GDOI MIB Support for GET VPN

The existing MIBs in crypto are the Internet Key Exchange (IKE) and IP security (IPsec) MIBs, which are not sufficient for Group Domain of Interpretation (GDOI). The GDOI MIB Support for GET VPN feature adds MIB support for RFC 6407, The Group Domain of Interpretation ; it supports only the objects related to the GDOI MIB IETF standard. You can import the GDOI MIB .my file into an SNMP management station and parse it to retrieve the table objects and hierarchy information.

The GDOI MIB consists of objects and notifications (formerly called traps) that include information about GDOI groups, group menber (GM) and key server (KS) peers, and the policies that are created or downloaded. Only "get" operations are supported for GDOI.

To configure GDOI MIB support for GET VPN, see the "Configuring GDOI MIB Support for GET VPN" section.

Information About GDOI MIB Support for GET VPN

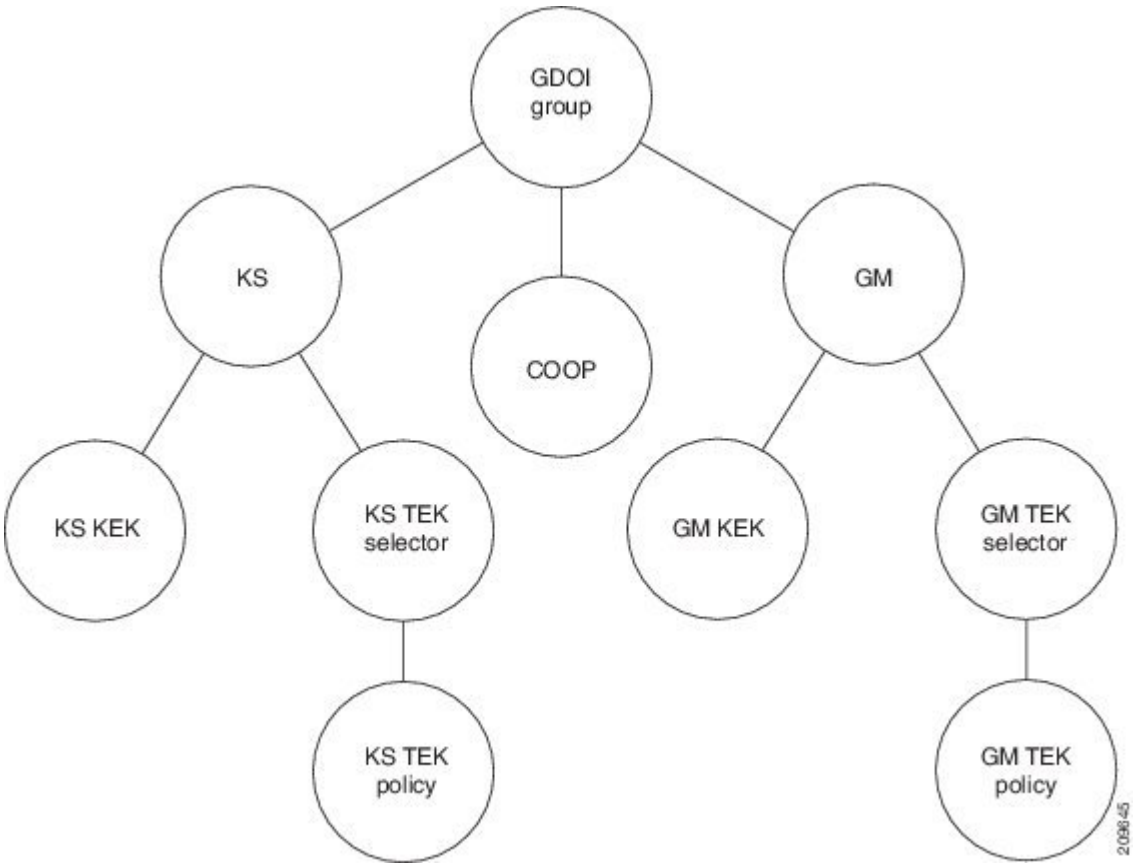
GDOI MIB Compatibility with Other GET VPN Software Versions

The GDOI MIB Support for GET VPN feature provides a command that you use on the KS (or primary KS) to check whether all the devices in the network are running versions that support the GDOI MIB. For more information, see the "Ensuring that GMs Are Running Software Versions That Support the GDOI MIB" section.

GDOI MIB Table Hierarchy

The GDOI MIB objects are organized into the following GDOI MIB tables. Following is the relationship (hierarchy) among the tables:

Figure 1: GDOI MIB Table Hierarchy



GDOI MIB Table Objects

Following is a list of the MIB table objects (listed per group).

Group table objects:

- Group ID type—Specifies whether the group ID is an IP address, group number, hostname, and so on.
- Group ID length—Number of octets in the group ID value.
- Group ID value—Group number, IP address, or hostname.
- Group name—String value.
- Group member count -- Specifies the number of registered KSs to this group.
- Group active peer KS count -- Specifies the number of active KSs to this group.
- Group last rekey retransmits -- Specifies the cumulative count of number of rekey messages and retransmit messages sent as a part of last rekey operation.
- Group last rekey time taken -- Specifies the time taken by the KS to complete the last rekey operation.

KS table objects:

- KS ID type
- KS ID length
- KS ID value
- Active KEK—SPI of the key encryption key (KEK) that is currently used by the KS to encrypt the rekey message.
- Last rekey sequence number—Last rekey number that was sent by the KS to the group.
- KS Role -- Primary or secondary.
- Number of registered GMs -- count of GMs registered to this KS.

COOP table objects:

- COOP peer ID type
- COOP peer ID length
- COOP peer ID value
- COOP peer ID role -- Primary or secondary
- COOP peer status -- Alive, dead or unknown
- Number of registered GMs -- count of GMs registered to the COOP peer

GM table:

- GM ID type
- GM ID length
- GM ID value
- Registered KS ID type—ID type of the KS to which the GM is registered.
- Registered KS ID length
- Registered KS ID value
- Active KEK—SPI of the KEK currently used by the GM to decrypt rekey messages.
- Last rekey seq number—Last rekey number received by the GM.
- Count of active TEKs -- number of active TEKs used by the GM to encrypt/decrypt/authenticate dataplane traffic.

KS KEK table:

- KEK index
- KEK SPI
- KEK source ID information—Source ID type, ID length, and ID value.
- KEK source ID port—Port associated with the source ID.
- KEK destination ID information—Destination ID type, ID length, and ID value.

- KEK destination ID port—Port associated with the destination ID.
- IP protocol ID—UDP or TCP.
- Key management algorithm (unused).
- Encryption algorithm and key length (bits)
- SIG payload hash algorithm, SIG payload signature algorithm, and SIG payload key length (bits).
- Hash algorithm (will be reused from the IPsec MIB)
- Diffie-Hellman group
- KEK original lifetime (seconds)—Maximum time for which a KEK is valid.
- KEK remaining lifetime (seconds)

KS TEK selector table (corresponds to the ACLs that are configured as part of the IPsec SA in the GDOI group configuration on the KS):

- TEK selector index—An integer index for traffic encryption keys (TEK).
- TEK source ID information—Source ID type, ID length, and ID value.
- TEK source ID port—Port associated with the source ID.
- TEK destination ID information—Destination ID type, ID length, and ID value.
- TEK destination ID port—Port associated with the destination ID.
- TEK Security protocol—GDOI_PROTO_IPSEC_ESP protocol ID value in the SA TEK payload (see RFC 6407).

KS TEK policy table:

- TEK policy index—An integer index.
- TEK SPI—Four octets
- Encapsulation mode—Tunnel or transport.
- Encryption algorithm and key length (bits)
- Integrity and authentication algorithm and key length (bits)
- TBAR window size (seconds)
- TEK original lifetime (seconds)—Maximum time for which a TEK is valid.
- TEK remaining lifetime (seconds)
- TEK Status—Inbound, outbound, or not in use.

GM KEK table:

- KEK index—An integer index.
- KEK SPI
- KEK source ID information—Source ID type, ID length , and ID value.

- KEK source ID port—Port associated with the source ID.
- KEK destination ID information—Destination ID type, ID length, and ID value.
- KEK destination ID port—Port associated with the destination ID.
- IP protocol ID—UDP or TCP.
- Key management algorithm (unused)
- Encryption algorithm and key length (bits)
- SIG payload hash algorithm, SIG payload signature algorithm, and SIG payload key length (bits)
- Hash algorithm
- Diffie-Hellman group
- KEK original lifetime (seconds)—Maximum time for which a KEK is valid.
- KEK remaining lifetime (seconds)

GM TEK selector table (corresponds to the ACLs that are downloaded to the GM as part of the TEK policy from the KS):

- TEK selector index—An integer index.
- TEK source ID information—Source ID type, ID length, and ID value.
- TEK source ID port—Port associated with the source ID.
- TEK destination ID information—Destination ID type, ID length , and ID value.
- TEK destination ID port—Port associated with the destination ID.
- TEK Security protocol—GDOI_PROTO_IPSEC_ESP protocol ID value in the SA TEK payload (see RFC 6407).

GM TEK policy table:

- TEK policy index—An integer index.
- TEK SPI —Four octets.
- Encapsulation mode—Tunnel or transport.
- Encryption algorithm and key length (bits)
- Integrity and authentication algorithm and key length (bits)
- TBAR window size (seconds)
- TEK original lifetime (seconds)—Maximum time for which a TEK is valid.
- TEK remaining lifetime (seconds)
- TEK Status—Inbound, outbound, or not in use.

GDOI MIB Notifications

The GDOI MIB supports the Simple Network Management Protocol (SNMP) notifications in the following table. The GDOI MIB contains two kinds of notifications: those generated by the KS and those generated by each GM. You can enable any combination of notifications (or all notifications).

Table 1: SNMP Notifications Supported by the GDOI MIB

Notification	Description
KS New Registration	A KS first received a registration request from a GM.
KS Registration Complete	A GM completed registration to the KS.
KS Rekey Pushed	A rekey message was sent by the KS.
KS No RSA Keys	An error notification was received from the KS because of missing RSA keys.
GM Register	A GM first sent a registration request to a KS.
GM Registration Complete	A GM completed registration to a KS.
GM Re-Register	A GM began the reregistration process with a KS.
GM Rekey Received	A rekey message was received by a GM.
GM Incomplete Config	A GM sent an error notification because of a missing configuration.
GM Rekey Failure	A GM sent an error notification because it cannot process and install a rekey.
KS Role Change	A KS switches between primary and secondary role.
KS GM Deleted	Generated when a GM is deleted from the KS.
KS Peer Reachable	Generated by a KS when unreachable COOP peer becomes reachable.
KS Peer Unreachable	Generated by a KS when reachable COOP peer becomes unreachable.

For more information, see the “Enabling GDOI MIB Notifications” section.

GDOI MIB Limitations

The GDOI MIB contains only objects that are listed in RFC 6407 and does not contain objects for functionality specific to the Cisco implementation of GDOI. This functionality includes:

- Cooperative key servers
- GM ACLs
- Receive-only SAs
- Fail-close/fail-open
- Crypto map objects
- Other Cisco GET VPN-specific features

How to Configure GDOI MIB Support for GET VPN

Ensuring that GMs Are Running Software Versions That Support the GDOI MIB

Perform this task on the KS (or primary KS) to ensure that all devices in the GET VPN network support the GDOI MIB.

SUMMARY STEPS

1. **enable**
2. **show crypto gdoi feature gdoi-mib**
3. **show crypto gdoi feature gdoi-mib | include No**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show crypto gdoi feature gdoi-mib** **Example:** `Device# show crypto gdoi feature gdoi-mib`	Displays the version of the GET VPN software running on each KS and GM in the network and displays whether that device supports the GDOI MIB.
Step 3	**show crypto gdoi feature gdoi-mib | include No** **Example:** `Device# show crypto gdoi feature gdoi-mib | include No`	(Optional) Finds only those devices that do not support the GDOI MIB.

Creating Access Control for an SNMP Community

You specify an SNMP community access string to define the relationship between the SNMP manager and the SNMP agent on the KS or GM in order to permit access to SNMP. Your community access string acts like a password to regulate access to the agent on the device.

Perform this task to specify the community access string.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server community** *community-string* [**view** *view-name*] [**ro** | **rw**] [**ipv6** *nacl*] [*access-list-number* | *extended-access-list-number* | *access-list-name*]

4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server community** *community-string* [**view** *view-name*] [**ro** | **rw**] [**ipv6** *nacl*] [*access-list-number* | *extended-access-list-number* | *access-list-name*] **Example:** `Device(config)# snmp-server community mycommunity`	Specifies the community access string.
Step 4	**end** **Example:** `Device(config)# end`	Exits global configuration mode, saves the configuration, and returns to privileged EXEC mode.

For more information about specifying a community access string, refer to the "Configuring SNMP Support" module in the *SNMP Configuration Guide*. For more information about the **snmp-server community** command (including syntax and usage guidelines), refer to the Cisco IOS SNMP Support Command Reference.

Enabling Communication with the SNMP Manager

Perform this task to enable communication between the SNMP agent on the KS or GM and the SNMP manager.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server host** {*hostname* | *ip-address*} **version** {**1** | **2c** | **3**} *community-string*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Device> enable`	
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server host** {*hostname* | *ip-address*} **version** {**1** | **2c** | **3**} *community-string* **Example:** `Device(config)# snmp-server host 209.165.200.225 version 2c mycommunity`	Specifies the host to receive SNMP notifications. • 2c is usually used as the SNMP version.
Step 4	**end** **Example:** `Device(config)# end`	Exits global configuration mode, saves the configuration, and returns to privileged EXEC mode.

For more information about enabling communication with the SNMP manager, refer to the "Configuring SNMP Support" module in the *SNMP Configuration Guide*. For more information about the **snmp-server host** command (including syntax and usage guidelines), refer to the Cisco IOS SNMP Support Command Reference.

Enabling GDOI MIB Notifications

Perform this task to enable GDOI MIB notifications on the KS or GM.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps gdoi** [*notification-type*]
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 3	**snmp-server enable traps gdoi** [*notification-type*] **Example:** `Device(config)# snmp-server enable traps gdoi gm-registration-complete gm-rekey-rcvd ks-new-registration ks-reg-complete`	Specifies the particular SNMP notifications to be enabled. You can specify any combination of the following types in any order. If you enter the command without any of the following keywords, all GDOI MIB notifications are enabled. • **gm-incomplete-cfg**—A GM sent an error notification because of a missing configuration. • **gm-re-register**—A GM began the reregistration process with a KS. • **gm-registration-complete**—A GM completed registration to a KS. • **gm-rekey-fail**—A GM sent an error notification because it cannot successfully process and install a rekey. • **gm-rekey-rcvd**—A rekey message was received by a GM. • **gm-start-registration**—A GM first sent a registration request to a KS. • **ks-new-registration**—A KS first received a registration request from a GM. • **ks-no-rsa-keys**—An error notification was received from the KS because of missing RSA keys. • **ks-reg-complete**—A GM completed registration to the KS. • **ks-rekey-pushed**—A rekey message was sent by the KS. • **ks-gm-deleted**—A GM is deleted by the KS. • **ks-peer-reachable**—An unreachable COOP peer becomes reachable. • **ks-peer-unreachable**—A reachable COOP peer becomes unreachable. • **ks-role-change**—A KS changes it's role from primary to secondary or vice-versa.
Step 4	**end** **Example:** `Device(config)# end`	Exits global configuration mode, saves the configuration, and returns to privileged EXEC mode.

Configuration Examples for GDOI MIB Support for GET VPN

Example: Ensuring That GMs Are Running Software Versions That Support the GDOI MIB

The following example shows how to use the GET VPN software versioning command on the KS (or primary KS) to check whether all the devices in the network support the GDOI MIB:

```
Device# show crypto gdoi feature gdoi-mib

Group Name: GET
 Key Server ID       Version   Feature Supported
    10.0.8.1         1.0.2          Yes
    10.0.9.1         1.0.2          Yes
    10.0.10.1        1.0.2          Yes
    10.0.11.1        1.0.2          Yes
 Group Member ID     Version   Feature Supported
    10.0.11.2          1.0.2          Yes
    10.0.11.3          1.0.1          No
```

The following example shows how to find only those devices that do not support the GDOI MIB:

```
Device# show crypto gdoi feature gdoi-mib | include No

       10.0.11.3          1.0.1          No
```

Example: Creating Access Control for an SNMP Community

The following example shows how to specify an SNMP community string named mycommunity to define the relationship between the SNMP manager and the SNMP agent on the KS or GM in order to permit access to SNMP:

```
Device> enable
Device# configure terminal
Device(config)# snmp-server community mycommunity
Device(config)# end
```

Example: Enabling Communication with the SNMP Manager

The following example shows how to enable communication with the SNMP manager. This example using a community string named mycommunity that has already been created:

```
Device> enable
Device# configure terminal
```

```
Device(config)# snmp-server host 209.165.200.225 version 2c mycommunity
Device(config)# end
```

Example: Enabling GDOI MIB Notifications

The following example shows how to enable GDOI MIB notifications:

```
Device> enable
Device# configure terminal
Device(config)# snmp-server enable traps gdoi gm-registration-complete gm-rekey-rcvd
ks-new-registration ks-reg-complete
Device(config)# end
```

Additional References for GDOI MIB Support for GET VPN

Related Documents

Related Topic	Document Title
Cisco IOS security commands	*Cisco IOS Security Command References*
Configuring SNMP	• "Configuring SNMP Support" module in the SNMP Configuration Guide, Cisco IOS Release 15.2M&T • Cisco IOS SNMP Support Command Reference

MIBs

MIB	MIBs Link
CISCO-GDOI-MIB	To locate and download MIBs for selected platforms, Cisco software 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 GDOI MIB Support for GET VPN

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 GDOI MIB Support for GET VPN

Feature Name	Releases	Feature Information
GDOI MIB Support for GET VPN		This feature adds MIB support for IETF RFC 6407, The Group Domain of Interpretation. This feature supports only the objects related to the GDOI MIB IETF standard. This feature also provides a command that displays whether devices on the network are running versions of GET VPN software that support the GDOI MIB. The GDOI MIB consists of objects and notifications that include information about GDOI groups, GM and KS peers, as well as the policies that are created or downloaded. The following command was introduced: **snmp-server enable traps gdoi.**
XE 3.16 GETVPN GDOI/COOP MIBS		The following command was modified: **snmp-server enable traps gdoi.**