Crypto Debug Commands on Cisco IOS XR Software

This chapter describes the Cisco IOS XR software crypto debug commands.

For high-level, conceptual information about using debug commands generally, see *Using Debug Commands on IOS XR Software*, Release 3.2.

debug crypto engine

To display information about crypto engines encryption and decryption functions, use the **debug crypto engine** command in EXEC mode. To disable debugging output, use the no form of this command.

debug crypto engine {**all** | **dump** | **error** | **event** | **keyevent**}

no debug crypto engine {**all** | **dump** | **error** | **event** | **keyevent**}

Syntax Description

all	Displays all crypto engine transactional information.
dump	Displays the hex dump for all crypto engine messages.
error	Displays crypto engine transactional errors.
event	Displays crypto engine transactional event.
keyevent	Displays events related to keys.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Use the **debug crypto engine** command to display information pertaining to the crypto engine, such as when Cisco IOS software is performing encryption or decryption operations.

Note The crypto engine is the actual mechanism that performs encryption and decryption. A crypto engine can be software or a hardware accelerator. Some platforms can have multiple crypto engines; therefore, the router will have multiple hardware accelerators.

Examples

The following is sample output from the **debug crypto engine** command using the **events** keyword:

```
RP/0/RP0/CPU0:router# debug crypto engine events

RP/0/RP0/CPU0:Aug 28 00:28:44.303 MET2MET,M3.5.0/: ce_cmd[65679]:
crypto_generate_dsa_keypair ...
RP/0/RP0/CPU0:Aug 28 00:28:44.455 MET2MET,M3.5.0/: ce_cmd[65679]:
crypto_convert_dsa_pubkey_in_der ...
```

```
RP/0/RP0/CPU0:Aug 28 00:28:44.456 MET2MET,M3.5.0/: ce_cmd[65679]: crypto_set_key_req
RP/0/RP0/CPU0:Aug 28 00:28:44.461 MET2MET,M3.5.0/: ce_cmd[65679]: crypto_set_key_req
```

debug crypto ipsec

To display IP Security (IPSec) events, use the **debug crypto ipsec** command in EXEC mode. To disable debugging output, use the **no** form of this command.

debug crypto ipsec {**all** | **distribute** | **errors** | **events** | **packets** | **sa-id** | **traffic** | **tunnel-interface**}

no debug crypto ipsec {**all** | **distribute** | **errors** | **events** | **packets** | **sa-id** | **traffic** | **tunnel-interface**}

Syntax Description

all	Enables all debugs for events, errors, traffic, and distribute.
distribute	Displays ipsec session control distribution info (between the IPSec control processes).
errors	Displays crypto engine transactional errors.
events	Displays crypto engine transactional events.
packets	Displays IPSec packet information.
sa-id	Displays information for a specific SA id.
traffic	Displays IPSec data traffic information.
tunnel-interface	Ddisplays IPSec tunnel interface event information.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Examples

The following is sample output from the **debug crypto ipsec** command using the **errors** keyword:

```
RP/0/RP0/CPU0:router# debug crypto ipsec errors

RP/0/RP1/CPU0:Apr 26 21:47:37.286 PST8PST: ipsec_pp[207]: Rcvd: Pulse Msg: 0
RP/0/RP1/CPU0:Apr 26 21:47:37.286 PST8PST: ipsec_pp[207]: Rcvd: Packet from ICF pak_handle
= eace99f7, flow_id = 2
RP/0/RP1/CPU0:Apr 26 21:47:37.286 PST8PST: ipsec_pp[207]: Failed to proc pak from ICF -
Flow 2
RP/0/RP1/CPU0:Apr 26 21:48:01.286 PST8PST: ipsec_pp[207]: Rcvd: Pulse Msg: 0
```

```
RP/0/RP1/CPU0:Apr 26 21:48:01.287 PST8PST: ipsec_pp[207]: Rcvd: Packet from ICF pak_handle
= eacfe677, flow_id = 2
RP/0/RP1/CPU0:Apr 26 21:48:01.288 PST8PST: ipsec_pp[207]: Failed to proc pak from ICF -
Flow 2
RP/0/RP1/CPU0:Apr 26 21:48:54.333 PST8PST: ipsec_pp[207]: Rcvd: Pulse Msg: 0
```

debug crypto isakmp

To display messages about Internet Key Exchange (IKE) events, use the **debug crypto isakmp** command in EXEC mode. To disable debugging output, use the **no** form of this command.

debug crypto isakmp {**detail | error | flow | packet | payload | trace | unit**}

no debug crypto isakmp {**detail | error | flow | packet | payload | trace | unit**}

Syntax Description

detail	Displays ISAKMP protocol details (including packet level information).
error	Displays ISAKMP protocol error information.
flow	Displays ISAKMP protocol flow information.
packet	Displays ISAKMP packet information.
payload	Displays ISAKMP protocol payload information.
trace	Displays procotocl trace information.
unit	Displays development level unit information (which is specific to the implementation).

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Examples

The following is sample output from the **debug crypto isakmp** command:

```
RP/0/RP0/CPU0:router# debug crypto isakmp

RP/0/RP0/CPU0:Aug 3 20:08:30.149 : rsvp[117]: Forwarding PATH message on POS0/3/0/0 from
51.51.51.51 to 70.70.70.70 (length=212 bytes, TTL=254, TOS=0xff, flags=0x1 ,RA)
```