Cisco IOS XR System Security Debug Command Reference

Cisco IOS XR Software Release 3.7.0

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

Text Part Number: OL-16982-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0807R)

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

Cisco IOS XR System Security Debug Command Reference
© 2008 Cisco Systems, Inc. All rights reserved.

Preface

This preface contains high-level information about Cisco documentation. It includes the following sections:

- Changes to This Document, page DSR-iii
- Obtaining Documentation, Obtaining Support, and Security Guidelines, page DSR-iii

Changes to This Document

Table 1 lists the technical changes made to this document since it was first printed.

Table 1 Changes to This Document

Revision	Date	Change Summary
OL-16982-01	August 2008	Initial release of this document.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

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 Cisco IOS XR Software*, Release 3.6.0.

debug crypto ace

To display information related to the IPSec SPA Crypto Engine Driver, use the **debug crypto ace** command in EXEC mode. To disable debugging output, use the **no** form of this command.

debug crypto ace {**all** | **error** | **ha** | **hapi** | **ike** | **ipsec** | **stats**} [**location** *node-id*] [**job** *job-id* | **process** *pid*]

no debug crypto ace {**all** | **error** | **ha** | **hapi** | **ike** | **ipsec** | **stats**} [**location** *node-id*] [**job** *job-id* | **process** *pid*]

Syntax Description

all	Enables all debug flags in the Application Control Engine (ACE) driver.
error	Displays errors in the Crypto Engine driver.
ha	Enables the debug High Availability (HA) in the ACE driver.
hapi	Displays debug HAPI messages.
ike	Enables debug Internet Key Exchange (IKE) in the ACE driver.
ipsec	Enables debug IP Security (IPSec) in the ACE driver.
stats	Enables IPSec stats collection.
location *node-id*	(Optional) Displays debugging information for a node. The *node-id* argument is entered in the *rack/slot/module* notation.
job *job-id*	(Optional) Displays debugging information for a job.
process *pid*	(Optional) Displays debugging information for a process.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.0	This command was supported on the Cisco XR 12000 Series Router.
Release 3.5.0	This command is not supported.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

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*.

Debugging output is assigned high priority in the CPU process and, therefore, can affect system performance. For more information about the impact on system performance when using debug commands, refer to *Using Debug Commands on Cisco IOS XR Software*.

Task ID

Task ID	Operations
crypto	read

Examples

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

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

RP/0/RP0/CPU0:router#RP/0/4/CPU0:Jan 18 12:19:50.014 : ike[379]: Crypto tunnel is UP  .
Peer 5.0.1.1:500 f_vrf:  default i_vrf:  default   Id: 83886337
LC/0/1/CPU0:Jan 18 12:19:49.930 : ace_driver_lc_1[268]: (ace_ipsec_grp_msg_hdlr):
msg_type=1 mlen=556 sender=(type:1 nodeid:0x40)
LC/0/1/CPU0:Jan 18 12:19:49.931 : ace_driver_lc_1[268]:
(ace_ipsec_handle_create_flows_cmd)
LC/0/1/CPU0:Jan 18 12:19:49.932 : ace_driver_lc_1[268]:
(ace_ipsec_handle_create_flow_cmd): ifHandle=0x501b880, flow=504
LC/0/1/CPU0:Jan 18 12:19:49.933 : ace_driver_lc_1[268]:
(ace_ipsec_handle_single_create_flow_cmd): ifHandle=0x501b880 flowId=504 vrf=0x60000000
LC/0/1/CPU0:Jan 18 12:19:49.934 : ace_driver_lc_1[268]: CREATE FLOW ifHandle=83998848,
flowId=504
LC/0/1/CPU0:Jan 18 12:19:49.935 : ace_driver_lc_1[268]:  instance:1, flags=0x1008
ipSrcAddr=0x4000101 ipDstAddr=0x5000101 aclName=acl1 lineNumber=10
LC/0/1/CPU0:Jan 18 12:19:49.936 : ace_driver_lc_1[268]: lifetime: kb=4194303 seconds=3600
soft_vol_kb=4193634 soft_sec=3551
LC/0/1/CPU0:Jan 18 12:19:49.937 : ace_driver_lc_1[268]: idleTimeout=0 localUdpPort=0
remoteUdpPort=0 origRemoteIpAddr=0x0
LC/0/1/CPU0:Jan 18 12:19:49.938 : ace_driver_lc_1[268]: fVrfId=60000000 iVrfId=60000000
mibIndex=0
LC/0/1/CPU0:Jan 18 12:19:49.939 : ace_driver_lc_1[268]: antiReplayWindowSize=64
dpdIdleIntervalSec=0
LC/0/1/CPU0:Jan 18 12:19:49.941 : ace_driver_lc_1[268]: transform[ESP]=esp-256-aes
LC/0/1/CPU0:Jan 18 12:19:49.941 : ace_driver_lc_1[268]: transform[AH]=
LC/0/1/CPU0:Jan 18 12:19:49.943 : ace_driver_lc_1[268]: In: seq=0 octHigh=0 octLow=0
LC/0/1/CPU0:Jan 18 12:19:49.944 : ace_driver_lc_1[268]: Out: seq=0 octHigh=0 octLow=0
LC/0/1/CPU0:Jan 18 12:19:49.945 : ace_driver_lc_1[268]:  Inbound ESP SPI : 0x2d9bfc56
key_len=32
LC/0/1/CPU0:Jan 18 12:19:49.946 : ace_driver_lc_1[268]:  Outbound ESP SPI : 0xd3bb8433
key_len=32
LC/0/1/CPU0:Jan 18 12:19:49.947 : ace_driver_lc_1[268]: (fill_ha_update_params): flags 0x1
windowTopSeqNum=0 octetsHigh=0 octetsLow=0
LC/0/1/CPU0:Jan 18 12:19:49.948 : ace_driver_lc_1[268]: (fill_ha_update_params): flags 0x0
windowTopSeqNum=0 octetsHigh=0 octetsLow=0
LC/0/1/CPU0:Jan 18 12:19:49.950 : ace_driver_lc_1[268]: (ace_ipsec_add_flow):
ifHandle=0x501b880 , flow=504 instance=1
LC/0/1/CPU0:Jan 18 12:19:49.951 : ace_driver_lc_1[268]: (ace_add_ivrf_entry):
ivrf_id=60000000
LC/0/1/CPU0:Jan 18 12:19:49.952 : ace_driver_lc_1[268]: (ace_update_ivrf_refcount):
ivrfId=0x60000000 add=1 cur_ref_count=0
LC/0/1/CPU0:Jan 18 12:19:49.958 : ace_driver_lc_1[268]: (ace_ipsec_hapi_resp_cb)
LC/0/1/CPU0:Jan 18 12:19:49.959 : ace_driver_lc_1[268]: (ace_ipsec_handle_ikea_ack): IKEA
COMB_SET_SA1 status=No error errcode=0x0
LC/0/1/CPU0:Jan 18 12:19:49.960 : ace_driver_lc_1[268]: (ace_ipsec_handle_end_of_chain):
CREATE_FLOW: ifHandle=0x501b880. flags 0 sender: type=1 node0x40
LC/0/1/CPU0:Jan 18 12:19:49.961 : ace_driver_lc_1[268]: (ace_ipsec_hapi_resp_cb)
LC/0/1/CPU0:Jan 18 12:19:49.962 : ace_driver_lc_1[268]: (ace_ipsec_handle_ikea_ack): IKEA
COMB_SET_SA1 status=No error errcode=0x0
LC/0/1/CPU0:Jan 18 12:19:49.963 : ace_driver_lc_1[268]: (ace_ipsec_handle_end_of_chain):
CREATE_FLOW: ifHandle=0x501b880. flags 0 sender: type=1 node0x40
LC/0/1/CPU0:Jan 18 12:19:49.964 : ace_driver_lc_1[268]: (ace_ipsec_handle_end_of_bundle):
CREATE_FLOW: ifHandle=0x501b880
```

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.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

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 encryption or decryption operations are performed.

Debugging output is assigned high priority in the CPU process and, therefore, can affect system performance. For more information about the impact on system performance when using debug commands, refer to *Using Debug Commands on Cisco IOS XR Software*.

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.

Task ID

Task ID	Operations
crypto	read

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 {*sa-id* {**all** | **errors** | **events** | **stats** | **traffics**}

no debug crypto ipsec {*sa-id* {**all** | **errors** | **events** | **stats** | **traffics**}

debug crypto ipsec {**crypto-engine** | **detail** | **distribute** | **errors** | **events** | **packets** | **rri** | **spi** | **stats** | **traffics** | **tunnel-interface**} [**location** *node-id*]}

no debug crypto ipsec {**crypto-engine** | **detail** | **distribute** | **errors** | **events** | **packets** | **rri** | **spi** | **stats** | **traffics** | **tunnel-interface**} [**location** *node-id*]}

Syntax Description

sa-id	Displays information for a specific service affecting (SA) ID. Range is 1 to 500.
all	Enables all debugs for events, errors, traffic, and distribute.
errors	Displays crypto engine transactional errors.
events	Displays crypto engine transactional events.
stats	Displays all IPSec statistics.
traffics	Displays IPSec data traffic information.
crypto-engine	Displays all crypto-engine IPSec events.
detail	Displays details for all IPSec events.
distribute	Displays IPSec session control distribution info (between the IPSec control processes).
packets	Displays IPSec packet information.
rri	Displays all reverse route injection (RRI) IPSec events.
spi	Displays all security parameter index (SPI) events.
tunnel-interface	Displays IPSec tunnel interface event information.
location *node-id*	(Optional) Displays IPSec information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

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.
Release 3.3.0	Command structure was rearranged and the **location** keyword was added.

Release	Modification
Release 3.4.0	The **crypto-engine** and **spi** keywords were introduced on the Cisco XR 12000 Series Router. The **detail**, **rri**, and **stats** keywords were introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

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*.

Debugging output is assigned high priority in the CPU process and, therefore, can affect system performance. For more information about the impact on system performance when using debug commands, refer to *Using Debug Commands on Cisco IOS XR Software*.

Task ID

Task ID	Operations
crypto	read

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 [**error** | **terse**]

no debug crypto isakmp [**error** | **terse**]

Syntax Description

error	Displays the failures or errors encountered in the IKE code.
terse	Displays the non-failure occurrences, based on the message exchange of the protocol.

DefaultsDefaults

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.
Release 3.3.0	No modification.
Release 3.4.0	The following keywords have been removed: **detail**, **error**, **flow**, **packet, payload**, **trace**, and **unit**.
Release 3.5.0	The following keywords have been added: **error** and **terse**.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

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*.

Debugging output is assigned high priority in the CPU process and, therefore, can affect system performance. For more information about the impact on system performance when using debug commands, refer to *Using Debug Commands on Cisco IOS XR Software*.

Task ID

Task ID	Operations
crypto	read

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)
```

debug crypto pki

To display messages about public key infrastructure (PKI) client events, use the **debug crypto pki** command in EXEC mode. To disable debugging output, use the **no** form of this command.

debug crypto pki {**errors** | **messages** | **transactions**}

no debug crypto pki {**errors** | **messages** | **transactions**}

Syntax Description

errors	Displays PKI error messages.
messages	Displays PKI input and output messages.
transactions	Displays PKI transactions.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

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*.

Debugging output is assigned high priority in the CPU process and, therefore, can affect system performance. For more information about the impact on system performance when using debug commands, refer to *Using Debug Commands on Cisco IOS XR Software*.

Task ID

Task ID	Operations
crypto	read

Examples

The following is an example of the use of the **debug crypto pki** command:

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

Authentication, Authorization, and Accounting Debug Commands on Cisco IOS XR Software

This chapter describes the Cisco IOS XR software authentication, authorization, and accounting (AAA) debug commands.

For high-level, conceptual information about using **debug** commands generally, see *Using Debug Commands on Cisco IOS XR Software*, Release 3.6.0.

debug aaa

To display authentication, authorization, and accounting (AAA) information originating from applications using AAA, use the **debug aaa** command in EXEC mode. To disable debugging output, use the **no** form of this command.

debug aaa {**accounting** | **all** | **authentication** | **authorization** | **comm** | **configuration** | **detail** | **task**}

no debug aaa {**accounting** | **all** | **authentication** | **authorization** | **comm** | **configuration** | **detail** | **task**}

Syntax Description

accounting	Displays accounting debug information from AAA applications.
all	Displays all debug information from AAA applications.
authentication	Displays authentication debug information from AAA applications.
authorization	Displays debug information for AAA authorization.
comm	Displays information related to connections made between the AAA applications and AAA daemon (locald).
configuration	Displays debug information related configuration of AAA parameters.
detail	Displays additional debug information. Use this keyword when other debug commands are not sufficiently helpful.
task	Displays debug information related to task ID processing.

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.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

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*.

The information displayed by the **debug aaa** command **accounting** keyword is independent of the accounting protocol used to transfer the accounting information to a server.

Use the **authentication** and **authorization** keywords to display the authentication and authorization methods in use and the results of these methods.

Debugging output is assigned high priority in the CPU process and, therefore, can affect system performance. For more information about the impact on system performance when using debug commands, refer to *Using Debug Commands on Cisco IOS XR Software*.

Note To view the debug information about how the system is processing AAA requests, use the **debug locald** commands.

Task ID

Task ID	Operations
aaa	read

Examples

The following example shows how to enable debug information for AAA accounting and the resulting show output:

```
RP/0/RP0/CPU0:router# debug aaa accounting
RP/0/RP0/CPU0:router# show run

RP/0/RP0/CPU0:Aug 18 01:11:17.613: exec[65686]: Composing an message for service CMD
RP/0/RP0/CPU0:Aug 18 01:11:17.646: exec[65686]: Sending request message to the server
RP/0/RP0/CPU0:Aug 18 01:11:17.732: exec[65686]: Interpreting the reply from the server
RP/0/RP0/CPU0:Aug 18 01:11:18.391: nvgen[65723]: Getting details on ttyname '/dev/con0'
```

Related Commands

Command	Description
debug radius / **debug tacacs**	Provides detailed information about protocol-level activities.
debug locald	Provides detailed information about AAA processing.
show accounting	Displays accounting information.

debug acctd

To enable debugging for basic acctd processes, use the **debug acctd** command in EXEC mode. To disable debugging output, use the **no** form of this command.

debug acctd [**configuration** | **detail**]

no debug acctd [**configuration** | **detail**]

Syntax Description

configuration	Displays accounting configuration debug information.
detail	Displays detailed accounting debug information.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.5.0	This command was supported on the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

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*.

Debugging output is assigned high priority in the CPU process and, therefore, can affect system performance. For more information about the impact on system performance when using debug commands, refer to *Using Debug Commands on Cisco IOS XR Software.*

Task ID

Task ID	Operations
aaa	read

Examples

The following example shows how to enable debug information for acctd processes and the resulting show output:

```
RP/0/0/CPU0:router# debug acctd
RP/0/0/CPU0:router# debug acctd detail

RP/0/0/CPU0:Feb 23 02:47:46.000 : acctd[373]: Transmitting records for session system (0
records)
RP/0/0/CPU0:Feb 23 02:47:46.000 : acctd[373]: Stop Periodic Timer for sess 14,
RP/0/0/CPU0:Feb 23 02:47:46.001 : acctd[373]: Transmitting records for session 14 (2
records)
```

```
RP/0/0/CPU0:Feb 23 02:47:46.001 : acctd[373]: Attempt to send record 1, svc:ike
option:UPDATE flags:UPDATE uflag:Stop pid:504031 sid:14
RP/0/0/CPU0:Feb 23 02:47:46.001 : acctd[373]: Managing update for id:1 service:ike
options:UPDATE uflag:Stop utype:Periodic pid:504031 sid:14
RP/0/0/CPU0:Feb 23 02:47:46.001 : acctd[373]: Attempt to send record 1, svc:ike
option:STOP flags:INIT uflag:Stop pid:504031 sid:14
RP/0/0/CPU0:Feb 23 02:47:46.001 : acctd[373]: Managing update for id:1 service:ike
options:STOP uflag:Stop utype:Periodic pid:504031 sid:14
```

Related Commands

Command	Description
debug radius / **debug tacacs**	Provides detailed information about protocol-level activities.
debug locald	Provides detailed information about AAA processing.
show accounting	Displays accounting information.

debug locald

To display debug information about AAA request processing by the AAA daemon (**locald**), use the **debug locald** command in EXEC mode. To disable debugging output, use the **no** form of this command.

debug locald {**accounting | authentication | authorization | configuration | connections | db | detail**}

no debug locald {**accounting | authentication | authorization | configuration | connections | db | detail**}

Syntax Description

accounting	Displays locald accounting debug information.
authentication	Displays locald authentication debug information.
authorization	Displays locald authorization debug information.
configuration	Displays locald configuration debug information.
connections	Displays locald connection debug information.
db	Displays local database debug information.
detail	Displays detailed local database processing 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.
Release 3.3.0	Corrected command line for missing keyword **authorization** and changed spelling of keyword **connections**.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

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*.

Debugging output is assigned high priority in the CPU process and, therefore, can affect system performance. For more information about the impact on system performance when using debug commands, refer to *Using Debug Commands on Cisco IOS XR Software*.

Task ID

Task ID	Operations
aaa	read

Examples

The following example shows how to enable debug information for locald accounting and the resulting show output:

```
RP/0/RP0/CPU0:router# debug locald accounting
RP/0/RP0/CPU0:router# show run

RP/0/RP0/CPU0:Aug 18 01:13:01.968: locald[233]: Interpreting the request message
RP/0/RP0/CPU0:Aug 18 01:13:01.993: locald[233]: Getting the methods from
accounting/commands/default
RP/0/RP0/CPU0:Aug 18 01:13:02.026: locald[233]: Adding session cisco0/dev/con05 with key
cisco0/dev/con05 to acct btree
RP/0/RP0/CPU0:Aug 18 01:13:02.026: locald[233]: Session cisco0/dev/con05 - add req 8055b3c
to recordsQ, size 1
RP/0/RP0/CPU0:Aug 18 01:13:02.027: locald[233]: Create timer for request id 51
RP/0/RP0/CPU0:Aug 18 01:13:02.027: locald[233]: Session system has no records to send
RP/0/RP0/CPU0:Aug 18 01:13:02.027: locald[233]: Session cisco0/dev/con05 recordsQ size 1,
peek 8055b3c
RP/0/RP0/CPU0:Aug 18 01:13:02.027: locald[233]: Using method <unknown method value> (2001)
RP/0/RP0/CPU0:Aug 18 01:13:02.307: locald[233]: Got account delivery confirmationfor
session 51
RP/0/RP0/CPU0:Aug 18 01:13:02.308: locald[233]: Session system has no records to send
RP/0/RP0/CPU0:Aug 18 01:13:02.308: locald[233]: Session cisco0/dev/con05 has no records to
send
RP/0/RP0/CPU0:Aug 18 01:13:02.308: locald[233]: Removing session cisco0/dev/con05 with key
cisco0/dev/con05 from acct btree
```

debug login

To display login information, use the **debug login** command in EXEC mode**.** To disable debugging output, use the **no** form of this command.

debug login [**detail**]

no debug login [**detail**]

Syntax Description

detail	(Optional) Displays more detailed login AAA processes.

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.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

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*.

Debugging output is assigned high priority in the CPU process and, therefore, can affect system performance. For more information about the impact on system performance when using debug commands, refer to *Using Debug Commands on Cisco IOS XR Software*.

Task ID

Task ID	Operations
aaa	read

Examples

The following example shows how to enable debugging login AAA information:

```
RP/0/RP0/CPU0:router# debug login
```

debug radius

To display information associated with remote authentication dial-in user service (RADIUS), use the **debug radius** command in EXEC mode. To disable debugging output, use the **no** form of this command.

debug radius {**accounting** | **authentication** | **authorization** | **configuration** | **detail** | **io**}

no debug radius {**accounting** | **authentication** | **authorization** | **configuration** | **detail** | **io**}

Syntax Description

accounting	Displays RADIUS accounting debug information.
authentication	Displays RADIUS authentication debug information.
authorization	Displays RADIUS authorization debug information.
configuration	Displays RADIUS configuration debug information.
detail	Displays detailed RADIUS AAA processing debug information.
io	Displays RADIUS I/O messages.

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.
Release 3.3.0	The **io** keyword was added.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

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*.

Debugging output is assigned high priority in the CPU process and, therefore, can affect system performance. For more information about the impact on system performance when using debug commands, refer to *Using Debug Commands on Cisco IOS XR Software*.

Task ID

Task ID	Operations
aaa	read

Examples

The following example shows debug outputs from **RADIUS** when logging in from VTY with RADIUS authentication configured:

```
RP/0/RP0/CPU0:router# debug radius
RP/0/RP0/CPU0:router# show debug all

####  debug flags set from tty 'con0_0_CPU0'  ####
radius basic flag is ON

RP/0/RP0/CPU0:router #RP/0/RP0/CPU0:Aug 18 01:16:24.735: radiusd[267]: [7] Received ASCII
LOGIN/LOGIN from <unknown> with user=, ifh=0x0, tty=/dev/vty0
RP/0/RP0/CPU0:Aug 18 01:16:24.736: radiusd[267]: Sending sync reply (status GETUSER) to
the client
RP/0/RP0/CPU0:Aug 18 01:16:27.857: radiusd[267]: [7] Received ASCII LOGIN/LOGIN from
<unknown> with user=user1, ifh=0x0, tty=/dev/vty0
RP/0/RP0/CPU0:Aug 18 01:16:27.858: radiusd[267]: Sending sync reply (status GETPASS) to
the client
RP/0/RP0/CPU0:Aug 18 01:16:29.584: radiusd[267]: [7] Received ASCII LOGIN/LOGIN from
<unknown> with user=user1, ifh=0x0, tty=/dev/vty0
RP/0/RP0/CPU0:Aug 18 01:16:29.585: radiusd[267]: method = server group map # 1003
RP/0/RP0/CPU0:Aug 18 01:16:29.587: radiusd[267]: Using server group vanquish-rad
RP/0/RP0/CPU0:Aug 18 01:16:29.591: radiusd[267]: Checking server 12.26.37.2 ...
RP/0/RP0/CPU0:Aug 18 01:16:29.621: radiusd[267]: Added standard attribute NAS-IP-Address =
12.22.57.4
RP/0/RP0/CPU0:Aug 18 01:16:29.626: radiusd[267]: Added standard attribute NAS-Port = 130
RP/0/RP0/CPU0:Aug 18 01:16:29.628: radiusd[267]: Added standard attribute NAS-Port-Type =
0 0 0 5 ...
RP/0/RP0/CPU0:Aug 18 01:16:29.630: radiusd[267]: Added standard attribute User Password =
*
RP/0/RP0/CPU0:Aug 18 01:16:29.631: radiusd[267]: RADIUS: Initial Transmit id 28 (16)
12.26.37.2:0, Access-Request, len 64
RP/0/RP0/CPU0:Aug 18 01:16:29.635: radiusd[267]: Attribute User Name = user1^D
RP/0/RP0/CPU0:Aug 18 01:16:29.638: radiusd[267]: Attribute NAS-IP-Address = 12.22.57.4
RP/0/RP0/CPU0:Aug 18 01:16:29.639: radiusd[267]: Attribute NAS-Port = 130
RP/0/RP0/CPU0:Aug 18 01:16:29.640: radiusd[267]: Attribute NAS-Port-Type = 0 0 0 5 ...
RP/0/RP0/CPU0:Aug 18 01:16:29.643: radiusd[267]: Attribute User Password = *
RP/0/RP0/CPU0:Aug 18 01:16:29.649: radiusd[267]: Sent request to 12.26.37.2
RP/0/RP0/CPU0:Aug 18 01:16:29.662: radiusd[267]: Received response from 12.26.37.2
RP/0/RP0/CPU0:Aug 18 01:16:29.663: radiusd[267]: RADIUS: Received id 28 (16) 12.26.37.2:0,
Access-Accept, len 118
RP/0/RP0/CPU0:Aug 18 01:16:29.665: radiusd[267]: Attribute Reply-Message = Hello, is this
the red pill or the blue one?, user1^O
RP/0/RP0/CPU0:Aug 18 01:16:29.666: radiusd[267]: Attribute Login-Service = 0 0 0 0 ...
RP/0/RP0/CPU0:Aug 18 01:16:29.669: radiusd[267]: Attribute Service-Type = EXEC
RP/0/RP0/CPU0:Aug 18 01:16:29.671: radiusd[267]: Attribute 26, len 32, vendor-id 9, vtype
1, vlen 26, value "shell:tasks=#root-system"
RP/0/RP0/CPU0:Aug 18 01:16:29.673: radiusd[267]: Saved authorization data for user user1
RP/0/RP0/CPU0:Aug 18 01:16:29.677: radiusd[267]: Sending sync reply (status PASS) to the
client
RP/0/RP0/CPU0:Aug 18 01:16:30.004: radiusd[267]: [0] Received ACCT START/EXEC from
<unknown> with user=user1, ifh=0x0, tty=/dev/vty0
RP/0/RP0/CPU0:Aug 18 01:16:30.005: radiusd[267]: method = server group map # 1003
RP/0/RP0/CPU0:Aug 18 01:16:30.006: radiusd[267]: Using server group vanquish-rad
RP/0/RP0/CPU0:Aug 18 01:16:30.009: radiusd[267]: Checking server 12.26.37.2 ...
RP/0/RP0/CPU0:Aug 18 01:16:30.012: radiusd[267]: Selected server 12.26.37.2
RP/0/RP0/CPU0:Aug 18 01:16:30.013: radiusd[267]: Added standard attribute User Name =
user1
RP/0/RP0/CPU0:Aug 18 01:16:30.029: radiusd[267]: Added standard attribute NAS-IP-Address =
12.22.57.4
RP/0/RP0/CPU0:Aug 18 01:16:30.031: radiusd[267]: Added standard attribute Service-Type =
EXEC
RP/0/RP0/CPU0:Aug 18 01:16:30.032: radiusd[267]: Added standard attribute Acct-Status-Type
= 0 0 0 1 ...
```

```
RP/0/RP0/CPU0:Aug 18 01:16:30.034: radiusd[267]: Translating attribute AAA_SVC_TYPE_ATTR
RP/0/RP0/CPU0:Aug 18 01:16:30.037: radiusd[267]: Translating attribute AAA_CONTEXT_ATTR
RP/0/RP0/CPU0:Aug 18 01:16:30.038: radiusd[267]: Translating attribute AAA_IPADDR_ATTR
RP/0/RP0/CPU0:Aug 18 01:16:30.040: radiusd[267]: Translated attribute AAA_IPADDR_ATTR to
standard RADIUS attr Framed-IP-Address = 0.0.0.0
RP/0/RP0/CPU0:Aug 18 01:16:30.042: radiusd[267]: Translating attribute AAA_TAC_METHOD_ATTR
RP/0/RP0/CPU0:Aug 18 01:16:30.043: radiusd[267]: RADIUS: Initial Transmit id 29 (16)
12.26.37.2:0, Accounting-Request, len 64
RP/0/RP0/CPU0:Aug 18 01:16:30.044: radiusd[267]: Attribute User Name = user1^D
RP/0/RP0/CPU0:Aug 18 01:16:30.044: radiusd[267]: Attribute NAS-IP-Address = 12.22.57.4
RP/0/RP0/CPU0:Aug 18 01:16:30.069: radiusd[267]: RADIUS: Received id 29 (16) 12.26.37.2:0,
Accounting-response, len 20
RP/0/RP0/CPU0:Aug 18 01:16:30.071: radiusd[267]: Sending sync reply (status PASS) to the
client
```

debug tacacs

To display information associated with Terminal Access Controller Access Control System Plus (TACACS+), use the **debug tacacs** command in EXEC mode. To disable debugging output, use the **no** form of this command.

debug tacacs {**accounting** | **authentication** | **authorization** | **configuration** | **detail** | **io**}

no debug tacacs {**accounting** | **authentication** | **authorization** | **configuration** | **detail** | **io**}

Syntax Description

accounting	Displays TACACS+ accounting debug information.
authentication	Displays TACACS+ authentication debug information.
authorization	Displays TACACS+ authorization debug information.
configuration	Displays TACACS+ configuration debug information.
detail	Displays detailed TACACS+ debug information.
io	Displays TACACS+ AAA messages.

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.
Release 3.3.0	Added the **io** keyword.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

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*.

TACACS+ is a distributed security system that secures networks against unauthorized access. Cisco supports TACACS+ under the authentication, authorization, and accounting (AAA) security system.

Debugging output is assigned high priority in the CPU process and, therefore, can affect system performance. For more information about the impact on system performance when using debug commands, refer to *Using Debug Commands on Cisco IOS XR Software*.

Task ID

Task ID	Operations
aaa	read

Examples

The following example shows debug output from TACACS+ and the resulting **show** command output when executing a command:

```
RP/0/RP0/CPU0:router# debug tacacs
RP/0/RP0/CPU0:router# show debug all

RP/0/RP0/CPU0:Aug 18 01:18:10.255: tacacsd[305]: tacacsd received a message
RP/0/RP0/CPU0:Aug 18 01:18:10.256: tacacsd[305]: Using server group # 2001
RP/0/RP0/CPU0:Aug 18 01:18:10.257: tacacsd[305]: Checking server 12.26.25.61 ...
RP/0/RP0/CPU0:Aug 18 01:18:10.257: tacacsd[305]: Selected server - 12.26.25.61/11000
RP/0/RP0/CPU0:Aug 18 01:18:10.257: tacacsd[305]: Unsupported method <notset>
RP/0/RP0/CPU0:Aug 18 01:18:10.258: tacacsd[305]: [session 71AC39DA] packet
ACCT/REQUEST/STOP selected server 12.26.25.61/11000 socket 24
RP/0/RP0/CPU0:Aug 18 01:18:10.258: tacacsd[305]: Starting timer for 5 seconds
RP/0/RP0/CPU0:Aug 18 01:18:10.259: tacacsd[305]: Attach socket handler for condition 0x10A
RP/0/RP0/CPU0:Aug 18 01:18:10.259: tacacsd[305]: Sending reply to client by TACACSD
RP/0/RP0/CPU0:Aug 18 01:18:10.261: tacacsd[305]: Packet ACCT/REQUEST/STOP (session
71AC39DA) to server 12.26.25.61
RP/0/RP0/CPU0:Aug 18 01:18:10.266: tacacsd[305]: Attach socket handler for condition 0x109
RP/0/RP0/CPU0:Aug 18 01:18:10.277: tacacsd[305]: Reconnect lock acquired in thread 3
RP/0/RP0/CPU0:Aug 18 01:18:10.278: tacacsd[305]: Error condition 2000 on socket 24
RP/0/RP0/CPU0:Aug 18 01:18:10.279: tacacsd[305]: Queueing the request back to to-be-sent 3
RP/0/RP0/CPU0:Aug 18 01:18:10.281: tacacsd[305]: Creating socket connection to TACACS+
server 12.26.25.61/11000
RP/0/RP0/CPU0:Aug 18 01:18:10.389: tacacsd[305]: Using source address 12.22.57.4
RP/0/RP0/CPU0:Aug 18 01:18:10.390: tacacsd[305]: Socket created 24
RP/0/RP0/CPU0:Aug 18 01:18:10.390: tacacsd[305]: Reuse address option set on socket
RP/0/RP0/CPU0:Aug 18 01:18:10.390: tacacsd[305]: Keepalive option set on socket
RP/0/RP0/CPU0:Aug 18 01:18:10.407: tacacsd[305]: Socket bound successfully with source
address 12.22.57.4
RP/0/RP0/CPU0:Aug 18 01:18:10.450: tacacsd[305]: Socket connected successfully
RP/0/RP0/CPU0:Aug 18 01:18:10.451: tacacsd[305]: Socket 24 to 12.26.25.61/11000 opened
RP/0/RP0/CPU0:Aug 18 01:18:10.451: tacacsd[305]: Attach socket handler for condition 0x10A
RP/0/RP0/CPU0:Aug 18 01:18:10.452: tacacsd[305]: Packet ACCT/REQUEST/STOP (session
71AC39DA) to server 12.26.25.61
RP/0/RP0/CPU0:Aug 18 01:18:10.453: tacacsd[305]: Attach socket handler for condition 0x109
RP/0/RP0/CPU0:Aug 18 01:18:10.552: tacacsd[305]: V0 REPLY (session 71AC39DA) from server
12.26.25.61
RP/0/RP0/CPU0:Aug 18 01:18:10.553: tacacsd[305]: Response hdr: version 0xC0, type 3, seq #
2, flag 0x1, session 1907112410, len 5
RP/0/RP0/CPU0:Aug 18 01:18:10.554: tacacsd[305]: Attach socket handler for condition 0x0

####  debug flags set from tty 'con0_0_CPU0'  ####
tacacs basic flag is ON
```

Related Commands

Command	Description
debug aaa	Provides detailed information about AAA processing.

debug task

To display debug task ID authorization information for the logged-in user, use the **debug task** command in EXEC mode. To disable debugging output, use the **no** form of this command.

debug task [**detail**]

no debug task [**detail**]

Syntax Description

detail	(Optional) Displays detailed task ID authorization information (for the logged-in user).

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.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

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*.

Debugging output is assigned high priority in the CPU process and, therefore, can affect system performance. For more information about the impact on system performance when using debug commands, refer to *Using Debug Commands on Cisco IOS XR Software*.

Task ID

Task ID	Operations
aaa	read

Examples

The following example shows debug output from the **debug task** command and the resulting show output:

```
RP/0/RP0/CPU0:router# debug task
RP/0/RP0/CPU0:router# show debug all

RP/0/RP0/CPU0:Aug 18 01:19:43.422: parser[255]: Created task table at 8292518
RP/0/RP0/CPU0:Aug 18 01:19:43.439: parser[255]: Created task table at 8292518
RP/0/RP0/CPU0:Aug 18 01:19:43.449: parser[255]: Created task table at 8292518
RP/0/RP0/CPU0:Aug 18 01:19:43.475: parser[255]: Created task table at 8292518

####  debug flags set from tty 'con0_0_CPU0'  ####
task basic flag is ON
On logging onto the router from a vty
RP/0/RP0/CPU0:router# RP/0/RP0/CPU0:Aug 18 01:21:10.315: locald[233]: Created task table
at 809be14
```

Related Commands

Command	Description
debug aaa	Displays debug information related to task ID processing (using the **task** keyword).

Crypto Conditional Debug Commands on Cisco IOS XR Software

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

For high-level, conceptual information about using **debug** commands generally, see *Using Debug Commands on Cisco IOS XR Software*, Release 3.6.0.

debug condition crypto ipv4

To select a peer by the IPv4 address, use the **debug condition crypto ivp4** command in EXEC mode. Information will be displayed for both the Internet Key Exchange (IKE) and the IP Security (IPSec) negotiation stages. To disable the peer selection, use the **no** form of this command.

debug condition crypto ipv4 *ip-address* [*/length*]

no debug condition crypto ipv4 *ip-address* [*/length*]

Syntax Description

ip-address	Specifies the IP address of the peer.
/length	(Optional) Prefix length, which can be indicated as a slash (/) and number. For example, /8 indicates that the first eight bits in the IP prefix are network bits. If the *length* argument is used, the slash is required.

Defaults

If conditional crypto debug statements are not used, crypto debug information will be displayed for all connections

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router and the Cisco CRS-1.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

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*.

Debugging output is assigned high priority in the CPU process and, therefore, can affect system performance. For more information about the impact on system performance when using debug commands, refer to *Using Debug Commands on Cisco IOS XR Software*.

Use conditional crypto debug commands in conjunction with crypto debug commands to select the peers or connections for which crypto debug information will be displayed. If crypto debug commands are not used, the conditional crypto debug commands will not display information. If multiple conditional debug commands are used, connections are selected using OR logic.

Use the **IP** condition when you know the IP address of the peer, and if the peer uses the IP as the identifier.

Task ID

Task ID	Operations
crypto	execute
basic-services	read, write

Related Commands

Command	Description
debug crypto engine	Displays information about crypto engines encryption and decryption functions.
debug crypto ipsec	Displays IPSec events.
debug crypto isakmp	Displays messages about IKE events.
debug crypto pki	Displays messages about PKI client events.

debug condition crypto hostname

To select a peer by the hostname string (to a maximum of 128 characters), use the **debug condition crypto hostname** command in EXEC mode. Information will be displayed for both the Internet Key Exchange (IKE) and the IP Security (IPSec) negotiation stages. To disable the peer selection, use the **no** form of this command.

debug condition crypto hostname {*peer-identity*}

no debug condition crypto hostname {*peer-identity*}

Syntax Description

peer-identity	Identity of the hostname of the peer in the format *hostname.domain*, to a maximum of 128 characters.

Defaults

If conditional crypto debug statements are not used, crypto debug information will be displayed for all connections

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router and the Cisco CRS-1.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

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*.

Debugging output is assigned high priority in the CPU process and, therefore, can affect system performance. For more information about the impact on system performance when using debug commands, refer to *Using Debug Commands on Cisco IOS XR Software*.

Use conditional crypto debug commands in conjunction with crypto debug commands to select the peers or connections for which crypto debug information will be displayed. If crypto debug commands are not used, the conditional crypto debug commands will not display information. If multiple conditional debug commands are used, connections are selected using OR logic.

Use the **hostname** condition when you know the domain and hostname of the peer, and if the peer uses the hostname as the identifier.

Task ID

Task ID	Operations
crypto	execute
basic-services	read, write

Related Commands

Command	Description
debug crypto ipsec	Displays IPSec events.

debug condition crypto ike

To display debug information about Internet Key Exchange (IKE) operations for specific connections, use the **debug condition crypto ike** command in EXEC mode. To disable the selection, use the **no** form of this command**.**

debug condition crypto ike {**connid** *connection-id* | **fvrf** *front-door-vrf* | **group** *unity-group* | **isakmp-profile** *isakmp-profile* | **ivrf** *inside-vrf* | **unmatch**}

no debug condition crypto ike {**connid** *connection-id* | **fvrf** ***front-door-vrf*** | **group** *unity-group* | **isakmp-profile** *isakmp-profile* | **ivrf** *inside-vrf* | **unmatch**}

Syntax Description

connid *connection-id*	Specifies a connection by the ID assigned to it. Range is 1 to 32767.
fvrf *front-door-vrf*	Specifies a connection by the front-door VPN routing and forwarding (VRF) instance it uses. Value is front-door VRF name.
group *unity-group*	Specifies a connection with a peer using a Unity Key-Group string as a the identifier. Value is unity group name string.
isakmp-profile *isakmp-profile*	Specifies the profile name of the specified IKE session as a crypto debug condition. Value is the name of the ISAKMP profile.
ivrf *inside-vrf*	Specifies a connection by the inside-door VRF instance it uses. Value is the inside-door VRF name.
unmatch	Sets the unlimited flag to produce a debug message even if no context is available.

Defaults

If conditional crypto debug statements are not used, crypto debug information will be displayed for all connections

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router and the Cisco CRS-1.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

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*.

Debugging output is assigned high priority in the CPU process and, therefore, can affect system performance. For more information about the impact on system performance when using debug commands, refer to *Using Debug Commands on Cisco IOS XR Software*.

Use conditional crypto debug commands in conjunction with crypto debug commands to select the peers or connections for which crypto debug information will be displayed. If crypto debug commands are not used, the conditional crypto debug commands will not display information. If multiple conditional debug commands are used, connections are selected using OR logic.

Use the **debug condition crypto ike** commands to debug peer-specific, configuration, or functionality-related IKE problems that could occur during a large-scale VPN deployment, in particular with hub routers that have large numbers of peers and live traffic. The condition statements focus on specific IKE sessions using different filters.

Use the **group** condition when the group to which the peer belongs is known, and if the peer uses the group as the identifier.

Use the **unmatch** condition to show messages that cannot be related to a specific session. By default, some messages are not displayed when other conditional debug commands are used. Combine other conditional debug commands with the **unmatch** condition and a crypto debug command to generate output for the specified session.

Task ID

Task ID	Operations
crypto	execute
basic-services	read, write

Related Commands

Command	Description
debug crypto engine	Displays information about crypto engines encryption and decryption functions.
debug crypto ipsec	Displays IPSec events.
debug crypto isakmp	Displays messages about IKE events.
debug crypto pki	Displays messages about PKI client events.
tunnel vrf ***vrf-name***	Determines the fvrf that the service IPSec uses.
vrf ***vrf-name***	Determines the ivrf that the service IPSec uses.

debug condition crypto ipsec

To display debug information about IP Security (IPSec) operations for a specific session, use the **debug condition crypto ipsec** command in EXEC mode. To disable the selection, use the **no** form of this command.

debug condition crypto ipsec {**flow-id** *flow-id* | **fvrf** *front-door-vrf* | **profile** *ipsec-profile* | **unmatch**}

no debug condition crypto ipsec {**flow-id** *flow-id* | **fvrf** *front-door-vrf* | **profile** *ipsec-profile* | **unmatch**}

Syntax Description

flow-id *flow-id*	Specifies a IPSec session by the ID assigned to it. Range is 1 to 16500.
fvrf *front-door-vrf*	Specifies an IPSec section by the front-door VRF instance it uses. Value is front-door VRF name.
profile *ipsec-profile*	Specifies an IPSec profile as a crypto debug condition. Value is the name of the IPSec profile.
unmatch	Sets the unlimited flag to produce a debug message even if no context is available.

Defaults

If conditional crypto debug statements are not used, crypto debug information will be displayed for all connections

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router and the Cisco CRS-1.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

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*.

Debugging output is assigned high priority in the CPU process and, therefore, can affect system performance. For more information about the impact on system performance when using debug commands, refer to *Using Debug Commands on Cisco IOS XR Software*.

Use conditional crypto debug commands in conjunction with crypto debug commands to select the peers or connections for which crypto debug information will be displayed. If crypto debug commands are not used, the conditional crypto debug commands will not display information. If multiple conditional debug commands are used, connections are selected using OR logic.

Use the **debug condition crypto ipsec** commands to debug peer-specific, configuration, or functionality-related IPSec problems that could occur during a large-scale VPN deployment, in particular with hub routers that have large numbers of peers and live traffic. The condition statements enable you to focus on specific IPSec sessions using different filters.

Use the **unmatch** condition to show messages that cannot be related to a specific session. By default, some messages are not displayed when other conditional debug commands are used. Combine other conditional debug commands with the **unmatch** condition and a crypto debug command to generate output for the specified session.

Task ID

Task ID	Operations
crypto	execute
basic-services	read, write

Related Commands

Command	Description
debug crypto engine	Displays information about crypto engines encryption and decryption functions.
debug crypto ipsec	Displays IPSec events.
debug crypto isakmp	Displays messages about IKE events.
debug crypto pki	Displays messages about PKI client events.
tunnel vrf ***vrf-name***	Determines the fvrf that the service IPSec uses.

debug condition crypto username

To select a peer by its username, use the **debug condition crypto username** command in EXEC mode. Information is displayed for both the Internet Key Exchange (IKE) and the IP Security (IPSec). To disable the peer selection, use the **no** form of this command.

debug condition crypto username *peer-identity*

no debug condition crypto username *peer-identity*

Syntax Description

peer-identity	Value is the fully qualified domain name (FQDN) username of the peer in the format *username@domain*.

Defaults

If conditional crypto debug statements are not used, crypto debug information will be displayed for all connections

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router and the Cisco CRS-1.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

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*.

Debugging output is assigned high priority in the CPU process and, therefore, can affect system performance. For more information about the impact on system performance when using debug commands, refer to *Using Debug Commands on Cisco IOS XR Software*.

Use conditional crypto debug commands in conjunction with crypto debug commands to select the peers or connections for which crypto debug information will be displayed. If crypto debug commands are not used, the conditional crypto debug commands will not display information. If multiple conditional debug commands are used, connections are selected using OR logic.

Use the **username** condition when you know the username and domain of the peer, and if the peer uses the username as the identifier.

Task ID

Task ID	Operations
crypto	execute
basic-services	read, write

Related Commands

Command	Description
debug crypto engine	Displays information about crypto engines encryption and decryption functions.
debug crypto ipsec	Displays IPSec events.
debug crypto isakmp	Displays messages about IKE events.
debug crypto pki	Displays messages about PKI client events.

debug condition crypto vi

To define a virtual interface name as a crypto debug condition, use the **debug condition crypto vi** command in EXEC mode. Information is displayed for both the Internet Key Exchange (IKE) and IP Security (IPSec). To disable the selection, use the **no** form of this command.

debug condition crypto vi {**tunnel-ipsec** *tunnel-id*}

no debug condition crypto vi {**tunnel-ipsec** *tunnel-id*}

Syntax Description

tunnel-ipsec *tunnel-id*	Specifies IPSec tunnel interface as a crypto debug condition. Value is the ID for the IPSec tunnel interface.
service-gre *gre-id*	Specifies the service-gre interface as a crypto debug condition. Value is the ID for the interface (Cisco XR 12000 Series Router only).
service-ipsec *ipsec-id*	Specifies the service-ipsec interface as a crypto debug condition. Value is the ID for the interface (Cisco XR 12000 Series Router only).

Defaults

If conditional crypto debug statements are not used, crypto debug information will be displayed for all connections

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router and the Cisco CRS-1.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

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*.

Debugging output is assigned high priority in the CPU process and, therefore, can affect system performance. For more information about the impact on system performance when using debug commands, refer to *Using Debug Commands on Cisco IOS XR Software*.

Use conditional crypto debug commands in conjunction with crypto debug commands to select the peers or connections for which crypto debug information will be displayed. If crypto debug commands are not used, the conditional crypto debug commands will not display information. If multiple conditional debug commands are used, connections are selected using OR logic.

Use this command to see output for all connections on the specified interface.

Task ID

Task ID	Operations
crypto	execute
basic-services	read, write

Related Commands

Command	Description
debug crypto engine	Displays information about crypto engines encryption and decryption functions.
debug crypto ipsec	Displays IPSec events.
debug crypto isakmp	Displays messages about IKE events.
debug crypto pki	Displays messages about PKI client events.

Keychain Management Debug Commands on Cisco IOS XR Software

This chapter describes the Cisco IOS XR software debug keychain management commands.

For high-level, conceptual information about using **debug** commands generally, see *Using Debug Commands on Cisco IOS XR Software*, Release 3.6.0.

debug keychain

To display debug keychain processing information, use the **debug keychain** command in EXEC mode. To disable debugging output, use the **no** form of this command.

debug keychain {**errors** | **events**} [**job** *jobid*]

no debug keychain {**errors** | **events**} [**job** *jobid*]

Syntax Description

errors	Displays all keychain-management-related errors.
event	Displays all keychain-management-related events.
job *jobid*	Specifies the job ID of the keychain client process. Range is from 0 to 4294967295.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

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*.

Debugging output is assigned high priority in the CPU process and, therefore, can affect system performance. For more information about the impact on system performance when using debug commands, refer to *Using Debug Commands on Cisco IOS XR Software*.

Task ID

Task ID	Operations
system	read

Examples

The following is sample output from the **debug keychain** command using the **events** keyword for the job with job ID 23:

```
RP/0/RP0/CPU0:router# debug keychain events job 23
```

Software Authentication Manager Debug Commands on Cisco IOS XR Software

This chapter describes the Cisco IOS XR software debug Software Authentication Manager (SAM) commands.

For high-level, conceptual information about using **debug** commands generally, see *Using Debug Commands on Cisco IOS XR Software*, Release 3.6.0.

debug sam

To display transactional information for the Software Authentication Manager (SAM), use the **debug sam** command in EXEC mode. To disable debugging output, use the **no** form of this command.

debug sam {**data** | **events**}

no debug sam {**data** | **events**}

Syntax Description

data	Displays data content for SAM events.
events	Displays all SAM events.

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.
Release 3.3.0	No modification.
Release 3.4.0	The **data** keyword was added, and the **detail** keyword was removed.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

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*.

Debugging output is assigned high priority in the CPU process and, therefore, can affect system performance. For more information about the impact on system performance when using debug commands, refer to *Using Debug Commands on Cisco IOS XR Software*.

Task ID

Task ID	Operations
crypto	read

Examples

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

```
RP/0/RP0/CPU0:router# debug sam events
```

```
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)
RP/0/RP0/CPU0:k2#RP/0/0/CPU0:Aug 28 00:33:21.725 MET2MET,M3.5.0/: sam_server[265]: SAM
Table completes set_nvram_digest (0)
RP/0/RP0/CPU0:Aug 28 00:33:22.301 MET2MET,M3.5.0/: sam_server[265]: SAM Event: SAM begins
initialization
RP/0/RP0/CPU0:Aug 28 00:33:22.303 MET2MET,M3.5.0/: sam_server[265]: SAM begins table setup
RP/0/RP0/CPU0:Aug 28 00:33:22.307 MET2MET,M3.5.0/: sam_server[265]: SAM server binding to
SysDB at /oper/sam/node/0/
RP/0/RP0/CPU0:Aug 28 00:33:22.395 MET2MET,M3.5.0/: sam_server[265]: SAM completes table
setup, rc=No error
RP/0/RP0/CPU0:Aug 28 00:33:22.408 MET2MET,M3.5.0/: sam_server[265]: SAM Server begins
comparing the nvram digest for table SysDB Digest
RP/0/RP0/CPU0:Aug 28 00:33:22.477 MET2MET,M3.5.0/: sam_server[265]: SAM Server completes
comparing the nvram digest
```

Secure Socket Layer Protocol Debug Commands on Cisco IOS XR Software

This chapter describesCisco IOS XR software Secure Socket Layer (SSL) debug commands.

For high-level, conceptual information about using **debug** commands generally, see *Using Debug Commands on Cisco IOS XR Software*, Release 3.6.0.

debug ssl

To display Secure Socket Layer (SSL) session information, use the **debug ssl** command in EXEC mode. To disable debugging output, use the **no** form of this command.

debug ssl {**error** | **event** | **handshake** | **traffic**}

no debug ssl {**error** | **event** | **handshake** | **traffic**}

Syntax Description

error	Displays any errors during control (negotiation) and data phase.
event	Displays SSL negotiation event.
handshake	Displays SSL handshake protocol information.
traffic	Displays SSL traffic 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.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

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*.

Debugging output is assigned high priority in the CPU process and, therefore, can affect system performance. For more information about the impact on system performance when using debug commands, refer to *Using Debug Commands on Cisco IOS XR Software*.

Task ID

Task ID	Operations
crypto	read

Examples

The following is sample output from the **debug ssl** command using the **error** keyword:

```
RP/0/RP0/CPU0:router# debug ssl error

SLOT0:Aug 4 15:26:18.729 : SSL_accept:error in SSLv2/v3 read client hello A
SLOT0:Aug 4 15:26:18.731 : Open 0x08057db4 20
SLOT0:Aug 4 15:26:19.815 : (ssl) network data event
SLOT0:Aug 4 15:26:19.821 : SSL_accept:error in SSLv3 read client certificate A
SLOT0:Aug 4 15:26:19.821 : SSL_accept:error in SSLv3 read client certificate A
```

Secure Shell Debug Commands Cisco IOS XR Software

This chapter describes the Cisco IOS XR software Secure Shell (SSH) debug commands.

For high-level, conceptual information about using **debug** commands generally, see *Using Debug Commands on Cisco IOS XR Software*, Release 3.6.0.

debug ssh

To display Secure Shell (SSH) session information, use the **debug ssh** command in EXEC mode. To disable debugging output, use the **no** form of this command.

debug ssh {**client** | **kex** | **server** | **sftp** | **traffic**}

no debug ssh {**client** | **kex** | **server** | **sftp** | **traffic**}

Syntax Description

client	Displays debug information pertaining to the SSH client.
kex	Displays key exchange related information.
server	Displays transactional information for the SSH server.
sftp	Displays transactional information for SFTP clients.
traffic	Displays SSH traffic 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.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

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*.

Debugging output is assigned high priority in the CPU process and, therefore, can affect system performance. For more information about the impact on system performance when using debug commands, refer to *Using Debug Commands on Cisco IOS XR Software*.

Task ID

Task ID	Operations
crypto	read

Examples

The following is sample output from the **debug ssh** command using the **server** keyword:

```
RP/0/RP0/CPU0:router# debug ssh server

RP/0/RP0/CPU0:Aug 28 00:52:19.483 MET2MET,M3.5.0/: SSHD_[320]: SSHD debug detail
RP/0/RP0/CPU0:Aug 28 00:52:19.556 MET2MET,M3.5.0/: SSHD_[320]: Server listening on port 22
RP/0/RP0/CPU0:Aug 28 00:52:20.077 MET2MET,M3.5.0/: config[65718]: %MGBL-LIBTARCF
```

Management Plane Protection Debug Commands on Cisco IOS XR Software

This chapter describes Cisco IOS XR software Management Plane Protection (MPP) debug commands.

For high-level, conceptual information about using **debug** commands generally, see *Using Debug Commands on Cisco IOS XR Software*, Release 3.6.0.

debug management-plane

To enable debugging for management-plane events such as configuration changes, protocol inquiries, or ip-address changes, use the **debug management-plane** command in EXEC mode. To disable debugging output, use the **no** form of this command.

debug management-plane {**detail** | **errors** | **events**} [**job** *job id*]

no debug management-plane {**detail** | **errors** | **events**} [**job** *job id*]

Syntax Description

detail	Displays details for all events.
errors	Displays all errors.
events	Displays all events.
job *job id*	(Optional) Enables debugging for a specified job.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.5.0	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

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*.

Debugging output is assigned high priority in the CPU process and, therefore, can affect system performance. For more information about the impact on system performance when using debug commands, refer to *Using Debug Commands on Cisco IOS XR Software*.

Task ID

Task ID	Operations
system	read

Examples

The following example shows the **debug management-plane** command using the **errors** keyword:

```
RP/0/RP0/CPU0:router# debug management-plane errors job 141
```

INDEX

DHR	Cisco IOS XR Interface and Hardware Component Debug Command Reference
DIR	Cisco IOS XR IP Addresses and Services Debug Command Reference
DMCR	Cisco IOS XR Multicast Debug Command Reference
DMPR	Cisco IOS XR MPLS Debug Command Reference
DQR	Cisco IOS XR Modular Quality of Service Debug Command Reference
DRR	Cisco IOS XR Routing Debug Command Reference
DSB	Cisco IOS XR Session Border Controller Debug Command Reference
DSMR	Cisco IOS XR System Management Debug Command Reference
DSR	Cisco IOS XR System Security Debug Command Reference

A

aaa, debug 12

acctd, debug 14

C

condition crypto hostname, debug 30

condition crypto ike, debug 32

condition crypto ipsec, debug 34

condition crypto ipv4, debug 28

condition crypto username, debug 36

condition crypto vi, debug 38

crypto ace, debug 2

crypto engine, debug 4

crypto ipsec, debug 6

crypto isakmp, debug 8

crypto pki, debug 10

K

keychain, debug 42

L

locald, debug 16

login, debug 18

M

management-plane, debug 58

R

radius, debug 19

S

sam, debug 46

ssh, debug 54

ssl, debug 50, 58

T

tacacs, debug 22

task, debug 24