Crypto Map IKEv2-IPv6 Payload Configuration Mode Commands

The Crypto Map IKEv2-IPv6 Payload Configuration Mode is used to assign the correct IPSec transform-set from a list of up to four different transform-sets, and to assign Mobile IP addresses.

**Command Modes**

```plaintext
Exec > Global Configuration > Context Configuration > Crypto Map IKEv2-IPv6 Configuration > Crypto Map IKEv2-IPv6 Payload Configuration
```

```plaintext
configure > context context_name > crypto map map_name ikev2-ipv6 > payload payload_name match ipv6
```

Entering the above command sequence results in the following prompt:

```plaintext
[context_name]host_name(cfg-crypto-ikev2-ipv6-payload)#
```

**Important**

The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

- end, on page 1
- exit, on page 2
- ipsec, on page 2
- lifetime, on page 3
- rekey, on page 5

**end**

Exits the current configuration mode and returns to the Exec mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```plaintext
end
```

**Usage Guidelines**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

<table>
<thead>
<tr>
<th>Product</th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privilege</td>
<td>Security Administrator, Administrator</td>
</tr>
</tbody>
</table>

**Syntax Description**

`exit`

**Usage Guidelines**

Use this command to return to the parent configuration mode.

ipsec

Configures the IPSec transform sets to be used for this crypto map payload.

**Important**

HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

<table>
<thead>
<tr>
<th>Product</th>
<th>ePDG</th>
<th>FA</th>
<th>GGSN</th>
<th>HA</th>
<th>HeNBGW</th>
<th>HNBGW</th>
<th>HSGW</th>
<th>MME</th>
<th>P-GW</th>
<th>PDSN</th>
<th>S-GW</th>
<th>SAEGW</th>
<th>SCM</th>
<th>SecGW</th>
<th>SGSN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privilege</td>
<td>Security Administrator</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Exec > Global Configuration > Context Configuration > Crypto Map IKEv2-IPv6 Configuration > Crypto Map IKEv2-IPv6 Payload Configuration

```
configure > context context_name > crypto map map_name ikev2-ipv6 > payload payload_name match ipv6
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-ikev2-ipv6-payload)#
```

### Syntax Description

- `ipsec transform-set list transform_set_name [ transform_set_name ] [ transform_set_name ] [ transform_set_name ]`
- `no ipsec transform-set list`

- `no`
  Disables the transform set list.

- `ipsec transform-set list transform_set_name`
  Specifies the context-level name of the IKEv2 IPsec Child Security Association (SA) transform set to be used in the crypto map payload. This is a space-separated list. From 1 to 4 transform sets can be entered. `transform_set_name` is an alphanumeric string of 1 through 127 characters.

### Usage Guidelines

Use this command to list the IPSec transform set(s) to use in this crypto map payload.

### Example

The following command configures IPSec transform sets named `ipset1` and `ipset2` to be used in this crypto template payload:

```
ipsec transform-set list ipset1 ipset2
```

### lifetime

Configures the number of seconds and/or kilobytes for IPsec Child SAs derived from this crypto template payload to exist.

#### Important

HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

### Product

- ePDG
- FA
- GGSN
- HA
- HeNBGW
Privilege
Administrator

Command Modes
Exec > Global Configuration > Context Configuration > Crypto Map IKEv2-IPv6 Configuration > Crypto Map IKEv2-IPv6 Payload Configuration

```
configure > context context_name > crypto map map_name ikev2-ipv6 > payload payload_name match ipv6
```

Entering the above command sequence results in the following prompt:

```
{context_name}host_name(cfg-crypto-ikev2-ipv6-payload)#
```

Syntax Description
```
lifetime { sec [ kilo-bytes kbytes ] | kilobytes kbytes }

default lifetime
```

default

Returns the lifetime value to the default setting of 86400 seconds.

sec

Specifies the number of seconds for IPSec Child Security Associations derived from this crypto template payload to exist. sec must be an integer from 60 through 604800. Default: 86400

kilo-bytes kbytes

Specifies lifetime in kilobytes for IPSec Child Security Associations derived from this Crypto Map. kbytes must be an integer from 1 through 2147483648.

Usage Guidelines

Use this command to configure the number of seconds and/or kilobytes for IPSec Child Security Associations derived from this crypto template payload to exist.

Example

The following command configures the IPSec child SA lifetime to be 120 seconds:

```
lifetime 120
```
rekey

Configures child security association rekeying.

---

**Important**

HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

---

**Product**

- ePDG
- FA
- GGSN
- HA
- HeNBGW
- HNBGW
- HSGW
- MME
- P-GW
- PDSN
- S-GW
- SAEGW
- SCM
- SecGW
- SGSN

**Privilege**

Security Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Crypto Map IKEv2-IPv6 Configuration > Crypto Map IKEv2-IPv6 Payload Configuration

```
configure > context context_name > crypto map map_name ikev2-ipv6 > payload payload_name match ipv6
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-ikev2-ipv6-payload)#
```

**Syntax Description**

```
rekey [ keepalive ]
[ default | no ] rekey
```

**default**

Returns the feature to the default setting of disabled.
no
Disables this feature.

keepalive
If specified, a session will be rekeyed even if there has been no data exchanged since the last rekeying operation. By default rekeying is only performed if there has been data exchanged since the previous rekey.

**Usage Guidelines**

Use this command to enable or disable the ability to rekey IPSec Child SAs after approximately 90% of the Child SA lifetime has expired. The default, and recommended setting, is not to perform rekeying. No rekeying means the P-GW will not originate rekeying operations and will not process CHILD SA rekeying requests from the MS.

**Example**
The following command disables rekeying:

no rekey