



IPsec Management Configuration Guide Cisco IOS Release 12.4

Americas Headquarters

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



CONTENTS

IP Security VPN Monitoring	1
Finding Feature Information	1
Prerequisites for IP Security VPN Monitoring	1
Restrictions for IP Security VPN Monitoring	2
Information About IPsec VPN Monitoring	2
Background Crypto Sessions	2
Per-IKE Peer Description	2
Summary Listing of Crypto Session Status	2
Syslog Notification for Crypto Session Up or Down Status	3
IKE and IPsec Security Exchange Clear Command	3
How to Configure IP Security VPN Monitoring	3
Adding the Description of an IKE Peer	3
Verifying Peer Descriptions	4
Clearing a Crypto Session	5
Configuration Examples for IP Security VPN Monitoring	6
show crypto session Command Output Examples	6
Additional References	7
Feature Information for IP Security VPN Monitoring	7
IPsec SNMP Support	9
Finding Feature Information	9
Restrictions for IPsec-SNMP Support	9
Information About IPsec-SNMP Support	10
IPsec-SNMP Support	10
VPN Device Manager	10
How to Configure IPsec-SNMP Support	11
Enabling IPsec SNMP Notifications	11
Configuring IPsec Failure History Table Size	12
Configuring IPsec Tunnel History Table Size	13
Verifying IPsec MIB Configuration	13

Monitoring and Maintaining IPsec MIB	14
Configuration Examples for IPsec-SNMP Support	15
Enabling IPsec Notifications Examples	15
Specifying History Table Size Examples	15
Additional References	16
Feature Information for IPsec-SNMP Support	16
Glossary	18
IPsec VPN Accounting	19
Finding Feature Information	19
Prerequisites for IPsec VPN Accounting	19
Information About IPsec VPN Accounting	19
RADIUS Accounting	20
RADIUS Start Accounting	20
RADIUS Stop Accounting	21
RADIUS Update Accounting	22
IKE and IPsec Subsystem Interaction	22
Accounting Start	22
Accounting Stop	23
Accounting Updates	24
How to Configure IPsec VPN Accounting	24
Configuring IPsec VPN Accounting	24
Configuring Accounting Updates	29
Troubleshooting for IPsec VPN Accounting	30
Configuration Examples for IPsec VPN Accounting	30
Accounting and ISAKMP-Profile Example	31
Accounting Without ISAKMP Profiles Example	32
Additional References	34
Feature Information for IPsec VPN Accounting	35
Glossary	36
VPN Device Manager Client for Cisco IOS Software XSM Configuration	39
Feature Overview	39
XML Subscription Manager	40
CLI Commands for VDM	40
Related Features and Technologies	41
Related Documents	41

Finding Feature Information	41
Supported Standards MIBs and RFCs	42
Prerequisites	42
Configuring VDM	42
Enabling the XSM Server for VDM	42
Configuring XSM Privilege Levels for XRDs	43
Disabling the XSM Server for VDM	43
Verifying VDM Status on the XSM Server	43
Clearing XSM Client Sessions	44
Configuring XSM Statistics Collection	44
Configuration Examples for VDM	44
Enabling the XSM Server for VDM Example	44
Configuring XSM Privilege Levels for XRDs Example	45
Disabling the XSM Server for VDM Example	45
Configuring XSM Statistics Collection Example	45
Feature Information for VPN Device Manager Client	45
Glossary	46



IP Security VPN Monitoring

The IP Security VPN Monitoring feature provides the following Virtual Private Network (VPN) session monitoring enhancements to troubleshoot and monitor the end-user interface:

- Ability to specify an Internet Key Exchange (IKE) peer description in the configuration file
- Summary listing of crypto session status
- Syslog notification for crypto session up or down status
- Ability to clear both IKE and IP Security (IPSec) security associations (SAs) using one command-line interface (CLI)
- [Finding Feature Information, page 1](#)
- [Prerequisites for IP Security VPN Monitoring, page 1](#)
- [Restrictions for IP Security VPN Monitoring, page 2](#)
- [Information About IPSec VPN Monitoring, page 2](#)
- [How to Configure IP Security VPN Monitoring, page 3](#)
- [Configuration Examples for IP Security VPN Monitoring, page 6](#)
- [Additional References, page 7](#)
- [Feature Information for IP Security VPN Monitoring, page 7](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for IP Security VPN Monitoring

- You should be familiar with IPSec and encryption.
- Your router must support IPSec, and before using the IP Security VPN Monitoring feature, you must have configured IPSec on your router.

Restrictions for IP Security VPN Monitoring

- You must be running Cisco IOS k8 or k9 crypto images on your router.

Information About IPsec VPN Monitoring

- [Background Crypto Sessions, page 2](#)
- [Per-IKE Peer Description, page 2](#)
- [Summary Listing of Crypto Session Status, page 2](#)
- [Syslog Notification for Crypto Session Up or Down Status, page 3](#)
- [IKE and IPsec Security Exchange Clear Command, page 3](#)

Background Crypto Sessions

A crypto session is a set of IPsec connections (flows) between two crypto endpoints. If the two crypto endpoints use IKE as the keying protocol, they are IKE peers to each other. Typically, a crypto session consists of one IKE security association (for control traffic) and at least two IPsec security associations (for data traffic--one per each direction). There may be duplicated IKE security associations (SAs) and IPsec SAs or duplicated IKE SAs or IPsec SAs for the same session in the duration of rekeying or because of simultaneous setup requests from both sides.

Per-IKE Peer Description

The Per-IKE Peer Description function allows you to enter a description of your choosing for an IKE peer. (Before Cisco IOS Release 12.3(4)T, you could use only the IP address or fully qualified domain name [FQDN] to identify the peer; there was no way to configure a description string.) The unique peer description, which can include up to 80 characters, can be used whenever you are referencing that particular IKE peer. To add the peer description, use the **description** command.



Note

IKE peers that “sit” behind a Network Address Translation (NAT) device cannot be uniquely identified; therefore, they have to share the same peer description.

The primary application of this description field is for monitoring purposes (for example, when using **show** commands or for logging [syslog messages]). The description field is purely informational (for example, it cannot act as a substitute for the peer address or FQDN when defining crypto maps).

Summary Listing of Crypto Session Status

You can get a list of all the active VPN sessions by entering the **show crypto session** command. The listing will include the following:

- Interface
- IKE peer description, if available
- IKE SAs that are associated with the peer by whom the IPsec SAs are created
- IPsec SAs serving the flows of a session

Multiple IKE or IPsec SAs may be established for the same peer (for the same session), in which case IKE peer descriptions will be repeated with different values for the IKE SAs that are associated with the peer and for the IPsec SAs that are serving the flows of the session.

You can also use the **show crypto session detail** variant of this command to obtain more detailed information about the sessions.

Syslog Notification for Crypto Session Up or Down Status

The Syslog Notification for Crypto Session Up or Down Status function provides syslog notification every time the crypto session comes up or goes down.

The following is a sample syslog notification showing that a crypto session is up:

```
%CRYPTO-5-SESSION_STATUS: Crypto session is UP. Peer 10.6.6.1:500 fvrf=name10
ivrf=name20 Description: SJC24-2-VPN-Gateway Id: 10.5.5.2
```

The following is a sample syslog notification showing that a crypto session is down:

```
%CRYPTO-5-SESSION_STATUS: Crypto session is DOWN. Peer 10.6.6.1:500 fvrf=name10
ivrf=name20 Description: SJC24-2-VPN-Gateway Id: 10.5.5.2
```

IKE and IPsec Security Exchange Clear Command

In previous IOS versions, there was no single command to clear both IKE and IPsec connections (that is, SAs). Instead, you had to use the **clear crypto isakmp** command to clear IKE and the **clear crypto ipsec** command to clear IPsec. The new **clear crypto session** command allows you to clear both IKE and IPsec with a single command. To clear a specific crypto session or a subset of all the sessions (for example, a single tunnel to one remote site), you need to provide session-specific parameters, such as a local or remote IP address, a local or remote port, a front door VPN routing and forwarding (FVRF) name, or an inside VRF (IVRF) name. Typically, the remote IP address will be used to specify a single tunnel to be deleted.

If a local IP address is provided as a parameter when you use the **clear crypto session** command, all the sessions (and their IKE SAs and IPsec SAs) that share the IP address as a local crypto endpoint (IKE local address) will be cleared. If you do not provide a parameter when you use the **clear crypto session** command, all IPsec SAs and IKE SAs that are in the router will be deleted.

How to Configure IP Security VPN Monitoring

- [Adding the Description of an IKE Peer, page 3](#)
- [Verifying Peer Descriptions, page 4](#)
- [Clearing a Crypto Session, page 5](#)

Adding the Description of an IKE Peer

To add the description of an IKE peer to an IPsec VPN session, perform the following steps.

SUMMARY STEPS

1. enable
2. configure terminal
3. crypto isakmp peer {ip-addressip-address }
4. description

DETAILED STEPS

Command or Action	Purpose
Step 1 enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2 configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3 crypto isakmp peer {ip-addressip-address } Example: <pre>Router (config)# crypto isakmp peer address 10.2.2.9</pre>	Enables an IPsec peer for IKE querying of authentication, authorization, and accounting (AAA) for tunnel attributes in aggressive mode and enters ISAKMP peer configuration mode.
Step 4 description Example: <pre>Router (config-isakmp-peer)# description connection from site A</pre>	Adds a description for an IKE peer.

Verifying Peer Descriptions

To verify peer descriptions, use the **show crypto isakmp peer** command.

SUMMARY STEPS

1. enable
2. show crypto isakmp peer

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>show crypto isakmp peer</p> <p>Example:</p> <pre>Router# show crypto isakmp peer</pre>	<p>Displays peer descriptions.</p>

Examples

The following output example verifies that the description “connection from site A” has been added for IKE peer 10.2.2.9:

```
Router# show crypto isakmp peer
Peer: 10.2.2.9 Port: 500
  Description: connection from site A
  flags: PEER_POLICY
```

When the peer at address 10.2.2.9 connects and the session comes up, the syslog status will be shown as follows:

```
%CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP. Peer 10.2.2.9:500 Description: connection
from site A Id: ezvpn
```

The following output example verifies that the description “connection from site A” has been added for IKE peer 10.2.2.9:

```
Router# show crypto isakmp peer
Peer: 10.2.2.9 Port: 500
  Description: connection from site A
  flags: PEER_POLICY
```

When the peer at address 10.2.2.9 connects and the session comes up, the syslog status will be shown as follows:

```
%CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP. Peer 10.2.2.9:500 Description: connection
from site A Id: ezvpn
```

Clearing a Crypto Session

To clear a crypto session, use the **clear crypto session** command from the router command line. No configuration statements are required in the configuration file to use this command.

SUMMARY STEPS

1. **enable**
2. **clear crypto session**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	clear crypto session Example: Router# clear crypto session	Deletes crypto sessions (IPSec and IKE SAs).

Configuration Examples for IP Security VPN Monitoring

- [show crypto session Command Output Examples, page 6](#)

show crypto session Command Output Examples

The following is sample output for the **show crypto session** output without the **detail** keyword:

```
Router# show crypto session
Crypto session current status
Interface: FastEthernet0/1
Session status: UP-ACTIVE
Peer: 172.0.0.2/500
  IKE SA: local 172.0.0.1/500 remote 172.0.0.2/500 Active
  IPSEC FLOW: permit ip 10.10.10.0/255.255.255.0 10.30.30.0/255.255.255.0
    Active SAs: 2, origin: crypto map
```

The following is sample output using the **show crypto session command and the detail** keyword:

```
Router# show crypto session detail
Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.1.1.3 port 500 fvrf: (none) ivrf: (none)
  Desc: this is my peer at 10.1.1.3:500 Green
  Phase1_id: 10.1.1.3
  IKE SA: local 10.1.1.4/500 remote 10.1.1.3/500 Active
    Capabilities:(none) connid:3 lifetime:22:03:24
  IPSEC FLOW: permit 47 host 10.1.1.4 host 10.1.1.3
    Active SAs: 0, origin: crypto map
    Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 0/0
    Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 0/0
  IPSEC FLOW: permit ip host 10.1.1.4 host 10.1.1.3
    Active SAs: 4, origin: crypto map
    Inbound:  #pkts dec'ed 4 drop 0 life (KB/Sec) 4605665/2949
    Outbound: #pkts enc'ed 4 drop 1 life (KB/Sec) 4605665/2949
```

Additional References

Related Documents

Related Topic	Document Title
IP security, encryption, and IKE	<ul style="list-style-type: none"> Configuring Internet Key Exchange for IPsec VPNs Configuring Security for VPNs with IPsec
Security commands	<i>Cisco IOS Security Command Reference</i>

MIBs

MIBs	MIBs Link
None.	<p>To locate and download MIBs for selected platforms, Cisco IOS software releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p>http://www.cisco.com/go/mibs</p>

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IP Security VPN Monitoring

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 **Feature Information for IP Security VPN Monitoring**

Feature Name	Releases	Feature Information
IP Security VPN Monitoring	12.3(4)T	<p>The IP Security VPN Monitoring feature provides the following Virtual Private Network (VPN) session monitoring enhancements to troubleshoot and monitor the end-user interface:</p> <ul style="list-style-type: none"> • Ability to specify an Internet Key Exchange (IKE) peer description in the configuration file • Summary listing of crypto session status • Syslog notification for crypto session up or down status • Ability to clear both IKE and IP Security (IPSec) security associations (SAs) using one command-line interface (CLI) <p>This feature was introduced in Cisco IOS Release 12.3(4)T.</p> <p>The following commands were introduced or modified: clear crypto session, description (isakmp peer), show crypto isakmp peers, show crypto session .</p>

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.



IPsec SNMP Support

The IPsec--SNMP Support feature can be used to learn the IPsec MIB feature version, enable and disable SNMP traps, and monitor and control the size of IPsec history tables.

- [Finding Feature Information, page 9](#)
- [Restrictions for IPsec-SNMP Support, page 9](#)
- [Information About IPsec-SNMP Support, page 10](#)
- [How to Configure IPsec-SNMP Support, page 11](#)
- [Configuration Examples for IPsec-SNMP Support, page 15](#)
- [Additional References, page 16](#)
- [Feature Information for IPsec-SNMP Support, page 16](#)
- [Glossary, page 18](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for IPsec-SNMP Support

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).

Information About IPsec-SNMP Support

- [IPsec-SNMP Support, page 10](#)
- [VPN Device Manager, page 10](#)

IPsec-SNMP Support

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.

VPN Device Manager

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.

See the VPN Device Manager Client for Cisco IOS Software (XSM Configuration) feature document for more information on Cisco VDM.

How to Configure IPsec-SNMP Support

- [Enabling IPsec SNMP Notifications](#), page 11
- [Configuring IPsec Failure History Table Size](#), page 12
- [Configuring IPsec Tunnel History Table Size](#), page 13
- [Verifying IPsec MIB Configuration](#), page 13
- [Monitoring and Maintaining IPsec MIB](#), page 14

Enabling IPsec SNMP Notifications

The following steps are used to enable a router to send IPsec trap or inform notifications to a specified host:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps ipsec cryptomap [add | delete | attach| detach]**
4. Router(config)# **snmp-server enable traps isakmp[policy{add | delete} | tunnel{start | stop}]**
5. **snmp-server host *host-address* traps *community-string* ipsec**

DETAILED STEPS

Command or Action	Purpose
Step 1 enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2 configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3 snmp-server enable traps ipsec cryptomap [add delete attach detach] Example: <pre>Router(config)# snmp-server enable traps ipsec cryptomap add</pre>	Enables a router to send IPsec SNMP notifications.

Command or Action	Purpose
<p>Step 4 Router(config)# snmp-server enable traps isakmp[policy{add delete} tunnel{start stop}]</p> <p>Example:</p> <pre>Router(config)# snmp-server enable traps isakmp</pre>	Enables a router to send IPsec ISAKMP SNMP notifications.
<p>Step 5 snmp-server host <i>host-address</i> traps <i>community-string</i> ipsec</p> <p>Example:</p> <pre>Router(config)# snmp-server host 10.10.10.1 traps community1 ipsec</pre>	Specifies the recipient of IPsec SNMP notification operations.

Configuring IPsec Failure History Table Size

Use the steps in this section to change the size of the failure history table. The default failure history table size is 200.

SUMMARY STEPS

1. enable
2. configure terminal
3. crypto mib ipsec flowmib history failure size *number*

DETAILED STEPS

Command or Action	Purpose
<p>Step 1 enable</p> <p>Example:</p> <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
<p>Step 2 configure terminal</p> <p>Example:</p> <pre>Router# configure terminal</pre>	Enters global configuration mode.

Command or Action	Purpose
Step 3 <code>crypto mib ipsec flowmib history failure size number</code> Example: <pre>Router(config)# crypto mib ipsec flowmib history failure size 50</pre>	Changes the size of the IPsec failure history table.

Configuring IPsec Tunnel History Table Size

Follow the steps in this section to change the size of the tunnel history table. The default tunnel history table size is 200.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `crypto mib ipsec flowmib history tunnel size number`

DETAILED STEPS

Command or Action	Purpose
Step 1 <code>enable</code> Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2 <code>configure terminal</code> Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3 <code>crypto mib ipsec flowmib history tunnel size number</code> Example: <pre>Router(config)# crypto mib ipsec flowmib history tunnel size 50</pre>	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

Use the steps in this section to monitor the status of IPsec MIB information.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **show crypto mib ipsec flowmib history failure size**
4. **show crypto mib ipsec flowmib history tunnel size**
5. **show crypto mib ipsec flowmib version**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.

Command or Action	Purpose
<p>Step 3 <code>show crypto mib ipsec flowmib history failure size</code></p> <p>Example:</p> <pre>Router# show crypto mib ipsec flowmib history failure size</pre>	Displays the size of the IPsec failure history table.
<p>Step 4 <code>show crypto mib ipsec flowmib history tunnel size</code></p> <p>Example:</p> <pre>Router# show crypto mib ipsec flowmib history tunnel size</pre>	Displays the size of the IPsec tunnel history table.
<p>Step 5 <code>show crypto mib ipsec flowmib version</code></p> <p>Example:</p> <pre>Router# show crypto mib ipsec flowmib version</pre>	Displays the IPsec Flow MIB version used by the router.

Configuration Examples for IPsec-SNMP Support

- [Enabling IPsec Notifications Examples, page 15](#)
- [Specifying History Table Size Examples, page 15](#)

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
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Security commands	<i>Cisco IOS Security Command Reference</i>
IPsec	Configuring Security for VPNs with IPsec
SNMP	<i>Cisco IOS Configuration Fundamentals Configuration Guide</i> and <i>Cisco IOS Configuration Fundamentals Command Reference</i>

MIBs

MIB	MIBs Link
<ul style="list-style-type: none"> • CISCO-IPSEC-FLOW-MONITOR- MIB • CISCO-IPSEC-MIB • CISCO-IPSEC-POLICY-MAP-MIB 	<p>To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p>http://www.cisco.com/go/mibs</p>

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IPsec-SNMP Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 2 **Feature Information for IPsec-SNMP Support**

Feature Name	Releases	Feature Information
IPsec-SNMP Support	12.1(4)E 12.1(5a)E 12.2(4)T 12.2(8)T 12.1(11b)E 12.2(14)S	<p>The IPsec--SNMP Support feature can be used to learn the IPsec MIB feature version, enable and disable SNMP traps, and monitor and control the size of IPsec history tables.</p> <p>This feature was introduced on the Cisco 7100, 7200, and 7500 series platforms in Cisco Release 12.1(4)E.</p> <p>Support for CISCO-IPSEC-FLOW-MONITOR-MIB notifications was added in Cisco IOS Release 12.1(5a)E.</p> <p>This feature was integrated into Cisco IOS Release 12.2(4)T.</p> <p>In Cisco IOS Releases 12.2(8)T, 12.1(11b)E, the following commands were added to enable and disable IP Security (IPsec) MIB notifications:</p> <ul style="list-style-type: none"> • snmp-server enable traps ipsec • snmp-server enable traps isakmp <p>This feature was integrated into Cisco IOS Release 12.2(14)S.</p> <p>The following commands were introduced or modified: 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.</p>

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.



IPsec VPN Accounting

The IPsec VPN Accounting feature allows a session to be accounted by indicating when the session starts and stops. A VPN session is defined as an Internet Key Exchange (IKE) security association (SA) and the one or more SA pairs that are created by the IKE SA. The session starts when the first IP Security (IPsec) pair is created and stops when all IPsec SAs are deleted. Session identifying information and session usage information is passed to the Remote Authentication Dial-In User Service (RADIUS) server through standard RADIUS attributes and vendor-specific attributes (VSAs).

- [Finding Feature Information, page 19](#)
- [Prerequisites for IPsec VPN Accounting, page 19](#)
- [Information About IPsec VPN Accounting, page 19](#)
- [How to Configure IPsec VPN Accounting, page 24](#)
- [Configuration Examples for IPsec VPN Accounting, page 30](#)
- [Additional References, page 34](#)
- [Feature Information for IPsec VPN Accounting, page 35](#)
- [Glossary, page 36](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for IPsec VPN Accounting

- You should understand how to configure RADIUS and authentication, authorization, and accounting (AAA) accounting.
- You should know how to configure IPsec accounting.

Information About IPsec VPN Accounting

- [RADIUS Accounting, page 20](#)

- [IKE and IPsec Subsystem Interaction, page 22](#)

RADIUS Accounting

For many large networks, it is required that user activity be recorded for auditing purposes. The method that is used most is RADIUS accounting.

RADIUS accounting allows for a session to be accounted for by indicating when the session starts and when it stops. Additionally, session identifying information and session usage information is passed to the RADIUS server through RADIUS attributes and VSAs.

- [RADIUS Start Accounting, page 20](#)
- [RADIUS Stop Accounting, page 21](#)
- [RADIUS Update Accounting, page 22](#)

RADIUS Start Accounting

The RADIUS Start packet contains many attributes that generally identify who is requesting the service and of what the property of that service consists. The table below represents the attributes required for the start.

Table 3 *RADIUS Accounting Start Packet Attributes*

RADIUS Attributes Value	Attribute	Description
1	user-name	Username used in extended authentication (XAUTH). The username may be NULL when XAUTH is not used.
4	nas-ip-address	Identifying IP address of the network access server (NAS) that serves the user. It should be unique to the NAS within the scope of the RADIUS server.
5	nas-port	Physical port number of the NAS that serves the user.
8	framed-ip-address	Private address allocated for the IP Security (IPsec) session.
40	acct-status-type	Status type. This attribute indicates whether this accounting request marks the beginning (start), the end (stop), or an update of the session.
41	acct-delay-time	Number of seconds the client has been trying to send a particular record.

RADIUS Attributes Value	Attribute	Description
44	acct-session-id	Unique accounting identifier that makes it easy to match start and stop records in a log file.
26	vrf-id	String that represents the name of the Virtual Route Forwarder (VRF).
26	isakmp-initiator-ip	Endpoint IP address of the remote Internet Key Exchange (IKE) initiator (V4).
26	isakmp-group-id	Name of the VPN group profile used for accounting.
26	isakmp-phase1-id	Phase 1 identification (ID) used by IKE (for example, domain name [DN], fully qualified domain name [FQDN], IP address) to help identify the session initiator.

RADIUS Stop Accounting

The RADIUS Stop packet contains many attributes that identify the usage of the session. Table 2 represents the additional attributes required for the RADIUS stop packet. It is possible that only the stop packet is sent without the start if configured to do so. If only the stop packet is sent, this allows an easy way to reduce the number of records going to the AAA server.

Table 4 *RADIUS Accounting Stop Packet Attributes*

RADIUS Attributes Value	Attribute	Description
42	acct-input-octets	Number of octets that have been received from the Unity client over the course of the service that is being provided.
43	acct-output-octets	Number of octets that have been sent to the Unity client in the course of delivering this service.
46	acct-session-time	Length of time (in seconds) that the Unity client has received service.

RADIUS Attributes Value	Attribute	Description
47	acct-input-packets	Quantity of packets that have been received from the Unity client in the course of delivering this service.
48	acct-output-packets	Quantity of packets that have been sent to the Unity client in the course of delivering this service.
49	acct-terminate-cause	For future use.
52	acct-input-gigawords	How many times the Acct-Input-Octets counter has wrapped around the 232 (2 to the 32nd power) over the course of this service.
52	acct-output-gigawords	How many times the Acct-Input-Octets counter has wrapped around the 232 (2 to the 32nd power) over the course of this service.

RADIUS Update Accounting

RADIUS accounting updates are supported. Packet and octet counts are shown in the updates.

IKE and IPsec Subsystem Interaction

- [Accounting Start, page 22](#)
- [Accounting Stop, page 23](#)
- [Accounting Updates, page 24](#)

Accounting Start

If IPsec accounting is configured, after IKE phases are complete, an accounting start record is generated for the session. New accounting records are not generated during a rekeying.

The following is an account start record that was generated on a router and that is to be sent to the AAA server that is defined:

```
*Aug 23 04:06:20.131: RADIUS(00000002): sending
*Aug 23 04:06:20.131: RADIUS(00000002): Send Accounting-Request to 10.1.1.4:1646 id 4,
len 220
*Aug 23 04:06:20.131: RADIUS: authenticator 38 F5 EB 46 4D BE 4A 6F - 45 EB EF 7D B7 19
FB 3F
*Aug 23 04:06:20.135: RADIUS: Acct-Session-Id [44] 10 "00000001"
*Aug 23 04:06:20.135: RADIUS: Vendor, Cisco [26] 31
*Aug 23 04:06:20.135: RADIUS: Cisco AVpair [1] 25 "isakmp-group-id=cclient"
```

```
*Aug 23 04:06:20.135: RADIUS: Framed-IP-Address [8] 6 10.13.13.1
*Aug 23 04:06:20.135: RADIUS: Vendor, Cisco [26] 20
*Aug 23 04:06:20.135: RADIUS: Cisco AVpair [1] 14 "vrf-id=cisco"
*Aug 23 04:06:20.135: RADIUS: Vendor, Cisco [26] 35
*Aug 23 04:06:20.135: RADIUS: Cisco AVpair [1] 29 "isakmp-initator-ip=11.1.2.2"
*Aug 23 04:06:20.135: RADIUS: Vendor, Cisco [26] 36
*Aug 23 04:06:20.135: RADIUS: Cisco AVpair [1] 30 "connect-progress=No
Progress"
*Aug 23 04:06:20.135: RADIUS: User-Name [1] 13 "joe@cclient"
*Aug 23 04:06:20.135: RADIUS: Acct-Status-Type [40] 6 Start [1]
*Aug 23 04:06:20.135: RADIUS: Vendor, Cisco [26] 25
*Aug 23 04:06:20.135: RADIUS: cisco-nas-port [2] 19 "FastEthernet0/0.1"
*Aug 23 04:06:20.135: RADIUS: NAS-Port [5] 6 0
*Aug 23 04:06:20.135: RADIUS: NAS-IP-Address [4] 6 10.1.1.147
*Aug 23 04:06:20.135: RADIUS: Acct-Delay-Time [41] 6 0
*Aug 23 04:06:20.139: RADIUS: Received from id 21645/4 10.1.1.4:1646, Accounting-
response, len 20
*Aug 23 04:06:20.139: RADIUS: authenticator B7 E3 D0 F5 61 9A 89 D8 - 99 A6 8A 8A 98 79
9D 5D
```

Accounting Stop

An accounting stop packet is generated when there are no more flows (IPsec SA pairs) with the remote peer.

The accounting stop records contain the following information:

- Packets out
- Packets in
- Octets out
- Gigawords in
- Gigawords out

Below is an account start record that was generated on a router. The account start record is to be sent to the AAA server that is defined.

```
*Aug 23 04:20:16.519: RADIUS(00000003): Using existing nas_port 0
*Aug 23 04:20:16.519: RADIUS(00000003): Config NAS IP: 100.1.1.147
*Aug 23 04:20:16.519: RADIUS(00000003): sending
*Aug 23 04:20:16.519: RADIUS(00000003): Send Accounting-Request to 100.1.1.4:1646 id 19,
len 238
*Aug 23 04:20:16.519: RADIUS: authenticator 82 65 5B 42 F0 3F 17 C3 - 23 F3 4C 35 A2 8A
3E E6
*Aug 23 04:20:16.519: RADIUS: Acct-Session-Id [44] 10 "00000002"
*Aug 23 04:20:16.519: RADIUS: Vendor, Cisco [26] 20
*Aug 23 04:20:16.519: RADIUS: Cisco AVpair [1] 14 "vrf-id=cisco"
*Aug 23 04:20:16.519: RADIUS: Vendor, Cisco [26] 35
*Aug 23 04:20:16.519: RADIUS: Cisco AVpair [1] 29 "isakmp-initator-ip=11.1.1.2"
*Aug 23 04:20:16.519: RADIUS: Vendor, Cisco [26] 36
*Aug 23 04:20:16.519: RADIUS: Cisco AVpair [1] 30 "connect-progress=No
Progress"
*Aug 23 04:20:16.519: RADIUS: Acct-Session-Time [46] 6 709
*Aug 23 04:20:16.519: RADIUS: Acct-Input-Octets [42] 6 152608
*Aug 23 04:20:16.519: RADIUS: Acct-Output-Octets [43] 6 152608
*Aug 23 04:20:16.519: RADIUS: Acct-Input-Packets [47] 6 1004
*Aug 23 04:20:16.519: RADIUS: Acct-Output-Packets [48] 6 1004
*Apr 23 04:20:16.519: RADIUS: Acct-Input-Giga-Word[52] 6 0
*Apr 23 04:20:16.519: RADIUS: Acct-Output-Giga-Wor[53] 6
0
*Aug 23 04:20:16.519: RADIUS: Acct-Terminate-Cause[49] 6 none [0]
*Aug 23 04:20:16.519: RADIUS: Vendor, Cisco [26] 32
*Aug 23 04:20:16.519: RADIUS: Cisco AVpair [1] 26 "disc-cause-ext=No Reason"
*Aug 23 04:20:16.519: RADIUS: Acct-Status-Type [40] 6 Stop [2]
*Aug 23 04:20:16.519: RADIUS: Vendor, Cisco [26] 25
*Aug 23 04:20:16.519: RADIUS: cisco-nas-port [2] 19 "FastEthernet0/0.1"
*Aug 23 04:20:16.519: RADIUS: NAS-Port [5] 6 0
*Aug 23 04:20:16.519: RADIUS: NAS-IP-Address [4] 6 100.1.1.147
*Aug 23 04:20:16.519: RADIUS: Acct-Delay-Time [41] 6 0
```

```
*Aug 23 04:20:16.523: RADIUS: Received from id 21645/19 100.1.1.4:1646, Accounting-
response, len 20
*Aug 23 04:20:16.523: RADIUS:  authenticator F1 CA C1 28 CE A0 26 C9 - 3E 22 C9 DA EA B8
22 A0
```

Accounting Updates

If accounting updates are enabled, accounting updates are sent while a session is “up.” The update interval can be configured. To enable the accounting updates, use the **aaa accounting update** command.

The following is an accounting update record that is being sent from the router:

```
Router#
*Aug 23 21:46:05.263: RADIUS(00000004): Using existing nas_port 0
*Aug 23 21:46:05.263: RADIUS(00000004): Config NAS IP: 100.1.1.147
*Aug 23 21:46:05.263: RADIUS(00000004): sending
*Aug 23 21:46:05.263: RADIUS(00000004): Send Accounting-Request to 100.1.1.4:1646 id 22,
len 200
*Aug 23 21:46:05.263: RADIUS:  authenticator 30 FA 48 86 8E 43 8E 4B - F9 09 71 04 4A F1
52 25
*Aug 23 21:46:05.263: RADIUS:  Acct-Session-Id      [44] 10  "00000003"
*Aug 23 21:46:05.263: RADIUS:  Vendor, Cisco      [26] 20
*Aug 23 21:46:05.263: RADIUS:  Cisco AVpair        [1] 14  "vrf-id=cisco"
*Aug 23 21:46:05.263: RADIUS:  Vendor, Cisco      [26] 35
*Aug 23 21:46:05.263: RADIUS:  Cisco AVpair        [1] 29  "isakmp-initator-ip=11.1.1.2"
*Aug 23 21:46:05.263: RADIUS:  Vendor, Cisco      [26] 36
*Aug 23 21:46:05.263: RADIUS:  Cisco AVpair        [1] 30  "connect-progress=No
Progress"
*Aug 23 21:46:05.263: RADIUS:  Acct-Session-Time   [46] 6   109
*Aug 23 21:46:05.263: RADIUS:  Acct-Input-Octets   [42] 6   608
*Aug 23 21:46:05.263: RADIUS:  Acct-Output-Octets  [43] 6   608
*Aug 23 21:46:05.263: RADIUS:  Acct-Input-Packets [47] 6   4
*Aug 23 21:46:05.263: RADIUS:  Acct-Output-Packets [48] 6   4
*Aug 23 21:46:05.263: RADIUS:  Acct-Status-Type   [40] 6   Watchdog           [3]
*Aug 23 21:46:05.263: RADIUS:  Vendor, Cisco      [26] 25
*Aug 23 21:46:05.263: RADIUS:  cisco-nas-port     [2] 19  "FastEthernet0/0.1"
*Aug 23 21:46:05.263: RADIUS:  NAS-Port           [5] 6   0
*Aug 23 21:46:05.263: RADIUS:  NAS-IP-Address    [4] 6   100.1.1.147
*Aug 23 21:46:05.263: RADIUS:  Acct-Delay-Time    [41] 6   0
*Aug 23 21:46:05.267: RADIUS: Received from id 21645/22 100.1.1.4:1646, Accounting-
response, len 20
*Aug 23 21:46:05.267: RADIUS:  authenticator 51 6B BB 27 A4 F5 D7 61 - A7 03 73 D3 0A AC
1C
```

How to Configure IPsec VPN Accounting

- [Configuring IPsec VPN Accounting, page 24](#)
- [Configuring Accounting Updates, page 29](#)
- [Troubleshooting for IPsec VPN Accounting, page 30](#)

Configuring IPsec VPN Accounting

To enable IPsec VPN Accounting, you need to perform the following required task:

Before configuring IPsec VPN accounting, you must first configure IPsec.

SUMMARY STEPS

1. enable
2. configure terminal
3. aaa new-model
4. aaa authentication login *list-name method*
5. aaa authorization network *list-name method*
6. aaa accounting network *list-name start-stop [broadcast] group group-name*
7. aaa session-id common
8. crypto isakmp profile *profile-name*
9. vrf *ivrif*
10. match identity group *group-name*
11. client authentication list *list-name*
12. isakmp authorization list *list-name*
13. client configuration address [initiate | respond]
14. accounting *list-name*
15. exit
16. crypto dynamic-map *dynamic-map-name dynamic-seq-num*
17. set transform-set *transform-set-name*
18. set isakmp-profile *profile-name*
19. reverse-route [remote-peer]
20. exit
21. crypto map *map-name ipsec-isakmp dynamic dynamic-template-name*
22. radius-server host *ip-address [auth-portport-number][acct-portport-number]*
23. radius-server key *string*
24. radius-server vsa send accounting
25. interface *type slot /port*
26. crypto map *map-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.
	Example:	
	Router> enable	<ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	aaa new-model Example: <pre>Router (config)# aaa new-model</pre>	Enables periodic interim accounting records to be sent to the accounting server.
Step 4	aaa authentication login <i>list-name method</i> Example: <pre>Router (config)# aaa authentication login cisco- client group radius</pre>	Enforces authentication, authorization, and accounting (AAA) authentication for extended authorization (XAUTH) through RADIUS or local.
Step 5	aaa authorization network <i>list-name method</i> Example: <pre>Router (config)# aaa authorization network cisco- client group radius</pre>	Sets AAA authorization parameters on the remote client from RADIUS or local.
Step 6	aaa accounting network <i>list-name start-stop [broadcast] group <i>group-name</i></i> Example: <pre>Router (config)# aaa accounting network acc start- stop broadcast group radius</pre>	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS +.
Step 7	aaa session-id common Example: <pre>Router (config)# aaa session-id common</pre>	Specifies whether the same session ID is used for each AAA accounting service type within a call or whether a different session ID is assigned to each accounting service type.
Step 8	crypto isakmp profile <i>profile-name</i> Example: <pre>Route (config)# crypto isakmp profile cisco</pre>	Audits IP security (IPsec) user sessions and enters isakmp-profile submode.

Command or Action	Purpose
<p>Step 9 <code>vrf ivrf</code></p> <p>Example:</p> <pre>Router (conf-isa-prof)# vrf cisco</pre>	<p>Associates the on-demand address pool with a Virtual Private Network (VPN) routing and forwarding (VRF) instance name.</p>
<p>Step 10 <code>match identity group group-name</code></p> <p>Example:</p> <pre>Router(conf-isa-prof)# match identity group cisco</pre>	<p>Matches an identity from a peer in an ISAKMP profile.</p>
<p>Step 11 <code>client authentication list list-name</code></p> <p>Example:</p> <pre>Router(conf-isa-prof)# client authentication list cisco</pre>	<p>Configures Internet Key Exchange (IKE) extended authentication (XAUTH) in an Internet Security Association and Key Management Protocol (ISAKMP) profile.</p>
<p>Step 12 <code>isakmp authorization list list-name</code></p> <p>Example:</p> <pre>Router(conf-isa-prof)# isakmp authorization list cisco-client</pre>	<p>Configures an IKE shared secret and other parameters using the AAA server in an ISAKMP profile. The shared secret and other parameters are generally pushed to the remote peer through mode configuration (MODECFG).</p>
<p>Step 13 <code>client configuration address [initiate respond]</code></p> <p>Example:</p> <pre>Router(conf-isa-prof)# client configuration address respond</pre>	<p>Configures IKE mode configuration (MODECFG) in the ISAKMP profile.</p>
<p>Step 14 <code>accounting list-name</code></p> <p>Example:</p> <pre>Router(conf-isa-prof)# accounting acc</pre>	<p>Enables AAA accounting services for all peers that connect through this ISAKMP profile.</p>
<p>Step 15 <code>exit</code></p> <p>Example:</p> <pre>Router(conf-isa-prof)# exit</pre>	<p>Exits isakmp-profile submode.</p>

Command or Action	Purpose
<p>Step 16 <code>crypto dynamic-map</code> <i>dynamic-map-name</i> <i>dynamic-seq-num</i></p> <p>Example:</p> <pre>Router(config)# crypto dynamic-map mymap 10 ipsec-isakmp</pre>	Creates a dynamic crypto map template and enters the crypto map configuration command mode.
<p>Step 17 <code>set transform-set</code> <i>transform-set-name</i></p> <p>Example:</p> <pre>Router(config-crypto-map)# set transform-set aswan</pre>	Specifies which transform sets can be used with the crypto map template.
<p>Step 18 <code>set isakmp-profile</code> <i>profile-name</i></p> <p>Example:</p> <pre>Router(config-crypto-map)# set isakmp-profile cisco</pre>	Sets the ISAKMP profile name.
<p>Step 19 <code>reverse-route [remote-peer]</code></p> <p>Example:</p> <pre>Router(config-crypto-map)# reverse-route</pre>	Allows routes (ip addresses) to be injected for destinations behind the VPN remote tunnel endpoint and may include a route to the tunnel endpoint itself (using the remote-peer keyword for the crypto map).
<p>Step 20 <code>exit</code></p> <p>Example:</p> <pre>Router(config-crypto-map)# exit</pre>	Exits dynamic crypto map configuration mode.
<p>Step 21 <code>crypto map</code> <i>map-name</i> ipsec-isakmp dynamic <i>dynamic-template-name</i></p> <p>Example:</p> <pre>Router(config)# crypto map mymap ipsec-isakmp dynamic dmap</pre>	Enters crypto map configuration mode
<p>Step 22 <code>radius-server host</code> <i>ip-address</i> [auth-port<i>port-number</i>] [acct-port<i>port-number</i>]</p> <p>Example:</p> <pre>Router(config)# radius-server host 172.16.1.4</pre>	Specifies a RADIUS server host.

Command or Action	Purpose
Step 23 <code>radius-server key <i>string</i></code> Example: <pre>Router(config)# radius-server key nsite</pre>	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
Step 24 <code>radius-server vsa send accounting</code> Example: <pre>Router(config)# radius-server vsa send accounting</pre>	Configures the network access server to recognize and use vendor-specific attributes.
Step 25 <code>interface <i>type slot /port</i></code> Example: <pre>Router(config)# interface FastEthernet 1/0</pre>	Configures an interface type and enters interface configuration mode.
Step 26 <code>crypto map <i>map-name</i></code> Example: <pre>Router(config-if)# crypto map mymap</pre>	Applies a previously defined crypto map set to an interface.

Configuring Accounting Updates

To send accounting updates while a session is “up,” perform the following optional task:

Before you configure accounting updates, you must first configure IPsec VPN accounting. See the section [“Configuring IPsec VPN Accounting, page 24.”](#)

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `aaa accounting update periodic number`

DETAILED STEPS

Command or Action	Purpose
Step 1 <code>enable</code> Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

Command or Action	Purpose
<p>Step 2 <code>configure terminal</code></p> <p>Example:</p> <pre>Router# configure terminal</pre>	Enters global configuration mode.
<p>Step 3 <code>aaa accounting update periodic number</code></p> <p>Example:</p> <pre>Router (config)# aaa accounting update periodic 1-2147483647</pre>	(Optional) Enables periodic interim accounting records to be sent to the accounting server.

Troubleshooting for IPsec VPN Accounting

To display messages about IPsec accounting events, perform the following optional task:

SUMMARY STEPS

1. `enable`
2. `debug crypto isakmp aaa`

DETAILED STEPS

Command or Action	Purpose
<p>Step 1 <code>enable</code></p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
<p>Step 2 <code>debug crypto isakmp aaa</code></p> <p>Example:</p> <pre>Router# debug crypto isakmp aaa</pre>	<p>Displays messages about Internet Key Exchange (IKE) events.</p> <ul style="list-style-type: none"> • The aaa keyword specifies accounting events.

Configuration Examples for IPsec VPN Accounting

- [Accounting and ISAKMP-Profile Example, page 31](#)
- [Accounting Without ISAKMP Profiles Example, page 32](#)

Accounting and ISAKMP-Profile Example

The following example shows a configuration for supporting remote access clients with accounting and ISAKMP profiles:

```

version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname sheep
!
aaa new-model
!
!
aaa accounting network ipsecaaa start-stop group radius
aaa accounting update periodic 1
aaa session-id common
ip subnet-zero
ip cef
!
!
no ip domain lookup
ip domain name cisco.com
ip name-server 172.29.2.133
ip name-server 172.29.11.48
!
!
crypto isakmp policy 1
authentication pre-share
group 2
!
crypto isakmp policy 10
hash md5
authentication pre-share
lifetime 200
crypto isakmp key cisco address 172.31.100.2
crypto iakmp client configuration group cclient
key jegjegjhrj
pool addressA

crypto-isakmp profile groupA
vrf cisco
match identity group cclient
client authentication list cisco-client
isakmp authorization list cisco-client
client configuration address respond
accounting acc
!
!
crypto ipsec transform-set esp-des-md5 esp-des esp-md5-hmac
!
crypto dynamic-map remotes 1
set peer 172.31.100.2
set security-association lifetime seconds 120
set transform-set esp-des-md5
reverse-route
!
crypto map test 10 ipsec-isakmp dynamic remotes
!
voice call carrier capacity active
!
interface Loopback0
ip address 10.20.20.20 255.255.255.0
no ip route-cache
no ip mroute-cache
!
interface FastEthernet0/0
ip address 10.2.80.203 255.255.255.0
no ip mroute-cache

```

```

load-interval 30
duplex full
!
interface FastEthernet1/0
ip address 192.168.219.2 255.255.255.0
no ip mroute-cache
duplex auto
speed auto
!
interface FastEthernet1/1
ip address 172.28.100.1 255.255.255.0
no ip mroute-cache
duplex auto
speed auto
crypto map test
!
no fair-queue
ip default-gateway 10.2.80.1
ip classless
ip route 10.0.0.0 0.0.0.0 10.2.80.1
ip route 10.20.0.0 255.0.0.0 10.2.80.56
ip route 10.10.10.0 255.255.255.0 172.31.100.2
ip route 10.0.0.2 255.255.255.255 10.2.80.73
ip local pool addressA 192.168.1.1 192.168.1.253
no ip http server
ip pim bidir-enable
!
!
ip access-list extended encrypt
permit ip host 10.0.0.1 host 10.5.0.1
!
access-list 101 permit ip host 10.20.20.20 host 10.10.10.10
!
!
radius-server host 172.27.162.206 auth-port 1645 acct-port 1646 key cisco123
radius-server retransmit 3
radius-server authorization permit missing Service-Type
radius-server vsa send accounting
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
exec prompt timestamp
line aux 0
line vty 5 15
  ntp server 172.31.150.52
end

```

Accounting Without ISAKMP Profiles Example

The following example shows a full Cisco IOS configuration that supports accounting remote access peers when ISAKMP profiles are not used:

```

version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname sheep
!
aaa new-model

```

```

!
!
aaa accounting network ipsecaaa start-stop group radius
aaa accounting update periodic 1
aaa session-id common
ip subnet-zero
ip cef
!
!
no ip domain lookup
ip domain name cisco.com
ip name-server 172.29.2.133
ip name-server 172.29.11.48
!
!
crypto isakmp policy 1
 authentication pre-share
 group 2
!
crypto isakmp policy 10
 hash md5
 authentication pre-share
 lifetime 200
crypto isakmp key cisco address 172.31.100.2
!
!
crypto ipsec transform-set esp-des-md5 esp-des esp-md5-hmac
!
crypto map test client accounting list ipsecaaa
crypto map test 10 ipsec-isakmp
 set peer 172.31.100.2
 set security-association lifetime seconds 120
 set transform-set esp-des-md5
 match address 101
!
voice call carrier capacity active
!
interface Loopback0
 ip address 10.20.20.20 255.255.255.0
 no ip route-cache
 no ip mroute-cache
!
interface FastEthernet0/0
 ip address 10.2.80.203 255.255.255.0
 no ip mroute-cache
 load-interval 30
 duplex full
!
interface FastEthernet1/0
 ip address 192.168.219.2 255.255.255.0
 no ip mroute-cache
 duplex auto
 speed auto
!
interface FastEthernet1/1
 ip address 172.28.100.1 255.255.255.0
 no ip mroute-cache
 duplex auto
 speed auto
 crypto map test
!
no fair-queue
ip default-gateway 10.2.80.1
ip classless
ip route 10.0.0.0 0.0.0.0 10.2.80.1
ip route 10.30.0.0 255.0.0.0 10.2.80.56
ip route 10.10.10.0 255.255.255.0 172.31.100.2
ip route 10.0.0.2 255.255.255.255 10.2.80.73
no ip http server
ip pim bidir-enable
!
!
ip access-list extended encrypt

```

```

    permit ip host 10.0.0.1 host 10.5.0.1
    !
access-list 101 permit ip host 10.20.20.20 host 10.10.10.10
    !
    !
radius-server host 172.27.162.206 auth-port 1645 acct-port 1646 key cisco123
radius-server retransmit 3
radius-server authorization permit missing Service-Type
radius-server vsa send accounting
call rsvp-sync
    !
    !
mgcp profile default
    !
dial-peer cor custom
    !
    !
gatekeeper
    shutdown
    !
    !
line con 0
    exec-timeout 0 0
    exec prompt timestamp
line aux 0
line vty 5 15
    !
exception core-file ioscrypto/core/sheep-core
exception dump 172.25.1.129
ntp clock-period 17208229
ntp server 172.71.150.52
    !
end

```

Additional References

Related Documents

Related Topic	Document Title
Configuring AAA accounting	<ul style="list-style-type: none"> Configuring Accounting
Configuring IPsec VPN accounting	<ul style="list-style-type: none"> Configuring Security for VPNs with IPsec
Configuring basic AAA RADIUS	<ul style="list-style-type: none"> The section “Configuring RADIUS” in the <i>Cisco IOS Security Configuration Guide: User Services</i> on Cisco.com
Configuring ISAKMP profiles	VRF Aware IPsec
Privilege levels with TACACS+ and RADIUS	<ul style="list-style-type: none"> Configuring TACACS+ “Configuring RADIUS” section of the <i>Cisco IOS Security Configuration Guide: User Services</i> on Cisco.com
IP security, RADIUS, and AAA commands	<i>Cisco IOS Security Command Reference</i>

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IPsec VPN Accounting

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 5 **Feature Information for <Phrase Based on Module Title>**

Feature Name	Releases	Feature Information
IPsec VPN Accounting	12.2(15)T	<p>The IPsec VPN Accounting feature allows a session to be accounted by indicating when the session starts and stops. A VPN session is defined as an Internet Key Exchange (IKE) security association (SA) and the one or more SA pairs that are created by the IKE SA. The session starts when the first IP Security (IPsec) pair is created and stops when all IPsec SAs are deleted. Session identifying information and session usage information is passed to the Remote Authentication Dial-In User Service (RADIUS) server through standard RADIUS attributes and vendor-specific attributes (VSAs).</p> <p>This feature was introduced in Cisco IOS Release 12.2(15)T</p> <p>The following commands were introduced or modified: client authentication list, client configuration address, crypto isakmp profile, crypto map (global IPsec), debug crypto isakmp, isakmp authorization list, match identity, set isakmp-profile, vrf</p>

Glossary

IKE --Internet Key Exchange. IKE establishes a shared security policy and authenticates keys for services (such as IP security [IPsec]) that require keys. Before any IPsec traffic can be passed, each router, firewall, and host must verify the identity of its peer. This can be done by manually entering preshared keys into both hosts or by a certification authority (CA) service.

IPsec --IP security. IPsec is 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 IKE to handle the negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPsec. IPsec can 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.

ISAKMP --Internet Security Association and Key Management Protocol. ISAKMP is an Internet IPsec protocol (RFC 2408) that negotiates, establishes, modifies, and deletes security associations. It also exchanges key generation and authentication data (independent of the details of any specific key generation technique), key establishment protocol, encryption algorithm, or authentication mechanism.

L2TP session --Layer 2 Transport Protocol. L2TP are communications transactions between the L2TP access concentrator (LAC) and the L2TP network server (LNS) that support tunneling of a single PPP connection. There is a one-to-one relationship among the PPP connection, L2TP session, and L2TP call.

NAS --network access server. A NAS is a Cisco platform (or collection of platforms, such as an AccessPath system) that interfaces between the packet world (for example, the Internet) and the circuit world (for example, the public switched telephone network [PSTN]).

PFS --perfect forward secrecy. **PFS is a cryptographic characteristic associated with a derived shared secret value. With PFS, if one key is compromised, previous and subsequent keys are not compromised because subsequent keys are not derived from previous keys.**

QM --Queue Manager. The Cisco IP Queue Manager (IP QM) is an intelligent, IP-based, call-treatment and routing solution that provides powerful call-treatment options as part of the Cisco IP Contact Center (IPCC) solution.

RADIUS --Remote Authentication Dial-In User Service. RADIUS is a database for authenticating modem and ISDN connections and for tracking connection time.

RSA --Rivest, Shamir, and Adelman. Rivest, Shamir, and Adelman are the inventors of the Public-key cryptographic system that can be used for encryption and authentication.

SA --security association. A SA is an instance of security policy and keying material that is applied to a data flow.

TACACS+ --Terminal Access Controller Access Control System Plus. TACACS+ is a security application that provides centralized validation of users attempting to gain access to a router or network access server.

TED --Tunnel Endpoint Discovery. TED is a Cisco IOS software feature that allows routers to discover IPsec endpoints.

VPN --Virtual Private Network. A VPN enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses "tunneling" to encrypt all information at the IP level.

VRF --A VPN routing/forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router.

VSA --vendor-specific attribute. A VSA is an attribute that has been implemented by a particular vendor. It uses the attribute Vendor-Specific to encapsulate the resulting AV pair: essentially, Vendor-Specific = protocol:attribute = value.

XAUTH --Extended authentication. XAUTH is an optional exchange between IKE Phase 1 and IKE Phase 2, in which the router demands additional authentication information in an attempt to authenticate the actual user (as opposed to authenticating the peer).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks.

Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.



VPN Device Manager Client for Cisco IOS Software XSM Configuration

This document describes the command-line interface (CLI) Cisco IOS commands required to activate the VPN Device Manager (VDM) client and includes the following sections:



Note

For the primary documentation of the latest version of the VPN Device Manager (version 1.2), see the "Installation Guide and Release Notes for VPN Device Manager 1.2" at <http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/vdm/vdm12rn.htm>.

- [Feature Overview, page 39](#)
- [Finding Feature Information, page 41](#)
- [Supported Standards MIBs and RFCs, page 42](#)
- [Prerequisites, page 42](#)
- [Configuring VDM, page 42](#)
- [Configuration Examples for VDM, page 44](#)
- [Feature Information for VPN Device Manager Client, page 45](#)
- [Glossary, page 46](#)

Feature Overview

VDM software is installed directly onto Cisco VPN devices. It allows network administrators to use a web browser to manage and configure site-to-site VPNs on a single device. VDM implements a wizard-based GUI that allows simplified VPN configuration of the device on which it resides and peer-to-peer interfaces from that device to remote devices. VDM requires configuration of some Cisco IOS commands before it can be fully operational.



Note

In addition to having the relevant Cisco IOS image installed on your device, make sure the VDM client software has been preinstalled in the device Flash memory. If it has not been, you must download it from Cisco.com. See the Installation and Release Notes for VPN Device Manager for the product version you are using for details on completing this task. See the *Cisco VPN Device Manager* index (<http://www.cisco.com/warp/public/cc/pd/nemnsw/vpdvmm>) for further information.

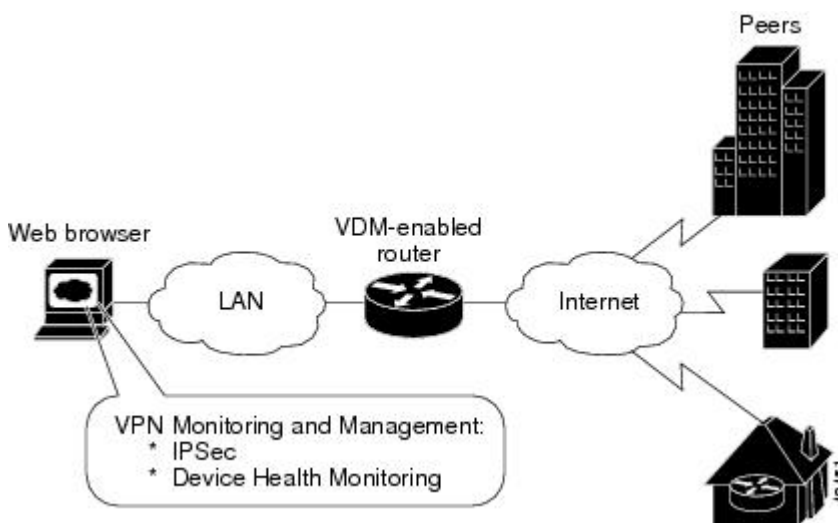
VDM also monitors general system statistics and VPN-specific information such as tunnel throughput and errors. The graphing capability allows comparison of such parameters as traffic volume, tunnel counts, and

system utilization. VDM supports site-to-site VPNs. Its step-by-step wizards simplify the configuration of common VPN setups, interfaces, and policies, including:

- IPsec tunnels
- Preshared keys and Internet Key Exchange (IKE) policies

The figure below shows a simplified VDM deployment within a VPN.

Figure 1 **Simplified VDM Deployment**



- [XML Subscription Manager, page 40](#)
- [CLI Commands for VDM, page 40](#)
- [Related Features and Technologies, page 41](#)
- [Related Documents, page 41](#)

XML Subscription Manager

XML Subscription Manager (XSM) is an HTTP-based service for retrieving information from a Cisco device. Once remote applications (such as VDM) are connected to the XSM server, they can subscribe to data sets called XML Request Descriptors (XRDs). These are XML-formatted messages describing configuration (access-control lists (ACLs), interfaces, crypto-maps, and others) and monitoring information (CPU, memory usage, interface statistics, and others).

XSM provides remote applications such as VDM with a constantly updated stream of data about Cisco device status by supplying real-time data without repeated device polling.

CLI Commands for VDM

This document gives details about Cisco IOS commands specific to VDM functionality. These commands are not related to general VPN functions but are designed to manage VDM itself via the XSM server. By using the Java-enabled VDM application, you can perform all VPN-related configuration and monitoring tasks within the application.

These commands are designed to complement VDM. The following tasks are performed by specific Cisco IOS XSM commands (command name in parentheses):

- Enabling VDM to receive data from the XSM feature set on the device (**xsm**)
- Enabling basic device monitoring, configuration, and data delivery for VDM (**xsm edm**)
- Enabling VPN-specific monitoring, configuration, and data delivery for VDM (**xsm vdm**)
- Enabling access to switch operations (for example, configuring switch ports and VLANs) when running VDM on a switch (**xsm dvdm**)
- Enabling collection of selected statistics generic to embedded devices on the XSM server (**xsm history edm**)
- Enabling collection of specific selected VPN statistics on the XSM server (**xsm history vdm**)
- Clearing VDM client sessions (**clear xsm**)
- Displaying information about the XSM server and VDM (**show xsm status**)
- Displaying all XRDs available to VDM (**show xsm xrd-list**)
- Setting user privilege levels for viewing VDM monitoring and configuration data (**xsm privilege monitor level** and **xsm privilege configuration level**)

For more information on VDM, the Installation and Release Notes for VPN Device Manager for the product version you are using. See the *Cisco VPN Device Manager* index (<http://www.cisco.com/warp/public/cc/pd/nemnsw/vpdvmm>) for further information.

Related Features and Technologies

- Virtual Private Networks (VPNs)
- Security

Related Documents

- Access VPN Solutions Using Tunneling Technology
- *Access VPDN Dial-in Using L2TP*
- Access VPDN Dial-in Using IPSec Over L2TP
- Cisco IOS Dial Technologies Command Reference
- Cisco IOS Security Command Reference
- Configuring Virtual Private Networks " chapter in the "Virtual Templates, Profiles, and Networks" part of the *Cisco IOS Dial Technologies Configuration Guide*
- Installation and Release Notes for VPN Device Manager
- VDM chapter in the *Cisco Enterprise VPN Configuration Guide*
- Cisco VPN Device Manager
- IPsec VPN Acceleration Services Module Installation and Configuration Note

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Supported Standards MIBs and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

No new or modified MIBs are supported by this feature.

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

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

RFCs

No new or modified RFCs are supported by this feature.

Prerequisites

The VDM client software must be installed on your device. It might already have been installed if you chose the VPN option at the time of configuration.

Configuring VDM

See the following sections for configuration tasks for this feature. Each task in the list is identified as either required or optional.

- [Enabling the XSM Server for VDM, page 42](#)
- [Configuring XSM Privilege Levels for XRDs, page 43](#)
- [Disabling the XSM Server for VDM, page 43](#)
- [Verifying VDM Status on the XSM Server, page 43](#)
- [Clearing XSM Client Sessions, page 44](#)
- [Configuring XSM Statistics Collection, page 44](#)

Enabling the XSM Server for VDM

Use the **xsm** command in global configuration mode to activate XSM clients (such as VDM) on your device. Enabling this command also enables the **xsm vdm** and **xsm edm** global configuration commands, so there is no need to enable them separately.

Command	Purpose
Router(config)# xsm	Enables XSM client access to the device.

Configuring XSM Privilege Levels for XRDs

To set the minimum required privilege levels and grant appropriate access to view, monitor, or configure the XSM client (such as VDM), use the following commands in global configuration mode. Privilege levels set on the device determine which access level users possess (configuration and monitoring, monitoring only, or neither).

Users with privilege levels lower than the required monitoring privilege level will not have access to either the configuration or monitoring data required for subscription to XML Request Descriptors (XRDs). The higher the number, the higher the privilege level. The privilege level for the **xsm privilege configuration level** command must be greater than or equal to that of the **xsm privilege monitor level** command.

Command	Purpose
Router(config)# xsm privilege configuration level <i>number</i>	<p>Enables configuration privilege level to subscribe to XRDs.</p> <ul style="list-style-type: none"> <i>number</i> --Privilege level (1-15). <p>Privilege level 15 is the default.</p>
Router(config)# xsm privilege monitor level <i>number</i>	<p>Enables monitor privilege level to subscribe to XRDs.</p> <ul style="list-style-type: none"> <i>number</i> --Privilege level (1-15). <p>Privilege level 15 is the default.</p>

Disabling the XSM Server for VDM

To disable the XSM server, use the command below in global configuration mode. Disabling this command also disables the **xsm vdm** and **xsm edm** global configuration commands.

Command	Purpose
Router(config)# no xsm	Disables XSM server.

Verifying VDM Status on the XSM Server

Use the **show xsm status** command to verify the status of clients (such as VDM) on the XSM server.

Command	Purpose
Router# show xsm status	Displays information and status about clients subscribed to the XSM server.

Use the **show xsm xrd-list** command to verify all XML Request Descriptors (XRDs) for XSM clients (such as VDM) made available by subscription to the XSM server.

Command	Purpose
Router# show xsm xrd-list	Displays all XRDs for clients subscribed to the XSM server.

Clearing XSM Client Sessions

Use the **clear xsm** command to clear data from XSM clients (such as VDM) on the XSM server. To disconnect a specific client, you must identify the session number. Use the **show xsm status** command to obtain specific session numbers.

Command	Purpose
Router# clear xsm [session number]	<p>Clears XSM client sessions.</p> <ul style="list-style-type: none"> • session --XSM session ID. • number --Number of the specific XSM client session you are clearing.

Configuring XSM Statistics Collection

To configure the XSM server and its related clients (such as VDM) for Embedded Device Manager (EDM) or VPN-specific statistics collection of up to 5 days of data, use the following commands in global configuration mode.

Command	Purpose
Router(config)# xsm history edm	Enables statistics collection for the EDM on the XSM server.
Router(config)# xsm history vdm	Enables specific VPN statistics collection on the XSM server.

Configuration Examples for VDM

- [Enabling the XSM Server for VDM Example, page 44](#)
- [Configuring XSM Privilege Levels for XRDs Example, page 45](#)
- [Disabling the XSM Server for VDM Example, page 45](#)
- [Configuring XSM Statistics Collection Example, page 45](#)

Enabling the XSM Server for VDM Example

The following example shows how to enable the XSM client on the device:

```
xsm
```

Configuring XSM Privilege Levels for XRDs Example

The following example shows how to set a privilege level of 11, for subscription to XRDs:

```
xsm privilege monitor level 11
```

Disabling the XSM Server for VDM Example

The following example shows how to enable and then disable the XSM client on the device to troubleshoot VDM:

```
no xsm  
xsm
```

Configuring XSM Statistics Collection Example

The following example shows how to configure the XSM server and its related clients (such as VDM) for Embedded Device Manager (EDM) or VPN-specific statistics collection of up to 5 days of data:

```
xsm history edm
```

```
xsm history vdm
```

Feature Information for VPN Device Manager Client

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 6 Feature Information for VPN Device Manager Client

Feature Name	Releases	Feature Information
VPN Device Manager Client	12.1(6)E 12.2(9)YE, 12.2(9)YO1, 12.2(13)T, 12.2(14)S	<p>VDM software is installed directly onto Cisco VPN devices.</p> <p>The following commands were introduced or modified:</p> <ul style="list-style-type: none"> • clear xsm • crypto mib topn • show xsm status • show xsm xrd-list • xsm • xsm dvdm • xsm edm • xsm history edm • xsm history vdm • xsm privilege configuration level • xsm privilege monitor level • xsm vdm .

Glossary

Internet Key Exchange (IKE) --A key management protocol standard used in conjunction with IPSec and other standards. IPSec can be configured without IKE, but IKE enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard. IKE authenticates the IPSec peers, negotiates IPSec keys, and negotiates IPSec security associations. Before any IPSec traffic can be passed, each router/firewall/host must be able to verify the identity of its peer. This can be done by manually entering preshared keys into both hosts or by a CA service.

IP security (IPSec) --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.

Virtual Private Network (VPN) --A virtual network that uses advanced encryption and tunneling to permit organizations to establish secure, end-to-end, private network connections over public IP infrastructure networks, such as the Internet or extranets.

VPN Device Manager (VDM) --A browser-based tool for configuring and monitoring VPNs on a VPN-enabled device. VDM allows users to configure and monitor advanced VPN functionality within Cisco devices.

XML Subscription Manager (XSM) -- A Cisco IOS subsystem that allows embedded device managers such as VDM to receive XML-based configuration and monitoring information for managing network devices.

XML Request Descriptor (XRD) --A specific requested type of data from XSM.

Embedded Device Manager (EDM) --An XSM adapter that publishes general network device configuration and monitoring information for device managers such as VDM.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

