

SNMP Commands

Instructions for SNMP Commands

Note Some configurations and protocols are identified as insecure and is a security risk for Cisco devices. Existing deployments continue to function, but new installations require intentional enablement. For more information on remediation, refer to Resilient Infrastructure: Cisco Catalyst SD-WAN and Routing

- snmp ifmib ifindex persist, on page 2
- snmp mib community-map, on page 2
- snmp-server community, on page 3
- snmp-server contact, on page 5
- snmp-server context, on page 5
- snmp-server enable traps, on page 6
- snmp-server enable traps alarms informational, on page 6
- snmp-server enable traps bgp, on page 7
- snmp-server enable traps config, on page 8
- snmp-server enable traps config-copy, on page 9
- snmp-server enable traps config-ctid, on page 9
- snmp-server enable traps cpu, on page 10
- snmp-server enable traps entity, on page 11
- snmp-server enable traps entity-state, on page 11
- snmp-server enable traps event-manager, on page 12
- snmp-server enable traps flash, on page 12
- snmp-server enable traps memory, on page 13
- snmp-server enable traps ospf cisco-specific errors config-error, on page 14
- snmp-server enable traps ospf errors, on page 14
- snmp-server enable traps ospf lsa, on page 15
- snmp-server enable traps ospf state-change, on page 16
- snmp-server enable traps sdwan, on page 17
- snmp-server enable traps snmp, on page 17
- snmp-server enable traps syslog, on page 18
- snmp-server engineID local, on page 19
- snmp-server engineID remote, on page 19

- snmp-server file-transfer access-group, on page 20
- snmp-server group, on page 21
- snmp-server host, on page 23
- snmp-server location, on page 24
- snmp-server packetsize, on page 24
- snmp-server sparse-tables, on page 25
- snmp-server system-shutdown, on page 26
- snmp-server trap authentication unknown-context, on page 27
- snmp-server trap-source, on page 28
- snmp-server trap timeout, on page 28
- snmp-server user, on page 29
- snmp-server view, on page 31
- snmp trap link-status, on page 32
- tftp-server, on page 33

snmp ifmib ifindex persist

To globally enable ifindex values to persist, use the **snmp ifmib ifindex persist** command in global configuration mode. To globally disable ifIndex persistence, use the **no** form of this command.

snmp ifmib ifindex persist
no snmp ifmib ifindex persist

Syntax Description

This command has no arguments or keywords.

Command Default

The ifIndex persistence on a router is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The value remains constant across reboots, for use by SNMP in global configuration mode. For usage guidelines, see the Cisco IOS XE snmp ifmib ifindex persist command.

Examples

The following example shows how to enable ifIndex persistence for all interfaces:

```
Device(config)# snmp ifmib ifindex persist
```

snmp mib community-map

To associate a Simple Network Management Protocol (SNMP) community with an SNMP context, engine ID, or security name, use the **snmp mib community-map** command in global configuration mode. To change an SNMP community mapping to its default mapping, use the **no** form of this command.

snmp mib community-map *community-name* [**engineid** *engine-id*]
no snmp mib community-map *community-name* [**engineid** *engine-id*]

Syntax Description

community-name	String that identifies the SNMP community.
engineid	(Optional) Specifies that an SNMP engine ID is mapped to the SNMP community.
engine-id	String that identifies the SNMP engine ID. Default is the local engine ID

Command Default

No SNMP communities and contexts are associated.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp mib community-map command.

Examples

The following example shows how to specify the SNMP engine ID on the local device, create an SNMP community named community1, and associate the community with with the SNMP engine ID.

```
Device(config)# snmp-server engineID local 876543211234
Device(config)# snmp-server community community1
Device(config)# snmp mib community-map community1 engineid 876543211234
```

snmp-server community

To set up the community access string to permit access to the Simple Network Management Protocol (SNMP), use the **snmp-server community** command in global configuration mode. To remove the specified community string, use the **no**form of this command.

snmp-server community *string* [**view** *view-name*] [**ro** [*access-list-number/name*]]
no snmp-server community *string* [**ro**]

Syntax Description

string	Community string that consists of 1 to 32 alphanumeric characters and functions much like a password, permitting access to SNMP. Blank spaces are not permitted in the community string. **Note** The @ symbol is used for delimiting the context information. Avoid using the @ symbol as part of the SNMP community string when configuring this command.
view	(Optional) Specifies a previously defined view. The view defines the objects available to the SNMP community.

view-name	Name of a previously defined view.
ro	(Optional) Specifies read-only access. Authorized management stations can retrieve only MIB objects.
access-list-number/name	(Optional) Integer from 1 to 99 that specifies a standard access list of IP addresses or a string (not to exceed 64 characters) that is the name of a standard access list of IP addresses allowed access to the SNMP agent. Alternatively, an integer from 1300 to 1999 that specifies a list of IP addresses in the expanded range of standard access list numbers that are allowed to use the community string to gain access to the SNMP agent.

Command Default

An SNMP community string permits read-only access to all objects.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server community command.

Examples

The following example shows how to set the read only community string to TEST:

```
Device(config)# snmp-server community TEST ro
```

The following example shows how to allow read-only access for all objects to members of the standard named access list ACL1 that specify the TEST community string. No other SNMP managers have access to any objects.

```
Device(config)# snmp-server community TEST ro ACL1
```

The following example shows how to assign the string TEST to SNMP, allow read-only access, and specify that IP access list 4 can use the community string:

```
Device(config)# snmp-server community TEST ro 4
```

The following example shows how to remove the community TEST:

```
Device(config)# no snmp-server community TEST
```

The following example shows how to disable all versions of SNMP:

```
Device(config)# no snmp-server
```

snmp-server contact

To set the system contact (sysContact) string, use the **snmp-server contact** command in global configuration mode. To remove the system contact information, use the **no** form of this command.

snmp-server contact *text*
no snmp-server contact

Syntax Description

text	String that describes the system contact information.

Command Default

No system contact string is set.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Examples

The following is an example of a system contact string:

```
Device(config)#snmp-server contact Bangalore
```

snmp-server context

To create an SNMP context, use the **snmp-server context** command in global configuration mode. To delete an SNMP context, use the **no** form of this command.

snmp-server context *context-name*
no snmp-server context *context-name*

Syntax Description

context-name	Name of the SNMP context being created.

Command Default

No SNMP contexts are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server context command.

Examples

The following example shows how to create an SNMP context named contextA and associate it with a virtual private network (VPN) routing and forwarding (VRF) instance named CustomerA:

```
Device(config)# snmp-server context contextA
Device(config)# ip vrf CustomerA
Device(config-vrf)# rd 100:120
Device(config-vrf)# context contextA
```

snmp-server enable traps

To enable all Simple Network Management Protocol (SNMP) notification types that are available on your system, use the **snmp-server enable traps**command in global configuration mode. To disable all available SNMP notifications, use the **no**form of this command.

snmp-server enable traps
no snmp-server enable traps

Syntax Description

This command has no keywords or arguments.

Command Default

No notifications controlled by this command are sent.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server enable traps command.

Examples

The following example shows how to enable all notification types available on your device:

```
Device(config)# snmp-server enable traps
```

snmp-server enable traps alarms informational

To enable alarm SNMP notifications, use the **snmp-server enable traps alarms** command in global configuration mode. To disable SNMP notifications, use the **no** form of this command.

snmp-server enable traps alarms *severity*
no snmp-server enable traps alarms *severity*

Syntax Description

alarms	Enables alarm filtering to limit the number of syslog messages generated. Alarms are generated for the severity configured as well as for the higher severity values.

severity	The severity argument is an integer or string value that identifies the severity of an alarm. Integer values are from 1 to 4. String values are critical, major, minor, and informational. The default is 4 (informational). Severity levels are defined as follows: • 1--Critical: The condition affects service. • 2--Major: Immediate action is needed. • 3--Minor: Minor warning conditions. • 4--Informational: No action is required. This is the default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server enable traps command.

Examples

```
Device(config)# snmp-server enable traps alarms informational
```

snmp-server enable traps bgp

To enable Border Gateway Protocol (BGP) support for SNMP operations on a router, use the **snmp-server enable traps bgp** command in global configuration mode. To disable BGP support for SNMP operations, use the **no** form of this command.

snmp-server enable traps bgp [**cbgp2**] [**state-changes** [**all**] [**backward-trans**] [**limited**] | **threshold prefix**]
no snmp-server enable traps bgp [**cbgp2**] [**state-changes** [**all**] [**backward-trans**] [**limited**] | **threshold prefix**]

Syntax Description

cbgp2	(Optional) Enables generation of the CISCO-BGP-MIBv8.1 traps.
state-changes	(Optional) Enables traps for finite state machine (FSM) state changes.
all	(Optional) Enables Cisco specific traps for all FSM state changes.
backward-trans	(Optional) Enables Cisco specific traps for backward transition events.
limited	(Optional) Enables traps for standard backward transition and established events.
threshold prefix	(Optional) Enables Cisco-specific trap for prefix threshold events.

Command Default

By default, SNMP notifications are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

If you have Cisco Catalyst SD-WAN Manager Release 20.15.3 and Cisco IOS XE Catalyst SD-WAN Release 17.12.2a, then update the cli template with the **snmp-server enable traps bgp-dep** command.

For usage guidelines, see the Cisco IOS XE snmp-server enable traps bgp command.

Examples

The following example enables the router to send BGP state change informs to the host at the address myhost.cisco.com using the community string defined as public:

```
Device(config)# snmp-server enable traps bgp
Device(config)# snmp-server host myhost.cisco.com informs version 2c public
```

The following example enables generation of the CISCO-BGP-MIBv8.1 traps:

```
Device(config)# snmp-server enable traps bgp cbgp2
```

snmp-server enable traps config

To enable SNMP trap notifications for configuration activity, use the **snmp-server enable traps config** command in global configuration mode. To disable SNMP trap notifications, use the **no** form of this command.

snmp-server enable traps config
no snmp-server enable traps config

Syntax Description

config	Controls configuration notifications, as defined in the CISCO-CONFIG-MAN-MIB (enterprise 1.3.6.1.4.1.9.9.43.2). The notification type is (1) ciscoConfigManEvent.

Command Default

No notifications controlled by this command are sent.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server enable traps command.

Example

```
Device(config)# snmp-server enable traps config
```

snmp-server enable traps config-copy

To send config-copy notifications to Cisco SD-WAN Manager or to the Simple Network Management Protocol (SNMP) manager, indicating successful completion of the config-copy operation to or from an SNMP agent, use the **snmp-server enable traps config-copy** command in global configuration mode. To disable sending notifications, use the **no** form of this command.

snmp-server enable traps config-copy
no snmp-server enable traps config-copy

Syntax Description

config-copy	Facilitates the task of copying SNMP agent configuration files to the startup configuration or to the local Cisco IOS file system, and vice versa.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

The Config-Copy MIB facilitates the copying of SNMP agent configuration files to the startup configuration or the local Cisco IOS file system, and vice versa. The config-copy notifications are sent to Cisco SD-WAN Manager or the SNMP manager to indicate the successful completion of the config-copy operation to or from the SNMP agent.

Examples

The following example shows how to configure config-copy traps to simulate the verification of config-copy traps:

```
Device(config)# snmp-server enable traps config-copy
```

snmp-server enable traps config-ctid

To enable configuration change tracking identifier (CTID) notifications, use the **snmp-server enable traps config-ctid** command in global configuration mode. To disable CTID notifications, use the **no** form of this command.

snmp-server enable traps config-ctid
no snmp-server enable traps config-ctid

Syntax Description

config-ctid	Specifies the configuration change tracking identifier.

Command Default

This command is disabled by default. If this command isn't run, the management system has to query the device for the current running-config file and then compare the results with the last-known configuration to determine if a change has been made.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

This configuration infrastructure command assigns a version number that is updated every time the running-config file is changed. This version number is called the configuration change tracking identifier (CTID). This identifier assigns a version number to each saved version of the running-config file. The CTID can be used to compare configuration files to track configuration changes and take appropriate actions, for example, a configuration rollback. Config Logger can also use the CTID to determine if there have been any changes to the running-config file.

CTID makes the management system more efficient by presenting information that indicates a change has been made to the running-config file. Without CTID, the management system has to query the device for the current running-config file and then compare the results with the last-known configuration to determine if a change has been made.

Examples

The following example shows how to enable configuration change tracking identifier (CTID) notifications:

```
Device(config)# snmp-server enable traps config-ctid
```

snmp-server enable traps cpu

To enable a device to send CPU thresholding violation notifications, use the **snmp-server enable traps cpu** command in global configuration mode. To stop a device from sending CPU threshold notifications, use the **no** form of this command.

snmp-server enable traps cpu threshold
no snmp-server enable traps cpu

Syntax Description

threshold	Enables notifications of CPU threshold violations.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server enable traps cpu command.

Examples

The following example shows how to enable a device to send CPU threshold-related information to the host at the address myhost.cisco.com using the community string defined as public:

```
Device(config)# snmp-server enable traps cpu threshold
Device(config)# snmp-server host myhost.cisco.com informs version 2c public cpu
```

snmp-server enable traps entity

To send entity MIB notifications to a host, use the **snmp-server enable traps entity** command in global configuration mode. To disable SNMP notifications, use the **no** form of this command.

snmp-server enable traps entity
no snmp-server enable traps entity

Syntax Description

entity	Controls Entity MIB modify notifications. This notification type is defined in the ENTITY-MIB (enterprise 1.3.6.1.2.1.47.2) as (1) entConfigChange.

Command Default

By default, the command is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

```
Device(config)# snmp-server enable traps entity
```

snmp-server enable traps entity-state

To send information about the state of physical components such as disk, memory, and CPU utilization, use the **snmp-server enable traps entity-state** command in global configuration mode. To disable sending information about physical components, use the **no** form of this command.

snmp-server enable traps entity-state
no snmp-server enable traps entity-state

Syntax Description

This command has no keywords or arguments.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

```
Device(config)# snmp-server enable traps entity-state
```

snmp-server enable traps event-manager

To permit Simple Network Management Protocol (SNMP) traps to be sent from the Cisco IOS XE Catalyst SD-WAN devices to the SNMP server, enable the **snmp-server enable traps event-manager** command in global configuration mode. Other relevant **snmp-server** commands must also be configured. For details see the **action snmp-trap** command page. To stop sending SNMP traps to the server, use the **no** form of this command.

snmp-server enable traps event-manager
no snmp-server enable traps event-manager

Syntax Description

event-manager	Enables SNMP-embedded event manager traps.

Command Default

No Embedded Event Manager (EEM) traps are registered.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Examples

The following example shows how to enable SNMP-embedded event manager traps:

```
Device(config)# snmp-server enable traps event-manager
```

snmp-server enable traps flash

To enable flash device insertion and removal Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps flash** command in global configuration mode. To disable flash device SNMP notifications, use the **no** form of this command.

snmp-server enable traps flash [**insertion** | **lowspace** | **removal**]
no snmp-server enable traps flash

Syntax Description

insertion	(Optional) Controls flash card insertion notifications.
low space	(Optional) Controls flash card low-space notifications.
removal	(Optional) Controls flash card removal notifications.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server enable traps flash command.

Examples

The following example shows how to enable a device to send information relating to flash card insertion, low space, and removal to the host at the address myhost.cisco.com using the community string defined as public:

```
Device(config)# snmp-server enable traps flash insertion lowspace removal
Device(config)# snmp-server host myhost.cisco.com informs version 2c public flash
```

snmp-server enable traps memory

To enable a device to send Simple Network Management Protocol (SNMP) notifications when memory pool buffer usage reaches a new peak, use the **snmp-server enable traps memory** command in global configuration mode. To stop notifications from being generated, use the **no** form of this command.

snmp-server enable traps memory [**bufferpeak**]
no snmp-server enable traps memory [**bufferpeak**]

Syntax Description

bufferpeak	(Optional) Specifies memory buffer peak notifications.

Command Default

SNMP notifications in the MEMPOOL-MIB are not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server enable traps memory command.

Examples

The following example shows how to configure memory traps to enable all the available memory-related SNMP notifications and configured to be sent as information to the host myhost.cisco.com using the community string public:

```
Device(config)# snmp-server enable traps memory
Device(config)# snmp-server host myhost.cisco.com informs version 3 public memory
```

snmp-server enable traps ospf cisco-specific errors config-error

To enable SNMP notifications for Open Shortest Path First (OSPF) nonvirtual interface mismatch errors, use the **snmp-server enable traps ospf cisco-specific errors config-error** command in global configuration mode. To disable OSPF nonvirtual interface mismatch error SNMP notifications, use the **no** form of this command.

snmp-server enable traps ospf cisco-specific errors config-error
no snmp-server enable traps ospf cisco-specific errors config-error

Syntax Description

This command has no keywords or arguments.

Command Default

This command is disabled by default; therefore, SNMP notifications for OSPF nonvirtual interface mismatch errors are not created.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server enable traps ospf cisco-specific errors command.

Examples

The following example enables the router to send nonvirtual interface mismatch error notifications to the host at the address myhost.cisco.com using the community string defined as public:

```
Device(config)# snmp-server enable traps ospf cisco-specific errors config-error
Device(config)# snmp-server host myhost.cisco.com informs version 2c public
```

snmp-server enable traps ospf errors

To enable SNMP notifications for Open Shortest Path First (OSPF) errors, use the **snmp-server enable traps ospf errors** command in global configuration mode. To disable SNMP notifications for OSPF errors, use the **no** form of this command.

snmp-server enable traps ospf errors [**authentication-failure**] [**bad-packet**] [**config-error**] [**virt-authentication-failure**] [**virt-bad-packet**] [**virt-config-error**]
no snmp-server enable traps ospf errors [**authentication-failure**] [**bad-packet**] [**config-error**] [**virt-authentication-failure**] [**virt-bad-packet**] [**virt-config-error**]

Syntax Description

authentication-failure	(Optional) Enables only the ospfIfFailure trap. Allows SNMP notifications to be sent when a packet has been received on a nonvirtual interface from a neighbor router whose authentication key or authentication type conflicts with the authentication key or authentication type of this router.

bad-packet	(Optional) Enables only the ospfIfRxBadPacket trap. Allows SNMP notifications to be sent when an OSPF packet that has not been parsed has been received on a nonvirtual interface.
config-error	(Optional) Enables only the ospfIfConfigError trap. Sends SNMP notifications when a packet has been received in a nonvirtual interface from a neighbor router whose configuration parameters conflict with the configuration parameters of this router.
virt-authentication-failure	(Optional) Enables only the ospfVirtIfFailure trap. Allows SNMP notifications to be sent when a packet has been received on a virtual interface from a neighbor router whose authentication key or authentication type conflicts with the authentication key or authentication type of this router.
virt-bad-packet	(Optional) Enables only the ospfVirtIfRxBadPacket trap. Allows SNMP notifications to be sent when an OSPF packet that has not been parsed has been received on a virtual interface.
virt-config-error	(Optional) Enables only the ospfVirtIfConfigError trap. Sends SNMP notifications when a packet has been received in a virtual interface from a neighbor router whose configuration parameters conflict with the configuration parameters of this router.

Command Default

SNMP notifications for OSPF errors are disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server enable traps ospf errors command.

Examples

The following example enables the router to send all OSPF error notifications:

```
Device(config)# snmp-server enable traps ospf errors
```

snmp-server enable traps ospf lsa

To enable SNMP notifications for Open Shortest Path First (OSPF) link-state advertisements (LSAs), use the **snmp-server enable traps ospf lsa** command in global configuration mode. To disable SNMP notifications for OSPF LSAs, use the **no** form of this command.

snmp-server enable traps ospf lsa [**lsa-maxage**] [**lsa-originate**]
no snmp-server enable traps ospf lsa [**lsa-maxage**] [**lsa-originate**]

Syntax Description

lsa-maxage	(Optional) Enables only the ospfMaxAgeLsa trap. Allows SNMP notifications to be sent when an LSA in the OSPF link-state database of the router has reached the maximum age.

lsa-originate	(Optional) Enables only the ospfOriginateLsa trap. Enables SNMP notifications when a new LSA has been originated by the router as a result of a topology change.

Command Default

SNMP notifications for OSPF LSAs are disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server enable traps ospf lsa command.

Examples

The following example enables the router to send SNMP notifications when new LSAs are originated by the router as a result of a topology change:

```
Device(config)# snmp-server enable traps ospf lsa lsa-originate
```

snmp-server enable traps ospf state-change

To enable SNMP notifications for Open Shortest Path First (OSPF) transition state changes, use the **snmp-server enable traps ospf state-change** command in global configuration mode. To disable SNMP notifications for OSPF transition state changes, use the **no** form of this command.

snmp-server enable traps ospf state-change
no snmp-server enable traps ospf state-change

Syntax Description

This command has no arguments or keywords.

Command Default

SNMP notifications for OSPF transition state changes are disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

To enable all traps for transition state changes, enter the **snmp-server enable traps ospf state-change** command.

Examples

The following example enables the router to send SNMP notifications for transition state changes:

```
Device(config)# snmp-server enable traps ospf state-change
```

snmp-server enable traps sdwan

To enable all ciscoSdwan traps, use **snmp-server enable traps sdwan** command. To disable traps, use the **no** form of this command.

snmp-server enable traps sdwan
no snmp-server enable traps sdwan

Syntax Description

This command has no keywords or arguments.

Command Default

ciscoSdwan traps are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

```
Device(config)# snmp-server enable traps sdwan
```

snmp-server enable traps snmp

To enable the RFC 1157 Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps snmp**command in global configuration mode. To disable RFC 1157 SNMP notifications, use the **no**form of this command.

snmp-server enable traps snmp [**authentication**] [**linkup**] [**linkdown**] [**coldstart**] [**warmstart**]
no snmp-server enable traps snmp [**authentication**] [**linkup**] [**linkdown**] [**coldstart**] [**warmstart**]

Syntax Description

authentication	(Optional) Controls the sending of SNMP authentication failure notifications.
linkup	(Optional) Controls the sending of SNMP linkUp notifications.
linkdown	(Optional) Controls the sending of SNMP linkDown notifications.
coldstart	(Optional) Controls the sending of SNMP coldStart notifications.
warmstart	(Optional) Controls the sending of SNMP warmStart notifications.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

For usage guidelines, see the Cisco IOS XE snmp-server enable traps snmp command.

Examples

The following example shows how to enable various SNMP trap types.

```
Device(config)# snmp-server enable traps snmp authentication

Device(config)# snmp-server enable traps snmp coldstart

Device(config)# snmp-server enable traps snmp linkdown

Device(config)# snmp-server enable traps snmp linkup

Device(config)# snmp-server enable traps snmp warmstart
```

snmp-server enable traps syslog

To enable sending of system logging message Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps syslog** command in global configuration mode. To disable sending SNMP notifications, use the **no** form of this command.

snmp-server enable traps syslog
no snmp-server enable traps syslog

Syntax Description

This command has no arguments or keywords.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server enable traps syslog command.

Examples

The following example shows how to enable the device to send system logging messages at severity levels 0 (emergencies) through 2 (critical) to the host at the address myhost.cisco.com using the community string defined as public:

```
Device(config)# snmp-server enable traps syslog
Device(config)# logging history 2
Device(config)# snmp-server host myhost.cisco.com traps version 2c public
```

snmp-server engineID local

To specify the Simple Network Management Protocol (SNMP) engine ID on the local device, use the **snmp-server engineID local** command in global configuration mode. To remove the configured engine ID, use the **no** form of this command.

snmp-server engineID local *engineid-string*
no snmp-server engineID local

Syntax Description

engineid-string	String of a minimum of 10 characters and a maximum of 64 characters that identifies the engine ID.

Command Default

An SNMP engine ID is generated automatically but is not displayed or stored in the running configuration. You can display the default or configured engine ID by using the **show snmp engineID** command.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server engineID local command.

Examples

The following example specifies the local SNMP engine ID:

```
Device(config)# snmp-server engineID local
```

snmp-server engineID remote

To specify the Simple Network Management Protocol (SNMP) engine ID of a remote SNMP device, use the **snmp-server engineID remote** command in global configuration mode. To remove a specified SNMP engine ID from the configuration, use the **no** form of this command.

snmp-server engineID remote *ipv4-address* [**udp-port** *udp-port-number*] [**vrf** *vrf-name*] [*engineid-string*]
no snmp-server engineID remote *ipv4-address* [**udp-port** *udp-port-number*] [**vrf** *vrf-name*] [*engineid-string*]

Syntax Description

ipv4-address	IPv4 address of the device that contains the remote copy of SNMP.
udp-port	(Optional) Specifies a User Datagram Protocol (UDP) port of the host to use.
udp-port-number	(Optional) Socket number on the remote device that contains the remote copy of SNMP. The default is 161.

vrf	(Optional) Specifies an instance of a routing table.
vrf-name	(Optional) Name of the Virtual Private Network (VPN) routing and forwarding (VRF) table to use for storing data.
engineid-string	String of a maximum of 64 characters and minimum of 10 characters that identifies the engine ID.

Command Default

The default is UDP port 161.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server engineID remote command.

Example

The following example specifies the SNMP engine ID and configures the VRF name BLR for SNMP communications with the remote device at 172.16.20.3:

```
Device(config)# snmp-server engineID remote 172.16.20.3 vrf BLR
80000009030000B064EFE100
```

The following example specifies the SNMP engine ID and UDP port for SNMP communications with the remote device at 10.1.1.1:

```
Device(config)# snmp-server engineID remote 10.1.1.1 udp-port 10 abcdef1234
```

snmp-server file-transfer access-group

To associate an access list to the transfer protocols TFTP, FTP, Remote Copy Protocol (RCP), Secure Copy Protocol (SCP), and Secured File Transfer Protocol (SFTP), use the **snmp-server file-transfer access-group** command in global configuration mode. To disassociate an access list, use **no** form of this command.

snmp-server file-transfer access-group { *acl-number* | *acl-name* }
no snmp-server file-transfer access-group

Syntax Description

acl-number	Integer from 1 to 99 that specifies a standard ACL.
acl-name	String that specifies a standard ACL.

Command Default

If a protocol is not specified, all protocols are associated with the access list.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

For usage guidelines, see the Cisco IOS XE snmp-server file-transfer access-group command.

Examples

The following example shows that configuration transfers that are initiated through SNMP are associated with access list 10 for all the protocols.

```
Device(config)# snmp-server file-transfer access-group 10
```

snmp-server group

To configure a new Simple Network Management Protocol (SNMP) group, use the **snmp-server group** command in global configuration mode. To remove a specified SNMP group, use the **no** form of this command.

snmp-server group *group-name* **v3** { **auth** | **noauth** | **priv** } [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] [**access** [*acl-number* | *acl-name*] [**ipv6** *named-access-list*]]
no snmp-server group *group-name* **v3** { **auth** | **noauth** | **priv** } [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] [**access** [*acl-number* | *acl-name*] [**ipv6** *named-access-list*]]

Syntax Description

group-name	Name of the group.
v3	Specifies that the group is using the SNMPv3 security model. SMNPv3 is the most secure of the supported security models. It allows you to explicitly configure authentication characteristics.
auth	Specifies authentication of a packet without encrypting it.
noauth	Specifies no authentication of a packet.
priv	Specifies authentication of a packet with encryption.
read	Specifies a read view for the SNMP group. This view enables you to view only the contents of the agent.
read-view	String of a maximum of 64 characters that is the name of the view. The default is that the read-view is assumed to be every object belonging to the Internet object identifier (OID) space (1.3.6.1), unless the **read** option is used to override this state.
write	(Optional) Specifies a write view for the SNMP group. This view enables you to enter data and configure the contents of the agent.
write-view	(Optional) String of a maximum of 64 characters that is the name of the view. The default is that nothing is defined for the write view (that is, the null OID). You must configure write access.

notify	(Optional) Specifies a notify view for the SNMP group. This view enables you to specify a notify, inform, or trap.
notify-view	(Optional) String of a maximum of 64 characters that is the name of the view. By default, nothing is defined for the notify view (that is, the null OID) until the **snmp-server host** command is configured. If a view is specified in the **snmp-server group** command, any notifications in that view that are generated will be sent to all users associated with the group (provided a SNMP server host configuration exists for the user). Cisco recommends that you let the software autogenerate the notify view. See the "Configuring Notify Views" section in this document.
access	(Optional) Specifies a standard access control list (ACL) to associate with the group.
acl-number	The *acl-number*argument is an integer from 1 to 99 that identifies a previously configured standard access list.
acl-name	The *acl-name* argument is a string of a maximum of 64 characters that is the name of a previously configured standard access list.
ipv6	(Optional) Specifies an IPv6 named access list. If both IPv6 and IPv4 access lists are indicated, the IPv6 named access list must appear first in the list.
named-access-list	(Optional) Name of the IPv6 access list.

Command Default

No SNMP server groups are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Additional parameters qualified: **priv** (specifies authenticating a packet with encryption), **access** (allows you to specify an ACL to associate with a group), and **ipv6** (allows you to specify an IPv6 named access list).

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server group command.

Examples

Create an SNMP Group

The following example shows how to create the SNMP server group "public", allowing read-only access for all objects to members of the standard named access list "view-public":

```
Device(config)# snmp-server group public v3 noauth read view-public
```

```
Device(config)# snmp-server group public v3 priv read view-public access 5
```

snmp-server host

To specify the recipient of a Simple Network Management Protocol (SNMP) notification operation, use the **snmp-server host** command in global configuration mode. To remove the specified host from the configuration, use the **no** form of this command.

snmp-server host *ip-address* { **vrf** *vrf-name* **version** [**2c** *string* **udp-port** *port*] | **version 3 noauth** *string* [**udp-port** *port*] }
no snmp-server host *ip-address* { **vrf** *vrf-name* **version** [**2c** *string* **udp-port** *port*] | **version 3 noauth** *string* [**udp-port** *port*] }

Syntax Description

ip-address	IPv4 address or IPv6 address of the SNMP notification host.
vrf	Specifies that a VPN routing and forwarding (VRF) instance should be used to send SNMP notifications.
vrf-name	VPN VRF instance used to send SNMP notifications.
version	Specifies the version of the SNMP that is used to send the traps or informs. The default is 1. One of the following three optional security level keywords can follow the **3** keyword:
2c	Specifies SNMPv2C as the SNMP version.
3	Specifies SNMPv3 as the SNMP version.
noauth	Specifies that the noAuthNoPriv security level applies to this host. This is the default security level for SNMPv3.
string	Password-like community string sent with the notification operation. **Note** You can set this string using the **snmp-server host** command by itself, but we recommend that you define the string using the **snmp-server community** command prior to using the **snmp-server host** command. **Note** The "at" sign (@) is used for delimiting the context information.
udp-port	Specifies that SNMP traps or informs are to be sent to an network management system (NMS) host.
port	User Datagram Protocol (UDP) port number of the NMS host. The default is 162.

Command Default

This command behavior is disabled by default. A recipient is not specified to receive notifications.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server host command.

Examples

```
Device(config)# snmp-server host 10.100.51.1 vrf 1 version 2c TEST udp-port 7081
Device(config)# snmp-server host 10.1.15.15 version 3 noauth TEST5 udp-port 161
```

snmp-server location

To set the system location string, use the **snmp-server location** command in global configuration mode. To remove the location string, use the **no** form of this command.

snmp-server location *text*
no snmp-server location

Syntax Description

text	String that describes the system location information.

Command Default

No system location string is set.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Examples

The following example shows how to set a system location string:

```
Device(config)# snmp-server location Bengaluru
```

snmp-server packetsize

To establish control over the largest Simple Network Management Protocol (SNMP) packet size permitted when the SNMP server is receiving a request or generating a reply, use the **snmp-server packetsize** command in global configuration mode. To restore the default value, use the **no** form of this command.

snmp-server packetsize *byte-count*
no snmp-server packetsize

Syntax Description

byte-count	Integer from 484 to 17892. The default is 1500.

Command Default

Packet size is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Examples

The following example establishes a packet filtering of a maximum size of 1024 bytes:

```
Device(config)# snmp-server packetsize 1024
```

snmp-server sparse-tables

To populate all the Simple Network Management Protocol (SNMP) tables when an object ID is applicable, use the **snmp-server sparse-tables** command in global configuration mode. To populate all the SNMP tables even if an object ID is not applicable in a specific case, use the **no** form of this command.

snmp-server sparse-tables [**community** *text* | **contact** *text* | **context** *context-name* | **enable** | **engineID** *engineID-string* | **file-transfer access-group** | **group** *group-name* | **host** *host-name* | **ifindex persist** | **ip** | **location** *text* | **packetsize** *byte-count* | **source-interface** *byte-count* | **trap** | **trap-source** *interface* | **view** *view-name*]
no snmp-server sparse-tables [*notification-types*]

Syntax Description

community *text*	(Optional) Community string that consists of 1 to 32 alphanumeric characters and functions, much like a password permitting access to SNMP. Blank spaces aren't permitted in the community string. **Note** The @ symbol is used for delimiting the context information. Avoid using the @ symbol as part of the SNMP community string when configuring this command.
contact *text*	(Optional) Specifies a string that describes the system contact information.
context *context-name*	(Optional) Specifies the name of the SNMP context being created.
enable	(Optional) Enables traps or logging types of SNMP notifications that are available in your system.
engineID *engineID-string*	(Optional) Specifies the SNMP engine ID in the local or remote devices. This can be a string having a maximum of 24 characters.

file-transfer access-group	(Optional) Associates an access list to the transfer protocols TFTP, FTP, Remote Copy Protocol (RCP), Secure Copy Protocol (SCP), and Secured File Transfer Protocol (SFTP).
group *group-name*	(Optional) Configures a new SNMP group. Supports SNMPv3 security model group.
host *host-name*	(Optional) Specifies the recipient of an SNMP notification operation. The SNMP notification host is typically a network management station (NMS) or SNMP manager. This IPv4 or IPv6 SNMP notification host is the recipient of the SNMP traps or information.
ifindex persist	(Optional) Enables ifindex values to persist, which remains constant across reboots, for use by SNMP.
ip	(Optional) Enables sending of local IP SNMP notifications.
location *text*	(Optional) Specifies a string that describes the system location information.
packetsize *byte-count*	(Optional) Specifies the packet size that is permitted when the SNMP server is receiving a request or generating a reply. Byte count is an integer from 484 to 8192. The default is 1500.
source-interface *byte-count*	(Optional) Specifies the interface from which an SNMP trap originates.
trap	(Optional) Enables trap type of notification.
trap-source *interface*	(Optional) Specifies the interface (and hence the corresponding IP address) from which an SNMP trap should originate.
view *view-name*	(Optional) Creates or updates a view entry. View name is used to reference the record. Label for the view record that you're updating or creating.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Examples

The following example shows how to set the read/write community string to newstring:

```
Device(config)# snmp-server sparse-tables community newstring rw
```

snmp-server system-shutdown

To enable the SNMP message reload feature, use the **snmp-server system-shutdown** command in global configuration mode. To prevent an SNMP system-shutdown request (from an SNMP manager) from resetting the Cisco agent, use the **no** form of this command.

snmp-server system-shutdown

no snmp-server system-shutdown

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Usage Guidelines For usage guidelines, see the Cisco IOS XE snmp-server system-shutdown command.

Examples The following example shows how to enable the SNMP message reload feature:

```
Device(config)# snmp-server system-shutdown
```

snmp-server trap authentication unknown-context

To enable the SNMP authorization failure (authFail) traps during an unknown context error, use the **snmp-server trap authentication unknown-context** command in global configuration mode. To disable the authFail traps, use the **no** form of this command.

snmp-server trap authentication unknown-context
no snmp-server trap authentication unknown-context

Syntax Description This command has no arguments or keywords.

Command Default By default, authfail is enabled.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples The following example shows how to enable the authorization failure traps during an unknown context error:

```
Device(config)# snmp-server trap authentication unknown-context
```

The following example shows how to disable the authorization failure traps during an unknown context error:

```
Device(config)# no snmp-server trap authentication unknown-context
```

snmp-server trap-source

To specify the interface (and hence the corresponding IP address) from which a Simple Network Management Protocol (SNMP) trap should originate, use the **snmp-server trap-source** command in global configuration mode. To remove the source designation, use the **no** form of the command.

snmp-server trap-source Loopback *number*
no snmp-server trap-source

Syntax Description

number	Specifies the interface number. The range is <0..4294967295>

Command Default

No interface is specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server trap-source command.

Examples

Please verify the following example and provide a description for the same

```
Device(config)# snmp-server trap-source Loopback 10
```

snmp-server trap timeout

To define an interval of time between retransmissions of trap messages on a retransmission queue, use the **snmp-server trap timeout** command in global configuration mode.

To remove the interval defined, use the **no** form of this command.

snmp-server trap timeout *seconds*
no snmp-server trap timeout

Syntax Description

seconds	Integer from 1 to 1000 that sets the interval, in seconds, for resending messages. The default is 30.

Command Default

This command is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server trap timeout command.

Examples

The following example shows how to set an interval of 100 seconds between retransmissions of traps:

```
Device(config)# snmp-server trap timeout 100
```

snmp-server user

To configure a new user to a SNMP group, use the **snmp-server user** command in global configuration mode. To remove a user from an SNMP group, use the **no** form of this command.

snmp-server user *username group-name* [**remote** *host* [**udp-port** *port*] [**vrf** *vrf-name*]] { **v1** | **v2c** | **v3** [**encrypted**] [**auth** { **md5** | **sha** } *auth-password*] } [**access** [**ipv6** *nacl*] [**priv** { **des** | **3des** | **aes** { **128** | **192** | **256** } } *privpassword*] { *acl-number acl-name* }]
no snmp-server user *username group-name* [**remote** *host* [**udp-port** *port*] [**vrf** *vrf-name*]] { **v1** | **v2c** | **v3** [**encrypted**] [**auth** { **md5** | **sha** } *auth-password*] } [**access** [**ipv6** *nacl*] [**priv** { **des** | **3des** | **aes** { **128** | **192** | **256** } } *privpassword*] { *acl-number acl-name* }]

Syntax Description

username	Name of the user on the host that connects to the agent.
group-name	Name of the group to which the user belongs.
remote	(Optional) Specifies a remote SNMP entity to which the user belongs, and the hostname or IPv6 address or IPv4 IP address of that entity. If both an IPv6 address and IPv4 IP address are being specified, the IPv6 host must be listed first.
host	(Optional) Name or IP address of the remote SNMP host.
udp-port	(Optional) Specifies the User Datagram Protocol (UDP) port number of the remote host.
port	(Optional) Integer value that identifies the UDP port. The default is 162.
vrf	(Optional) Specifies an instance of a routing table.
vrf-name	(Optional) Name of the Virtual Private Network (VPN) routing and forwarding (VRF) table to use for storing data.
v1	Specifies that SNMPv1 should be used.
v2c	Specifies that SNMPv2c should be used.

v3	Specifies that the SNMPv3 security model should be used. Allows the use of the **encrypted** keyword or **auth** keyword or both.
encrypted	(Optional) Specifies whether the password appears in encrypted format.
auth	(Optional) Specifies which authentication level should be used.
md5	(Optional) Specifies the HMAC-MD5-96 authentication level.
sha	(Optional) Specifies the HMAC-SHA-96 authentication level.
auth-password	(Optional) String (not to exceed 64 characters) that enables the agent to receive packets from the host.
access	(Optional) Specifies an Access Control List (ACL) to be associated with this SNMP user.
ipv6	(Optional) Specifies an IPv6 named access list to be associated with this SNMP user.
nacl	(Optional) Name of the ACL. IPv4, IPv6, or both IPv4 and IPv6 access lists may be specified. If both are specified, the IPv6 named access list must appear first in the statement.
priv	(Optional) Specifies the use of the User-based Security Model (USM) for SNMP version 3 for SNMP message level security.
des	(Optional) Specifies the use of the 56-bit Digital Encryption Standard (DES) algorithm for encryption.
3des	(Optional) Specifies the use of the 168-bit 3DES algorithm for encryption.
aes	(Optional) Specifies the use of the Advanced Encryption Standard (AES) algorithm for encryption.
128	(Optional) Specifies the use of a 128-bit AES algorithm for encryption.
192	(Optional) Specifies the use of a 192-bit AES algorithm for encryption.
256	(Optional) Specifies the use of a 256-bit AES algorithm for encryption.
privpassword	(Optional) String (not to exceed 64 characters) that specifies the privacy user password.
acl-number	(Optional) Integer in the range from 1 to 99 that specifies a standard access list of IP addresses.
acl-name	(Optional) String (not to exceed 64 characters) that is the name of a standard access list of IP addresses.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server user command.

Examples

The following example configures a new user with an authentication and an authentication password and a privacy and privacy password, to receive traps at the priv security level when the SNMPv3 security model is enabled:

```
Device(config)# snmp-server user v3user AuthPriv groupAuthPriv v3 auth sha <PASSWORD> priv
 aes 128 <PASSWORD>
```

The following example configures a new user with an authentication and an authentication password, to receive traps at the authNoPriv security level when the SNMPv3 security model is enabled:

```
Device(config)# snmp-server user v3user AuthNoPriv groupAuthNoPriv v3 auth sha <PASSWORD>
```

The following example configures a new user without authentication or privacy credentials, to receive traps at the noAuthNoPriv security level when the SNMPv3 security model is enabled:

```
Device(config)# snmp-server user v3user NoAuthNoPriv groupNoAuthNoPriv v3
```

Note The **show running-config** command does not display any of the active SNMP users created in authPriv or authNoPriv mode, though it does display the users created in noAuthNoPriv mode. To display any active SNMPv3 users created in authPriv, authNoPrv, or noAuthNoPriv mode, use the **show snmp user** command.

snmp-server view

To create or update a view entry, use the **snmp-server view** command in global configuration mode. To remove the specified Simple Network Management Protocol (SNMP) server view entry, use the **no**form of this command.

snmp-server view *view-name oid-tree* **included**
no snmp-server view *view-name*

Syntax Description

view-name	Label for the view record that you are updating or creating. The name is used to reference the record.
oid-tree	Object identifier of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as system. Replace a single subidentifier with the asterisk (*) wildcard to specify a subtree family; for example 1.3.*.4.
included	Configures the OID (and subtree OIDs) specified in *oid-tree* argument to be included in the SNMP view.

Command Default

No view entry exists.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server view command.

Examples

In the following example, A view name TEST is created, which includes the MIB tree under 1.3.1 OID. Therefore, this view can be used to access the objects under the MIB tree 1.3.1 only.

```
Device(config)# snmp-server view TEST 1.3.1 included
```

snmp trap link-status

To enable Simple Network Management Protocol (SNMP) link trap generation when the interface state changes, use the **snmp trap link-status** command in interface configuration mode or service instance configuration mode. To disable SNMP link trap generation, use the **no** form of this command.

snmp trap link-status [**permit**]
no snmp trap link-status

Syntax Description

permit	(Optional) Permits SNMP linkup and linkdown traps.

Command Default

SNMP link trap status is the default.

Command Modes

Interface configuration (config-if)

Service instance configuration (config-if-srv)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp trap link-status command.

Examples

The following example shows how to disable SNMP link traps related to the ISDN BRI interface 0:

```
Device(config)# interface bri 0
Device(config-if)# no snmp trap link-status
```

The following example shows how to enable SNMP link traps for service instance 50 on Ethernet interface 0/1:

```
Device(config)# interface virtual-template 1
Device(config-if)# service instance 50 ethernet
Device(config-if-srv)# snmp trap link-status
```

tftp-server

To configure a router or a Flash memory device on the router as a TFTP server, use one of the following **tftp-server** commands in global configuration mode. This command replaces the **tftp-server system** command. To remove a previously defined filename, use the **no** form of this command with the appropriate filename.

tftp-server bootflash *bootflash-filename*
no tftp-server bootflash

Syntax Description

bootflash	Specifies TFTP service of a file in Flash memory.
bootflash-filename	Name of a file in Flash or in ROM that the TFTP server uses in answering TFTP Read Requests.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates

Usage Guidelines

You can specify multiple filenames by repeating the **tftp-server** command. The system sends a copy of the system image contained in ROM or one of the system images contained in Flash memory to any client that issues a TFTP Read Request with this filename.

If the specified *bootflash-filename1*or *bootflash-filename2*argument exists in Flash memory, a copy of the Flash image is sent. On systems that contain a complete image in ROM, the system sends the ROM image if the specified *bootflash-filename1*or *bootflash-filename2*argument is not found in Flash memory.

Examples

In the following example, the command **tftp-server bootflash:***c2900-universalk9-mz.SPA.154-3.M3.bin* configures a Cisco IOS XE Catalyst SD-WAN device to act as a TFTP server, making the specified IOS image file (c2900-universalk9-mz.SPA.154-3.M3.bin) located in its bootflash: memory available for other network devices to download.

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# tftp-server bootflash:c2900-universalk9-mz.SPA.154-3.M3.bin
```