

GET VPN GM Removal and Policy Trigger

The GET VPN GM Removal and Policy Trigger feature lets you easily remove unwanted group members (GMs) from the group encrypted transport (GET) VPN network, provides a rekey triggering method to install new security associations (SAs) and remove obsolete SAs, and lets you check whether devices are running versions of GET VPN software that support these capabilities.

Note Overlapping ACLs in GETVPN groups are prohibited. It is essential to clearly state and enforce this policy to avoid configuration issues that can lead to security vulnerabilities or operational problems within the VPN network.

- Information About GM Removal and Policy Trigger, on page 1
- How to Configure GET VPN GM Removal and Policy Trigger, on page 5
- Configuration Examples for GET VPN GM Removal and Policy Trigger, on page 10
- Additional References for GET VPN GM Removal and Policy Trigger, on page 13
- Feature Information for GET VPN GM Removal and Policy Trigger, on page 13

Information About GM Removal and Policy Trigger

GET VPN Software Versioning

GET VPN software versions are of the form

major-version.minor-version.mini-version

where

- *major-version* defines compatibility for all GET VPN devices.
- *minor-version* defines compatibility for key server (KS)-to-KS (cooperative key server) associations and for GM-to-GM interoperability.
- *mini-version* tracks feature changes that have no compatibility impact.

For example, the base version (for all prior GET VPN features) is 1.0.1. Also, for example, the version that contains the GM removal feature and the policy replacement feature is 1.0.2, which means that these features

are fully backward compatible with the base version (despite the introduction of behavior in these features for triggered rekeys).

GMs send the GET VPN software version to the KS in the vendor-ID payload during Internet Key Exchange (IKE) phase 1 negotiation (which is defined in RFC 2408, *Internet Security Association and Key Management Protocol [ISAKMP]*). KSs send the software version to other cooperative KSs in the version field of the cooperative KS announcement (ANN) messages. Cooperative KSs also synchronize their lists of versions that each GM is using.

The GM removal feature and the policy replacement feature each provide a command that you run on the KS (or primary KS) to find devices in the group that do not support that feature.

GM Removal

Without the GM removal and policy replacement features, you would need to complete the following steps to remove unwanted GMs from a group:

1. Revoke the phase 1 credential (for example, the preshared key or one or more PKI certificates).
2. Clear the traffic encryption key (TEK) and key encryption key (KEK) database on the KS.
3. Clear the TEK and KEK database on each GM individually and force each GM to re-register.

The third step is time-consuming when a GET VPN group serves thousands of GMs. Also, clearing the entire group in a production network might cause a network disruption. The GET VPN GM Removal and Policy Trigger feature automates this process by introducing a command that you enter on the KS (or primary KS) to create a new set of TEK and KEK keys and propagate them to the GMs.

GM Removal Compatibility with Other GET VPN Software Versions

You should use the GET VPN GM Removal and Policy Trigger feature only after all devices in the GET VPN network are upgraded to GET VPN software versions that support this feature. Otherwise, secondary KSs or GMs running older software will ignore the GM removal message and continue to encrypt and decrypt traffic using the old SAs. This behavior causes network traffic disruption.

This feature provides a command that you use on the KS (or primary KS) to check whether all devices in the network are running versions that support GM removal. When the primary KS tries to remove GMs in a network containing devices that do not support GM removal, a warning message appears. For more information, see the “Ensuring That GMs Are Running Software Versions That Support GM Removal” section.

GM Removal with Transient IPsec SAs

The GET VPN GM Removal and Policy Trigger feature provides a command that you use on the KS (or primary KS) to trigger GM removal with transient IPsec SAs. This behavior shortens key lifetimes for all GMs and causes them to re-register before keys expire. During GM removal, no network disruption is expected, because traffic continues to be encrypted and decrypted using the transient IPsec SA until its lifetime expires. For more information, see the “Removing GMs with Transient IPsec SAs” section.

GM Removal with Immediate IPsec SA Deletion

The GET VPN GM Removal and Policy Trigger feature provides an optional keyword that you can use on the KS (or primary KS) to force GMs to delete old TEKs and KEKs immediately (without using transient SAs) and re-register. However, this behavior can cause a disruption to the data plane, so you should use this

method only for important security reasons. For more information, see the “Removing GMs and Deleting IPsec SAs Immediately” section.

Policy Replacement and Rekey Triggering

The GET VPN GM Removal and Policy Trigger feature provides a new rekey triggering method to remove obsolete SAs and install new SAs.

Inconsistencies Regarding Which TEK and KEK Policy Changes Will Trigger Rekeys

Without this feature, there are inconsistencies regarding which TEK and KEK policy changes will trigger rekeys:

- Multiple rekeys could be sent during the course of security policy updates.
- Some policy changes (for example, transform set, profile, lifetime, and anti-replay) will install new SAs on GMs; however, the SAs from the existing policies remain active until their lifetimes expire.
- Some policy changes (for example, a TEK’s access control entry/access control list (ACE/ACL) changes) will install new SAs on GMs and take effect immediately. However, the obsolete SAs are kept in each GM’s database (and can be displayed using the **show crypto ipsec sa** command until their lifetimes expire).

For example, if the KS changes the policy from Data Encryption Standard (DES) to Advanced Encryption Standard (AES), when the GM receives this triggered rekey, it installs the new SAs (for example, for AES) and shortens the lifetimes of the old SAs (for example, for DES). The GM continues to encrypt and decrypt traffic using the old SAs until their shortened lifetimes expire.

Following is the formula to calculate the shortened lifetime:

TEK_SLT = MIN(TEK_RLT, MAX(90s, MIN(5%(TEK_CLT), 3600s)))

where

- TEK_SLT is the TEK shortened lifetime
- TEK_RLT is the TEK remaining lifetime
- TEK_CLT is the TEK configured lifetime

The following table summarizes the inconsistencies regarding rekeys.

Table 1: Rekey Behavior After Security Policy Changes

Policy Changes	Rekey Sent?	Rekey Behavior After Policy Changes
TEK: SA lifetime	No	The old SA remains active until its lifetime expires. The new lifetime will be effective after the next scheduled rekey. Even if you enter the **clear crypto sa** command, it will re-register and download the old SA with the old lifetime again.
TEK: IPSEC transform set	Yes	The SA of the old transform set remains active until its lifetime expires.

Policy Changes	Rekey Sent?	Rekey Behavior After Policy Changes
TEK: IPSEC profile	Yes	The SA of the old profile remains active until its lifetime expires.
TEK: Matching ACL	Yes	Outbound packet classification immediately uses the ACL. But the old SAs remain in the SA database (you can view them by using the **show crypto ipsec sa** command).
TEK: Enable replay counter	Yes	But the old SA without counter replay remains active until its lifetime expires.
TEK: Change replay counter value	No	The SA with a new replay counter is sent out in the next scheduled rekey.
TEK: Disable replay counter	Yes	But the old SA with counter replay enabled remains active until its lifetime expires.
TEK: Enable TBAR	Yes	But the old SA with time-based anti-replay (TBAR) disabled remains active until its lifetime expires.
TEK: Change TBAR window	No	The SA with a new TBAR window will be sent out in the next scheduled rekey.
TEK: Disable TBAR	Yes	But the old SA with TBAR enabled remains active until its lifetime expires.
TEK: Enable receive-only	Yes	Receive-only mode is activated right after the rekey.
TEK: Disable receive-only	Yes	Receive-only mode is deactivated right after the rekey.
KEK: SA lifetime behavior	No	The change is applied with the next rekey.
KEK: Change authentication key	Yes	The change is applied immediately.
KEK: Change crypto algorithm	Yes	The change is applied immediately.

This feature solves these problems by ensuring consistency. With this feature, GET VPN policy changes alone will no longer trigger a rekey. When you change the policy (and exit from global configuration mode), a syslog message appears on the primary KS indicating that the policy has changed and a rekey is needed. This feature provides a new command that you then enter on the KS (or primary KS) to send a rekey (that is based on the latest security policy in the running configuration).

This feature also provides an extra keyword to the new command to force a GM receiving the rekey to remove the old TEKs and KEK immediately and install the new TEKs and KEK. Therefore, the new policy takes effect immediately without waiting for old policy SAs to expire. (However, using this keyword could cause a temporary traffic discontinuity, because all GMs might not receive the rekey message at the same time.)

Policy Replacement and Rekey Triggering Compatibility with Other GET VPN Software Versions

You should use rekey triggering only after all devices in the GET VPN network are upgraded to GET VPN software versions that support this feature. For GMs running older versions that do not yet support the **crypto gdoi ks** command, the primary KS uses the software versioning feature to detect those versions and only triggers a rekey without sending instruction for policy replacement. Therefore, when a GM receives the rekey,

it installs the new SAs but does not shorten the lifetimes of the old SAs. (This behavior is the same as the prior rekey method and ensures backward compatibility for devices that cannot support policy replacement.)

This 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 policy replacement. For more information, see the "Ensuring That GMs Are Running Software Versions That Support Policy Replacement" section.

How to Configure GET VPN GM Removal and Policy Trigger

Ensuring That GMs Are Running Software Versions That Support GM Removal

You should use the GET VPN GM Removal and Policy Trigger feature only after all devices in the GET VPN network are upgraded to GET VPN software versions that support this feature. Otherwise, secondary KSs or GMs that are running older software will ignore the GM removal message and continue to encrypt and decrypt traffic using the old SAs. This behavior causes network traffic disruption.

Perform this task on the KS (or primary KS) to ensure that all devices in the network support GM removal.

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	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 gm-removal** **Example:** `Device# show crypto gdoi feature gm-removal`	Displays the version of the GET VPN software running on each KS and GM in the GET VPN network and displays whether that device supports GM removal.
Step 3	**show crypto gdoi feature gm-removal | include No** **Example:** `Device# show crypto gdoi feature gm-removal | include No`	(Optional) Displays only those devices that do not support GM removal.

Removing GMs with Transient IPsec SAs

Perform this task on the KS (or primary KS) to trigger removal of GMs with transient IPsec SAs.

SUMMARY STEPS

1. **enable**
2. **clear crypto gdoi** [**group** *group-name*] **ks members**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear crypto gdoi** [**group** *group-name*] **ks members** **Example:** `Device# clear crypto gdoi ks members`	Creates a new set of TEK and KEK keys. This command also sends out GM removal messages to all GMs to clean up their old TEK and KEK databases.

Examples

A message appears on the KS as follows:

```
Device# clear crypto gdoi ks members

% This GM-Removal message will shorten all GMs' key lifetimes and cause them to
re-register before keys expiry.
Are you sure you want to proceed? ? [yes/no]: yes
Sending GM-Removal message to group GET...
```

After each GM receives the GM removal message, the following syslog message appears on each GM:

```
*Jan 28 08:37:03.103: %GDOI-4-GM_RECV_DELETE: GM received delete-msg from KS in group GET.

TEKs lifetime are reduced and re-registration will start before SA expiry
```

Each GM removes the KEK immediately and shortens the lifetimes of the old TEKs as follows:

```
TEK_SLT = MIN(TEK_RLT, MAX(90s, MIN(5%(TEK_CLT), 3600s)))
TEK_SLT: TEK shortened lifetime
TEK_RLT: TEK Remaining LIfeTime
TEK_CLT: TEK Configured LIfeTime
```

Also, the GMs start re-registering to the KS to obtain the new TEKs and KEK according to the conventional re-registration timer and with jitter (random delay) applied. Jitter prevents all GMs from reregistering at the same time and overloading the key server CPU. Only GMs that pass the authentication based on the new credential installed on the KS will receive the new TEKs and KEK.

GM removal should not cause a network disruption, because traffic continues to be encrypted and decrypted using the transient IPsec SA until its lifetime expires.

If you try to use this command on the secondary KS, it is rejected as follows:

```
Device# clear crypto gdoi ks members

ERROR for group GET: can only execute this command on Primary KS
```

Removing GMs and Deleting IPsec SAs Immediately

Perform this task on the KS (or primary KS) to force GMs to delete old TEKs and KEKs immediately and re-register.

SUMMARY STEPS

1. **enable**
2. **clear crypto gdoi** [**group** *group-name*] **ks members now**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear crypto gdoi** [**group** *group-name*] **ks members now** **Example:** `Device# clear crypto gdoi ks members now`	Creates a new set of TEK and KEK keys. This command also sends out GM removal messages to all GMs to clean up their old TEK and KEK databases. **Note** Using the **now** keyword can cause a network disruption to the data plane. Proceed with the GM removal only if a security concern is more important than a disruption.

Examples

A message appears on the KS as follows:

```
Device# clear crypto gdoi ks members now

% This GM-Removal immediate message will cleanup all GMs downloaded policies
% This will cause all GMs to re-register.
Are you sure you want to proceed? ? [yes/no]: yes
Sending GM-Removal message to group GET...
```

After you enter the above command, the KS sends a “remove now” message to each GM to trigger the following actions on each GM:

1. Immediately cleans up its downloaded TEKs and KEK and its policy and returns to fail-open mode (unless fail-close mode is explicitly configured).
2. Sets up a timer with a randomly chosen period within 2 percent of the configured TEK lifetime.
3. When the timer in Step 2 expires, the GM starts re-registering to the KS to download the new TEKs and KEK.

On each GM, the following syslog message is displayed to indicate that the GM will re-register in a random time period:

```
*Jan 28 08:27:05.627: %GDOI-4-GM_RECV_DELETE_IMMEDIATE: GM receive REMOVAL-NOW in group
GET to cleanup downloaded policy now. Re-registration will start in a randomly chosen
period of 34 sec
```

If you try to remove GMs in a network containing devices that do not support GM removal, a warning message appears:

```
Device# clear crypto gdoi ks members now

% This GM-Removal immediate message will cleanup all GMs downloaded policies
% This will cause all GMs to re-register.
Are you sure you want to proceed? ? [yes/no]: yes
WARNING for group GET: some devices cannot support GM-REMOVAL and can cause network
disruption. Please check 'show crypto gdoi feature'.
Are you sure you want to proceed ? [yes/no]: no
```

Ensuring that GMs Are Running Software Versions That Support Policy Replacement

Perform this task on the KS (or primary KS) to check whether all devices in the network support policy replacement.

SUMMARY STEPS

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

DETAILED STEPS

Procedure

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

	Command or Action	Purpose
Step 2	**show crypto gdoi feature policy-replace** **Example:** `Device# show crypto gdoi feature policy-replace`	Displays the version of the GET VPN software running on each KS and GM in the GET VPN network and displays whether that device supports policy replacement.
Step 3	**show crypto gdoi feature policy-replace | include No** **Example:** `Device# show crypto gdoi feature policy-replace | include No`	(Optional) Finds only those devices that do not support policy replacement. For these devices, the primary KS sends only the triggered rekey without instructions for policy replacement. Therefore, when a GM receives the rekey, it installs the new SAs but does not shorten the lifetimes of the old SAs. This behavior is the same as the existing rekey method and ensures backward compatibility.

Triggering a Rekey

If you change the security policy (for example, from DES to AES) on the KS (or primary KS) and exit from global configuration mode, a syslog message appears on the KS indicating that the policy has changed and a rekey is needed. You enter the rekey triggering command as described below to send a rekey based on the latest policy in the running configuration.

Perform this task on the KS (or primary KS) to trigger a rekey.

SUMMARY STEPS

1. **enable**
2. **crypto gdoi ks** [**group** *group-name*] **rekey** [**replace-now**]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**crypto gdoi ks** [**group** *group-name*] **rekey** [**replace-now**] **Example:** `Device# crypto gdoi ks group mygroup rekey`	Triggers a rekey on all GMs. The optional **replace-now** keyword immediately replaces the old TEKs and KEK on each GM to enable the new policy before the SAs expire. **Note** Using the **replace-now** keyword could cause a temporary traffic discontinuity.

Examples

A message appears on the KS as follows:

```
Device# crypto gdoi ks rekey
Device#
*Jan 28 09:17:44.363: %GDOI-5-KS_SEND_UNICAST_REKEY: Sending Unicast Rekey with
policy-replace for group GET from address 10.0.8.1 with seq # 2
```

After the policy change, when each GM receives this triggered rekey, it installs the new SAs (for example, for AES) and shortens the lifetimes of the old SAs (for example, for DES). Each GM continues to encrypt and decrypt traffic using the old SA until its shortened lifetime expires.

If you try to trigger a rekey on the secondary KS, it rejects the command as shown below:

```
Device# crypto gdoi ks rekey
ERROR for group GET: This command must be executed on Pri-KS
```

Configuration Examples for GET VPN GM Removal and Policy Trigger

Example: Removing GMs from the GET VPN Network

Ensuring That GMs Are Running Software Versions That Support GM Removal

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 GM removal feature:

```
Device# show crypto gdoi feature gm-removal

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
    10.0.0.2         1.0.2          Yes
    10.0.0.3         1.0.1          No
```

The following example shows how to find only those devices that do not support GM removal:

```
Device# show crypto gdoi feature gm-removal | include No

       10.0.0.3          1.0.1          No
```

The above example shows that the GM with IP address 10.0.0.3 is running older software version 1.0.1 (which does not support GM removal) and should be upgraded.

Removing GMs with Transient IPsec SAs

The following example shows how to trigger GM removal with transient IPsec SAs. You use this command on the KS (or primary KS).

```
Device# clear crypto gdoi ks members

% This GM-Removal message will shorten all GMs' key lifetimes and cause them to
re-register before keys expiry.
Are you sure you want to proceed? ? [yes/no]: yes
Sending GM-Removal message to group GET...
```

Removing GMs and Deleting IPsec SAs Immediately

The following example shows how to force GMs to delete old TEKs and KEKs immediately and re-register. You use this command on the KS (or primary KS).

```
Device# clear crypto gdoi ks members now

% This GM-Removal immediate message will cleanup all GMs downloaded policies
% This will cause all GMs to re-register.
Are you sure you want to proceed? ? [yes/no]: yes
Sending GM-Removal message to group GET...
```

Example: Triggering Rekeys on Group Members

Ensuring That GMs Are Running Software Versions That Support Rekey Triggering

The following example shows how to use the GET VPN software versioning command on the KS (or primary KS) to display the version of software on devices in the GET VPN network and display whether they support rekey triggering after a policy change:

```
Device# show crypto gdoi feature policy-replace

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
  5.0.0.2          1.0.2          Yes
  9.0.0.2          1.0.1          No
```

The following example shows how to find only those devices that do not support rekey triggering after policy replacement:

```
Device# show crypto gdoi feature policy-replace  | include No

       9.0.0.2          1.0.1          No
```

For these devices, the primary KS sends only the triggered rekey without instructions for policy replacement. Therefore, when a GM receives the rekey, it installs the new SAs but does not shorten the lifetimes of the old SAs.

Triggering a Rekey

The following example shows how to trigger a rekey after you have performed a policy change. In this example, an IPsec policy change (for example, DES to AES) occurs with the **profile gdoi-p2** command:

```
Device# configure terminal
Device(config)# crypto gdoi group GET
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# sa ipsec 1
Device(gdoi-sa-ipsec)# no profile gdoi-p
Device(gdoi-sa-ipsec)# profile gdoi-p2
Device(gdoi-sa-ipsec)# end
Device#

*Jan 28 09:15:15.527: %SYS-5-CONFIG_I: Configured from console by console
*Jan 28 09:15:15.527: %GDOI-5-POLICY_CHANGE: GDOI group GET policy has changed. Use
'crypto gdoi ks rekey' to send a rekey, or the changes will be send in the next scheduled
rekey
Device# crypto gdoi ks rekey
Device#
*Jan 28 09:17:44.363: %GDOI-5-KS_SEND_UNICAST_REKEY: Sending Unicast Rekey with
policy-replace for group GET from address 10.0.8.1 with seq # 2
```

The following example shows the error message that appears if you try to trigger a rekey on the secondary KS:

```
Device# crypto gdoi ks rekey

ERROR for group GET: This command must be executed on Pri-KS
```

Note If time-based antireplay (TBAR) is set, the key server periodically sends a rekey to the group members every 2 hours (7200 sec). In the following example, even though the lifetime is set to 8 hours (28800 sec), the rekey timer is set to 2 hours.

```
Device(config)# crypto ipsec profile atm-profile
Device(ipsec-profile)# set security-association lifetime seconds 28800
!
Device(ipsec-profile)# exit
Device(config)# crypto gdoi group ATM-DSL
Device(config-gdoi-group)# server local
Device(gdoi-sa-ipsec)# sa ipsec 1
!
Device(gdoi-sa-ipsec)# replay time window-size 100
```

The commands **show crypto gdoi gm replay** and **show crypto gdoi ks replay** displays TBAR information.

Additional References for GET VPN GM Removal and Policy Trigger

Related Documents

Related Topic	Document Title
Cisco IOS security commands	*Cisco IOS Security Command References*

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 GET VPN GM Removal and Policy Trigger

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 GET VPN GM Removal and Policy Trigger

Feature Name	Releases	Feature Information
GET VPN GM Removal and Policy Trigger		This feature provides a command that lets you efficiently eliminate unwanted GMs from the GET VPN network, provides a rekey triggering command to install new SAs and remove obsolete SAs, and provides commands that display whether devices on the network are running versions of GET VPN software that support these features. The following commands were introduced or modified: **clear crypto gdoi, crypto gdoi ks, show crypto gdoi.**