



IPSec—SNMP Support

Feature History

Release	Modification
12.1(4)E	This feature was introduced on the Cisco 7100, 7200, and 7500 series.
12.1(5a)E	Support for CISCO-IPSEC-FLOW-MONITOR-MIB notifications was added.
12.2(4)T	Support for this feature was added for platforms in Release 12.2 T.
12.2(8)T, 12.1(11b)E	The following Command Line Interface (CLI) commands were added to enable and disable IP Security (IPSec) MIB notifications: <ul style="list-style-type: none">• snmp-server enable traps ipsec• snmp-server enable traps isakmp
12.2(14)S	This feature was integrated into Cisco IOS Release 12.2(14)S.

This document describes the IPSec—SNMP Support feature in Cisco IOS Release 12.1 E, 12.2 T, and 12.2 S and includes the following sections:

- [Feature Overview, page 2](#)
- [Supported Platforms, page 3](#)
- [Supported Standards, MIBs, and RFCs, page 5](#)
- [Configuration Tasks, page 5](#)
- [Monitoring and Maintaining IPSec MIB, page 7](#)
- [Configuration Examples, page 7](#)
- [Command Reference, page 8](#)
- [Glossary, page 23](#)



Note

This document focuses on Cisco IOS CLI support for the Cisco IPSec MIBs. This document also lists which elements of the MIBs are currently supported. This document does not describe SNMP configuration (from a Network Management Station) of the Cisco IPSec MIBs.

Feature Overview

The IP Security (IPSec) - SNMP Support feature introduces support for industry-standard IPSec MIBs and Cisco IOS-software specific IPSec MIBs.

The IPSec MIBs allow IPSec configuration monitoring and IPSec status monitoring using SNMP, and can be integrated in a variety of Virtual Private Network (VPN) management solutions.

For example, this feature allows you to specify the desired size of a tunnel history table or a tunnel failure table using the Cisco IOS CLI. The history table archives attribute and statistic information about the tunnel; the failure table archives tunnel failure reasons along with the time failure occurred. A failure history table can be used as a simple method to distinguish between a normal and an abnormal tunnel termination. That is, if a tunnel entry in the tunnel history table has no associated failure record, the tunnel must have terminated normally. However, a tunnel history table does not accompany every failure table because every failure does not correspond to a tunnel. Thus, supported setup failures are recorded in the failure table, but an associated history table is not recorded because a tunnel was never set up.

This feature also provides IPSec Simple Network Management Protocol (SNMP) notifications for use with network management systems.

Benefits

The commands in this feature allow you to examine the version of the IPSec MIB feature, to enable and disable SNMP traps, and to monitor and control the size of the buffers used by this feature.

Restrictions

Only the following tunnel setup failure logs are supported with the IPSec - SNMP Support feature:

- NOTIFY_MIB_IPSEC_PROPOSAL_INVALID
“A tunnel could not be established because the peer did not supply an acceptable proposal.”
- NOTIFY_MIB_IPSEC_ENCRYPT_FAILURE
“A tunnel could not be established because it failed to encrypt a packet to be sent to a peer.”
- NOTIFY_MIB_IPSEC_SYSCAP_FAILURE
“A tunnel could not be established because the system ran out of resources.”
- NOTIFY_MIB_IPSEC_LOCAL_FAILURE
“A tunnel could not be established because of an internal error.”

Note that these failure notices are recorded in the failure tables, but are not available as SNMP notifications (traps).

The following functions are not supported with the IPSec MIB feature:

- Checkpointing
- The Dynamic Cryptomap table of the CISCO-IPSEC-MIB



Note

CISCO-IPSEC-FLOW-MONITOR-MIB notifications are not supported before Cisco IOS Release 12.1(5a)E.

The CISCO-IPSEC-POLICY-MAP-MIB (ciscoIpSecPolMap) defines no notifications (the “IPSec Policy Map Notifications Group” is empty).

Related Features and Technologies

The IPSec—SNMP Support feature was designed to support the VPN Device Manager (VDM). VDM enables network administrators to manage and configure site-to-site VPNs on a single device from a web browser and to see the effects of changes in real time. VDM implements a wizard-based graphical user interface (GUI) to simplify the process of configuring site-to-site VPNs using the IPSec protocol. VDM software is installed directly on Cisco VPN routers, and is designed for use and compatibility with future Device Manager products.

For more information on Cisco VDM, refer to the following URL:

<http://www.cisco.com/warp/public/cc/pd/nemnsw/vpdvnm/>

Related Documents

IPSec and Related Security Information

- *Cisco IOS Security Configuration Guide*
- *Cisco IOS Security Command Reference*

SNMP Configuration Information

- *Cisco IOS Configuration Fundamentals Configuration Guide*
- *Cisco IOS Configuration Fundamentals Command Reference*

For the Cisco IOS Release 12.1 E implementation of security and SNMP features, refer to the Cisco IOS Release 12.1 versions of these documents. For Cisco IOS Release 12.2 T and 12.2 S implementation of these features, refer to the Cisco IOS Release 12.2 versions of these documents.

Supported Platforms

The IPSec MIB feature is supported on the following platforms in Cisco IOS Release 12.1(4)E:

- Cisco 7100 series
- Cisco 7200 series
- Cisco 7500 series (RSP7000 and 7500)

The IPSec MIB feature is supported on the following platforms in Cisco IOS Release 12.2(4)T:

- Cisco 800 series (800, 805, 806, 820, 827, 828)
- Cisco 900 series
- Cisco 1600 and 1600R series
- Cisco 1700 series (1710, 1720, 1750, 1751, 1760)
- Cisco 2400 series
- Cisco 2600 and 2600XM series
- Cisco 3600 series (Cisco 3620, 3640, and 3660)

- Cisco 3745
- Cisco 4000
- Cisco 4500
- Cisco 5300 series
- Cisco 5400 series
- Cisco 5800 series
- Cisco 7100 series
- Cisco 7200 series
- Cisco 7400 series
- Cisco 7500 series (Cisco IOS Release 12.2(4)T2 and later releases)
- Cisco 7700 series
- Cisco MC3810
- Cisco uBR900 series (uBR900, uBR904, uBR905, uBR910, uBR920, uBR925)
- Cisco uBR7200

The IPSec MIB feature is supported on the following platforms in Cisco IOS Release 12.2(14)S:

- Cisco 7200 series
- Cisco 7400 series
- Cisco 7500 series

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

The following MIBs are supported by the IPSec—SNMP Support feature:

- CISCO-IPSEC-FLOW-MONITOR- MIB
- CISCO-IPSEC-MIB
- CISCO-IPSEC-POLICY-MAP-MIB

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

RFCs

No new or modified RFCs are supported by this feature.

Configuration Tasks

See the following sections for configuration tasks for the IPSec—SNMP Support feature. Each task in the list is identified as either required or optional:

- [Enabling IPSec SNMP Notifications](#) (required)
- [Configuring IPSec Failure History Table Size](#) (optional)
- [Configuring IPSec Tunnel History Table Size](#) (optional)

Enabling IPSec SNMP Notifications

To enable a router to send IPSec trap or inform notifications to a specified host, use the following commands in global configuration mode:

	Command	Purpose
Step 1	Router(config)# snmp-server enable traps ipsec cryptomap [add delete attach detach]	Enables a router to send IPSec SNMP notifications.
Step 2	Router(config)# snmp-server enable traps isakmp [policy {add delete} tunnel {start stop}]	Enables a router to send IPSec ISAKMP SNMP notifications.
Step 3	Router(config)# snmp-server host host-address traps community-string ipsec	Specifies the recipient of IPSec SNMP notification operations.

For more information on configuring SNMP, refer to the chapter “Configuring SNMP Support” in the *Cisco IOS Configuration Fundamentals Configuration Guide*.

Configuring IPSec Failure History Table Size

The default failure history table size is 200. To change the size of the failure history table, use the following command in global configuration mode:

Command	Purpose
Router(config)# crypto mib ipsec flowmib history failure size number	Changes the size of the IPSec failure history table.

Configuring IPSec Tunnel History Table Size

The default tunnel history table size is 200. To change the size of the tunnel history table, use the following command in global configuration mode:

Command	Purpose
Router(config)# crypto mib ipsec flowmib history tunnel size number	Changes the size of the IPSec tunnel history table.

Verifying IPSec MIB Configuration

To verify that the IPSec MIB feature is configured properly, perform the following tasks:

- Enter the **show crypto mib ipsec flowmib history failure size** privileged EXEC command to display the size of the failure history table:

```
Router# show crypto mib ipsec flowmib history failure size
IPSec Failure Window Size: 140
```

- Enter the **show crypto mib ipsec flowmib history tunnel size** privileged EXEC command to display the size of the tunnel history table:

```
Router# show crypto mib ipsec flowmib history tunnel size
IPSec History Window Size: 130
```
- Enter the **show crypto mib ipsec flowmib version** privileged EXEC command to display the MIB version used by the management applications to identify the feature set:

```
Router# show crypto mib ipsec flowmib version
IPSec Flow MIB version: 1
```
- Enter the **debug crypto mib** command to display the IPSec MIB debug message notifications:

```
Router# debug crypto mib
Crypto IPSec Mgmt Entity debugging is on
```

Monitoring and Maintaining IPSec MIB

To monitor the status of IPSec MIB information, use any of the following commands in EXEC mode:

Command	Purpose
Router# show crypto mib ipsec flowmib history failure size	Displays the size of the IPSec failure history table.
Router# show crypto mib ipsec flowmib history tunnel size	Displays the size of the IPSec tunnel history table.
Router# show crypto mib ipsec flowmib version	Displays the IPSec Flow MIB version used by the router.

Configuration Examples

This section provides the following configuration examples:

- [Enabling IPSec Notifications Examples](#)
- [Specifying History Table Size Examples](#)

Enabling IPSec Notifications Examples

In the following example, IPSec notifications are enabled:

```
snmp-server enable traps ipsec isakmp
```

In the following example, the router is configured to send IPSec notifications to the host nms1.cisco.com:

```
snmp-server host nms1.cisco.com public ipsec isakmp
Translating "nms1.cisco.com"...domain server (171.00.0.01) [OK]
```

Specifying History Table Size Examples

In the following example, the specified failure history table size is 140:

```
crypto mib ipsec flowmib history failure size 140
```

In the following example, the specified tunnel history table size is 130:

```
crypto mib ipsec flowmib history tunnel size 130
```

Command Reference

This section documents new and modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

- [crypto mib ipsec flowmib history failure size](#)
- [crypto mib ipsec flowmib history tunnel size](#)
- [debug crypto mib](#)
- [show crypto mib ipsec flowmib history failure size](#)
- [show crypto mib ipsec flowmib history tunnel size](#)
- [show crypto mib ipsec flowmib version](#)
- [snmp-server enable traps ipsec](#)
- [snmp-server enable traps isakmp](#)
- [snmp-server host](#)

crypto mib ipsec flowmib history failure size

To change the size of the IP Security (IPSec) MIB failure history table, use the **crypto mib ipsec flowmib history failure size** command in global configuration mode.

crypto mib ipsec flowmib history failure size *number*

Syntax Description	<i>number</i>	Size of the failure history table.
--------------------	---------------	------------------------------------

Defaults If this command is not used, the default table size is 200.

Command Modes Global configuration

Command History	Release	Modification
	12.1(4)E	This command was introduced.
	12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Usage Guidelines Use the **crypto mib ipsec flowmib history failure size** command to change the size of a failure history table. If you do not configure the size of a failure history table, the default of 200 will be implemented.

A failure history table stores the reason for tunnel failure and the time failure occurred. A failure history table can be used as a simple method to distinguish between a normal and an abnormal tunnel termination. That is, if a tunnel entry in the tunnel history table has no associated failure record, the tunnel must have terminated normally. However, every failure does not correspond to a tunnel. Supported setup failures are recorded in the failure table, but a history table is not associated because a tunnel was never set up.

Examples The following example shows the size of a failure history table configured to be 140:

```
crypto mib ipsec flowmib history failure size 140
```

Related Commands	Command	Description
	crypto mib ipsec flowmib history tunnel size	Changes the size of the IPSec tunnel history table.
	show crypto mib ipsec flowmib history failure size	Displays the size of the IPSec failure history table.

crypto mib ipsec flowmib history tunnel size

To change the size of the IP Security (IPSec) tunnel history table, use the **crypto mib ipsec flowmib history tunnel size** command in global configuration mode.

crypto mib ipsec flowmib history tunnel size *number*

Syntax Description	<i>number</i>	Size of the tunnel history table.
---------------------------	---------------	-----------------------------------

Defaults The default table size is 200.

Command Modes Global configuration

Command History	Release	Modification
	12.1(4)E	This command was introduced.
	12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Usage Guidelines Use the **crypto mib ipsec flowmib history tunnel size** command to change the size of a tunnel history table. If you do not configure the size of a tunnel history table, the default of 200 will be implemented.

A tunnel history table stores the attribute and statistics records, which contain the attributes and the last snapshot of the traffic statistics of a given tunnel. A tunnel history table accompanies a failure table, so you can display the complete history of a given tunnel. However, a tunnel history table does not accompany every failure table because every failure does not correspond to a tunnel. Thus, supported setup failures are recorded in the failure table, but an associated history table is not recorded because a tunnel was never set up.

As an optimization, a tunnel endpoint table can be combined with a tunnel history table. However, if a tunnel endpoint table is combined, all three tables (the failure history table, tunnel history table, and the endpoint table) must remain the same size even though the MIB allows each table to be distinct.

Examples The following example shows the size of a tunnel history table configured to be 130:

```
crypto mib ipsec flowmib history tunnel size 130
```

Related Commands	Command	Description
	crypto mib ipsec flowmib history failure size	Changes the size of the IPSec failure history table.
	show crypto mib ipsec flowmib history tunnel size	Displays the size of the IPSec tunnel history table.

debug crypto mib

To display debug messages for the IP Security (IPSec) MIB subsystem, use the **debug crypto mib** command in privileged EXEC mode. To disable the IPSec MIB debug message notifications, use the **no** form of this command.

debug crypto mib

no debug crypto mib

Syntax Description This command has no arguments or keywords.

Defaults Message notification debugging is not enabled.

Command Modes Privileged EXEC

Release	Modification
12.1(4)E	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Examples The following example shows IPSec MIB debug message notification being enabled:

```
Router# debug crypto mib

Crypto IPSec Mgmt Entity debugging is on
```

Command	Description
show crypto mib ipsec flowmib history failure size	Displays the size of the IPSec failure history table.
show crypto mib ipsec flowmib history tunnel size	Displays the size of the IPSec tunnel history table.
show crypto mib ipsec flowmib version	Displays the IPSec Flow MIB version used by the router.

show crypto mib ipsec flowmib history failure size

To display the size of the IP Security (IPSec) failure history table, use the **show crypto mib ipsec flowmib history failure size** command in privileged EXEC mode.

show crypto mib ipsec flowmib history failure size

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(4)E	This command was introduced.
	12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Usage Guidelines Use the **show crypto mib ipsec flowmib history failure size** command to display the size of the failure history table.

Examples The following is sample output from the **show crypto mib ipsec flowmib history failure size** command:

```
Router# show crypto mib ipsec flowmib history failure size

IPSec Failure Window size: 140
```

Related Commands	Command	Description
	crypto mib ipsec flowmib history failure size	Changes the size of the IPSec failure history table.
	show crypto mib ipsec flowmib version	Displays the IPSec Flow MIB version used by the router.

show crypto mib ipsec flowmib history tunnel size

To display the size of the IP Security (IPSec) tunnel history table, use the **show crypto mib ipsec flowmib history tunnel size** command in privileged EXEC mode.

show crypto mib ipsec flowmib history tunnel size

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(4)E	This command was introduced.
	12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Usage Guidelines Use the **show crypto mib ipsec flowmib history tunnel size** command to display the size of the tunnel history table.

Examples The following is sample output from the **show crypto mib ipsec flowmib history tunnel size** command:

```
Router# show crypto mib ipsec flowmib history tunnel size

IPSec History Window Size: 130
```

Related Commands	Command	Description
	crypto mib ipsec flowmib history tunnel size	Changes the size of the IPSec tunnel history table.
	show crypto mib ipsec flowmib version	Displays the IPSec Flow MIB version used by the router.

show crypto mib ipsec flowmib version

To display the IP Security (IPSec) MIB version used by the router, use the **show crypto mib ipsec flowmib version** command in privileged EXEC mode.

show crypto mib ipsec flowmib version

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(4)E	This command was introduced.
	12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Usage Guidelines Use the **show crypto mib ipsec flowmib version** command to display the MIB version used by the management applications to identify the feature set.



Note

The MIB version can also be obtained by querying the MIB element cipSecMibLevel using Simple Network Management Protocol (SNMP).

Examples The following is sample output from the **show crypto mib ipsec flowmib version** command:

```
Router# show crypto mib ipsec flowmib version

IPSec Flow MIB version: 1
```

Related Commands	Command	Description
	show crypto mib ipsec flowmib history failure size	Displays the size of the IPSec failure history table.
	show crypto mib ipsec flowmib history tunnel size	Displays the size of the IPSec tunnel history table.

snmp-server enable traps ipsec

To enable the router to send IP Security (IPSec) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps ipsec** command in global configuration mode. To disable IPSec SNMP notifications, use the **no** form of this command.

```
snmp-server enable traps ipsec [cryptomap [add | delete | attach | detach] | tunnel [start | stop] | too-many-sas]
```

```
no snmp-server enable traps ipsec [cryptomap [add | delete | attach | detach] | tunnel [start | stop] | too-many-sas]
```

Syntax Description	
cryptomap add	(Optional) Enables the generation of cipsCryptomapAdded { cipsMIBNotifications 3 } notifications as defined in the CISCO-IPSEC-MIB. These notifications are generated when a new cryptomap is added to the specified cryptomap set.
cryptomap delete	(Optional) Enables the generation of cipsCryptomapDeleted { cipsMIBNotifications 4 } notifications as defined in the CISCO-IPSEC-MIB. These notifications are generated when a cryptomap is removed from the specified cryptomap set.
cryptomap attach	(Optional) Enables the generation of cipsCryptomapSetAttached{ cipsMIBNotifications 5 } notifications as defined in the CISCO-IPSEC-MIB. These notifications are generated when a cryptomap set is attached to an active interface of the managed entity.
cryptomap detach	(Optional) Enables the generation of cipsCryptomapSetDetached{ cipsMIBNotifications 6 } notifications as defined in the CISCO-IPSEC-MIB. These notifications are generated when a cryptomap set is detached from an interface to which it was previously bound.
tunnel start	(Optional) Enables the generation of notifications for cipSecTunnelStart { cipSecMIBNotifications 7 } events, as defined by in the CISCO-IPSEC-FLOW-MONITOR-MIB. These notifications are generated when an IPsec Phase-2 tunnel becomes active.
tunnel stop	(Optional) Enables the generation of notifications for cipSecTunnelStop { cipSecMIBNotifications 8 } events, as defined in the CISCO-IPSEC-FLOW-MONITOR-MIB. These notifications are generated when an IPsec Phase-2 tunnel becomes inactive.
too-many-sas	(Optional) Enables the generation of notifications for cipsTooManySAs { cipsMIBNotifications 7 } events, as defined in the CISCO-IPSEC-MIB.my. These notifications are generated when an attempt to make a new security association (SA) is made but there is insufficient memory on the device.

Defaults

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History	Release	Modification
	12.2(8)T	This command was introduced.
	12.1(11b)E	This command was integrated into Cisco IOS Release 12.1(11b)E.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Usage Guidelines SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

A cryptomap is a table that maps an IPSec Phase-2 tunnel to the corresponding IPSec Policy element.

For a complete description of the notification types, and additional MIB functions, refer to the CISCO-IP-SEC.my and CISCO-IPSEC-FLOW-MONITOR-MIB.my files, available on Cisco.com through:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

The **snmp-server enable traps ipsec** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

In the following example, the router is configured to send IPSec MIB inform notifications to the host nms.cisco.com using the community string named public:

```
snmp-server enable traps ipsec
snmp-server host nms.cisco.com informs public ipsec
```

Related Commands	Command	Description
	snmp-server enable traps isakmp	Controls the sending of IPSec Internet Security Association and Key Exchange Protocol (ISAKMP) SNMP notifications
	snmp-server host	Specifies the recipient of an SNMP notification operation.
	snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps isakmp

To enable the router to send IP Security (IPSec) Internet Security Association and Key Exchange Protocol (ISAKMP) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps isakmp** command in global configuration mode. To disable IPSec SNMP notifications, use the **no** form of this command.

snmp-server enable traps isakmp [policy {add | delete} | tunnel {start | stop}]

no snmp-server enable traps isakmp [policy {add | delete} | tunnel {start | stop}]

Syntax Description		
policy add	(Optional) Enables the generation of notifications for cipsIsakmpPolicyAdded { cipsMIBNotifications 1 } events, as defined in the CISCO-IPSEC-MIB. These notifications are generated when a new ISAKMP policy element is defined on the managed entity. The context of the event includes the updated number of ISAKMP policy elements currently available.	
policy delete	(Optional) Enables the generation of notifications for cipsIsakmpPolicyDeleted { cipsMIBNotifications 2 } events, as defined in the CISCO-IPSEC-MIB. These notifications are generated when an existing ISAKMP policy element is deleted on the managed entity. The context of the event includes the updated number of ISAKMP policy elements currently available.	
tunnel start	(Optional) Enables the generation of notifications for cikeTunnelStart { cipSecMIBNotifications 1 } events, as defined in the CISCO-IPSEC-FLOW-MONITOR-MIB.my. These notifications are generated when an IPsec Phase-1 IKE Tunnel becomes active.	
tunnel stop	(Optional) Enables the generation of notifications for cikeTunnelStop { cipSecMIBNotifications 2 } events, as defined in the CISCO-IPSEC-FLOW-MONITOR-MIB.my. These notifications are generated when an IPsec Phase-1 IKE Tunnel becomes inactive.	

Defaults

SNMP notifications are disabled by default.

If no keywords are specified, all available ISAKMP traps are enabled (or disabled if the **no** form is used).

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.1(11b)E	This command was integrated into Cisco IOS Release 12.1(11b)E
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both ISAKMP trap and inform requests.

For a complete description of these notifications and additional MIB functions, see the CISCO-IPSEC-MIB.my and CISCO-IPSEC-FLOW-MONITOR-MIB.my files, available on Cisco.com through:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

The **snmp-server enable traps isakmp** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

In the following example, the router is configured to send IPsec MIB inform notifications to the host nms.cisco.com using the community string named public:

```
snmp-server enable traps isakmp
snmp-server host nms.cisco.com informs public ipsec
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface (and hence the corresponding IP address) from which an SNMP trap should originate.

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, use the **no** form of this command.

```
snmp-server host host-address [traps | informs] [version {1 | 2c | 3 [auth | noauth | priv]}]
community-string [udp-port port] [notification-type]
```

```
no snmp-server host host-address [traps | informs]
```

Syntax Description	
<i>host-address</i>	Name or Internet address of the host (the targeted recipient).
traps	(Optional) Sends SNMP traps to this host.
informs	(Optional) Sends SNMP informs to this host.
version	(Optional) Version of the SNMP used to send the traps. Version 3 is the most secure model, because it allows packet encryption with the priv keyword. If you use the version keyword, one of the following keywords must be specified: <ul style="list-style-type: none"> • 1—SNMP Version 1. This option is not available with informs. • 2c—SNMP Version 2C. • 3—SNMP Version 3. The following three optional keywords can follow the 3 keyword: <ul style="list-style-type: none"> – auth—(Optional) Enables Message Digest 5 (MD5) algorithm and Secure Hash Algorithm (SHA) packet authentication. – noauth—(Optional) The noAuthNoPriv security level. This is the default if the [auth noauth priv] keyword choice is not specified. – priv—(Optional) Enables Data Encryption Standard (DES) packet encryption (also called “privacy”).
<i>community-string</i>	Password-like community string sent with the notification operation. Though you can set this string using the snmp-server host command by itself, we recommend you define this string using the snmp-server community command prior to using the snmp-server host command.
udp-port <i>port</i>	(Optional) User Datagram Protocol port of the host to use. The default is 162.

<i>notification-type</i>	<p>(Optional) Type of notification to be sent to the host. If no type is specified, all notifications are sent. The notification type can be one or more of the following keywords:</p> <ul style="list-style-type: none"> • bgp—Sends Border Gateway Protocol (BGP) state change notifications. • calltracker—Sends Call Tracker notifications. • config—Sends configuration notifications. • dspu—Sends downstream physical unit (DSPU) notifications. • entity—Sends Entity MIB modification notifications. • envmon—Sends Cisco enterprise-specific environmental monitor notifications when an environmental threshold is exceeded. • frame-relay—Sends Frame Relay notifications. • hsrp—Sends Hot Standby Routing Protocol (HSRP) notifications. • ipsec—Sends IP Security (IPSec) notifications. • isdn—Sends ISDN notifications. • llc2—Sends Logical Link Control, type 2 (LLC2) notifications. • repeater—Sends standard repeater (hub) notifications. • rsrb—Sends remote source-route bridging (RSRB) notifications. • rsvp—Sends Resource Reservation Protocol (RSVP) notifications. • rtr—Sends Service Assurance Agent (response time reporter) notifications. • sdlc—Sends Synchronous Data Link Control (SDLC) notifications. • sdllc—Sends SDLC Logical Link Control notifications. • snmp—Sends SNMP notifications (as defined in RFC 1157). • stun—Sends serial tunnel (STUN) notifications. • syslog—Sends error message notifications (Cisco Syslog MIB). Specify the level of messages to be sent with the logging history level command. • tty—Sends Cisco enterprise-specific notifications when a TCP connection closes. • x25—Sends X.25 event notifications.
--------------------------	--

Defaults

This command is disabled by default. No notifications are sent.

If you enter this command with no keywords, the default is to send all trap types to the host. No informs will be sent to this host.

If no **version** keyword is present, the default is version 1. The **no snmp-server host** command with no keywords will disable traps, but not informs, to the host. In order to disable informs, use the **no snmp-server host informs** command.

If the **version 3** keyword is present and the [**auth** | **noauth** | **priv**] keyword choice is not specified, **noauth** is the default.

If the **udp-port** keyword is not present, the default UDP port is port 162.

**Note**

If the *community-string* is not defined using the **snmp-server community** command prior to using this command, the default form of the **snmp-server community** command will automatically be inserted into the configuration. The password (*community-string*) used for this automatic configuration of the **snmp-server community** command will be the same as specified in the **snmp-server host** command. This is the default behavior for Cisco IOS Release 12.0(3) and later releases.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(3)T	The following keywords were added: <ul style="list-style-type: none"> • version 3 [auth noauth priv] • hsrp
11.3(1) MA	The voice notification-type keyword was added.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.
12.1(3)T	The calltracker notification-type keyword was added for the Cisco AS5300 and AS5800 platforms.
12.1(5a)E	The ipsec notification-type keyword was added.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response protocol data unit. If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely to reach their intended destination.

However, informs consume resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once, but an inform may be retried several times. The retries increase traffic and contribute to higher overhead on the network.

If you do not enter an **snmp-server host** command, no notifications are sent. In order to configure the router to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no keywords, all trap types are enabled for the host.

In order to enable multiple hosts, you must issue a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

When multiple **snmp-server host** commands are given for the same host and kind of notification (trap or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command will be in effect. For example, if you enter an **snmp-server host informs** command for a host and then enter another **snmp-server host informs** command for the same host, the second command will replace the first.

The **snmp-server host** command is used in conjunction with the **snmp-server enable traps** command. Use the **snmp-server enable traps** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable traps** command and the **snmp-server host** command for that host must be enabled.

The availability of a specific notification type depends on the router type and Cisco IOS software features supported on the router. For example, the envmon notification type is available only if the environmental monitor is part of the system. To display what notification types are available on your system, use the help command **?** at the end of the **snmp-server host** command.

Examples

If you want to configure a unique SNMP community string for traps, but you want to prevent SNMP polling access with this string, the configuration should include an access list. In the following example, the community string is defined as comaccess and the access list is numbered 10:

```
snmp-server community comaccess ro 10
snmp-server host 172.20.2.160 comaccess
access-list 10 deny any
```

In the following example, all available SNMP traps are enabled to be sent to the host specified by the name myhost.cisco.com. The community string is defined as comaccess.

```
snmp-server enable traps
snmp-server host myhost.cisco.com comaccess snmp
```

In the following example, IPSec MIB traps are enabled to be sent to the host nms.cisco.com using the community string defined as public:

```
snmp-server enable traps ipsec
snmp-server host nms.cisco.com public ipsec
```

Related Commands

Command	Description
snmp-server enable traps	Enables the router to send SNMP traps.
snmp-server informs	Specifies inform request options.
snmp-server trap-source	Specifies the interface (and hence the corresponding IP address) from which an SNMP trap should originate.
snmp-server trap-timeout	Defines how often to try resending trap messages on the retransmission queue.
snmp trap link-status	Enables SNMP trap notifications to be generated when a specific port is brought up or down.

Glossary

CA—certificate authority. A certificate authority (CA) is an entity in a network that issues and manages security credentials and public keys (in the form of X509v3 certificates) for message encryption. As part of a public key infrastructure (PKI), a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can then issue a certificate. Certificates generally include the owner's public key, the expiration date of the certificate, the owner's name, and other information about the public key owner.

IP Security—See IPSec.

IPSec—Internet Protocol Security. A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer. IPSec uses Internet Key Exchange (IKE) to handle negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPSec. IPSec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

Management Information Base—See MIB.

MIB—Management Information Base. Database of network management information that is used and maintained by a network management protocol such as Simple Network Management Protocol (SNMP) or Common Management Information Protocol (CMIP). The value of a MIB object can be changed or retrieved using SNMP or CMIP commands, usually through a graphical user interface (GUI) network management system (NMS). MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

Simple Network Management Protocol—See SNMP.

SNMP—Simple Network Management Protocol. An application-layer protocol that provides a message format for communication between SNMP managers and agents.

trap—Message sent by an SNMP agent to a network management system, console, or terminal to indicate the occurrence of a significant event, such as a specifically defined condition or a threshold that was reached.

