list describing the authorization methods (such as TACACS+), in sequence. Method lists enable you to designate one or more security protocols for authorization, thus ensuring a backup system in case the initial method fails. Cisco IOS XR software uses the first method listed to authorize users for specific network services; if that method fails to respond, Cisco IOS XR software selects the next method listed in the method list. This process continues until there is successful communication with a listed authorization method or until all methods defined have been exhausted.

Note Cisco IOS XR software attempts authorization with the next listed method only when there is no response (not a failure) from the previous method. If authorization fails at any point in this cycle—meaning that the security server or local username database responds by denying the user services—the authorization process stops and no other authorization methods are attempted.

The Cisco IOS XR software supports the following methods for authorization:

- **none—**The router does not request authorization information; authorization is not performed over this line or interface.
- **local—**Use the local database for authorization.
- **prefer-external—**Use the external database for authorization. The external group names are added to the list of local group names list to determine the access control rules. External group names are preferred from the list. If the option is not mentioned, the local group names are preferred from the list.
- **only-external—**Use only external group names to determine the access control rules.
- **group tacacs+—**Use the list of all configured TACACS+ servers for authorization.
- **group radius—**Use the list of all configured RADIUS servers for authorization.
- **group group-name—**Uses a named subset of TACACS+ or RADIUS servers for authorization.

Note The group RADIUS is not applicable to NACM and command authorizations.

Method lists are specific to the type of authorization being requested. Cisco IOS XR software supports four types of AAA authorization:

- **Commands authorization—**Applies to the EXEC mode commands a user issues. Command authorization attempts authorization for all EXEC mode commands.

Note "Command" authorization is distinct from "task-based" authorization, which is based on the task profile established during authentication.

- **EXEC authorization—**Applies authorization for starting an EXEC session.

Note The **exec** keyword is no longer used to authorize the fault manager service. The **eventmanager** keyword (fault manager) is used to authorize the fault manager service. The **exec** keyword is used for EXEC authorization.

- **Network authorization—**Applies authorization for network services, such as IKE.
- **Event manager authorization—**Applies an authorization method for authorizing an event manager (fault manager). You are allowed to use TACACS+ or LOCAL.

Note The **eventmanager** keyword (fault manager) replaces the **exec** keyword to authorize event managers (fault managers).

When you create a named method list, you are defining a particular list of authorization methods for the indicated authorization type. When defined, method lists must be applied to specific lines or interfaces before any of the defined methods are performed.

To know more about command authorization using local user account feature which was introduced in Cisco IOS XR Software Release 7.5.1, see the *Configuring AAA Services* chapter in the *System Security Configuration Guide for Cisco ASR 9000 Series Routers*.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to define the network authorization method list named listname1, which specifies that TACACS+ authorization is used:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa authorization commands listname1 group tacacs+
```

Examples

The following example shows how to enable the NACM authorization to use the external group names for determining the access control rules. NACM is disabled by default. To enable NACM, you must have `root-lr` or `aaa` write task privilege to enable or disable NACM.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa authorization nacm default only-external local
```

The following examples show how to configure command authorization using local user account:

```
Router#configure
Router(config)#aaa authorization commands default group tacacs+ local
Router(config)#commit
```

or

```
Router(config)#aaa authorization commands default local
Router(config)#commit
```

Related Commands

Command	Description
aaa accounting, on page 4	Creates a method list for accounting.

aaa authorization (System Admin-VM)

To create command rules and data rules on System Admin VM for user authorization, use the **aaa authorization** command in Admin Configuration mode. To delete the command rules and data rules, use the **no** form of this command.

aaa authorization { **cmdrules cmdrule** { *integer* | **range** *integer* } [{ **action** *action-type* | **command** *cmd-name* | **context** *context-name* | **group** *group-name* | **ops** *ops-type* }] | **commands group** { **none** | **tacacs** } | **datarules datarule** { *integer* | **range** *integer* } [{ **action** *action-type* | **context** *context-name* | **group** *group-name* | **keypath** *keypath-name* | **namespace** *namespace-string* | **ops** *ops-type* }] }

Syntax Description

cmdrules	Configures command rules.
cmdrule *integer*	Specifies the command rule number.
range *integer*	Specifies the range of the command rules or data rules to be configured.
action	Specifies whether users are permitted or not allowed to perform the operation specified for the **ops** keyword.
action-type	Specifies the action type for the command rule or data rule. Available options are: **accept**, **accept_log** and **reject**.
command *cmd-name*	Specifies the command to which the command rule applies. The command must be entered within double-quotes. Example, **get**.
context *context-name*	Specifies to which type of connection the command rule or data rule applies. The connection type can be netconf, cli, or xml.
group *group-name*	Specifies the group to which the command rule or data rule applies. Example, **admin-r**.
ops *ops-type*	Specifies whether the user has read, execute, or read and execute permissions for the command. Available options for command rules are: **r**, rx, and **x**. To know the available options for data rules, use a **?** after the **ops** keyword.
commands group	Sets the command authorization lists for server groups. Available options are **none** that specifies no authorization and **tacacs** that specifies use of the list of all tacacs+ hosts.
datarules	Configures data rules.
datarule *integer*	Specifies the data rule number.
keypath	Specifies the keypath of the data element. If you enter an asterisk '*' for keypath, it indicates that the command rule is applicable to all configuration data.

namespace	Enter asterisk "*" to indicate that the data rule is applicable for all namespace values.

Command Default

None

Command Modes

Admin Configuration mode

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines

From Cisco IOS XR Software Release 7.4.1 and later, the system internally maps the users configured on the XR VM to System Admin VM of the router, based on the task table of the user on the XR VM. With this feature, NETCONF and gRPC users can access the admin-related information on the router even if their user profiles do not exist on System Admin VM. For a sample configuration, see the example section.

For more details, see the *Configuring AAA Services* chapter in the *System Security Configuration Guide for Cisco ASR 9000 Series Routers*.

This example shows how to create a command rule:

```
sysadmin-vm:0_RP0#config
sysadmin-vm:0_RP0(config)#aaa authorization cmdrules cmdrule 10 action accept command "show
 platform" context cli group group1 ops rx
```

This example shows how to create a data rule:

```
sysadmin-vm:0_RP0#config
sysadmin-vm:0_RP0(config)#aaa authorization datarules datarule 20 action accept context cli
 group group10 keypath * namespace * ops rwx
```

This example shows how to configure a command rule for a NETCONF or gRPC session to allow read access for **admin-r** group users:

```
sysadmin-vm:0_RP0(config)#aaa authorization cmdrules cmdrule 6 context netconf command get
 group admin-r ops rx action accept
```

aaa authorization policy-intf

To configure authorization lists for DIAMETER policy interface (Gx interface), use the **aaa authorization policy-intf** command in Global Configuration mode. To remove the authorization lists for DIAMETER policy interface (Gx interface), use the **no** form of this command.

aaa authorization policy-if {*list-name* | **default**} **group** {*server-group-name* | **diameter**}

Syntax Description

list-name	Specifies the list name for AAA authorization.
default	Specifies default list name for AAA authorization.
group	Specifies the server-group.
server-group-name	Specifies the server-group name.
diameter	Specifies the list of all DIAMETER peers.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 5.3.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
aaa	read, write

This example shows how to configure authorization lists for DIAMETER policy interface (Gx interface) in BNG:

```
RP/0/RSP0/CPU0:router(config)# aaa authorization policy-intf default group diameter
```

Related Commands

Command	Description
aaa authorization prepaid, on page 27	Configures authorization lists for DIAMETER prepaid interface (Gy interface).

aaa authorization prepaid

To configure authorization lists for DIAMETER prepaid interface (Gy interface), use the **aaa authorization prepaid** command in Global Configuration mode. To remove the authorization lists for DIAMETER prepaid interface (Gy interface), use the **no** form of this command.

aaa authorization prepaid {*list-name* | **default**} **group** {*server-group-name* | **diameter**}

Syntax Description

list-name	Specifies the list name for AAA authorization.
default	Specifies default list name for AAA authorization.
group	Specifies the server-group.
server-group-name	Specifies the server-group name.
diameter	Specifies the list of all DIAMETER peers.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 5.3.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
aaa	read, write

This example shows how to configure authorization lists for DIAMETER prepaid interface (Gy interface) in BNG:

```
RP/0/RSP0/CPU0:router(config)# aaa authorization prepaid default group diameter
```

Related Commands

Command	Description
aaa authorization policy-intf, on page 26	Configures authorization lists for DIAMETER policy interface (Gx interface).

aaa authorization subscriber

To create authorization-related configurations, use the **aaa authorization subscriber** command in Global Configuration mode. To disable this subscriber authorization method, use the **no** form of this command.

aaa authorization subscriber {*list_name* | **default**} **group** {*server_group_name* | **diameter** | **radius**}

Syntax Description

default	Uses the listed authentication methods that follow this keyword as the default list of methods for authentication.
list-name	Represents the character string for the list name for AAA authorization.
group	Specifies the server-group.
diameter	Specifies the list of all DIAMETER peers.
radius	Specifies the list of all RADIUS hosts.
server_group_name	Specifies the server group name.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.
Release 5.3.0	The **diameter** keyword was added for DIAMETER protocol support in BNG.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
aaa	read, write

This is an example of configuring the **aaa authorization subscriber** command in the Global Configuration mode:

```
RP/0/RSP0/CPU0:router(config)# aaa authorization subscriber sub1 group sg1 group sg2
```

This example shows how to configure the **aaa authorization subscriber** command to carry subscriber authorization with DIAMETER protocol using NASREQ application:

```
RP/0/RSP0/CPU0:router(config)# aaa authorization subscriber default group diameter
```

Related Commands

Command	Description
aaa authentication subscriber, on page 18	Creates a method list for subscriber authentication.

aaa default-taskgroup

To specify a task group for both remote TACACS+ authentication and RADIUS authentication, use the **aaa default-taskgroup** command in Global Configuration mode. To remove this default task group, enter the **no** form of this command.

aaa default-taskgroup *taskgroup-name*

Syntax Description

taskgroup-name	Name of an existing task group.

Command Default

No default task group is assigned for remote authentication.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **aaa default-taskgroup** command to specify an existing task group for remote TACACS+ authentication.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to specify taskgroup1 as the default task group for remote TACACS+ authentication:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa default-taskgroup taskgroup1
```

aaa group server diameter (BNG)

To configure the named server group for DIAMETER, and to enter the server group sub-mode, use the **aaa group server diameter** command in Global Configuration mode. To remove the named server group for DIAMETER, use the **no** form of this command.

aaa group server diameter *server-group-name*

Syntax Description

server-group-name	Specifies the server-group name.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 5.3.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
aaa	read, write

This example shows how to configure the named server group for DIAMETER, and to enter the server group sub-mode in BNG:

```
RP/0/RSP0/CPU0:router(config)# aaa group server diameter GX_SG
```

aaa group server radius

To group different RADIUS server hosts into distinct lists, use the **aaa group server radius** command in Global Configuration mode. To remove a group server from the configuration list, enter the **no** form of this command.

aaa group server radius *group-name*

Syntax Description

group-name	Character string used to name the group of servers.

Command Default

This command is not enabled.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **aaa group server radius** command to group existing server hosts, which allows you to select a subset of the configured server hosts and use them for a particular service. A server group is used in conjunction with a global server-host list. The server group lists the IP addresses or hostnames of the selected server hosts.

Server groups can also include multiple host entries for the same server, as long as each entry has a unique identifier. The combination of an IP address and User Datagram Protocol (UDP) port number creates a unique identifier, allowing different ports to individually defined as RADIUS hosts providing a specific authentication, authorization, and accounting (AAA) service. In other words, this unique identifier enables RADIUS requests to be sent to different UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service, for example, accounting, the second host entry acts as an automatic switchover backup to the first host entry. Using this example, if the first host entry fails to provide accounting services, the network access server tries the second host entry on the same device for accounting services. The RADIUS host entries are tried in the order in which they are configured in the server group.

All members of a server group must be the same type, that is, RADIUS.

The server group cannot be named radius or tacacs.

This command enters server group configuration mode. You can use the server command to associate a particular RADIUS server with the defined server group.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows the configuration of an AAA group server named radgroup1, which comprises three member servers:

```
RP/0/RSP0/CPU0:router# configure
```

```
RP/0/RSP0/CPU0:router(config)# aaa group server radius radgroup1
RP/0/RSP0/CPU0:router(config-sg-radius)# server 10.0.0.5 auth-port 1700 acct-port 1701
RP/0/RSP0/CPU0:router(config-sg-radius)# server 10.0.0.10 auth-port 1702 acct-port 1703
RP/0/RSP0/CPU0:router(config-sg-radius)# server 10.0.0.20 auth-port 1705 acct-port 1706
```

Note If the **auth-port** *port-number* and **acct-port** *port-number* keywords and arguments are not specified, the default value of the *port-number* argument for the **auth-port** keyword is 1645 and the default value of the *port-number* argument for the **acct-port** keyword is 1646.

Related Commands

Command	Description
key (RADIUS), on page 67	Specifies the authentication and encryption key that is used between the router and the RADIUS daemon running on the RADIUS server.
radius source-interface(BNG), on page 96	Forces RADIUS to use the IP address of a specified interface or subinterface for all outgoing RADIUS packets.
retransmit (RADIUS), on page 100	Specifies the number of times a RADIUS request is resent to a server if the server is not responding or is responding slowly.
server (RADIUS), on page 104	Associates a RADIUS server with a defined server group.
server-private (RADIUS), on page 107	Configures the IP address of the private RADIUS server for the group server.
timeout (RADIUS), on page 173	Specifies the number of seconds the router waits for the RADIUS server to reply before retransmitting.
vrf (RADIUS), on page 188	Configures the Virtual Private Network (VPN) routing and forwarding (VRF) reference of an AAA RADIUS server group.

aaa group server tacacs+

To group different TACACS+ server hosts into distinct lists, use the **aaa group server tacacs+** command in Global Configuration mode. To remove a server group from the configuration list, enter the **no** form of this command.

aaa group server tacacs+ *group-name*

Syntax Description

group-name	Character string used to name a group of servers.

Command Default

This command is not enabled.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 5.3.0	IPv6 support was introduced on this command.

Usage Guidelines

The AAA server-group feature introduces a way to group existing server hosts. The feature enables you to select a subset of the configured server hosts and use them for a particular service.

The **aaa group server tacacs+** command enters server group configuration mode. The **server** command associates a particular TACACS+ server with the defined server group.

A *server group* is a list of server hosts of a particular type. The supported server host type is TACACS+ server hosts. A server group is used with a global server host list. The server group lists the IP addresses or hostnames of the selected server hosts.

The server group cannot be named radius or tacacs.

Note Group name methods refer to a set of previously defined TACACS+ servers. Use the **tacacs-server host** command to configure the host servers.

From Cisco IOS XR Software Release 7.4.1 and later, you can configure a hold-down timer for TACACS+ server. For details, see the **holddown-time** command.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows the configuration of an AAA group server named tacgroup1, which comprises three member servers:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa group server tacacs+ tacgroup1
RP/0/RSP0/CPU0:router(config-sg-tacacs)# server 192.168.200.226
RP/0/RSP0/CPU0:router(config-sg-tacacs)# server 192.168.200.227
RP/0/RSP0/CPU0:router(config-sg-tacacs)# server 192.168.200.228
```

Related Commands

Command	Description
aaa accounting, on page 4	Creates a method list for accounting.
aaa authentication , on page 15	Creates a method list for authentication.
aaa authorization , on page 20	Creates a method list for authorization.
server (TACACS+), on page 106	Specifies the host name or IP address of an external TACACS+ server.
tacacs-server host, on page 158	Specifies a TACACS+ host.

aaa intercept

To enable RADIUS-based Lawful Intercept (LI) feature on a router, use the **aaa intercept** command in Global Configuration mode. To disable RADIUS-based Lawful Intercept feature, use the **no** form of this command.

aaa intercept

Syntax Description

This command has no keywords or arguments.

Command Default

RADIUS-based Lawful Intercept feature is not enabled.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 4.3.0	This command was introduced.
Release 4.3.2	By default, Lawful Intercept (LI) is not a part of the Cisco IOS XR software. The LI package needs to be installed separately. So, this command is enabled only after installing and activating the asr9k-li-px.pie.

Usage Guidelines

To use **aaa intercept** command, you must install and activate the **asr9k-li-px.pie**.

Use the **aaa intercept** command to enable a RADIUS-Based Lawful Intercept solution on your router. Intercept requests are sent (through Access-Accept packets or CoA-Request packets) to the network access server (NAS) or the Layer 2 Tunnel Protocol (L2TP) access concentrator (LAC) from the RADIUS server. All data traffic going to, or from, a PPP or L2TP session is passed to a mediation device.

Task ID

Task ID	Operation
aaa	read, write
li	read

This example shows how to configure **aaa intercept** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa intercept
```

aaa password-policy

To define a AAA password security policy, use the **aaa password-policy** command in Global Configuration mode. To remove the AAA password security policy, use the **no** form of this command.

aaa password-policy *policy-name* {**min-length** *min-length* | **max-length** *max-length* | **special-char** *special-char* | **upper-case** *upper-case* | **lower-case** *lower-case* | **numeric** *numeric* | **lifetime** {**years** | **months** | **days** | **hours** | **minutes** | **seconds**} *lifetime* | **min-char-change** *min-char-change* | **authen-max-attempts** *authen-max-attempts* | **lockout-time** {**days** | **hours** | **minutes** | **seconds**} *lockout-time* | **warn-interval** { **years** | **months** | **days** | **hours** | **minutes** | **seconds** } | **restrict-old-time** { **years** | **months** | **days** } | **max-char-repetition** *max-char-repetition* | **restrict-old-count** *restrict-old-count* | **restrict-password-advanced** | **restrict-password-reverse** | **restrict-username** | **restrict-username-reverse** }

Syntax Description

policy-name	Specifies the name of the password, in characters.
min-length	Specifies the minimum length of the password, in integer.
max-length	Specifies the maximum length of the password, in integer.
special-char	Specifies the number of special characters allowed in the password policy, in integer.
upper-case	Specifies the number of upper case alphabets allowed in the password policy, in integer.
lower-case	Specifies the number of lower case alphabets allowed in the password policy, in integer.
numeric	Specifies the number of numerals allowed in the password policy, in integer.
lifetime	Specifies the maximum lifetime for the password, the value of which is specified in integer, as years, months, days, hours, minutes or seconds.
min-char-change	Specifies the number of character change required between subsequent passwords, in integer.
authen-max-attempts	Specifies, in integer, the maximum number of authentication failure attempts allowed for a user, in order to restrict users who authenticate with invalid login credentials.
lockout-time	Specifies, in integer, the duration (in days, hours, minutes or seconds) for which the user is locked out when he exceeds the maximum limit of authentication failure attempts allowed.
warn-interval	Specifies the amount of time to notify the user about an expiring password, the value of which is specified in integer, as years, months, days, hours, minutes or seconds.
restrict-old-time	Specifies, in integer, the amount of time for which an old password is considered as valid. The value is specified in years, months, or days.

max-char-repetition	Specifies the consecutive number of times a character can be repeated in a password.
restrict-old-count	Specifies the count for the number of old passwords that cannot be reused.
restrict-password-advanced	Specifies the advanced restrictions on a new password.
restrict-password-reverse	Restricts the new password from being the same as the reversed old password.
restrict-username	Restricts the use of an associated username as a password.
restrict-username-reverse	Restricts the usage of associated username reversed as a password.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 6.2.1	This command was introduced.

Usage Guidelines

AAA password security policy works as such for Cisco IOS XR platforms. Whereas, this feature is supported only on XR VM, for Cisco IOS XR 64 bit platforms.

For more details on the usage of each option of this command, refer the section on *AAA Password Security for FIPS Compliance* in *Configuring AAA Services* chapter in the *System Security Configuration Guide for Cisco ASR 9000 Series Routers*.

You must configure both **authen-max-attempts** and **lockout-time** in order for the lock out functionality to take effect.

The **min-char-change** option is effective only for password change through logon, and not for password change by configuration.

Use **username** command along with **password-policy** option, in the Global Configuration mode, to associate the password policy with a particular user.

When **warn-interval** is enabled and it expires, the user is prompted at login to change the password or has the option to skip. If **warn-interval** and **lifetime** have both expired, the user must change their password.

From Cisco IOS XR Software Release 7.2.1 and later, most of the options of the **aaa password-policy** command listed in the syntax above are applicable to user password as well as secret. Whereas, the options listed below are supported only for password, and not for secret:

- **max-char-repetition**
- **min-char-change**
- **restrict-password-reverse**
- **restrict-password-advanced**

This table lists the default, maximum and minimum values of various command variables:

Command Variables	Default Value	Maximum Value	Minimum Value
policy-name	None	253	1
max-length	253	253	2
min-length	2	253	2
special-char	0	253	0
upper-case	0	253	0
lower-case	0	253	0
numeric	0	253	0
For **lifetime** :			
years	0	99	1
months	0	11	1
days	0	30	1
hours	0	23	1
minutes	0	59	1
seconds	0	59	1
min-char-change	4	253	0
authen-max-attempts	0	24	1
For **lockout-time** :			
days	0	225	1
hours	0	23	1
minutes	0	59	1
seconds	0	59	1
For **warn-interval** :			
years	0	99	1
months	0	11	1
days	0	30	1
hours	0	23	1
minutes	0	59	1
seconds	0	59	1

Command Variables	Default Value	Maximum Value	Minimum Value
For **restrict-old-time** :			
years	0	99	1
months	0	11	1
days	0	30	1
max-char-repetition	0	5	2
restrict-old-count	0	10	1

Task ID

Task ID	Operation
aaa	read, write

This example shows how to define a AAA password security policy:

```
RP/0/RSP0/CPU0:router(config)#aaa password-policy test-policy
RP/0/RSP0/CPU0:router(config-aaa)#min-length 8
RP/0/RSP0/CPU0:router(config-aaa)#max-length 15
RP/0/RSP0/CPU0:router(config-aaa)#lifetime months 3
RP/0/RSP0/CPU0:router(config-aaa)#min-char-change 5
RP/0/RSP0/CPU0:router(config-aaa)#authen-max-attempts 3
RP/0/RSP0/CPU0:router(config-aaa)#lockout-time days 1
RP/0/RSP0/CPU0:router(config-aaa)#warn-interval months 2
RP/0/RSP0/CPU0:router(config-aaa)#restrict-old-time years 3
RP/0/RSP0/CPU0:router(config-aaa)#max-char-repetition 3
RP/0/RSP0/CPU0:router(config-aaa)#restrict-old-count 3
RP/0/RSP0/CPU0:router(config-aaa)#restrict-password-reverse
RP/0/RSP0/CPU0:router(config-aaa)#restrict-password-advanced
RP/0/RSP0/CPU0:router(config-aaa)#restrict-username
RP/0/RSP0/CPU0:router(config-aaa)#restrict-username-reverse
```

Related Commands

Command	Description
show aaa password-policy, on page 118	Displays the details of AAA password policy.
username, on page 178	

aaa radius attribute

To configure a format e encode string for particular interface or NAS-Port type and to create an AAA radius attribute format configuration, use the **aaa radius attribute** command in Global Configuration mode. To disable this AAA Radius attribute, use the **no** form of this command.

aaa radius attribute {**called-station-id** {**format** *format_name* | **type** *value*} | **calling-station-id** {**format** *format_name* | **type** *value*} | **nas-port** {**format e** *format_name* | **type** *value*} | **nas-port-id** {**format e** *format_name* | **type** *value*}}

Syntax Description

called-station-id	Specifies the AAA nas-port attribute.
calling-station-id	Specifies the AAA nas-port attribute.
nas-port	Specifies the AAA nas-port attribute.
nas-port-id	Specifies the AAA nas-port-id attribute.
format	Specifies the AAA nas-port attribute format.
e	Specifies the AAA format type.
format_name	Specifies a 32 character string representing the format to be used.
type	Specifies the AAA nas-port attribute format.
value	Specifies the Nas-Port-Type value to apply format string on. The nas port value ranges from 0-44.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
ip-services	read, write

This is an example of configuring the **aaa radius attribute** command in the Global Configuration mode:

```
RP/0/RSP0/CPU0:router(config)# aaa radius attribute format e red type 40
```

aaa service-accounting

To set accounting parameters for service, use the **aaa service-accounting** command in Global Configuration mode or Admin Configuration mode. To disable this behavior, use the **no** form of this command.

aaa service-accounting [{**extended** | **brief**}]

Syntax Description

extended	Sends extended service accounting records.
brief	Sends brief service accounting records.

Command Default

The default setting is **extended**.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

The **extended** keyword allows to report all the subscriber accounting identities and state attributes within all the service accounting records. While, the **brief** keyword allows to report only brief information about service accounting records without any parent accounting record details.

Task ID

Task ID	Operation
aaa	read, write

This example shows how to set service accounting parameters to send brief information about service accounting records:

```
RP/0/RSP0/CPU0:router(config)# aaa service-accounting brief
```

aaa server radius dynamic-author

To configure radius dynamic author server, use the**aaa server radius dynamic-author** command in Global Configuration mode or Admin Configuration mode. To disable this subscriber authentication method, use the **no** form of this command.

aaa server radius dynamic-author {**client** *hostname* | **ignore** {**server-key** | **session-key**} | **port** *port_number* | **server-key** {**0** | **7** | **line_number**}}

Syntax Description

session-key	Specifies that the session-key could be ignored.
client	Represents the CoA client configuration.
hostname	Specifies the hostname (IPv4 address or domain or IPv6 address)of the CoA client. IPv6 domain name is not supported.
ignore	Specifies the ignore options.
port	Specifies the CoA server port to listen on.
server-key	Sets the shared secret to verify client CoA requests.
port_number	Represents the port number and the value ranges from 1000 to 5000.
0	Specifies that the unencrypted key will follow.
7	Specifies that the encrypted key will follow.
line_number	Represents the unencrypted (cleartext) key.

Command Default

No default behavior or values

Command Modes

Global Configuration mode.

Command History

Release	Modification
Release 4.2.0	This command was introduced.
Release 4.2.1	The support for the keywords, **auth-key** and **ignore {session-key}** were removed.
Release 5.3.1	The command was modified to add IPv6 address support for **aaa server radius dynamic-author client** configuration, as part of RADIUS over IPv6 feature.

Usage Guidelines

If multiple session identification keys are present in the CoA request, an AND operation is performed such that all the keys participate in the session selection. That is, if the CoA request contains the Accounting-Session-ID attribute and a Framed-IP-Address, then these parameters must match on the targeted session. For example, if the Session-ID referenced is 00001111 and the Framed-IP-Address is 10.0.0.10, and

if the BNG is having a subscriber session with ID as 00001111 but with address as 10.10.10.1, then the session is not subjected to the CoA action. A CoA NACK is returned in this case.

Task ID

Task ID	Operation
aaa	read, write

```
RP/0/RSP0/CPU0:router(config)# aaa server radius dynamic-author ignore server-key
```

aaa radius attribute nas-port-type

To configure the AAA RADIUS attribute nas-port-type for a physical interface or a VLAN sub-interface, use the **aaa radius attribute nas-port-type** command in the interface configuration mode. To remove the configuration of nas-port-type from the interface or VLAN sub-interface, use the **no** form of this command.

aaa radius attribute nas-port-type {*value string*}

Syntax Description

value	The nas-port-type value for the interface or VLAN sub-interface. The range is from 0 to 44.
string	The nas-port-type name for the interface or VLAN sub-interface.

Command Default

None

Command Modes

Interface or VLAN sub-interface configuration

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

The permissible values for nas-port-type within the given range are 0 - 6, 9, 15 and 30 - 44.

Task ID

Task ID	Operation
aaa	read, write

This example shows how to configure the AAA RADIUS attribute, **nas-port-type** for each physical interface :

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface gigabitEthernet 0/0/0/0
RP/0/RSP0/CPU0:router(config-if)# aaa radius attribute nas-port-type 15
```

Related Commands

Command	Description
aaa radius attribute, on page 41	Configures a format e encode string for particular interface or NAS-Port type.

accounting (line)

To enable authentication, authorization, and accounting (AAA) accounting services for a specific line or group of lines, use the **accounting** command in line template configuration mode. To disable AAA accounting services, use the **no** form of this command.

accounting {**commands** | **exec**} {**default***list-name*}

Syntax Description

commands	Enables accounting on the selected lines for all EXEC shell commands.
exec	Enables accounting of EXEC session.
default	The name of the default method list, created with the **aaa accounting** command.
list-name	Specifies the name of a list of accounting methods to use. The list is created with the **aaa accounting** command.

Command Default

Accounting is disabled.

Command Modes

Line template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

After you enable the **aaa accounting** command and define a named accounting method list (or use the default method list) for a particular type of accounting, you must apply the defined lists to the appropriate lines for accounting services to take place. Use the **accounting** command to apply the specified method lists to the selected line or group of lines. If a method list is not specified this way, no accounting is applied to the selected line or group of lines.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to enable command accounting services using the accounting method list named *listname2* on a line template named *configure:*

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# line template configure
RP/0/RSP0/CPU0:router(config-line)# accounting commands listname2
```

Related Commands

Command	Description
aaa accounting, on page 4	Creates a method list for accounting.

accounting aaa list

To configure the subscriber accounting feature, use the **accounting aaa list** command in the dynamic template configuration mode. To disable this feature, use the **no** form of this command.

accounting aaa list {*method_list_name* | **default**} **type session** {**dual-stack-delay** *time* | **periodic-interval** *time*}

Syntax Description

method_list_name	Specifies the preconfigured method list name.
default	Specifies the default method list.
type	Specifies the type of accounting performed.
session	Applies the accounting to a session.
dual-stack-delay	Specifies the dual stack set delay wait in seconds.
time	Specifies the value of the dual stack delay time in seconds. The value ranges from 1-30.
periodic-interval	Specifies the periodic accounting interval in minutes.
time	Specifies the value of the periodic accounting interval in minutes. The value ranges from 1-65535.

Command Default

None

Command Modes

Dynamic template configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

Use the **dynamic-template** command to enter dynamic template configuration mode.

Task ID

Task ID	Operation
config-services	read, write

This is an example of configuring **accounting aaa list** command for periodic accounting interval of 456 minutes:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template
RP/0/RSP0/CPU0:router(config-dynamic-template)# type service s1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# accounting aaa list l1 type session
periodic-interval 456
```

accounting aaa list type service

To configure the service accounting feature, use the **accounting aaa list type service** command in the dynamic template configuration mode. To disable this feature, use the **no** form of this command.

accounting aaa list {*method_list_name* | **default**} **type service** [**periodic-interval** *time*]

Syntax Description

method_list_name	Specifies the pre-configured method list name.
default	Specifies the default method list.
type	Specifies the type of accounting performed.
service	Applies the accounting to a service.
periodic-interval	Specifies the periodic accounting interval in minutes.
time	Value of the periodic accounting interval in minutes. The range is from 1 to 65535.

Command Default

None

Command Modes

Dynamic template configuration

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

Use the **dynamic-template** command to enter dynamic template configuration mode.

Task ID

Task ID	Operation
config-services	read, write

This is an example of configuring service accounting for periodic accounting interval of 600 minutes:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template
RP/0/RSP0/CPU0:router(config-dynamic-template)# type service s1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# accounting aaa list l1 type service
periodic-interval 600
```

accounting prepaid

To configure accounting information for subscriber prepaid feature in BNG, use the **accounting prepaid** command in subscriber configuration mode. To remove this configuration, use the **no** form of this command.

accounting prepaid *name* [{**method-list authorization** *list-name* | **password** *password* | **quota-holding time** *quota-holding-time* | **quota-validity time** *quota-validity-time* | **threshold** {**time** *time-threshold* | **volume** *volume-threshold* } | **traffic** {**both** | **inbound** | **outbound**}}]

Syntax Description

name	Prepaid configuration name or default.
method-list	Specifies method list configuration.
authorization	Specifies authorization method list.
list-name	Name of the authorization method list.
password	Specifies the password to be used when placing prepaid authorization or re-authorization requests.
password	Password string.
quota-holding time	Specifies quota holding time.
quota-validity time	Specifies quota validity time.
quota-holding-time	Quota holding time, in seconds. The range is from 0 to 99000; the default is 100.
quota-validity-time	Quota validity time, in seconds. The range is from 0 to 99000; the default is 50.
threshold	Specifies the threshold configuration for prepaid feature.
time	Specifies the time threshold.
time-threshold	Time threshold, in seconds. The range is 0 to 4294967295; the default is 100.
volume	Specifies the volume threshold.

volume-threshold	Volume threshold, in bytes. The range is 0 to 4294967295; the default is 100.
traffic	Specifies the traffic direction to be considered while deriving the volume. The default is **inbound** .
both	Considers both inbound and outbound traffic while deriving the volume.
inbound	Considers inbound traffic while deriving the volume.
outbound	Considers outbound traffic while deriving the volume.

Command Default

None

Command Modes

Subscriber configuration

Command History

Release	Modification
Release 5.3.0	This command was introduced.

Usage Guidelines

To configure the authorization method list, the accounting network name must already be created using **aaa accounting network** command in global configuration mode.

Task ID

Task ID	Operation
config-services	read, write

This example shows how to configure accounting information for subscriber prepaid feature in BNG:

```
RP/0/RSP0/CPU0:router(config)# subscriber
RP/0/RSP0/CPU0:router(config-subscriber)# accounting prepaid feat1
RP/0/RSP0/CPU0:router(config-prepaid)# traffic both
```

authorization (line)

To enable authentication, authorization, and accounting (AAA) authorization for a specific line or group of lines, use the **authorization** command in line template configuration mode. To disable authorization, use the **no** form of this command.

authorization {**commands** | **exec** | **eventmanager**} {**default***list-name*}

Syntax Description

commands	Enables authorization on the selected lines for all commands.
exec	Enables authorization for an interactive (EXEC) session.
default	Applies the default method list, created with the **aaa authorization** command.
eventmanager	Sets eventmanager authorization method. This method is used for the embedded event manager.
list-name	Specifies the name of a list of authorization methods to use. If no list name is specified, the system uses the default. The list is created with the **aaa authorization** command.

Command Default

Authorization is not enabled.

Command Modes

Line template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

After you use the **aaa authorization** command to define a named authorization method list (or use the default method list) for a particular type of authorization, you must apply the defined lists to the appropriate lines for authorization to take place. Use the **authorization** command to apply the specified method lists (or, if none is specified, the default method list) to the selected line or group of lines.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to enable command authorization using the method list named *listname4* on a line template named *configure:*

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# line template configure
RP/0/RSP0/CPU0:router(config-line)# authorization commands listname4
```

Related Commands

Command	Description
aaa authorization , on page 20	Creates a method list for authorization.

clear tacacs counters

To clear AAA counters for all the TACACS+ servers in the system, use the **clear tacacs counters** command in the EXEC mode.

clear tacacs counters

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.5.4	This command was introduced.

Usage Guidelines

Use the **clear tacacs counters** command to clear all AAA counter statistics for all the TACACS+ server configured in the system.

Task ID

Task ID	Operations
aaa	read

Examples

The following is sample output from the **clear tacacs counters** command:

```
Router:ios# show tacacs counters
TACACS+ Server:   10.105.236.101/4010 [global]

  Authentication:
   10 requests, 4 accepts, 3 failure, 2 error, 1 timeout

  Exec Authorization:
   0 requests, 0 accepts, 0 denied, 0 error, 0 timeout

  Command Authorization:
   6 requests, 6 accepts, 0 denied, 0 error, 0 timeout

  Exec Accounting:
   0 requests, 0 accepts, 0 fail, 0 error, 0 timeout

  Command Accounting:
   6 requests, 6 accepts, 0 fail, 0 error, 0 timeout

TACACS+ Server:   10.105.236.101/2201 [private] vrf = default

  Authentication:
   0 requests, 0 accepts, 0 failure, 0 error, 0 timeout

  Exec Authorization:
   0 requests, 0 accepts, 0 denied, 0 error, 0 timeout
```

```
  Command Authorization:
   0 requests, 0 accepts, 0 denied, 0 error, 0 timeout

  Exec Accounting:
   0 requests, 0 accepts, 0 fail, 0 error, 0 timeout

  Command Accounting:
   0 requests, 0 accepts, 0 fail, 0 error, 0 timeout

Router:ios# clear tacacs counters
Router:ios# show tacacs counters
TACACS+ Server:   10.105.236.101/4010 [global]

  Authentication:
   0 requests, 0 accepts, 0 failure, 0 error, 0 timeout

  Exec Authorization:
   0 requests, 0 accepts, 0 denied, 0 error, 0 timeout

  Command Authorization:
   0 requests, 0 accepts, 0 denied, 0 error, 0 timeout

  Exec Accounting:
   0 requests, 0 accepts, 0 fail, 0 error, 0 timeout

  Command Accounting:
   0 requests, 0 accepts, 0 fail, 0 error, 0 timeout


TACACS+ Server:   10.105.236.101/2201 [private] vrf = default

  Authentication:
   0 requests, 0 accepts, 0 failure, 0 error, 0 timeout

  Exec Authorization:
   0 requests, 0 accepts, 0 denied, 0 error, 0 timeout

  Command Authorization:
   0 requests, 0 accepts, 0 denied, 0 error, 0 timeout

  Exec Accounting:
   0 requests, 0 accepts, 0 fail, 0 error, 0 timeout

  Command Accounting:
   0 requests, 0 accepts, 0 fail, 0 error, 0 timeout
```

deadtime (server-group configuration)

To configure the deadtime value at the RADIUS server group level, use the **deadtime** command in server-group configuration mode. To set deadtime to 0, use the **no** form of this command.

deadtime *minutes*

Syntax Description

minutes	Length of time, in minutes, for which a RADIUS server is skipped over by transaction requests, up to a maximum of 1440 (24 hours). The range is from 1 to 1440.

Command Default

Deadtime is set to 0.

Command Modes

Server-group configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

The value of the deadtime set in the server groups overrides the deadtime that is configured globally. If the deadtime is omitted from the server group configuration, the value is inherited from the primary list. If the server group is not configured, the default value of 0 applies to all servers in the group. If the deadtime is set to 0, no servers are marked dead.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example specifies a one-minute deadtime for RADIUS server group **group1** when it has failed to respond to authentication requests for the **deadtime** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa group server radius group1
RP/0/RSP0/CPU0:router(config-sg-radius)# server 10.1.1.1 auth-port 1645 acct-port 1646
RP/0/RSP0/CPU0:router(config-sg-radius)# server 10.2.2.2 auth-port 2000 acct-port 2001
RP/0/RSP0/CPU0:router(config-sg-radius)# deadtime 1
```

Related Commands

Command	Description
aaa group server tacacs+, on page 34	Groups different RADIUS server hosts into distinct lists and distinct methods.
radius-server dead-criteria time, on page 79	Forces one or both of the criteria that is used to mark a RADIUS server as dead.

Command	Description
radius-server deadtime(BNG), on page 83	Defines the length of time in minutes for a RADIUS server to remain marked dead.

description (AAA)

To create a description of a task group or user group during configuration, use the **description** command in task group configuration or user group configuration mode. To delete a task group description or user group description, use the **no** form of this command.

description *string*

Syntax Description

string	Character string describing the task group or user group.

Command Default

None

Command Modes

Task group configuration

User group configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **description** command inside the task or user group configuration submode to define a description for the task or user group, respectively.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows the creation of a task group description:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# taskgroup alpha
RP/0/RSP0/CPU0:router(config-tg)# description this is a sample taskgroup
```

The following example shows the creation of a user group description:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# usergroup alpha
RP/0/RSP0/CPU0:router(config-ug)# description this is a sample user group
```

Related Commands

Command	Description
taskgroup, on page 171	Accesses task group configuration mode and configures a task group by associating it with a set of task IDs.
usergroup, on page 176	Accesses user group configuration mode and configures a user group by associating it with a set of task groups.

group (AAA)

To add a user to a group, use the **group** command in username configuration mode. To remove the user from a group, use the **no** form of this command.

group {**root-system** | **root-lr** | **netadmin** | **sysadmin** | **operator** | **cisco-support** | **serviceadmin***group-name*}

Syntax Description

root-system	Adds the user to the predefined root-system group and provides access to commands included in the cisco-support group. Only users with root-system authority may use this option.
root-lr	Adds the user to the predefined root-lr group. Only users with root-system authority or root-lr authority may use this option.
netadmin	Adds the user to the predefined network administrators group.
sysadmin	Adds the user to the predefined system administrators group.
operator	Adds the user to the predefined operator group.
cisco-support	Adds the user to the predefined Cisco support personnel group. **Note** Starting from IOS XR 4.3.1 release, the cisco-support group is combined with the root-system group. This means a user who is part of the root-system group can also access commands that are included in the cisco-support group.
serviceadmin	Adds the user to the predefined service administrators group.
group-name	Adds the user to a named user group that has already been defined with the **usergroup** command.

Command Modes

Username configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 3.3.0	The root-system group includes privileges for cisco-support groupd.

Usage Guidelines

The predefined group root-system may be specified only by root-system users while configuring administration.

Use the **group** command in username configuration mode. To access username configuration mode, use the username, on page 178 command in global configuration mode.

If the **group** command is used in administration configuration mode, only root-system and cisco-support keywords can be specified.

The privileges associated with the cisco-support group are now included in the root-system group. The cisco-support group is no longer required to be used for configuration.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to assign the user group operator to the user named user1:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# username user1
RP/0/RSP0/CPU0:router(config-un)# group operator
```

Related Commands

Command	Description
password (AAA), on page 73	Creates a login password for a user.
usergroup, on page 176	Configures a user group and associates it with a set of task groups.
username, on page 178	Accesses username configuration mode, configures a new user with a username, and establishes a password and permissions for that user.

holddown-time (TACACS+)

To specify a duration for which an unresponsive TACACS+ server is to be marked as down, and not be used for sending further client requests for that duration, use the **holddown-time** command in various configuration modes. To disable this feature, use the **no** form of this command or configure the hold down timer value as zero.

holddown-time *time*

Syntax Description

time	Specifies the hold-down timer value, in seconds. The range is from 0 to 1200. Zero indicates that the hold-down timer feature is disabled.

Command Default

By default, the TACACS+ hold-down timer is disabled.

Command Modes

TACACS server

TACACS+ server group

TACACS+ private server

Command History

Release	Modification
Release 7.4.1	This command was introduced for Cisco IOS XR 64-bit platforms.
Release 6.8.1	This command was introduced for Cisco IOS XR 32-bit platforms.

Usage Guidelines

Note To set the hold-down timer at global level, use the **tacacs-server holddown-time** command in Global Configuration mode.

While selecting the timer at various configuration levels, the system gives preference to the one which is more specific to the server. That is, the server-level timer has the highest precedence, followed by server group-level and finally, the global-level.

Also, see the *Guidelines for Configuring Hold-Down Timer for TACACS+* section in the *Configuring AAA Services* chapter in the *System Security Configuration Guide for Cisco ASR 9000 Series Routers*.

Task ID

Task ID	Operations
aaa	read, write

Examples

This example shows how to mark an unresponsive TACACS+ server as being down, and not to use it for sending further client requests for a duration of 35 seconds:

```
Router(config)#tacacs-server host 10.105.236.102 port 2020
Router(config-tacacs-host)#holddown-time 35
```

This example shows how to set a hold-down timer at global level:

```
Router#configure
Router(config)#tacacs-server holddown-time 30
```

This example shows how to set a hold-down timer at server-group level:

```
Router#configure
Router(config)#aaa group server tacacs+ test-group
Router(config-sg-tacacs)#holddown-time 40
```

This example shows how to set a hold-down timer at private server level:

```
Router(config)#aaa group server tacacs+ test-group
Router(config-sg-tacacs)#server-private 10.105.236.109 port 2020
Router(config-sg-tacacs-private)#holddown-time 55
Router(config-sg-tacacs-private)#commit
```

Related Commands

Command	Description
aaa group server tacacs+, on page 34	Groups different TACACS+ server hosts into distinct lists.
server-private (TACACS+), on page 110	Configures the IP address of the private TACACS+ server for the group server.
tacacs-server host, on page 158	Configures a TACACS+ host server.

inherit taskgroup

To enable a task group to derive permissions from another task group, use the **inherit taskgroup** command in task group configuration mode.

inherit taskgroup {*taskgroup-name* | **netadmin** | **operator** | **sysadmin** | **cisco-support** | **root-lr** | **root-system** | **serviceadmin**}

Syntax Description

taskgroup-name	Name of the task group from which permissions are inherited.
netadmin	Inherits permissions from the network administrator task group.
operator	Inherits permissions from the operator task group.
sysadmin	Inherits permissions from the system administrator task group.
cisco-support	Inherits permissions from the cisco support task group.
root-lr	Inherits permissions from the root-lr task group.
root-system	Inherits permissions from the root system task group.
serviceadmin	Inherits permissions from the service administrators task group.

Command Default

None

Command Modes

Task group configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **inherit taskgroup** command to inherit the permissions (task IDs) from one task group into another task group. Any changes made to the taskgroup from which they are inherited are reflected immediately in the group from which they are inherited.

Task ID

Task ID	Operations
aaa	read, write

Examples

In the following example, the permissions of task group tg2 are inherited by task group tg1:

```
RP/0/RSP0/CPU0:router# configure
```

```
RP/0/RSP0/CPU0:router(config)# taskgroup tg1
RP/0/RSP0/CPU0:router(config-tg)# inherit taskgroup tg2
RP/0/RSP0/CPU0:router(config-tg)# end
```

inherit usergroup

To enable a user group to derive characteristics of another user group, use the **inherit usergroup** command in user group configuration mode.

inherit usergroup *usergroup-name*

Syntax Description

usergroup-name	Name of the user group from which permissions are to be inherited.

Command Default

None

Command Modes

User group configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Each user group is associated with a set of task groups applicable to the users in that group. A task group is defined by a collection of task IDs. Task groups contain task ID lists for each class of action. The task permissions for a user are derived (at the start of the EXEC or XML session) from the task groups associated with the user groups to which that user belongs.

User groups support inheritance from other user groups. Use the **inherit usergroup** command to copy permissions (task ID attributes) from one user group to another user group. The "destination" user group inherits the properties of the inherited group and forms a union of all task IDs specified in those groups. For example, when user group A inherits user group B, the task map of the user group A is a union of that of A and B. Cyclic inclusions are detected and rejected. User groups cannot inherit properties from predefined groups, such as root-system users, root-sdr users, netadmin users, and so on. Any changes made to the usergroup from which it is inherited are reflected immediately in the group from which it is inherited.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to enable the purchasing user group to inherit properties from the sales user group:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# usergroup purchasing
RP/0/RSP0/CPU0:router(config-ug)# inherit usergroup sales
```

Related Commands

Command	Description
description (AAA), on page 58	Creates a description of a task group in task group configuration mode, or creates a description of a user group in user group configuration mode.

Command	Description
taskgroup, on page 171	Configures a task group to be associated with a set of task IDs.
usergroup, on page 176	Configures a user group to be associated with a set of task groups.

key (RADIUS)

To specify the authentication and encryption key that is used between the router and the RADIUS daemon running on the RADIUS server, use the **key (RADIUS)** command in RADIUS server-group private configuration mode.

key {**0** *clear-text-key* | **7** *encrypted-keyclear-text-key*}

Syntax Description

0 *clear-text-key*	Specifies an unencrypted (cleartext) shared key.
7 *encrypted-key*	Specifies an encrypted shared key.
clear-text-key	Specifies an unencrypted (cleartext) user password.

Command Default

For submode **key** commands, the default is to use the **radius-server key** command in global configuration mode, if defined. If the global key is also not defined, the configuration is not complete.

Command Modes

RADIUS server-group private configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to set the encrypted key to anykey:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa group server radius group1
RP/0/RSP0/CPU0:router(config-sg-radius)# server-private 10.1.1.1 auth-port 300
RP/0/RSP0/CPU0:router(config-sg-radius-private)# key anykey
```

Related Commands

Command	Description
aaa group server tacacs+, on page 34	Groups different RADIUS server hosts into distinct lists.
radius-server key(BNG), on page 88	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.

Command	Description
retransmit (RADIUS), on page 100	Specifies the number of times a RADIUS request is resent to a server if the server is not responding or is responding slowly.
server-private (RADIUS), on page 107	Configures the IP address of the private RADIUS server for the group server.
timeout (RADIUS), on page 173	Specifies the number of seconds the router waits for the RADIUS server to reply before retransmitting.

key (TACACS+)

To specify an authentication and encryption key shared between the AAA server and the TACACS+ server, use the **key (TACACS+)** command in TACACS host configuration mode. To disable this feature, use the **no** form of this command.

key {**0** *clear-text-key* | **7** *encrypted-keyauth-key*}

Syntax Description

0 *clear-text-key*	Specifies an unencrypted (cleartext) shared key.
7 *encrypted-key*	Specifies an encrypted shared key.
auth-key	Specifies the unencrypted key between the AAA server and the TACACS+ server.

Command Default

None

Command Modes

TACACS host configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

The TACACS+ packets are encrypted using the key, and it must match the key used by the TACACS+ daemon. Specifying this key overrides the key set by the **tacacs-server key** command for this server only.

The key is used to encrypt the packets that are going from TACACS+, and it should match with the key configured on the external TACACS+ server so that the packets are decrypted properly. If a mismatch occurs, the result fails.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to set the encrypted key to anykey

```
RP/0/RSP0/CPU0:router(config)# tacacs-server host 209.165.200.226
RP/0/RSP0/CPU0:router(config-tacacs-host)# key anykey
```

Related Commands

Command	Description
tacacs-server host, on page 158	Specifies a TACACS+ host.
tacacs-server key, on page 161	Globally sets the authentication encryption key used for all TACACS+ communications between the router and the TACACS+ daemon.

login authentication

To enable authentication, authorization, and accounting (AAA) authentication for logins, use the **login authentication** command in line template configuration mode. To return to the default authentication settings, use the **no** form of this command.

login authentication {**default***list-name*}

Syntax Description

default	Default list of AAA authentication methods, as set by the **aaa authentication login** command.
list-name	Name of the method list used for authenticating. You specify this list with the **aaa authentication login** command.

Command Default

This command uses the default set with the **aaa authentication login** command.

Command Modes

Line template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

The **login authentication** command is a per-line command used with AAA that specifies the name of a list of AAA authentication methods to try at login.

Caution If you use a *list-name* value that was not configured with the **aaa authentication login** command, the configuration is rejected.

Entering the **no** form of the **login authentication** command has the same effect as entering the command with the **default** keyword.

Before issuing this command, create a list of authentication processes by using the **aaa authentication login** command.

Task ID

Task ID	Operations
aaa	read, write
tty-access	read, write

Examples

The following example shows that the default AAA authentication is used for the line template *template1*:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# line template template1
RP/0/RSP0/CPU0:router(config-line)# login authentication default
```

The following example shows that the AAA authentication list called *list1* is used for the line template *template2*:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# line template template2
RP/0/RSP0/CPU0:router(config-line)# login authentication list1
```

Related Commands

Command	Description
aaa authentication , on page 15	Creates a method list for authentication.

nacm enable-external-policies

To enable dynamic NETCONF Access Control Model (NACM) policy authorization on a router, use the **nacm enable-external-policies** command in the Global Configuration mode. To remove the configuration, use the **no** form of this command.

nacm enable-external-policies

Syntax Description

This command has no keywords or arguments.

Command Default

Disabled, by default.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 7.8.1	This command was introduced.

Usage Guidelines

If this configuration is not present, update the NACM policies manually on each router.

Task ID

Task ID	Operation
nacm	read, write

This example shows how to enable the dynamic NACM on a router.

```
Router#configure
Router(config)# nacm enable-external-policies
Router(config)# commit
```

password (AAA)

To create a login password for a user, use the **password** command in username configuration mode or line template configuration mode. To remove the password, use the **no** form of this command.

password {[**0**] | **7** *password*}

Syntax Description

0	(Optional) Specifies that an unencrypted clear-text password follows.
7	Specifies that an encrypted password follows.
password	Specifies the unencrypted password text to be entered by the user to log in, for example, “lab”. If encryption is configured, the password is not visible to the user. Can be up to 253 characters in length.

Command Default

The password is in unencrypted clear text.

Command Modes

Username configuration

Line template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

You can specify one of two types of passwords: encrypted or clear text.

When an EXEC process is started on a line that has password protection, the process prompts for the password. If the user enters the correct password, the process issues the prompt. The user can try three times to enter a password before the process exits and returns the terminal to the idle state.

Passwords are two-way encrypted and should be used for applications such as PPP that need decryptable passwords that can be decrypted.

Note The **show running-config** command always displays the clear-text login password in encrypted form when the **0** option is used.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to establish the unencrypted password *pwd1* for user. The output from the **show** command displays the password in its encrypted form.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# username user1
RP/0/RSP0/CPU0:router(config-un)# password 0 pwd1
RP/0/RSP0/CPU0:router(config-un)# commit
RP/0/RSP0/CPU0:router(config-un)# show running-config
Building configuration...
username user1
 password 7 141B1309
```

Related Commands

Command	Description
group (AAA), on page 59	Adds a user to a group.
usergroup, on page 176	Accesses user group configuration mode and configures a user group, associating it with a set of task groups.
username, on page 178	Accesses username configuration mode and configures a new user with a username, establishing a password and granting permissions for that user.
line	Enters line template configuration mode for the specified line template. For more information, see the Cisco IOS XR *System Management Command Reference.*

aaa display-login-failed-users

aaa display-login-failed-users

Syntax Description

This command has no keywords or arguments.

Command Default

Disabled, by default

Command Modes

Global configuration mode

Command History

Release	Modification
Release 7.10.1	The command was introduced to make the **display-login-failed-users** option available to display user ID for failed user login attempts.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
aaa	read, write

This example shows how to enable the functioanlity to display the username for a failed authentication:

```
Router#Configure
Router(config)# aaa display-login-failed-users
Router(config)#commit
```

radius-server attribute

To customize the selected radius attributes, use the **radius-server attribute** command in the Global Configuration mode. To disable the Radius server attribute, use the **no** form of this command.

radius-server attribute list *list_name* [**attribute** {*list* | **vendor-id** *value*}]

Syntax Description

list	Specifies a list of attributes that are used in conjunction with server-groups to accept or reject a list of attributes.
list_name	Specifies the list name.
attribute	Specifies a list of Radius attributes.
list	Specifies the list of comma-delimited Radius attributes.
vendor-id	Specifies the vendor-id of the RADIUS attribute.
value	Specifies the vendor-id value. The value ranges from 0 to 429496729.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
aaa	read, write

Examples

This is an example of configuring the **radius-server attribute** command in the Global Configuration mode:

```
RP/0/RSP0/CPU0:router(config)# radius-server attribute list list1
RP/0/RSP0/CPU0:router(config-attribute-filter)# attribute list_1
RP/0/RSP0/CPU0:router(config-attribute-filter)# radius-server attribute vendor-id 429
```

radius-server attribute 11 default direction inbound

To change the direction in which the Remote Authentication Dial In User Service (RADIUS) filter-ID attribute is applied, use the **radius-server attribute 11 default direction inbound** command in Global Configuration mode.

radius-server attribute 11 default direction inbound

Syntax Description

This command has no keywords or arguments.

Command Default

RADIUS filter-ID attribute is applied by default in the output direction of the corresponding subscriber interface.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 5.3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
ethernet-services	read, write

Example

This example shows how to change the direction of the RADIUS filter-ID attribute:

```
RP/0/RSP0/CPU0:router # configure
RP/0/RSP0/CPU0:router(config)# radius-server attribute 11 default direction inbound
```

radius-server dead-criteria

To configure the dead server detection criteria for a configured RADIUS server, use the **radius-server dead-criteria** command in the Global Configuration mode. To disable the Radius server dead-criteria, use the **no** form of this command.

radius-server dead-criteria {**time** *value* | **tries** *number_of_tries*}

Syntax Description

time	Specifies the minimum time that must elapse since a response was received from this RADIUS server.
value	Specifies the time in seconds. The value ranges from 1 to 120.
tries	Specifies the minimum number of transmissions (original attempts plus retransmits) to this RADIUS server.
number_of_tries	Specifies the number of tries. The range is from 1 to 100.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
aaa	read, write

Examples

This is an example of configuring the **radius-server dead-criteria** command with 100s time and 34 tries:

```
RP/0/RSP0/CPU0:router(config)#radius-server dead-criteria time 100
RP/0/RSP0/CPU0:router(config)#radius-server dead-criteria tries 34
```

radius-server dead-criteria time

To specify the minimum amount of time, in seconds, that must elapse from the time that the router last received a valid packet from the RADIUS server to the time the server is marked as dead, use the **radius-server dead-criteria time** command in Global Configuration mode mode. To disable the criteria that were set, use the **no** form of this command.

radius-server dead-criteria time *seconds*

Syntax Description

seconds	Length of time, in seconds. The range is from 1 to120 seconds. If the *seconds* argument is not configured, the number of seconds ranges from 10 to 60, depending on the transaction rate of the server. **Note** The time criterion must be met for the server to be marked as dead.

Command Default

If this command is not used, the number of seconds ranges from 10 to 60 seconds, depending on the transaction rate of the server.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Note If you configure the **radius-server dead-criteria time** command before the **radius-server deadtime** command, the **radius-server dead-criteria time** command may not be enforced.

If a packet has not been received since the router booted and there is a timeout, the time criterion is treated as though it were met.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to establish the time for the dead-criteria conditions for a RADIUS server to be marked as dead for the **radius-server dead-criteria time** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# radius-server dead-criteria time 5
```

Related Commands

Command	Description
radius-server dead-criteria tries, on page 81	Specifies the number of consecutive timeouts that must occur on the router before the RADIUS server is marked as dead.
radius-server deadtime(BNG), on page 83	Defines the length of time, in minutes, for a RADIUS server to remain marked dead.
show radius dead-criteria, on page 133	Displays information for the dead-server detection criteria.

radius-server dead-criteria tries

To specify the number of consecutive timeouts that must occur on the router before the RADIUS server is marked as dead, use the **radius-server dead-criteria tries** command in Global Configuration mode. To disable the criteria that were set, use the **no** form of this command.

radius-server dead-criteria *tries*

Syntax Description

tries Number of timeouts from 1 to 100. If the *tries* argument is not configured, the number of consecutive timeouts ranges from 10 to 100, depending on the transaction rate of the server and the number of configured retransmissions.

Note The tries criterion must be met for the server to be marked as dead.

Command Default

If this command is not used, the number of consecutive timeouts ranges from 10 to 100, depending on the transaction rate of the server and the number of configured retransmissions.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

If the server performs both authentication and accounting, both types of packet are included in the number. Improperly constructed packets are counted as though they were timeouts. All transmissions, including the initial transmit and all retransmits, are counted.

Note If you configure the **radius-server dead-criteria tries** command before the **radius-server deadtime** command, the **radius-server dead-criteria tries** command may not be enforced.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to establish the number of tries for the dead-criteria conditions for a RADIUS server to be marked as dead for the **radius-server dead-criteria tries** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# radius-server dead-criteria tries 4
```

Related Commands

Command	Description
radius-server dead-criteria time, on page 79	Defines the length of time in seconds that must elapse from the time that the router last received a valid packet from the RADIUS server to the time the server is marked as dead.
radius-server deadtime(BNG), on page 83	Defines the length of time, in minutes, for a RADIUS server to remain marked dead.
show radius dead-criteria, on page 133	Displays information for the dead-server detection criteria.

radius-server deadtime(BNG)

To improve RADIUS response times when some servers are unavailable and cause the unavailable servers to be skipped immediately, use the **radius-server deadtime** command in Global Configuration mode. To set deadtime to 0, use the **no** form of this command.

radius-server deadtime *minutes*

Syntax Description

minutes	Length of time, in minutes, for which a RADIUS server is skipped over by transaction requests, up to a maximum of 1440 (24 hours). The range is from 1 to 1440. The default value is 0.

Command Default

Dead time is set to 0.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

A RADIUS server marked as dead is skipped by additional requests for the duration of minutes unless all other servers are marked dead and there is no rollover method.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example specifies five minutes of deadtime for RADIUS servers that fail to respond to authentication requests for the **radius-server deadtime** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# radius-server deadtime 5
```

radius-server disallow null-username

To drop radius access-requests that has blank or no username, use the **radius-server disallow null-username** command in the Global Configuration mode. To disable the Radius server disallow null-username, use the **no** form of this command.

radius-server disallow null-username

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
aaa	read, write

Examples

This is an example of configuring the **radius-server disallow null-username** command in the Global Configuration mode:

```
RP/0/RSP0/CPU0:router(config)#radius-server disallow null-username
```

radius-server ipv4 dscp

To mark the dscp bit for the ipv4 packets, use the **radius-server ipv4 dscp** command in the Global Configuration mode. To disable the Radius server IPv4 dscp, use the **no** form of this command.

radius-server ipv4 dscp *value*

Syntax Description

value	Specifies the differentiated services codepoint value. The value ranges from 1 to 63.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
aaa	read, write

Examples

This is an example of configuring the **radius-server ipv4 dscp** command in the Global Configuration mode:

```
RP/0/RSP0/CPU0:router(config)#radius-server ipv4 dscp 34
```

radius-server host (BNG)

To specify a RADIUS server host, use the **radius-server host** command in Global Configuration mode. To delete the specified RADIUS host, use the **no** form of this command.

radius-server host *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

Syntax Description

ip-address	IP address of the RADIUS server host.
auth-port *port-number*	(Optional) Specifies the User Datagram Protocol (UDP) destination port for authentication requests; the host is not used for authentication if set to 0. If unspecified, the port number defaults to 1645.
acct-port *port-number*	(Optional) Specifies the UDP destination port for accounting requests; the host is not used for accounting if set to 0. If unspecified, the port number defaults to 1646.
timeout *seconds*	(Optional) The time interval (in seconds) that the router waits for the RADIUS server to reply before retransmitting. This setting overrides the global value of the **radius-server timeout** command. If no timeout value is specified, the global value is used. Enter a value in the range from 1 to 1000. Default is 5.
retransmit *retries*	(Optional) The number of times a RADIUS request is re-sent to a server, if that server is not responding or is responding slowly. This setting overrides the global setting of the **radius-server retransmit** command. If no retransmit value is specified, the global value is used. Enter a value in the range from 1 to 100. Default is 3.
key *string*	(Optional) Specifies the authentication and encryption key used between the router and the RADIUS server. This key overrides the global setting of the **radius-server key** command. If no key string is specified, the global value is used. The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the **radius-server host** command syntax. This is because the leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.

Command Default

No RADIUS host is specified; use global **radius-server** command values.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.2.0	This command was supported on BNG.
Release 5.3.1	The command was modified to add IPv6 address support for the RADIUS server host configuration.

Usage Guidelines

You can use multiple **radius-server host** commands to specify multiple hosts. The Cisco IOS XR software searches for hosts in the order in which you specify them.

If no host-specific timeout, retransmit, or key values are specified, the global values apply to each host.

Task ID

Task ID	Operations
aaa	read, write

Examples

This example shows how to establish the host with IP address 172.29.39.46 as the RADIUS server, use ports 1612 and 1616 as the authorization and accounting ports, set the timeout value to 6, set the retransmit value to 5, and set “rad123” as the encryption key, matching the key on the RADIUS server:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# radius-server host 172.29.39.46 auth-port 1612 acct-port
1616 timeout 6 retransmit 5 key rad123
```

To use separate servers for accounting and authentication, use the zero port value as appropriate.

Related Commands

Command	Description
aaa accounting subscriber	Creates a method list for accounting.
aaa authentication subscriber	Creates a method list for authentication.
aaa authorization subscriber	Creates a method list for authorization.
radius-server key(BNG), on page 88	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
radius-server retransmit(BNG), on page 91	Specifies how many times Cisco IOS XR software retransmits packets to a server before giving up.
radius-server timeout(BNG), on page 93	Sets the interval a router waits for a server host to reply.

radius-server key(BNG)

To set the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon, use the **radius-server key** command in Global Configuration mode. To disable the key, use the **no** form of this command.

radius-server key {**0** *clear-text-key* | **7** *encrypted-keyclear-text-key*}

Syntax Description

0 *clear-text-key*	Specifies an unencrypted (cleartext) shared key.
7 *encrypted-key*	Specifies a encrypted shared key.
clear-text-key	Specifies an unencrypted (cleartext) shared key.

Command Default

The authentication and encryption key is disabled.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

The key entered must match the key used on the RADIUS server. All leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to set the cleartext key to “samplekey”:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# radius-server key 0 samplekey
```

The following example shows how to set the encrypted shared key to “anykey”:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# radius-server key 7 anykey
```

Related Commands

Command	Description
key (RADIUS)	Specifies the authentication and encryption key that is used between the router and the RADIUS daemon running on the RADIUS server.
server-private (RADIUS), on page 107	Configures the IP address of the private RADIUS server for the group server.

radius-server load-balance

To configure the RADIUS load-balancing options, use the **radius-server load-balance** command in the Global Configuration mode. To disable the Radius server load-balance, use the **no** form of this command.

radius-server load-balance method least-outstanding [{**batch-size** *value* | **ignore-preferred-server**}]

Syntax Description

method	Specifies the method by which the next host will be picked.
least-outstanding	Picks the server with the least transactions outstanding.
batch-size	Specifies the batch size for the selection of the server.
value	Specifies the batch size value. The value ranges from 1 to 1500. The default is 25.
ignore-preferred-server	Disables the preferred server for this server group.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
aaa	read, write

Examples

This is an example of configuring the **radius-server load-balance** command in the Global Configuration mode:

```
RP/0/RSP0/CPU0:router(config)#radius-server load-balance method lead-outstanding batch-size
 25
RP/0/RSP0/CPU0:router(config)#radius-server load-balance method lead-outstanding batch-size
 ignore-preferred-server
```

radius-server retransmit(BNG)

To specify the number of times the Cisco IOS XR software retransmits a packet to a server before giving up, use the **radius-server retransmit** command in Global Configuration mode. To disable retransmission, use the **no** form of this command.

radius-server retransmit *retries*

Syntax Description

retries	Maximum number of retransmission attempts. The range is from 1 to 100. Default is 3.

Command Default

The RADIUS servers are retried three times, or until a response is received.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

The RADIUS client tries all servers, allowing each one to time out before increasing the retransmit count.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to specify a retransmit counter value of five times:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# radius-server retransmit 5
```

Related Commands

Command	Description
radius-server key(BNG), on page 88	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
retransmit (RADIUS)	Specifies the number of times a RADIUS request is resent to a server if the server is not responding or is responding slowly.
server-private (RADIUS), on page 107	Configures the IP address of the private RADIUS server for the group server.

radius-server source-port

To configure the NAS to use a total of 50 ports as the source ports for sending out RADIUS requests, use the **radius-server source-port** command in the Global Configuration mode. To disable the Radius server source-port, use the **no** form of this command.

radius-server source-port extended

Syntax Description

extended	Specifies that the source-port can be extended to 50.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

Having 200 source ports allows up to 256*200 authentication and accounting requests to be outstanding at one time. During peak call volume, typically when a router first boots or when an interface flaps, the extra source ports allow sessions to recover more quickly on large-scale aggregation platforms.

Task ID

Task ID	Operations
aaa	read, write

Examples

This is an example of configuring the **radius-server source-port** command in theGlobal Configuration mode:

```
RP/0/RSP0/CPU0:router(config)#radius-server source-port extended
```

radius-server timeout(BNG)

To set the interval for which a router waits for a server host to reply before timing out, use the **radius-server timeout** command in Global Configuration mode. To restore the default, use the **no** form of this command.

radius-server timeout *seconds*

Syntax Description

seconds	Number that specifies the timeout interval, in seconds. Range is from 1 to 1000.

Command Default

5 seconds

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **radius-server timeout** command to set the number of seconds a router waits for a server host to reply before timing out.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to change the interval timer to 10 seconds:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# radius-server timeout 10
```

Related Commands

Command	Description
radius-server key(BNG), on page 88	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
server-private (RADIUS), on page 107	Configures the IP address of the private RADIUS server for the group server.
timeout (RADIUS)	Specifies the number of seconds the router waits for the RADIUS server to reply before retransmitting.

radius-server throttle

To configure RADIUS throttling options for access and accounting to flow control the number of access and accounting requests sent to a RADIUS server, use the **radius-server throttle** command in the Global Configuration mode. To disable the radius server throttle, use the **no** form of this command.

radius-server throttle {**access** *value* {**access-timeout** *time* | **accounting** *value*} | **accounting** *acc_value*}

Syntax Description

access	Controls the number of access requests sent to a radius server.
value	Specifies the number of outstanding access requests after which throttling should be performed. The value ranges from 0 to 65535 and the preferred value 100.
access-timeout	Specifies the number of timeouts exceeding which a throttled access request is dropped.
time	Specifies the number of timeouts for a transaction. The default value is 3.
accounting	Controls the number of accounting requests sent to a radius server.
acc_value	Specifies the number of outstanding accounting transactions after which throttling should be performed. The value ranges from 0 to 65535 and the preferred value 100.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 4.2.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
aaa	read, write

This is an example of configuring the **radius-server throttle** command in the Global Configuration mode:

```
RP/0/RSP0/CPU0:router(config)# radius-server throttle access 10 access-timeout 5 accounting
 10
```

radius-server vsa attribute ignore unknown

To specify the unknown vsa ignore configuration for RADIUS server, use the **radius-server vsa attribute ignore unknown** command in the Global Configuration mode. To disable this feature, use the **no** form of this command.

radius-server vsa attribute ignore unknown

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
aaa	read, write

Examples

This is an example of configuring the **radius-server vsa attribute ignore unknown** command in the Global Configuration mode:

```
RP/0/RSP0/CPU0:router(config)#radius-server vsa attribute ignore unknown
```

radius source-interface(BNG)

To force RADIUS to use the IP address of a specified interface or subinterface for all outgoing RADIUS packets, use the **radius source-interface** command in Global Configuration mode. To prevent only the specified interface from being the default and not from being used for all outgoing RADIUS packets, use the **no** form of this command.

radius source-interface *interface-name* [**vrf** *vrf-id*]

Syntax Description

interface-name	Name of the interface that RADIUS uses for all of its outgoing packets.
vrf *vrf-id*	Specifies the name of the assigned VRF.

Command Default

If a specific source interface is not configured, or the interface is down or does not have an IP address configured, the system selects an IP address.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **radius source-interface** command to set the IP address of the specified interface or subinterface for all outgoing RADIUS packets. This address is used as long as the interface or subinterface is in the up state. In this way, the RADIUS server can use one IP address entry for every network access client instead of maintaining a list of IP addresses.

The specified interface or subinterface must have an IP address associated with it. If the specified interface or subinterface does not have an IP address or is in the down state, then RADIUS reverts to the default. To avoid this, add an IP address to the interface or subinterface or bring the interface to the up state.

The **radius source-interface** command is especially useful in cases in which the router has many interfaces or subinterfaces and you want to ensure that all RADIUS packets from a particular router have the same IP address.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to make RADIUS use the IP address of subinterface s2 for all outgoing RADIUS packets:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# radius source-interface Loopback 10 vrf vrf-1
```

Related Commands

Command	Description
aaa group server tacacs+, on page 34	Groups different RADIUS server hosts into distinct lists.
radius-server key(BNG), on page 88	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.

restrict-consecutive-characters

To restrict consecutive characters (that includes regular English alphabets, and English alphabets from QWERTY keyboard layout and numbers), for user passwords and secrets, use the **restrict-consecutive-characters** command in *aaa password-policy* configuration mode. To disable the feature, use the **no** form of the command.

restrict-consecutive-characters { **english-alphabet** | **qwerty-keyboard** } *num-of-chars* [**cyclic-wrap**]

Syntax Description

english-alphabet	Restricts consecutive English alphabets for user passwords and secrets. For example, "abcd", "wxyz", and so on.
qwerty-keyboard	Restricts consecutive English alphabets from QWERTY keyboard layout and numbers, for user passwords and secrets. For example, "qwer", "mnbv", "7890", and so on.
num-of-chars	Specifies the number of consecutive characters to be restricted for user passwords and secrets. Range is 2 to 26, for **english-alphabet**. Range is 2 to 10, for **qwerty-keyboard**.
cyclic-wrap	Restricts cyclic wrapping of the alphabet or the number for user passwords and secrets. For example, "yzab", "opqw", "9012", and so on.

Command Default

Disabled, by default.

Command Modes

aaa password-policy configuration mode

Command History

Release	Modification
Release 7.7.1	This command was introduced.

Usage Guidelines

All password policies are applicable only to locally configured users.

After creating the password policy, you must explicitly apply that policy to the user profiles to have an effect of that policy in the password and secret configuration.

For more details about the feature and configuration task, see the section *Enhanced Security for User Passwords and Secrets* in *Configuring AAA Services* chapter in the *System Security Configuration Guide for Cisco ASR 9000 Series Routers*.

Task ID

Task ID	Operation
aaa	read, write

This example shows how to configure a AAA password policy that restricts cyclic wrapping of 4 consecutive English alphabets and 6 consecutive characters from QWERTY keyboard.

```
Router(config)#aaa password-policy test-policy
Router(config-pp)#restrict-consecutive-characters english-alphabet 4 cyclic-wrap
Router(config-pp)#restrict-consecutive-characters qwerty-keyboard 6
```

This example shows how to apply the password policy to the user profile, *user1*:

```
Router(config)#username user1
Router(config-un)#policy test-policy
Router(config-un)#commit
```

Related Commands

Command	Description
aaa password-policy, on page 37	Defines the FIPS-compliant AAA password security policy.

retransmit (RADIUS)

To specify the number of times a RADIUS request is resent to a server if the server is not responding or is responding slowly, use the **retransmit** command in RADIUS server-group private configuration mode.

retransmit *retries*

Syntax Description

retries	The *retries* argument specifies the retransmit value. The range is from 1 to 100. If no retransmit value is specified, the global value is used.

Command Default

The default value is 3.

Command Modes

RADIUS server-group private configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to set the retransmit value:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa group server radius group1
RP/0/RSP0/CPU0:router(config-sg-radius)# server-private 10.1.1.1 auth-port 300
RP/0/RSP0/CPU0:router(config-sg-radius-private)# retransmit 100
```

Related Commands

Command	Description
aaa group server tacacs+, on page 34	Groups different RADIUS server hosts into distinct lists.
server-private (RADIUS), on page 107	Configures the IP address of the private RADIUS server for the group server.
timeout (RADIUS), on page 173	Specifies the number of seconds the router waits for the RADIUS server to reply before retransmitting.

secret

To configure an encrypted or clear-text password for the user, use the **secret** command in username configuration mode or line template configuration mode. To remove this configuration, use the **no** form of this command.

secret [{**0** [**enc-type** *enc-type-value*] | **5** | **8** | **9** | **10**}] *secret-login*

Syntax Description

0	(Optional) Specifies that an unencrypted (clear-text) password follows.
5	Specifies that an MD5-encrypted password (secret) follows.
8	(Optional) Specifies that SHA256-encrypted password follows.
9	(Optional) Specifies that scrypt-encrypted password follows.
10	(Optional) Specifies that SHA512-encrypted password follows.
secret-login	Configures the specified secret for the user. Can be clear text (for Type 0 secret) or text string in alphanumeric characters that is stored as encrypted password entered by the user in association with the user's login ID. Can be up to 253 characters in length. **Note** The characters entered must conform to the respective encryption standards.
enc-type	(Optional) Configures the encryption type for a password entered in clear text.
enc-type-value	Specifies the encryption type to be used. Prior to Release 6.3.1, the only supported value was 5. (See Release History and Usage Guidelines sections for the currently supported values).

Command Default

No password is specified.

Command Modes

Username configuration

Line template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 6.3.1	Added the support for Type 8 (SHA256) and Type 9 (scrypt) encryption for **secret** configuration on classic Cisco IOS XR (32-bit) operating system. Added the support for **enc-type** option under **secret 0** to specify the type of encryption for password entered in clear-text format.

Release	Modification
Release 7.0.1	Extended the support for Type 8 (SHA256) and Type 9 (scrypt) encryption for **secret** configuration on Cisco IOS XR 64-bit operating system as well. Added support for Type 10 (SHA512) encryption for **secret** configuration on Cisco IOS XR 64-bit operating system only.

Usage Guidelines

From Release 7.0.1 and later, Type 10 encryption is applied as the default encryption type for the **secret** on Cisco IOS XR 64-bit operating systems. Prior to this, Type 5 (MD5) was the default one.

Prior to Release 7.0.1, Cisco IOS XR software allows you to configure only Message Digest 5 (MD5) encryption for username logins and passwords. MD5 encryption is a one-way hash function that makes reversal of an encrypted password impossible, providing strong encryption protection. Using MD5 encryption, you cannot retrieve clear-text passwords. Therefore, MD5 encrypted passwords cannot be used with protocols that require the clear-text password to be retrievable, such as Challenge Handshake Authentication Protocol (CHAP).

When an EXEC process is started on a line that has password protection, the process prompts for the secret. If the user enters the correct secret, the process issues the prompt. The user can try entering the secret thrice before the terminal returns to the idle state.

Secrets are one-way encrypted and should be used for login activities that do not require a decryptable secret.

To verify that respective password encryption has been enabled, use the **show running-config** command. For example, if the command output shows “username name secret 5”, it means that enhanced password security with MD5 encryption is enabled.

Note The **show running-config** command does not display the login password in clear text when the **0** option is used to specify an unencrypted password. See the “Examples” section.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to establish the clear-text secret “lab” for the user *user2*:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# username user2
RP/0/RSP0/CPU0:router(config-un)# secret 0 lab
RP/0/RSP0/CPU0:router(config-un)# commit
RP/0/RSP0/CPU0:router(config-un)# show running-config
Building configuration...
username user2
 secret 5 $1$DTmd$q7C6fhzje7Cc7Xzmu2Frx1
!
end
```

The following examples show how to configure a Type 10 (SHA512) password for the user, *user10*. You can also see the examples and usage of the username, on page 178 command.

You can specify Type as '10' under the **secret** keyword, to explicitly configure Type 10 password.

```
Router#configure
Router(config)#username user10 secret 10
$6$9UvJidvsTEqgkAPU$3CL1Ei/F.E4v/Hi.UaqLwX8UsSEr9ApG6c5pzhMJmZtgW4jObAQ7meAwyhu5VM/aRFJqe/jxZG17h6xPrvJWf1
Router(config-un)#commit
```

You can also use the **enc-type** keyword under the **secret 0** option, to specify Type 10 as the encryption for a password entered in clear text.

```
Router#configure
Router(config)#username user10 secret 0 enc-type 10 testpassword
Router(config-un)#commit
```

Related Commands

Command	Description
group (AAA), on page 59	Adds a user to a group.
password (AAA), on page 73	Creates a login password for a user.
usergroup, on page 176	Accesses user group configuration mode and configures a user group, associating it with a set of task groups.
username, on page 178	Accesses username configuration mode and configures a new user with a username, establishing a password and granting permissions for that user.

server (RADIUS)

To associate a particular RADIUS server with a defined server group, use the **server** command in RADIUS server-group configuration mode. To remove the associated server from the server group, use the **no** form of this command.

server *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]

Syntax Description

ip-address	IP address of the RADIUS server host.
auth-port *port-number*	(Optional) Specifies the User Datagram Protocol (UDP) destination port for authentication requests. The *port-number* argument specifies the port number for authentication requests. The host is not used for authentication if this value is set to 0. Default is 1645.
acct-port *port-number*	(Optional) Specifies the UDP destination port for accounting requests. The *port-number* argument specifies the port number for accounting requests. The host is not used for accounting services if this value is set to 0. Default is 1646.

Command Default

If no port attributes are defined, the defaults are as follows:

- Authentication port: 1645
- Accounting port: 1646

Command Modes

RADIUS server-group configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **server** command to associate a particular RADIUS server with a defined server group.

There are two different ways in which you can identify a server, depending on the way you want to offer AAA services. You can identify the server simply by using its IP address, or you can identify multiple host instances or entries using the optional **auth-port** and **acct-port** keywords.

When you use the optional keywords, the network access server identifies RADIUS security servers and host instances associated with a group server based on their IP address and specific UDP port numbers. The combination of the IP address and UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS host entries providing a specific AAA service. If two different host entries on the same RADIUS server are configured for the same service, for example, accounting, the second host entry configured acts as an automatic switchover backup to the first one. Using this example, if the first host entry fails to provide accounting services, the network access server tries the second host entry configured on the same device for accounting services. (The RADIUS host entries are tried in the order they are configured.)

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to use two different host entries on the same RADIUS server that are configured for the same services—authentication and accounting. The second host entry configured acts as switchover backup to the first one.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa group server radius group1
RP/0/RSP0/CPU0:router(config-sg-radius)# server 10.1.1.1 auth-port 1645 acct-port 1646
RP/0/RSP0/CPU0:router(config-sg-radius)# server 10.2.2.2 auth-port 2000 acct-port 2001
```

Related Commands

Command	Description
aaa group server radius, on page 32	Groups different RADIUS server hosts into distinct lists and distinct methods.
deadtime (server-group configuration), on page 56	Configures the deadtime value at the RADIUS server group level.
server-private (RADIUS), on page 107	Configures the IP address of the private RADIUS server for the group server.

server (TACACS+)

To associate a particular TACACS+ server with a defined server group, use the **server** command in TACACS+ server-group configuration mode. To remove the associated server from the server group, use the **no** form of this command.

server {*hostnameip-address*}

Syntax Description

hostname	Character string used to name the server host.
ip-address	IP address of the server host.

Command Default

None

Command Modes

TACACS+ server-group configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **server** command to associate a particular TACACS+ server with a defined server group. The server need not be accessible during configuration. Later, you can reference the configured server group from the method lists used to configure authentication, authorization, and accounting (AAA).

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to associate the TACACS+ server with the IP address 192.168.60.15 with the server group tac1:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa group server tacacs+ tac1
RP/0/RSP0/CPU0:router(config-sg-tacacs+)# server 192.168.60.15
```

Related Commands

Command	Description
aaa group server tacacs+, on page 34	Groups different TACACS+ server hosts into distinct lists.

server-private (RADIUS)

To configure the IP address of the private RADIUS server for the group server, use the **server-private** command in RADIUS server-group configuration mode. To remove the associated private server from the AAA group server, use the **no** form of this command.

server-private *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

Syntax Description

ip-address	IP address of the RADIUS server host.
auth-port *port-number*	(Optional) Specifies the User Datagram Protocol (UDP) destination port for authentication requests. The *port-number* argument specifies the port number for authentication requests. The host is not used for authentication if this value is set to 0. The default value is 1645.
acct-port *port-number*	(Optional) Specifies the UDP destination port for accounting requests. The *port-number* argument specifies the port number for accounting requests. The host is not used for accounting services if this value is set to 0. The default value is 1646.
timeout *seconds*	(Optional) Specifies the number of seconds the router waits for the RADIUS server to reply before retransmitting. The setting overrides the global value of the **radius-server timeout** command. If no timeout is specified, the global value is used. The *seconds* argument specifies the timeout value in seconds. The range is from 1 to 1000. If no timeout is specified, the global value is used.
retransmit *retries*	(Optional) Specifies the number of times a RADIUS request is resent to a server if the server is not responding or is responding slowly. The setting overrides the global setting of the **radius-server transmit** command. The *retries* argument specifies the retransmit value. The range is from 1 to 100. If no retransmit value is specified, the global value is used.
key *string*	(Optional) Specifies the authentication and encryption key that is used between the router and the RADIUS daemon running on the RADIUS server. This key overrides the global setting of the **radius-server key** command. If no key string is specified, the global value is used.

Command Default

If no port attributes are defined, the defaults are as follows:

- Authentication port: 1645
- Accounting port: 1646

Command Modes

RADIUS server-group configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **server-private** command to associate a particular private server with a defined server group. Possible overlapping of IP addresses between VRF instances are permitted. Private servers (servers with private addresses) can be defined within the server group and remain hidden from other groups, while the servers in the global pool (for example, default radius server group) can still be referred to by IP addresses and port numbers. Thus, the list of servers in server groups includes references to the hosts in the configuration and the definitions of private servers.

Both the **auth-port** and **acct-port** keywords enter RADIUS server-group private configuration mode.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to define the group1 RADIUS group server, to associate private servers with it, and to enter RADIUS server-group private configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa group server radius group1
RP/0/RSP0/CPU0:router(config-sg-radius)# server-private 10.1.1.1 timeout 5
RP/0/RSP0/CPU0:router(config-sg-radius)# server-private 10.1.1.1 retransmit 3
RP/0/RSP0/CPU0:router(config-sg-radius)# server-private 10.1.1.1 key coke
RP/0/RSP0/CPU0:router(config-sg-radius)# server-private 10.1.1.1 auth-port 300
RP/0/RSP0/CPU0:router(config-sg-radius-private)# exit
RP/0/RSP0/CPU0:router(config-sg-radius)# server-private 10.2.2.2 timeout 5
RP/0/RSP0/CPU0:router(config-sg-radius)# server-private 10.2.2.2 retransmit 3
RP/0/RSP0/CPU0:router(config-sg-radius)# server-private 10.2.2.2 key coke
RP/0/RSP0/CPU0:router(config-sg-radius)# server-private 10.2.2.2 auth-port 300
RP/0/RSP0/CPU0:router(config-sg-radius-private)#
```

Related Commands

Command	Description
aaa group server tacacs+, on page 34	Groups different RADIUS server hosts into distinct lists and distinct methods.
radius-server key(BNG), on page 88	Sets the authentication and encryption key for all RADIUS communication between the router and the RADIUS daemon.
radius-server retransmit(BNG), on page 91	Specifies the number of times the Cisco IOS XR software retransmits a packet to a server before giving up.
radius-server timeout(BNG), on page 93	Sets the interval for which a router waits for a server host to reply before timing out.
key (RADIUS), on page 67	Specifies the authentication and encryption key that is used between the router and the RADIUS daemon running on the RADIUS server.
retransmit (RADIUS), on page 100	Specifies the number of times a RADIUS request is resent to a server if the server is not responding or is responding slowly.
timeout (RADIUS), on page 173	Specifies the number of seconds the router waits for the RADIUS server to reply before retransmitting.

Command	Description
vrf (RADIUS), on page 188	Configures the Virtual Private Network (VPN) routing and forwarding (VRF) reference of an AAA RADIUS server group.

server-private (TACACS+)

To configure the IP address of the private TACACS+ server for the group server, use the **server-private** command in TACACS+ server-group configuration mode. To remove the associated private server from the AAA group server, use the **no** form of this command.

server-private {*hostnameip-address*} [**holddown-time** *time*][**port** *port-number*] [**timeout** *seconds*] [**key** *string*]

Syntax Description

hostname	Character string used to name the server host.
ip-address	IP address of the TACACS+ server host. Both IPv4 and IPv6 addresses are supported.
holddown-time *time*	Specifies a duration, in seconds, for which an unresponsive TACACS+ server is to be marked as DOWN. The range is from 0 to 1200. Zero indicates that the hold-down timer feature is disabled.
port *port-number*	(Optional) Specifies a server port number. This option overrides the default, which is port 49. Valid port numbers range from 1 to 65535.
timeout *seconds*	(Optional) Specifies, in seconds, a timeout value that sets the length of time the authentication, authorization, and accounting (AAA) server waits to receive a response from the TACACS+ server. This option overrides the global timeout value set with the **tacacs-server timeout** command for only this server. The range is from 1 to 1000. The default is 5.
key *string*	(Optional) Specifies the authentication and encryption key that is used between the router and the TACACS+ daemon running on the TACACS+ server. This key overrides the global setting of the **tacacs-server key** command. If no key string is specified, the global value is used.

Command Default

The *port-name* argument, if not specified, defaults to the standard port 49.

The *seconds* argument, if not specified, defaults to 5 seconds.

Command Modes

TACACS+ server-group configuration

Command History

Release	Modification
Release 7.4.1	This command was modified for Cisco IOS XR 64-bit platforms to include **holddown-time** option.
Release 6.8.1	This command was modified for Cisco IOS XR 32-bit platforms to include **holddown-time** option.
Release 5.3.0	IPv6 support was introduced.
Release 4.1.0	This command was introduced.

Usage Guidelines

Use the **server-private** command to associate a particular private server with a defined server group. Possible overlapping of IP addresses between VRF instances are permitted. Private servers (servers with private addresses) can be defined within the server group and remain hidden from other groups, while the servers in the global pool (for example, default tacacs+ server group) can still be referred by IP addresses and port numbers. Therefore, the list of servers in server groups includes references to the hosts in the global configuration and the definitions of private servers.

For details on TACACS+ hold-down timer, see the **holddown-time** command.

Task ID

Task ID	Operations
aaa	read, write

Examples

This example shows how to define the myserver TACACS+ group server, to associate private servers with it, and to enter TACACS+ server-group private configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa group server tacacs+ myserver
RP/0/RSP0/CPU0:router(config-sg-tacacs+)# server-private 10.1.1.1 timeout 5
RP/0/RSP0/CPU0:router(config-sg-tacacs+)# server-private 10.1.1.1 key a_secret
RP/0/RSP0/CPU0:router(config-sg-tacacs+)# server-private 10.1.1.1 port 51
RP/0/RSP0/CPU0:router(config-sg-tacacs-private)# exit
RP/0/RSP0/CPU0:router(config-sg-tacacs+)# server-private 10.2.2.2 timeout 5
RP/0/RSP0/CPU0:router(config-sg-tacacs+)# server-private 10.2.2.2 key coke
RP/0/RSP0/CPU0:router(config-sg-tacacs+)# server-private 10.2.2.2 port 300
RP/0/RSP0/CPU0:router(config-sg-tacacs-private)#
```

Related Commands

Command	Description
aaa group server tacacs+, on page 34	Groups different TACACS+ server hosts into distinct lists and distinct methods.
tacacs-server key, on page 161	Sets the authentication encryption key used for all TACACS+ communications between the router and the TACACS+ daemon.
tacacs-server timeout, on page 163	Sets the interval for which a router waits for a server host to reply before timing out.
key (TACACS+), on page 69	Specifies an authentication and encryption key shared between the AAA server and the TACACS+ server.
timeout (TACACS+), on page 174	Specifies a timeout value that sets the length of time the authentication, authorization, and accounting (AAA) server waits to receive a response from the TACACS+ server.
vrf (TACACS+), on page 189	Configures the Virtual Private Network (VPN) routing and forwarding (VRF) reference of an AAA TACACS+ server group.

show aaa

To display information about an Internet Key Exchange (IKE) Security Protocol group, user group, local user, login traces, or task group; to list all task IDs associated with all IKE groups, user groups, local users, or task groups in the system; or to list all task IDs for a specified IKE group, user group, local user, or task group, use the **show aaa** command in EXEC mode.

show aaa {**ikegroup** *ikegroup-name* | **login trace** | **usergroup** [*usergroup-name*] | **trace** | **userdb** [*username*] | **task supported** | **taskgroup** [{**root-lr** | **netadmin** | **operator** | **sysadmin** | **root-system** | **service-admin** | **cisco-support** | *askgroup-name*}]}

Syntax Description

ikegroup	Displays details for all IKE groups.
ikegroup-name	(Optional) IKE group whose details are to be displayed.
login trace	Displays trace data for login subsystem.
usergroup	Displays details for all user groups.
root-lr	(Optional) Usergroup name.
netadmin	(Optional) Usergroup name.
operator	(Optional) Usergroup name.
sysadmin	(Optional) Usergroup name.
root-system	(Optional) Usergroup name.
cisco-support	(Optional) Usergroup name.
usergroup-name	(Optional) Usergroup name.
trace	Displays trace data for AAA subsystem.
userdb	Displays details for all local users and the usergroups to which each user belongs.
username	(Optional) User whose details are to be displayed.
task supported	Displays all AAA task IDs available.
taskgroup	Displays details for all task groups. **Note** For taskgroup keywords, see optional usergroup name keyword list.
taskgroup-name	(Optional) Task group whose details are to be displayed.

Command Default

Details for all user groups, or all local users, or all task groups are listed if no argument is entered.

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **show aaa** command to list details for all IKE groups, user groups, local users, or task groups in the system. Use the optional *ikegroup-name*, *usergroup-name*, *username*, or *taskgroup-name* argument to display the details for a specified IKE group, user group, user, or task group, respectively.

Task ID

Task ID	Operations
aaa	read

Examples

The following sample output is from the **show aaa** command, using the **ikegroup** keyword:

```
RP/0/RSP0/CPU0:router# show aaa ikegroup

IKE Group ike-group
        Max-Users = 50
IKE Group ikeuser
        Group-Key = test-password
        Default Domain = cisco.com
IKE Group ike-user
```

The following sample output is from the **show aaa** command, using the **usergroup** command:

```
RP/0/RSP0/CPU0:router# show aaa usergroup operator

User group 'operator'
  Inherits from task group 'operator'
User group 'operator' has the following combined set
of task IDs (including all inherited groups):
Task:       basic-services  : READ    WRITE    EXECUTE DEBUG
Task:                  cdp  : READ
Task:                 diag  : READ
Task:           ext-access  : READ             EXECUTE
Task:              logging  : READ
```

The following sample output is from the **show aaa** command, using the **taskgroup** keyword for a task group named netadmin:

```
RP/0/RSP0/CPU0:router# show aaa taskgroup netadmin

Task group 'netadmin'

Task group 'netadmin' has the following combined set
  of task IDs (including all inherited groups):

Task:                  aaa  : READ
Task:                  acl  : READ    WRITE    EXECUTE    DEBUG
Task:                admin  : READ
Task:                 ancp  : READ    WRITE    EXECUTE    DEBUG
Task:                  atm  : READ    WRITE    EXECUTE    DEBUG
Task:       basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:                bcdl  : READ
Task:                  bfd  : READ    WRITE    EXECUTE    DEBUG
Task:                  bgp  : READ    WRITE    EXECUTE    DEBUG
```

```
Task:                boot  : READ    WRITE    EXECUTE    DEBUG
Task:              bundle  : READ    WRITE    EXECUTE    DEBUG
Task:                 cdp  : READ    WRITE    EXECUTE    DEBUG
Task:                 cef  : READ    WRITE    EXECUTE    DEBUG
Task:                 cgn  : READ    WRITE    EXECUTE    DEBUG
Task:         config-mgmt  : READ    WRITE    EXECUTE    DEBUG
Task:     config-services  : READ    WRITE    EXECUTE    DEBUG
Task:              crypto  : READ    WRITE    EXECUTE    DEBUG
Task:                diag  : READ    WRITE    EXECUTE    DEBUG
Task:             drivers  : READ
Task:                dwdm  : READ    WRITE    EXECUTE    DEBUG
Task:                 eem  : READ    WRITE    EXECUTE    DEBUG
Task:               eigrp  : READ    WRITE    EXECUTE    DEBUG
Task:   ethernet-services  : READ
Task:          ext-access  : READ    WRITE    EXECUTE    DEBUG
Task:              fabric  : READ    WRITE    EXECUTE    DEBUG
Task:           fault-mgr  : READ    WRITE    EXECUTE    DEBUG
Task:          filesystem  : READ    WRITE    EXECUTE    DEBUG
Task:            firewall  : READ    WRITE    EXECUTE    DEBUG
Task:                  fr  : READ    WRITE    EXECUTE    DEBUG
Task:                hdlc  : READ    WRITE    EXECUTE    DEBUG
Task:       host-services  : READ    WRITE    EXECUTE    DEBUG
Task:                hsrp  : READ    WRITE    EXECUTE    DEBUG
Task:           interface  : READ    WRITE    EXECUTE    DEBUG
Task:           inventory  : READ
Task:         ip-services  : READ    WRITE    EXECUTE    DEBUG
Task:                ipv4  : READ    WRITE    EXECUTE    DEBUG
Task:                ipv6  : READ    WRITE    EXECUTE    DEBUG
Task:                isis  : READ    WRITE    EXECUTE    DEBUG
Task:               l2vpn  : READ    WRITE    EXECUTE    DEBUG
Task:                  li  : READ    WRITE    EXECUTE    DEBUG
Task:             logging  : READ    WRITE    EXECUTE    DEBUG
Task:                lpts  : READ    WRITE    EXECUTE    DEBUG
Task:             monitor  : READ
Task:           mpls-ldp  : READ    WRITE    EXECUTE    DEBUG
Task:         mpls-static  : READ    WRITE    EXECUTE    DEBUG
Task:             mpls-te  : READ    WRITE    EXECUTE    DEBUG
Task:           multicast  : READ    WRITE    EXECUTE    DEBUG
Task:             netflow  : READ    WRITE    EXECUTE    DEBUG
Task:             network  : READ    WRITE    EXECUTE    DEBUG
Task:                ospf  : READ    WRITE    EXECUTE    DEBUG
Task:                ouni  : READ    WRITE    EXECUTE    DEBUG
Task:             pkg-mgmt  : READ
Task:             pos-dpt  : READ    WRITE    EXECUTE    DEBUG
Task:                 ppp  : READ    WRITE    EXECUTE    DEBUG
Task:                 qos  : READ    WRITE    EXECUTE    DEBUG
Task:                 rib  : READ    WRITE    EXECUTE    DEBUG
Task:                 rip  : READ    WRITE    EXECUTE    DEBUG
Task:             root-lr  : READ                                (reserved)
Task:           route-map  : READ    WRITE    EXECUTE    DEBUG
Task:        route-policy  : READ    WRITE    EXECUTE    DEBUG
Task:                 sbc  : READ    WRITE    EXECUTE    DEBUG
Task:                snmp  : READ    WRITE    EXECUTE    DEBUG
Task:           sonet-sdh  : READ    WRITE    EXECUTE    DEBUG
Task:              static  : READ    WRITE    EXECUTE    DEBUG
Task:             sysmgr  : READ
Task:             system  : READ    WRITE    EXECUTE    DEBUG
Task:          transport  : READ    WRITE    EXECUTE    DEBUG
Task:          tty-access  : READ    WRITE    EXECUTE    DEBUG
Task:             tunnel  : READ    WRITE    EXECUTE    DEBUG
Task:          universal  : READ                                (reserved)
Task:               vlan  : READ    WRITE    EXECUTE    DEBUG
Task:               vrrp  : READ    WRITE    EXECUTE    DEBUG
```

The following sample output is from the **show aaa** command, using the **taskgroup** keyword for an operator. The task group operator has the following combined set of task IDs, which includes all inherited groups:

```
Task:       basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:                  cdp  : READ
Task:                 diag  : READ
Task:           ext-access  : READ             EXECUTE
Task:              logging  : READ
```

The following sample output is from the **show aaa** command, using the **taskgroup** keyword for a root system. The task-group root system has the following combined set of task IDs, which includes all inherited groups:

```
Task:                  aaa  : READ    WRITE    EXECUTE    DEBUG
Task:                  aaa acl  : READ    WRITE    EXECUTE    DEBUG
Task:                  acl admin  : READ    WRITE    EXECUTE    DEBUG
Task:                  admin atm  : READ    WRITE    EXECUTE    DEBUG
Task:                  atm basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:       basic-services           bcdl  : READ    WRITE    EXECUTE    DEBUG
Task:                 bcdl  bfd  : READ    WRITE    EXECUTE    DEBUG
Task:                  bfd bgp  : READ    WRITE    EXECUTE    DEBUG
Task:                  bgp boot  : READ    WRITE    EXECUTE    DEBUG
Task:                 boot bundle  : READ    WRITE    EXECUTE    DEBUG
Task:               bundle    cdp  : READ    WRITE    EXECUTE    DEBUG
Task:                  cdp cef  : READ    WRITE    EXECUTE    DEBUG
Task:                  cef config-mgmt  : READ    WRITE    EXECUTE    DEBUG
Task:          config-mgmt services  : READ    WRITE    EXECUTE    DEBUG
Task:      config-services           crypto  : READ    WRITE    EXECUTE    DEBUG
Task:                crypto   diag  : READ    WRITE    EXECUTE    DEBUG
Task:                  diag  drivers  : READ    WRITE    EXECUTE    DEBUG
Task:               drivers ext-access  : READ    WRITE    EXECUTE    DEBUG
Task:             ext-access     fabric  : READ    WRITE    EXECUTE    DEBUG
Task:                 fabric  fault-mgr  : READ    WRITE    EXECUTE    DEBUG
Task:              fault-mgr filesystem  : READ    WRITE    EXECUTE    DEBUG
Task:             filesystem         fr  : READ    WRITE    EXECUTE    DEBUG
Task:                    fr hdlc  : READ    WRITE    EXECUTE    DEBUG
Task:                  hdlc  host-services  : READ    WRITE    EXECUTE    DEBUG
Task:         host-services           hsrp  : READ    WRITE    EXECUTE    DEBUG
Task:                  hsrp  interface  : READ    WRITE    EXECUTE    DEBUG
Task:              interface inventory  : READ    WRITE    EXECUTE    DEBUG
Task:              inventory ip-services  : READ    WRITE    EXECUTE    DEBUG
Task:            ip-services         ipv4  : READ    WRITE    EXECUTE    DEBUG
Task:                  ipv4 ipv6  : READ    WRITE    EXECUTE    DEBUG
Task:                  ipv6 isis  : READ    WRITE    EXECUTE    DEBUG
Task:                  isis  logging  : READ    WRITE    EXECUTE    DEBUG
Task:                logging     lpts  : READ    WRITE    EXECUTE    DEBUG
Task:                  lpts  monitor  : READ    WRITE    EXECUTE    DEBUG
Task:                monitor mpls-ldp  : READ    WRITE    EXECUTE    DEBUG
Task:                mpls-ldp static  : READ    WRITE    EXECUTE    DEBUG
Task:                mpls-static te  : READ    WRITE    EXECUTE    DEBUG
Task:                mpls-te multicast  : READ    WRITE    EXECUTE    DEBUG
Task:                multicast netflow  : READ    WRITE    EXECUTE    DEBUG
Task:                netflow network  : READ    WRITE    EXECUTE    DEBUG
Task:                network     ospf  : READ    WRITE    EXECUTE    DEBUG
Task:                   ospf ouni  : READ    WRITE    EXECUTE    DEBUG
Task:                   ouni pkg-mgmt  : READ    WRITE    EXECUTE    DEBUG
Task:               pkg  pos-mgmt dpt  : READ    WRITE    EXECUTE    DEBUG
Task:                    ppp  : READ    WRITE    EXECUTE    DEBUG
Task:                    qos  : READ    WRITE    EXECUTE    DEBUG
Task:                    rib  : READ    WRITE    EXECUTE    DEBUG
Task:                    rip  : READ    WRITE    EXECUTE    DEBUG
```

```
Task:              root-lr  : READ    WRITE    EXECUTE    DEBUG
Task:          root-system  : READ    WRITE    EXECUTE    DEBUG
Task:            route-map  : READ    WRITE    EXECUTE    DEBUG
Task:         route-policy  : READ    WRITE    EXECUTE    DEBUG
Task:                 snmp  : READ    WRITE    EXECUTE    DEBUG
Task:            sonet-sdh  : READ    WRITE    EXECUTE    DEBUG
Task:               static  : READ    WRITE    EXECUTE    DEBUG
Task:               sysmgr  : READ    WRITE    EXECUTE    DEBUG
Task:               system  : READ    WRITE    EXECUTE    DEBUG
Task:            transport  : READ    WRITE    EXECUTE    DEBUG
Task:           tty-access  : READ    WRITE    EXECUTE    DEBUG
Task:               tunnel  : READ    WRITE    EXECUTE    DEBUG
Task:            universal  : READ    WRITE    EXECUTE    DEBUG
Task:                 vlan  : READ    WRITE    EXECUTE    DEBUG
Task:                 vrrp  : READ    WRITE    EXECUTE    DEBUG
```

The following sample output is from **show aaa** command with the **userdb** keyword:

```
RP/0/RSP0/CPU0:router# show aaa userdb

Username lab (admin plane)
User group root-system
User group cisco-support
Username acme
User group root-system
```

The following sample output is from the **show aaa** command, using the **task supported** keywords. Task IDs are displayed in alphabetic order.

```
RP/0/RSP0/CPU0:router# show aaa task supported

aaa
acl
admin
atm
basic-services
bcdl
bfd
bgp
boot
bundle
cdp
cef
cisco-support
config-mgmt
config-services
crypto
diag
disallowed
drivers
eigrp
ext-access
fabric
fault-mgr
filesystem
firewall
fr
hdlc
host-services
hsrp
interface
inventory
ip-services
```

```
ipv4
ipv6
isis
logging
lpts
monitor
mpls-ldp
mpls-static
mpls-te
multicast
netflow
network
ospf
ouni
pkg-mgmt
pos-dpt
ppp
qos
rib
rip
User group root-systemlr
root-system
route-map
route-policy
sbc
snmp
sonet-sdh
static
sysmgr
system
transport
tty-access
tunnel
universal
vlan
vrrp
```

Related Commands

Command	Description
show user, on page 150	Displays task IDs enabled for the currently logged-in user.

show aaa password-policy

To display the details of AAA password policy configured in a system, use the **show aaa password-policy** command in EXEC mode.

show aaa password-policy [*policy-name*]

Syntax Description

policy-name	Specifies the name of password policy.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.2.1	This command was introduced.
Release 7.2.1	This release introduces the following output: • Warning Interval • Restrict Old Time • Maximum Char Repetition • Restrict Old Count • Restrict Username • Restrict Username Reverse • Restrict Password Reverse • Restrict Password Advanced

Usage Guidelines

If the option *policy-name* is not specified, the command output displays the details of all password policies configured in the system.

Refer **aaa password-policy** command details of each field in this command output.

Task ID

Task ID	Operation
aaa	read

This is a sample out of **show aaa password-policy** command:

```
RP/0/RSP0/CPU0:router#show aaa password-policy test-policy

Fri Feb  3 16:50:58.086 EDT
Password Policy Name : test-policy
```

```
  Number of Users : 1
  Minimum Length : 2
  Maximum Length : 253
  Special Character Len : 0
  Uppercase Character Len : 0
  Lowercase Character Len : 1
  Numeric Character Len : 0
  Policy Life Time :
    seconds : 0
    minutes : 0
    hours : 0
    days : 0
    months : 0
    years : 0
 Warning Interval :
    seconds : 0
    minutes : 0
    hours : 0
    days : 0
    months : 2
    years : 0
Lockout Time :
    seconds : 0
    minutes : 0
    hours : 0
    days : 0
    months : 0
    years : 0
 Restrict Old Time :
    days : 0
    months : 0
    years : 3
Character Change Len : 4
Maximum Failure Attempts : 3
Reference Count : 0
Error Count : 0
Lockout Count Attempts : 0
Maximum char repetition : 3
Restrict Old count : 3
Restrict Username : 1
Restrict Username Reverse  : 1
Restrict Password Reverse  : 1
Restrict Password Advanced : 1
RP/0/RSP0/CPU0:ios#
```

Related Commands

Command	Description
aaa password-policy, on page 37	Defines the FIPS-compliant AAA password security policy.

show aaa trace

To display all trace data for AAA sub-system, use the **show aaa trace** command in the EXEC mode.

show aaa trace [{**basic** | **errors** | **file** | **func** | **hexdump** | **job** | **last** | **location** | **reverse** | **stats** | **tailf** | **unique** | **usec** | **verbose** | **wide** | **wrapping**}]

Syntax Description

basic	Displays the data for AAA basic events.
errors	Displays the data for AAA client library errors.
file	Displays the specific file.
func	Displays the data for AAA function.
hexdump	Displays the traces in hexadecimal.
job	Displays the job ID.
last	Displays the last n entries.
location	Displays the card location.
reverse	Displays the latest traces first.
stats	Displays the statistics.
tailf	Displays the new traces as they were added.
unique	Displays the unique entries with counts.
verbose	Displays the internal debugging information.
wrapping	Displays the wrapping entries.
|	Displays the output modifiers.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
aaa	read

This is the sample output of the **show aaa trace** command:

```
RP/0/RSP0/CPU0:router# show aaa trace func
Tue Jan 15 07:59:10.381 UTC
4 wrapping entries (1088 possible, 64 allocated, 0 filtered, 4 total)
Jan 15 06:11:00.958 aaa/func 0/RSP0/CPU0 t5  ENTERING aaa_connect2
Jan 15 06:11:00.962 aaa/func 0/RSP0/CPU0 t5  ENTERING get_unique_context
Jan 15 06:11:00.963 aaa/func 0/RSP0/CPU0 t5  EXITTING get_unique_context
Jan 15 06:11:00.963 aaa/func 0/RSP0/CPU0 t5  EXITTING aaa_connect2
```

show nacm (XR-VM)

To display information about NETCONF Access Control information such as users, groups, rule-lists and traces, use the **show nacm** command in Global Configuration mode. To disable authorization for a function, use the **no** form of this command.

show nacm {**summary** | | **users** [<*user-name*>] | | **groups** [<*group-name*>] | | **rule-list** [<*rule-list-name*> [| **rule** [<*rule-name*>]]] | | **trace**}

Syntax Description

summary	Displays NACM summary information.
Users	Displays list of users in NACM database.
user-name	Displays info for a given user-name.
groups	Displas list of groups in the NACM database.
group-name	Displays information for a given group name.
rule-list	Displays list of rule-lists in the NACM database.
rule-list-name	Displays info for given rule-list-name.
rule	Displays list of rules under the rule-list in the NACM database.
rule-name	Displays info for given rule-name under rule-name in the NACM database.
trace tacacs+	Displays NACM process traces.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 6.4.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
nacm	read

Examples

The following example shows how to use the show nacm command:

```
RP/0/RP0/CPU0:xr-nacm #show nacm summary
 NACM SUMMARY
```

```
 ------------------------------------------------------------------------------
 Enable Nacm : False
 Enable External Groups : True
 Number of Groups : 2
 Number of Users : 2
 Number of Rules : 2
 Number of Rulelist : 2
 Default Read : permit
 Default Write : permit
 Default Exec : permit
 Denied Operations : 0
 Denied Data Writes : 0
 Denied Notifications : 0
 ------------------------------------------------------------------------------
RP/0/RP0/CPU0:xr-nacm#
RP/0/RP0/CPU0:xr-nacm#show nacm users
USERS LIST:
------------------------------------------------------------------------------
lab,    admin,
------------------------------------------------------------------------------
RP/0/RP0/CPU0:xr-nacm#
RP/0/RP0/CPU0:xr-nacm#show nacm users lab

USER NAME: lab
------------------------------------------------------------------------------
Groups List For User:
root-lr,    root-system,
------------------------------------------------------------------------------

RP/0/RP0/CPU0:xr-nacm#


RP/0/RP0/CPU0:xr-nacm#show nacm groups

GROUPS LIST:
------------------------------------------------------------------------------
root-system,    root-lr,
------------------------------------------------------------------------------
RP/0/RP0/CPU0:xr-nacm#
RP/0/RP0/CPU0:xr-nacm#show nacm groups root-system

GROUP NAME: root-system
------------------------------------------------------------------------------
Users List:
admin,    lab,
Rules List:
rule-list-1,    rule-list-2,
------------------------------------------------------------------------------
RP/0/RP0/CPU0:xr-nacm#
RP/0/RP0/CPU0:xr-nacm#show nacm rule-list
RULELISTS:
------------------------------------------------------------------------------
   Rulelist Index       Rulelist Name
     rule-list-2        rule-list-2
     rule-list-1        rule-list-1
------------------------------------------------------------------------------
RP/0/RP0/CPU0:xr-nacm#
RP/0/RP0/CPU0:xr-nacm#show nacm rule-list rule-list-1,rule-list-1
RULELIST NAME: rule-list-1
------------------------------------------------------------------------------
   Rule Index              Rule Name
           rule1        rule1
           rule2        rule2
   Group List
```

```
root-system,    root-lr,
-------------------------------------------------------------------------------
RP/0/RP0/CPU0:xr-nacm#
RP/0/RP0/CPU0:xr-nacm#show nacm rule-list rule-list-1,rule-list-1 rule

Rule Info:
        Name:                   rule1
        Index:                  rule1
        Value:                  edit-config
        ModuleName:             *
        Action:                 permit
        RuleType:               Rpc
        Comment:
        AccessOperations:       All
        HitCount:               0
 -------------------------------------------------------------------------------
 Rule Info:
        Name:                   rule2
        Index:                  rule2
        Value:                  /nacm/rule-list
        ModuleName:             ietf-netconf-acm
        Action:                 deny
        RuleType:               Data
        Comment:
        AccessOperations:       Read,
        HitCount:               0
 -------------------------------------------------------------------------------
RP/0/RP0/CPU0:xr-nacm#
RP/0/RP0/CPU0:xr-nacm#show nacm rule-list rule-list-1,rule-list-1 rule rule2,rule2
RULELIST NAME: rule-list-1
 -------------------------------------------------------------------------------
Rule Info:
        Name:                   rule2
        Index:                  rule2
        Value:                  /nacm/rule-list
        ModuleName:             ietf-netconf-acm
        Action:                 deny
        RuleType:               Data
        Comment:
        AccessOperations:       Read,
        HitCount:               0
 -------------------------------------------------------------------------------
RP/0/RP0/CPU0:xr-nacm#
```

Related Commands

Command	Description
aaa accounting, on page 4	Creates a method list for accounting.

show radius

To display information about the RADIUS servers that are configured in the system, use the **show radius** command in EXEC mode.

show radius

Syntax Description

This command has no keywords or arguments.

Command Default

If no radius servers are configured, no output is displayed.

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **show radius** command to display statistics for each configured RADIUS server.

Task ID

Task ID	Operations
aaa	read

Examples

The following sample output is for the **show radius** command:

Output for IPV4 server

```
RP/0/RSP0/CPU0:router# show radius

Global dead time: 0 minute(s)
Number of Servers: 1

Server: 2.3.4.5/2000/2001  is UP
  Address family: IPv6
  Total Deadtime: 0s Last Deadtime: 0s
  Timeout: 5 sec, Retransmit limit: 3
  Quarantined: No
```

Output for IPV6 server

```
RP/0/RSP0/CPU0:router# show radius

Global dead time: 0 minute(s)
Number of Servers: 1

Server: 2001:b::2/2000/2001  is UP
  Address family: IPv6
  Total Deadtime: 0s Last Deadtime: 0s
  Timeout: 5 sec, Retransmit limit: 3
```

```
Quarantined: No
```

This table describes the significant fields shown in the display.

Table 2: show radius Field Descriptions

Field	Description
Server	Server IP address/UDP destination port for authentication requests/UDP destination port for accounting requests.
Timeout	Number of seconds the router waits for a server host to reply before timing out.
Retransmit limit	Number of times the Cisco IOS XR software searches the list of RADIUS server hosts before giving up.

Related Commands

Command	Description
vrf (RADIUS), on page 188	Configures the Virtual Private Network (VPN) routing and forwarding (VRF) reference of an AAA RADIUS server group.
radius-server retransmit(BNG), on page 91	Specifies how many times Cisco IOS XR software searches the list of RADIUS server hosts before giving up.
radius-server timeout(BNG), on page 93	Sets the interval for which a router waits for a server host to reply.

show radius accounting

To obtain information and detailed statistics for the RADIUS accounting server and port, use the **show radius accounting** command in EXEC mode.

show radius accounting

Syntax Description

This command has no keywords or arguments.

Command Default

If no RADIUS servers are configured on the router, the output is empty. If the default values are for the counter (for example, request and pending), the values are all zero because the RADIUS server was just defined and not used yet.

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
aaa	read

Examples

The following sample output is displayed on a per-server basis for the **show radius accounting** command:

```
RP/0/RSP0/CPU0:router# show radius accounting

Server: 12.26.25.61, port: 1813
0 requests, 0 pending, 0 retransmits
0 responses, 0 timeouts, 0 bad responses
0 bad authenticators, 0 unknown types, 0 dropped
0 ms latest rtt

Server: 12.26.49.12, port: 1813
0 requests, 0 pending, 0 retransmits
0 responses, 0 timeouts, 0 bad responses
0 bad authenticators, 0 unknown types, 0 dropped
0 ms latest rtt

Server: 12.38.28.18, port: 29199
0 requests, 0 pending, 0 retransmits
0 responses, 0 timeouts, 0 bad responses
0 bad authenticators, 0 unknown types, 0 dropped
0 ms latest rtt
```

This table describes the significant fields shown in the display.

Table 3: show radius accounting Field Descriptions

Field	Description
Server	Server IP address/UDP destination port for authentication requests; UDP destination port for accounting requests.

Related Commands

Command	Description
aaa accounting, on page 4	Creates a method list for accounting.
aaa authentication , on page 15	Creates a method list for authentication.
show radius authentication, on page 129	Obtains information and detailed statistics for the RADIUS authentication server and port.

show radius authentication

To obtain information and detailed statistics for the RADIUS authentication server and port, use the **show radius authentication** command in EXEC mode.

show radius authentication

Syntax Description

This command has no keywords or arguments.

Command Default

If no RADIUS servers are configured on the router, the output is empty. If the default values are for the counter (for example, request and pending), the values are all zero because the RADIUS server was just defined and not used yet.

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
aaa	read

Examples

The following sample output is for the **show radius authentication** command:

```
RP/0/RSP0/CPU0:router# show radius authentication

Server: 12.26.25.61, port: 1812
0 requests, 0 pending, 0 retransmits
0 accepts, 0 rejects, 0 challenges
0 timeouts, 0 bad responses, 0 bad authenticators
0 unknown types, 0 dropped, 0 ms latest rtt

Server: 12.26.49.12, port: 1812
0 requests, 0 pending, 0 retransmits
0 accepts, 0 rejects, 0 challenges
0 timeouts, 0 bad responses, 0 bad authenticators
0 unknown types, 0 dropped, 0 ms latest rtt

Server: 12.38.28.18, port: 21099
0 requests, 0 pending, 0 retransmits
0 accepts, 0 rejects, 0 challenges
0 timeouts, 0 bad responses, 0 bad authenticators
0 unknown types, 0 dropped, 0 ms latest rtt
```

This table describes the significant fields shown in the display.

Table 4: show radius authentication Field Descriptions

Field	Description
Server	Server IP address/UDP destination port for authentication requests; UDP destination port for accounting requests.

Related Commands

Command	Description
aaa accounting, on page 4	Creates a method list for accounting.
aaa authentication , on page 15	Creates a method list for authentication.
show radius accounting, on page 127	Obtains information and detailed statistics for the RADIUS accounting server and port.

show radius client

To obtain general information about the RADIUS client on Cisco IOS XR software, use the **show radius client** command in EXEC mode.

show radius client

Syntax Description

This command has no keywords or arguments.

Command Default

The default value for the counters (for example, an invalid address) is 0. The network access server (NAS) identifier is the hostname that is defined on the router.

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

The **show radius client** command displays the authentication and accounting responses that are received from the invalid RADIUS servers, for example, unknown to the NAS. In addition, the **show radius client** command displays the hostname or NAS identifier for the RADIUS authentication client, accounting client, or both.

Task ID

Task ID	Operations
aaa	read

Examples

The following sample output is for the **show radius client** command:

```
RP/0/RSP0/CPU0:router# show radius client

Client NAS identifier:                          miniq
Authentication responses from invalid addresses:      0
Accounting responses from invalid addresses:          0
```

This table describes the significant fields shown in the display.

Table 5: show radius client Field Descriptions

Field	Description
Client NAS identifier	Identifies the NAS-identifier of the RADIUS authentication client.

Related Commands

Command	Description
server (RADIUS), on page 104	Associates a particular RADIUS server with a defined server group.

Command	Description
show radius, on page 125	Displays information about the RADIUS servers that are configured in the system.

show radius dead-criteria

To obtain information about the dead server detection criteria, use the **show radius dead-criteria** command in EXEC mode.

show radius dead-criteria host *ip-addr* [**auth-port** *auth-port*] [**acct-port** *acct-port*]

Syntax Description

host *ip-addr*	Specifies the name or IP address of the configured RADIUS server.
auth-port *auth-port*	(Optional) Specifies the authentication port for the RADIUS server. The default value is 1645.
acct-port *acct-port*	(Optional) Specifies the accounting port for the RADIUS server. The default value is 1646.

Command Default

The default values for time and tries are not fixed to a single value; therefore, they are calculated and fall within a range of 10 to 60 seconds for time and 10 to 100 for tries.

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
aaa	read

Examples

The following sample output is for the **show radius dead-criteria** command:

```
RP/0/RSP0/CPU0:router# show radius dead-criteria host 12.26.49.12 auth-port 11000 acct-port
 11001

Server: 12.26.49.12/11000/11001
Dead criteria time: 10 sec (computed) tries: 10 (computed)
```

This table describes the significant fields shown in the display.

Table 6: show radius dead-criteria Field Descriptions

Field	Description
Server	Server IP address/UDP destination port for authentication requests/UDP destination port for accounting requests.
Timeout	Number of seconds the router waits for a server host to reply before timing out.

Field	Description
Retransmits	Number of times Cisco IOS XR software searches the list of RADIUS server hosts before giving up.

Related Commands

Command	Description
radius-server dead-criteria time, on page 79	Forces one or both of the criteria that is used to mark a RADIUS server as dead.
radius-server deadtime(BNG), on page 83	Defines the length of time in minutes for a RADIUS server to remain marked dead.

show radius server-groups

To display information about the RADIUS server groups that are configured in the system, use the **show radius server-groups** command in EXEC mode.

show radius server-groups [*group-name* [**detail**]]

Syntax Description

group-name	(Optional) Name of the server group.The properties are displayed.
detail	(Optional) Displays properties for all the server groups.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **show radius server-groups** command to display information about each configured RADIUS server group, including the group name, numbers of servers in the group, and a list of servers in the named server group. A global list of all configured RADIUS servers, along with authentication and accounting port numbers, is also displayed.

Task ID

Task ID	Operations
aaa	read

Examples

The inherited global message is displayed if no group level deadtime is defined for this group; otherwise, the group level deadtime value is displayed and this message is omitted. The following sample output is for the **show radius server-groups** command:

```
RP/0/RSP0/CPU0:router# show radius server-groups

Global list of servers
  Contains 2 server(s)
    Server 10.1.1.1/1645/1646
    Server 10.2.2.2/1645/1646

Server group 'radgrp1' has 2 server(s)
  Dead time: 0 minute(s) (inherited from global)
  Contains 2 server(s)
    Server 10.1.1.1/1645/1646
    Server 10.2.2.2/1645/1646

Server group 'radgrp-priv' has 1 server(s)
  Dead time: 0 minute(s) (inherited from global)
  Contains 1 server(s)
    Server 10.3.3.3/1645/1646 [private]
```

The following sample output shows the properties for all the server groups in group “radgrp1:”

```
RP/0/RSP0/CPU0:router# show radius server-groups radgrp1 detail

Server group 'radgrp1' has 2 server(s)
    VRF default (id 0x60000000)
    Dead time: 0 minute(s) (inherited from global)
    Contains 2 server(s)
      Server 10.1.1.1/1645/1646
    Authentication:
      0 requests, 0 pending, 0 retransmits
      0 accepts, 0 rejects, 0 challenges
      0 timeouts, 0 bad responses, 0 bad authenticators
      0 unknown types, 0 dropped, 0 ms latest rtt
    Accounting:
      0 requests, 0 pending, 0 retransmits
      0 responses, 0 timeouts, 0 bad responses
      0 bad authenticators, 0 unknown types, 0 dropped
      0 ms latest rtt
      Server 10.2.2.2/1645/1646
    Authentication:
      0 requests, 0 pending, 0 retransmits
      0 accepts, 0 rejects, 0 challenges
      0 timeouts, 0 bad responses, 0 bad authenticators
      0 unknown types, 0 dropped, 0 ms latest rtt
    Accounting:
      0 requests, 0 pending, 0 retransmits
      0 responses, 0 timeouts, 0 bad responses
      0 bad authenticators, 0 unknown types, 0 dropped
      0 ms latest rtt
```

The following sample output shows the properties for all the server groups in detail in the group “raddgrp-priv:”

```
RP/0/RSP0/CPU0:router# show radius server-groups radgrp-priv detail

Server group 'radgrp-priv' has 1 server(s)
    VRF default (id 0x60000000)
    Dead time: 0 minute(s) (inherited from global)
    Contains 1 server(s)
      Server 10.3.3.3/1645/1646 [private]
    Authentication:
      0 requests, 0 pending, 0 retransmits
      0 accepts, 0 rejects, 0 challenges
      0 timeouts, 0 bad responses, 0 bad authenticators
      0 unknown types, 0 dropped, 0 ms latest rtt
    Accounting:
      0 requests, 0 pending, 0 retransmits
      0 responses, 0 timeouts, 0 bad responses
      0 bad authenticators, 0 unknown types, 0 dropped
      0 ms latest rtt
```

This table describes the significant fields shown in the display.

Table 7: show radius server-groups Field Descriptions

Field	Description
Server	Server IP address/UDP destination port for authentication requests/UDP destination port for accounting requests.

Related Commands

Command	Description
vrf (RADIUS), on page 188	Configures the Virtual Private Network (VPN) routing and forwarding (VRF) reference of an AAA RADIUS server group.

show radius server-groups detail

To display the detailed summary of the RADIUS server group information, use the **show radius server-groups detail** command in theEXEC mode.

show radius server-groups *server_group_name* **detail**

Syntax Description

server_group_name	Specifies the name of the RADIUS server group.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
aaa	read

This is sample output of the **show radius server-groups detail** command:

```
RP/0/RSP0/CPU0:router# show radius server-groups SG1 detail
Wed Jan 18 06:04:59.432 EST

Server group 'SG1' has 1 server(s)
  VRF  (id 0x0)
  Dead time: 0 minute(s) (inherited from global)
  Contains 1 server(s)
Server 99.0.0.10/1812/1813
  Authentication:
    100 requests, 0 pending, 0 retransmits
    100 accepts, 0 rejects, 0 challenges
    0 timeouts, 0 bad responses, 0 bad authenticators
    0 unknown types, 0 dropped, 0 ms latest rtt
    Throttled: 0 transactions, 0 timeout, 0 failures
    Estimated Throttled Access Transactions: 0
    Maximum Throttled Access Transactions: 0

    Automated TEST Stats:
        0 requests, 0 timeouts, 0 response, 0 pending
```

This table describes the significant fields shown in the display.

Table 8: show radius Field Descriptions

Field	Description
Server	Server IP address/UDP destination port for authentication requests/UDP destination port for accounting requests.
Deadtime	Length of time in minutes for a RADIUS server to remain marked dead.
Authentication	Specifies the authentication details.
Automated TEST Stats	Specifies the total time taken for sending requests, total timeouts, and the response time.

show subscriber database configuration brief service-profile

The commands displays a list of downloaded service profile in cache and whether service profile is being used or not.

how subscriber database configuration brief service-profile

Command Default

None

Command Modes

Global Configuration Mode

Command History

Release	Modification
6.6.3	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

This example displays a list of downloaded service profile in cache:

```
RP/0/0/CPU0:router#show subscriber database configuration brief service-profile
Wed Apr 24 14:55:11.173 IST

Location 0/0/CPU0

ServiceName:MethodList        In Use By Subcriber
----------------------        -------------------
1_Mbps_FQOS:default           True
2_Mbps_FQOS:default           False
```

show tacacs

To display information about the TACACS+ servers that are configured in the system, use the **show tacacs** command in EXEC mode.

show tacacs

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 5.3.0	IPv6 support was introduced on this command.

Usage Guidelines

Use the **show tacacs** command to display statistics for each configured TACACS+ server.

Task ID

Task ID	Operations
aaa	read

Examples

The following is sample output from the **show tacacs** command:

```
RP/0/RSP0/CPU0:router# show tacacs

For IPv4 IP addresses:
Server:10.1.1.1/21212 opens=0 closes=0 aborts=0 errors=0
        packets in=0 packets out=0
        status=up single-connect=false

Server:10.2.2.2/21232 opens=0 closes=0 aborts=0 errors=0
        packets in=0 packets out=0
        status=up single-connect=false

For IPv6 IP addresses:
Server: 10.2.3.5/49  family = AF_INET opens=0 closes=0 aborts=0 errors=0
        packets in=0 packets out=0
        status=up single-connect=false
```

This table describes the significant fields shown in the display.

Table 9: show tacacs Field Descriptions

Field	Description
Server	Server IP address.

Field	Description
opens	Number of socket opens to the external server.
closes	Number of socket closes to the external server.
aborts	Number of tacacs requests that have been terminated midway.
errors	Number of error replies from the external server.
packets in	Number of TCP packets that have been received from the external server.
packets out	Number of TCP packets that have been sent to the external server.

show tacacs counters

To display statistics of authentication, executive and command authorization, and executive and command accounting for each TACACS+ servers configured in the system, use the **show tacacs counters** command in the EXEC mode.

show tacacs counters

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.5.4	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
aaa	read

Examples

The following is a sample output from the **show tacacs counters** command:

```
RP/0/RSP0/CPU0:router# show tacacs counters

TACACS+ Server:   10.105.236.101/4010 [global]

  Authentication:
   10 requests, 4 accepts, 3 failure, 2 error, 1 timeout

  Exec Authorization:
   0 requests, 0 accepts, 0 denied, 0 error, 0 timeout

  Command Authorization:
   6 requests, 6 accepts, 0 denied, 0 error, 0 timeout

  Exec Accounting:
   0 requests, 0 accepts, 0 fail, 0 error, 0 timeout

  Command Accounting:
   6 requests, 6 accepts, 0 fail, 0 error, 0 timeout

TACACS+ Server:   10.105.236.101/2201 [private] vrf = default

  Authentication:
   0 requests, 0 accepts, 0 failure, 0 error, 0 timeout

  Exec Authorization:
   0 requests, 0 accepts, 0 denied, 0 error, 0 timeout
```

```
Command Authorization:
 0 requests, 0 accepts, 0 denied, 0 error, 0 timeout

Exec Accounting:
 0 requests, 0 accepts, 0 fail, 0 error, 0 timeout

Command Accounting:
 0 requests, 0 accepts, 0 fail, 0 error, 0 timeout
```

show tacacs details

To display detailed information about the TACACS+ server and server groups that are configured in the system, use the **show tacacs details** command in the EXEC mode.

show tacacs details

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.5.4	This command was introduced.

Usage Guidelines

Use the **show tacacs details** command to display information about each configured TACACS+ server, including the group name, numbers of servers in the group, and a list of servers in the named server group. A global list of all configured TACACS+ servers is also displayed.

Task ID

Task ID	Operations
aaa	read

Examples

The following is sample output from the **show tacacs details** command:

```
RP/0/RSP0/CPU0:router# show tacacs details

TACACS+ Server                                                  : 10.105.236.101/4010
[Global]
    Family                                                      : IPv4
    Timeout(in secs)                                            : 3
    Connection Opens                                            : 8
    Connection Closes                                           : 8
    Requests sent                                               : 6
    Response received                                           : 6
    Packets Abort                                               : 2
    Server State                                                : Down
    Server On-Hold                                              : True
    Tacacs-Single-Connect                                       : False
    Tacacs-Single-Connect-Idle-Timeout(in secs)                 : 0
    Last Connection Attempted                                   : 08:32:43 UTC Tue Aug
02 2022


TACACS+ Server                                                  : 10.105.236.101/8010
[Private] vrf=default
    Family                                                      : IPv4
    Timeout(in secs)                                            : 3
    Connection Opens                                            : 8
    Connection Closes                                           : 7
```

```
    Requests sent                                                   : 7
    Response received                                               : 7
    Packets Abort                                                   : 0
    Server State                                                    : Up
    Server On-Hold                                                  : False
    Tacacs-Single-Connect                                           : False
    Tacacs-Single-Connect-Idle-Timeout(in secs)                     : 0
    Last Connection Attempted                                       : 08:32:52 UTC Tue Aug
02 2022


TACACS+ Server-groups:

Global list of servers
    Server 10.105.236.101/4010 family=IPv4

Server group 'tac1' has 1 servers
    Servers in this group are under 'default' vrf
    Server 10.105.236.101/8010 [private] family=IPv4

TACACS+ Source-Interface:

Interface                                          VRF Id
IPV4-Address

GigabitEthernet0/0/0/0                            0x60000001
0.0.0.0
MgmtEth0/RP0/CPU0/0                               0x60000000
192.168.122.222


Interface                                           VRF Id
IPV6-Address

GigabitEthernet0/0/0/0                            0x60000001
 ::
MgmtEth0/RP0/CPU0/0                               0x60000000
 ::
```

show tacacs server-groups

To display information about the TACACS+ server groups that are configured in the system, use the **show tacacs server-groups** command in EXEC mode.

show tacacs server-groups

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **show tacacs server-groups** command to display information about each configured TACACS+ server group, including the group name, numbers of servers in the group, and a list of servers in the named server group. A global list of all configured TACACS+ servers is also displayed.

Task ID

Task ID	Operations
aaa	read

Examples

The following is sample output from the **show tacacs server-groups** command:

```
RP/0/RSP0/CPU0:router# show tacacs server-groups

Global list of servers
  Server 192.168.25.61/23456
  Server 192.168.49.12/12345
  Server 192.168.49.12/9000
  Server 192.168.25.61/23432
  Server 10.5.5.5/23456
  Server 10.1.1.1/49
Server group 'tac100' has 1 servers
Server 192.168.49.12
```

This table describes the significant fields shown in the display.

Table 10: show tacacs server-groups Field Descriptions

Field	Description
Server	Server IP address.

Related Commands

Command	Description
tacacs-server host, on page 158	Specifies a TACACS+ host.

show tacacs source-interface

To display information about the source interface for the TACACS+ server that are configured in the system, use the **show tacacs source-interface** command in the EXEC mode.

show tacacs source-interface

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.5.4	This command was introduced.

Usage Guidelines

Use the **show tacacs source-interface** command to display source interface information about each configured TACACS+ server, including the interface name, vrf-id, and IPv4 and IPv6 address.

Task ID

Task ID	Operations
aaa	read

Examples

The following is sample output from the **show tacacs source-interface** command:

```
RP/0/RSP0/CPU0:router# show tacacs source-interface
Interface                               VRF Id                          IPV4-Address

MgmtEth0/RP0/CPU0/0                   0x60000000                      192.168.122.222


Interface                               VRF Id                          IPV6-Address

MgmtEth0/RP0/CPU0/0                   0x60000000                            ::
RP/0/RP0/CPU0:ios#
```

show user

To display all user groups and task IDs associated with the currently logged-in user, use the **show user** command in EXEC mode.

show user [{**all** | **authentication** | **group** | **tasks**}]

Syntax Description

all	(Optional) Displays all user groups and task IDs for the currently logged-in user.
authentication	(Optional) Displays authentication method parameters for the currently logged-in user.
group	(Optional) Displays the user groups associated with the currently logged-in user.
tasks	(Optional) Displays task IDs associated with the currently logged-in user. The **tasks** keyword indicates which task is reserved in the sample output.

Command Default

When the **show user** command is used without any option, it displays the ID of the user who is logged in currently.

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **show user** command to display all user groups and task IDs associated with the currently logged-in user.

Task ID

Task ID	Operations
none	—

Examples

The following sample output displays the authentication method parameters from the **show user** command:

```
RP/0/RSP0/CPU0:router# show user authentication

local
```

The following sample output displays the groups from the **show user** command:

```
RP/0/RSP0/CPU0:router# show user group

root-system
```

The following sample output displays all the information for the groups and tasks from the **show user** command:

```
RP/0/RSP0/CPU0:router# show user all
Username: lab
Groups: root-system
Authenticated using method local
User lab has the following Task ID(s):

Task:                  aaa  : READ    WRITE    EXECUTE    DEBUG
Task:                  aaa  : READ    WRITE    EXECUTE    DEBUG
Task:                  acl  : READ    WRITE    EXECUTE    DEBUG
Task:                admin  : READ    WRITE    EXECUTE    DEBUG
Task:                  atm  : READ    WRITE    EXECUTE    DEBUG
Task:       basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:                 bcdl  : READ    WRITE    EXECUTE    DEBUG
Task:                  bfd  : READ    WRITE    EXECUTE    DEBUG
Task:                  bgp  : READ    WRITE    EXECUTE    DEBUG
Task:                 boot  : READ    WRITE    EXECUTE    DEBUG
Task:               bundle  : READ    WRITE    EXECUTE    DEBUG
Task:                  cdp  : READ    WRITE    EXECUTE    DEBUG
Task:                  cef  : READ    WRITE    EXECUTE    DEBUG
Task:          config-mgmt  : READ    WRITE    EXECUTE    DEBUG
Task:      config-services  : READ    WRITE    EXECUTE    DEBUG
Task:               crypto  : READ    WRITE    EXECUTE    DEBUG
Task:                 diag  : READ    WRITE    EXECUTE    DEBUG
Task:              drivers  : READ    WRITE    EXECUTE    DEBUG
Task:               eigrp  : READ    WRITE    EXECUTE    DEBUG
Task:           ext-access  : READ    WRITE    EXECUTE    DEBUG
Task:               fabric  : READ    WRITE    EXECUTE    DEBUG
Task:            fault-mgr  : READ    WRITE    EXECUTE    DEBUG
Task:           filesystem  : READ    WRITE    EXECUTE    DEBUG
Task:             firewall  : READ    WRITE    EXECUTE    DEBUG
Task:                   fr  : READ    WRITE    EXECUTE    DEBUG
Task:                 hdlc  : READ    WRITE    EXECUTE    DEBUG
Task:        host-services  : READ    WRITE    EXECUTE    DEBUG
Task:                 hsrp  : READ    WRITE    EXECUTE    DEBUG
Task:            interface  : READ    WRITE    EXECUTE    DEBUG
Task:            inventory  : READ    WRITE    EXECUTE    DEBUG
Task:          ip-services  : READ    WRITE    EXECUTE    DEBUG
Task:                 ipv4  : READ    WRITE    EXECUTE    DEBUG
Task:                 ipv6  : READ    WRITE    EXECUTE    DEBUG
Task:                 isis  : READ    WRITE    EXECUTE    DEBUG
Task:              logging  : READ    WRITE    EXECUTE    DEBUG
Task:                 lpts  : READ    WRITE    EXECUTE    DEBUG
Task:              monitor  : READ    WRITE    EXECUTE    DEBUG
Task:              mpls-ldp  : READ    WRITE    EXECUTE    DEBUG
Task:              mpls-static  : READ    WRITE    EXECUTE    DEBUG
Task:              mpls-te  : READ    WRITE    EXECUTE    DEBUG
Task:              multicast  : READ    WRITE    EXECUTE    DEBUG
Task:              netflow  : READ    WRITE    EXECUTE    DEBUG
Task:              network  : READ    WRITE    EXECUTE    DEBUG
Task:                 ospf  : READ    WRITE    EXECUTE    DEBUG
Task:                 ouni  : READ    WRITE    EXECUTE    DEBUG
Task:              pkg-mgmt  : READ    WRITE    EXECUTE    DEBUG
Task:                  ppp  : READ    WRITE    EXECUTE    DEBUG
Task:                  qos  : READ    WRITE    EXECUTE    DEBUG
Task:                  rib  : READ    WRITE    EXECUTE    DEBUG
Task:                  rip  : READ    WRITE    EXECUTE    DEBUG
Task:              root-lr  : READ    WRITE    EXECUTE    DEBUG (reserved)
Task:           root-system  : READ    WRITE    EXECUTE    DEBUG (reserved)
Task:            route-map  : READ    WRITE    EXECUTE    DEBUG
Task:         route-policy  : READ    WRITE    EXECUTE    DEBUG
Task:                  sbc  : READ    WRITE    EXECUTE    DEBUG
Task:                 snmp  : READ    WRITE    EXECUTE    DEBUG
Task:            sonet-sdh  : READ    WRITE    EXECUTE    DEBUG
```

```
Task:               static  : READ    WRITE    EXECUTE    DEBUG
Task:               sysmgr  : READ    WRITE    EXECUTE    DEBUG
Task:               system  : READ    WRITE    EXECUTE    DEBUG
Task:            transport  : READ    WRITE    EXECUTE    DEBUG
Task:          tty-access  : READ    WRITE    EXECUTE    DEBUG
Task:               tunnel  : READ    WRITE    EXECUTE    DEBUG
Task:            universal  : READ    WRITE    EXECUTE    DEBUG (reserved)
Task:                 vlan  : READ    WRITE    EXECUTE    DEBUG
Task:                 vrrp  : READ    WRITE    EXECUTE    DEBUG
```

The following sample output displays the tasks and indicates which tasks are reserved from the **show user** command:

```
RP/0/RSP0/CPU0:router# show user tasks

Task:                  aaa  : READ    WRITE    EXECUTE    DEBUG
Task:                  aaa  : READ    WRITE    EXECUTE    DEBUG
Task:                  acl  : READ    WRITE    EXECUTE    DEBUG
Task:                admin  : READ    WRITE    EXECUTE    DEBUG
Task:                  atm  : READ    WRITE    EXECUTE    DEBUG
Task:       basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:                 bcdl  : READ    WRITE    EXECUTE    DEBUG
Task:                  bfd  : READ    WRITE    EXECUTE    DEBUG
Task:                  bgp  : READ    WRITE    EXECUTE    DEBUG
Task:                 boot  : READ    WRITE    EXECUTE    DEBUG
Task:               bundle  : READ    WRITE    EXECUTE    DEBUG
Task:                  cdp  : READ    WRITE    EXECUTE    DEBUG
Task:                  cef  : READ    WRITE    EXECUTE    DEBUG
Task:          config-mgmt  : READ    WRITE    EXECUTE    DEBUG
Task:      config-services  : READ    WRITE    EXECUTE    DEBUG
Task:               crypto  : READ    WRITE    EXECUTE    DEBUG
Task:                 diag  : READ    WRITE    EXECUTE    DEBUG
Task:              drivers  : READ    WRITE    EXECUTE    DEBUG
Task:                eigrp  : READ    WRITE    EXECUTE    DEBUG
Task:           ext-access  : READ    WRITE    EXECUTE    DEBUG
Task:               fabric  : READ    WRITE    EXECUTE    DEBUG
Task:            fault-mgr  : READ    WRITE    EXECUTE    DEBUG
Task:           filesystem  : READ    WRITE    EXECUTE    DEBUG
Task:             firewall  : READ    WRITE    EXECUTE    DEBUG
Task:                   fr  : READ    WRITE    EXECUTE    DEBUG
Task:                 hdlc  : READ    WRITE    EXECUTE    DEBUG
Task:        host-services  : READ    WRITE    EXECUTE    DEBUG
Task:                 hsrp  : READ    WRITE    EXECUTE    DEBUG
Task:            interface  : READ    WRITE    EXECUTE    DEBUG
Task:            inventory  : READ    WRITE    EXECUTE    DEBUG
Task:          ip-services  : READ    WRITE    EXECUTE    DEBUG
Task:                 ipv4  : READ    WRITE    EXECUTE    DEBUG
Task:                 ipv6  : READ    WRITE    EXECUTE    DEBUG
Task:                 isis  : READ    WRITE    EXECUTE    DEBUG
Task:              logging  : READ    WRITE    EXECUTE    DEBUG
Task:                 lpts  : READ    WRITE    EXECUTE    DEBUG
Task:              monitor  : READ    WRITE    EXECUTE    DEBUG
Task:              mpls-ldp  : READ    WRITE    EXECUTE    DEBUG
Task:              mpls-static  : READ    WRITE    EXECUTE    DEBUG
Task:              mpls-te  : READ    WRITE    EXECUTE    DEBUG
Task:              multicast  : READ    WRITE    EXECUTE    DEBUG
Task:              netflow  : READ    WRITE    EXECUTE    DEBUG
Task:              network  : READ    WRITE    EXECUTE    DEBUG
Task:                 ospf  : READ    WRITE    EXECUTE    DEBUG
Task:                 ouni  : READ    WRITE    EXECUTE    DEBUG
Task:              pkg-mgmt  : READ    WRITE    EXECUTE    DEBUG
Task:                  ppp  : READ    WRITE    EXECUTE    DEBUG
Task:                  qos  : READ    WRITE    EXECUTE    DEBUG
```

```
Task:                  rib  : READ    WRITE    EXECUTE    DEBUG
Task:                  rip  : READ    WRITE    EXECUTE    DEBUG
Task:              root-lr  : READ    WRITE    EXECUTE    DEBUG (reserved)
Task:          root-system  : READ    WRITE    EXECUTE    DEBUG (reserved)
Task:            route-map  : READ    WRITE    EXECUTE    DEBUG
Task:         route-policy  : READ    WRITE    EXECUTE    DEBUG
Task:                  sbc  : READ    WRITE    EXECUTE    DEBUG
Task:                 snmp  : READ    WRITE    EXECUTE    DEBUG
Task:            sonet-sdh  : READ    WRITE    EXECUTE    DEBUG
Task:               static  : READ    WRITE    EXECUTE    DEBUG
Task:               sysmgr  : READ    WRITE    EXECUTE    DEBUG
Task:               system  : READ    WRITE    EXECUTE    DEBUG
Task:            transport  : READ    WRITE    EXECUTE    DEBUG
Task:          tty-access  : READ    WRITE    EXECUTE    DEBUG
Task:               tunnel  : READ    WRITE    EXECUTE    DEBUG
Task:            universal  : READ    WRITE    EXECUTE    DEBUG (reserved)
Task:                 vlan  : READ    WRITE    EXECUTE    DEBUG
Task:                 vrrp  : READ    WRITE    EXECUTE    DEBUG
```

Related Commands

Command	Description
show aaa , on page 112	Displays the task maps for selected user groups, local users, or task groups.

single-connection

To multiplex all TACACS+ requests to this server over a single TCP connection, use the **single-connection** command in TACACS host configuration mode. To disable the single TCP connection for all new sessions that use a separate connection, use the **no** form of this command.

single-connection

Syntax Description

This command has no keywords or arguments.

Command Default

By default, a separate connection is used for each session.

Command Modes

TACACS host configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

The **single-connection** command allows the TACACS+ server to handle a greater number of TACACS operations than would be possible if multiple TCP connections were used to send requests to a server.

The TACACS+ server that is being used must support single-connection mode for this to be effective; otherwise, the connection between the network access server and the TACACS+ server locks up or you can receive unauthentic errors.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to configure a single TCP connection to be made with the TACACS+ server (IP address 209.165.200.226) and all authentication, authorization, accounting requests to use this TCP connection. This works only if the TACACS+ server is also configured in single-connection mode. To configure the TACACS+ server in single connection mode, refer to the respective server manual.

```
RP/0/RSP0/CPU0:router(config)# tacacs-server host 209.165.200.226
RP/0/RSP0/CPU0:router(config-tacacs-host)# single-connection
```

Related Commands

Command	Description
tacacs-server host, on page 158	Specifies a TACACS+ host.

single-connection-idle-timeout

To set the idle timeout value for the single TCP connection to the TACACS+ server, use the **single-connection-idle-timeout** command in *tacacs-server host* configuration mode. To remove the configuration or to disable the idle timeout for the single connection, use the **no** form of this command.

single-connection-idle-timeout *time-in-seconds*

Syntax Description

time-in-seconds	Specifies the single connection timeout value, in seconds. The range is: • 500 to 7200 (prior to Cisco IOS XR Software Release 7.4.1/Release 7.3.2/Release 6.8.1) • 5 to 7200 (from Cisco IOS XR Software Release 7.4.1/Release 7.3.2/Release 6.8.1, and later)

Command Default

Single connection idle timeout is not set, by default.

Command Modes

tacacs-server host

Command History

Release	Modification
Release 6.8.1	This command was modified to change the timeout range (for Cisco IOS XR 32-bit routers).
Release 7.3.2 Release 7.4.1	This command was modified to change the timeout range (for Cisco IOS XR 64-bit routers).
Release 6.6.3	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
aaa	read, write

Examples

This example shows how to set an idle timeout value of 500 seconds for the single TCP connections to the TACACS+ server:

```
RP/0/RSP0/CPU0:router(config)#tacacs-server host 209.165.200.226
RP/0/RSP0/CPU0:router(config-tacacs-host)#single-connection-idle-timeout 500
RP/0/RSP0/CPU0:router(config-tacacs-host)#commit
```

Related Commands

Command	Description
single-connection, on page 154	Multiplexes all TACACS+ requests to the server over a single TCP connection.

statistics period service-accounting

To set collection period for statistics collectors, use the **statistics period service-accounting** command in Global Configuration mode or Admin Configuration mode. To disable this behavior, use the **no** form of this command.

statistics period service-accounting {*period* | **disable**}

Syntax Description

period	Collection period in seconds. The range is from 30 to 3600. The default is 900.
disable	Disables periodic statistics collection.

Command Default

Default collection period is 900 seconds.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
diag	read, write

This example shows how to change the collection period or polling interval for statistics collector:

```
RP/0/RSP0/CPU0:router(config)# statistics period service-accounting 2000
```

tacacs-server host

To specify a TACACS+ host server, use the **tacacs-server host** command in Global Configuration mode. To delete the specified name or address, use the **no** form of this command.

tacacs-server host host-name [**holddown-time** *time*][**port port-number**] [**timeout seconds**] [**key** [{**0** | **7**}] **auth-key**] [**single-connection**]
[**single-connection-idle-timeout** *time-in-seconds*]

Syntax Description

host-name	Host or domain name or IP address of the TACACS+ server.
holddown-time *time*	Specifies a duration, in seconds, for which an unresponsive TACACS+ server is to be marked as DOWN. The range is from 0 to 1200. Zero indicates that the hold-down timer feature is disabled.
port *port-number*	(Optional) Specifies a server port number. This option overrides the default, which is port 49. Valid port numbers range from 1 to 65535.
timeout *seconds*	(Optional) Specifies a timeout value that sets the length of time the authentication, authorization, and accounting (AAA) server waits to receive a response from the TACACS+ server. This option overrides the global timeout value set with the **tacacs-server timeout** command for this server only. The valid timeout range is from 1 to 1000 seconds. Default is 5. Note: You can use this parameter only in the config-tacacs-host sub-mode.
key [**0** | **7**] *auth-key*	(Optional) Specifies an authentication and encryption key shared between the AAA server and the TACACS+ server. The TACACS+ packets are encrypted using this key. This key must match the key used by the TACACS+ daemon. Specifying this key overrides the key set by the **tacacs-server key**command for this server only. (Optional) Entering **0** specifies that an unencrypted (clear-text) key follows. (Optional) Entering **7** specifies that an encrypted key follows. The *auth-key* argument specifies the unencrypted key between the AAA server and the TACACS+ server. Note: You can use this parameter only in the config-tacacs-host sub-mode.
single-connection	(Optional) Multiplexes all TACACS+ requests to this server over a single TCP connection. By default, a separate connection is used for each session. Note: You can use this parameter only in the config-tacacs-host sub-mode.

single-connection-idle-timeout *time-in-seconds*	(Optional) Specifies the single connection idle timeout value, in seconds. The range is: • 500 to 7200 (prior to Cisco IOS XR Software Release 7.4.1/Release 7.3.2/Release 6.8.1) • 5 to 7200 (from Cisco IOS XR Software Release 7.4.1/Release 7.3.2/Release 6.8.1, and later)

Command Default

No TACACS+ host is specified.

The *port-name* argument, if not specified, defaults to the standard port 49.

The *seconds* argument, if not specified, defaults to 5 seconds.

Single connection idle timeout is not set, by default.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 5.3.0	IPv6 support is introduced on this command.
Release 6.6.3	This command was modified to include **single-connection-idle-timeout** option.
Release 6.8.1	This command was modified for 32-bit Cisco IOS XR routers to include these: • **holddown-time** option • modified the range for **single-connection-idle-timeout** parameter.
Release 7.3.2 Release 7.4.1	This command was modified for 64-bit Cisco IOS XR routers to change the range for **single-connection-idle-timeout** parameter.
Release 7.4.1	This command was modified for Cisco IOS XR 64-bit platforms to include **holddown-time** option.

Usage Guidelines

You can use multiple **tacacs-server host** commands to specify additional hosts. Cisco IOS XR software searches for hosts in the order in which you specify them.

For details on TACACS+ hold-down timer, see the **holddown-time** command.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to specify a TACACS+ host with the IP address 209.165.200.226:

```
RP/0/RSP0/CPU0:router(config)# tacacs-server host 209.165.200.226
RP/0/RSP0/CPU0:router(config-tacacs-host)#
```

The following example shows that the default values from the **tacacs-server host** command are displayed from the **show run** command:

```
RP/0/RSP0/CPU0:router# show run

Building configuration...
!! Last configuration change at 13:51:56 UTC Mon Nov 14 2005 by lab
!
tacacs-server host 209.165.200.226 port 49
 timeout 5
!
```

The following example shows how to specify that the router consult the TACACS+ server host named host1 on port number 51. The timeout value for requests on this connection is 30 seconds; the encryption key is a_secret.

```
RP/0/RSP0/CPU0:router(config)# tacacs-server host host1 port 51
RP/0/RSP0/CPU0:router(config-tacacs-host)# timeout 30
RP/0/RSP0/CPU0:router(config-tacacs-host)# key a_secret
```

Related Commands

Command	Description
key (TACACS+), on page 69	Specifies an authentication and encryption key shared between the AAA server and the TACACS+ server.
single-connection, on page 154	Multiplexes all TACACS+ requests to this server over a single TCP connection.
single-connection-idle-timeout, on page 155	Sets the idle timeout value for the single TCP connection to the TACACS+ server.
tacacs-server key, on page 161	Globally sets the authentication encryption key used for all TACACS+ communications between the router and the TACACS+ daemon.
tacacs-server timeout, on page 163	Globally sets the interval that the router waits for a server host to reply.
timeout (TACACS+), on page 174	Specifies a timeout value that sets the length of time the authentication, authorization, and accounting (AAA) server waits to receive a response from the TACACS+ server.

tacacs-server key

To set the authentication encryption key used for all TACACS+ communications between the router and the TACACS+ daemon, use the **tacacs-server key** command in Global Configuration mode. To disable the key, use the **no** form of this command.

tacacs-server key {**0** *clear-text-key* | **7** *encrypted-keyauth-key*}

Syntax Description

0 *clear-text-key*	Specifies an unencrypted (cleartext) shared key.
7 *encrypted-key*	Specifies an encrypted shared key.
auth-key	Specifies the unencrypted key between the AAA server and the TACACS+ server.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

The key name entered must match the key used on the TACACS+ daemon. The key name applies to all servers that have no individual keys specified. All leading spaces are ignored; spaces within and after the key are not. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.

The key name is valid only when the following guidelines are followed:

- The *clear-text-key* argument must be followed by the **0** keyword.
- The *encrypted-key* argument must be followed by the **7** keyword.

The TACACS server key is used only if no key is configured for an individual TACACS server. Keys configured for an individual TACACS server always override this global key configuration.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example sets the authentication and encryption key to key1:

```
RP/0/RSP0/CPU0:router(config)# tacacs-server key key1
```

Related Commands

Command	Description
key (TACACS+), on page 69	Specifies an authentication and encryption key shared between the AAA server and the TACACS+ server.
tacacs-server host, on page 158	Specifies a TACACS+ host.

tacacs-server timeout

To set the interval that the server waits for a server host to reply, use the **tacacs-server timeout** command in Global Configuration mode. To restore the default, use the **no** form of this command.

tacacs-server timeout *seconds*

Syntax Description

seconds	Integer that specifies the timeout interval (in seconds) from 1 to 1000.

Command Default

5 seconds

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

The TACACS+ server timeout is used only if no timeout is configured for an individual TACACS+ server. Timeout intervals configured for an individual TACACS+ server always override this global timeout configuration.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows the interval timer being changed to 10 seconds:

```
RP/0/RSP0/CPU0:router(config)# tacacs-server timeout 10
```

Related Commands

Command	Description
tacacs-server host, on page 158	Specifies a TACACS+ host.

tacacs-server ipv4

To set the Differentiated Services Code Point (DSCP), which is represented by the first six bits in the Type of Service (ToS) byte of the IP header, use the **tacacs-server ipv4** command in Global Configuration mode.

tacacs-server ipv4 dscp *dscp-value*

Syntax Description

ipv4	Specifies the dscp bit for the IPv4 packets.
dscp	Sets the DSCP in the IP header.
dscp-value	Specifies the options for setting the value of DSCP. The available options are: • <0-63> Differentiated services codepoint value • af11 Match packets with AF11 dscp (001010) • af12 Match packets with AF12 dscp (001100) • af13 Match packets with AF13 dscp (001110) • af21 Match packets with AF21 dscp (010010) • af22 Match packets with AF22 dscp (010100) • af23 Match packets with AF23 dscp (010110) • af31 Match packets with AF31 dscp (011010) • af32 Match packets with AF32 dscp (011100) • af33 Match packets with AF33 dscp (011110) • af41 Match packets with AF41 dscp (100010) • af42 Match packets with AF42 dscp (100100) • af43 Match packets with AF43 dscp (100110) • cs1 Match packets with CS1(precedence 1) dscp (001000) • cs2 Match packets with CS2(precedence 2) dscp (010000) • cs3 Match packets with CS3(precedence 3) dscp (011000) • cs4 Match packets with CS4(precedence 4) dscp (100000) • cs5 Match packets with CS5(precedence 5) dscp (101000) • cs6 Match packets with CS6(precedence 6) dscp (110000) • cs7 Match packets with CS7(precedence 7) dscp (111000) • default Match packets with default dscp (000000) • ef Match packets with EF dscp (101110)

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 4.3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
aaa	read, write

Examples

The following example sets the DSCP value to Assured Forwarding (AF)11:

```
RP/0/RSP0/CPU0:router(config)# tacacs-server ipv4 dscp af11
```

tacacs source-interface

To specify the source IP address of a selected interface for all outgoing TACACS+ packets, use the **tacacs source-interface** command in Global Configuration mode. To disable use of the specified interface IP address, use the **no** form of this command.

tacacs source-interface *type path-id* [**vrf** *vrf-id*]

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command in EXEC mode to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
vrf *vrf-id*	Specifies the name of the assigned VRF.

Command Default

If a specific source interface is not configured, or the interface is down or does not have an IP address configured, the system selects an IP address.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.1.0	The **vrf** keyword was added.

Usage Guidelines

Use the **tacacs source-interface** command to set the IP address of the specified interface for all outgoing TACACS+ packets. This address is used as long as the interface is in the *up* state. In this way, the TACACS+ server can use one IP address entry associated with the network access client instead of maintaining a list of all IP addresses.

This command is especially useful in cases where the router has many interfaces and you want to ensure that all TACACS+ packets from a particular router have the same IP address.

When the specified interface does not have an IP address or is in a *down* state, TACACS+ behaves as if no source interface configuration is used.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to set the IP address of the specified interface for all outgoing TACACS+ packets:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# tacacs source-interface GigabitEthernet 0/0/0/29 vrf abc
```

Related Commands

Command	Description
aaa group server tacacs+, on page 34	Groups different server hosts into distinct lists and distinct methods.

task

To add a task ID to a task group, use the **task** command in task group configuration mode. To remove a task ID from a task group, use the **no** form of this command.

task {**read** | **write** | **execute** | **debug**} *taskid-name*

Syntax Description

read	Enables read-only privileges for the named task ID.
write	Enables write privileges for the named task ID. The term "write" implies read also.
execute	Enables execute privileges for the named task ID.
debug	Enables debug privileges for the named task ID.
taskid-name	Name of the task ID.

Command Default

No task IDs are assigned to a newly created task group.

Command Modes

Task group configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **task** command in task group configuration mode. To access task group configuration mode, use the **taskgroup** command in global configuration mode.

Task IDs are the base of command authorization. Only users who have the required permissions can execute a particular command on the router. To execute a command, the user must be part of a user group that consists of task group(s) that includes required task IDs and privileges. Cisco IOS XR software supports multiple task IDs. For example, **aaa**, **config-services**, **crypto**, **system**, and so on. To see the list of task IDs available for the user, use the **show user tasks** command.

Likewise, all commands are associated with one or more task IDs, and their corresponding operations (such as **read**, **write**, **execute**, and **debug**) that denote the permissions required to execute those commands. You can use the **describe** command to know the task ID and permissions that are required to execute a particular command.

For example, the following output shows that the user needs **aaa** task ID with **read** and **write** permission to execute the **show run aaa** command. So, users can execute this command if they belong to a user group associated with a task group that includes this **aaa** task ID having read and write privileges.

```
Router# describe show run aaa
The command is defined in aaa_cmds.parser

User needs ALL of the following taskids:

    aaa (READ WRITE) ----------->

It will take the following actions:
Wed Mar 16 07:58:01.451 UTC
```

```
  Spawn the process:
    nvgen "-c" "-q" "gl/aaa/"
Router#
```

Root users (users in **root-lr** or **root-system** user group) have all task IDs, and hence will be able to execute all commands. Also, certain commands might not require any task ID as such to execute it. So, all users will have permission to execute such commands. If you do not have the required permission to execute a command, the command authorization fails. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

A few other examples that describe the commands to list the task ID:

```
Router#describe show interfaces
The command is defined in show_interface.parser

show_interface.parser
User needs ALL of the following taskids:

   interface (READ)---------->

It will take the following actions:
Thu Mar 17 06:42:08.264 UTC
  Spawn the process:
    show_interface "-a"
Router#


Router(config)#describe ssh server
The command is defined in ssh.parser

ssh.parser
User needs ALL of the following taskids:

   crypto (READ WRITE) ---------->

It will take the following actions:
  Create/Set the configuration item:
       Path: gl/crypto/ssh/server/sshd/vrf/default
       Value: packed[ 0x1 <string> <string> ]
Router(config)#
```

For more details, see *Configuring AAA Services* chapter in the *System Security Configuration Guide for Cisco ASR 9000 Series Routers*.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to enable execute privileges for the config-services task ID and associate that task ID with the task group named taskgroup1:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# taskgroup taskgroup1
RP/0/RSP0/CPU0:router(config-tg)# task execute config-services
```

Related Commands

Command	Description
taskgroup, on page 171	Configures a task group to be associated with a set of task IDs.

taskgroup

To configure a task group to be associated with a set of task IDs, and to enter task group configuration mode, use the **taskgroup** command in Global Configuration mode. To delete a task group, use the **no** form of this command.

taskgroup *taskgroup-name* [{**description** *string* | **task** {**read** | **write** | **execute** | **debug**} *taskid-name* | **inherit taskgroup** *taskgroup-name*}]

Syntax Description

taskgroup-name	Name of a particular task group.
description	(Optional) Enables you to create a description for the named task group.
string	(Optional) Character string used for the task group description.
task	(Optional) Specifies that a task ID is to be associated with the named task group.
read	(Optional) Specifies that the named task ID permits read access only.
write	(Optional) Specifies that the named task ID permits read and write access only.
execute	(Optional) Specifies that the named task ID permits execute access.
debug	(Optional) Specifies that the named task ID permits debug access only.
taskid-name	(Optional) Name of a task: the task ID.
inherit taskgroup	(Optional) Copies permissions from the named task group.
taskgroup-name	(Optional) Name of the task group from which permissions are to be inherited.

Command Default

Five predefined user groups are available by default.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Task groups are configured with a set of task IDs for each action type. Deleting a task group that is still referenced in the system results in a warning and rejection of the deletion. For more details on task IDs, see the Usage Guidelines section of the **task** command.

You can use the **show user group** command in Global Configuration mode to know the group(s) that the current user is part of. Similarly, you can use the **show user all** to know the group or task information (such as username, groups, authentication method, task IDs, and so on) of the current user.

From global configuration mode, you can display all the configured task groups. However, you cannot display all the configured task groups in taskgroup configuration mode.

Entering the **taskgroup** command with no keywords or arguments enters task group configuration mode, in which you can use the **description**, **inherit**, **show**, and **task** commands.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example assigns read bgp permission to the task group named alpha:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# taskgroup alpha
RP/0/RSP0/CPU0:router(config-tg)# task read bgp
```

Related Commands

Command	Description
description (AAA), on page 58	Creates a task group description in task configuration mode.
task, on page 168	Adds a task ID to a task group.

timeout (RADIUS)

To specify the number of seconds the router waits for the RADIUS server to reply before retransmitting, use the **timeout** command in RADIUS server-group private configuration mode. To disable this command and return to the default timeout value of 5 seconds, use the **no** form of this command.

timeout *seconds*

Syntax Description

seconds	Timeout value (in seconds). The range is from 1 to 1000. If no timeout is specified, the global value is used.

Command Default

seconds: 5

Command Modes

RADIUS server-group private configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to set the number of seconds for the timeout value:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa group server radius group1
RP/0/RSP0/CPU0:router(config-sg-radius)# server-private 10.1.1.1 auth-port 300
RP/0/RSP0/CPU0:router(config-sg-radius-private)# timeout 500
```

Related Commands

Command	Description
radius-server timeout(BNG), on page 93	Sets the interval for which a router waits for a server host to reply before timing out.
retransmit (RADIUS), on page 100	Specifies the number of times a RADIUS request is resent to a server if the server is not responding or is responding slowly.
server-private (RADIUS), on page 107	Configures the IP address of the private RADIUS server for the group server.

timeout (TACACS+)

To specify a timeout value that sets the length of time the authentication, authorization, and accounting (AAA) server waits to receive a response from the TACACS+ server, use the **timeout** (TACACS+) command in TACACS host configuration mode. To disable this command and return to the default timeout value of 5 seconds, use the **no** form of this command.

timeout *seconds*

Syntax Description

seconds	Timeout value (in seconds). The range is from 1 to 1000. If no timeout is specified, the global value is used.

Command Default

seconds: 5

Command Modes

TACACS host configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

The **timeout** (TACACS+) command overrides the global timeout value set with the **tacacs-server timeout** command for this server only.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to set the number of seconds for the timeout value:

```
RP/0/RSP0/CPU0:router(config)# tacacs-server host 209.165.200.226
RP/0/RSP0/CPU0:router(config-tacacs-host)# timeout 500
```

Related Commands

Command	Description
tacacs-server host, on page 158	Specifies a TACACS+ host.

timeout login response

To set the interval that the server waits for a reply to a login, use the **timeout login response** command in line template configuration mode. To restore the default, use the **no** form of this command.

timeout login response *seconds*

Syntax Description

seconds	Integer that specifies the timeout interval (in seconds) from 0 to 300.

Command Default

seconds: 30

Command Modes

Line template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **timeout login response** command in line template configuration mode to set the timeout value. This timeout value applies to all terminal lines to which the entered line template is applied. This timeout value cannot be applied to the line console. After the timeout value has expired, the user is prompted again. The retry is allowed three times.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to change the interval timer to 20 seconds:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# line template alpha
RP/0/RSP0/CPU0:router(config-line)# timeout login response 20
```

Related Commands

Command	Description
login authentication, on page 70	Enables AAA authentication for logging in.

usergroup

To configure a user group and associate it with a set of task groups, and to enter user group configuration mode, use the **usergroup** command in Global Configuration mode. To delete a user group, or to delete a task-group association with the specified user group, use the **no** form of this command.

usergroup *usergroup-name*

Syntax Description

usergroup-name	Name of the user group. The *usergroup-name* argument can be only one word. Spaces and quotation marks are not allowed.

Command Default

Five predefined user groups are available by default.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

User groups are configured with the command parameters for a set of users, such as task groups. You can remove specific user groups by using the **no** form of the **usergroup** command. You can remove the user group itself by using the **no** form of the command without giving any parameters. Deleting a user group that is still referenced in the system results in a warning and a rejection of the deletion.

Use the inherit usergroup, on page 65 command to copy permissions from other user groups. The user group is inherited by the parent group and forms a union of all task IDs specified in those groups. Circular inclusions are detected and rejected. User groups cannot inherit properties from predefined groups, such as root-system and owner-sdr.

From global configuration mode, you can display all the configured user groups. However, you cannot display all the configured user groups in usergroup configuration mode.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to add permissions from the user group beta to the user group alpha:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# usergroup alpha
RP/0/RSP0/CPU0:router(config-ug)# inherit usergroup beta
```

Related Commands

Command	Description
description (AAA), on page 58	Creates a description of a task group during configuration.
inherit usergroup, on page 65	Enables a user group to derive permissions from another user group.
taskgroup, on page 171	Configures a task group to be associated with a set of task IDs.

username

To configure a new user with a username, establish a password, associate a password policy with the user, grant permissions for the user, and to enter username configuration mode, use the **username** command in Global Configuration mode or Admin Configuration mode. To delete a user from the database, use the **no** form of this command.

username *name* [{ **group** *name* | [**password-policy** *name*] { **password** | **masked-password** } [*type*] *password* | { **secret** | **masked-secret** } [{ *type* | **0** [**enc-type** *type*] *secret* | **login-history** { **enable** | **disable** } }] }]
no username *name* [{ **group** *name* | **password** | **masked-password** | **secret** | **masked-secret** | **password-policy** *name* [**masked-password** [*type*] *password*] | **login-history** { **enable** | **disable** } }]

Syntax Description

name	Name of the user. The *name* argument can be only one word. Spaces and quotation marks are not allowed. The allowed range for a user-defined username is 2-253 characters.
group *name*	Enables a user to be associated with a user group, as defined with the **usergroup** command.
policy *name*	Configures a password policy that is common to user password and secret.
password-policy*name*	(Optional) Specifies the password policy for cleartext and Type 7 password authentication.
password	Enables a password to be created for the specified user.
masked-password	Enables a password to be created for the specified user. When you key in the password, it is not visible on the screen.

type password	Specifies the password type and the password to be keyed in. Enter 0 or 7 for the *type* argument. 0 specifies a cleartext password, and 7 specifies a Type 7 encrypted password. If Type 7 encryption is enabled with the **password** keyword, the password is not visible to the user. The password can be up to 253 characters in length. (Optional) *type* argument
secret	Enables a secret to be created for the specified user.
masked-secret	Enables a secret to be created for the specified user. When you key in the secret, it is not visible on the screen.
type secret	Specifies the secret type and the secret to be keyed in. Enter 0, or enter 5, 8, 9, or 10, for the *type* argument. Details: • 0 specifies a cleartext secret that will be encrypted for use. • 5 specifies a Type 5 password that uses MD5 hashing algorithm. • 8 specifies a Type 8 password that uses SHA256 hashing algorithm. • 9 specifies a Type 9 password that uses scrypthashing algorithm. • 10 specifies a Type 10 password that uses SHA512 hashing algorithm. **Note** Type 10 is only available for Cisco IOS XR 64 bit platforms. (Optional) *type* argument.

0 enc-type *type secret*	Specifies that you enter a cleartext secret to be encrypted by a specified encryption method. • 0 specifies that you should enter a cleartext secret. • **enc-type** specifies that you enter 5, 8, 9, or 10, for the *type* argument. • Enter the cleartext secret for the *secret* argument. (Optional) **enc-type** *type* keyword-argument combination.
login-history {**enable** | **disable**}	Enables or disables the login history for a specified user.

Command Default

No usernames are defined in the system.

Command Modes

Global Configuration mode

Admin Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 6.2.1	Added support for **password-policy**, as part of AAA password security for FIPS compliance.
Release 6.3.1	Added the support for Type 8 (SHA256) and Type 9 (scrypt) encryption for **secret** configuration on classic Cisco IOS XR (32-bit) operating system.
Release 7.0.1	Extended the support for Type 8 (SHA256) and Type 9 (scrypt) encryption for **secret** configuration on Cisco IOS XR 64-bit operating system as well.
Release 7.0.1	Added support for Type 10 (SHA512) encryption for **secret** configuration only on Cisco IOS XR 64-bit operating system.
Release 7.0.1	The **login-history** keyword was added.
Release 7.3.1	Password Masking feature options (**masked-password** and **masked-secret**) were added. When you key in a password or secret, it is not displayed on the screen

Usage Guidelines

Note

- A user is never allowed to have cisco-support privileges as the only group.
- The Type 10 for the **secret** configuration is available only on Cisco IOS XR 64-bit operating system.
- From Release 7.0.1 and later, Type 10 (SHA512) is applied as the default type for the **secret** configuration. Prior to this, Type 5 (MD5) was the default one.
- The support for Type 8 and 9 for the secret configuration on Cisco IOS XR 64-bit operating system is available only from Release 7.0.1 and later.

Use the **username** command to identify the user and enter username configuration mode. Password and user group assignments can be made from either Global Configuration mode mode or username configuration submode. Permissions (task IDs) are assigned by associating the user with one or more defined user groups.

From global configuration mode, you can display all the configured usernames. However, you cannot display all the configured usernames in username configuration mode.

Each user is identified by a username that is unique across the administrative domain. Each user should be made a member of at least one user group. Deleting a user group may orphan the users associated with that group. The AAA server authenticates orphaned users, but most commands are not authorized.

The **username** command is associated with a particular user for local login authentication by default. Alternatively, a user and password can be configured in the database of the TACACS+ server for TACACS+ login authentication. For more information, see the description of the aaa authentication , on page 15 command.

The predefined group root-system may be specified only by root-system users while administration is configured.

Note To enable the local networking device to respond to remote Challenge Handshake Authentication Protocol (CHAP) challenges, one **username** command entry must be the same as the hostname entry that has already been assigned to the other networking device.

For more details on defining a password policy, see the **aaa password-policy** command. The AAA password security policy feature works as such for Cisco IOS XR platforms. Whereas, it is supported only on XR VM, for Cisco IOS XR 64 bit platforms.

Password Masking guidelines for various command forms

- **username** *name* **password** *type password*

  username *name* **masked-password** *type password*

  Enter 0 or 7 for the *type* argument. *0* specifies a cleartext password, and *7* specifies a Type 7 encrypted password.

- **secret** *type secret*

  masked-secret *type secret*

  Enter 0, or enter 5, 8, 9, or 10, for the *type* argument. 0 specifies a cleartext secret, and 5, 8, 9, and 10 specify a Type 5, Type 8, Type 9, and Type 10 secret, respectively.

- **secret 0 enc-type** *type secret*

  masked-secret 0 enc-type *type secret*

  Enter 5, 8, 9, or 10, for the *type* argument.

- **masked-password** *type password*

  masked-secret *type secret*

  After specifying the password encryption type, press **Enter** or **return** on your keyboard. The password/secret option appears in the next line. Example:

```
Router(config)# masked-secret 10

Enter secret:
Re-enter secret:
```

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows the commands available after executing the **username** command:

```
Router# config
Router(config)# username user1
Router(config-un)# ?
```

clear	Clear the uncommitted configuration
commit	Commit the configuration changes to running
describe	Describe a command without taking real actions
do	Run an exec command
exit	Exit from this submode
group	User group in which this user will be a member of
login-history	Option to set whether to display previous login details
no	Negate a command or set its defaults
password	Specify the password for the user
password-policy	Specify the password policy for the user
pwd	Commands used to reach current submode
root	Exit to the global configuration mode
secret	Specify the secure password for the user
show	Show contents of configuration

The following example shows how to establish the clear-text password *password1* for the user name *user1*:

```
Router# configure
Router(config)# username user1
Router(config-un)# password 0 password1
```

The following example shows how to establish a secured secret for the user *user1* in administration configuration mode:

```
Router(admin-config)# username user1
Router(admin-config-un)# secret 0 lab
Router(admin-config-un)# commit
Router(admin-config)# do show run username
username user1 secret 5 $1$QB03$3H29k3ZT.0PMQ8GQQKXCF0
!
```

This example shows how to apply a AAA password policy for a user:

```
Router# config
Router(config)# username user1 password-policy test-policy password abc
```

The following example shows how to configure a Type 8 (SHA256) password for the user, *user8*. You can also see the examples and usage of the secret, on page 101 command.

You can specify Type as '8' under the **secret** keyword, to explicitly configure Type 8 password.

```
Router#configure
Router(config)#username user8 secret 8
$8$ZYKGl1dZIw73Dl$IUWJOqTLoMyExhsNKoL5vMtvCOYguM5ajXf4uGeQj6I
Router(config-un)#commit
```

This example shows how to configure Type 9 password:

```
Router#configure
Router(config)#username user9 secret 9
$9$/rIQL1B3rplRBL$oS2fLWKFYH6B/kApxkkXmIqbPAHpRZkPEoh3WqGbvwQ
Router(config-un)#commit
```

Similarly, this example shows how to configure Type 10 password :

```
Router#configure
Router(config)#username user10 secret 10
$6$9UvJidvsTEqgkAPU$3CL1Ei/F.E4v/Hi.UaqLwX8UsSEr9ApG6c5pzhMJmZtgW4jObAQ7meAwyhu5VM/aRFJqe/jxZG17h6xPrvJWf1
Router(config-un)#commit
```

This example shows how to specify the Type 10 password in System Admin VM:

```
Router#admin
sysadmin-vm:0_RP0# configure
sysadmin-vm:0_RP0(config)# aaa authentication users user user10 password testpassword
sysadmin-vm:0_RP0(config)# commit
```

This example shows how to enable login-history for user1:

```
Router(config)# username user1 login-history enable
```

This example shows login history information for a successful and an unsuccessful login from user1:

```
Username: user1
Password:
RP/0/RSP0/CPU0:Aug 21 17:20:35.566 UTC: exec[68609]: %SECURITY-LOGIN-4-AUTHEN_FAILED :
Failed authentication attempt by user '<unknown>' from 'console' on 'con0_RSP0_CPU0'


User Access Verification

Username: user1
Password:
User user1 failed to login 1 time(s)
Most recent Failure Fri Aug 21 2020 17:20:35 UTC
to con0_RSP0_CPU0 from console

User user1 last logged in successfully Fri Aug 21 2020 17:20:03 UTC
to con0_RSP0_CPU0 from console
```

Password Masking Examples

The following example shows how to enable password masking for a cleartext password entry:

In this example, for user us3, a cleartext password is entered.

```
Router(config)# username us3 masked-password 0


Enter password:
Re-enter password:

Router(config)#commit
```

In the **show** command output, you can see the encrypted password:

```
Router# show run aaa
..

username us3
 password 7 105A1D0D
```

The encrypted password 105A1D0D is entered in the **Enter password:** and **Re-enter password:** fields, for Type 7 password encryption:

```
Router(config)# username us3 masked-password 7

Enter password:
Re-enter password:


Router(config)#commit
```

If there is a password mismatch between the two entries, an error message is displayed.

The following example shows how to enable password masking for a AAA password policy:

In this example, for user us6, a cleartext password is entered.

```
Router(config)# aaa password-policy security
Router(config)# username us6 password-policy security masked-password 0

Enter password:
Re-enter password:

Router(config)#commit
```

In the **show** command output, you can see the encrypted password.

```
Router# show run aaa
..

aaa password-policy security
..
username us6
 password-policy security password 7 0835585A
```

The encrypted password 0835585A is entered in the **Enter password:** and **Re-enter password:** fields for Type 7 password encryption.

```
Router(config)# username us6 password-policy test-policy masked-password 7

Enter password:
Re-enter password:


Router(config)#commit
```

Related Commands

Command	Description
aaa authentication , on page 15	Defines a method list for authentication.
aaa password-policy, on page 37	Defines the FIPS-compliant AAA password security policy
group (AAA), on page 59	Adds a user to a group.
password (AAA), on page 73	Creates a login password for a user.
secret, on page 101	Creates a secure login secret for a user.

users group

To associate a user group and its privileges with a line, use the **users group** command in line template configuration mode. To delete a user group association with a line, use the **no** form of this command.

users group {*usergroup-name* | **cisco-support** | **netadmin** | **operator** | **root-lr** | **root-system** | **sysadmin**}

Syntax Description

usergroup-name	Name of the user group. The *usergroup-name* argument can be only one word. Spaces and quotation marks are not allowed.
cisco-support	Specifies that users logging in through the line are given Cisco support personnel privileges.
netadmin	Specifies that users logging in through the line are given network administrator privileges.
operator	Specifies that users logging in through the line are given operator privileges.
root-lr	Specifies that users logging in through the line are given root logical router (LR) privileges.
root-system	Specifies that users logging in through the line are given root system privileges.
serviceadmin	Specifies that users logging in through the line are given service administrator group privileges.
sysadmin	Specifies that users logging in through the line are given system administrator privileges.

Command Default

None

Command Modes

Line template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **users group** command to enable a user group and its privileges to be associated with a line, meaning that users logging in through the line are given the privileges of the particular user group.

Task ID

Task ID	Operations
aaa	read, write

Examples

In the following example, if a vty-pool is created with line template *vty*, users logging in through vty are given operator privileges:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa authen login vty-authen line
RP/0/RSP0/CPU0:router(config)# commit
RP/0/RSP0/CPU0:router(config)# line template vty
```

```
RP/0/RSP0/CPU0:router(config-line)# users group operator
RP/0/RSP0/CPU0:router(config-line)# login authentication
```

vrf (RADIUS)

To configure the Virtual Private Network (VPN) routing and forwarding (VRF) reference of an AAA RADIUS server group, use the **vrf** command in RADIUS server-group configuration mode. To enable server groups to use the global (default) routing table, use the **no** form of this command.

vrf *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF.

Command Default

The default VRF is used.

Command Modes

RADIUS server-group configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **vrf** command to specify a VRF for an AAA RADIUS server group and enable dial-up users to use AAA servers in different routing domains.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to use the **vrf** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa group server radius group1
RP/0/RSP0/CPU0:router(config-sg-radius)# vrf vrf1
```

Related Commands

Command	Description
radius source-interface(BNG), on page 96	Forces RADIUS to use the IP address of a specified interface or subinterface for all outgoing RADIUS packets.
server-private (RADIUS), on page 107	Configures the IP address of the private RADIUS server for the group server.

vrf (TACACS+)

To configure the Virtual Private Network (VPN) routing and forwarding (VRF) reference of an AAA TACACS+ server group, use the **vrf** command in TACACS+ server-group configuration mode. To enable server groups to use the global (default) routing table, use the **no** form of this command.

vrf *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF.

Command Default

The default VRF is used.

Command Modes

TACACS+ server-group configuration

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

Use the **vrf** command to specify a VRF for an AAA TACACS+ server group and enable dial-up users to use AAA servers in different routing domains.

Task ID

Task ID	Operations
aaa	read, write

Examples

This example shows how to use the **vrf** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa group server tacacs+ myserver
RP/0/RSP0/CPU0:router(config-sg-tacacs+)# server 9.27.10.6
RP/0/RSP0/CPU0:router(config-sg-tacacs+)# vrf abc
```

Related Commands

Command	Description
aaa group server tacacs+, on page 34	Groups different TACACS+ server hosts into distinct lists and distinct methods.
server (TACACS+), on page 106	Specifies the source IP address of a selected interface for all outgoing TACACS+ packets.
server-private (TACACS+), on page 110	Configures the IP address of the private TACACS+ server for the group server.

Cisco TrustSec Commands

This module describes the commands used to configure Cisco TrustSec (CTS).

For detailed information about CTS concepts, configuration tasks, and examples, see the *Cisco TrustSec L2 and L3 Security Group Tag Propagation* chapter in *System Security Configuration Guide for Cisco ASR 9000 Series Routers*.

hw-module cts-enable all

To enable the Cisco TrustSec (CTS) for all ASR 9000 Enhanced Ethernet Line Cards use the **hw-module cts-enable all**command in Global Configuration mode.

hw-module cts-enable all

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 5.2.0	This command was introduced.

Usage Guidelines

The CTS solution allows you to intelligently control access to corporate data, allowing access control policies to be applied uniformly anywhere in the network. Use the **hw-module cts-enable all**command to manually enable an interface on the device for CTS, so that the device can propagate the CTS packet throughout the network.

Task ID

Task ID	Operation
root-lr	read, write

Example

The following example shows how to enable CTS.

```
RP/0/0RP0RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:IMC0(config)#hw-module cts-enable all
```

Related Commands

Command	Description
show controllers NP configSram, on page 193	Indicates if CTS is enabled for a device.

show controllers NP configSram

To command to check if CTS tag is enabled for a given port or not use the **show controllers NP configSram**command in EXEC mode.

show controllers NP configSram *portnum* {**all** | {**np0** | **np1**} **location** *node-id*}

Syntax Description

portnum	Represents the port number and the value ranges from 0 to 4294967295.
{**all**| {**np0**|**np1**}	Indicates if results for all nodes or only the designated node must be included in the output.
location *node id*	Clears detailed adjacency statistics for the designated node. The node-id argument is entered in the rack/slot/module notation.

Command Default

No default behavior or values

Command Modes

EXEC mode

Command History

Release	Modification
Release 5.2.0	This command was introduced.

Usage Guidelines

Use the command to check if CTS tag is enabled for a given port or not.

Task ID

Task ID	Operation
sonet-sdh, dwdm, interface, drivers	read

Example

This example shows the configuration with CTS-enabled for the specified port.

```
RP/0/RSP0/CPU0:IMC0#show controllers NP configSram 16 np1 location
0/0/CPU0
Step 4
Node: 0/0/CPU0:
----------------------------------------------------------------
NP1 Port=16 Port Config SRAM
-----------------------------------------
0xce400000 00000000 00201005 9c66eb5f
-----------------------------------------------
Field Name #Bits Value
-----------------------------------------------
ELMI Enable 0x0
CFM Enable 0x0
EFM Enable 0x0
EFM Block 0x0
EFM Loopback 0x0
LLDP Enable 0x0
Sat Port Uses MACinMAC Encaps 0x0
Ingress MAC Accounting 0x0
UDLD Enable 0x0
```

```
MPLS Racetrack Enable 0x1
L2 Racetrack Enable 0x1
Ipv4 Racetrack Enable 0x1
IPV6 Racetrack Enable 0x1Satellite NP Port 0x4c45
Bundle NP Port of Sat 0x494d
Port Sampled Span 0x0
Port Sampled Span Rate 0x0
Satellite Mode Hub & Spoke 0x0
satellite ingress unicast state 0x0
Member of ICL Bundle 0x0
Port CTS Enable 0x1
Router ID 0x9c66eb5f
MPLS Propagate TTL 0x1
Global Bundle L2 LB 0x0
Egr QoS ACL Bypass 0x1
Global Hash Rotate Value 0x0
MT Enable 0x0
Qos before PBR 0x0
MPLS Global LSR, FRR match 0x1
MPLS LSR 0x1
MPLS Global FRR 0x0
My MAC 0x0
```

Related Commands

Command	Description
hw-module cts-enable all, on page 192	Enables Cisco TrustSec (CTS).

IPSec Commands

This module describes the IPSec commands.

Note The following IPSec commands are available only if the <platform>-k9sec.pie is installed.

IPSec is supported only for Open Shortest Path First version 3 (OSPFv3).

clear crypto ipsec sa

To delete specific security associations (SAs), or all SAs in the IP Security (IPSec) security associations database (SADB), use the **clear crypto ipsec sa** command.

clear crypto ipsec sa {*sa-id* | **all** | **counters** | {*sa-id* | **all**} | **interface tunnel-ipsec**}

Syntax Description

sa-id	Identifier for the SA. IPSec supports from 1 to 64,500 sessions.
all	Deletes all IPSec SAs in the IPSec SADB.
counters	Clears the counters in the IPSec SADB.
interface	Clears the interfaces in the IPSec SADB.
tunnel-ipsec	The range of tunnel-ipsec is <0-4294967295>.

Command Default

No default behavior or values

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

SAs are established to secure data flows in IPSec. Use the **clear crypto ipsec sa** command to delete active IPSec sessions or force IPSec to reestablish new SAs. Usually, the establishment of SAs is negotiated between peers through Internet Key Exchange (IKE) on behalf of IPSec.

Task ID

Task ID	Operations
crypto	execute

Examples

The following example shows how to remove the SA with ID 100 from the SADB:

```
RP/0/RSP0/CPU0:router# clear crypto ipsec sa 100
```

Related Commands

Command	Description
show crypto ipsec sa, on page 199	Displays the settings used by current SAs.

description (IPSec profile)

To create a description of an IPSec profile, use the **description** command in profile configuration mode. To delete a profile description, use the **no** form of this command.

description *string*

Syntax Description

string	Character string describing the IPSec profile.

Command Default

None

Command Modes

Crypto IPSec profile

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **description** command inside the profile configuration submode to create a description for an IPSec profile.

Task ID

Task ID	Operations
profile configuration	read, write

Examples

The following example shows the creation of a profile description:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ipsec profile newprofile
RP/0/RSP0/CPU0:router(config-newprofile)# description this is a sample profile
```

interface tunnel-ip (GRE)

To configure a tunnel interface for generic routing encapsulation (GRE), use the **interface tunnel-ip** command in global configuration mode. To delete the IP tunnel interface, use the **no** form of this command.

interface tunnel-ip *number*
no interface tunnel-ip *number*

Syntax Description

number	Instance number of the interface. The range is from 0 to 65535.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to use the **interface tunnel-ip** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface tunnel-ip 50000
RP/0/RSP0/CPU0:router(config-if)#
```

show crypto ipsec sa

To display security association (SA) information based on the rack/slot/module location, use the **show crypto ipsec sa** command in EXEC mode.

show crypto ipsec sa [{*sa-id* | **peer** *ip-address* | **profile** *profile-name* | **detail** | **count** | **fvrf** *fvrf-name* | **ivrf** *ivrf-name* | **location** *node-id*}]

Syntax Description

sa-id	(Optional) Identifier for the SA. The range is from 1 to 64500.
peer *ip-address*	(Optional) IP address used on the remote (PC) side. Invalid IP addresses are not accepted.
profile *profile-name*	(Optional) Specifies the alphanumeric name for a security profile. The character range is from 1 to 64. Profile names cannot be duplicated.
detail	(Optional) Provides additional dynamic SA information.
count	(Optional) Provides SA count.
fvrf *fvrf-name*	(Optional) Specifies that all existing SAs for front door virtual routing and forwarding (FVRF) is the same as the fvrf-name.
ivrf *ivrf-name*	(Optional) Specifies that all existing SAs for inside virtual routing and forwarding (IVRF) is the same as the ivrf-name.
location *node-id*	(Optional) Specifies that the SAs are configured on a specified location.

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

If no optional argument or keyword is used, all SAs are displayed within a flow. Within a flow, the SAs are listed by protocol (Encapsulating Security Payload [ESP] or Authentication Header [AH]) and direction (inbound or outbound).

The **detail** keyword provides additional information only for SAs that are configured in a software crypto engine. The SAs are configured by using tunnel-ipsec and transport.

Task ID

Task ID	Operations
crypto	read

Examples

The following sample output is from the **show crypto ipsec sa** command:

```
RP/0/RSP0/CPU0:router# show crypto ipsec sa
```

```
SSA id:          510
Node id:        0/1/0
SA Type:        MANUAL
interface:      service-ipsec22
profile  :      p7
local  ident (addr/mask/prot/port) : (0.0.0.0/0.0.0.255/512/0)
remote ident (addr/mask/prot/port) : (0.0.0.0/0.0.0.0/512/0)
local crypto endpt: 0.0.0.0, remote crypto endpt: 0.0.0.0, vrf default

 #pkts tx         :0                      #pkts rx         :0
 #bytes tx        :0                      #bytes rx        :0
 #pkts encrypt    :0                      #pkts decrypt    :0
 #pkts digest     :0                      #pkts verify     :0
 #pkts encrpt fail:0                      #pkts decrpt fail:0
 #pkts digest fail:0                      #pkts verify fail:0
 #pkts replay fail:0
 #pkts tx errors  :0                      #pkts rx errors  :0

outbound esp sas:
        spi: 0x322(802)
        transform: esp-3des-md5
        in use settings = Tunnel
        sa agreed lifetime: 3600s, 4194303kb
        sa timing: remaining key lifetime: 3142303931sec/0kb
        sa DPD: disable, mode none, timeout 0s
        sa idle timeout: disable, 0s
        sa anti-replay (HW accel): enable, window 64
inbound esp sas:
        spi: 0x322(802)
        transform: esp-3des-md5
        in use settings = Tunnel
        sa agreed lifetime: 3600s, 4194303kb
        sa timing: remaining key lifetime: 3142303931sec/0kb
        sa DPD: disable, mode none, timeout 0s
        sa idle timeout: disable, 0s
        sa anti-replay (HW accel): enable, window 64
```

This table describes the significant fields shown in the display.

Table 11: show crypto ipsec sa Field Descriptions

Field	Description
SA id	Identifier for the SA.
interface	Identifier for the interface.
profile	String of alphanumeric characters that specify the name of a security profile.
local ident	IP address, mask, protocol, and port of the local peer.
remote ident	IP address, mask, protocol and port of the remote peer.
outbound esp sas	Outbound ESP SAs.
inbound esp sas	Inbound ESP SAs.
transform	The transform being used in the SA.

Field	Description
sa lifetime	The lifetime value used in the SA.

The following sample output is from the **show crypto ipsec sa** command for the **profile** keyword for a profile named pn1:

```
RP/0/RSP0/CPU0:router# show crypto ipsec sa profile pn1

SA id: 2
interface: tunnel0
profile: pn1
local ident (addr/mask/prot/port): (172.19.70.92/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (172.19.72.120/255.255.255.255/0/0)
local crypto endpt: 172.19.70.92, remote crypto endpt: 172.19.72.120
outbound esp sas:
spi: 0x8b0e950f (2332988687)
transform: esp-3des-sha
in use settings = Tunnel
sa lifetime: 3600s, 4194303kb

SA id: 2
interface: tunnel0
profile: pn1
local ident (addr/mask/prot/port): (172.19.72.120/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (172.19.70.92/255.255.255.255/0/0)
local crypto endpt: 172.19.72.120, remote crypto endpt: 172.19.70.92
inbound esp sas:
spi: 0x2777997c (662149500)
transform: esp-3des-sha
in use settings = Tunnel
sa lifetime: 3600s, 4194303kb
```

The following sample output is from the **show crypto ipsec sa** command for the **peer** keyword:

```
RP/0/RSP0/CPU0:router# show crypto ipsec sa peer 172.19.72.120

SA id: 2
interface: tunnel0
profile: pn1
local ident (addr/mask/prot/port): (172.19.70.92/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (172.19.72.120/255.255.255.255/0/0)
local crypto endpt: 172.19.70.92, remote crypto endpt: 172.19.72.120
outbound esp sas:
spi: 0x8b0e950f (2332988687)
transform: esp-3des-sha
in use settings = Tunnel
sa lifetime: 3600s, 4194303kb

SA id: 2
interface: tunnel0
profile: pn1
local ident (addr/mask/prot/port): (172.19.72.120/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (172.19.70.92/255.255.255.255/0/0)
local crypto endpt: 172.19.72.120, remote crypto endpt: 172.19.70.92
inbound esp sas:
spi: 0x2777997c (662149500)
transform: esp-3des-sha
in use settings = Tunnel
sa lifetime: 3600s, 4194303kb
```

show crypto ipsec summary

To display IP Security (IPSec) summary information, use the **show crypto ipsec summary** command in EXEC mode.

show crypto ipsec summary

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
crypto	read

Examples

The following sample output is from the **show crypto ipsec summary** command:

```
RP/0/RSP0/CPU0:router# show crypto ipsec summary

# * Attached to a transform indicates a bundle

# Active IPSec Sessions: 1

SA  Interface       Local Peer/Port   Remote Peer/Port  FVRF    Profile  Transform Lifetime
------------------------------------------------------------------------------------------
502 tunnel-ipsec100 70.70.70.2/500    60.60.60.2/500    default ipsec1   esp-3des  esp
3600/100000000
```

This table describes the significant fields shown in the display.

Table 12: show crypto ipsec summary Field Descriptions

Field	Description
SA	Identifier for the security association.
Node	Identifier for the node.
Local Peer	IP address of the local peer.
Remote Peer	IP address of the remote peer.

Field	Description
FVRF	The front door virtual routing and forwarding (FVRF) of the SA. If the FVRF is global, the output shows f_vrf as an empty field
Mode	Profile mode type.
Profile	Crypto profile in use.
Transform	Transform in use.
Lifetime	Lifetime value, displayed in seconds followed by kilobytes.

show crypto ipsec transform-set

To display the configured transform sets, use the **show crypto ipsec transform-set** command in EXEC mode.

show crypto ipsec transform-set [*transform-set-name*]

Syntax Description

transform-set-name	(Optional) IPSec transform set with the specified value for the *transform-set-name* argument are displayed.

Command Default

No default values. The default behavior is to print all the available transform-sets.

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

If no transform is specified, all transforms are displayed.

Task ID

Task ID	Operations
crypto	read

Examples

The following sample output is from the **show crypto ipsec transform-set** command:

```
RP/0/RSP0/CPU0:router# show crypto ipsec transform-set

Transform set combined-des-sha: {esp-des esp-sha-hmac}
Transform set tsfm2: {esp-md5-hmac esp-3des }
        Mode: Transport
Transform set tsfm1: {esp-md5-hmac esp-3des }
        Mode: Tunnel
Transform set ts1: {esp-des  }
        Mode: Tunnel
```

Keychain Management Commands

This module describes the commands used to configure keychain management.

For detailed information about keychain management concepts, configuration tasks, and examples, see the *Implementing Keychain Management on the Cisco ASR 9000 Series Router* configuration module in the *System Security Configuration Guide for Cisco ASR 9000 Series Routers*.

accept-lifetime

To set the time period during which the authentication key on a keychain is received as valid, use the **accept-lifetime** command in key configuration mode. To revert to the default value, use the **no** form of this command.

accept-lifetime *start-time* [{**duration** *duration value* | **infinite***end-time*}]

Syntax Description

start-time	Start time, in *hh:mm:ss day month year* format, in which the key becomes valid. The range is from 0:0:0 to 23:59:59. The range for the number of days of the month is from 1 to 31. The range for the years is from 1993 to 2035.
duration *duration value*	(Optional) Determines the lifetime of the key in seconds. The range is from 1-2147483646.
infinite	(Optional) Specifies that the key never expires after it becomes valid.
end-time	(Optional) Time, in *hh:mm:ss day month year* format, after which the key expires. The range is from 0:0:0 to 23:59:59.

Command Default

None

Command Modes

Key configuration

Command History

Release	Modification
Release 3.7.2	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 use the **accept-lifetime** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# key chain isis-keys
RP/0/RSP0/CPU0:router(config-isis-keys)# key 8
RP/0/RSP0/CPU0:router(config-isis-keys-0x8)# accept-lifetime 1:00:00 June 29 2006 infinite
```

Related Commands

Command	Description
key (key chain), on page 213	Creates or modifies a keychain key.
key chain (key chain), on page 216	Creates or modifies a keychain.
key-string (keychain), on page 218	Specifies the text for the key string.
send-lifetime, on page 220	Sends the valid key.
show key chain, on page 222	Displays the keychain.

ao

To specify the name the key chain used in the authentication option **ao** command in BGP neighbor configuration mode.

ao *key-chain-name* { **inheritance-disable** | **include-tcp-options** { **disable** | **enable** } **accept-ao-mismatch-connection** }

Syntax Description

key-chain-name	Specifies the name of the key chain. String of maximum length of 32 characters.
inheritance-disable	Prevents the key chain from being inherited from the parent.
include-tcp-options	Includes or excludes other TCP options in the header for MAC calculation.
disable	Excludes other TCP options in the header.
enable	Includes other TCP options in the header.
accept-ao-mismatch-connection	Accepts connection even if there is a mismatch of AO options between peers.

Command Default

The key chain has no specified name.

Command Modes

BGP neighbor

Command History

Release	Modification
Release 6.5.1	This command was introduced.

This example shows how to specify the name the key chain used in the authentication option :

```
RP/0/RSP0/CPU0:router#configure
RP/0/RSP0/CPU0:router(config)#router bgp 100
RP/0/RSP0/CPU0:router(config-bgp)#neighbor 10.51.51.1
RP/0/RSP0/CPU0:router(config-bgp-nbr)#address-family vpnv4 unicast
RP/0/RSP0/CPU0:router(config-bgp-nbr)#ao tcpao1 include-tcp-options disable
accept-ao-mismatch-connection
```

accept-tolerance

To specify the tolerance or acceptance limit, in seconds, for an accept key that is used by a peer, use the **accept-tolerance** command in keychain configuration mode. To disable this feature, use the **no** form of this command.

accept-tolerance [{*value* | **infinite**}]

Syntax Description

value	(Optional) Tolerance range, in seconds. The range is from 1 to 8640000.
infinite	(Optional) Specifies that the tolerance specification is infinite. The accept key never expires. The tolerance limit of infinite indicates that an accept key is always acceptable and validated when used by a peer.

Command Default

The default value is 0, which is no tolerance.

Command Modes

Keychain configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

If you do not configure the **accept-tolerance** command, the tolerance value is set to zero.

Even though the key is outside the active lifetime, the key is deemed acceptable as long as it is within the tolerance limit (for example, either prior to the start of the lifetime, or after the end of the lifetime).

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to use the **accept-tolerance** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# key chain isis-keys
RP/0/RSP0/CPU0:router(config-isis-keys)# accept-tolerance infinite
```

Related Commands

Command	Description
accept-lifetime, on page 206	Accepts the valid key.
key chain (key chain), on page 216	Creates or modifies a keychain.
show key chain, on page 222	Displays the keychain.

clear type6 client

To clear the Type 6 client state in case the primary key update process is stuck at any stage, use the **clear type6** command in EXEC mode.

clear type6 client { **keychain** | **snmp** }

Syntax Description

keychain	Clears the key chain client information.
snmp	Clears the snmp client information.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

You can track the primary key update operation using the **show type6 server** command output. If the *Master key Inprogress* field in that output displays as *YES*, then you can use **show type6 masterkey update status** command (or, **show type6 clients** command, prior to Cisco IOS XR Software Release 7.0.2) to check which client has not completed the operation. Accordingly, you can clear that particular client using this **clear** command.

Task ID

Task ID	Operation
system	read, write

This example shows how to clear the Type 6 client state:

```
Router#clear type6 client keychain
```

Related Commands

Command	Description
show type6, on page 224	Displays Type 6 password encryption information.

cryptographic-algorithm

To specify the choice of the cryptographic algorithm to be applied to the packets using the key string configured for the key ID, use the **cryptographic-algorithm** command in keychain-key configuration mode. To disable this feature, use the **no** form of this command.

cryptographic-algorithm [{**HMAC-MD5** | **HMAC-SHA1-12** | **HMAC-SHA1-20** | **MD5** | **SHA-1** | **HMAC-SHA-256** | **HMAC-SHA1-96** | **AES-128-CMAC-96** }]

Syntax Description

HMAC-MD5	Configures HMAC-MD5 as a cryptographic algorithm with a digest size of 16 bytes.
HMAC-SHA1-12	Configures HMAC-SHA1-12 as a cryptographic algorithm with a digest size of 12 bytes.
HMAC-SHA1-20	Configures HMAC-SHA1-20 as a cryptographic algorithm with a digest size of 20 bytes.
MD5	Configures MD5 as a cryptographic algorithm with a digest size of 16 bytes.
SHA-1	Configures SHA-1-20 as a cryptographic algorithm with a digest size of 20 bytes.
HMAC-SHA-256	Configures HMAC-SHA-256 as a cryptographic algorithm with a digest size of 32 bytes.
HMAC-SHA1-96	Configures HMAC-SHA1-96 as a cryptographic algorithm with a digest size of 12 bytes.
AES-128-CMAC-96	Configures AES-128-CMAC as a cryptographic algorithm with a digest size of 12 bytes.

Command Default

No default behavior or values

Command Modes

Keychain-key configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 6.5.1	Support for the following algorithms are added: • HMAC-SHA-256 • HMAC-SHA1-96 • AES-128-CMAC-96

Usage Guidelines

If you do not specify the cryptographic algorithm, MAC computation and API verification would be invalid.

These protocols support the following cryptographic algorithms:

- Border Gateway Protocol (BGP) supports only HMAC-MD5, HMAC-SHA1-12, AES-128-CMAC-96 and HMAC-SHA1-96.

- Intermediate System-to-Intermediate System (IS-IS) supports HMAC-MD5, SHA-1, MD5, AES-128-CMAC-96, HMAC-SHA-256, HMAC-SHA1-12, HMAC-SHA1-20, and HMAC-SHA1-96.
- Open Shortest Path First (OSPF) supports MD5, HMAC-MD5, HMAC-SHA-256, HMAC-SHA1-12, HMAC-SHA1-20, and HMAC-SHA1-96.

From Cisco IOS XR Software Release 6.7.2, Release 7.1.2, and later, you must follow these guidelines while enabling FIPS mode:

- You must configure the session with a FIPS-approved cryptographic algorithm. A session configured with non-approved cryptographic algorithm for FIPS (such as, **MD5** and **HMAC-MD5**) does not work. This is applicable for OSPF, BGP, RSVP, ISIS, or any application using key chain with non-approved cryptographic algorithm, in crypto FIPS mode.
- If you are using any **HMAC-SHA** algorithm for a session, then you must ensure that the configured *key-string* has a minimum length of 14 characters. Otherwise, the session goes down.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to use the **cryptographic-algorithm** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# key chain isis-keys
RP/0/RSP0/CPU0:router(config-isis-keys)# key 8
RP/0/RSP0/CPU0:router(config-isis-keys-0x8)# cryptographic-algorithm HMAC-MD5
```

Related Commands

Command	Description
accept-lifetime, on page 206	Accepts the valid key.
key chain (key chain), on page 216	Creates or modifies a keychain.
show key chain, on page 222	Displays the keychain.

key (key chain)

To create or modify a keychain key, use the **key** command in keychain-key configuration mode. To disable this feature, use the **no** form of this command.

key *key-id*

Syntax Description

key-id	48-bit integer key identifier of from 0 to 281474976710655.

Command Default

No default behavior or values

Command Modes

Keychain-key configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

For a Border Gateway Protocol (BGP) keychain configuration, the range for the *key-id* argument must be from 0 to 63. If the range is above the value of 63, the BGP keychain operation is rejected.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to use the **key** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# key chain isis-keys
RP/0/RSP0/CPU0:router(config-isis-keys)# key 8
RP/0/RSP0/CPU0:router(config-isis-keys-0x8)#
```

Related Commands

Command	Description
accept-lifetime, on page 206	Accepts the valid key.
key chain (key chain), on page 216	Creates or modifies a keychain.
key-string (keychain), on page 218	Specifies the text for the key string.
send-lifetime, on page 220	Sends the valid key.
show key chain, on page 222	Displays the keychain.

key (tcp ao keychain)

To configure in send and receive identifiers for the key, use the **key** command in TCP authentication option keychain configuration mode.

key *key-identifier* **sendID** *send-id-value* **ReceiveID** *receive-id-value*

Syntax Description

key-identifier	Identifier of the key. Acceptable values are 48-bit integers. Range is 0 to 281474976710655.
SendID *send-id-value*	Specifies the send identifier value. Range is 0 to 255.
ReceiveID *receive-id-value*	Specifies the receive identifier value to be used for the key. The range is 0 to 255.

Command Default

The key is not enabled.

Command Modes

TCP authentication option keychain

Command History

Release	Modification
Release 6.5.1	This command was introduced.

Task ID

Task ID	Operations
bgp	read

Examples

This example shows how to configure the send and receive identifier for the key.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# tcp ao
RP/0/RSP0/CPU0:router(conf-tcp-ao)# keychain tcpao1
RP/0/RSP0/CPU0:router(config-tcp-ao-tpcao1)# key 10 sendID 5 receiveID 5
```

keychain

To configure the keychain to be used in TCP authentication option, use the **tcp ao** command in TCP authentication option configuration mode.

keychain *keychain-name*

Syntax Description

This command has no arguments or keywords.

Command Default

The keychain is not enabled.

Command Modes

TCP authentication option

Command History

Release	Modification
Release 6.5.1	This command was introduced.

Task ID

Task ID	Operations
bgp	read

Examples

This example shows how to configure the **keychain** for TCP Authentication option:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# tcp ao
RP/0/RSP0/CPU0:router(conf-tcp-ao)keychain tcpao1
```

key chain (key chain)

To create or modify a keychain, use the **key chain** command in Global Configuration mode. To disable this feature, use the **no** form of this command.

key chain *key-chain-name*

Syntax Description

key-chain-name	Specifies the name of the keychain. The maximum number of characters is 48.

Command Default

No default behavior or values

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

You can configure a keychain for Border Gateway Protocol (BGP) as a neighbor, session group, or neighbor group. BGP can use the keychain to implement a hitless key rollover for authentication.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows that the name of the keychain isis-keys is for the **key chain** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# key chain isis-keys
RP/0/RSP0/CPU0:router(config-isis-keys)#
```

Related Commands

Command	Description
accept-lifetime, on page 206	Accepts the valid key.
accept-tolerance, on page 209	Configures a tolerance value to accept keys for the keychain.
key (key chain), on page 213	Creates or modifies a keychain key.
key-string (keychain), on page 218	Specifies the text for the key string.
send-lifetime, on page 220	Sends the valid key.
show key chain, on page 222	Displays the keychain.

key config-key password-encryption

To create a primary key for the Type 6 password encryption feature, use the **key config-key password-encryption** command in EXEC mode.

key config-key password-encryption [**delete**]

Syntax Description

delete	(Optional) Deletes the primary key for Type 6 password encryption.

Command Default

No primary key exists.

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Examples

The following example shows how to create a primary key for Type 6 password encryption:

```
Router# key config-key password-encryption

New password Requirements: Min-length 6, Max-length 64
Characters restricted to [A-Z][a-z][0-9]
Enter new key :
Enter confirm key :
Master key operation is started in background
```

The following example shows how to delete a primary key for Type 6 password encryption:

```
Router# key config-key password-encryption delete

WARNING: All type 6 encrypted keys will become unusable
Continue with master key deletion ? [yes/no]: yes
Master key operation is started in background
```

Related Commands

Command	Description
password6 encryption aes	Enables Type 6 password encryption feature.
show type6 server	Displays Type 6 password information.

key-string (keychain)

To specify the text string for the key, use the **key-string** command in keychain-key configuration mode. To disable this feature, use the **no** form of this command.

key-string [{**clear** | **password**}] *key-string-text*

Syntax Description

clear	Specifies the key string in clear-text form.
password	Specifies the key in encrypted form.
key-string-text	Text string for the key, which is encrypted by the parser process before being saved to the configuration. The text string has the following character limitations: • Plain-text key strings—Minimum of 1 character and a maximum of 32. • Encrypted key strings—Minimum of 4 characters and no maximum.

Command Default

The default value is clear.

Command Modes

Keychain-key configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

For an encrypted password to be valid, the following statements must be true:

- String must contain an even number of characters, with a minimum of four.
- The first two characters in the password string must be decimal numbers and the rest must be hexadecimals.
- The first two digits must not be a number greater than 53.

Either of the following examples would be valid encrypted passwords:

1234abcd

or

50aefd

From Cisco IOS XR Software Release 6.7.2, Release 7.1.2, and later, if you are using any **HMAC-SHA** algorithm for a session, then you must ensure that the configured *key-string* has a minimum length of 14 characters. Otherwise, the session goes down. This guideline is applicable only for FIPS mode.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to use the **keystring** command:

```
RP/0/RSP0/CPU0:router:# configure
RP/0/RSP0/CPU0:router(config)# key chain isis-keys
RP/0/RSP0/CPU0:router(config-isis-keys)# key 8
RP/0/RSP0/CPU0:router(config-isis-keys-0x8)# key-string password 850aefd
```

Related Commands

Command	Description
accept-lifetime, on page 206	Accepts the valid key.
key (key chain), on page 213	Creates or modifies a keychain key.
key chain (key chain), on page 216	Creates or modifies a keychain.
send-lifetime, on page 220	Sends the valid key.
show key chain, on page 222	Displays the keychain.

send-lifetime

To send the valid key and to authenticate information from the local host to the peer, use the **send-lifetime** command in keychain-key configuration mode. To disable this feature, use the **no** form of this command.

send-lifetime *start-time* [{**duration** *duration value* | **infinite***end-time*}]

Syntax Description

start-time	Start time, in *hh:mm:ss day month year* format, in which the key becomes valid. The range is from 0:0:0 to 23:59:59. The range for the number of days of the month to start is from 1 to 31. The range for the years is from 1993 to 2035.
duration *duration value*	(Optional) Determines the lifetime of the key in seconds.
infinite	(Optional) Specifies that the key never expires once it becomes valid.
end-time	(Optional) Time, in *hh:mm:ss day month year* format, after which the key expires. The range is from 0:0:0 to 23:59:59

Command Default

No default behavior or values

Command Modes

Keychain-key configuration

Command History

Release	Modification
Release 3.7.2	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 use the **send-lifetime** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# key chain isis-keys
RP/0/RSP0/CPU0:router(config-isis-keys)# key 8
RP/0/RSP0/CPU0:router(config-isis-keys-0x8)# send-lifetime 1:00:00 June 29 2006 infinite
```

Related Commands

Command	Description
accept-lifetime, on page 206	Accepts the valid key.

Command	Description
key (key chain), on page 213	Creates or modifies a keychain key.
key chain (key chain), on page 216	Creates or modifies a keychain.
key-string (keychain), on page 218	Specifies the text for the key string.

show key chain

To display the keychain, use the **show key chain** command in EXEC mode.

show key chain *key-chain-name*

Syntax Description

key-chain-name	Names of the keys in the specified keychain. The maximum number of characters is 32.

Command Default

If the command is used without any parameters, then it lists out all the key chains.

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
system	read

Examples

When a secure key storage becomes available, it is desirable for keychain management to alternatively prompt you for a primary password and display the key label after decryption. The following example displays only the encrypted key label for the **show key chain** command:

```
RP/0/RSP0/CPU0:router# show key chain isis-keys

Key-chain: isis-keys/ -

accept-tolerance -- infinite
Key 8 -- text "8"
  cryptographic-algorithm -- MD5
  Send lifetime:   01:00:00, 29 Jun 2006 - Always valid  [Valid now]
  Accept lifetime: 01:00:00, 29 Jun 2006 - Always valid [Valid now]
```

Related Commands

Command	Description
accept-lifetime, on page 206	Accepts the valid key.
accept-tolerance, on page 209	Configures a tolerance value to accept keys for the keychain.
key (key chain), on page 213	Creates or modifies a keychain key.
key chain (key chain), on page 216	Creates or modifies a keychain.
key-string (keychain), on page 218	Specifies the text for the key string.

Command	Description
send-lifetime, on page 220	Sends the valid key.

show type6

To view Type 6 password encryption information, use the **show type6** command in EXEC mode.

show type6 { **clients** | **masterkey update status** | **server** | **trace server** { **all** | **error** | **info** } [*trace-server-parameter*] }

Syntax Description

clients	Displays Type 6 client information.
masterkey update status	Displays Type 6 primary key operation status.
server	Displays Type 6 server information.
trace server	Displays Type 6 trace server information.
all	Displays all Type 6 traces.
error	Displays Type 6 error traces.
info	Displays Type 6 information trace entries.
trace-server-parameter	(Optional) Displays Type 6 trace server information for the specified parameter. Use one from the list of parameters defined in the Usage Guidelines section.

Command Default

None.

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.0.1	This command was introduced.
Release 7.0.2	This command was modified to include the **masterkey update status** option.

Usage Guidelines

In the command form **show type6 trace server info** *trace-server-parameter*, replace *trace-server-parameter* with one of the following parameters:

The **show type6 clients** command is deprecated with the introduction of **masterkey update status**.

Trace Server Parameter	Displayed Trace Server Information
file	The specified file.
hexdump	Hexadecimal format.
last	The most recent entries.
location	Line card location.
reverse	From the most recent entry to the first entry.

Trace Server Parameter	Displayed Trace Server Information
stats	Statistics information.
tailf	New traces as they are added.
udir	Copies trace information from remote locations to the specifed temporary directory.
unique	Unique entries with counts.
usec	User security information, with time stamp.
verbose	Internal debugging information.
wide	Removes buffer name, node name, and tid information.
wrapping	Wrapping entries.

Examples

The following command displays Type 6 password encryption feature information:

```
Router# show type6 server

Server detail information:
==========================
AES config State : Enabled
Masterkey config State : Enabled
Type6 feature State : Enabled
Master key Inprogress : No
```

```
Router# show type6 trace server all

Client file lib/type6/type6_server_wr
25 wrapping entries (18496 possible, 64 allocated, 0 filtered, 25 total)
Jul 19 09:59:27.168 lib/type6/type6_server_wr 0/RP0/CPU0 t7145 ***** Type6 server process
started Respawn count (1) ****
…
…
Jul 19 12:22:59.908 lib/type6/type6_server_wr 0/RP0/CPU0 t7145 User has started Master key
 operation (CREATE)
Jul 19 12:22:59.908 lib/type6/type6_server_wr 0/RP0/CPU0 t7145 Created Master key in TAM
successfully
Jul 19 12:23:00.265 lib/type6/type6_server_wr 0/RP0/CPU0 t7145 Master key Available set to
 (AVAILABLE)
Jul 19 12:23:00.272 lib/type6/type6_server_wr 0/RP0/CPU0 t7145 Master key inprogress set
to (NOT INPROGRESS)
```

```
Router# show type6 clients

Type6 Clients information:

Client Name   MK State
====================
keychain      UNKNOWN
```

This example shows a sample output of the **masterkey update status** command:

```
Router#show type6 masterkey update status
Thu Sep 17 06:50:07.980 UTC
```

```
Type6 masterkey operation is inprogress

Masterkey upate status information:
Client Name                Status
====================================
keychain                   INPROGRESS
```

Related Commands

Command	Description
clear type6 client, on page 210	Clears the Type 6 client state.

tcp ao

To enable the TCP authentication option, use the **tcp ao** command in global configuration mode.

tcp ao
no tcp ao

Syntax Description

This command has no arguments or keywords.

Command Default

The TCP authentication option is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
Release 6.5.1	This command was introduced.

Task ID

Task ID	Operations
bgp	read

Examples

This example shows how to configure the **tcp ao** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# tcp ao
```

MACsec Encryption Commands

This module describes the commands used to configure MACsec encryption.

Command History

Release	Modification
Release 5.3.2	The following commands were introduced. • cipher-suite • conf-offset • key-server-priority • lifetime • macsec • macsec-policy • security-policy • window-size
Release 6.0.1	The vlan-tags-in-clear command was introduced.
Release 6.1.2	macsec-service command was introduced.
Release 6.1.3	The following commands were introduced. • key chain • fallback-psk-keychain

allow (macsec)

To specify MACsec policy exception to allow packets in clear text, use **allow** command under MACsec policy configuration mode. To remove this configuration, use the **no** form of this command.

allow lacp-in-clear

Syntax Description

lacp-in-clear	Allows Link Aggregation Control Plane protocol (LACP) packets in clear text.

Command Default

None

Command Modes

MACsec policy configuration mode

Command History

Release	Modification
Release 7.3.1	This command was introduced.

Usage Guidelines

The **policy-exception lacp-in-clear** command under MACsec policy configuration mode is deprecated. Hence, it is recommended to use the **allow lacp-in-clear** command instead, to allow LACP packets in clear-text format.

Task ID

Task ID	Operations
system	read, write

Examples

This example shows how to create a MACsec policy exception to allow LACP packets in clear text:

```
Router#configure
Router(config)#macsec-policy P1
Router(config-macsec-policy-P1)#allow lacp-in-clear
Router(config-macsec-policy-P1)#commit
```

cipher-suite

Configures the cipher suite for encrypting traffic with MACsec in the MAcsec policy configuration mode.

The first portion of the cipher name indicates the encryption method, the second portion indicates the hash or integrity algorithm, and the third portion indicates the length of the cipher (128/256).

To disable this feature, use the **no** form of this command.

cipher-suite *encryption_ suite*

Syntax Description

encryption_suite	The GCM encryption method that uses the AES encryption algorithm. The available encryption suites are: • GCM-AES-128 • GCM-AES-256 • GCM-AES-XPN-128 • GCM-AES-XPN-256

Command Default

The default cipher suite chosen for encryption is GCM-AES-XPN-256.

Command Modes

MACsec policy configuration.

Command History

Release	Modification
Release 5.3.2	This command was introduced.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to use the **cipher-suite** command:

```
RP/0/RSP0/CPU0:router# configure t
RP/0/RSP0/CPU0:router(config)# macsec-policy mac_policy
RP/0/RSP0/CPU0:router(config-mac_policy)# cipher-suite GCM-AES-XPN-256
RP/0/RSP0/CPU0:router(config-mac_policy)#
```

conf-offset

Configures the confidentiality offset for MACsec encryption in the MACsec policy configuration mode.

To disable this feature, use the **no** form of this command.

conf-offset *offset_value*

Syntax Description

offset_value	Configures the offset value. The options are: • CONF-OFFSET-0 : Does not offset the encryption • CONF-OFFSET-30: Offsets the encryption by 30 characters • CONF-OFFSET-50: Offsets the encryption by 50 characters.

Command Default

Default value is 0.

Command Modes

MACsec policy configuration.

Command History

Release	Modification
Release 5.3.2	This command was introduced.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to use the **conf-offset** command:

```
RP/0/RSP0/CPU0:router# configure t
RP/0/RSP0/CPU0:router(config)# macsec-policy mac_policy
RP/0/RSP0/CPU0:router(config-mac_policy)# conf-offset CONF-OFFSET-30
RP/0/RSP0/CPU0:router(config-mac_policy)#
```

cryptographic-algorithm (MACsec)

Configures the cryptographic algorithm used for authenticating a peer for MACsec encryption in the Keychain-key configuration mode.

To disable this feature, use the **no** form of this command.

cryptographic-algorithm *authentication algorithm*

Syntax Description

authentication algorithm	Configures the 128-bit or 256-bit AES encryption algorithm.

Command Default

No default behavior or values.

Command Modes

Keychain-key configuration.

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

If you do not specify the cryptographic algorithm, MAC computation and API verification would be invalid.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to use the **cryptographic-algorithm** command for MACsec Encryption:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router# key chain mac_chain macsec
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec)# key 1234abcd5678
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec-1234abcd5678)# key-string
11111111111111111111111111111111 cryptographic-algorithm aes-256-cmac
```

Examples

The following example shows how to use the **AES-128-CMAC authentication algorithm** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router# key chain mac_chain macsec
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec)# key 1234abcd5678
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec-1234abcd5678)# key-string
12345678123456781234567812345678 cryptographic-algorithm aes-128-cmac
```

Examples

The following example shows how to use the **AES-256-CMAC authentication algorithm** command:

```
RP/0/RSP0/CPU0:router#configure
RP/0/RSP0/CPU0:router# key chain mac_chain macsec
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec) # key 1234abcd5678
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec-1234abcd5678)# key-string
12345678123456781234567812345678123456781234567812345678 cryptographic-algorithm
aes-256-cmac
```

enable-legacy-fallback

To enable interoperability with peer devices that do not support MACsec active fallback feature, use the **enable-legacy-fallback** command in MACsec policy configuration mode. To remove the configuration, use the **no** form of this command.

enable-legacy-fallback

Syntax Description

This command has no keywords or arguments.

Command Default

Disabled, by default.

Command Modes

MACsec policy configuration mode

Command History

Release	Modification
Release 6.7.2	This command was introduced for Cisco IOS XR 32-bit platforms.
Release 7.1.2	This command was introduced for Cisco IOS XR 64-bit platforms.

Usage Guidelines

For more details on MACsec active fallback feature, see the *Fallback PSK* section in the *Configuring MACsec Encryption* chapter in the *System Security Configuration Guide for Cisco ASR 9000 Series Routers*.

Task ID

Task ID	Operation
system	read, write

This example shows how to enable interoperability with peer devices that do not support MACsec active fallback feature:

```
Router#configure
Router(config)#macsec-policy P1
Router(config-macsec-policy-P1)#enable-legacy-fallback
Router(config-macsec-policy-P1)#commit
```

fallback-psk-keychain

To create or modify a fallback psk keychain key, use the **fallback-psk-keychain** command in keychain-key configuration mode.

To disable this feature, use the **no** form of this command.

fallback-psk-keychain *key-id*

Syntax Description

key-id	64-character hexadecimal string.

Command Default

No default behavior or values.

Command Modes

Key chain configuration

Command History

Release	Modification
Release 6.1.3	This command is introduced.

Usage Guidelines

The key must be of even number of characters. Entering an odd number of characters will exit the MACsec configuration mode.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to use the **key** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router# fallback-psk-keychain fallback_mac_chain
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec)# key 1234abcd5678
```

key

To create or modify a keychain key, use the **key** command in keychain-key configuration mode. To disable this feature, use the **no** form of this command.

key *key-id*

Syntax Description

key-id	64-character hexadecimal string.

Command Default

No default behavior or values.

Command Modes

Key chain configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

The key must be of even number of characters. Entering an odd number of characters will exit the MACsec configuration mode.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to use the **key** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router# key chain mac_chain macsec
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec)# key 1234abcd5678
```

key chain

To create or modify a keychain, use the **key chain** command in the key chain configuration mode.

To disable this feature, use the **no** form of this command.

key chain *key-chain-name*

Syntax Description

key-chain-name	Specifies the name of the keychain. The maximum length is 32 (128-bit encryption)/64 (256-bit encryption) character hexadecimal string.

Note If you are configuring MACsec to interoperate with a MACsec server that is running software prior to IOS XR 6.1.3, then ensure that the MACsec key length is of 64 characters. If the key length is lesser than 64 characters, authentication will fail.

Command Modes

Key chain configuration

Command Default

No default behavior or values

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how you can configure a key chain for MACsec encryption:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# key chain mac_chain macsec
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec)#
```

key-string

To specify the text string for the key, use the **key-string** command in keychain-key configuration mode.

To disable this feature, use the **no** form of this command.

key-string [{**clear** | **password**}] *key-string-text*

Syntax Description

clear	Specifies the key string in clear-text form.
passwordpassword	Specifies the key in encrypted form.
key-string-text	Text string for the key, which is encrypted by the parser process before being saved to the configuration. The text string has the following character limitations: • Plain-text key strings—Minimum of 1 character and a maximum of 32 (128-bit encryption)/64 (256-bit encryption) characters (hexadecimal string). • Encrypted key strings—Minimum of 4 characters and no maximum.

Command Default

The default value is clear.

Command Modes

Key chain configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

For an encrypted password to be valid, the following statements must be true:

- String must contain an even number of characters, with a minimum of four.
- The first two characters in the password string must be decimal numbers and the rest must be hexadecimals.
- The first two digits must not be a number greater than 53.

Either of the following examples would be valid encrypted passwords:

1234abcd

or

50aefd

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to use the **keystring** command:

```
! For AES 128-bit encryption

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# key chain mac_chain macsec
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec)# key 1234abcd5678
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec-1234abcd5678)# key-string
12345678123456781234567812345678 cryptographic-algorithm AES-128-CMAC

! For AES 256-bit encryption

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# key chain mac_chain macsec
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec)# key 1234abcd5678
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec-1234abcd5678)# key-string
1234567812345678123456781234567812345678123456781234567812345678 cryptographic-algorithm
AES-256-CMAC
```

key-server-priority

Configures the preference for a device to serve as the key server for MACsec encryption in the MACsec policy configuration mode. To disable this feature, use the **no** form of this command.

key-server-priority *value*

Syntax Description

value	Indicates the priority for a device to become the key server. Lower the value, higher the preference. The range is 0-255.

Command Default

Default value is 16.

Command Modes

MACsec policy configuration.

Command History

Release	Modification
Release 5.3.2	This command was introduced.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to use the **key-server-priority** command:

```
RP/0/RSP0/CPU0:router# configure t
RP/0/RSP0/CPU0:router(config)# macsec-policy mac_policy
RP/0/RSP0/CPU0:router(config-mac_policy)# key-server-priority 16
RP/0/RSP0/CPU0:router(config-mac_policy)#
```

lifetime

Configures the validity period for the MACsec key or CKN in the Keychain-key configuration mode. To disable this feature, use the **no** form of this command.

The lifetime period can be configured with a duration in seconds, as a validity period between two dates (for example, Jan 01 2014 to Dec 31 2014), or with an infinite validity.

The key is valid from the time you configure in HH:MM:SS format. Duration is configured in seconds.

When a key has expired, the MACsec session is torn down and running the **show macsec mka session** command does not display any information. If you run the **show macsec mka interface** and **show macsec mka interface detail** commands, you can see that the session is unsecured.

lifetime *start_time start_date*
{
end_time end_date |
duration *validity* | **infinite**
}

Syntax Description

start-time	Start time in hh:mm:ss from which the key becomes valid. The range is from 0:0:0 to 23:59:59.
end-time	End time in hh:mm:ss at which point the key becomes invalid. The range is from 0:0:0 to 23:59:59.
start_date	The date in DD month YYYY format that the key becomes valid.
end_date	The date in DD month YYYY format that the key becomes invalid.
duration *validity*	The key chain is valid for the duration you configure. You can configure duration in seconds.
infinite	The key chain is valid indefinitely.

Command Default

No default behavior or values

Command Modes

Keychain-key configuration

Command History

Release	Modification
Release 5.3.2	This command was introduced.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to use the **lifetime** command:

```
! For AES 128-bit encryption

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# key chain mac_chain macsec
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec)# key 1234abcd5678
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec-1234abcd5678)# key-string
12345678123456781234567812345678 cryptographic-algorithm AES-128-CMAC
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec-1234abcd5678)# lifetime 05:00:00 20 february
 2015 12:00:00 30 september 2016

! For AES 256-bit encryption

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# key chain mac_chain macsec
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec)# key 1234abcd5678
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec-1234abcd5678)# key-string
1234567812345678123456781234567812345678123456781234567812345678 cryptographic-algorithm
AES-256-CMAC
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec-1234abcd5678)# lifetime 05:00:00 20 february
 2015 12:00:00 30 september 2016
```

macsec

Enables MACsec on the router in the keychain configuration mode. To disable this feature, use the **no** form of this command.

macsec [**key** *key-id*]

Syntax Description

key-id	The key can be up to 64 bytes in length. The configured key is the CKN that is exchanged between the peers.

Command Default

No default behavior or values.

Command Modes

Keychain configuration

Command History

Release	Modification
Release 5.3.2	This command was introduced.

Usage Guidelines

From Cisco IOS XR Software Release 6.7.2, Release 7.1.2 and later, the MACsec key IDs are considered to be case insensitive. These key IDs are stored as uppercase letters. For example, a key ID of value 'FF' and of value 'ff' are considered to be the same, and both these key IDs are now stored in uppercase as 'FF'. Whereas, prior to Release 6.7.2 and Release 7.1.2, both these values were treated as case sensitive, and hence considered as two separate key IDs. However, the support for this case insensitive IDs is applicable only for the configurations done through CLI, and not for configurations done through Netconf protocol. Hence, it is recommended to have unique strings as key IDs for a MACsec key chain to avoid flapping of MACsec sessions.

For example, the key IDs ('FF' and 'ff') in this example are not unique (although one is in uppercase and other is in lowercase), and hence this might cause a MACsec session flap.

```
key chain 1
 macsec
  key FF
   lifetime 02:01:01 may 18 2020 infinite
  !
  key ff
   lifetime 01:01:01 may 18 2020 infinite
```

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to use the **macsec** command:

```
RP/0/RSP0/CPU0:router# configure t
RP/0/RSP0/CPU0:router(config)# key chain mac_chain macsec
```

```
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec)# key 1234abcd5678
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec-1234abcd5678)#
```

macsec-service

Configures a MACsec service for MACsec encryption in Global Configuration mode. To disable this feature, use the **no** form of this command.

macsec-service decrypyt-port *interface_number /port_number***psk-keychain** *key_chain_name***[policy]** *[policy_name]*

Syntax Description

interface_number /port_number	The port or interface number. The interfaces or ports are: Tthe port configured to face the Customer Edge router. The MACsec encryption port The MACsec decryption port
key-chain_name	Name of the key chain configured using the **key chain** command.
(optional) policy_name	Name of the MACsec policy for encryption configured using the **mac-sec policy** command. This is an optional keyword.

Command Default

No default behavior or values.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 6.1.1	This command was introduced.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to use the **macsec-service** command:

```
RP/0/RSP0/CPU0:router# interface  <interface>15.10  l2transport
RP/0/RSP0/CPU0:router(config)# encapsulation dot1q 10
RP/0/RSP0/CPU0:router macsec-service  decrypt-port  <intf>17.10   psk-keychain
<keychain_name>   [policy <macsec_policy>]
```

macsec shutdown

To enable MACsec shutdown, use the **macsec shutdown** command in Global Configuration mode. To disable MACsec shutdown, use the **no** form of the command.

macsec shutdown

Syntax Description

This command has no keywords or arguments.

Command Default

The **macsec shutdown** command is disabled by default.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 6.3.3	This command was introduced.

Usage Guidelines

Enabling the **macsec shutdown** command, brings down all macsec sessions on the MACsec-enabled interfaces and resets ports to non-macsec mode. The already existing MACsec configurations remain unaffected by enabling this feature.

Disabling the **macsec shutdown** command, brings up MACsec sessions for the configured interfaces and enforces MACsec policy on the port.

Warning Configuring **macsec shutdown** command disables MACsec on all data ports, system wide. Execute **clear** command to erase cached configuration or **commit** command to continue.

Task ID

Task ID	Operation
system	read, write

Example

The following example shows how to enable MACsec shutdown:

```
RP/0/RSP0/CPU0:router# configure terminal
RP/0/RSP0/CPU0:router(config)# macsec shutdown
```

macsec-policy

Creates a MACsec policy for MACsec encryption in Global Configuration mode. To disable this feature, use the **no** form of this command.

macsec-policy *policy_name*

Syntax Description

policy_name	Name of the MACsec policy for encryption.

Command Default

No default behavior or values.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 5.3.2	This command was introduced.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to use the **macsec-policy** command:

```
RP/0/RSP0/CPU0:router# configure t
RP/0/RSP0/CPU0:router(config)# macsec-policy mac_policy
RP/0/RSP0/CPU0:router(config-mac_policy)#
```

sak-rekey-interval

To set a timer value to rekey the MACsec secure association key (SAK) at a specified interval, use the **sak-rekey-interval** command in the macsec-policy configuration mode. To disable this feature, use the **no** form of this command.

sak-rekey-interval *timer-value*

Syntax Description

timer-value	Specifies the timer value, in seconds. Range is 60 to 2592000.

Command Default

The timer is set to OFF, by default

Command Modes

MACsec policy configuration.

Command History

Release	Modification
Release 6.3.3	This command was introduced.

Task ID

Task ID	Operations
system	read, write

Examples

This example shows how to set a timer value to rekey the MACsec SAK:

```
Router#configure
Router(config)#macsec-policy test-policy
Router(config-macsec-policy)#sak-rekey-interval 120
Router(config-macsec-policy)#commit
```

security-policy

Configures the type of data that is allowed to transit out of the interface configured with MACsec in the MACsec policy configuration mode. To disable this feature, use the **no** form of this command.

security-policy {**should-secure** | **must-secure**}

Syntax Description

should-secure	Configures the interface on which the MACsec policy is applied, to permit all data.
must-secure	Configures the interface on which the MACsec policy is applied, to permit only MACsec encrypted data.

Command Default

Default value is **must-secure**.

Command Modes

MACsec policy configuration.

Command History

Release	Modification
Release 5.3.2	This command was introduced.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to use the **security-policy** command:

```
RP/0/RSP0/CPU0:router# configure t
RP/0/RSP0/CPU0:router(config)# macsec-policy mac_policy
RP/0/RSP0/CPU0:router(config-mac_policy)# security-policy must-secure
RP/0/RSP0/CPU0:router(config-mac_policy)#
```

show macsec mka summary

To display the Summary of MACsec Sessions, use the **show macsec mka summary** command in EXEC mode.

show macsec mka summary

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values.

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

The **show macsec mka summary** command is available only with the installation of the k9sec rpm.

Task ID

Task ID	Operation
interface	read

This example shows how to view MACsec mka summary information for a specific interface.

```
 Router# show macsec mka summary
Fri Dec 15 06:41:13.299 UTC

NODE: node0_RP0_CPU0
================================================================================================
   Interface-Name     Status     Cipher-Suite       KeyChain       PSK/EAP       CKN
================================================================================================
     TF0/0/0/24       Secured  GCM-AES-XPN-256         kc1          PRIMARY     1111
     TF0/0/0/25       Secured  GCM-AES-XPN-256         kc1          PRIMARY     1111
     TF0/0/0/26       Secured  GCM-AES-XPN-256         kc1          PRIMARY     1111
     TF0/0/0/27       Secured  GCM-AES-XPN-256         kc1          PRIMARY     1111

Total MACSec Sessions  : 4
    Secured Sessions   : 4
    Pending Sessions   : 0
    Suspended Sessions : 0
    Active  Sessions   : 0
```

show macsec mka session

To display the detailed Information of MACsec Sessions, use the **show macsec mka session** command in EXEC mode.

show macsec mka session interface *interface name* **location** *location name* **detail**

Syntax Description

interface	Specifies the interface name to view MACsec details.
interface name	Enables MACsec mode for a specified interface.
location	Specifies the node location to enable the MACsec details.
location name	Enables MACsec mode for a specific node.
detail	(Optional) Detailed information specific to session.

Command Default

No default behavior or values.

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

The **show macsec mka session** command is available only with the installation of the k9sec rpm.

Task ID

Task ID	Operation
interface	read

This example shows how to view MACsec mka session information for a specific interface.

```
 Router# show macsec mka session
Fri Dec 15 06:31:38.457 UTC

NODE: node0_RP0_CPU0
==============================================================================================

   Interface-Name        Local-TxSCI       #Peers   Status   Key-Server   PSK/EAP      CKN
==============================================================================================

     TF0/0/0/24      ac3a.67ee.281c/0001     1      Secured      YES      PRIMARY     1111
     TF0/0/0/25      ac3a.67ee.281d/0001     1      Secured      YES      PRIMARY     1111
     TF0/0/0/26      ac3a.67ee.281e/0001     1      Secured      YES      PRIMARY     1111
     TF0/0/0/27      ac3a.67ee.281f/0001     1      Secured      YES      PRIMARY     1111
```

show macsec mka interface detail

To display detailed information on MACsec interfaces, use the **show macsec mka interface detail** command in the EXEC mode.

show macsec mka interface *interface name* **detail**

Syntax Description

interface name	Specifies the name of the interface for which you want to view the MACsec details.

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

The **show macsec mka interface detail** command is available only with the installation of the k9sec rpm.

The **show macsec mka interface detail** command displays information about all MACsec-enabled interfaces across all nodes. If you need MACsec information for a specific interface, use the **show macsec mka interface** *interface name* **detail** command.

Task ID

Task ID	Operation
system	read

This example shows how to view the MACsec information for a specific interface:

```
 Router# show macsec mka interface detail
Fri Dec 15 09:03:02.553 UTC

Number of interfaces on node node0_RP0_CPU0 : 4
--------------------------------------------------

Interface Name : TwentyFiveGigE0/0/0/24
    Interface Namestring     : TwentyFiveGigE0/0/0/24
    Interface short name     : TF0/0/0/24
    Interface handle         : 0x3c000060
    Interface number         : 0x3c000060
    MacSecControlledIfh      : 0x3c0081b0
    MacSecUnControlledIfh    : 0x3c0081b8
    Interface MAC            : ac3a.67ee.281c
    Ethertype                : 888E
    EAPoL Destination Addr   : 0180.c200.0003
    MACsec Shutdown          : FALSE
    Config Received          : TRUE
    IM notify Complete       : TRUE
    MACsec Power Status      : N/A
    Interface CAPS Add       : TRUE
    RxSA CAPS Add            : TRUE
    TxSA CAPS Add            : TRUE
```

```
Principal Actor          : Primary
MKA PSK Info
  Key Chain Name         : kc1
  MKA Cipher Suite       : AES-128-CMAC
  CKN                    : 11 11
MKA fallback_PSK Info
  fallback keychain Name : - NA -
Policy                   : DEFAULT-POLICY
SKS Profile              : N/A
Traffic Status           : Protected
Rx SC 1
  Rx SCI                 : ac4a6730061c0001
  Rx SSCI                : 1
  Peer MAC               : ac:4a:67:30:06:1c
  Is XPN                 : YES
  SC State               : Provisioned
  SAK State[0]           : Provisioned
  Rx SA Program Req[0]   : 2023 Dec 13 09:26:12.110
  Rx SA Program Rsp[0]   : 2023 Dec 13 09:26:12.172
  SAK Data
    SAK[0]               : ***
    SAK Len              : 32
    SAK Version          : 1
    HashKey[0]           : ***
    HashKey Len          : 16
    Conf offset          : 0
    Cipher Suite         : GCM-AES-XPN-256
    CtxSalt[0]           : ea ae af 7a b4 8b 1f 60 dd e9 60 a9
    CtxSalt Len          : 12
    ssci                 : 1
```

This example shows how to view the MACsec information for a interface:

```
router#show macsec mka interface
Fri Dec 15 06:45:25.738 UTC
================================================================================
   Interface-Name      KeyChain-Name   Fallback-KeyChain     Policy Name
================================================================================
     TF0/0/0/24             kc1              - NA -        DEFAULT-POLICY
     TF0/0/0/25             kc1              - NA -        DEFAULT-POLICY
     TF0/0/0/26             kc1              - NA -        DEFAULT-POLICY
     TF0/0/0/27             kc1              - NA -        DEFAULT-POLICY
```

show macsec mka statistics

To display MKA interface and session statistics, use the **show macsec mka statistics** command in EXEC mode.

show macsec mka statistics [**interface** *interface name* | **location** *location name*]

Syntax Description

interface	Specifies the interface name to view MACsec details.
interface name	Enables MACsec mode for a specified interface.
location *location name*	(Optional) Location of the node to view global statistics of the MKA instance.

Command Default

No default behavior or values.

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

The **show macsec mka statistics** command is available only with the installation of the k9sec rpm.

Task ID

Task ID	Operation
interface	read

This example shows the output for **show macsec mka statistics**:

```
 Router# show macsec mka statistics location 0/RP0/CPU0
Fri Dec 15 06:43:21.985 UTC


MKA Global Statistics
=====================
MKA Session Totals
   Secured..................... 10
   Reauthentication Attempts.. 0

   Deleted (Secured).......... 6
   Keepalive Timeouts......... 0

CA Statistics
   Pairwise CAKs Derived...... 0
   Pairwise CAK Rekeys........ 0
   Group CAKs Generated....... 0
   Group CAKs Received........ 0

SA Statistics
   SAKs Generated............. 10
   SAKs Rekeyed............... 0
   SAKs Received.............. 0
```

```
   SAK Responses Received..... 10
   PPK Tuple Generated........ 0
   PPK Retrieved.............. 0

MKPDU Statistics
   MKPDUs Validated & Rx...... 480156
      "Distributed SAK"..... 0
      "Distributed CAK"..... 0
      "Distributed PPK"..... 0
      "PPK Capable"......... 0
   MKPDUs Transmitted......... 480167
      "Distributed SAK"..... 10
      "Distributed CAK"..... 0
      "Distributed PPK"..... 0
      "PPK Capable"......... 0
```

show macsec mka client

To display MACsec MKA client traces, use the **show macsec mka client** command in EXEC mode.

show macsec mka client [trace {all | errors | events | info}]

Syntax Description

all	(Optional) Show all MACsec MKA client traces for the specified node, or the current node if none is specified.
errors	(Optional) Show MACsec MKA client error traces for the specified node, or the current node if none is specified.
events	(Optional) Show MACsec MKA client event traces for the specified node, or the current node if none is specified
info	(Optional) Show MACsec MKA client info traces for the specified node, or the current node if none is specified

Command Default

No default behavior or values.

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

The **show macsec mka trace** command is available only with the installation of the k9sec rpm.

Task ID

Task ID	Operation
interface	read

This example shows the output for **show macsec mka client trace all**:

```
 Router# show macsec mka client trace all
Tue Dec  5 10:32:14.266 UTC
1 wrapping entries (10432 possible, 192 allocated, 0 filtered, 1 total)
Dec  4 09:56:25.544 macsec_mka/client/events 0/RP0/CPU0 t5544 TP257:aipc, server:driver,
client:default, init from pid:4779
```

show macsec mka standby

To display MACsec MKA information from hot standby node, use the **show macsec mka standby** command in EXEC mode.

show macsec mka standby [interface | session | statistics] { *interface name* **detail** } **[summary]**

Syntax Description

interface	Specifies the interface name to view MACsec details.
interface name	Enables MACsec mode for a specified interface.
detail	(Optional) detailed information specific to Interface/Session

Command Default

No default behavior or values.

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

The **show macsec mka standby** command is available only with the installation of the k9sec rpm.

Task ID

Task ID	Operation
interface	read

This example shows the output for **show macsec mka standby summary**:

```
 Router# show macsec mka standby summary
Tue Dec  5 10:38:29.004 UTC

Total MACSec Sessions  : 0
    Secured Sessions   : 0
    Pending Sessions   : 0
    Suspended Sessions : 0
     Active  Sessions : 0
```

show macsec mka trace

To display MACsec MKA traces, use the **show macsec mka trace** command in EXEC mode.

show macsec mka trace [all | base | config | errors | events | new-errors | new-events]

Syntax Description

all	(Optional) Show all MACsec MKA traces for the specified node, or the current node if none is specified.
base	(Optional) Show MACsec MKA base traces for the specified node, or the current node if none is specified.
config	(Optional) Show MACsec MKA config traces for the specified node, or the current node if none is specified.
errors	(Optional) Show MACsec MKA error traces for the specified node, or the current node if none is specified.
events	(Optional) Show MACsec MKA event traces for the specified node, or the current node if none is specified.
new-errors	(Optional) Show MACsec MKA new-errors traces for the specified node, or the current node if none is specified.
new-events	(Optional) Show MACsec MKA new-event traces for the specified node, or the current node if none is specified.

Command Default

No default behavior or values.

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

The **show macsec mka trace** command is available only with the installation of the k9sec rpm.

Task ID

Task ID	Operation
interface	read

This example shows the output for **show macsec mka trace all**:

```
 Router# show macsec mka trace all
Fri Dec 15 06:42:04.919 UTC
2385 wrapping entries (8576 possible, 3968 allocated, 0 filtered, 2385 total)
Dec 12 15:12:30.077 macsec_mka/base 0/RP0/CPU0 t10778 TP1002: ********** MacSec MKA(10778)
 init start ********.
Dec 12 15:12:30.077 macsec_mka/new_events 0/RP0/CPU0 t10778 TP1002: ********** MacSec
MKA(10778) init start ********.
```

```
Dec 12 15:12:30.077 macsec_mka/events 0/RP0/CPU0 t10778 TP18: MKA_EVENT: Successfully created
 mka event queue
Dec 12 15:12:30.077 macsec_mka/base 0/RP0/CPU0 t10778 TP10: Timer init Success
Dec 12 15:12:30.077 macsec_mka/base 0/RP0/CPU0 t10778 TP801: process respawn_count:1
Dec 12 15:12:30.080 macsec_mka/base 0/RP0/CPU0 t10778 TP164: platform_capa : macsec:1,
macsec-service:0, macsec-subif:0, if_capa:1, ddp:1, secy_intf:1
Dec 12 15:12:30.080 macsec_mka/base 0/RP0/CPU0 t10778 TP164: platform_capa : ea_ha:0,
driver_ha:1, ea_retry:1, plt_sci:0, persist:0, max_an:3, no_secure_loc:1
Dec 12 15:12:30.080 macsec_mka/base 0/RP0/CPU0 t10778 TP164: platform_capa : issu:0,
ppk_support:1, pl_if_data:0, power_status:0, hot_stdby:0
Dec 12 15:12:30.080 macsec_mka/base 0/RP0/CPU0 t10778 TP1341: HA role: Active
```

show macsec secy

To display Interface based MACsec dataplane (SecY) statistics, use the **show macsec secy** command in EXEC mode.

show macsec secy [**stats** { **interface** *interface name* **sc** }]

Syntax Description

interface name	MACsec enabled Interface to be specified..
sc	(Optional) Display Secure Channel Statistics for both Rx-SC,SA and Tx-SC,SA specific to the given interface

Command Default

No default behavior or values.

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

The **show macsec secy** command is available only with the installation of the k9sec rpm.

Task ID

Task ID	Operation
interface	read

This example shows the output for **show macsec secy**:

```
 Router# show macsec mka secy stats interface HundredGigE 0/0/0/29 sc
Interface Stats
    InPktsUntagged     :  0
    InPktsNoTag        :  0
    InPktsBadTag       :  0
    InPktsUnknownSCI   :  0
    InPktsNoSCI        :  0
    InPktsOverrun      :  0
    InOctetsValidated  :  0
    InOctetsDecrypted  :  3510182
    OutPktsUntagged    :  0
    OutPktsTooLong     :  0
    OutOctetsProtected :  0
    OutOctetsEncrypted :  1827580
```

show macsec ea

To display MACsec programming details for each interface, use the **show macsec ea** command in EXEC mode.

show macsec ea [idb { **interface** *interface name* | | **location** *location name* } **| trace {all | errors | events| base}**

Syntax Description

interface	Specifies the interface name to view MACsec details.
interface name	Enables MACsec mode for a specified interface.
location	Specifies the node location to enable the MACsec details.
location name	Enables MACsec mode for a specific node.
all	(Optional) Show **all** MACsec EA traces for the specified node, or the current node if none is specified.
base	(Optional) Show MACsec EA **base** traces for the specified node, or the current node if none is specified.
errors	(Optional) Show MACsec EA **error** traces for the specified node, or the current node if none is specified.
events	(Optional) Show MACsec EA **event** traces for the specified node, or the current node if none is specified.

Command Default

No default behavior or values.

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

The **show macsec ea** command is available only with the installation of the k9sec rpm.

Task ID

Task ID	Operation
interface	read

This example shows how to view MACsec information for a specific interface located on location 0/RP0/CPU0.

```
 Router# show macsec ea idb location 0/RP0/CPU0
Mon Dec  4 03:59:07.481 UTC
```

```
IDB Details:
  if_sname                : TF0/0/0/23
  if_handle               : 0x3c000068
  MacSecControlledIfh     : 0x3c008120
  MacSecUnControlledIfh   : 0x3c008128
  Replay window size      : 64
  Local MAC               : ac:4a:67:30:06:1b
  Rx SC Option(s)         : Validate-Frames Replay-Protect
  Tx SC Option(s)         : Protect-Frames Always-Include-SCI
  Security Policy         : MUST SECURE
  Delay Protection        : FALSE
  Sectag offset           : 0
  db_init Req             : 2023 Dec 03 09:36:22.656
  db_init Rsp             : 2023 Dec 03 09:36:22.662
  if_enable Req           : 2023 Dec 03 09:36:22.663
  if_enable Rsp           : 2023 Dec 03 09:36:23.127
  Rx SC 1
    Rx SCI                : ac3a67ee281b0001
    Peer MAC              : ac:3a:67:ee:28:1b
    Stale                 : NO
    SAK Data
      SAK[2]              : ***
      SAK Len             : 32
      SAK Version         : 1
      HashKey[2]          : ***
      HashKey Len         : 16
      Conf offset         : 0
      Cipher Suite        : GCM-AES-XPN-256
      CtxSalt[2]          : e8 5c ca 8f b3 7a 9d 65 2a 35 ac f8
      ssci                : 2
      Rx SA Program Req[2]: 2023 Dec 03 09:36:27.632
      Rx SA Program Rsp[2]: 2023 Dec 03 09:36:27.712
```

This example shows how to view events associated with the MACsec ea command.

```
Router#show macsec ea trace events

Mon Dec  4 03:57:58.463 UTC
59 wrapping entries (18496 possible, 320 allocated, 0 filtered, 59 total)
Dec  3 09:36:02.903 macsec_ea/events 0/RP0/CPU0 t6945 TP155: ********** MacSec EA(0x1b21)
process START ********.
Dec  3 09:36:02.926 macsec_ea/events 0/RP0/CPU0 t6945 TP180: macsec_ea_programming_conn_up_cb
 received.
Dec  3 09:36:02.966 macsec_ea/events 0/RP0/CPU0 t6945 TP191: macsec_ea_platform_init success
Dec  3 09:36:03.050 macsec_ea/events 0/RP0/CPU0 t6945 TP208: ea_plat_cb_evq:
event_async_attach success, pulse_code:0x7c
Dec  3 09:36:03.050 macsec_ea/events 0/RP0/CPU0 t6945 TP211: ea_plat_cb_evq: created
successfully
Dec  3 09:36:03.083 macsec_ea/events 0/RP0/CPU0 t6945 TP121: ********** Started MacSec
EA(0x1b21) Successfully ********.
```

show macsec open-config

To display Open-config MACSEC traces, use the **show macsec open-config** command in EXEC mode.

show macsec opwn-config trace

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values.

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

The **show macsec open-config** command is available only with the installation of the k9sec rpm.

Task ID

Task ID	Operation
cisco-support	read

This example shows the output for **show macsec open-config trace**:

```
 Router#show macsec open-config trace
Fri Dec 15 09:08:37.760 UTC
20 wrapping entries (320 possible, 64 allocated, 0 filtered, 20 total)
Dec 12 12:42:43.823 oc_macsec/all 0/RP0/CPU0 t16252 oc_macsec_edm_open:313, Successful
Dec 12 12:42:43.823 oc_macsec/all 0/RP0/CPU0 t16252 oc_macsec_mka_oper_gl_sysdb_bind:173,
sysdb_bind successful
Dec 12 12:42:43.823 oc_macsec/all 0/RP0/CPU0 t16252 oc_macsec_if_sysdb_bind:315, sysdb bind
 successful
Dec 12 12:42:43.827 oc_macsec/all 0/RP0/CPU0 t16252 oc_macsec_mka_sysdb_bind:343, sysdb
bind: success
Dec 12 12:42:43.827 oc_macsec/all 0/RP0/CPU0 t16252
oc_macsec_mka_gl_stats_oper_sysdb_bind:372, sysdb_bind success
Dec 12 12:42:43.847 oc_macsec/all 0/RP0/CPU0 t16252 oc_macsec_reg_cfg_notif:250, Successful
Dec 12 15:12:31.317 oc_macsec/all 0/RP0/CPU0 t16252 oc_macsec_notify_if_macsec:74,
TwentyFiveGigE0_0_0_20: notif macsec_if_config, create/update
Dec 12 15:13:52.560 oc_macsec/all 0/RP0/CPU0 t16252 oc_macsec_notify_if_macsec:74,
TwentyFiveGigE0_0_0_21: notif macsec_if_config, create/update
Dec 12 15:16:41.447 oc_macsec/all 0/RP0/CPU0 t16252 oc_macsec_notify_if_macsec:74,
TwentyFiveGigE0_0_0_22: notif macsec_if_config, create/update
Dec 12 15:18:12.700 oc_macsec/all 0/RP0/CPU0 t16252 oc_macsec_notify_if_macsec:74,
TwentyFiveGigE0_0_0_23: notif macsec_if_config, create/update
Dec 12 15:47:30.887 oc_macsec/all 0/RP0/CPU0 t16252 oc_macsec_notify_if_macsec:74,
TenGigE0_0_0_24: notif macsec_if_config, create/update
Dec 13 08:39:35.878 oc_macsec/all 0/RP0/CPU0 t16252 oc_macsec_notify_if_macsec:74,
TenGigE0_0_0_24: notif macsec_if_config, delete
Dec 13 08:46:15.995 oc_macsec/all 0/RP0/CPU0 t16252 oc_macsec_notify_if_macsec:74,
TwentyFiveGigE0_0_0_20: notif macsec_if_config, delete
Dec 13 08:46:15.995 oc_macsec/all 0/RP0/CPU0 t16252 oc_macsec_notify_if_macsec:74,
```

```
TwentyFiveGigE0_0_0_21: notif macsec_if_config, delete
Dec 13 08:46:15.995 oc_macsec/all 0/RP0/CPU0 t16252 oc_macsec_notify_if_macsec:74,
TwentyFiveGigE0_0_0_22: notif macsec_if_config, delete
Dec 13 08:46:15.995 oc_macsec/all 0/RP0/CPU0 t16252 oc_macsec_notify_if_macsec:74,
TwentyFiveGigE0_0_0_23: notif macsec_if_config, delete
Dec 13 09:25:40.478 oc_macsec/all 0/RP0/CPU0 t16252 oc_macsec_notify_if_macsec:74,
TwentyFiveGigE0_0_0_24: notif macsec_if_config, create/update
Dec 13 09:27:59.242 oc_macsec/all 0/RP0/CPU0 t16252 oc_macsec_notify_if_macsec:74,
TwentyFiveGigE0_0_0_25: notif macsec_if_config, create/update
Dec 13 09:29:32.355 oc_macsec/all 0/RP0/CPU0 t16252 oc_macsec_notify_if_macsec:74,
TwentyFiveGigE0_0_0_26: notif macsec_if_config, create/update
Dec 13 09:31:03.658 oc_macsec/all 0/RP0/CPU0 t16252 oc_macsec_notify_if_macsec:74,
TwentyFiveGigE0_0_0_27: notif macsec_if_config, create/update
```

show macsec platform hardware

To display hardware-specific details for MACsec on each interface, use the **show macsec platform hardware** command in EXEC mode.

show macsec platform hardware [flow | sa | stats] { **interface** *interface name* | **location** *location name* }

Syntax Description

interface	Specifies the interface name to view MACsec details.
interface name	Enables MACsec mode for a specified interface.
location	Specifies the node location to enable the MACsec details.
location name	Enables MACsec mode for a specific node.

Command Default

No default behavior or values.

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

The **show macsec platform hardware** command is available only with the installation of the k9sec rpm.

Task ID

Task ID	Operation
interface	read

This example shows how to view MACsec platform hardware information for a specific interface located on location 0/RP0/CPU0.

```
 Router# show macsec platform hardware flow location 0/RP0/CPU0
Wed Dec 20 08:39:18.958 UTC
------------------------------------------
Interface : TwentyFiveGigE0_0_0_27


------------------------------------------
Interface : TwentyFiveGigE0_0_0_26


------------------------------------------
Interface : TwentyFiveGigE0_0_0_25


------------------------------------------
```

```
Interface : TwentyFiveGigE0_0_0_24
```

show macsec platform idb

To display interface database (IDB) details specific to MACsec, use the **show macsec platform idb** command in EXEC mode.

show macsec platform idb { **interface** *interface name* | **location** *location name* }

Syntax Description

interface	Specifies the interface name to view MACsec details.
interface name	Enables MACsec mode for a specified interface.
location	Specifies the node location to enable the MACsec details.
location name	Enables MACsec mode for a specific node.

Command Default

No default behavior or values.

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

The **show macsec platform idb** command is available only with the installation of the k9sec rpm.

Task ID

Task ID	Operation
interface	read

This example shows how to view MACsec platform idb information for a specific interface located on location 0/RP0/CPU0.

```
 Router# show macsec platform idb location 0/RP0/CPU0
Wed Dec 20 08:55:47.745 UTC

------------------------------------------------------------------
        EA IDB Details:
------------------------------------------------------------------
    IF Handle             : 0x3c000048
    IF Name               : TF0/0/0/27

------------------------------------------------------------------
        EA IDB Details:
------------------------------------------------------------------
    IF Handle             : 0x3c000050
    IF Name               : TF0/0/0/26

------------------------------------------------------------------
        EA IDB Details:
```

```
-------------------------------------------------------------------
    IF Handle             : 0x3c000058
    IF Name               : TF0/0/0/25

-------------------------------------------------------------------
        EA IDB Details:
-------------------------------------------------------------------
    IF Handle             : 0x3c000060
    IF Name               : TF0/0/0/24
```

show macsec platform stats

To display MACsec platform statistics, use the **show macsec platform stats** command in EXEC mode.

show macsec platform stats { **interface** *interface name* | **location** *location name* }

Syntax Description

interface	Specifies the interface name to view MACsec details.
interface name	Enables MACsec mode for a specified interface.
location	Specifies the node location to enable the MACsec details.
location name	Enables MACsec mode for a specific node.

Command Default

No default behavior or values.

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

The **show macsec platform stats** command is available only with the installation of the k9sec rpm.

Task ID

Task ID	Operation
interface	read

This example shows how to view MACsec platform statistics information for a specific interface located on location 0/RP0/CPU0.

```
 Router# show macsec platform stats location 0/RP0/CPU0
Wed Dec 20 08:56:13.285 UTC

------------------------------------------
Interface : TwentyFiveGigE0_0_0_27

------------------------------------------------------------------
    Global Statistics: Ingress
------------------------------------------------------------------
    Rx Ctrl Pkts                          : 47300
    Rx Ctrl Octets                        : 6905732
    Rx Data Pkts                          : 13
    Rx Data Octets                        : 894
    Rx OverSized Pkts                     : 0
    Rx Pkts Bad Tag                       : 0
    Rx Pkts No SCI                        : 0
    Rx Pkts No Tag                        : 0
    Rx Pkts Tagged                        : 0
    Rx Pkts Untagged                      : 0
```

```
    Rx Pkts Unknown SCI                     : 0
    Rx Pkts Untagged Miss                   : 0
    Rx Transform Error Pkts                 : 0
    Rx Pkts SA Not In Use                   : 0

-----------------------------------------------------------------
    Global Statistics: Egress
-----------------------------------------------------------------
    Tx Ctrl Pkts                            : 47308
    Tx Ctrl Octets                          : 6906216
    Tx Data Pkts                            : 16
    Tx Data Octets                          : 894
    Tx Pkts SA Not In Use                   : 0
    Tx Untagged Pkts                        : 0
    Tx Transform Error Pkts                 : 0

-----------------------------------------------------------------
    SA Statistics:Ingress
-----------------------------------------------------------------
    Index                                   : 0
    SCI                                     : ac3a67ee281f0001
    Current AN                              : 0
    Port                                    : 27
    Rx Data Pkts Decrypted                  : 13
    Rx Data Octets Decrypted                : 894
    Rx Pkts Delayed                         : 0
    Rx Pkts Invalid                         : 0
    Rx Pkts Late                            : 0
    Rx Pkts Not Using SA                    : 0
    Rx Pkts Not Valid                       : 0
    Rx Pkts Unchecked                       : 0
    Rx Pkts Untagged Hit                    : 0
    Rx Pkts Unused SA                       : 0
```

show macsec platform trace

To display MACsec platform trace logs, use the **show macsec platform trace** command in EXEC mode.

show macsec platform hardware trace [all | detail | errors | events] { **interface** *interface name* | **location** *location name* }

Syntax Description

interface	Specifies the interface name to view MACsec details.
interface name	Enables MACsec mode for a specified interface.
location	Specifies the node location to enable the MACsec details.
location name	Enables MACsec mode for a specific node.
all	(Optional) Show **all** MACsec Platform traces for the specified node, or the current node if none is specified.
detail	(Optional) Show MACsec Platform**detail** traces for the specified node, or the current node if none is specified.
errors	Optional) Show MACsec Platform **error** traces for the specified node, or the current node if none is specified.
events	(Optional) Show MACsec Platform **event** traces for the specified node, or the current node if none is specified.

Command Default

No default behavior or values.

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

The **show macsec platform trace** command is available only with the installation of the k9sec rpm.

Task ID

Task ID	Operation
interface	read

This example shows how to view MACsec platform trace information for a specific interface located on location 0/RP0/CPU0.

```
 Router# show macsec platform trace detail location 0/RP0/CPU0
Wed Dec 20 08:57:03.178 UTC
2023-12-19:06.28.09.556530212:34390:secydrv_client_commu_ipc_common_fvt_init:COMMU_IPC_DET_36:secydrv_client_commu_ipc_common_fvt_init
```

```
 called
2023-12-19:06.28.09.556530980:34390:secydrv_client_commu_ipc_fvt_init:COMMU_IPC_DET_53:secydrv_client_commu_ipc_fvt_init
 called
2023-12-19:06.28.09.558317574:34390:secydrv_commu_ipc_platform_init:COMMU_IPC_DET_83:secydrv_commu_ipc_platform_init
 called
2023-12-19:06.28.10.579426302:34390:secydrv_commu_ipc_resync_start:COMMU_IPC_DET_106:secydrv_commu_ipc_resync_start
 called
2023-12-19:06.28.10.596378984:34390:secydrv_commu_ipc_resync_stop:COMMU_IPC_DET_129:secydrv_commu_ipc_resync_stop
 called
2023-12-19:06.28.19.598852376:34390:macsec_ea_platform_poll_pn_exceeded:EAPD_DET_3192:PN
Threshold Check:No active sessions
2023-12-19:06.28.29.598939886:34390:macsec_ea_platform_poll_pn_exceeded:EAPD_DET_3192:PN
Threshold Check:No active sessions
2023-12-19:06.28.39.599043710:34390:macsec_ea_platform_poll_pn_exceeded:EAPD_DET_3192:PN
Threshold Check:No active sessions
2023-12-19:06.28.49.599136368:34390:macsec_ea_platform_poll_pn_exceeded:EAPD_DET_3192:PN
Threshold Check:No active sessions
2023-12-19:06.28.59.599221556:34390:macsec_ea_platform_poll_pn_exceeded:EAPD_DET_3192:PN
Threshold Check:No active sessions
2023-12-19:06.29.09.599315246:34390:macsec_ea_platform_poll_pn_exceeded:EAPD_DET_3192:PN
Threshold Check:No active sessions
2023-12-19:06.29.19.599396186:34390:macsec_ea_platform_poll_pn_exceeded:EAPD_DET_3192:PN
Threshold Check:No active sessions
2023-12-19:06.29.29.599470492:34390:macsec_ea_platform_poll_pn_exceeded:EAPD_DET_3192:PN
Threshold Check:No active sessions
2023-12-19:06.29.39.599542858:34390:macsec_ea_platform_poll_pn_exceeded:EAPD_DET_3192:PN
Threshold Check:No active sessions
2023-12-19:06.29.49.599616712:34390:macsec_ea_platform_poll_pn_exceeded:EAPD_DET_3192:PN
Threshold Check:No active sessions
2023-12-19:06.29.59.599691262:34390:macsec_ea_platform_poll_pn_exceeded:EAPD_DET_3192:PN
Threshold Check:No active sessions
2023-12-19:06.30.09.599768752:34390:macsec_ea_platform_poll_pn_exceeded:EAPD_DET_3192:PN
Threshold Check:No active sessions
2023-12-19:06.30.19.599842944:34390:macsec_ea_platform_poll_pn_exceeded:EAPD_DET_3192:PN
Threshold Check:No active sessions
2023-12-19:06.30.27.011625732:34390:macsec_ea_platform_idb_init:EAPD_DET_1026:IDB Init:
ifh: 0x3c000060, if_name TF0/0/0/24, slot 0
2023-12-19:06.30.27.011632184:34390:secydrv_commu_ipc_if_init:COMMU_IPC_DET_151:secydrv_commu_ipc_if_init
 called
```

suspendFor

In an ISSU scenario, you can use the **suspendFor** command in macsec policy configuration mode to control the MACsec Key Agreement (MKA) protocol suspension initiation on the key server or the request for suspension from the non-key server. To remove the configuration, use the **no** form of this command

suspendFor disable

Syntax Description

disable	Disables the MKA protocol suspension initiation on the key server or disables the request for suspension from the non-key server.

Command Default

By default, the option is enabled.

Command Modes

Macsec policy configuration

Command History

Release	Modification
Release 7.1.1	This command was introduced.

Usage Guidelines

If the key server has the **suspendfor disable** command configured under the macsec policy, then it does not allow ISSU process from any non-key server.

Task ID

Task ID	Operation
system	read, write

This example shows how to disable MKA protocol suspension initiation on the key server or to disable the request for suspension from the non-key server:

```
Router(config)#macsec-policy test-policy-mp
Router(config-macsec-policy)#suspendFor disable
Router(config-macsec-policy)#commit
```

Related Commands

Command	Description
suspendOnRequest, on page 277	Initiates MKA protocol suspension if it is the key server and when another participant has requested for suspension.

suspendOnRequest

In an ISSU scenario, to control the MACsec Key Agreement (MKA) protocol suspension initiation if it is the key server and when another peer has requested for suspension, use the **suspendOnRequest** command in macsec policy configuration mode. To remove the configuration, use the **no** form of this command.

suspendOnRequest disable

Syntax Description

disable	Rejects the suspension request from the non-key server, in an ISSU scenario.

Command Default

By default, the option is enabled.

Command Modes

Macsec policy configuration

Command History

Release	Modification
Release 7.1.1	This command was introduced.

Usage Guidelines

This command is applicable only to the key server.

Task ID

Task ID	Operation
system	read, write

This example shows how to disable the suspension request from the non-key server, in an ISSU scenario:

```
Router(config)#macsec-policy test-policy-mp
Router(config-macsec-policy)#suspendOnrequest disable
Router(config-macsec-policy)#commit
```

Related Commands

Command	Description
suspendFor, on page 276	Controls MKA protocol suspension on the key server or the request for suspension from the non-key server in an ISSU scenario.

vlan-tags-in-clear

Configures the number of VLAN tags in clear for MACsec encryption in the MACsec policy configuration mode. To disable this feature, use the **no** form of this command.

vlan-tags-in-clear *number*

Syntax Description

number	Specifies the number of VLAN tags in clear. For 802.1q encapsulation with a single tag, the value is 1. For 802.1q encapsulation with two tags, the value is 2. For 802.1ad encapsulation with a single tag, the value is 1. For 802.1ad encapsulation with a two tags, the value is 2.

Command Default

Default value is 1.

Command Modes

MACsec policy configuration mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to use the **vlan-tags-in-clear** command:

```
RP/0/RSP0/CPU0:router# configure t
RP/0/RSP0/CPU0:router(config)# macsec-policy mac_policy
RP/0/RSP0/CPU0:router(config-mac_policy)# vlan-tags-in-clear 1
```

window-size

Configures the replay protection window size in MACsec policy configuration mode. To disable this feature, use the **no** form of this command.

The replay protection window size indicates the number of out-of-sequence frames that can be accepted at the interface configured with MACsec, without being dropped.

window-size *value*

Syntax Description

value	Number of out-of-sequence frames that can be accepted at the interface without being dropped. The range is 0-1024.

Command Default

Default value is 64.

Command Modes

MACsec policy configuration.

Command History

Release	Modification
Release 5.3.2	This command was introduced.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to use the **window-size** command:

```
RP/0/RSP0/CPU0:router# configure t
RP/0/RSP0/CPU0:router(config)# macsec-policy mac_policy
RP/0/RSP0/CPU0:router(config-mac_policy)# window-size 64
```

Lawful Intercept Commands

This module describes the Cisco IOS XR software commands used to configure lawful intercept (LI).

For detailed information about keychain management concepts, configuration tasks, and examples, see the *Implementing Lawful Intercept inthe Cisco ASR 9000 Series RouterSoftware the Configuration Module* .

lawful-intercept disable

To disable the Lawful Intercept (LI) feature, use the **lawful-intercept disable** command in Global Configuration mode. To re-enable the LI feature, use the **no** form of this command.

lawful-intercept disable

Syntax Description

This command has no keywords or arguments.

Command Default

LI feature is enabled by default only if the LI package is installed.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 4.1.0	This command is introduced.
Release 4.3.2	By default, Lawful Intercept (LI) is not a part of the Cisco IOS XR software. The LI image needs to be installed separately by activating the asr9k-li-px.pie. So this command is available only after installing and activating the asr9k-li-px.pie.

Usage Guidelines

If you disable lawful intercept, all Mediation Devices and associated TAPs are deleted.

To enable this command, you must install and activate the LI image.

Task ID

Task ID	Operations
li	read, write

Examples

This example shows how to configure the **lawful-intercept disable** command:

```
RP/0/RSP0/CPU0:router(config)# lawful-intercept disable
```

overlap-tap enable

To configure traffic interception separately for two inter-communicating intercepted hosts, use the **overlap-tap enable** command in Global Configuration mode. To revert to the default configuration, use the **no** form of this command.

overlap-tap enable

Syntax Description

This command has no keywords or arguments.

Command Default

For two inter-communicating hosts where both the hosts are separately intercepted, only the ingress traffic on the ASR 9000 router related to one of the hosts is intercepted.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 5.3.2	This command was introduced.

Usage Guidelines

To use **overlap-tap enable** command, you must have lawful intercept configured by installing and activating **asr9k-li-px.pie**.

Task ID

Task ID	Operation
li	read

Example

The following example shows how to configure interception of both the ingress and egress traffic on the ASR 9000 router related to two inter-communicating hosts.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# overlap-tap enable
```

Management Plane Protection Commands

This module describes the commands used to configure management plane protection (MPP).

For detailed information about keychain management concepts, configuration tasks, and examples, see the *Implementing Management Plane Protection on* the Cisco ASR 9000 Series Router module in the *System Security Configuration Guide for Cisco ASR 9000 Series Routers* .

address ipv4 (MPP)

To configure the peer IPv4 address in which management traffic is allowed on the interface, use the **address ipv4**command in interface peer configuration mode. To remove the IP address that was previously configured on this interface, use the **no** form of this command.

address ipv4 {*peer-ip-address* | *peer-ip-address/ length*}

Syntax Description

peer-ip-address	Peer IPv4 address in which management traffic is allowed on the interface. This address can effectively be the source address of the management traffic that is coming in on the configured interface.
peer ip-address/length	Prefix of the peer IPv4 address. • IPv4—*A.B.C.D/length*

Command Default

If no specific peer is configured, all peers are allowed.

Command Modes

Interface peer configuration

Command History

Release	Modification
Release 3.7.2	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 configure the peer IPv4 address 10.1.0.0 with a prefix of 16 for management traffic:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# control-plane
RP/0/RSP0/CPU0:router(config-ctrl)# management-plane
RP/0/RSP0/CPU0:router(config-mpp)# inbandout-of-band
RP/0/RSP0/CPU0:router(config-mpp-inbandoutband)# interface GigabitEthernet POS 0/16/10/12
RP/0/RSP0/CPU0:router(config-mpp-inbandoutband-GigabitEthernet0_1_1_1POS0_6_0_2)# allow
Telnet TFTP peer
RP/0/RSP0/CPU0:router(config-telnettftp-peer)# address ipv4 10.1.0.0/16ipv6 33::33
```

Related Commands

Command	Description
address ipv6 (MPP), on page 288	Configures the peer IPv6 address in which management traffic is allowed on the interface.

Command	Description
allow, on page 290	Configures an interface as an inband or out-of-band interface to allow all peer addresses for a specified protocol or all protocols.
control-plane, on page 294	Configures the control plane.
inband, on page 295	Configures an inband interface or protocol.
interface (MPP), on page 296	Configures a specific inband or out-of-band interface or all inband or out-of-band interfaces.
management-plane, on page 298	Configures management plane protection to allow and disallow protocols.
out-of-band, on page 299	Configures out-of-band interfaces or protocols and enters management plane protection out-of-band configuration mode.
show mgmt-plane, on page 301	Displays the management plane.

address ipv6 (MPP)

To configure the peer IPv6 address in which management traffic is allowed on the interface, use the **address ipv6** command in interface peer configuration mode. To remove the IP address that was previously configured on this interface, use the **no** form of this command.

address ipv6 {*peer-ip-address* | *peer-ip-address*/*length*}

Syntax Description

peer-ip-address	Peer IPv6 address in which management traffic is allowed on the interface. This address can effectively be the source address of the management traffic that is coming in on the configured interface.
s*peer ip-address/length*	Prefix of the peer IPv6 address.

Command Default

If no specific peer is configured, all peers are allowed.

Command Modes

Interface peer configuration

Command History

Release	Modification
Release 3.7.2	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 configure the peer IPv6 address 33::33 for management traffic:

```
RR/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# control-plane
RP/0/RSP0/CPU0:router(config-ctrl)# management-plane
RP/0/RSP0/CPU0:router(config-mpp)# out-of-band
RP/0/RSP0/CPU0:router(config-mpp-outband)# interface
            GigabitEthernet 0/1/1/2

RP/0/RSP0/CPU0:router(config-mpp-outband-GigabitEthernet0_1_1_2)# allow TFTP peer
RP/0/RSP0/CPU0:router(config-tftp-peer)# address ipv6 33::33
```

Related Commands

Command	Description
address ipv4 (MPP), on page 286	Configures the peer IPv4 address in which management traffic is allowed on the interface.
allow, on page 290	Configures an interface as an inband or out-of-band interface to allow all peer addresses for a specified protocol or all protocols.
control-plane, on page 294	Configures the control plane.
inband, on page 295	Configures an inband interface or protocol.
interface (MPP), on page 296	Configures a specific inband or out-of-band interface or all inband or out-of-band interfaces.
management-plane, on page 298	Configures management plane protection to allow and disallow protocols.
out-of-band, on page 299	Configures out-of-band interfaces or protocols and enters management plane protection out-of-band configuration mode.
show mgmt-plane, on page 301	Displays the management plane.

allow

To configure an interface as an inband or out-of-band interface to allow all peer addresses for a specified protocol or all protocols, use the **allow** command in management plane protection inband interface configuration mode or management plane protection out-of-band interface configuration. To disallow a protocol on an interface, use the **n**o form of this command.

allow {*protocol* | **all**} [**peer**]

Syntax Description

protocol	Interface configured to allow peer-filtering for the following specified protocol's traffic: • HTTP(S) • SNMP (also versions) • Secure Shell (v1 and v2) • TFTP • Telnet • XML
all	Configures the interface to allow peer-filtering for all the management traffic that is specified in the list of protocols.
peer	(Optional) Configures the peer address on the interface. Peer refers to the neighboring router interface in which traffic might arrive to the main router.

Command Default

By default, no management protocol is allowed on any interface except the management interfaces.

Command Modes

Management plane protection inband interface configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.0.0	The XML keyword was added.

Usage Guidelines

If you permit or allow a specific protocol to an interface, traffic is allowed only for that protocol, and all other management traffic is dropped.

After you configure the interface as inband or out-of-band, the specified protocol's traffic, or all protocol traffic, is allowed on the interface. Interfaces that are not configured as inband or out-of-band interfaces, drop the protocol traffic.

The IOS XR XML API provides a programmatic interface to the router for use by external management applications. This interface provides a mechanism for router configuration and monitoring utilizing XML formatted request and response streams. As one of the management services, XML should be capable of applying MPP. To secure XML MPP data, XML keyword has been added to the command.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to configure all management protocols for all inband interfaces:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# control-plane
RP/0/RSP0/CPU0:router(config-ctrl)# management-plane
RP/0/RSP0/CPU0:router(config-mpp)# inband
RP/0/RSP0/CPU0:router(config-mpp-inband)# interface all
RP/0/RSP0/CPU0:router(config-mpp-inband-all)# allow all
```

The following example shows how to configure peer interface for the TFTP protocol for out-of-band interfaces:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# control-plane
RP/0/RSP0/CPU0:router(config-ctrl)# management-plane
RP/0/RSP0/CPU0:router(config-mpp)# out-of-band
RP/0/RSP0/CPU0:router(config-mpp-outband)# interface GigabitEthernet 0/1/1/2
RP/0/RSP0/CPU0:router(config-mpp-outband-GigabitEthernet0_1_1_2)# allow TFTP peer
RP/0/RSP0/CPU0:router(config-tftp-peer)#
```

The following example shows how to configure MPP support on an XML peer in-band interface:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# control-plane
RP/0/RSP0/CPU0:router(config-ctrl)# management-plane
RP/0/RSP0/CPU0:router(config-ctrl-mpp)# inband interface all allow xml peer address ipv4
172.10.10.1
```

Related Commands

Command	Description
control-plane, on page 294	Configures the control plane.
inband, on page 295	Configures an inband interface or protocol.
interface (MPP), on page 296	Configures a specific inband or out-of-band interface or all inband or out-of-band interfaces.
management-plane, on page 298	Configures management plane protection to allow and disallow protocols.
out-of-band, on page 299	Configures out-of-band interfaces or protocols and enters management plane protection out-of-band configuration mode.
show mgmt-plane, on page 301	Displays the management plane.

allow local-port

To configure a local port and third-party application protocols for management plane protection (MPP) on an interface, use the **allow local-port** command in management plane protection TPA mode. To disallow a protocol on an interface, use the **no** form of this command.

allow local-port *port-number* **protocol** *protocol-number* **interface** *interface-name* **local-address** *IP local address* **remote-address** *IP remote address*

Syntax Description

local-port	Specifies local L4 port of an interface.
protocol	Specifies the L4 protocol to be configured on MPP.
Protocol number	Enter the protocol number corresponding to different protocols. You can choose a value from range 1 to 255. Following are some of the protocol numbers dedicated to different protocols: • gre - Generic Routing Encapsulation. (47) • udp - User Datagram Protocol, RFC 768. (17) • tcp - Transmission Control Protocol, RFC 793. (6) • pptp - Point-to-Point Tunneling Protocol. Entering the pptp protocol literal is equivalent to entering the gre protocol literal. (47) • pim - Protocol Independent Multicast. (103) • ospf - Open Shortest Path First routing protocol, RFC 1247. (89) • ipsec - IP Security. Entering the ipsec protocol literal is equivalent to entering the esp protocol literal. (50) • ipinip - IP-in-IP encapsulation. (4) • icmp6 - Internet Control Message Protocol for IPv6, RFC 2463. (58) • igmp - Internet Group Management Protocol, RFC 1112. (2) • igrp - Interior Gateway Routing Protocol. (9) **Note** In IOS XR release 6.5.2, protocol number is replaced by protocol names. The supported protocols are *tcp* and *udp*.
interface	Specify the MPP interface on which the protocol has to be configured.
local-address	Specify the local IP address of the host or client.
remote-address	Specify the remote IP address of the host or client.

Command Default

Not Applicable

Command Modes

Management plane protection TPA

Command History

Release	Modification
Release 6.3.2	This command was introduced.

Example

```
Router(config)# control-plane
Router(config-ctrl)# management-plane
Router(config-mpp)# tpa vrf default address-family [ipv4 | ipv6]
Router(config-mpp-tpa-vrf-afi)# allow local-port 57600 protocol tcp interface mgmtEth
0/RP0/CPU0/0 local-address 10.1.1.1/32 remote-address 10.2.2.2/32
```

control-plane

To enter the control plane configuration mode, use the **control-plane** command in Global Configuration mode. To disable all the configurations under control plane mode, use the **no** form of this command.

control-plane

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **control-plane** command to enter control plane configuration mode.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to enter control plane configuration mode using the **control-plane** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# control-plane
RP/0/RSP0/CPU0:router(config-ctrl)#
```

Related Commands

Command	Description
management-plane, on page 298	Configures management plane protection to allow and disallow protocols.

inband

To configure an inband interface and to enter management plane protection inband configuration mode, use the **inband** command in management plane protection configuration mode. To disable all configurations under inband configuration mode, use the **no** form of this command.

inband

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Management plane protection configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **inband** command to enter management plane protection inband configuration mode.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to enter management plane protection inband configuration mode using the **inband** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# control-plane
RP/0/RSP0/CPU0:router(config-ctrl)# management-plane
RP/0/RSP0/CPU0:router(config-mpp)# inband
RP/0/RSP0/CPU0:router(config-mpp-inband)#
```

Related Commands

Command	Description
control-plane, on page 294	Configures the control plane.
interface (MPP), on page 296	Configures a specific inband or out-of-band interface or all inband or out-of-band interfaces.
management-plane, on page 298	Configures management plane protection to allow and disallow protocols.
out-of-band, on page 299	Configures out-of-band interfaces or protocols and enters management plane protection out-of-band configuration mode.
show mgmt-plane, on page 301	Displays the management plane.

interface (MPP)

To configure a specific interface or all interfaces as an inband or out-of-band interface, use the **interface** command in management plane protection inband configuration mode or management plane protection out-of-band configuration mode. To disable all the configurations under an interface mode, use the **no** form of this command.

interface {*type* *interface-path-id* | **all**}

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Virtual interface instance. Number range varies depending on interface type. **Note** Use the **show interfaces** command in EXEC mode to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
all	Configures all interfaces to allow for management traffic.

Command Default

None

Command Modes

Management plane protection out-of-band configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **interface** command to enter management plane protection inband interface configuration mode or management plane protection out-of-band interface configuration mode.

For the *instance* argument, you cannot configure Management Ethernet interfaces as inband interfaces.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to configure all inband interfaces for MPP:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# control-plane
RP/0/RSP0/CPU0:router(config-ctrl)# management-plane
RP/0/RSP0/CPU0:router(config-mpp)# inband
RP/0/RSP0/CPU0:router(config-mpp-inband)# interface all
RP/0/RSP0/CPU0:router(config-mpp-inband-all)#
```

The following example shows how to configure all out-of-band interfaces for MPP:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# control-plane
RP/0/RSP0/CPU0:router(config-ctrl)# management-plane
RP/0/RSP0/CPU0:router(config-mpp)# out-of-band
RP/0/RSP0/CPU0:router(config-mpp-outband)# interface all
RP/0/RSP0/CPU0:router(config-mpp-outband-all)#
```

Related Commands

Command	Description
allow, on page 290	Configures an interface as an inband or out-of-band interface to allow all peer addresses for a specified protocol or all protocols.
control-plane, on page 294	Configures the control plane.
inband, on page 295	Configures an inband interface or protocol.
management-plane, on page 298	Configures management plane protection to allow and disallow protocols.
out-of-band, on page 299	Configures out-of-band interfaces or protocols and enters management plane protection out-of-band configuration mode.
show mgmt-plane, on page 301	Displays the management plane.

management-plane

To configure management plane protection to allow and disallow protocols, use the **management-plane** command in control plane configuration mode. To disable all configurations under management-plane mode, use the **no** form of this command.

management-plane

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Control plane configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **management-plane** command to enter the management plane protection configuration mode.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to enter management plane protection configuration mode using the **management-plane** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# control-plane
RP/0/RSP0/CPU0:router(config-ctrl)# management-plane
RP/0/RSP0/CPU0:router(config-mpp)#
```

out-of-band

To configure out-of-band interfaces or protocols and to enter management plane protection out-of-band configuration mode, use the **out-of-band** command in management plane protection configuration mode. To disable all configurations under management plane protection out-of-band configuration mode, use the **no** form of this command.

out-of-band

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Management plane protection out-of-band configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **out-of-band** command to enter management plane protection out-of-band configuration mode.

Out-of-band refers to an interface that allows only management protocol traffic to be forwarded or processed. An *out-of-band management interface* is defined by the network operator to specifically receive network management traffic. The advantage is that forwarding (or customer) traffic cannot interfere with the management of the router.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to enter management plane protection out-of-band configuration mode using the **out-of-band** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# control-plane
RP/0/RSP0/CPU0:router(config-ctrl)# management-plane
RP/0/RSP0/CPU0:router(config-mpp)# out-of-band
RP/0/RSP0/CPU0:router(config-mpp-outband)#
```

Related Commands

Command	Description
control-plane, on page 294	Configures the control plane.
inband, on page 295	Configures an inband interface or protocol.
interface (MPP), on page 296	Configures a specific inband or out-of-band interface or all inband or out-of-band interfaces.

Command	Description
management-plane, on page 298	Configures management plane protection to allow and disallow protocols.
show mgmt-plane, on page 301	Displays the management plane.
vrf (MPP), on page 304	Configures a Virtual Private Network (VPN) routing and forwarding (VRF) reference of an out-of-band interface.

show mgmt-plane

To display information about the management plane such as type of interface and protocols enabled on the interface, use the **show mgmt-plane** command in EXEC mode.

show mgmt-plane [{**inband** | **out-of-band**}] [{**interface** *type interface-path-id* | **vrf**}]

Syntax Description

inband	(Optional) Displays the inband management interface configurations that are the interfaces that process management packets as well as data-forwarding packets. An inband management interface is also called a *shared management interface*.
out-of-band	(Optional) Displays the out-of-band interface configurations. Out-of-band interfaces are defined by the network operator to specifically receive network management traffic.
interface	(Optional) Displays all the protocols that are allowed in the specified interface.
type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Interface instance. Number range varies depending on interface type. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
vrf	(Optional) Displays the Virtual Private Network (VPN) routing and forwarding reference of an out-of-band interface.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

The **vrf** keyword is valid only for out-of-band VRF configurations.

Task ID

Task ID	Operations
system	read

Examples

The following sample output displays all the interfaces that are configured as inband or out-of-band interfaces under MPP:

```
RP/0/RSP0/CPU0:router# show mgmt-plane
```

```
Management Plane Protection

inband interfaces
----------------------

interface - GigabitEthernet0_1_1_0
        ssh configured -
                All peers allowed
        telnet configured -
                peer v4 allowed - 10.1.0.0/16
        all configured -
                All peers allowed
interface - GigabitEthernet0_1_1_0
        telnet configured -
                peer v4 allowed - 10.1.0.0/16

interface - all
        all configured -
                All peers allowed

outband interfaces
----------------------
interface - GigabitEthernet0_1_1_0
        tftp configured -
                peer v6 allowed - 33::33
```

The following sample output displays the Virtual Private Network (VPN) routing and forwarding (VRF) reference of an out-of-band interface:

```
RP/0/RSP0/CPU0:router# show mgmt-plane out-of-band vrf

Management Plane Protection -
        out-of-band VRF - my_out_of_band
```

Related Commands

Command	Description
management-plane, on page 298	Configures management plane protection to allow and disallow protocols.

tpa (MPP)

To configure a third-party application protocol for Management Plane Protection (MPP), use the **tpa** command in management plane protection configuration mode. To disable all configurations related to the third-party application, use the **no** form of this command.

tpa vrf default address-family [ipv4 |ipv6]

Syntax Description

vrf	Configures a Virtual Private Network (VPN) routing and forwarding (VRF) reference.
address-family	Enables support for various address family configuration modes while configuring TPA.
ipv4	Specifies IP Version 4 address prefixes.
ipv6	Specifies IP Version 6 address prefixes.

Command Default

Not Applicable

Command Modes

Management plane protection configuration

Command History

Release	Modification
Release 6.3.2	This command was introduced.

Usage Guidelines

Only default vrf is supported for TPA configuration.

Example

```
Router(config)# control-plane
Router(config-ctrl)# management-plane
Router(config-mpp)# tpa vrf default address-family [ipv4 | ipv6]
```

vrf (MPP)

To configure a Virtual Private Network (VPN) routing and forwarding (VRF) reference of an out-of-band interface, use the **vrf** command in management plane protection out-of-band configuration mode. To remove the VRF definition before the VRF name is used, use the **no** form of this command.

vrf *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF.

Command Default

The VRF concept must be used to configure interfaces as out-of-band. If no VRF is configured during an out-of-band configuration, the interface goes into a default VRF.

Command Modes

Management plane protection out-of-band configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

If the VRF reference is not configured, the default name MPP_OUTBAND_VRF is used.

If there is an out-of-band configuration that is referring to a VRF and the VRF is deleted, all the MPP bindings are removed.

Task ID

Task ID	Operations
system	read

Examples

The following example shows how to configure the VRF:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# vrf my_out_of_band
RP/0/RSP0/CPU0:router(config-vrf)# address-family ipv4 unicast
RP/0/RSP0/CPU0:router(config-vrf-af)# exit
RP/0/RSP0/CPU0:router(config-vrf)# address-family ipv6 unicast
RP/0/RSP0/CPU0:router(config-vrf-af)# commit
RP/0/RSP0/CPU0:router(config-vrf-af)# end
RP/0/RSP0/CPU0:router#
```

The following example shows how to configure the VRF definition for MPP:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# control-plane
RP/0/RSP0/CPU0:router(config-ctrl)# management-plane
RP/0/RSP0/CPU0:router(config-mpp)# out-of-band
RP/0/RSP0/CPU0:router(config-mpp-outband)# vrf my_out_of_band
```

Related Commands

Command	Description
control-plane, on page 294	Configures the control plane.
interface (MPP), on page 296	Configures a specific inband or out-of-band interface or all inband or out-of-band interfaces.
management-plane, on page 298	Configures management plane protection to allow and disallow protocols.
out-of-band, on page 299	Configures out-of-band interfaces or protocols and enters management plane protection out-of-band configuration mode.
show mgmt-plane, on page 301	Displays the management plane.

Public Key Infrastructure Commands

This module describes the commands used to configure Public Key Infrastructure (PKI).

For detailed information about PKI concepts, configuration tasks, and examples, see the *Implementing Certification Authority Interoperability on the Cisco ASR 9000 Series Router* module in the *System Security Configuration Guide for Cisco ASR 9000 Series Routers*.

auto-enroll

To specify the duration after which the router request for automatic renewal of a PKI certificate from the CA, , use the **auto-enroll** command in trustpoint configuration mode. To disable the automatic renewal of the certificate after the said period, use the **no** form of this command.

auto-enroll *percentage*

Syntax Description

percentage	Percentage of the certificate validity after which the router will request for a new certificate from the CA. The range is from 1 to 99.

Command Default

None

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 7.5.3	This command was introduced.

Usage Guidelines

This command is applicable only for Cisco IOS XR 64-bit Software.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to configure auto renewal of PKI certificate in the router:

```
Router#configure
Router(config)#crypto ca trustpoint system-trustpoint
Router(config-trustp)#auto-enroll 30
Router(config-trustp)#commit
```

ca-keypair

To create the key pair for the root certificate on the router, use the **ca-keypair** command in trustpoint configuration mode. To remove this configuration, use the **no** form of this command.

ca-keypair { **dsa** | **ecdsanistp256** | **ecdsanistp384** | **ecdsanistp521** | **ed25519** | **rsa** } *key-pair-label*

Syntax Description

key-pair-label	Specifies the key pair label for the respective key signature algorithm (DSA, ECDSA, Ed25519 or RSA).

Command Default

None

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 7.0.1	This command was introduced.
Release 7.3.1	The command was modified to include the **ed25519** option.

Usage Guidelines

This command is applicable only for Cisco IOS XR 64-bit Software.

Task ID

Task ID	Operations
crypto	read, write

Examples

This example shows how to create the RSA key pair for the root certificate on the router:

```
Router#configure
Router(config)#crypto ca trustpoint system-trustpoint
Router(config-trustp)# ca-keypair rsa system-root-key
Router(config-trustp)#commit
```

Related Commands

Command	Description
keypair, on page 359	Creates the key pair for the leaf certificate on the router.

clear crypto ca certificates

To clear certificates associated with trustpoints that no longer exist in the configuration file, use the **clear crypto ca certificates** command in EXEC mode.

clear crypto ca certificates *trustpoint*

Syntax Description

trustpoint	Trustpoint name.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

If the router is loaded with a new configuration file and certificates in the new configuration file do not have their corresponding trustpoint configuration, use the **clear crypto ca certificates** command to clear the certificates associated with trustpoints that no longer exist in the configuration file.

The **clear crypto ca certificates** command deletes both certification authority (CA) and router certificates from the system.

Task ID

Task ID	Operations
crypto	execute

Examples

The following example shows how to clear the certificates associated with trustpoints that no longer exist in the configuration file:

```
RP/0/RSP0/CPU0:router# clear crypto ca certificates tp_1
```

clear crypto ca crl

To clear all the Certificate Revocation Lists (CRLs) stored on the router, use the **clear crypto ca crl** command.

clear crypto ca crl

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **clear crypto ca crl** command to clear all CRLs stored on the router. As a result, the router goes through the certification authorities (CAs) to download new CRLs for incoming certificate validation requests.

Task ID

Task ID	Operations
crypto	execute

Examples

The following example shows how to clear all CRLs stored on the router:

```
RP/0/RSP0/CPU0:router# show crypto ca crls

CRL Entry
==========================================
  Issuer : cn=Certificate Manager,ou=HFR,o=Cisco Systems,l=San Jose,st=CA,c=US
  Last Update : [UTC] Wed Jun  5 02:40:04 2002
  Next Update : [UTC] Wed Jun  5 03:00:04 2002
  CRL Distribution Point :
ldap://manager.cisco.com/CN=Certificate Manager,O=Cisco Systems

RP/0/RSP0/CPU0:router# clear crypto ca crl
RP/0/RSP0/CPU0:router# show crypto ca crls
RP/0/RSP0/CPU0:router#
```

Related Commands

Command	Description
show crypto ca crls, on page 376	Displays the information about CRLs on the router.

crl optional (trustpoint)

To allow the certificates of other peers to be accepted without trying to obtain the appropriate CRL, use the **crl optional** command in trustpoint configuration mode. To return to the default behavior in which CRL checking is mandatory before your router can accept a certificate, use the **no** form of this command.

crl optional

Syntax Description

This command has no keywords or arguments.

Command Default

The router must have and check the appropriate CRL before accepting the certificate of another IP security peer.

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

When your router receives a certificate from a peer, it searches its memory for the appropriate CRL. If the router finds the appropriate CRL, that CRL is used. Otherwise, the router downloads the CRL from either the certificate authority (CA) or from a CRL distribution point (CDP) as designated in the certificate of the peer. Your router will then check the CRL to ensure that the certificate that the peer sent has not been revoked. If the certificate appears on the CRL, your router cannot accept the certificate and will not authenticate the peer. To instruct the router not to download the CRL and treat the certificate as not revoked, use the **crl optional** command.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example declares a CA and permits your router to accept certificates without trying to obtain a CRL. This example also specifies a nonstandard retry period and retry count.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RSP0/CPU0:router(config-trustp)# enrollment url http://ca_server
RP/0/RSP0/CPU0:router(config-trustp)# enrollment retry period 20
RP/0/RSP0/CPU0:router(config-trustp)# enrollment retry count 100
RP/0/RSP0/CPU0:router(config-trustp)# crl optional
```

Related Commands

Command	Description
crypto ca trustpoint, on page 323	Configures a trusted point with a selected name.
enrollment retry count, on page 349	Specifies how many times a router resends a certificate request.

Command	Description
enrollment retry period, on page 351	Specifies the wait period between certificate request retries.
enrollment url, on page 353	Specifies the URL of the CA.

crypto-sks-kme

To display details of the Quantum Key Distribution (QKD) server, use the **crypto-sks-kme** command in EXEC mode.

crypto-sks-kme *profile-name* { **entropy** | **capability** }

Syntax Description

profile-name	Specifies the key string in clear-text form.
entropy	Specifies the key in encrypted form.
capability	Specifies the key in Type 6 encrypted form.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.10.1	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 examples shows how to use the **crypto-sks-kme** command:

```
Router# crypto sks kme remote_qkd_prof1 entropy
Entropy Details:
Key details Dump: 0000 - 406b004c9c7f00000000000000000000280c71794fa6f029d0ee2f6c4cd01b46
Key : 406b004c9c7f00000000000000000000280c71794fa6f029d0ee2f6c4cd01b46
Entropy Length: 32
```

```
Router# crypto sks kme QkdIP capability
Capability Details:
  Entropy supported : False
  Key supported     : False
  Algorithm         : QKD
  Local identifier  : Alice1
  Remote identifier : Alice1, Bob1,
```

crypto ca authenticate

To authenticate the certification authority (CA) by getting the certificate for the CA, use the **crypto ca authenticate** command in EXEC mode.

crypto ca authenticate {*ca-name* | **system-trustpoint**}

Syntax Description

ca-name	Name of the CA Server.
system-trustpoint	Generates self-signed root certificate.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 7.0.1	The command was modified to include the **system-trustpoint** option to specify the default system trustpoint.

Usage Guidelines

The **crypto ca authenticate** command is required when you initially configure CA support at your router.

This command authenticates the CA to your router by obtaining the CA certificate, which contains the public key for the CA. For self-signed root CA, because the CA signs its own certificate, you should manually authenticate the CA public key by contacting the CA administrator when you use this command. The certificate fingerprint matching is done out-of-band (for example, phone call, and so forth).

Authenticating a second-level CA requires prior authentication of the root CA.

After the **crypto ca authenticate** command is issued and the CA does not respond by the specified timeout period, you must obtain terminal control again to re-enter the command.

The **system-trustpoint** option is applicable only for Cisco IOS XR 64-bit Software.

Task ID

Task ID	Operations
crypto	execute

Examples

The CA sends the certificate, and the router prompts the administrator to verify the certificate by checking the certificate fingerprint (a unique identifier). The CA administrator can also display the CA certificate fingerprint, so you should compare what the CA administrator sees to what the router displays on the screen. If the fingerprint on the display matches the fingerprint displayed by the CA administrator, you should accept the certificate as valid.

The following example shows that the router requests the CA certificate:

```
Router# crypto ca authenticate msiox
```

```
Retrieve Certificate from SFTP server? [yes/no]: yes
Read 860 bytes as CA certificate
  Serial Number  : 06:A5:1B:E6:4F:5D:F7:83:41:11:D5:F9:22:7F:95:23
  Subject:
    Name: CA2
    CN= CA2
  Issued By      :
        cn=CA2
  Validity Start : 07:51:51 UTC Wed Jul 06 2005
  Validity End   : 08:00:43 UTC Tue Jul 06 2010
  CRL Distribution Point
        http://10.56.8.236/CertEnroll/CA2.crl
Certificate has the following attributes:
   Fingerprint: D0 44 36 48 CE 08 9D 29 04 C4 2D 69 80 55 53 A3

Do you accept this certificate? [yes/no]: yes


Router#:Apr 10 00:28:52.324 : cepki[335]: %SECURITY-CEPKI-6-INFO : certificate database
updated
Do you accept this certificate? [yes/no] yes
```

This example shows how to generate a self-signed root certificate:

```
Router#crypto ca authenticate system-trustpoint
```

Related Commands

Command	Description
crypto ca trustpoint, on page 323	Configures a trusted point with a selected name.
show crypto ca certificates, on page 373	Displays information about your certificate and the certificate of the CA.

crypto ca cancel-enroll

To cancel a current enrollment request, use the **crypto ca cancel-enroll** command in EXEC mode.

crypto ca cancel-enroll *ca-name*

Syntax Description

ca-name	Name of the certification authority (CA).

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **crypto ca enroll** command to request certificates from the CA for the Rivest, Shamir, and Adelman (RSA) key pairs for the router defined by the rsakeypair, on page 366 command in trustpoint configuration mode. If no rsakeypair, on page 366 command is configured for the current trustpoint, the default RSA key pair is used for enrollment. This task is also known as enrolling with the CA. Use the **crypto ca cancel-enroll** command to cancel a current enrollment request.

Task ID

Task ID	Operations
crypto	execute

Examples

The following example shows how to cancel a current enrollment request from a CA named **myca**:

```
RP/0/RSP0/CPU0:router# crypto ca cancel-enroll myca
```

Related Commands

Command	Description
crypto ca enroll, on page 319	Obtains a router certificate from the CA.
rsakeypair, on page 366	Specifies a named RSA key pair for a trustpoint.

crypto ca enroll

To obtain a router certificate from the certification authority (CA), use the **crypto ca enroll** command in EXEC mode.

crypto ca enroll {*ca-name* | **system-trustpoint**}

Syntax Description

ca-name	Name of the CA Server.
system-trustpoint	Generates the leaf certificate.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 7.0.1	The command was modified to include the **system-trustpoint** option.

Usage Guidelines

Use the **crypto ca enroll** command to request certificates from the CA for the Rivest, Shamir, and Adelman (RSA) key pairs for the router defined by the rsakeypair, on page 366 command in trustpoint configuration mode. If no rsakeypair, on page 366 command is configured for the current trustpoint, the default RSA key pair is used for enrollment. This task is also known as enrolling with the CA. (Enrolling and obtaining certificates are two separate events, but they both occur when the **crypto ca enroll** command is issued.) When using manual enrollment, these two operations occur separately.

The router needs a signed certificate from the CA for each of the RSA key pairs on the router; if you previously generated general-purpose keys, this command obtains the one certificate corresponding to the one general-purpose RSA key pair. If you previously generated special-usage keys, this command obtains two certificates corresponding to each of the special-usage RSA key pairs.

If you already have a certificate for your keys, you are unable to configure this command; instead, you are prompted to remove the existing certificate first. (You can remove existing certificates by removing the trustpoint configuration with the **no crypto ca trustpoint** command.)

The **crypto ca enroll** command is not saved in the router configuration.

The **system-trustpoint** option is applicable only for Cisco IOS XR 64-bit Software.

Note The root certificate signs the leaf certificate.

Task ID

Task ID	Operations
crypto	execute

Examples

The following sample output is from the **crypto ca enroll** command:

```
Router# crypto ca enroll msiox
% Start certificate enrollment...
% Create a challenge password. You will need to verbally provide this password to the
  CA Administrator in order to revoke your certificate.
% For security reasons you password will not be saved in the configuration.
% Please make a note of it.
%Password
re-enter Password:
    Fingerprint: 4F35ADC9 2791997A CE211437 AFC66CF7
RP/0/RSP0/CPU0:May 29 18:49:15.572 : pki_cmd: %PKI-6-LOG_INFO : certificate request pending
RP/0/RSP0/CPU0:May 29 18:52:17.705 : pki_get_cert: %PKI-6-LOG_INFO : certificate is granted
```

This example shows how to generate a leaf certificate:

```
Router#crypto ca enroll system-trustpoint
```

Related Commands

Command	Description
crypto ca trustpoint, on page 323	Configures a trusted point with a selected name.
rsakeypair, on page 366	Specifies a named RSA key pair for a trustpoint.

crypto ca fqdn-check ip-address allow

To avoid server certificate (leaf certificate) failure in the router, resulting from the IP addresses in the Subject Alternate Name (SAN) field of the certificates instead of Fully Qualified Domain Names (FQDNs) when the certificate extension type doesn't specifies the IP address, use the **crypto ca fqdn-check ip-address allow** command in Global Configuration mode.

crypto ca fqdn-check ip-address allow

Syntax Description

This command has no keywords or arguments.

Command Default

When the certificate extension type doesn't specifies the IP address, the certificates with IP addresses in the SAN field don't function properly.

Command Modes

Global Configuration

Command History

Release	Modification
Release 7.4.2	This command was introduced.

Usage Guidelines

In Cisco IOS XR Routers, to use an IP address in the SAN field in server certificates, the certificate extension type is IP addresses. The router rejects certificates that don't meet this criterion. To prevent such failures when an IP address is present in the SAN field, configure the **crypto ca fqdn-check ip-address allow** command. This command enables the router to validate and accept server certificates with IP addresses in the SAN field without the IP addresses certificate extension type.

Task ID

Task ID	Operations
crypto	execute

Examples

This example shows how to run the command for the router to accept server certificates with ip-address in the SAN field:

```
Router# config
Router(config)# crypto ca fqdn-check ip-address allow
```

crypto ca import

To import a certification authority (CA) certificate manually through TFTP, SFTP, or cut and paste it at the terminal, use the **crypto ca import** command in EXEC mode.

crypto ca import *name* **certificate**

Syntax Description

name	Name of the certification authority (CA). This name is the same name used when the CA was declared with the crypto ca trustpoint, on page 323 command.
certificate	

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
crypto	execute

Examples

The following example shows how to import a CA certificate through cut-and-paste. In this example, the certificate is myca.

```
RP/0/RSP0/CPU0:router# crypto ca import myca certificate
```

Related Commands

Command	Description
crypto ca trustpoint, on page 323	Configures a trusted point with a selected name.
show crypto ca certificates, on page 373	Displays information about your certificate and the certification authority (CA) certificate.

crypto ca trustpoint

To configure a trusted point with a selected name, use the **crypto ca trustpoint** command. To unconfigure a trusted point, use the **no** form of this command in Global Configuration mode.

crypto ca trustpoint {*ca-name* | **system-trustpoint**}

Syntax Description

ca-name	Name of the CA.
system-trustpoint	Specifies the default system trustpoint.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 7.0.1	The command was modified to include the **system-trustpoint** option to specify the default system trustpoint.

Usage Guidelines

Use the **crypto ca trustpoint** command to declare a CA.

This command allows you to configure a trusted point with a selected name so that your router can verify certificates issued to peers. Your router need not enroll with the CA that issued the certificates to the peers.

The **crypto ca trustpoint** command enters trustpoint configuration mode, in which you can specify characteristics for the CA with a set of commands. See the Related Commands section for details.

The **system-trustpoint** option is applicable only for Cisco IOS XR 64-bit Software.

Task ID

Task ID	Operations
crypto	execute

Examples

The following example shows how to use the **crypto ca trustpoint** command to create a trustpoint:

```
Router# configure
Router(config)# crypto ca trustpoint msiox
Router(config-trustp)# sftp-password xxxxxx
Router(config-trustp)# sftp-username tmordeko
Router(config-trustp)# enrollment url sftp://192.168..254.254/tftpboot/tmordeko/CAcert
Router(config-trustp)# rsakeypair label-2
```

This example shows how to create a default system trustpoint:

```
Router#configure
```

```
Router(config)#crypto ca trustpoint system-trustpoint
Router(config-trustp)#commit
```

Related Commands

Command	Description
ca-keypair, on page 310	Creates the key pair for the root certificate on the router.
crl optional (trustpoint), on page 313	Allows the certificates of other peers to be accepted without trying to obtain the appropriate CRL.
enrollment retry count, on page 349	Specifies how many times a router resends a certificate request.
enrollment retry period, on page 351	Specifies the wait period between certificate request retries.
enrollment terminal, on page 352	Specifies manual cut-and-paste certificate enrollment.
enrollment url, on page 353	Specifies the URL of the CA.
ip-address (trustpoint), on page 355	Specifies a dotted IP address that is included as an unstructured address in the certificate request.
key-usage, on page 357	Specifies the key usage field for the self-enrollment certificate.
keypair, on page 359	Creates the key pair for the leaf certificate on the router.
lifetime (trustpoint), on page 362	Configures the lifetime for self-enrollment of certificates.
message-digest, on page 363	Configures the message digest hashing algorithm for the certificates.
query url, on page 364	Specifies the LDAP URL of the CRL distribution point.
rsakeypair, on page 366	Specifies a named RSA key pair for this trustpoint.
serial-number (trustpoint), on page 367	Specifies a router serial number in the certificate request.
sftp-password (trustpoint), on page 369	Secures the FTP password.
sftp-username (trustpoint), on page 370	Secures the FTP username.
subject-name (trustpoint), on page 371	Specifies a subject name in the certificate request.

crypto ca trustpool import url

To manually update certificates in the trust pool if they are not current, are corrupt, or if certain certificates need to be updated, use the **crypto ca trustpool import url** command in EXEC mode.

crypto ca trustpool import url { **clean** *URL* }

Syntax Description

clean	(Optional) Manually remove all downloaded certificate authority (CA) certificates.
URL	Specify the URL from which the CA trust pool certificate bundle must be downloaded. This manually imports (downloads) the CA certificate bundle into the CA trust pool to update or replace the existing CA certificate bundle. This parameter can either be the URL of an external server or the local folder path (**/tmp**) in the router where the certificate is available.

Command Default

The CA trust pool feature is enabled. The router uses the built-in CA certificate bundle in the CA trust pool which is updated automatically from Cisco.

Command Modes

EXEC mode

Command History

Release	Modification
Release 5.2.0	This command was introduced.
Release 7.1.2 Release 6.7.2 (for 32-bit IOS XR platforms)	This command was modified to also allow a local folder path (**/tmp**) in the router as the *URL* parameter.

Usage Guidelines

The CA trust pool feature is enabled by default and uses the built-in CA certificate bundle in the trust pool, which receives automatic updates from Cisco. Use the **crypto ca trustpool import url** command to manually update certificates in the trust pool if they are not current, are corrupt, or if certain certificates need to be updated.

From Cisco IOS XR Software Release 7.1.2 (Release 6.7.2, for 32-bit IOS XR platforms) and later, you can also specify a local folder path (**/tmp**) in the router as the *URL* parameter for **crypto ca trustpool import url** command. This is useful in scenarios where the router does not have connectivity to an external server to download the certificate. In such cases, you can download the certificate from an external server to elsewhere, and then copy it to the **/tmp** folder in the router.

Note The local folder path in the router has to be **/tmp** itself; no other folder paths are allowed.

The format of the certificate can .pem, .der, or .p7b(bundle).

For example,

crypto ca trustpool import url /tmp/certificate.pem

crypto ca trustpool import url /tmp/certificate.der

crypto ca trustpool import url /tmp/pki_bundle_tmp.p7b

Task ID

Task ID	Operation
crypto	execute

This example shows how to run the command to manually update certificates in the trust pool if they are not current, are corrupt, or if certain certificates need to be updated. The certificate is directly downloaded from an external server, in this case.

```
Router#crypto ca trustpool import url http://www.cisco.com/security/pki/trs/ios.p7b
```

This example shows how to import a certificate that resides in the local **/tmp** folder in the router:

```
Router#crypto ca trustpool import url /tmp/certificate.der
```

Related Commands

Command	Description
show crypto ca trustpool policy, on page 377	Display the CA trust pool certificates of the router in a verbose format.
crypto ca trustpool policy, on page 327	Configure CA trust pool policy parameters.

crypto ca trustpool policy

To configure certificate authority (CA) trust pool policy, use the **crypto ca trustpool policy** command in Global Configuration mode.

crypto ca trustpool policy {**cabundle url** *url* | **crl optional** | **description** *line*}

Syntax Description

cabundle url *URL*	Configures the URL from which the CA trust pool bundle is downloaded.
crl optional	To specify the certificate revocation list (CRL) query for the CA trust pool, use the crl command in ca-trustpool configuration mode. By default, the router enforces a check of the revocation status of the certificate by querying the certificate revocation list (CRL). Setting this to optional disables revocation checking when the trust pool policy is in use.
description *line*	Indicates the description for the trust pool policy.

Command Default

The default CA trust pool policy is used.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 5.2.0	This command was introduced.

Usage Guidelines

The **crypto ca trustpool policy** command enters ca-trustpool configuration mode, where commands can be accessed to configure certificate authority (CA) trustpool policy parameters.

Task ID

Task ID	Operation
crypto	READ, WRITE

Example

This example shows you how to disable certificate revocation checks when the trust pool policy is in use.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:IMC0(config)#crypto ca trustpool policy
RP/0/RSP0/CPU0:IMC0(config-trustpool)#RP/0/RSP0/CPU0:IMC0(config-trustpool)#crl optional
```

Related Commands

Command	Description
crypto ca trustpool import url, on page 325	Allows you to manually update certificates in the trust pool.

Command	Description
show crypto ca trustpool policy, on page 377	Displays the CA trust pool certificates of the router in a verbose format.

crypto key generate authentication-ssh

To generate the cryptographic key pair for public key-based authentication of logged-in users on Cisco IOS XR routers that are configured as SSH clients, use the **crypto key generate authentication-ssh** command in EXEC mode.

crypto key generate authentication-ssh rsa

Syntax Description

rsa	Generates RSA key pairs for signing and encryption of packets for SSH public key-based authentication.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

Remote AAA servers such as RADIUS and TACACS+ servers do not support public key-based authentication. Hence this functionality is available only for users who are configured locally on the router and not for users who are configured remotely.

To delete the RSA key of a user, use the **crypto key zeroize authentication-ssh rsa username** command in EXEC mode.

A user with root privileges has permission to create and delete keys for other users.

Task ID

Task ID	Operations
crypto	execute

Examples

This example shows how to generate an RSA key pair for public key-based authentication of SSH clients on Cisco IOS XR routers:

```
Router#crypto key generate authentication-ssh rsa
Wed Dec 21 10:02:57.684 UTC
The name for the keys will be: cisco
  Choose the size of the key modulus in the range of 512 to 4096. Choosing a key modulus
greater than 512 may take a few minutes.

How many bits in the modulus [2048]:
Generating RSA keys ...
Done w/ crypto generate keypair
[OK]

Router#
```

crypto key generate dsa

To generate Digital Signature Algorithm (DSA) key pairs, use the **crypto key generate dsa** command in EXEC mode.

crypto key generate dsa [{**system-enroll-key** | **system-root-key**}]

Syntax Description

system-enroll-key	Specifies key pair generation for the leaf certificate.
system-root-key	Specifies key pair generation for the root certificate.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 7.0.1	The command was modified to include **system-enroll-key** and **system-root-key** options for the key pair generation of leaf and root certificates. This update is applicable only for Cisco IOS XR 64-bit Software.

Usage Guidelines

Use the **crypto key generate dsa** command to generate DSA key pairs for your router.

DSA keys are generated in pairs—one public DSA key and one private DSA key.

If your router already has DSA keys when you issue this command, you are warned and prompted to replace the existing keys with new keys.

To remove the DSA key generated, use the **crypto key zeroize dsa** command.

The options **system-enroll-key** and **system-root-key** are applicable only for Cisco IOS XR 64-bit Software.

Task ID

Task ID	Operations
crypto	execute

Examples

The following example shows how to generate a 512-bit DSA key:

```
RP/0/RSP0/CPU0:router# crypto key generate dsa
The name for the keys will be: the_default
    Choose the size of your DSA key modulus. Modulus size can be 512, 768, or 1024 bits.
Choosing a key modulus
How many bits in the modulus [1024]: 512
Generating DSA keys...
Done w/ crypto generate keypair
[OK]
```

This example shows how to generate a DSA key pair for the root certificate:

```
Router#crypto key generate dsa system-root-key
```

This example shows how to generate a DSA key pair for the leaf certificate:

```
Router#crypto key generate dsa system-enroll-key
```

Related Commands

Command	Description
crypto key zeroize dsa, on page 343	Deletes a DSA key pair from your router.
show crypto key mypubkey dsa, on page 380	Displays the DSA public keys for your router.

crypto key generate ecdsa

To generate an Elliptic Curve Digital Signature Algorithm (ECDSA) key pair, use the **crypto key generate ecdsa** command in EXEC mode.

crypto key generate ecdsa [{**nistp256** | **nistp384** | **nistp521**}] [{**system-enroll-key** | **system-root-key**}]

Syntax Description

nistp256	Generates an ECDSA key of curve type nistp256, with key size 256 bits.
nistp384	Generates an ECDSA key of curve type nistp384, with key size 384 bits.
nistp521	Generates an ECDSA key of curve type nistp521, with key size 521 bits.
system-enroll-key	Specifies key pair generation for the leaf certificate.
system-root-key	Specifies key pair generation for the root certificate.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.4.1	This command was introduced.
Release 7.0.1	The command was modified to include **system-enroll-key** and **system-root-key** options for the key pair generation of leaf and root certificates.

Usage Guidelines

The options **system-enroll-key** and **system-root-key** are applicable only for Cisco IOS XR 64-bit Software.

To remove an ECDSA key, use the **crypto key zeroize ecdsa** command.

Task ID

Task ID	Operation
crypto	execute

The following example shows how to generate a ECDSA key pair:

```
Router# crypto key generate ecdsa nistp384
Wed Mar 28 12:53:57.355 UTC
% You already have keys defined for the_default
Do you really want to replace them? [yes/no]: yes
Generating ECDSA keys ...
Done w/ crypto generate ECDSA keypair
[OK]
```

This example shows how to generate a ECDSA key pair for the root certificate:

```
Router#crypto key generate ecdsa system-root-key
```

This example shows how to generate a ECDSA key pair for the leaf certificate:

```
Router#crypto key generate dsa system-enroll-key
```

crypto key generate ed25519

To generate Ed25519 crypto key pairs as part of supporting the Ed25519 public key signature system, use the **crypto key generate ed25519** command in EXEC mode.

crypto key generate ed25519 [{ **system-enroll-key** | **system-root-key** }]

Syntax Description

system-enroll-key	Specifies key pair generation for the leaf certificate.
system-root-key	Specifies key pair generation for the root certificate.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.3.1	This command was introduced.

Usage Guidelines

This command is applicable only for Cisco IOS XR 64-bit platforms.

To remove the Ed25519 keys, use the **crypto key zeroize ed25519** command.

You can generate the crypto keys either with an empty label or with two predefined labels (**system-root-key** and **system-enroll-key**). In case of empty label, the system generates the key pair against the default label. The key pairs with the predefined labels are used to integrate Cisco IOS XR with Cisco Crosswork Trust Insights.

Task ID

Task ID	Operations
crypto	execute

Examples

This example shows how to generate a Ed25519 crypto key pair:

```
Router# crypto key generate ed25519

Mon Nov 30 07:03:17.058 UTC
The name for the keys will be: the_default
Generating ED25519 keys ...
Done w/ crypto generate keypair
[OK]
```

This example shows how to generate a Ed25519 crypto key pair for the root certificate:

```
Router#crypto key generate ed25519 system-root-key
```

This example shows how to generate a Ed25519 crypto key pair for the leaf certificate:

```
Router#crypto key generate ed25519 system-enroll-key
```

Related Commands

Command	Description
crypto key zeroize ed25519, on page 345	Deletes Ed25519 crypto key pairs from the router.
show crypto key mypubkey ed25519, on page 382	Displays the Ed25519 public keys of the router.

crypto key generate rsa

To generate a Rivest, Shamir, and Adelman (RSA) key pair, use the **crypto key generate rsa** command in EXEC mode.

crypto key generate rsa [{**usage-keys** | **general-keys** | **system-enroll-key** | **system-root-key**}] [*keypair-label*]

Syntax Description

usage-keys	(Optional) Generates separate RSA key pairs for signing and encryption.
general-keys	(Optional) Generates a general-purpose RSA key pair for signing and encryption.
keypair-label	(Optional) RSA key pair label that names the RSA key pairs.
system-enroll-key	Specifies key pair generation for the leaf certificate.
system-root-key	Specifies key pair generation for the root certificate.

Command Default

RSA key pairs do not exist. If the **usage-keys** keyword is not used, general-purpose keys are generated. If no RSA label is specified, the key is generated as the default RSA key.

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 7.0.1	The command was modified to include **system-enroll-key** and **system-root-key** options for the key pair generation of leaf and root certificates.

Usage Guidelines

Use the **crypto key generate rsa** command to generate RSA key pairs for your router.

RSA keys are generated in pairs—one public RSA key and one private RSA key.

If your router already has RSA keys when you issue this command, you are warned and prompted to replace the existing keys with new keys. The keys generated by this command are saved in the secure NVRAM (which is not displayed to the user or backed up to another device).

To remove an RSA key, use the **crypto key zeroize rsa** command.

The options **system-enroll-key** and **system-root-key** are applicable only for Cisco IOS XR 64-bit Software.

Task ID

Task ID	Operations
crypto	execute

Examples

The following example shows how to generate an RSA key pair:

```
Router# crypto key generate rsa
```

```
The name for the keys will be: the_default

Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus[1024]: <return>
Router(config)#
```

This example shows how to generate an RSA key pair for the root certificate:

```
Router#crypto key generate rsa system-root-key
```

This example shows how to generate an RSA key pair for the leaf certificate:

```
Router#crypto key generate rsa system-enroll-key
```

Related Commands

Command	Description
crypto key zeroize rsa, on page 346	Deletes the RSA key pair for your router.
show crypto key mypubkey rsa, on page 383	Displays the RSA public keys for your router.

crypto key import authentication rsa

To import a public key using the Rivest, Shamir, and Adelman (RSA) method, use the **crypto key import authentication rsa** command in EXEC mode.

crypto key import authentication rsa [**username** *name*] [**WORD** | **second** | **third** | **fourth**]

Syntax Description

rsa	Imports the RSA public key on the router.
username	(Optional) Imports the RSA public key for the user *name*.
name	Specifies the name of the user for which the RSA public key is imported. If you do not specify a *name*, the RSA public key for the currently logged-in user is imported.
WORD	(Optional) Specifies the path (`harddisk:/` or `disk0:/` or `tftp`) to the RSA public key file.
second	(Optional) Imports the second RSA public key for a user.
third	(Optional) Imports the third RSA public key for a user.
fourth	(Optional) Imports the fourth RSA public key for a user.

Command Default

- The **crypto key import authentication rsa** command imports the first RSA public key for the currently logged-in user if you do not specify the **WORD**, **second**, **third**, or **fourth** option.
- The **crypto key import authentication rsa username** *name* command imports the first RSA public key for the user *name* if you do not specify the **second**,**third**, or **fourth** option.

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.11.1	This command was modified to include the **second**,**third**,and **fourth** options.
Release 3.9.0	This command was introduced.

Usage Guidelines

1. Use shh-keygen generation mechanism to generate keys using either a LINUX or UNIX client. This creates two keys: one public and one private.
2. Remove the comment and other header tag from the keys, except the base64encoded text.
3. Decode the base64encoded text, and use the for authentication.

Task ID

Task ID	Operations
crypto	execute

Examples

This example shows how to import the second RSA public key for the currently logged-in user.

```
RP/0/RP0/CPU0:OC_router1#crypto key import authentication rsa harddisk:/id_rsa_key2.pub
Thu Nov  9 20:43:19.568 IST
RP/0/RP0/CPU0:Nov  9 20:43:19.740 IST: cepki[129]: %SECURITY-CEPKI-6-KEY_INFO : crypto key
 RSA(public key authentication) generated, label:cafyauto, modBits:4096
RP/0/RP0/CPU0:OC_router1#RP/0/RP0/CPU0:Nov  9 20:43:20.964 IST: cepki[129]:
%SECURITY-CEPKI-6-INFO : key database updated successfully
RP/0/RP0/CPU0:OC_router1#
```

This example shows how to import the third RSA public key for the currently logged-in user by manually copy-pasting the key.

```
RP/0/RP0/CPU0:OC_router1#crypto key import authentication rsa third
Thu Nov  9 20:51:52.599 IST
Enter the public key
ssh-rsa
[redacted]

RP/0/RP0/CPU0:Nov  9 20:52:38.122 IST: cepki[129]: %SECURITY-CEPKI-6-KEY_INFO : crypto key
 RSA(public key authentication) generated, label:cafyauto, modBits:4096
RP/0/RP0/CPU0:OC_router1#
```

This example shows how to import the fourth RSA public key for user *test*.

```
RP/0/RP0/CPU0:OC_router1#crypto key import authentication rsa username test fourth
harddisk:/id_rsa_key4.pub
Thu Nov  9 20:55:02.586 IST
RP/0/RP0/CPU0:Nov  9 20:55:02.757 IST: cepki[129]: %SECURITY-CEPKI-6-KEY_INFO : crypto key
 RSA(public key authentication) generated, label:test, modBits:4096
RP/0/RP0/CPU0:OC_router1
```

crypto key zeroize authentication-ssh

To delete the cryptographic key pair on the router that was generated for public key-based authentication of SSH clients, use the **crypto key zeroize authentication-ssh** command in EXEC mode.

crypto key zeroize authentication-ssh rsa [**username** *name*]

Syntax Description

rsa	Deletes the RSA key pair on the router.
username *name*	Specifies the name of the user whose RSA key pairs are to be deleted from the router.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

If the **username** is not specified, then the command deletes the key for the user who is currently logged in.

A user with root privileges has permission to create and delete keys for other users.

Task ID

Task ID	Operations
crypto	execute

Examples

This example shows how to delete the RSA key pair that was generated for public key-based authentication of SSH clients.

```
Router#crypto key zeroize authentication-ssh rsa username user1
```

crypto key zeroize authentication rsa

To delete a public key imported on the router using the Rivest, Shamir, and Adelman (RSA) method, use the **crypto key zeroize authentication rsa** command in EXEC mode.

crypto key zeroize authentication rsa [**username** *name*] [**all** | **second** | **third** | **fourth**]

Syntax Description

rsa	Deletes the RSA public key on the router.
username	Deletes the RSA public key for the user specified in the *name*.
name	(Optional) Specifies the name of the user for which the RSA public key is deleted. If you do not specify a *name*, the RSA public key for the currently logged-in user is deleted.
all	Deletes all imported RSA public keys.
second	Deletes second imported RSA public key.
third	Deletes third imported RSA public key.
fourth	Deletes fourth imported RSA public key.

Command Default

- The **crypto key zeroize authentication rsa** command deletes the first imported RSA public key if you do not specify the **all**, **second**, **third**, or **fourth** option.
- The **crypto key zeroize authentication rsa username** *name* command deletes the first imported RSA public key for the user *name* if you do not specify the **second**,**third**, or **fourth** option.

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.11.1	This command was modified to include the **second**,**third**, and **fourth** options.
Release 7.2.1	This command was introduced.

Usage Guidelines

If the **username** is not specified, then the command deletes the first imported RSA public key for the currently logged-in user.

A user with root privileges can create and delete keys for other users.

Task ID

Task ID	Operations
crypto	execute

Examples

This example shows how to delete the first imported RSA public key for the currently logged-in user *test1*.

```
RP/0/RP0/CPU0:OC_router1#crypto key zeroize authentication rsa

Wed Oct 25 18:32:30.421 IST
% Keys to be removed are named test1
Do you really want to remove these keys ?? [yes/no]: yes

RP/0/RP0/CPU0:OC_router1#
```

This example shows how to delete the fourth imported RSA public key for the currently logged-in user *test1*.

```
RP/0/RP0/CPU0:OC_router1#crypto key zeroize authentication rsa fourth

Wed Oct 25 21:18:04.336 IST
% Keys to be removed are named test1
Do you really want to remove these keys ?? [yes/no]: yes

RP/0/RP0/CPU0:OC_router1#
```

This example shows how to delete the first imported RSA public key for user *test2*.

```
RP/0/RP0/CPU0:OC_router1#crypto key zeroize authentication rsa username test2

Wed Oct 25 18:54:34.153 IST
% Keys to be removed are named test2
Do you really want to remove these keys ?? [yes/no]: yes

RP/0/RP0/CPU0:OC_router1#
```

This example shows how to delete the second imported RSA public key for user *test3*.

```
RP/0/RP0/CPU0:OC_router1#crypto key zeroize authentication rsa username test3 second

Wed Oct 25 18:54:34.153 IST
% Keys to be removed are named test3
Do you really want to remove these keys ?? [yes/no]: yes

RP/0/RP0/CPU0:OC_router1#
```

This example shows how to delete all imported RSA public keys on the router in EXEC mode.

```
RP/0/RP0/CPU0:OC_router1#crypto key zeroize authentication rsa all

Wed Oct 25 18:32:58.007 IST
Do you really want to remove all these keys ?? [yes/no]: yes

RP/0/RP0/CPU0:OC_router1#
```

crypto key zeroize dsa

To delete the Digital Signature Algorithm (DSA) key pair from your router, use the **crypto key zeroize dsa** command in EXEC mode.

crypto key zeroize dsa

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **crypto key zeroize dsa** command to delete the DSA key pair that was previously generated by your router.

Task ID

Task ID	Operations
crypto	execute

Examples

The following example shows how to delete DSA keys from your router:

```
RP/0/RSP0/CPU0:router# crypto key zeroize dsa
% Keys to be removed are named the_default
Do you really want to remove these keys? [yes/no]: yes
```

Related Commands

Command	Description
crypto key generate dsa, on page 330	Generates DSA key pairs.
show crypto key mypubkey dsa, on page 380	Displays the DSA public keys for your router.

crypto key zeroize ecdsa

To delete the Elliptic Curve Digital Signature Algorithm (ECDSA) key pair from your router, use the **crypto key zeroize ecdsa** command in EXEC mode.

crypto key zeroize ecdsa [**nistp256** | **nistp384** | **nistp521**]

Syntax Description

nistp256	Deletes an ECDSA key of curve type nistp256, with key size 256 bits.
nistp384	Deletes an ECDSA key of curve type nistp384, with key size 384 bits.
nistp521	Deletes an ECDSA key of curve type nistp521, with key size 521 bits.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.4.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
crypto	execute

Example

The following example shows how to delete ECDSA keys from your router:

```
RP/0/RP0/CPU0:router# crypto key zeroize ecdsa nistp384

% Keys to be removed are named the_default
Do you really want to remove these keys ?? [yes/no]: yes
```

crypto key zeroize ed25519

To delete the Ed25519 crypto key pair from the router, use the **crypto key zeroize ed25519** command in EXEC mode.

crypto key zeroize ed25519

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.3.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
crypto	execute

Examples

This example shows how to delete Ed25519 crypto key pairs from your router:

```
Router# crypto key zeroize ed25519
% Keys to be removed are named the_default
Do you really want to remove these keys? [yes/no]: yes
```

Related Commands

Command	Description
crypto key generate ed25519, on page 334	Generates Ed25519 crypto key pairs.
show crypto key mypubkey ed25519, on page 382	Displays the Ed25519 public keys of your router.

crypto key zeroize rsa

To delete all Rivest, Shamir, and Adelman (RSA) keys from the router, use the **crypto key zeroize rsa** command in EXEC mode.

crypto key zeroize rsa [*keypair-label*]

Syntax Description

keypair-label	(Optional) Names the RSA key pair to be removed.

Command Default

If the key pair label is not specified, the default RSA key pair is removed.

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **crypto key zeroize rsa** command to delete all RSA keys that were previously generated by the router. After issuing this command, you must perform two additional tasks:

- Ask the certification authority (CA) administrator to revoke the certificates for the router at the CA; you must supply the challenge password you created when you originally obtained the router certificates with the crypto ca enroll, on page 319 command CA.
- Manually remove the certificates from the configuration using the **clear crypto ca certificates** command.

Task ID

Task ID	Operations
crypto	execute

Examples

The following example shows how to delete the general-purpose RSA key pair that was previously generated:

```
RP/0/RSP0/CPU0:router# crypto key zeroize rsa key1
% Keys to be removed are named key1
Do you really want to remove these keys? [yes/no]: yes
```

Related Commands

Command	Description
clear crypto ca certificates, on page 311	Clears certificates associated with trustpoints that no longer exist in the configuration file.
crypto ca enroll, on page 319	Obtains a router certificate from the CA.
crypto key generate rsa, on page 336	Generates RSA key pairs.

Command	Description
show crypto key mypubkey rsa, on page 383	Displays the RSA public keys for your router.

description (trustpoint)

To create a description of a trustpoint, use the **description** command in trustpoint configuration mode. To delete a trustpoint description, use the **no** form of this command.

description *string*

Syntax Description

string	Character string describing the trustpoint.

Command Default

The default description is blank.

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **description** command in the trustpoint configuration mode to create a description for a trustpoint.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to create a trustpoint description:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RSP0/CPU0:router(config-trustp)# description this is the primary trustpoint
```

enrollment retry count

To specify the number of times a router resends a certificate request to a certification authority (CA), use the **enrollment retry count** command in trustpoint configuration mode. To reset the retry count to the default, use the **no** form of this command.

enrollment retry count *number*

Syntax Description

number	Number of times the router resends a certificate request when the router does not receive a certificate from the previous request. The range is from 1 to 100.

Command Default

If no retry count is specified, the default value is 10.

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

After requesting a certificate, the router waits to receive a certificate from the CA. If the router does not receive a certificate within a specified time (the retry period), the router sends another certificate request. The router continues to send requests until it receives a valid certificate, the CA returns an enrollment error, or the configured number of retries (the retry count) is exceeded.

To reset the retry count to the default of 10, use the **no** form of this command. Setting the retry count to 0 indicates an infinite number of retries. The router sends the CA certificate requests until a valid certificate is received (there is no limit to the number of retries).

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to declare a CA, change the retry period to 10 minutes, and change the retry count to 60 retries. The router resends the certificate request every 10 minutes until receipt of the certificate or approximately 10 hours pass since the original request was sent, whichever occurs first (10 minutes x 60 tries = 600 minutes = 10 hours).

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RSP0/CPU0:router(config-trustp)# enrollment url http://ca_server
RP/0/RSP0/CPU0:router(config-trustp)# enrollment retry period 10
RP/0/RSP0/CPU0:router(config-trustp)# enrollment retry count 60
```

Related Commands

Command	Description
crl optional (trustpoint), on page 313	Allows the certificates of other peers to be accepted without trying to obtain the appropriate CRL.
crypto ca trustpoint, on page 323	Configures a trusted point with a selected name.
enrollment retry period, on page 351	Specifies the wait period between certificate request retries.
enrollment url, on page 353	Specifies the certification authority (CA) location by naming the CA URL.

enrollment retry period

To specify the wait period between certificate request retries, use the **enrollment retry period** command in trustpoint configuration mode. To reset the retry period to the default of 1 minute, use the **no** form of this command.

enrollment retry period *minutes*

Syntax Description

minutes	Period (in minutes) between certificate requests issued to a certification authority (CA) from the router. The range is from 1 to 60 minutes.

Command Default

minutes: *1*

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

After requesting a certificate, the router waits to receive a certificate from the CA. If the router does not receive a certificate within a specified time (the retry period), the router sends another certificate request. The router continues to send requests until it receives a valid certificate, the CA returns an enrollment error, or the configured number of retries (the retry count) is exceeded.

The router sends the CA another certificate request every minute until a valid certificate is received. (By default, the router sends ten requests, but you can change the number of permitted retries with the **enrollment retry count** command.)

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to declare a CA and change the retry period to 5 minutes:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RSP0/CPU0:router(config-trustp)# enrollment retry period 5
```

Related Commands

Command	Description
crl optional (trustpoint), on page 313	Allows the certificates of other peers to be accepted without trying to obtain the appropriate CRL.
crypto ca trustpoint, on page 323	Configures a trusted point with a selected name.
enrollment retry count, on page 349	Specifies the number of times a router resends a certificate request.

enrollment terminal

To specify manual cut-and-paste certificate enrollment, use the **enrollment terminal** command in trustpoint configuration mode. To delete a current enrollment request, use the **no** form of this command.

enrollment terminal

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

You can manually cut and paste certificate requests and certificates when you do not have a network connection between the router and certification authority (CA). When the **enrollment terminal** command is enabled, the router displays the certificate request on the console terminal, which allows you to enter the issued certificate on the terminal.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to manually specify certificate enrollment through cut-and-paste. In this example, the CA trustpoint is myca.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RSP0/CPU0:router(config-trustp)# enrollment terminal
```

Related Commands

Command	Description
crypto ca trustpoint, on page 323	Configures a trusted point with a selected name.

enrollment url

To specify the certification authority (CA) location by naming the CA URL, use the **enrollment url** command in trustpoint configuration mode. To remove the CA URL from the configuration, use the **no** form of this command.

enrollment url *CA-URL*

Syntax Description

CA-URL	URL of the CA server. The URL string must start with http://CA_name, where CA_name is the host Domain Name System (DNS) name or IP address of the CA (for example, http://ca-server). If the CA cgi-bin script location is not /cgi-bin/pkiclient.exe at the CA (the default CA cgi-bin script location), you must also include the nonstandard script location in the URL, in the form of http://CA-name/script-location, where script-location is the full path to the CA scripts.

Command Default

None

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **enrollment url** command to specify the CA URL. This command is required when you declare a CA with the **crypto ca trustpoint** command. The URL must include the CA script location if the CA scripts are not loaded into the default cgi-bin script location. The CA administrator should be able to tell you where the CA scripts are located.

This table lists the available enrollment methods.

Table 13: Certificate Enrollment Methods

Enrollment Method	Description
SFTP	Enroll through SFTP: file system
TFTP[1]	Enroll through TFTP: file system

[1] If you are using TFTP for enrollment, the URL must be in the form tftp://certserver/file_specification. (The file specification is optional.)

TFTP enrollment sends the enrollment request and retrieves the certificate of the CA and the certificate of the router. If the file specification is included in the URL, the router appends an extension to the file specification.

To change the CA URL, repeat the **enrollment url** command to overwrite the previous URL

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows the absolute minimum configuration required to declare a CA:

```
 RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)#
               crypto ca trustpoint myca
 RP/0/RSP0/CPU0:router(config-trustp)#
               enrollment url http://ca.domain.com/certsrv/mscep/mscep.dll
```

Related Commands

Command	Description
crl optional (trustpoint), on page 313	Allows the certificates of other peers to be accepted without trying to obtain the appropriate CRL.
crypto ca trustpoint, on page 323	Configures a trusted point with a selected name.
ip-address (trustpoint), on page 355	Specifies a dotted IP address that is included as an unstructured address in the certificate request.

ip-address (trustpoint)

To specify a dotted IP address that is included as an unstructured address in the certificate request, use the **ip-address** command in trustpoint configuration mode. To restore the default behavior, use the **no** form of this command.

ip-address {*ip-address* | **none**}

Syntax Description

ip-address	Dotted IP address that is included in the certificate request.
none	Specifies that an IP address is not included in the certificate request.

Command Default

You are prompted for the IP address during certificate enrollment.

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **ip-address** command to include the IP address of the specified interface in the certificate request or to specify that an IP address should not be included in the certificate request.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to include the IP address of the Ethernet-0 interface in the certificate request for the trustpoint frog:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint frog
RP/0/RSP0/CPU0:router(config-trustp)# enrollment url http://frog.phoobin.com
RP/0/RSP0/CPU0:router(config-trustp)# subject-name OU=Spiral Dept., O=tiedye.com
RP/0/RSP0/CPU0:router(config-trustp)# ip-address 172.19.72.120
```

The following example shows that an IP address is not to be included in the certificate request:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RSP0/CPU0:router(config-trustp)# enrollment url http://10.3.0.7:80
RP/0/RSP0/CPU0:router(config-trustp)# subject-name CN=subject1, OU=PKI, O=Cisco Systems,
C=US
RP/0/RSP0/CPU0:router(config-trustp)# ip-address none
```

Related Commands

Command	Description
crl optional (trustpoint), on page 313	Allows the certificates of other peers to be accepted without trying to obtain the appropriate CRL.
crypto ca trustpoint, on page 323	Configures a trusted point with a selected name.
enrollment url, on page 353	Specifies the certification authority (CA) location by naming the CA URL.
serial-number (trustpoint), on page 367	Specifies whether the router serial number should be included in the certificate request.
subject-name (trustpoint), on page 371	Specifies the subject name in the certificate request.

key-usage

To specify the key usage field for the self-enrollment certificate, use the **key-usage** command in trustpoint configuration mode. To remove this configuration, use the **no** form of this command.

key-usage {**ca-certificate** {**crlsign** | **digitalsignature** | **keycertsign** | **nonrepudiation**} | **certificate** {**dataencipherment** | **digitalsignature** | **keyagreement** | **keyencipherment** | **nonrepudiation**}}

Syntax Description

ca-certificate	Specifies the key usage field for the CA certificate.
certificate	Specifies the key usage field for the leaf certificate.
crlsign	Asserts **cRLSign** (bit 6) for the key usage field to verify signatures on certificate revocation list (CRL).
digitalsignature	Asserts **digitalSignature** (bit 0) for the key usage field. This is used when the subject public key is used with a digital signature mechanism to support security services other than certificate signing (bit 5), or CRL signing (bit 6).
keycertsign	Asserts **keyCertSign** (bit 5) for the key usage field when the subject public key is used for verifying a signature on public key certificates.
nonrepudiation	Asserts **nonRepudiation** (bit 1) for the key usage field when the subject public key is used to verify digital signatures that is used to provide a non-repudiation service.
dataencipherment	Asserts **dataEncipherment** (bit 3) for the key usage field when the subject public key is used for enciphering user data, other than cryptographic keys.
keyagreement	Asserts **keyAgreement** (bit 4) for the key usage field when the subject public key is used for key agreement.
keyencipherment	Asserts **keyEncipherment** (bit 2) for the key usage field when the subject public key is used for key transport.

Command Default

None

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

This command is applicable only for Cisco IOS XR 64-bit Software.

Task ID

Task ID	Operations
crypto	read, write

Examples

This example shows how to specify the key usage field for the self-enrollment certificate:

```
Router#configure
Router(config)#crypto ca trustpoint system-trustpoint
Router(config-trustp)#key-usage certificate digitalsignature keyagreement dataencipherment
Router(config-trustp)#commit
```

keypair

To create the key pair for the leaf certificate on the router, use the **keypair** command in trustpoint configuration mode. To remove this configuration, use the **no** form of this command.

keypair { **dsa** | **ecdsanistp256** | **ecdsanistp384** | **ecdsanistp521** | **ed25519** | **rsa** } *key-pair-label*

Syntax Description

key-pair-label	Specifies the key pair label for the respective key signature algorithm (DSA, ECDSA, Ed25519 or RSA).

Command Default

None

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 7.0.1	This command was introduced.
Release 7.3.1	The command was modified to include the **ed25519** option.

Usage Guidelines

This command is applicable only for Cisco IOS XR 64-bit Software.

Task ID

Task ID	Operations
crypto	read, write

Examples

This example shows how to create the RSA key pair for the leaf certificate on the router:

```
Router#configure
Router(config)#crypto ca trustpoint system-trustpoint
Router(config-trustp)# keypair rsa system-enroll-key
Router(config-trustp)# commit
```

Related Commands

Command	Description
ca-keypair, on page 310	Creates the key pair for the root certificate on the router.

keystring

To import the RSA public key in SSH format into the router for authenticating a user, use the **keystring** command in the SSH user key configuration mode. To remove the imported public key, use the **no** form of this command.

keystring [**second** | **third** | **fourth**] *key*

Syntax Description

second	(Optional) Imports the second RSA public key.
third	(Optional) Imports the third RSA public key.
fourth	(Optional) Imports the fourth RSA public key.
key	Specifies the key in SSH format.

Command Default

The command imports the first RSA public key into the router if none of the options are specified.

Command Modes

SSH user key configuration mode

Command History

Release	Modification
Release 7.11.1	This command was modified to include the **second**,**third**, and **fourth** options.
Release 7.2.1	This command was introduced.

Usage Guidelines

This command imports the first RSA public key if you do not specify the **second**,**third**, or **fourth** option.

Task ID

Task ID	Operations
crypto	read, write

Examples

This example shows how to import the first RSA public key specified in SSH format for user *test*.

```
RP/0/RP0/CPU0:OC_router1#conf t
Tue Nov  7 20:28:58.585 IST
RP/0/RP0/CPU0:OC_router1(config)#ssh server username test
RP/0/RP0/CPU0:OC_router1(config-user-key)#keystring ssh-rsa
[redacted]
RP/0/RP0/CPU0:OC_router1(config-user-key)#commit
Tue Nov  7 20:29:19.109 IST
RP/0/RP0/CPU0:OC_router1(config-user-key)#
```

This example shows how to import the third RSA public key specified in SSH format for user *test*.

```
RP/0/RP0/CPU0:OC_router1#conf t
Tue Nov  7 20:28:58.585 IST
RP/0/RP0/CPU0:OC_router1(config)#ssh server  username test
```

```
RP/0/RP0/CPU0:OC_router1(config-user-key)#keystring third ssh-rsa
[redacted]

RP/0/RP0/CPU0:OC_router1(config-user-key)#commit
Tue Nov  7 20:30:51.892 IST
RP/0/RP0/CPU0:OC_router1(config-user-key)#
```

lifetime (trustpoint)

To configure the lifetime for self-enrollment of certificates, use the **lifetime** command in trustpoint configuration mode. To remove this configuration, use the **no** form of this command.

lifetime {**ca-certificate** | **certificate**} *validity*

Syntax Description

ca-certificate	Configures the lifetime for self-enrollment of CA certificate.
validity	Specifies the validity for the certificates, in days. The range is from 30 to 5474 days.

Command Default

None

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

This command is applicable only for Cisco IOS XR 64-bit Software.

Task ID

Task ID	Operations
crypto	read, write

Examples

This example shows how to configure the lifetime for self-enrollment of CA certificate:

```
Router#configure
Router(config)#crypto ca trustpoint system-trustpoint
Router(config-trustp)#lifetime ca-certificate 30
Router(config-trustp)#commit
```

message-digest

To configure the message digest hashing algorithm for the certificates, use the **message-digest** command in trustpoint configuration mode. To remove this configuration, use the **no** form of this command.

message-digest {**md5** | **sha1** | **sha256** | **sha384** | **sha512**}

Syntax Description

md5	Specifies MD5 as the message digest hashing algorithm for the certificate.
sha1	Specifies SHA1 as the message digest hashing algorithm for the certificate.
sha256	Specifies SHA256 as the message digest hashing algorithm for the certificate.
sha384	Specifies SHA384 as the message digest hashing algorithm for the certificate.
sha512	Specifies SHA512 as the message digest hashing algorithm for the certificate.

Command Default

None

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

This command is applicable only for Cisco IOS XR 64-bit Software.

Task ID

Task ID	Operations
crypto	read, write

Examples

This example shows how to specify SHA256 as the message digest hashing algorithm for the certificate:

```
Router#configure
Router(config)#crypto ca trustpoint system-trustpoint
Router(config-trustp)#message-digest sha256
Router(config-trustp)#commit
```

query url

To specify Lightweight Directory Access Protocol (LDAP) protocol support, use the **query url** command in trustpoint configuration mode. To remove the query URL from the configuration, use the **no** form of this command.

query url *LDAP-URL*

Syntax Description

LDAP-URL	URL of the LDAP server (for example, ldap://another-server). This URL must be in the form of ldap://server-name where server-name is the host Domain Name System (DNS) name or IP address of the LDAP server.

Command Default

The URL provided in the router certificate's CRLDistributionPoint extension is used.

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

LDAP is a query protocol used when the router retrieves the Certificate Revocation List (CRL). The certification authority (CA) administrator should be able to tell you whether the CA supports LDAP; if the CA supports LDAP, the CA administrator can tell you the LDAP location where certificates and certificate revocation lists should be retrieved.

To change the query URL, repeat the **query url** command to overwrite the previous URL.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows the configuration required to declare a CA when the CA supports LDAP:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RSP0/CPU0:router(config-trustp)# query url ldap://my-ldap.domain.com
```

Related Commands

Command	Description
crypto ca trustpoint, on page 323	Configures a trusted point with a selected name.

renewal-message-type

Allows you to configure the request type from the router to the CA for automatic PKI certificate renewal.

renewal-message-type { **pkcsreq** | **renewalreq** }

Syntax Description

pkcsreq	The router uses Public Key Cryptography Standards (PKCS) requests for automatic PKI certificate renewal.
renewalreq	The router uses Renew requests for automatic PKI certificate renewal.

Command Default

By default, the PKCS request is available in the router.

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 7.5.3	This command was introduced.

Usage Guidelines

This command is applicable only for Cisco IOS XR 64-bit Software.

Task ID

Task ID	Operations
crypto	read, write

Examples

This example shows how to use this command in the router:

```
Router#configure
Router(config)#crypto ca trustpoint system-trustpoint
Router(config-trustp)# renewal-message-type renewalreq
Router(config-trustp)# keypair rsa system-enroll-key
Router(config-trustp)# commit
```

rsakeypair

To specify a named Rivest, Shamir, and Adelman (RSA) key pair for this trustpoint, use the **rsakeypair** command in trustpoint configuration mode. To reset the RSA key pair to the default, use the **no** form of this command.

rsakeypair *keypair-label*

Syntax Description

keypair-label	RSA key pair label that names the RSA key pairs.

Command Default

If the RSA key pair is not specified, the default RSA key is used for this trustpoint.

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **rsakeypair** command to specify a named RSA key pair generated using the **crypto key generate rsa** command for this trustpoint.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to specify the named RSA key pair key1 for the trustpoint myca:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RSP0/CPU0:router(config-trustp)# rsakeypair key1
```

Related Commands

Command	Description
crypto key generate rsa, on page 336	Generates RSA key pairs.

serial-number (trustpoint)

To specify whether the router serial number should be included in the certificate request, use the **serial-number** command in trustpoint configuration mode. To restore the default behavior, use the **no** form of this command.

serial-number [**none**]

Syntax Description

none	(Optional) Specifies that a serial number is not included in the certificate request.

Command Default

You are prompted for the serial number during certificate enrollment.

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Before you can use the **serial-number** command, you must enable the **crypto ca trustpoint** command, which declares the certification authority (CA) that your router should use and enters trustpoint configuration mode.

Use this command to specify the router serial number in the certificate request, or use the **none** keyword to specify that a serial number should not be included in the certificate request.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to omit a serial number from the root certificate request:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint root
RP/0/RSP0/CPU0:router(config-trustp)# enrollment url http://10.3.0.7:80
RP/0/RSP0/CPU0:router(config-trustp)# ip-address none
RP/0/RSP0/CPU0:router(config-trustp)# serial-number none
RP/0/RSP0/CPU0:router(config-trustp)# subject-name ON=Jack, OU=PKI, O=Cisco Systems, C=US
```

Related Commands

Command	Description
crl optional (trustpoint), on page 313	Allows the certificates of other peers to be accepted without trying to obtain the appropriate CRL.
crypto ca trustpoint, on page 323	Configures a trusted point with a selected name.
enrollment url, on page 353	Specifies the certification authority (CA) location by naming the CA URL.

Command	Description
ip-address (trustpoint), on page 355	Specifies a dotted IP address that is included as an unstructured address in the certificate request.
subject-name (trustpoint), on page 371	Specifies the subject name in the certificate request.

sftp-password (trustpoint)

To secure the FTP password, use the **sftp-password** command in trustpoint configuration mode. To disable this feature, use the **no** form of this command.

sftp-password {*clear text* | **clear** *text* | **password** *encrypted string*}

Syntax Description

clear text	Clear text password and is encrypted only for display purposes.
password *encrypted string*	Enters the password in an encrypted form.

Command Default

The *clear text* argument is the default behavior.

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Passwords are stored in encrypted form and not as plain text. The command-line interface (CLI) contains the provisioning (for example, clear and encrypted) to specify the password input.

The username and password are required as part of the SFTP protocol. If you specify the URL that begins with the prefix (sftp://), you must configure the parameters for the **sftp-password** command under the trustpoint. Otherwise, the certificate from the SFTP server, which is used for manual certificate enrollment, cannot be retrieved.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to secure the FTP password in an encrypted form:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint msiox
RP/0/RSP0/CPU0:router(config-trustp)# sftp-password password xxxxxx
```

Related Commands

Command	Description
crypto ca trustpoint, on page 323	Configures a trusted point with a selected name.
sftp-username (trustpoint), on page 370	Secures the FTP username.

sftp-username (trustpoint)

To secure the FTP username, use the **sftp-username** command in trustpoint configuration mode. To disable this feature, use the **no** form of this command.

sftp-username *username*

Syntax Description

username	Name of the user.

Command Default

None

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

The **sftp-username** command is used only if the URL has (sftp://) in the prefix. If (sftp://) is not specified in the prefix, the manual certificate enrollment using SFTP fails.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to secure the FTP username:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint msiox
RP/0/RSP0/CPU0:router(config-trustp)# sftp-username tmordeko
```

Related Commands

Command	Description
crypto ca trustpoint, on page 323	Configures a trusted point with a selected name.
sftp-password (trustpoint), on page 369	Secures the FTP password.

subject-name (trustpoint)

To specify the subject name in the certificate request, use the **subject-name** command in trustpoint configuration mode. To clear any subject name from the configuration, use the **no** form of this command.

subject-name [**ca-certificate**] *subject-name*

Syntax Description

ca-certificate	(Optional) Specifies the subject name for the CA certificate for self-enrollment.
subject-name	(Optional) Specifies the subject name used in the certificate request.

Command Default

If the *subject-name* argument is not specified, the fully qualified domain name (FQDN), which is the default subject name, is used.

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 7.0.1	The command was modified to include the **ca-certificate** option.

Usage Guidelines

Before you can use the **subject-name** command, you must enable the **crypto ca trustpoint** command, which declares the certification authority (CA) that your router should use and enters trustpoint configuration mode.

The **subject-name** command is an attribute that can be set for automatic enrollment; thus, issuing this command prevents you from being prompted for a subject name during enrollment.

The **ca-certificate** option is applicable only for Cisco IOS XR 64-bit Software.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to specify the subject name for the frog certificate:

```
Router# configure
Router(config)# crypto ca trustpoint frog
Router(config-trustp)# enrollment url http://frog.phoobin.com
Router(config-trustp)# subject-name OU=Spiral Dept., O=tiedye.com
Router(config-trustp)# ip-address 172.19.72.120
```

This example shows how to specify the subject name for the CA certificate for self-enrollment.

```
Router#configure
Router(config)#crypto ca trustpoint system-trustpoint
Router(config-trustp)#subject-name ca-certificate CN=labuser-ca,C=US,ST=CA,L=San Jose,O=cisco
```

```
 systems,OU=ASR
Router(config-trustp)#commit
```

Related Commands

Command	Description
crl optional (trustpoint), on page 313	Allows the certificates of other peers to be accepted without trying to obtain the appropriate CRL.
crypto ca trustpoint, on page 323	Configures a trusted point with a selected name.
enrollment url, on page 353	Specifies the certification authority (CA) location by naming the CA URL.
ip-address (trustpoint), on page 355	Specifies a dotted IP address that is included as an unstructured address in the certificate request.
serial-number (trustpoint), on page 367	Specifies whether the router serial number should be included in the certificate request.

show crypto ca certificates

To display information about your certificate and the certification authority (CA) certificate, use the **show crypto ca certificates** command in EXEC mode.

show crypto ca certificates

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.10.1	This command was modified to include the **Trusted Certificate Chain** field in the output as part of supporting multi-tier CA for trustpoint authentication.
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **show crypto ca certificates** command to display information about the following certificates:

- Your certificate, if you have requested one from the CA (see the **crypto ca enroll** command).
- CA certificate, if you have received the certificate (see the **crypto ca authenticate** command).

Task ID

Task ID	Operations
crypto	read

Examples

The following sample output is from the **show crypto ca certificates** command:

```
RP/0/RSP0/CPU0:router# show crypto ca certificates
Trustpoint       : msiox
================================================
CAa certificate
  Serial Number  : 06:A5:1B:E6:4F:5D:F7:83:41:11:D5:F9:22:7F:95:23
  Subject:
    Name: CA2
    CN= CA2
  Issued By      :
        cn=CA2
  Validity Start : 07:51:51 UTC Wed Jul 06 2005
  Validity End   : 08:00:43 UTC Tue Jul 06 2010
  CRL Distribution Point
        http://10.56.8.236/CertEnroll/CA2.crl
Router certificate
  Status         : Available
  Key usage      : Signature
  Serial Number  : 38:6B:C6:B8:00:04:00:00:01:45
  Subject:
```

```
    Name: tdlr533.cisco.com
    IP Address: 3.1.53.3
    Serial Number: 8cd96b64
  Issued By      :
        cn=CA2
  Validity Start : 08:30:03 UTC Mon Apr 10 2006
  Validity End   : 08:40:03 UTC Tue Apr 10 2007
  CRL Distribution Point
        http://10.56.8.236/CertEnroll/CA2.crl
Associated Trustpoint: MS-IOX
Router certificate
  Status         : Available
  Key usage      : Encryption
  Serial Number  : 38:6D:2B:A7:00:04:00:00:01:46
  Subject:
    Name: tdlr533.cisco.com
    IP Address: 3.1.53.3
    Serial Number: 8cd96b64
  Issued By      :
        cn=CA2
  Validity Start : 08:31:34 UTC Mon Apr 10 2006
  Validity End   : 08:41:34 UTC Tue Apr 10 2007
  CRL Distribution Point
        http://10.56.8.236/CertEnroll/CA2.crl
Associated Trustpoint: msiox
```

The following is a sample output with multi-tier CA. The command output displays the **Trusted Certificate Chain** field if there is one or more subordinate CAs involved in the hierarchy.

```
Router#show crypto ca certificates test-ca
Mon Feb  6 09:03:53.019 UTC

Trustpoint       : test-ca
================================================
CA certificate
  Serial Number  : 10:01
  Subject:
            CN=SUB_CA_CERT,OU=SPBU,O=CSCO,L=BGL,ST=KA,C=IN
  Issued By      :
            CN=TWO-LEVEL-CA,OU=SPBU,O=CSCO,L=BGL,ST=KA,C=IN
  Validity Start : 12:31:40 UTC Sun Jun 14 2020
  Validity End   : 12:31:40 UTC Wed Jun 12 2030

  CRL Distribution Point
            http://10.105.236.78/crl_akshath_two_level_ca/crl.der
  SHA1 Fingerprint:
             D8E0C11ECED96F67FDBC800DB6A126676A76BD62
Trusted Certificate Chain
  Serial Number  : 0F:A0:06:7A:C9:5E:A9:E7:61:A2:B9:2B:27:D1:D6:8F:3D:51:43:3B
  Subject:
            CN=TWO-LEVEL-CA,OU=SPBU,O=CSCO,L=BGL,ST=KA,C=IN
  Issued By      :
            CN=TWO-LEVEL-CA,OU=SPBU,O=CSCO,L=BGL,ST=KA,C=IN
  Validity Start : 13:12:32 UTC Sun Jun 07 2020
  Validity End   : 13:12:32 UTC Sat Jun 02 2040

  CRL Distribution Point
            http://10.105.236.78/crl_akshath_two_level_ca/crl.der
  SHA1 Fingerprint:
             08E71248FB7578614442E713AC87C461D173952F
Router certificate
  Key usage      : General Purpose
  Status         : Available
  Serial Number  : 28:E5
```

```
  Subject:
            CN=test
  Issued By      :
            CN=SUB_CA_CERT,OU=SPBU,O=CSCO,L=BGL,ST=KA,C=IN
  Validity Start : 08:49:54 UTC Mon Feb 06 2023
  Validity End   : 08:49:54 UTC Wed Mar 08 2023
  SHA1 Fingerprint:
             6C8644FA67D9CEBC7C5665C35838265F578835AB
Associated Trustpoint: test-ca
```

Related Commands

Command	Description
crypto ca authenticate, on page 316	Authenticates the CA by obtaining the certificate of the CA.
crypto ca enroll, on page 319	Obtains the certificates of your router from the CA.
crypto ca import, on page 322	Imports a certification authority (CA) certificate manually through TFTP, SFTP, or cut and paste it at the terminal.
crypto ca trustpoint, on page 323	Configures a trustpoint with a selected name.

show crypto ca crls

To display information about the local cache Certificate Revocation List (CRL), use the **show crypto ca crls** command in EXEC mode.

show crypto ca crls

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
crypto	read

Examples

The following sample output is from the **show crypto ca crls** command:

```
RP/0/RSP0/CPU0:router# show crypto ca crls
CRL Entry
==========================================
Issuer : cn=xyz-w2k-root,ou=HFR,o=Cisco System,l=San Jose,st=CA,c=US
Last Update : [UTC] Thu Jan 10 01:01:14 2002
Next Update : [UTC] Thu Jan 17 13:21:14 2002
CRL Distribution Point :
http://xyz-w2k.cisco.com/CertEnroll/xyz-w2k-root.crl
```

Related Commands

Command	Description
clear crypto ca crl, on page 312	Clears all the CRLs stored on the router.

show crypto ca trustpool policy

To display the CA trust pool certificates of the router in a verbose format use the **show crypto ca trustpool policy**command in EXEC mode.

show crypto ca trustpool policy

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

EXEC mode

Command History

Release	Modification
Release 5.2.0	This command was introduced.

Usage Guidelines

Use the command to display the CA trust pool certificates of the router in a verbose format.

Task ID

Task ID	Operation
crypto	read

Example

This example shows you how to run the command to view details of your CA certificate trust pool policy.

```
RP/0/RSP0/CPU0:IMC0#show crypto ca trustpool policy

Trustpool Policy

   Trustpool CA certificates will expire [UTC] Thu Sep 30 14:01:15 2021
   CA Bundle Location: http://cisco.com/security/pki/trs/ios.p7b
```

Related Commands

Command	Description
crypto ca trustpool import url, on page 325	Allows you to manually update certificates in the trust pool.
crypto ca trustpool policy, on page 327	Configures CA trust pool policy parameters.

show crypto key mypubkey authentication-ssh

To display the cryptographic keys that are used for the public key-based authentication of SSH clients on the router, use the **show crypto key mypubkey authentication-ssh** command in EXEC mode.

show crypto key mypubkey authentication-ssh rsa [{ **all** | **username** *name* }]

Syntax Description

rsa	Displays the RSA key of the user.
username *name*	Specifies the name of the user whose RSA key is to be displayed.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

If the **username** is not specified, then the command displays the key for the currently logged-in user.

Task ID

Task ID	Operations
crypto	read

Examples

This example shows how to display the RSA key used for public key-based authentication of SSH clients on Cisco IOS XR routers:

```
Router#show crypto key mypubkey authentication-ssh rsa
Wed Dec 21 10:24:34.226 UTC
Key label: cisco
Type     : RSA Authentication
Size     : 2048
Created  : 10:02:59 UTC Wed Dec 21 2022
Data     :
 30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
 00A292B0 E45ACBB9 47B9EDA8 47E4664E 58FC3EA5 CE0F6B7A 3C6B7A73 537E6CEB
 .
 .
 .
 FF6BAF95 D9617CF6 65C058CC 7C6C22A9 9E48CC43 FDFF0EB7 ABADEB77 55A274DB
 15020301 0001

OpenSSH Format:
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCikrDkWsu5R7ntqEfkZk5Y/.../2uvldlhfPZlwFjMfGwiqZ5IzEP9/w63q63rd1WidNsV

Router#
```

The key value starts with *ssh-rsa* in the above output.

show crypto key mypubkey dsa

To display the Directory System Agent (DSA) public keys for your router, use the **show crypto key mypubkey dsa** command in EXEC mode.

show crypto key mypubkey dsa

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
crypto	read

Examples

The following sample output is from the **show crypto key mypubkey dsa** command:

```
RP/0/RSP0/CPU0:router# show crypto key mypubkey dsa

Key label: mykey
Type : RSA General purpose
Size : 1024
Created : 17:33:23 UTC Thu Sep 18 2003
Data :
3081F230 81AA0605 2B0E0302 0C3081A0 02020200 024100C8 A36B6179 56B8D620
1F77595C 32EF3004 577A9F79 0A8ABDA4 89FB969D 35C04E7E 5491ED4E 120C657C
610576E5 841696B6 0948846C C92F56E5 B4921458 70FC4902 1500AB61 5C0D63D3
EB082BB9 F16030C5 AA0B5D1A DFE50240 73F661EA 9F579E77 B413DBC4 9047B4F2
10A1CFCB 14D98B57 3E0BBA97 9B5120AD F52BBDC7 15B63454 8CB54885 92B6C9DF
7DC27768 FD296844 42024945 5E86C81A 03430002 4071B49E F80F9E4B AF2B62E7
AA817460 87EFD503 C668AD8C D606050B 225CC277 7C0A0974 8072D7D7 2ADDDE42
329FE896 AB015ED1 3A414254 6935FDCA 0043BA4F 66
```

Related Commands

Command	Description
crypto key generate dsa, on page 330	Generates DSA key pairs.
crypto key zeroize dsa, on page 343	Deletes all DSA keys from the router.

show crypto key mypubkey ecdsa

To display the Elliptic Curve Digital Signature Algorithm (ECDSA) public keys for your router, use the **show crypto key mypubkey ecdsa** command in EXEC mode.

show crypto key mypubkey ecdsa

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.4.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
crypto	read

Example

```
RP/0/RSP0/CPU0:Router# show crypto key mypubkey ecdsa

Key label: the_default
Type     : ECDSA General Curve Nistp256
Degree   : 256
Created  : 19:10:54 IST Mon Aug 21 2017
Data     :
 04255331 89B3CC40 BCD5A5A3 3BCCE7FF 522BF88D F3CC300D CEC9D7FD 98796ABB
 6A69523F E5FBAB66 804A05BF ECCDABC6 63F73AE8 E89827DD 18EB106A 7735C34A
```

show crypto key mypubkey ed25519

To display the Ed25519 crypto public keys of your router, use the **show crypto key mypubkey ed25519** command in EXEC mode.

show crypto key mypubkey ed25519

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.3.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
crypto	read

Examples

This example shows the sample output of the **show crypto key mypubkey ed25519** command:

```
Router# show crypto key mypubkey  ed25519

Mon Nov 30 07:05:06.532 UTC
Key label: the_default
Type : ED25519
Size : 256
Created : 07:03:17 UTC Mon Nov 30 2020
Data :
FF0ED4E7 71531B3D 9ED72C48 3F79EC59 9EFECCC3 46A129B2 FAAA12DD EE9D0351
```

Related Commands

Command	Description
crypto key generate ed25519, on page 334	Generates Ed25519 crypto key pairs.
crypto key zeroize ed25519, on page 345	Deletes all Ed25519 keys from the router.

show crypto key mypubkey rsa

To display the Rivest, Shamir, and Adelman (RSA) public keys for your router, use the **show crypto key mypubkey rsa** command in EXEC mode.

show crypto key mypubkey rsa

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
crypto	read

Examples

The following is sample output from the **show crypto key mypubkey rsa** command:

```
RP/0/RSP0/CPU0:router# show crypto key mypubkey rsa

Key label: mykey
Type : RSA General purpose
Size : 1024
Created  : 07:46:15 UTC Fri Mar 17 2006
Data :
30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00CF8CDF
5BFCA055 DA4D164D F6EDB78B 926B1DDE 0383027F BA71BCC6 9D5592C4 5BA8670E
35CD19B7 1C973A46 62CC5F8C 82BD596C F292410F 8E83B753 4BA71BAC 41AB6B60
F34A2499 EDE11639 F88B4210 B2A0CF5F DD678C36 0D8B7DE1 A2AB5122 9ED947D5
76CF5BCD D9A2039F D02841B0 7F8BFF97 C080B791 10A9ED41 00FB6F40 95020301
0001

Key label: the_default
Type : RSA General purpose
Size : 512
Created  : 07:46:15 UTC Fri Mar 17 2006
Data :
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00C7DE73 7B3EA447
CCE8F3DF DD1327D8 C1C30C45 2EEB4981 B1B48D2B 1AF14665 178058FB 8F6BB6BB
E08C6163 FA0EE356 395C8E5F 2AC59383 0706BDDF EC8E5822 9B020301 0001
```

Related Commands

Command	Description
crypto key generate rsa, on page 336	Generates RSA key pairs.
crypto key zeroize rsa, on page 346	Deletes all RSA keys from the router.

show crypto sks profile

To display the details of one or all sks profiles in the router, use the **show crypto sks profile** command in the EXEC mode.

show crypto sks profile { *profile-name* | **all** } **stats**

Syntax Description

profile name	Specifies the name of the SKS profile.
all	Specifies all the SKS profiles in the router.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
system	read

This example shows how to view the SKS profile details in a router:

```
Router(ios)# show crypto sks profile all
Profile Name        :ProfileR1toR2
Myidentifier       :Router1
Type               :Remote
Reg Client Count     :1

Server
IP                  :192.0.2.35
Port                :10001
Vrf                 :Notconfigured
Source Interface    :Notconfigured
Status              :Connected
Entropy             :true
Key                 :true
Algorithm           :QKD
Local identifier    :Alice
Remote identifier   :Alice, Bob

Peerlist
QKD ID               :Alice
State                :Connected

QKD ID               :Bob
State                :Connected
```

This example shows how to view the SKS profile statistics in a router:

```
Router(ios)# show crypto sks profile all stats
Profile Name            : ProfileR1toR2
My identifier           : Router1
Server
 IP                     : 192.0.2.35
 Port                   : 10001
 Status                 : connected
Counters
 Capability request         : 1
 Key request                : 3
 Key-id request             : 0
 Entropy request            : 0
 Capability response        : 1
 Key response               : 3
 Key-id response            : 0
 Entropy response           : 0
 Total request              : 4
 Request failed             : 0
 Request success            : 4
 Total response             : 4
 Response failed            : 0
 Response success           : 4
 Retry count                : 0
 Response Ignored           : 0
 Cancelled count            : 0
Response time
 Max Time                   : 100 ms
 Avg Time                   : 10  ms
 Min Time                   : 50  ms
Last transaction
 Transaction Id             : 9
 Transaction type           : Get key
 Transaction status         : Response data received, successfully
 Http code                  : 200 OK (200)
```

show platform security integrity dossier

To collect the data from various IOS XR applications, use the **show platform security integrity dossier** command in EXEC mode.

show platform security integrity dossier [**include** { **packages** | **reboot-history** | **rollback-history** | **running-config** | **system-integrity-snapshot** | **system-inventory** | **filesystem-inventory** }] [**nonce** *nonce-value* | **display compact**]

Syntax Description

packages	Displays active package(s) installed.
reboot-history	Displays reboot history of the node.
rollback-history	Displays rollback history of the node.
running-config	Displays the currently committed running configuration on the node, as displayed by **show running configuration** command.
system-integrity-snapshot	Displays the system integrity snapshot.
system-inventory	Displays the system inventory.
filesystem-inventory	Displays the metadata of filesystem inventory.
nonce	Specifies the nonce to generate the signature.
nonce-value	Specifies the nonce value in hexadecimal string format.
display compact	Displays IMA event logs in the protobuf format.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.0.1	This command was introduced.
Release 7.3.1	Added support to collect metadata about the filesystem inventory.
Release 7.4.1	Display compact keyword was introduced.

Usage Guidelines

This command is applicable only for Cisco IOS XR 64-bit Software.

The output of this command is displayed in JSON format.

Task ID

Options	Task ID	Operations
packages	pkg-mgmt	read
reboot-history	system	read
rollback-history	config-services	read
running-config	NA (available to all users)	read
system-integrity-snapshot	basic-services	read
system-inventory	sysmgr	read
filesystem-inventory	NA (available to all users)	read

Examples

This example shows the usage of **show platform security integrity dossier** command with various selectors:

```
Router#show platform security integrity dossier include packages reboot-history
rollback-history system-integrity-snapshot system-inventory filesystem-inventory nonce 1580
 | utility sign nonce 1580 include-certificate
```

utility sign

To sign the command output with the enrollment key to verify its data integrity and authenticity, use the **utility sign** command along with any of the Cisco IOS XR commands.

utility sign [{**include-certificate** | **nonce** *nonce-value*}]

Syntax Description

include-certificate	Includes the certificate of the signer.
nonce	Indicates the nonce to generate the signature.
nonce-value	Specifies the nonce value in hexadecimal string format.

Command Default

None

Command Modes

Any IOS XR command configuration mode.

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

This command is applicable only for Cisco IOS XR 64-bit Software.

Task ID

Task ID	Operations
crypto	execute

Examples

This example shows how to add a signature to the command output data to verify its data integrity and authenticity:

```
Router#show version | utility sign nonce 1234 include-certificate
```

Software Authentication Manager Commands

This module describes the Cisco IOS XR software commands used to configure Software Authentication Manager (SAM).

For detailed information about SAM concepts, configuration tasks, and examples, see the *Configuring Software Authentication Manager on* the Cisco ASR 9000 Series Router module in the *System Security Configuration Guide for Cisco ASR 9000 Series Routers* .

sam add certificate

To add a new certificate to the certificate table, use the **sam add certificate** command in EXEC mode.

sam add certificate *filepath location* {**trust** | **untrust**}

Syntax Description

filepath	Absolute path to the source location of the certificate.
location	Storage site of the certificate. Use one of the following: **root**, **mem**, **disk0**, **disk1**, or **other flash device name on router**.
trust	Adds the certificate to the certificate table without validation by the Software Authentication Manager (SAM). To add a root certificate, you must use the **trust** keyword. Adding a root certificate with the **untrust** keyword is not allowed.
untrust	Adds the certificate to the certificate table after the SAM has validated it. Adding a root certificate with the **untrust** keyword is not allowed. To add a root certificate, you must use the **trust** keyword.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

For security reasons, the **sam add certificate** command can be issued only from the console or auxiliary port of the networking device; the command cannot be issued from a Telnet connection to any other interface on the networking device.

The certificate must be copied to the network device before it can be added to the certificate table. If the certificate is already present in the certificate table, the SAM rejects the attempt to add it.

When adding root certificates, follow these guidelines:

- Only the certificate authority (CA) root certificate can be added to the root location.
- To add a root certificate, you must use the **trust** keyword. Adding the root certificate with the **untrust** keyword is not allowed.

Use of the **trust** keyword assumes that you received the new certificate from a source that you trust, and therefore have enough confidence in its authenticity to bypass validation by the SAM. One example of acquiring a certificate from a trusted source is downloading it from a CA server (such as Cisco.com) that requires user authentication. Another example is acquiring the certificate from a person or entity that you can verify, such as by checking the identification badge for a person. If you bypass the validation protection offered by the SAM, you must verify the identity and integrity of the certificate by some other valid process.

Certificates added to the memory (**mem**) location validate software installed in memory. Certificates added to the **disk0** or **disk1** location validate software installed on those devices, respectively.

Note If the **sam add certificate** command fails with a message indicating that the certificate has expired, the networking device clock may have been set incorrectly. Use the **show clock** command to determine if the clock is set correctly.

Task ID

Task ID	Operations
crypto	execute

Examples

The following example shows how to add the certificate found at **/bootflash/ca.bin** to the certificate table in the root location without first validating the certificate:

```
RP/0/RSP0/CPU0:router# sam add certificate /bootflash/ca.bin root trust

SAM: Successful adding certificate /bootflash/ca.bin
```

The following example shows how to add the certificate found at **/bootflash/css.bin** to the certificate table in the memory (**mem**) location after validating the certificate:

```
RP/0/RSP0/CPU0:router# sam add certificate /bootflash/css.bin mem untrust

SAM: Successful adding certificate /bootflash/css.bin
```

Related Commands

Command	Description
sam delete certificate, on page 394	Deletes a certificate from the certificate table.
show sam certificate, on page 400	Displays records in the certificate table, including the location of the certificates.
show clock	Displays networking device clock information. For more information, see *System Management Command Reference for Cisco ASR 9000 Series Routers*.

sam delete certificate

To delete a certificate from the certificate table, use the **sam delete certificate** command in EXEC mode.

sam delete certificate *location certificate-index*

Syntax Description

location	Storage site of the certificate. Use one of the following: **root**, **mem**, **disk0**, **disk1**, or **other flash device name on the router**.
certificate-index	Number in the range from 1 to 65000.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

For security reasons, the **sam delete certificate** command can be issued only from the console port of the networking device; the command cannot be issued from a Telnet connection to any other interface on the networking device.

Use the **show sam certificate summary** command to display certificates by their index numbers.

Because the certificate authority (CA) certificate must not be unknowingly deleted, the Software Authentication Manager (SAM) prompts the user for confirmation when an attempt is made to delete the CA certificate.

If a certificate stored on the system is no longer valid (for example, if the certificate has expired), you can use the **sam delete certificate** command to remove the certificate from the list.

Task ID

Task ID	Operations
crypto	execute

Examples

The following example shows how to delete the certificate identified by the index number 2 from the memory location:

```
RP/0/RSP0/CPU0:router# sam delete certificate mem 2

SAM: Successful deleting certificate index 2
```

The following example shows how to cancel the deletion of the certificate identified by the index number 1 from the root location:

```
RP/0/RSP0/CPU0:router# sam delete certificate root 1

Do you really want to delete the root CA certificate (Y/N): N
SAM: Delete certificate (index 1) canceled
```

The following example shows how to delete the certificate identified by the index number 1 from the root location:

```
RP/0/RSP0/CPU0:router# sam delete certificate root 1

Do you really want to delete the root CA certificate (Y/N): Y
SAM: Successful deleting certificate index 1
```

Related Commands

Command	Description
sam add certificate, on page 392	Adds a new certificate to the certificate table.
show sam certificate, on page 400	Displays records in the certificate table, including the location of the certificates stored.

sam prompt-interval

To set the interval that the Software Authentication Manager (SAM) waits after prompting the user for input when it detects an abnormal condition at boot time and to determine how the SAM responds when it does not receive user input within the specified interval, use the **sam prompt-interval** command in Global Configuration mode. To reset the prompt interval and response to their default values, use the **no** form of this command.

sam prompt-interval *time-interval* {**proceed** | **terminate**}

Syntax Description

time-interval	Prompt time, in the range from 0 to 300 seconds.
proceed	Causes the SAM to respond as if it had received a "yes" when the prompt interval expires.
terminate	Causes the SAM to respond as if it had received a "no" when the prompt interval expires.

Command Default

The default response is for the SAM to wait 10 seconds and then terminate the authentication task.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **sam prompt-interval** command to control the action taken when the system detects an exception condition, such as an expired certificate during initialization of the SAM at boot time. The following message appears when the software detects the abnormal condition of a certificate authority (CA) certificate expired:

```
SAM detects expired CA certificate. Continue at risk (Y/N):
```

The SAM waits at the prompt until you respond or the time interval controlled by the **sam prompt-interval** command expires, whichever is the earlier event. If you respond "N" to the prompt, the boot process is allowed to complete, but no packages can be installed.

The following message appears when the software detects the abnormal condition of a Code Signing Server (CSS) certificate expired:

```
SAM detects CA certificate (Code Signing Server Certificate Authority) has expired. The
validity period is Oct 17, 2000 01:46:24 UTC - Oct 17, 2015 01:51:47 UTC. Continue at risk?
 (Y/N) [Default:N w/in 10]:
```

If you do not respond to the prompt, the SAM waits for the specified interval to expire, and then it takes the action specified in the **sam prompt-interval** command (either the **proceed** or **terminate** keyword).

If you enter the command with the **proceed** keyword, the SAM waits for the specified interval to expire, and then it proceeds as if you had given a "yes" response to the prompt.

If you enter the command with the **terminate** keyword, the SAM waits for the specified interval to expire, and then it proceeds as if you had given a "no" response to the prompt. This use of the command keeps the system from waiting indefinitely when the system console is unattended.

Note After the software has booted up, the *time-interval* argument set using this command has no effect. This value applies at boot time only.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to tell the SAM to wait 30 seconds for a user response to a prompt and then terminate the requested SAM processing task:

```
RP/0/RSP0/CPU0:router/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# sam prompt-interval 30 terminate
```

Related Commands

Command	Description
show sam sysinfo, on page 410	Displays the current status information for the SAM.

sam verify

To use the Message Digest 5 (MD5) hash algorithm to verify the integrity of the software component on a flash memory card and ensure that it has not been tampered with during transit, use the **sam verify** command in EXEC mode.

sam verify {*locationfile-system*} {**MD5** | **SHA** [*digest*]}

Syntax Description

location	Name of the flash memory card slot, either disk0 or disk1.
file-system	Absolute path to the file to be verified.
MD5	Specifies a one-way hashing algorithm to generate a 128-bit hash (or message digest) of the specified software component.
SHA	Specifies the Secure Hash Algorithm, a hashing algorithm that takes a message of less than 264 bits in length and produces a 160-bit message digest. The large message digest provides security against brute-force collision and inversion attacks.
digest	(Optional) Message digest generated by the hashing algorithm, to be compared in determining the integrity of the software component.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **sam verify** command to generate a message digest for a given device. The message digest is useful for determining whether software on a flash memory card has been tampered with during transit. The command generates a hash code that can be used to compare the integrity of the software between the time it was shipped and the time you received it.

For example, if you are given a flash memory card with preinstalled software and a previously generated MD5 message digest, you can verify the integrity of the software using the **sam verify** command:

```
sam verify device MD5 digest
```

The *device* argument specifies the flash device. The *digest* argument specifies the message digest supplied by the originator of the software.

If the message digest matches the message digest generated by the **sam verify** command, the software component is valid.

Note You should calculate the hash code on the contents of the flash memory code at the destination networking device using a different set of files from the one loaded on the flash memory card. It is possible for an unauthorized person to use the same software version to produce the desired (matching) hash code and thereby disguise that someone has tampered with the new software.

Task ID

Task ID	Operations
crypto	execute

Examples

The example shows a third **sam verify** command, issued with a mismatched message digest, to show the Software Authentication Manager (SAM) response to a mismatch. The following example shows how to use MD5 to generate a message digest on the entire file system on the flash memory card in slot 0 and then use that message digest as input to perform the digest comparison:

```
RP/0/RSP0/CPU0:router# sam verify disk0: MD5

Total file count in disk0: = 813
082183cb6e65a44fd7ca95fe8e93def6

RP/0/RSP0/CPU0:router# sam verify disk0: MD5 082183cb6e65a44fd7ca95fe8e93def6

Total file count in disk0: = 813
Same digest values

RP/0/RSP0/CPU0:router# sam verify disk0: MD5 3216c9282d97ee7a40b78a4e401158bd

Total file count in disk0: = 813
Different digest values
```

The following example shows how to use MD5 to generate a message digest and then uses that message digest as input to perform the digest comparison:

```
RP/0/RSP0/CPU0:router# sam verify disk0: /crl_revoked.bin MD5

38243ffbbe6cdb7a12fa9fa6452956ac

RP/0/RSP0/CPU0:router# sam verify disk0: /crl_revoked.bin MD5 38243ffbbe6cdb7a12fa9fa6452956ac

Same digest values
```

show sam certificate

To display records in the certificate table, use the **show sam certificate** command in EXEC mode.

Syntax Description

detail	Displays all the attributes for the selected table entry (specified by the *location* and *certificate-index* arguments).
location	Specifies where the entry to display is stored. Use one of the following values: • **root—**Certificate is stored on the root device. • **mem—**Certificate is stored in memory. • *device-name*—Certificate is stored on the named device. Use the values disk0, disk1, or the name of any other flash-device on the router. You can research flash-device names using the **show filesystem** command.
certificate-index	Index number for the entry in the Certificate Table that you want to display, in the range from 1 to 65000.
brief	Displays a subset of attributes for entries in a Certificate Table.
location	Specifies where the entries to display are stored. Use one of the following values: • **all**—Displays a subset of attributes for all certificates. • **root—**Displays a subset of attributes for all certificates stored on the root device. • **mem—**Displays a subset of attributes for all certificates stored in memory. • *device-name*—Displays a subset of attributes for all certificates stored on the named device. Use the values disk0, disk1, or the name of any other flash-device on the router. You can research flash-device names using the **show filesystem** command.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **show sam certificate** command when you want to display all the certificates stored in the system. Attributes are certificate number, certificate flag, serial number, subject name, issued by, version, issuing algorithm, not-before and not-after dates, public key, and signature.

To get the certificate number, use the *certificate-index* argument. When used with the **brief** keyword, the **all** keyword displays selected attributes for all the entries in the table.

Task ID

Task ID	Operations
none	—

Examples

In the example, the root location has one certificate, and disk0 has one certificate. The following sample output is from the **show sam certificate** command:

```
RP/0/RSP0/CPU0:router# show sam certificate
            brief

            all

-------------------- SUMMARY OF CERTIFICATES -------------------

Certificate Location    :root
Certificate Index       :1
Certificate Flag        :VALIDATED
  Serial Number  :32:E0:A3:C6:CA:00:39:8C:4E:AC:22:59:1B:61:03:9F
  Subject Name   :
        cn=Code Signing Server Certificate Authority,o=Cisco,c=US
  Issued By      :
        cn=Code Signing Server Certificate Authority,o=Cisco,c=US
  Validity Start :[UTC] Tue Oct 17 01:46:24 2000
  Validity End   :[UTC] Sat Oct 17 01:51:47 2015
  CRL Distribution Point

file://\\CodeSignServer\CertEnroll\Code%20Signing%20Server%20Certificate
%20Authority.crl

Certificate Location    :mem
Certificate Index       :1
Certificate Flag        :VALIDATED
  Serial Number  :01:27:FE:79:00:00:00:00:00:05
  Subject Name   :
        cn=Engineer code sign certificate
  Issued By      :
        cn=Code Signing Server Certificate Authority,o=Cisco,c=US
  Validity Start :[UTC] Tue Oct  9 23:14:28 2001
  Validity End   :[UTC] Wed Apr  9 23:24:28 2003
  CRL Distribution Point

file://\\CodeSignServer\CertEnroll\Code%20Signing%20Server%20Certificate %20Authority.crl
```

This table describes the significant fields shown in the display.

Table 14: show sam certificate summary all Field Descriptions

Field	Description
Certificate Location	Location of the certificate; one of the following: **root**, **mem**, **disk0**, or **disk1** , or other flash device name.
Certificate Index	Index number that the Software Authentication Manager automatically assigns to the certificate.
Certificate Flag	One of the following: TRUSTED, VALIDATED, EXPIRED, or REVOKED.

Field	Description
Serial Number	Unique serial number of the certificate, assigned by its issuer.
Subject Name	Name of the entity for which the certificate is issued.
Issued By	Name of the entity that issued the certificate.

The following sample output from the **show sam certificate** command shows how to display particular SAM details:

```
RP/0/RSP0/CPU0:router# show sam certificate detail mem 1
------------------------------------------------------------

Certificate Location    :mem
Certificate Index       :1
Certificate Flag        :VALIDATED

----------------------- CERTIFICATE ------------------------
  Serial Number  :01:27:FE:79:00:00:00:00:00:05
  Subject Name   :
        cn=Engineer code sign certificate
  Issued By      :
        cn=Code Signing Server Certificate Authority,o=Cisco,c=US
  Validity Start :[UTC] Tue Oct  9 23:14:28 2001
  Validity End   :[UTC] Wed Apr  9 23:24:28 2003
  CRL Distribution Point

file://\\CodeSignServer\CertEnroll\Code%20Signing%20Server%20Certificate
%20Authority.crl
  Version 3 certificate
  Issuing Algorithm:MD5withRSA
  Public Key BER (294 bytes):
 30 82 01 22 30 0d 06 09 2a 86 48 86 f7 0d 01 01      [0.."0...*.H.....]
 01 05 00 03 82 01 0f 00 30 82 01 0a 02 82 01 01      [........0.......]
 00 be 75 eb 9b b3 d9 cb 2e d8 c6 db 68 f3 5a ab      [..u.........h.Z.]
 0c 17 d3 84 16 22 d8 18 dc 3b 13 99 23 d8 c6 94      [....."...;..#...]
 91 15 15 ec 57 ea 68 dc a5 38 68 6a cb 0f 4b c2      [....W.h..8hj..K.]
 43 4b 2d f9 92 94 93 04 df ff ca 0b 35 1d 85 12      [CK-.........5...]
 99 e9 bd bc e2 98 99 58 fe 6b 45 38 f0 52 b4 cb      [.......X.kE8.R..]
 a9 47 cd 22 aa ce 70 0e 4c 9b 48 a1 cf 0f 4a db      [.G."..p.L.H...J.]
 35 f5 1f 20 b7 68 cb 71 2c 27 01 84 d6 bf 4e d1      [5.. .h.q,'....N.]
 ba e1 b2 50 e7 f1 29 3a b4 85 3e ac d7 cb 3f 36      [...P..):..>...?6]
 96 65 30 13 27 48 84 f5 fe 88 03 4a d7 05 ed 72      [.e0.'H.....J...r]
 4b aa a5 62 e6 05 ac 3d 20 4b d6 c9 db 92 89 38      [K..b...= K.....8]
 b5 14 df 46 a3 8f 6b 05 c3 54 4d a2 83 d4 b7 02      [...F..k..TM.....]
 88 2d 58 e7 a4 86 1c 48 77 68 49 66 a1 35 3e c4      [.-X....HwhIf.5>.]
 71 20 aa 18 9d 9f 1a 38 52 3c e3 35 b2 19 12 ad      [q .....8R<.5....]
 99 ad ce 68 8b b0 d0 29 ba 25 fd 1e e0 5d aa 12      [...h...).%...]..]
 9c 44 89 63 89 62 e3 cb f3 5d 5f a3 7c b7 b9 ef      [.D.c.b...]_.|...]
 01 89 5b 33 35 a8 81 60 38 61 4e d8 4f 6a 53 70      [..[35..`8aN.OjSp]
 35 02 03 01 00 01                                    [5.....]
  Certificate signature (256 bytes):
 67 f6 12 25 3f d4 d2 dd 6a f7 3e 55 b8 9f 33 53      [g..%?...j.>U..3S]
 20 4d d1 17 54 08 8a 70 22 35 92 59 9c 03 9c 0f      [ M..T..p"5.Y....]
 ce 46 3c 06 74 d0 a9 8e b1 88 a2 35 b3 eb 1b 00      [.F<.t......5....]
 5c 6d bb 1d b5 ad 17 19 f2 c6 96 87 9b e7 15 01      [\m..............]
 b2 04 af 7d 92 60 d9 ee ef bc 60 4e 2e af 84 e2      [...}.`....`N....]
 42 fe 07 71 7e fc ee ee f5 d1 6d 71 e7 46 f0 97      [B..q~.....mq.F..]
 e0 e8 b3 0e f9 07 e0 de 6e 36 5a 56 1e 80 10 05      [........n6ZV....]
 59 d9 88 ba f7 a3 d1 f6 cd 00 12 9f 90 f0 65 83      [Y.............e.]
```

```
e9 0f 76 a4 da eb 1b 1b 2d ea bd be a0 8a fb a7      [..v.....-.......]
a5 18 ff 9f 5c e9 99 66 f0 d3 90 ae 49 3f c8 cc      [....\..f....I?..]
32 6b db 64 da fd f5 42 ea bc f3 b0 8a 2f 17 d8      [2k.d...B...../..]
cf c0 d8 d4 3a 41 ae 1d cf 7a c6 a6 a1 65 c2 94      [....:A...z...e..]
8a ba ea d3 da 3e 8a 44 9b 47 35 10 ab 61 1b 4f      [.....>.D.G5..a.O]
82 dd 59 16 d5 f2 1d f3 c2 08 cc 1c 7f ab be 9c      [..Y.............]
be 52 73 ea e0 89 d7 6f 4d d0 d8 aa 3d 50 d6 b0      [.Rs....oM...=P..]
e1 ea 3b 27 50 42 08 d6 71 eb 66 37 b1 f5 f6 5d      [..;'PB..q.f7...]]
```

This table describes the significant fields shown in the display.

Table 15: show sam certificate detail mem 1 Field Descriptions

Field	Descriptions
Certificate Location	Location of the certificate; one of the following: **root**, **mem**, **disk0**, or **disk1**.
Certificate Index	Index number that the SAM automatically assigns to the certificate.
Certificate Flag	One of the following: TRUSTED, VALIDATED, EXPIRED, or REVOKED.
Serial Number	Unique serial number of the certificate, assigned by its issuer.
Subject Name	Name of the entity for which the certificate is issued.
Issued By	Name of the entity that issued the certificate.
Version	The ITU-T X.509 version of the certificate. The version can be 1 (X.509v1), 2 (X.509v2), or 3 (X.509v3).
Issuing Algorithm	Hash and public key algorithm that the issuer uses to sign the certificate.
Public Key	Subject public key for the certificate.
Certificate signature	Encrypted hash value (or signature) of the certificate. The hash value of the certificate is encrypted using the private key of the issuer.

show sam crl

To display the records in the certificate revocation list (CRL) table, use the **show sam crl** command in EXEC mode.

show sam crl {**summary** | **detail** *crl-index*}

Syntax Description

summary	Displays selected attributes for all entries in the table.
detail	Displays all the attributes for the selected table entry (specified by the *crl-index* argument).
crl-index	Index number for the entry, in the range from 1 to 65000.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **show sam crl** command when you want to display all the revoked certificates currently stored on the system. Attributes are CRL index number, issuer, and update information.

To get the CRL index number, use the **summary** keyword.

Task ID

Task ID	Operations
crypto	read

Examples

The following sample output is from the **show sam crl** command for the **summary** keyword:

```
RP/0/RSP0/CPU0:router# show sam crl summary

----------------------- SUMMARY OF CRLs --------------------------

CRL Index       :1
Issuer:CN = Code Sign Server Certificate Manager, OU = Cisco HFR mc , O =
Cisco,
  L = San Jose, ST = CA, C = US, EA =<16> iosmx-css-cert@cisco.com
Including updates of:
                      Sep 09, 2002 03:50:41 GMT
```

This table describes the significant fields shown in the display.

Table 16: show sam crl summary Field Descriptions

Field	Description
CRL Index	Index number for the entry, in the range from 1 to 65000. The index is kept in the certificate revocation list table.
Issuer	Certificate authority (CA) that issued this CRL.
Including updates of	Versions of CRLs from this CA that are included in the CRL table.

The following sample output is from the **show sam crl** command for the **detail** keyword:

```
RP/0/RSP0/CPU0:router# show sam crl detail 1

------------------------------------------------------------------

CRL Index      :1

-------------- CERTIFICATE REVOCATION LIST (CRL) -----------------

Issuer:CN = Code Sign Server Certificate Manager, OU = Cisco HFR mc , O = Cisco,
 L = San Jose, ST = CA, C = US, EA =<16> iosmx-css-cert@cisco.com
Including updates of:
                    Sep 09, 2002 03:50:41 GMT
Revoked certificates include:

   Serial #:61:2C:5C:83:00:00:00:00:00:44, revoked on Nov 03, 2002 00:59:02 GMT
   Serial #:21:2C:48:83:00:00:00:00:00:59, revoked on Nov 06, 2002 19:32:51 GMT
------------------------------------------------------------------------------
```

This table describes the significant fields shown in the display.

Table 17: show sam crl detail Field Descriptions

Field	Descriptions
CRL Index	Index number for the entry, in the range from 1 to 65000. The index is kept in the certificate revocation list table.
Issuer	CA that issued this CRL.
Including updates of	Versions of CRLs from this CA that are included in the CRL table.
Revoked certificates include	List of certificates that have been revoked, including the certificate serial number and the date and time the certificate was revoked.

show sam log

To display the contents of the Software Authentication Manager (SAM) log file, use the **show sam log** command in EXEC mode.

show sam log [*lines-number*]

Syntax Description

lines-number	(Optional) Number of lines of the SAM log file to display, in the range from 0 to 200, where 0 displays all lines in the log file and 200 displays the most recent 200 lines (or as many lines as there are in the log file if there are fewer than 200 lines).

Command Default

The **show sam log** command without a *lines-number* argument displays all the lines in the log file.

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

The SAM log file records changes to the SAM tables, including any expired or revoked certificates, table digest mismatches, and SAM server restarts.

Task ID

Task ID	Operations
crypto	read

Examples

The following sample output is from the **show sam log** command:

```
RP/0/RSP0/CPU0:router# show sam log

06/16/02 12:03:44 UTC Added certificate in table root/1 CN = Certificate Manage, 0x01
06/16/02 12:03:45 UTC SAM server restarted through router reboot
06/16/02 12:03:47 UTC Added CRL in table CN = Certificate Manage, updated at Nov 10, 2001
   04:11:42 GMT
06/16/02 12:03:48 UTC Added certificate in table mem:/1 CN = Certificate Manage, 0x1e
06/16/02 12:16:16 UTC SAM server restarted through router reboot
06/16/02 12:25:02 UTC SAM server restarted through router reboot
06/16/02 12:25:04 UTC Added certificate in table mem:/1 CN = Certificate Manage, 0x1e
06/16/02 12:39:30 UTC SAM server restarted through router reboot
06/16/02 12:39:30 UTC SAM server restarted through router reboot
06/16/02 12:40:57 UTC Added certificate in table mem/1 CN = Certificate Manage, 0x1e

33 entries shown
```

Each line of output shows a particular logged event such as a table change, expired or revoked certificates, table digest mismatches, or SAM server restarts.

show sam package

To display information about the certificate used to authenticate the software for a particular package installed on the networking device, use the **show sam package** command in EXEC mode.

show sam package *package-name*

Syntax Description

package-name	Location of the software package, including the memory device (**disk0:**, **disk1:**, **mem**:, and so on) and the file system path to the file. Use the **show install all** command to display the Install Manager package name and location information.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **show install all** command to display the installed location and name of the software package—for example, mem:ena-base-0.0.0 or disk1:crypto-exp-lib-0.4.0—and then use the **show sam package** command to display information about the certificate used to authenticate that installed package. The **show sam package** command displays the same information as the **show sam certificate** command for the **detail** keyword.

Task ID

Task ID	Operations
crypto	read

Examples

The following sample output is from the **show sam package** command:

```
RP/0/RSP0/CPU0:router# show sam package mem:12k-rp-1.0.0

------------------------------------------------------------

Certificate Location    :mem
Certificate Index       :1
Certificate Flag        :VALIDATED

----------------------- CERTIFICATE ------------------------
  Serial Number  :01:27:FE:79:00:00:00:00:00:05
  Subject Name   :
        cn=Engineer code sign certificate
  Issued By      :
        cn=Code Signing Server Certificate Authority,o=Cisco,c=US
  Validity Start :[UTC] Tue Oct  9 23:14:28 2001
  Validity End   :[UTC] Wed Apr  9 23:24:28 2002
  CRL Distribution Point

file://\\CodeSignServer\CertEnroll\Code%20Signing%20Server%20Certificate
```

```
%20Authority.crl
  Version 3 certificate
  Issuing Algorithm:MD5withRSA
  Public Key BER (294 bytes):
 30 82 01 22 30 0d 06 09 2a 86 48 86 f7 0d 01 01      [0.."0...*.H.....]
 01 05 00 03 82 01 0f 00 30 82 01 0a 02 82 01 01      [........0.......]
 00 be 75 eb 9b b3 d9 cb 2e d8 c6 db 68 f3 5a ab      [..u.........h.Z.]
 0c 17 d3 84 16 22 d8 18 dc 3b 13 99 23 d8 c6 94      [....."...;..#...]
 91 15 15 ec 57 ea 68 dc a5 38 68 6a cb 0f 4b c2      [....W.h..8hj..K.]
 43 4b 2d f9 92 94 93 04 df ff ca 0b 35 1d 85 12      [CK-.........5...]
 99 e9 bd bc e2 98 99 58 fe 6b 45 38 f0 52 b4 cb      [.......X.kE8.R..]
 a9 47 cd 22 aa ce 70 0e 4c 9b 48 a1 cf 0f 4a db      [.G."..p.L.H...J.]
 35 f5 1f 20 b7 68 cb 71 2c 27 01 84 d6 bf 4e d1      [5.. .h.q,'....N.]
 ba e1 b2 50 e7 f1 29 3a b4 85 3e ac d7 cb 3f 36      [...P..):..>...?6]
 96 65 30 13 27 48 84 f5 fe 88 03 4a d7 05 ed 72      [.e0.'H.....J...r]
 4b aa a5 62 e6 05 ac 3d 20 4b d6 c9 db 92 89 38      [K..b...= K.....8]
 b5 14 df 46 a3 8f 6b 05 c3 54 4d a2 83 d4 b7 02      [...F..k..TM.....]
 88 2d 58 e7 a4 86 1c 48 77 68 49 66 a1 35 3e c4      [.-X....HwhIf.5>.]
 71 20 aa 18 9d 9f 1a 38 52 3c e3 35 b2 19 12 ad      [q .....8R<.5....]
 99 ad ce 68 8b b0 d0 29 ba 25 fd 1e e0 5d aa 12      [...h...).%...]..]
 9c 44 89 63 89 62 e3 cb f3 5d 5f a3 7c b7 b9 ef      [.D.c.b...]_.|...]
 01 89 5b 33 35 a8 81 60 38 61 4e d8 4f 6a 53 70      [..[35..`8aN.OjSp]
 35 02 03 01 00 01                                    [5.....]
  Certificate signature (256 bytes):
 67 f6 12 25 3f d4 d2 dd 6a f7 3e 55 b8 9f 33 53      [g..%?...j.>U..3S]
 20 4d d1 17 54 08 8a 70 22 35 92 59 9c 03 9c 0f      [ M..T..p"5.Y....]
 ce 46 3c 06 74 d0 a9 8e b1 88 a2 35 b3 eb 1b 00      [.F<.t......5....]
 5c 6d bb 1d b5 ad 17 19 f2 c6 96 87 9b e7 15 01      [\m.............]
 b2 04 af 7d 92 60 d9 ee ef bc 60 4e 2e af 84 e2      [...}.`....`N....]
 42 fe 07 71 7e fc ee ee f5 d1 6d 71 e7 46 f0 97      [B..q~.....mq.F..]
 e0 e8 b3 0e f9 07 e0 de 6e 36 5a 56 1e 80 10 05      [........n6ZV....]
 59 d9 88 ba f7 a3 d1 f6 cd 00 12 9f 90 f0 65 83      [Y............e.]
 e9 0f 76 a4 da eb 1b 1b 2d ea bd be a0 8a fb a7      [..v.....-.......]
 a5 18 ff 9f 5c e9 99 66 f0 d3 90 ae 49 3f c8 cc      [....\..f....I?..]
 32 6b db 64 da fd f5 42 ea bc f3 b0 8a 2f 17 d8      [2k.d...B...../..]
 cf c0 d8 d4 3a 41 ae 1d cf 7a c6 a6 a1 65 c2 94      [....:A...z...e..]
 8a ba ea d3 da 3e 8a 44 9b 47 35 10 ab 61 1b 4f      [.....>.D.G5..a.O]
 82 dd 59 16 d5 f2 1d f3 c2 08 cc 1c 7f ab be 9c      [..Y.............]
 be 52 73 ea e0 89 d7 6f 4d d0 d8 aa 3d 50 d6 b0      [.Rs....oM...=P..]
```

This table describes the significant fields shown in the display.

Table 18: show sam package Field Descriptions

Field	Description
Certificate Location	Location of the certificate; one of the following: **root**, **mem**, **disk0**, or **disk1**.
Certificate Index	Index number that the Software Authentication Manager (SAM) automatically assigns to the certificate.
Certificate Flag	One of the following: TRUSTED, VALIDATED, EXPIRED, or REVOKED.
Serial Number	Unique serial number of the certificate, assigned by its issuer.
Subject Name	Name of the entity for which the certificate is issued.
Issued By	Name of the entity that issued the certificate.
Version	ITU-T X.509 version of the certificate. The version can be 1 (X.509v1), 2 (X.509v2), or 3 (X.509v3).

Field	Description
Issuing Algorithm	Hash and public key algorithm that the issuer uses to sign the certificate.
Public Key	Subject public key for the certificate.
Certificate signature	Encrypted hash value (or signature) of the certificate. The hash value of the certificate is encrypted using the private key of the issuer.

Related Commands

Command	Description
show install	Displays the installed location and name of the software package. You can use the **all** keyword to display the active packages from all locations. For more information, see *System Management Command Reference for Cisco ASR 9000 Series Routers*.
show sam certificate, on page 400	Displays records in the SAM certificate table.

show sam sysinfo

To display current configuration settings for the Software Authentication Manager (SAM), use the **show sam sysinfo** command in EXEC mode.

show sam sysinfo

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **show sam sysinfo** command to determine the configuration settings of the SAM.

The display shows the status of the SAM, current prompt interval setting, and current prompt default response.

Task ID

Task ID	Operations
crypto	read

Examples

The following sample output is from the **show sam sysinfo** command:

```
RP/0/RSP0/CPU0:router# show sam sysinfo

Software Authentication Manager System Information
==================================================
Status                  : running
Prompt Interval         : 10 sec
Prompt Default Response : NO
```

This table describes the significant fields shown in the display.

Table 19: show sam sysinfo Field Descriptions

Field	Description
Status	One of the following: running or not running. If the SAM is not running, the System Manager should detect that state and attempt to restart the SAM. If problems prevent the System Manager from restarting the SAM after a predefined number of repeated attempts, the SAM will not be restarted. In such a case, you should contact Cisco Technical Assistance Center (TAC) personnel.
Prompt Interval	Current setting for the prompt interval. The interval can be set in the range from 0 to 300 seconds. The value shown in the sample output (10 seconds) is the default.

Field	Description
Prompt Default Response	Current setting that specifies the action taken by the SAM if the prompt interval expires before the user responds to the prompt. If the user does not respond to the prompt, the SAM waits for the specified interval to expire and then takes the action specified in the **sam prompt-interval** command (either **proceed** keyword or **terminate** keyword). Entering the **sam promptinterval** command with the **proceed** keyword causes the **show sam sysinfo** command to display "Yes," meaning that the default action taken by the SAM is to wait for the prompt interval to expire and then respond as if it had received a "yes" from the user. Entering the **sam promptinterval** command with the **terminate** keyword causes the **show sam sysinfo** command to display "No," meaning that the default action taken by the SAM is to wait for the prompt interval to expire and then respond as if it had received a "no" from the user.

Related Commands

Command	Description
sam prompt-interval, on page 396	Sets the interval that the SAM waits after prompting the user for input when it detects an abnormal condition and determines how the SAM responds when it does not receive user input within the specified interval.

Secure Shell Commands

This module describes the Cisco IOS XR software commands used to configure Secure Shell (SSH).

For detailed information about SSH concepts, configuration tasks, and examples, see the *Implementing Secure Shell on* the Cisco ASR 9000 Series Router Software configuration module in the *System Security Configuration Guide for Cisco ASR 9000 Series Routers.*

clear ssh

To terminate an incoming or outgoing Secure Shell (SSH) connection, use the **clear ssh** command in EXEC mode.

clear ssh {*session-id* | **outgoing** *session-id*}

Syntax Description

session-id	Session ID number of an incoming connection as displayed in the **show ssh** command output. Range is from 0 to 1024.
outgoing *session-id*	Specifies the session ID number of an outgoing connection as displayed in the **show ssh** command output. Range is from 1 to 10.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **clear ssh** command to disconnect incoming or outgoing SSH connections. Incoming connections are managed by the SSH server running on the local networking device. Outgoing connections are initiated from the local networking device.

To display the session ID for a connection, use the **show ssh** command.

Task ID

Task ID	Operations
crypto	execute

Examples

In the following example, the **show ssh** command is used to display all incoming and outgoing connections to the router. The **clear ssh** command is then used to terminate the incoming session with the ID number 0.

```
RP/0/RSP0/CPU0:router# show ssh

SSH version: Cisco-2.0
session     pty  location   state       userid     host        ver
-------------------------------------------------------------------
Incoming sessions
0           vty0 0/33/1  SESSION_OPEN   cisco   172.19.72.182   v2
1           vty1 0/33/1  SESSION_OPEN   cisco   172.18.0.5      v2
2           vty2 0/33/1  SESSION_OPEN   cisco   172.20.10.3     v1
3           vty3 0/33/1  SESSION_OPEN   cisco   3333::50        v2

Outgoing sessions
1               0/33/1  SESSION_OPEN    cisco   172.19.72.182   v2
2               0/33/1  SESSION_OPEN    cisco   3333::50        v2
```

```
RP/0/RSP0/CPU0:router# clear ssh 0
```

The following output is applicable for the **clear ssh** command starting IOS-XR 5.3.2 releases and later.

```
RP/0/RSP0/CPU0:router# show ssh
SSH version : Cisco-2.0

id  chan pty     location        state           userid    host                  ver
authentication connection type
-----------------------------------------------------------------------------------------------
Incoming sessions
0   1    vty0    0/RSP0/CPU0     SESSION_OPEN    lab       12.22.57.75           v2
rsa-pubkey     Command-Line-Interface
0   2    vty1    0/RSP0/CPU0     SESSION_OPEN    lab       12.22.57.75           v2
rsa-pubkey     Command-Line-Interface
0   3            0/RSP0/CPU0     SESSION_OPEN    cisco     12.22.57.75           v2
rsa-pubkey     Sftp-Subsystem
1       vty7    0/RSP0/CPU0     SESSION_OPEN    cisco     12.22.22.57          v1  password
       Command-Line-Interface
3   1           0/RSP0/CPU0     SESSION_OPEN    lab       12.22.57.75           v2  password
       Netconf-Subsystem
4   1    vty3    0/RSP0/CPU0     SESSION_OPEN    lab       192.168.1.55          v2  password
       Command-Line-Interface

Outgoing sessions
1               0/RSP0/CPU0     SESSION_OPEN    lab       192.168.1.51          v2  password

RP/0/RSP0/CPU0:router# clear ssh 0
```

Related Commands

Command	Description
show ssh, on page 431	Displays the incoming and outgoing connections to the router.

clear netconf-yang agent session

To clear the specified netconf agent session, use the **clear netconf-yang agent session** in EXEC mode.

clear netconf-yang agent session *session-id*

Syntax Description

session-id	The session-id which needs to be cleared.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 5.3.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

The **show netconf-yang clients** command can be used to get the required session-id(s).

Task ID

Task ID	Operation
config-services	read, write

Example

This example shows how to use the **clear netconf-yang agent session** command:

```
RP/0/RSP0/CPU0:router (config) #  clear netconf-yang agent session 32125
```

disable auth-methods

To selectively disable the authentication methods for the SSH server, use the **disable auth-methods** command in ssh server configuration mode. To remove the configuration, use the **no** form of this command.

disable auth-methods { **keyboard-interactive** | **password** | **public-key** }

Syntax Description

keyboard-interactive	Disables keyboard-interactive authentication method for the SSH server
password	Disables password authentication method for the SSH server
public-key	Disables publick-key authentication method for the SSH server

Command Default

Allows all the authentication methods, by default.

Command Modes

ssh server

Command History

Release	Modification
Release 7.8.1	This command was introduced.

Usage Guidelines

If this configuration is not present, you can consider that the SSH server on the router allows all the authentication methods.

The public-key authentication method includes certificate-based authentication as well.

Task ID

Task ID	Operation
crypto	read, write

This example shows how to disable the public-key authentication method for the SSH server on the router.

```
Router#configure
Router(config)# ssh server
Router(config-ssh)# disable auth-methods public-key
Router(config-ssh)# commit
```

netconf-yang agent ssh

To enable netconf agent over SSH (Secure Shell) , use the **netconf-yang agent ssh** command in Global Configuration mode. To disable netconf, use the **no** form of the command.

netconf-yang agent ssh

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 5.3.0	This command was introduced.

Usage Guidelines

SSH is currently the supported transport method for Netconf.

Task ID

Task ID	Operation
config-services	read, write

Example

This example shows how to use the **netconf-yang agent ssh** command:

```
RP/0/RSP0/CPU0:router (config) #  netconf-yang agent ssh
```

sftp

To start the secure FTP (SFTP) client, use the **sftp** command in EXEC mode.

sftp [*username* **@** *host* **:** *remote-filename*] *source-filename* *dest-filename* [**port** *port-num*] [**source-interface** *type* *interface-path-id*] [**vrf** *vrf-name*]

Syntax Description

username	(Optional) Name of the user performing the file transfer. The at symbol (@) following the username is required.
hostname:remote-filename	(Optional) Name of the Secure Shell File Transfer Protocol (SFTP) server. The colon (:) following the hostname is required.
source-filename	SFTP source, including the path.
dest-filename	SFTP destination, including the path.
port *port-num*	Specifies the non-default port number of the server to which the SFTP client on the router attempts a connection. The port number ranges from 1025 - 65535.
source-interface	(Optional) Specifies the source IP address of a selected interface for all outgoing SSH connections.
type	Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command in EXEC mode to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
vrf *vrf-name*	Specifies the name of the VRF associated with the source interface.

Command Default

If no *username* argument is provided, the login name on the router is used. If no *hostname* argument is provided, the file is considered local.

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.7.1	Modified the command to include the **port** option that specifies the non-default port for outbound connections.
Release 3.7.2	This command was introduced.

Usage Guidelines

SFTP provides for the secure (and authenticated) copying of files between a router and a remote host. Like the **copy** command, the **sftp** command can be invoked only in EXEC mode.

If a username is not provided, the login name on the router is used as the default. If a host name is not provided, the file is considered local.

If the source interface is specified in the **sftp** command, the **sftp** interface takes precedence over the interface specified in the **ssh client source-interface** command.

When the file destination is a local path, all of the source files should be on remote hosts, and vice versa.

When multiple source files exist, the destination should be a preexisting directory. Otherwise, the destination can be either a directory name or destination filename. The file source cannot be a directory name.

If you download files from different remote hosts, that is, the source points to different remote hosts, the SFTP client spawns SSH instances for each host, which may result in multiple prompts for user authentication.

If you have configured a non-default SSH server port on the router, then the SCP and SFTP services also use that SSH port for their connections. The **port** option to specify the non-default port number is available for the **ssh** command also.

The non-default SSH port number is supported only for SSHv2 and only on Cisco IOS XR SSH; not on CiscoSSH, the Open-SSH-based implementation of SSH. For more details, see *Non-default SSH Port* section in the *System Security Configuration Guide for Cisco ASR 9000 Series Routers*.

From Cisco IOS XR Software Release 7.10.1 and later, you can use public-key based user authentication for Cisco IOS XR routers configured as SSH clients as well. This feature thereby allows you to use password-less authentication for secure file transfer and copy operations using SFTP and SCP protocols.

Task ID

Task ID	Operations
crypto	execute
basic-services	execute

Examples

In the following example, user *abc* is downloading the file *ssh.diff* from the SFTP server *ena-view1* to *disk0:*

```
RP/0/RSP0/CPU0:router#sftp abc@ena-view1:ssh.diff disk0
```

In the following example, user *abc* is uploading multiple files from disk 0:/sam_* to /users/abc/ on a remote SFTP server called ena-view1:

```
RP/0/RSP0/CPU0:router# sftp disk0:/sam_* abc@ena-view1:/users/abc/
```

In the following example, user *admin* is downloading the file *run* from *disk0a:* to *disk0:/v6copy* on a local SFTP server using an IPv6 address:

```
RP/0/RSP0/CPU0:router#sftp admin@[2:2:2::2]:disk0a:/run disk0:/V6copy
Connecting to 2:2:2::2...
Password:

disk0a:/run
  Transferred 308413 Bytes
  308413 bytes copied in 0 sec (338172)bytes/sec
```

```
RP/0/RSP0/CPU0:router#dir disk0:/V6copy

Directory of disk0:

70144       -rwx  308413      Sun Oct 16 23:06:52 2011  V6copy

2102657024 bytes total (1537638400 bytes free)
```

In the following example, user *admin* is uploading the file *v6copy* from *disk0:* to *disk0a:/v6back* on a local SFTP server using an IPv6 address:

```
RP/0/RSP0/CPU0:router#sftp disk0:/V6copy admin@[2:2:2::2]:disk0a:/v6back
Connecting to 2:2:2::2...
Password:

/disk0:/V6copy
  Transferred 308413 Bytes
  308413 bytes copied in 0 sec (421329)bytes/sec

RP/0/RSP0/CPU0:router#dir disk0a:/v6back

Directory of disk0a:

66016       -rwx  308413      Sun Oct 16 23:07:28 2011  v6back

2102788096 bytes total (2098987008 bytes free)
```

In the following example, user *admin* is downloading the file *sampfile* from *disk0:* to *disk0a:/sampfile_v4* on a local SFTP server using an IPv4 address:

```
RP/0/RSP0/CPU0:router#sftp admin@2.2.2.2:disk0:/sampfile disk0a:/sampfile_v4
Connecting to 2.2.2.2...
Password:

disk0:/sampfile
  Transferred 986 Bytes
  986 bytes copied in 0 sec (493000)bytes/sec

RP/0/RSP0/CPU0:router#dir disk0a:/sampfile_v4

Directory of disk0a:

131520      -rwx  986         Tue Oct 18 05:37:00 2011  sampfile_v4

502710272 bytes total (502001664 bytes free)
```

In the following example, user *admin* is uploading the file *sampfile_v4* from *disk0a:* to *disk0:/sampfile_back* on a local SFTP server using an IPv4 address:

```
RP/0/RSP0/CPU0:router#sftp disk0a:/sampfile_v4 admin@2.2.2.2:disk0:/sampfile_back
Connecting to 2.2.2.2...
Password:

disk0a:/sampfile_v4
  Transferred 986 Bytes
  986 bytes copied in 0 sec (564000)bytes/sec

RP/0/RSP0/CPU0:router#dir disk0:/sampfile_back

Directory of disk0:
```

```
121765      -rwx  986         Tue Oct 18 05:39:00 2011  sampfile_back

524501272 bytes total (512507614 bytes free)
```

This example shows how to connect to the non-default port of a remote SFTP server and download a file to the local *disk0:* on the router.

```
RP/0/RSP0/CPU0:router#sftp user1@198.51.100.1:disk0:/test-file port 5525 disk0
```

Related Commands

Command	Description
ssh client source-interface, on page 452	Specifies the source IP address of a selected interface for all outgoing SSH connections.
ssh client vrf, on page 453	Configures a new VRF for use by the SSH client.

sftp (Interactive Mode)

To enable users to start the secure FTP (SFTP) client, use the **sftp** command in EXEC mode.

sftp [*username* **@** *host* **:** *remote-filenam* **e**] [**port** *port-num*] [**source-interface** *type interface-path-id*] [**vrf** *vrf-name*]

Syntax Description

username	(Optional) Name of the user performing the file transfer. The at symbol (@) following the username is required.
*hostname:remote-filenam*e	(Optional) Name of the Secure Shell File Transfer Protocol (SFTP) server. The colon (:) following the hostname is required.
port *port-num*	Specifies the non-default port number of the server to which the SFTP client on the router attempts a connection. The port number ranges from 1025 - 65535.
source-interface	(Optional) Specifies the source IP address of a selected interface for all outgoing SSH connections.
type	Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command in EXEC mode to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
vrf *vrf-name*	Specifies the name of the VRF associated with the source interface.

Command Default

If no *username* argument is provided, the login name on the router is used. If no *hostname* argument is provided, the file is considered local.

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.7.1	Modified the command to include the **port** option that specifies the non-default port for outbound connections.
Release 3.9.0	This command was introduced.

Usage Guidelines

The SFTP client, in the interactive mode, creates a secure SSH channel where the user can enter any supported command. When a user starts the SFTP client in an interactive mode, the SFTP client process creates a secure SSH channel and opens an editor where user can enter any supported command.

More than one request can be sent to the SFTP server to execute the commands. While there is no limit on the number of 'non-acknowledged' or outstanding requests to the server, the server might buffer or queue these requests for convenience. Therefore, there might be a logical sequence to the order of requests.

The following unix based commands are supported in the interactive mode:

- bye
- **cd** <*path*>
- **chmod** <*mode*> <*path*>
- exit
- **get** <*remote-path*> *[local-path]*
- help
- **ls** *[-alt] [path]*
- **mkdir <path>**
- **put** <*local-path*> *[remote-path]*
- pwd
- quit
- **rename <old-path> <new-path>**
- **rmdir <path>**
- **rm <path>**

The following commands are not supported:

- lcd, lls, lpwd, lumask, lmkdir
- ln, symlink
- chgrp, chown
- !, !command
- ?
- mget, mput

If you have configured a non-default SSH server port on the router, then the SCP and SFTP services also use that SSH port for their connections. The **port** option to specify the non-default port number is available for the **ssh** command also.

The non-default SSH port number is supported only for SSHv2 and only on Cisco IOS XR SSH; not on CiscoSSH, the Open-SSH-based implementation of SSH. For more details, see *Non-default SSH Port* section in the *System Security Configuration Guide for Cisco ASR 9000 Series Routers*.

From Cisco IOS XR Software Release 7.10.1 and later, you can use public-key based user authentication for Cisco IOS XR routers configured as SSH clients as well. This feature thereby allows you to use password-less authentication for secure file transfer and copy operations using SFTP and SCP protocols.

Task ID

Task ID	Operations
crypto	execute
basic-services	execute

Examples

In the following example, user *admin* is downloading and uploading a file from/to an external SFTP server using an IPv6 address:

```
RP/0/RSP0/CPU0:router#sftp admin@[2:2:2::2]

Connecting to 2:2:2::2...
Password:
sftp> pwd
Remote working directory: /
sftp> cd /auto/tftp-server1-users5/admin
sftp> get frmRouter /disk0:/frmRouterdownoad

/auto/tftp-server1-users5/admin/frmRouter
  Transferred 1578 Bytes
  1578 bytes copied in 0 sec (27684)bytes/sec
sftp> put /disk0:/frmRouterdownoad againtoServer

/disk0:/frmRouterdownoad
  Transferred 1578 Bytes
  1578 bytes copied in 0 sec (14747)bytes/sec
sftp>
```

In the following example, user *abc* is downloading and uploading a file from/to an external SFTP server using an IPv4 address:

```
RP/0/RSP0/CPU0:router#sftp abc@2.2.2.2
Connecting to 2.2.2.2...
Password:
sftp> pwd
Remote working directory: /
sftp> cd /auto/tftp-server1-users5/abc
sftp> get frmRouter /disk0:/frmRouterdownoad

/auto/tftp-server1-users5/abc/frmRouter
  Transferred 1578 Bytes
  1578 bytes copied in 0 sec (27684)bytes/sec
sftp> put /disk0:/frmRouterdownoad againtoServer

/disk0:/frmRouterdownoad
  Transferred 1578 Bytes
  1578 bytes copied in 0 sec (14747)bytes/sec
sftp>
```

Related Commands

Command	Description
ssh client source-interface, on page 452	Specifies the source IP address of a selected interface for all outgoing SSH connections.

Command	Description
ssh client vrf, on page 453	Configures a new VRF for use by the SSH client.

show netconf-yang clients

To display the client details for netconf-yang, use the **show netconf-yang clients** command in EXEC mode.

show netconf-yang clients

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 5.3.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
config-services	read

Example

This example shows how to use the **show netconf-yang clients** command:

```
RP/0/RSP0/CPU0:router (config) #  sh netconf-yang clients
Netconf clients
client session ID|   NC version|    client connect time|        last OP time|        last
OP type|    <lock>|
 22969|                     1.1|          0d  0h  0m  2s|            11:11:24|
close-session|        No|
 15389|                     1.1|          0d  0h  0m  1s|            11:11:25|
get-config|        No|
```

Table 20: Field descriptions

Field name	Description
Client session ID	Assigned session identifier
NC version	Version of the Netconf client as advertised in the hello message
Client connection time	Time elapsed since the client was connected
Last OP time	Last operation time
Last OP type	Last operation type
Lock (yes or no)	To check if the session holds a lock on the configuration datastore

show netconf-yang statistics

To display the statistical details for netconf-yang, use the **show netconf-yang statistics** command in EXEC mode.

show netconf-yang statistics

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 5.3.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
config-services	read

Example

This example shows how to use the **show netconf-yang statistics** command:

```
RP/0/RSP0/CPU0:router (config) #  sh netconf-yang statistics
Summary statistics
                          # requests|             total time|   min time per request|   max
 time per request|   avg time per request|
other                              0|       0h  0m  0s   0ms|       0h  0m  0s   0ms|
 0h  0m  0s   0ms|       0h  0m  0s   0ms|
close-session                      4|       0h  0m  0s   3ms|       0h  0m  0s   0ms|
 0h  0m  0s   1ms|       0h  0m  0s   0ms|
kill-session                       0|       0h  0m  0s   0ms|       0h  0m  0s   0ms|
 0h  0m  0s   0ms|       0h  0m  0s   0ms|
get-schema                         0|       0h  0m  0s   0ms|       0h  0m  0s   0ms|
 0h  0m  0s   0ms|       0h  0m  0s   0ms|
get                                0|       0h  0m  0s   0ms|       0h  0m  0s   0ms|
 0h  0m  0s   0ms|       0h  0m  0s   0ms|
get-config                         1|       0h  0m  0s   1ms|       0h  0m  0s   1ms|
 0h  0m  0s   1ms|       0h  0m  0s   1ms|
edit-config                        3|       0h  0m  0s   2ms|       0h  0m  0s   0ms|
 0h  0m  0s   1ms|       0h  0m  0s   0ms|
commit                             0|       0h  0m  0s   0ms|       0h  0m  0s   0ms|
 0h  0m  0s   0ms|       0h  0m  0s   0ms|
cancel-commit                      0|       0h  0m  0s   0ms|       0h  0m  0s   0ms|
 0h  0m  0s   0ms|       0h  0m  0s   0ms|
lock                               0|       0h  0m  0s   0ms|       0h  0m  0s   0ms|
 0h  0m  0s   0ms|       0h  0m  0s   0ms|
unlock                             0|       0h  0m  0s   0ms|       0h  0m  0s   0ms|
 0h  0m  0s   0ms|       0h  0m  0s   0ms|
```

```
discard-changes                      0|       0h  0m  0s   0ms|       0h  0m  0s   0ms|
 0h  0m  0s   0ms|       0h  0m  0s   0ms|
validate                             0|       0h  0m  0s   0ms|       0h  0m  0s   0ms|
 0h  0m  0s   0ms|       0h  0m  0s   0ms|
xml parse                            8|       0h  0m  0s   4ms|       0h  0m  0s   0ms|
 0h  0m  0s   1ms|       0h  0m  0s   0ms|
netconf processor                    8|       0h  0m  0s   6ms|       0h  0m  0s   0ms|
 0h  0m  0s   1ms|       0h  0m  0s   0ms|
```

Table 21: Field descriptions

Field name	Description
Requests	Total number of processed requests of a given type
Total time	Total processing time of all requests of a given type
Min time per request	Minimum processing time for a request of a given type
Max time per request	Maximum processing time for a request of a given type
Avg time per request	Average processing time for a request type

show ssh

To display all incoming and outgoing connections to the router, use the **show ssh** command in EXEC mode.

show ssh

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 5.3.2	The command output was enhanced to reflect multichannel and subsystem support for ssh.

Usage Guidelines

Use the **show ssh** command to display all incoming and outgoing Secure Shell (SSH) Version 1 (SSHv1) and SSH Version 2 (SSHv2) connections.

The connection type field in the command output of **show ssh** command shows as **port-forwarded local** for SSH port-forwarded sessions.

Use the **show ssh server** command to see the details of the SSH server. The **Port Forwarding** column shows as **local** for the port-forwarded session. Whereas, for a regular SSH session, the field displays as **disabled**.

Task ID

Task ID	Operations
crypto	read

Examples

This is sample output from the **show ssh** command when SSH is enabled:

```
RP/0/RSP0/CPU0:router# show ssh

SSH version : Cisco-2.0

id  pty   location    state         userid    host          ver       authentication
-------------------------------------------------------------------------------------------------
Incoming sessions

Outgoing sessions
1         0/3/CPU0    SESSION_OPEN    lab     12.22.57.     v2        password
2         0/3/CPU0    SESSION_OPEN    lab     12.22.57.75   v2        keyboard-interactive
```

The following output is applicable for the **show ssh** command starting IOS-XR 5.3.2 releases and later.

```
RP/0/RSP0/CPU0:router# show ssh
SSH version : Cisco-2.0


id  chan pty     location        state           userid    host                  ver
authentication connection type
-----------------------------------------------------------------------------------------------
Incoming sessions
0   1    vty0    0/RSP0/CPU0     SESSION_OPEN    lab       12.22.57.75           v2
rsa-pubkey     Command-Line-Interface
0   2    vty1    0/RSP0/CPU0     SESSION_OPEN    lab       12.22.57.75           v2
rsa-pubkey     Command-Line-Interface
0   3            0/RSP0/CPU0     SESSION_OPEN    cisco     12.22.57.75           v2
rsa-pubkey     Sftp-Subsystem
1       vty7    0/RSP0/CPU0     SESSION_OPEN    cisco     12.22.22.57          v1  password
       Command-Line-Interface
3   1           0/RSP0/CPU0     SESSION_OPEN    lab       12.22.57.75           v2  password
       Netconf-Subsystem
4   1    vty3    0/RSP0/CPU0     SESSION_OPEN    lab       192.168.1.55          v2  password
       Command-Line-Interface

Outgoing sessions
1               0/RSP0/CPU0     SESSION_OPEN    lab       192.168.1.51          v2  password
```

This table describes significant fields shown in the display.

Table 22: show ssh Field Descriptions

Field	Description
id	Session identifier for the incoming and outgoing SSH connections.
chan	Channel identifier for incoming (v2) SSH connections. NULL for SSH v1 sessions.
pty	pty-id allocated for the incoming session. Null for outgoing SSH connection.
location	Specifies the location of the SSH server for an incoming connection. For an outgoing connection, location specifies from which route processor the SSH session is initiated.
state	The SSH state that the connection is currently in.
userid	Authentication, authorization and accounting (AAA) username used to connect to or from the router.
host	IP address of the remote peer.
ver	Specifies if the connection type is SSHv1 or SSHv2.
authentication	Specifies the type of authentication method chosen by the user.
connection type	Specifies which application is performed over this connection (Command-Line-Interface, Remote-Command, Scp, Sftp-Subsystem, or Netconf-Subsystem)

The following is a sample output of SSH port-forwarded session:

```
Router#show ssh

Wed Oct 14 11:22:05.575 UTC
```

```
SSH version : Cisco-2.0

id chan pty location   state        userid host          ver authentication connection type
-----------------------------------------------------------------------------------------------
Incoming sessions
15 1    XXX 0/RP0/CPU0 SESSION_OPEN admin  192.168.122.1 v2  password
port-forwarded-local

Outgoing sessions

Router#
```

The following is a sample output of **show ssh server** command with SSH port forwarding enabled:

```
Router#show ssh server
Tue Sep  7 17:43:22.483 IST
---------------------
SSH Server Parameters
---------------------

Current supported versions := v2
                 SSH port := 22
                 SSH vrfs := vrfname:=default(v4-acl:=, v6-acl:=)
             Netconf Port := 830
             Netconf Vrfs := vrfname:=default(v4-acl:=, v6-acl:=)

 Algorithms
---------------
        Hostkey Algorithms :=
x509v3-ssh-rsa,ecdsa-sha2-nistp521,ecdsa-sha2-nistp384,ecdsa-sha2-nistp256,rsa-sha2-512,rsa-sha2-256,ssh-rsa,ssh-dsa,ssh-ed25519

   Key-Exchange Algorithms :=
ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group14-sha1
     Encryption Algorithms :=
aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com
            Mac Algorithms := hmac-sha2-512,hmac-sha2-256,hmac-sha1

 Authentication Method Supported
------------------------------------
                PublicKey := Yes
                 Password := Yes
      Keyboard-Interactive := Yes
         Certificate Based := Yes

 Others
------------
                     DSCP  := 0
                Ratelimit  := 600
             Sessionlimit  := 110
                Rekeytime  := 30
       Server rekeyvolume  := 1024
  TCP window scale factor  := 1
            Backup Server  := Disabled
          Host Trustpoint  :=
          User Trustpoint  := tes,test,x509user
          Port Forwarding  := local
Max Authentication Limit  := 16
     Certificate username  := Common name(CN) User principle name(UPN)
Router#
```

Related Commands

Command	Description
show sessions	Displays information about open Telnet or rlogin connections. For more information, see the *System Management Command Reference for Cisco ASR 9000 Series Routers*
show ssh session details, on page 440	Displays the details for all the incoming and outgoing SSHv2 connections, to the router.

show ssh history

To display the last hundred SSH connections that were terminated, use the **show ssh history** command in EXEC mode.

show ssh history

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.4.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
crypto	read

Examples

The following is sample output from the **show ssh history** command to display the last hundred SSH sessions that were teminated:

```
RP/0/RSP0/CPU0:router# show ssh history

SSH version : Cisco-2.0

id       chan pty     location        userid    host                  ver authentication
connection type
-----------------------------------------------------------------------------------------------------
Incoming sessions
1        1    XXXXX   0/RP0/CPU0      root      10.105.227.252        v2  password
Netconf-Subsystem
2        1    XXXXX   0/RP0/CPU0      root      10.105.227.252        v2  password
Netconf-Subsystem
3        1    XXXXX   0/RP0/CPU0      root      10.105.227.252        v2  password
Netconf-Subsystem
4        1    XXXXX   0/RP0/CPU0      root      10.105.227.252        v2  password
Netconf-Subsystem
5        1    XXXXX   0/RP0/CPU0      root      10.105.227.252        v2  password
Netconf-Subsystem
6        1    XXXXX   0/RP0/CPU0      root      10.105.227.252        v2  password
Netconf-Subsystem
7        1    XXXXX   0/RP0/CPU0      root      10.105.227.252        v2  password
Netconf-Subsystem
8        1    XXXXX   0/RP0/CPU0      root      10.105.227.252        v2  password
Netconf-Subsystem
```

```
9        1     vty0     0/RP0/CPU0       root       10.196.98.106          v2  key-intr
Command-Line-Interface
```

Pty – VTY number used. This is represented as ‘XXXX’ when connection type is SFTP, SCP or Netconf.

show ssh history details

To display the last hundred SSH connections that were terminated, and also the start and end time of the session, use the **show ssh history details** command in EXEC mode.

show ssh history details

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.4.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
crypto	read

Examples

The following is sample output from the **show ssh history details** command to display the last hundred SSH sessions that were teminated along with the start and end time of the sessions:

```
RP/0/RSP0/CPU0:router# show ssh history details

SSH version : Cisco-2.0

id      key-exchange           pubkey               incipher    outcipher   inmac
outmac          start_time              end_time
------------------------------------------------------------------------------------------

Incoming Session
1       ecdh-sha2-nistp256     ssh-rsa              aes128-ctr  aes128-ctr  hmac-sha2-256
hmac-sha2-256   14-02-18 14:00:39       14-02-18 14:00:41
2       ecdh-sha2-nistp256     ssh-rsa              aes128-ctr  aes128-ctr  hmac-sha2-256
hmac-sha2-256   14-02-18 16:21:54       14-02-18 16:21:55
3       ecdh-sha2-nistp256     ssh-rsa              aes128-ctr  aes128-ctr  hmac-sha2-256
hmac-sha2-256   14-02-18 16:22:18       14-02-18 16:22:19
4       ecdh-sha2-nistp256     ssh-rsa              aes128-ctr  aes128-ctr  hmac-sha2-256
hmac-sha2-256   15-02-18 12:17:44       15-02-18 12:17:46
5       ecdh-sha2-nistp256     ssh-rsa              aes128-ctr  aes128-ctr  hmac-sha2-256
hmac-sha2-256   15-02-18 12:18:16       15-02-18 12:18:17
6       ecdh-sha2-nistp256     ssh-rsa              aes128-ctr  aes128-ctr  hmac-sha2-256
hmac-sha2-256   15-02-18 14:44:08       15-02-18 14:44:09
7       ecdh-sha2-nistp256     ssh-rsa              aes128-ctr  aes128-ctr  hmac-sha2-256
hmac-sha2-256   15-02-18 14:50:15       15-02-18 14:50:16
8       ecdh-sha2-nistp256     ssh-rsa              aes128-ctr  aes128-ctr  hmac-sha2-256
```

```
hmac-sha2-256   15-02-18 14:50:52       15-02-18 14:50:53
9       ecdh-sha2-nistp256     ssh-rsa             aes128-ctr  aes128-ctr  hmac-sha2-256
hmac-sha2-256   15-02-18 15:31:26       15-02-18 15:31:38
```

This table describes the significant fields shown in the display.

Table 23: Field Descriptions

Field	Description
session	Session identifier for the incoming and outgoing SSH connections.
key-exchange	Key exchange algorithm chosen by both peers to authenticate each other.
pubkey	Public key algorithm chosen for key exchange.
incipher	Encryption cipher chosen for the receiver traffic.
outcipher	Encryption cipher chosen for the transmitter traffic.
inmac	Authentication (message digest) algorithm chosen for the receiver traffic.
outmac	Authentication (message digest) algorithm chosen for the transmitter traffic.
start_time	Start time of the session.
end_time	End time of the session.

show ssh rekey

To display session rekey details such as session id, session rekey count, time to rekey, data to rekey, use the **show ssh rekey** command in EXEC mode.

show ssh rekey

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.2.1	This command was introduced.

Usage Guidelines

The ssh rekey data is updated ten times between two consecutive rekeys.

Task ID

Task ID	Operations
crypto	read

Examples

The following sample output is from the **show ssh rekey** command:

```
 # show ssh rekey

id    RekeyCount   TimeToRekey(min)     VolumeToRekey(MB)
-------------------------------------------------------------
Incoming Session
0        8               59.5             1024.0
```

This table describes the fields shown in the display.

Table 24: show ssh rekey Field Descriptions

Field	Description
Rekey Count	Number of times the ssh rekey is generated.
TimeToRekey	Time remaining (in minutes) before the ssh rekey is regenerated based on the value set using the **ssh server rekey-time** command.
VolumeToRekey	Volume remaining (in megabytes) before the ssh rekey is regenerated based on the value set using the **ssh server rekey-volume** command.

show ssh session details

To display the details for all incoming and outgoing Secure Shell Version 2 (SSHv2) connections, use the **show ssh session details** command in EXEC mode.

show ssh session details

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **show ssh session details** command to display a detailed report of the SSHv2 connections to or from the router, including the cipher chosen for the specific session.

Task ID

Task ID	Operations
crypto	read

Examples

The following is sample output from the **show ssh session details** command to display the details for all the incoming and outgoing SSHv2 connections:

```
RP/0/RSP0/CPU0:router# show ssh session details

id  key-exchange               pubkey    incipher   outcipher   inmac      outmac

------------------------------------------------------------------------------
Incoming Session
0  diffie-hellman-group14    ssh-rsa   aes128-ctr   aes128-ctr  hmac-sha1  hmac-sha1
1  ecdh-sha2-nistp521       ssh-rsa   aes256-ctr   aes256-ctr  hmac-sha2-512  hmac-sha2-512
```

This table describes the significant fields shown in the display.

Table 25: show ssh session details Field Descriptions

Field	Description
session	Session identifier for the incoming and outgoing SSH connections.
key-exchange	Key exchange algorithm chosen by both peers to authenticate each other.
pubkey	Public key algorithm chosen for key exchange.

Field	Description
incipher	Encryption cipher chosen for the Rx traffic.
outcipher	Encryption cipher chosen for the Tx traffic.
inmac	Authentication (message digest) algorithm chosen for the Rx traffic.
outmac	Authentication (message digest) algorithm chosen for the Tx traffic.

Related Commands

Command	Description
show sessions	Displays information about open Telnet or rlogin connections.
show ssh, on page 431	Displays all the incoming and outgoing connections to the router.

show tech-support ssh

To automatically run show commands that display system information, use the show tech-support command, use the **show tech-support ssh** command in EXEC mode.

show tech-support ssh

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.4.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
crypto	read

Examples

The following is sample output from the **show tech-support ssh** command:

```
RP/0/RSP0/CPU0:router# show tech-support ssh
++ Show tech start time: 2018-Feb-20.123016.IST ++
Tue Feb 20 12:30:27 IST 2018 Waiting for gathering to complete
.............................
Tue Feb 20 12:32:35 IST 2018 Compressing show tech output
Show tech output available at 0/RP0/CPU0 :
/harddisk:/showtech/showtech-ssh-2018-Feb-20.123016.IST.tgz
++ Show tech end time: 2018-Feb-20.123236.IST ++
RP/0/RP0/CPU0:turin-sec1#
```

The **show tech-support ssh** command collects the output of these CLI:

Command	Description
show logging	Displays the contents of the logging buffer.
show context location all	
show running-config	Displays the contents of the currently running configuration or a subset of that configuration.
show ip int brief	Displays brief information about each interface.

Command	Description
show ssh	Displays all incoming and outgoing connections to the router.
show ssh session details	Displays the details for all the incoming and outgoing SSHv2 connections, to the router.
show ssh rekey	Displays session rekey details such as session id, session rekey count, time to rekey, data to rekey.
show ssh history	Displays the last hundred SSH connections that were terminated.
show tty trace info all all	
show tty trace error all all	

ssh

To start the Secure Shell (SSH) client connection and enable an outbound connection to an SSH server, use the **ssh** command in EXEC mode.

ssh [**vrf** **vrf-name**] { *ipv4-address* [**port** *port-num*] | *ipv6-address* [**port** *port-num*] | *hostname* [**port** *port-num*] } [**username** *user-id*] [**cipher aes** { **128-ctr** | **192-ctr** | **256-ctr** | **128-gcm** | **256-gcm** }] [**source-interface** *type* *interface-path-id*] [**command** *command-name*]

Syntax Description

ipv4-address	IPv4 address in A:B:C:D format.
ipv6-address	IPv6 address in X:X::X format.
hostname	Hostname of the remote node. If the hostname has both IPv4 and IPv6 addresses, the IPv6 address is used.
port *port-num*	Specifies the non-default SSH port number of the remote SSH server to which the SSH client on the router attempts a connection. The port number ranges from 1025 - 65535.
username*user-id*	(Optional) Specifies the username to use when logging in on the remote networking device running the SSH server. If no user ID is specified, the default is the current user ID.
cipher aes	SSHv2 supports only AES (protocol supports only ciphers greater than or equal to 128 bits)
source interface	(Optional) Specifies the source IP address of a selected interface for all outgoing SSH connections.
type	Interface type. For more information, use the question mark (**?**)online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the**showinterfaces** command in EXEC mode to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark(**?**)online help function.
command	(Optional) Specifies a remote command. Adding this keyword prompts the SSHv2 server to parse and execute the**ssh**command in non-interactive mode instead of initiating the interactive session.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Release	Modification
Release 3.9.1	Support for the **command** keyword was added.
Release 6.2.1	Cipher suite SSHv2 supports only AES (protocol supports only ciphers greater than or equal to 128 bits)
Release 7.7.1	Modified the command to include the **port** option that specifies the non-default port for outbound SSH connections.

Usage Guidelines

Use the **ssh** command to make an outbound client connection. The SSH client tries to make an SSHv2 connection to the remote peer. If the remote peer supports only the SSHv1 server, it internally spawns an SSHv1 connection to the remote server. The process of the remote peer version detection and spawning the appropriate client connection is transparent to the user.

If the **source-interface** keyword is specified in the **ssh** command, the **ssh** interface takes precedence over the interface specified in the **ssh client source-interface** ssh client source-interface, on page 452command.

Use the **command** keyword to enable the SSHv2 server to parse and execute the **ssh** command in non-interactive mode instead of initiating an interactive session.

The non-default SSH port number is supported only for SSHv2 and only on Cisco IOS XR SSH; not on CiscoSSH, the Open-SSH-based implementation of SSH. For more details, see *Non-default SSH Port* section in the *System Security Configuration Guide for Cisco ASR 9000 Series Routers*.

If you have configured a non-default SSH server port on the router, then the SCP and SFTP services also use that SSH port for their connections. The **port** option to specify the non-default port number is available for the **scp** and **sftp** commands also.

Task ID

Task ID	Operations
crypto	execute
basic-services	execute

Examples

The following sample output is from the **ssh** command to enable an outbound SSH client connection:

```
RP/0/RSP0/CPU0:router# ssh remote-host   username userabc

Password:
Remote-host>
```

This examples shows how to initiate an outbound SSH client connection to an SSH server which uses a port number other than the standard default port, 22. Here, the SSH server listens on port 5525 for client connections:

```
Router#ssh 198.51.100.1 port 5525 username user1
```

Related Commands

Command	Description
show ssh, on page 431	Displays all the incoming and outgoing connections to the router.

ssh algorithms cipher

To configure the list of supported SSH algorithms on the client or on the server, use the **ssh client algorithms cipher** command or **ssh server algorithms cipher** command in Global Configuration mode. To remove the configuration, use the **no** form of this command.

ssh {**client** | **server**} **algorithms cipher** {**aes256-cbc** | **aes256-ctr** | **aes192-ctr** | **aes192-cbc** | **aes128-ctr** | **aes128-cbc** | **aes128-gcm@openssh.com** | **aes256-gcm@openssh.com** | **3des-cbc**}

Syntax Description

client	Configures the list of supported SSH algorithms on the client.
server	Configures the list of supported SSH algorithms on the server.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
crypto	read, write

This example shows how to enable CTR cipher on the client and CBC cipher on the server:

```
Router1#ssh client algorithms cipher aes128-ctr aes192-ctr aes256-ctr

Router1#ssh server algorithms cipher aes128-cbc aes192-cbc aes256-cbc 3des-cbc
```

Related Commands

Command	Description
ssh client enable cipher , on page 449	Enables CBC mode ciphers on the SSH client.
ssh server enable cipher, on page 460	Enables CBC mode ciphers on the SSH server.

ssh client auth-method

To set the preferred order of SSH client authentication methods to be negotiated with the SSH server while establishing SSH sessions, use the **ssh client auth-method** command in the Global Configuration mode. To revert to the default order of SSH client authentication methods, use the **no** form of this command.

```
ssh client auth-method list-of-auth-method
```

Syntax Description

list-of-auth-method	Specifies the list of SSH client authentication methods in the respective order. The available options are: • **keyboard-interactive** • **password** • **public-key**

Command Default

None

Command Modes

Global Configuration

Command History

Release	Modification
Release 7.9.2/Release 7.10.1	This command was introduced.

Usage Guidelines

The default order of SSH client authentication methods on Cisco IOS XR routers is as follows:

- On routers running Cisco IOS XR SSH:
  - **public-key**, **password** and **keyboard-interactive** (prior to Cisco IOS XR Software Release 24.1.1)
  - **public-key**, **keyboard-interactive** and **password** (from Cisco IOS XR Software Release 24.1.1 and later)
- On routers running CiscoSSH (open source-based SSH):
  - **public-key**, **keyboard-interactive** and **password**

Task ID

Task ID	Operation
crypto	read, write

This example shows how to set the order of SSH client authentication methods in such a way that public key authentication is negotiated first, followed by keyboard-interactive, and then password-based authentication.

```
Router#configure
Router(config)#ssh client auth-method public-key keyboard-interactive password
Router(config-ssh)#commit
```

ssh client enable cipher

To enable the CBC mode ciphers 3DES-CBC and/or AES-CBC for an SSH client connection, use the **ssh client enable cipher** command in Global Configuration mode. To disable the ciphers, use the **no** form of this command.

ssh client enable cipher {**aes-cbc** | **3des-cbc**}

Syntax Description

3des-cbc	Specifies that the 3DES-CBC cipher be enabled for the SSH client connection.
aes-cbc	Specifies that the AES-CBC cipher be enabled for the SSH client connection.

Command Default

CBC mode ciphers are disabled.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

The support for CBC ciphers were disabled by default, from Cisco IOS XR Software Release 6.1.2. Hence, **ssh client enable cipher** and **ssh server enable cipher** commands were introduced to explicitly enable CBC ciphers in required scenarios.

If a client tries to reach the router which acts as a server with CBC cipher, and if the CBC cipher is not explicitly enabled on that router, then the system displays an error message:

```
ssh root@x.x.x. -c aes128-cbc
Unable to negotiate with x.x.x.x port 22: no matching cipher found.
Their offer: aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com
```

You must configure **ssh server enable cipher aes-cbc** command in this case, to connect to the router using the CBC cipher.

Task ID

Task ID	Operation
crypto	read, write

Examples

The following example shows how to enable the 3DES-CBC and AES-CBC ciphers for an SSH client connection:

```
Router# configure
```

```
Router(config)# ssh client enable cipher aes-cbc 3des-cbc
Router(config)# commit
```

Related Commands

Command	Description
ssh server enable cipher, on page 460	Enables CBC mode ciphers on the SSH server.

ssh client knownhost

To authenticate a server public key (pubkey), use the **ssh client knownhost** command in Global Configuration mode. To disable authentication of a server pubkey, use the **no** form of this command.

ssh client knownhost device : / filename

Syntax Description

device:/*filename*	Complete path of the filename (for example, slot0:/server_pubkey). The colon (:) and slash (/) are required.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

The *server pubkey* is a cryptographic system that uses two keys at the client end—a public key known to everyone and a private, or secret, key known only to the owner of the keys. In the absence of certificates, the server pubkey is transported to the client through an out-of-band secure channel. The client stores this pubkey in its local database and compares this key against the key supplied by the server during the early stage of key negotiation for a session-building handshake. If the key is not matched or no key is found in the local database of the client, users are prompted to either accept or reject the session.

The operative assumption is that the first time the server pubkey is retrieved through an out-of-band secure channel, it is stored in the local database. This process is identical to the current model adapted by Secure Shell (SSH) implementations in the UNIX environment.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following sample output is from the **ssh client knownhost** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh client knownhost disk0:/ssh.knownhost
RP/0/RSP0/CPU0:router(config)# commit
RP/0/RSP0/CPU0:router# ssh host1 username user1234
Host key not found from the list of known hosts.
Are you sure you want to continue connecting (yes/no)? yes
Password:
RP/0/RSP0/CPU0:host1# exit
RP/0/RSP0/CPU0:router# ssh host1 username user1234
```

ssh client source-interface

To specify the source IP address of a selected interface for all outgoing Secure Shell (SSH) connections, use the **ssh client source-interface** command in Global Configuration mode. To disable use of the specified interface IP address, use the **no** form of this command.

ssh client source-interface *type interface-path-id*

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

No source interface is used.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **ssh client source-interface** command to set the IP address of the specified interface for all outgoing SSH connections. If this command is not configured, TCP chooses the source IP address when the socket is connected, based on the outgoing interface used—which in turn is based on the route required to reach the server. This command applies to outbound shell over SSH as well as Secure Shell File Transfer Protocol (SFTP) sessions, which use the ssh client as a transport.

The source-interface configuration affects connections only to the remote host in the same address family. The system database (Sysdb) verifies that the interface specified in the command has a corresponding IP address (in the same family) configured.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to set the IP address of the Management Ethernet interface for all outgoing SSH connections:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh client source-interface MgmtEth 0/RSP0/CPU0/0
```

ssh client vrf

To configure a new VRF for use by the SSH client, use the **ssh client vrf** command in Global Configuration mode. To remove the specified VRF, use the **no** form of this command.

ssh client vrf *vrf-name*

Syntax Description

vrf-name	Specifies the name of the VRF to be used by the SSH client.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.8.0	This command was introduced.

Usage Guidelines

An SSH client can have only one VRF.

If a specific VRF is not configured for the SSH client, the default VRF is assumed when applying other SSH client-related commands, such as ssh client knownhost, on page 451 or ssh client source-interface, on page 452.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows the SSH client being configured to start with the specified VRF:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh client vrf green
```

Related Commands

Command	Description
ssh client dscp <value from 0 - 63>	SSH Client supports setting DSCP value in the outgoing packets. If not configured, the default DSCP value set in packets is 16 (for both client and server).

ssh server

To bring up the Secure Shell (SSH) server and to configure one or more VRFs for its use, use the **ssh server** command in Global Configuration mode. To stop the SSH server from receiving any further connections for the specified VRF, use the **no** form of this command. Optionally ACLs for IPv4 and IPv6 can be used to restrict access to the server before the port is opened.

ssh server vrf *vrf-name* [**ipv4 access-list** *ipv4 access list name*] [**ipv6 access-list** *ipv6 access list name*]]
ssh server v2

Syntax Description

vrf *vrf-name*	Specifies the name of the VRF to be used by the SSH server. The maximum VRF length is 32 characters. **Note** If no VRF is specified, the default VRF is assumed.
ipv4 access-list *access list namr*	Configures an IPv4 access-list for access restrictions to the ssh server.
ipv6 access-list *access list name*	Configures an IPv6 access-list for access restrictions to the ssh server
v2	Forces the SSH server version to be of only version 2.

Command Default

The default SSH server version is 2 (SSHv2), which falls back to 1 (SSHv1) if the incoming SSH client connection is set to SSHv1.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 3.8.0	The **vrf** keyword was supported.
Release 4.0	The ipv4 / ipv6 access-list keywords are supported.

Usage Guidelines

An SSH server must be configured at minimum for one VRF. If you delete all configured VRFs, including the default, the SSH server process stops. If you do not configure a specific VRF for the SSH client when applying other commands, such as **ssh client knownhost** or **ssh client source-interface,** the default VRF is assumed.

The SSH server listens for an incoming client connection on port 22. This server handles both Secure Shell Version 1 (SSHv1) and SSHv2 incoming client connections for both IPv4 and IPv6 address families. To accept only Secure Shell Version 2 connections, use the ssh server v2, on page 471 command.

To verify that the SSH server is up and running, use the **show process sshd** command.

Task ID

Task ID	Operations
crypto	read, write

Examples

In the following example, the SSH server is brought up to receive connections for VRF “green”:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh server
```

Examples

In the following example, the SSH server is configured to use IPv4 ACLs:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh servervrf vrf nameipv4 access-list access list name
```

Related Commands

Command	Description
show processes	Displays information about the SSH server. For more information, see the *System Management Command Reference for Cisco ASR 9000 Series Routers*.
ssh server v2, on page 471	Forces the SSH server version to be only 2 (SSHv2).
ssh server dscp <value from 0 - 63>	SSH server supports setting DSCP value in the outgoing packets. If not configured, the default DSCP value set in packets is 16 (for both client and server).

ssh server algorithms host-key

To configure the allowed SSH host-key pair algorithms from the list of auto-generated host-key pairs on the SSH server, use the **ssh server algorithms host-key** command in Global Configuration mode. To remove the configuration, use the **no** form of this command.

ssh server algorithms host-key { **dsa** | **ecdsa-nistp256** | **ecdsa-nistp384** | **ecdsa-nistp521** | **ed25519** | **rsa** | **x509v3-ssh-rsa** }

Syntax Description

• **dsa** • **ecdsa-nistp256** • **ecdsa-nistp384** • **ecdsa-nistp521** • **ed25519** • **rsa** • **x509v3-ssh-rsa**	Selects the specified host keys to be offered to the SSH client. While configuring this, you can specify the algorithms in any order.

Command Default

In the absence of this configuration, the SSH server considers that it can send all the available algorithms to the user as host key algorithm, based on the availability of the key or the certificate.

Command Modes

Global Configuration mode

Usage Guidelines

This configuration is optional. If this configuration is not present, it is considered that all the SSH host-key pairs are configured. In that case, the SSH client is allowed to connect to the SSH sever with any of the host-key pairs.

You can also use the **crypto key zeroize** command to remove the SSH host keys that are not required.

With the introduction of the automatic generation of SSH host-key pairs, the **show crypto key mypubkey** command output displays key information of all the keys that are auto-generated. Before its introduction, the output of this command displayed key information of only those host-key pairs that were explicitly configured using the **crypto key generate** command.

Task ID

Task ID	Operation
crypto	read, write

This example shows how to select the **ecdsa** algorithm from the list of auto-generated host-key pairs on the SSH server:

```
Router(config)#ssh server algorithms host-key ecdsa-nistp521
```

Similarly, this example shows how to select the **ed25519** algorithm:

```
Router(config)#ssh server algorithms host-key ed25519
```

Similarly, this example shows how to select the **x509v3-ssh-rsa** algorithm:

```
Router(config)#ssh server algorithms host-key x509v3-ssh-rsa
```

ssh server certificate

To configure the certificate-related parameters of SSH server, use the **ssh server certificate** command in Global Configuration mode. To remove the configuration, use the **no** form of this command.

ssh server certificate username { **common-name** | **user-principle-name** }

Syntax Description

username	Specifies which field in the certificate to be used as the username.
common-name	Configures the user common name (CN) from the subject name field.
user-principle-name	Configures the user principle name (UPN) from subject alternate name.

Command Default

In the absence of this configuration, the SSH server considers common name (CN) as the username.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 7.3.1	This command was introduced.

Usage Guidelines

The user name must match the user name provided in the CLI.

Task ID

Task ID	Operation
crypto	read, write

This example shows how to specify which field in the certificate is to be used as the username. Here, it specifies the user common name to be picked up from the subject name field.

```
Router#configure
Router(config)#ssh server certificate username common-name
Router(config)#commit
```

Here, it specifies the user principle name to be picked up from the subject alternate name field.

```
Router#configure
Router(config)#ssh server certificate username user-principle-name
Router(config)#commit
```

ssh disable hmac

To disable HMAC cryptographic algorithm on the SSH server, use the **ssh server disable hmac** command, and to disable HMAC cryptographic algorithm on the SSH client, use the **ssh client disable hmac** command in Global Configuration mode. To disable this feature, use the **no** form of this command.

ssh {**client** | **server**} **disable hmac** {**hmac-sha1** | **hmac-sha2-512**}

Syntax Description

hmac-sha1	Disables the SHA-1 HMAC cryptographic algorithm.
hmac-sha2-512	Disables the SHA-2 HMAC cryptographic algorithm. **Note** This option is available only for the **server**.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
crypto	read, write

This example shows how to disable SHA1 HMAC cryptographic algorithm on the SSH client:

```
Router#ssh client disable hmac hmac-sha1
```

This example shows how to disable SHA-2 HMAC cryptographic algorithm on the SSH server:

```
Router#ssh server disable hmac hmac-sha2-512
```

ssh server enable cipher

To enable CBC mode ciphers 3DES-CBC and/or AES-CBC for an SSH server connection, use the **ssh server enable cipher** command in Global Configuration mode. To disable the ciphers, use the **no** form of this command.

ssh server enable cipher {**aes-cbc** | **3des-cbc**}

Syntax Description

3des-cbc	Specifies that the 3DES-CBC cipher be enabled for the SSH server connection.
aes-cbc	Specifies that the AES-CBC cipher be enabled for the SSH server connection.

Command Default

CBC mode ciphers are disabled.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

The support for CBC ciphers were disabled by default, from Cisco IOS XR Software Release 6.1.2. Hence, **ssh client enable cipher** and **ssh server enable cipher** commands were introduced to explicitly enable CBC ciphers in required scenarios.

Task ID

Task ID	Operation
crypto	read, write

Examples

The following example shows how to enable the 3DES-CBC and AES-CBC ciphers for an SSH server connection:

```
Router# configure
Router(config)# ssh server enable cipher aes-cbc 3des-cbc
Router(config)# commit
```

Related Commands

Command	Description
ssh client enable cipher , on page 449	Enables CBC mode ciphers on the SSH client.

ssh server max-auth-limit

To configure the maximum number of authentication attempts allowed for SSH connection, use the **ssh server max-auth-limit** command in Global Configuration mode. To remove the configuration, use the **no** form of this command.

ssh server max-auth-limit *limit*

Syntax Description

limit	Specifies the maximum authentication attempts allowed for SSH connection. The limit ranges from 3 to 20; default being 20 (prior to Cisco IOS XR Software Release 7.3.2, the limit range was from 4 to 20).

Command Default

The default authentication limit is 20.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 7.3.2	The command was modified to change the minimum value of limit range from 4 to 3.
Release 7.3.1	This command was introduced

Usage Guidelines

The SSH server limits the number of authentication attempts using the password authentication method to a maximum of 3 due to security reasons. You cannot change this particular limit of 3 by configuring the maximum authentication attempts limit for SSH.

For example, even if you configure the maximum authentication attempts limit as 5, the number of authentication attempts allowed using the password authentication method still remain as 3.

Task ID

Task ID	Operations
crypto	read, write

Examples

This example shows how to configure the maximum number of authentication attempts allowed for SSH connection:

```
Router# configure
Router(config)# ssh server max-auth-limit 5
Router(config)# commit
```

ssh server port

To configure a non-default port for the SSH server, use the **ssh server port** command in Global Configuration mode. To remove the configuration and to change the SSH port number to the default port (22), use the **no** form of this command.

ssh server port *port-number*

Syntax Description

port-number	Specifies the non-default SSH port number. The limit ranges from 5520 to 5529.

Command Default

Disabled, by default.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 7.7.1	This command was introduced

Usage Guidelines

If this command is not configured, then the SSH server uses the default port number, 22, for all SSH services.

Task ID

Task ID	Operations
crypto	read, write

Examples

This example shows how to configure a non-default SSH port for the SSH server on your router:

```
Router# configure
Router(config)# ssh server port 5520
Router(config)# commit
```

ssh server port-forwarding local

To enable SSH port forwarding feature on SSH server, use the **ssh server port-forwarding local** command in Global Configuration mode. To disable the feature, use the **no** form of this command.

ssh server port-forwarding local

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

The Cisco IOS XR software supports SSH port forwarding only on SSH server; not on SSH client. Hence, to utilize this feature, the SSH client running at the end host must already have the support for SSH port forwarding or tunneling.

Task ID

Task ID	Operations
crypto	read, write

Examples

This example shows how to enable SSH port forwarding feature on SSH server:

```
Router#configure
Router(config)#ssh server port-forwarding local
Router(config)#commit
```

Related Commands

Command	Description
show ssh, on page 431	Displays all incoming and outgoing SSH connections on the router.

ssh server rekey-time

To configure rekey of the ssh server key based on time, use the **ssh server** command in Global Configuration mode. Use the **no** form of this command to remove the rekey interval.

ssh server rekey-time *time in minutes*

Syntax Description

rekey-time *time in minutes*	Specifies the rekey-time interval in minutes. The range is between 30 to 1440 minutes.
Note	If no time interval is specified, the default interval is considered to be 60 minutes.

Command Default

None.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 6.2.1	This command was introduced.

Task ID

Task ID	Operations
crypto	read, write

Examples

In the following example, the SSH server rekey-interval of 450 minutes is used:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh server rekey-time 450
```

ssh server rekey-volume

To configure a volume-based rekey threshold for an SSH session, use the **ssh server** command in Global Configuration mode. Use the **no** form of this command to remove the volume-based rekey threshold.

ssh server rekey-volume *data in megabytes*

Syntax Description

rekey-volume *data in megabytes*	Specifies the volume-based rekey threshold in megabytes. The range is between 1024 to 4095 megabytes. **Note** If no volume threshold is specified, the default size is considered to be 1024 MB.

Command Default

None.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 6.2.1	This command was introduced.

Task ID

Task ID	Operations
crypto	read, write

Examples

In the following example, the SSH server rekey-volume of 2048 minutes is used:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh server rekey-volume 2048
```

ssh server logging

To enable SSH server logging, use the **ssh server logging** command in Global Configuration mode. To discontinue SSH server logging, use the **no** form of this command.

ssh server logging

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.8.0	This command was introduced.

Usage Guidelines

Only SSHv2 client connections are allowed.

Once you configure the logging, the following messages are displayed:

- Warning: The requested term-type is not supported
- SSH v2 connection from %s succeeded (*user:%s, cipher:%s, mac:%s, pty:%s*)

The warning message appears if you try to connect using an unsupported terminal type. Routers running the Cisco IOS XR software support only the vt100 terminal type.

The second message confirms a successful login.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows the initiation of an SSH server logging:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh server logging
```

Related Commands

Command	Description
ssh server, on page 454	Initiates the SSH server.

ssh server rate-limit

To limit the number of incoming Secure Shell (SSH) connection requests allowed per minute, use the **ssh server rate-limit** command in Global Configuration mode. To return to the default value, use the **no** form of this command.

ssh server rate-limit *rate-limit*

Syntax Description

rate-limit Number of incoming SSH connection requests allowed per minute. Range is from 1 to 600.

Despite being configured in minute the implementation of rate-limit is per second, per sub-second or per several seconds.

There are two different behaviors for this command depending on whether the configured value is <120 or >=120.

- If the configured value is <120, it means 1 session is allowed within (60/configured value) second(s). Below are the examples based on the configured value, which is <120:
  - If you configure 30 sessions per minute it means 1 session every (60/30) = 2 seconds.
  - If you configure 60 sessions per minute it means 1 session every (60/60) = 1 second.
  - If you configure 80 sessions per minute it means 1 session every (60/80) = 0.75 second.
- If the configured value is >=120, it means n sessions are allowed within 1 second and it allows for these connections to be simultaneous (at the exact same time). Below are the examples based on the configured value, which is >=120:
  - If you configure 120 sessions per minute it means 2 sessions every 1 second (which can be simultaneous).
  - If you configure 180 sessions per minute it means 3 sessions every 1 second (which can be simultaneous).
  - If you configure 180 sessions per minute it means 3 sessions every 1 second (which can be simultaneous).

In all the above listed cases, if you exceed the allowed configured value the subsequent connection attempts will be refused.

The connection attempts are to the ssh server and not bound per interface or username.

Command Default

rate-limit: 60 connection requests per minute

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **ssh server rate-limit** command to limit the incoming SSH connection requests to the configured rate. Any connection request beyond the rate limit is rejected by the SSH server. Changing the rate limit does not affect established SSH sessions.

If, for example, the *rate-limit* argument is set to 30, then 30 requests are allowed per minute, or more precisely, a two-second interval between connections is enforced.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to set the limit of incoming SSH connection requests to 20 per minute:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh server rate-limit 20
```

ssh server session-limit

To configure the number of allowable concurrent incoming Secure Shell (SSH) sessions, use the **ssh server session-limit** command in Global Configuration mode. To return to the default value, use the **no** form of this command.

ssh server session-limit *sessions*

Syntax Description

sessions Number of incoming SSH sessions allowed across the router. The range is from 1 to 100.

Note Although CLI output option has 1024, you are recommended to configure session-limit not more than 100. High session count may cause resource exhaustion .

Command Default

sessions: 64 per router

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **ssh server session-limit** command to configure the limit of allowable concurrent incoming SSH connections. Outgoing connections are not part of the limit.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to set the limit of incoming SSH connections to 50:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh server session-limit 50
```

ssh server trustpoint

To configure the trustpoint for SSH certificates, use the **ssh server trustpoint** command in Global Configuration mode. To disable this feature, use the **no** form of this command.

ssh server trustpoint { **host** | **user** } *trustpoint-name*

Syntax Description

host	Configures the trustpoint from where server takes its certificate.
user	Configures the trustpoints used for user certificate validation.
trustpoint-name	Specifies the name of the trustpoint.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 7.3.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
crypto	read, write

This example shows how to configure the trustpoint from where SSH server takes its certificate:

```
Router#configure
Router(config)#ssh server trustpoint host test-host-tp
Router(config)#commit
```

This example shows how to configure the trustpoint used for user certificate validation:

```
Router#configure
Router(config)#ssh server trustpoint user test-user-tp
Router(config)#commit
```

ssh server v2

To force the SSH server version to be only 2 (SSHv2), use the **ssh server v2** command in Global Configuration mode. To bring down an SSH server for SSHv2, use the **no** form of this command.

ssh server v2

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Only SSHv2 client connections are allowed.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to initiate the SSH server version to be only SSHv2:

```
 RP/0/RSP0/CPU0:router#configure
RP/0/RSP0/CPU0:router(config)# ssh server v2
```

ssh server netconf port

To configure a port for the netconf SSH server, use the **ssh server netconf port** command in Global Configuration mode. To return to the default port, use the **no** form of the command.

ssh server netconf port *port number*

Syntax Description

port *port-number*	Port number for the netconf SSH server (default port number is 830).

Command Default

The default port number is 830.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 5.3.0	This command was introduced.
Release 6.0	The **ssh server netconf** command is no longer auto completed to configure the default port. This command is now optional

Usage Guidelines

Starting with IOS-XR 6.0.0 it is no longer sufficient to configure a netconf port to enable netconf subsystem support. ssh server netconf needs to be at least configured for one vrf.

Task ID

Task ID	Operations
crypto	read, write

Examples

This example shows how to use the ssh server netconf port command with port 831:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh server netconf port 831
```

Related Commands

Command	Description
ssh server netconf	Configures the vrf(s), where netconf subsystem requests are to be received.
netconf-yang agent ssh	Configures the **ssh netconf-yang backend** for the netconf subsystem (Required to allow the system to service netconf-yang requests). For more information, see the *Cisco ASR 9000 Series Aggregation Services Router System Management Command Reference*.

ssh server netconf

To bring up the netconf subsystem support using a dedicated communication port with the Secure Shell (SSH) server and to configure one or more VRFs for its use, use the **ssh server netconf** command in Global Configuration mode. To stop the SSH server from receiving any further netconf subsystem connections for the specified VRF, use the **no** form of this command.

Optionally ACLs for IPv4 and IPv6 can be used to restrict access to the netconf subsystem of the SSH server before the port is opened.

ssh server netconf [**vrf***vrf name* [**ipv4 access-list** *access list name*] [**ipv6 access-list***access list name*]]

Syntax Description

vrf name	Specifies the name of the VRF to be used by the netconf subsystem of the SSH server. The maximum VRF length is 32 characters. **Note** If no VRF is specified, the default VRF is assumed.
IPv4 access list name	Configures an IPv4 access-list for access restrictions to the netconf subsystem of the SSH server.
IPv6 access list name	Configures an IPv6 access-list for access restrictions to the netconf subsystem of the SSH server.

Command Default

If no vrf is specified, the command is auto expanded using the default vrf.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 5.3.0	This command was introduced.
Release 6.0.0	The **ssh server netconf** command is no longer auto completed to configure the default port. The **vrf** keyword was supported. Without parameter the command is now auto expanded to enable the netconf subsystem for vrf default. To start netconf subsystem support at least one vrf needs to be configured.

Usage Guidelines

Netconf subsystem support of the SSH server must be configured at minimum for one VRF. If you delete all configured VRFs, including the default, the SSH server process stops serving the netconf subsystem requests. If you do not configure a specific VRF the default VRF is assumed. The SSH server listens for netconf subsystem connections an incoming client connection on the configured port (using ssh server netconf port) or port 8030 (as the iana assigned default port)

Netconf subsystem support is only available with Secure Shell Version 2 SSHv2 incoming client connections for both IPv4 and IPv6 address families. To verify that the SSH server is up and running, use the show process sshd command.

Task ID

Task ID	Operation
crypto	read, write

Example

This example shows how to use the **ssh server netconf vrf***vrf name* command:

```
RP/0/RSP0/CPU0:router (config) #  ssh server netconf vrf red
```

ssh timeout

To configure the timeout value for authentication, authorization, and accounting (AAA) user authentication, use the **ssh timeout** command in Global Configuration mode. To set the timeout value to the default time, use the **no** form of this command.

ssh timeout *seconds*

Syntax Description

seconds	Time period (in seconds) for user authentication. The range is from 5 to 120.

Command Default

seconds: 30

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

Use the **ssh timeout** command to configure the timeout value for user authentication to AAA. If the user fails to authenticate itself within the configured time to AAA, the connection is terminated. If no value is configured, the default value of 30 seconds is used.

Task ID

Task ID	Operations
crypto	read, write

Examples

In the following example, the timeout value for AAA user authentication is set to 60 seconds:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh timeout 60
```

Secure Socket Layer Protocol Commands

This module describes the commands used to configure the Secure Socket Layer (SSL) protocol.

For detailed information about SSL concepts, configuration tasks, and examples, see the *Implementing Secure Socket Layer on* the Cisco ASR 9000 Series Router module in the *System Security Configuration Guide for Cisco ASR 9000 Series Routers*.

show ssl

To display active Secure Socket Layer (SSL) sessions, use the **show ssl** command in EXEC mode.

show ssl [*process-id*]

Syntax Description

process-id	(Optional) Process ID (PID) of the SSL application. The range is from 1 to 1000000000.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To display a specific process, enter the process ID number. To get a specific process ID number, enter **run pidin** from the command line or from a shell.

The absence of any argument produces a display that shows all processes that are running SSL.

Task ID

Task ID	Operations
crypto	read

Examples

The following sample output is from the **show ssl** command:

```
RP/0/RSP0/CPU0:router# show ssl

PID         Method      Type        Peer                Port    Cipher-Suite
================================================================================

1261711     sslv3       Server      172.16.0.5          1296    DES-CBC3-SHA
```

This table describes the fields shown in the display.

Table 26: show ssl Field Descriptions

Field	Description
PID	Process ID of the SSL application.
Method	Protocol version (sslv2, sslv3, sslv23, or tlsv1).
Type	SSL client or server.
Peer	IP address of the SSL peer.
Port	Port number on which the SSL traffic is sent.

Field	Description
Cipher-Suite	Exact cipher suite chosen for the SSL traffic. The first portion indicates the encryption, the second portion the hash or integrity method. In the sample display, the encryption is Triple DES and the Integrity (message digest algorithm) is SHA.

Related Commands

Command	Description
run pidin	Displays the process ID for all processes that are running.

Secure Logging Commands

This module describes the Cisco IOS XR software commands used to configure secure logging on the Cisco ASR 9000 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 ASR 9000 Series Routers*.

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 483	Configures syslog over TLS server.
trustpoint , on page 485	Configures the trustpoint for the TLS server.

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.

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)#
```

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 483	Configures syslog over TLS server.
trustpoint , on page 485	Configures the trustpoint for the TLS server.

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 483	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 483	Configures syslog over TLS server.

FIPS commands

This module describes the commands used in enabling the FIPS mode.

For detailed information about FIPS configuration tasks, and examples, see the *Configuring FIPS Mode* chapter in *System Security Configuration Guide for Cisco ASR 9000 Series Routers*.

crypto fips-mode

To configure FIPS, use the **crypto fips-mode** command in Global Configuration mode. To remove FIPS configuration, use the **no** form of this command.

crypto fips-mode

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Global Configuration mode

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines Install and activate the **asr9k-k9sec-px.pie** file before using this command.

Note For the configuration to take effect, reload the router by using the reload command in the admin mode.

Use the **show logging** command to display the contents of logging buffers. You can use the **show logging | i fips** command to filter FIPS specific logging messages.

You must configure the session with a FIPS-approved cryptographic algorithm. A session configured with non-approved cryptographic algorithm for FIPS (such as, **MD5** and **HMAC-MD5**) does not work. This is applicable from Cisco IOS XR Software Release 6.7.2, Release 7.1.2, and later, for OSPF, BGP, RSVP, ISIS, or any application using key chain with non-approved cryptographic algorithm, and only for FIPS mode (that is, when **crypto fips-mode** is configured).

Task ID

Task ID	Operation
crypto	read, write

Example

This example shows how to configure FIPS:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto fips-mode
```