CHAPTER 13

database path through debug cxsc Commands

database path

To specify a path or location for the local CA server database, use the **database** command in ca server configuration mode. To reset the path to flash memory, the default setting, use the **no** form of this command.

[**no**] **database path** *mount-name directory-path*

Syntax Description

directory-path	Specifies the path to a directory on the mount point where the CA files are stored.
mount-name	Specifies the mount name.

Defaults

By default, the CA server database is stored in flash memory.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Ca server configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The local CA files stored in the database include the certificate database, user database files, temporary PKCS12 files, and the current CRL file. The *mount-name* argument is the same as the *name* argument for the **mount** command that is used to specify a file system for the ASA.

Note These CA files are internal, stored files and should not be modified.

Examples

The following example defines the mount point for the CA database as cifs_share and the database files directory on the mount point as ca_dir/files_dir:

```
hostname(config)# crypto ca server
hostname(config-ca-server)# database path cifs_share ca_dir/files_dir/
hostname(config-ca-server)#
```

Related Commands

Command	Description
crypto ca server	Provides access to the ca server configuration mode CLI command set, which allows the user to configure and manage a local CA.
crypto ca server user-db write	Writes the user information configured in the local CA database to disk.
debug crypto ca server	Shows debugging messages when the user configures the local CA server.
mount	Makes the Common Internet File System (CIFS) and/or File Transfer Protocol file systems (FTPFS) accessible to the ASA.
show crypto ca server	Displays the characteristics of the CA configuration on the ASA.
show crypto ca server cert-db	Displays the certificates issued by the CA server.

ddns

To specify a Dynamic DNS (DDNS) update method type, use the **ddns** command in ddns-update-method mode. To remove an update method type from the running configuration, use the **no** form of this command.

ddns [**both**]

no ddns [**both**]

Syntax Description

both	(Optional) Specifies updates to both the DNS A and PTR resource records (RRs).

Defaults

Update only the DNS A RRs.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Ddns-update-method	•	—	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

DDNS updates the name-to-address and address-to-name mapping maintained by DNS. Of the two methods for performing DDNS updates—the IETF standard defined by RFC 2136 and a generic HTTP method—the ASA supports the IETF method in this release.

Name and address mappings are contained in two types of RRs:

- The A resource record contains domain name-to-IP address mapping.
- The PTR resource record contains IP address-to-domain name mapping.

DDNS updates can be used to maintain consistent information between the DNS A and PTR RR types.

When issued in ddns-update-method configuration mode, the **ddns** command defines whether the update is just to a DNS A RR, or to both DNS A and PTR RR types.

Examples

The following example configures updates to both the DNS A and PTR RRs for the DDNS update method named ddns-2:

```
hostname(config)# ddns update method ddns-2
hostname(DDNS-update-method)# ddns both
```

Related Commands

Command	Description
ddns update	Associates a DDNS update method with an ASA interface or a DDNS update hostname.
ddns update method	Creates a method for dynamically updating DNS resource records.
dhcp-client update dns	Configures the update parameters that the DHCP client passes to the DHCP server.
dhcpd update dns	Enables a DHCP server to perform DDNS updates.
interval maximum	Configures the maximum interval between update attempts by a DDNS update method.

ddns update

To associate a dynamic DNS (DDNS) update method with an ASA interface or an update hostname, use the **ddns update** command in interface configuration mode. To remove the association between the DDNS update method and the interface or the hostname from the running configuration, use the **no** form of this command.

ddns update [*method-name* | **hostname** *hostname*]

no ddns update [*method-name* | **hostname** *hostname*]

Syntax Description

hostname	Specifies that the next term in the command string is a hostname.
hostname	Specifies a hostname to be used for updates.
method-name	Specifies a method name for association with the interface being configured.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Interface configuration	•	—	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

After defining a DDNS update method, you must associate it with an ASA interface to trigger DDNS updates.

A hostname could be a Fully Qualified Domain Name (FQDN) or just a hostname. If just a hostname, the ASA appends a domain name to the hostname to create a FQDN.

Examples

The following example associates the interface GigabitEthernet0/2 with the DDNS update method named ddns-2 and the hostname hostname1.example.com:

```
hostname(config)# interface GigabitEthernet0/2
hostname(config-if)# ddns update ddns-2
hostname(config-if)# ddns update hostname hostname1.example.com
```

Related Commands

Command	Description
ddns	Specifies a DDNS update method type for a created DDNS method.
ddns update method	Creates a method for dynamically updating DNS resource records.
dhcp-client update dns	Configures the update parameters that the DHCP client passes to the DHCP server.
dhcpd update dns	Enables a DHCP server to perform DDNS updates.
interval maximum	Configures the maximum interval between update attempts by a DDNS update method.

ddns update method

To create a method for dynamically updating DNS resource records (RRs), use the **ddns update method** command in global configuration mode. To remove a dynamic DNS (DDNS) update method from the running configuration, use the **no** form of this command.

ddns update method *name*

no ddns update method *name*

Syntax Description

name	Specifies the name of a method for dynamically updating DNS records.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

DDNS updates the name-to-address and address-to-name mapping maintained by DNS. The update method configured by the **ddns update method** command determines what and how often DDNS updates are performed. Of the two methods for performing DDNS updates—the IETF standard defined by RFC 2136 and a generic HTTP method—the ASA supports the IETF method in this release.

Name and address mapping is contained in two types of resource records (RRs):

- The A resource record contains domain name-to IP-address mapping.
- The PTR resource record contains IP address-to-domain name mapping.

DDNS updates can be used to maintain consistent information between the DNS A and PTR RR types.

Note Before the **ddns update method** command will work, you must configure a reachable default DNS server using the **dns** command with domain lookup enabled on the interface.

Examples

The following example configures the DDNS update method named ddns-2:

```
hostname(config)# ddns update method ddns-2
```

Related Commands

Command	Description
ddns	Specifies a DDNS update method type for a created DDNS method.
ddns update	Associates a DDNS update method with an ASA interface or a DDNS update hostname.
dhcp-client update dns	Configures the update parameters that the DHCP client passes to the DHCP server.
dhcpd update dns	Enables a DHCP server to perform dynamic DNS updates.
interval maximum	Configures the maximum interval between update attempts by a DDNS update method.

debug aaa

To show debugging messages for AAA, use the **debug aaa** command in privileged EXEC mode. To disable the display of AAA messages, use the **no** form of this command.

debug aaa [**accounting | authentication | authorization | common | internal | vpn** [*level*]]

no debug aaa

Syntax Description

accounting	(Optional) Show debugging messages for accounting only.
authentication	(Optional) Show debugging messages for authentication only.
authorization	(Optional) Show debugging messages for authorization only.
common	(Optional) Show debugging messages for different states within the AAA feature.
internal	(Optional) Show debugging messages for AAA functions supported by the local database only.
level	(Optional) Specifies the debugging level. Valid with the **vpn** keyword only.
vpn	(Optional) Show debugging messages for VPN-related AAA functions only.

Defaults

The default debugging level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was modified to include new keywords.

Usage Guidelines

The **debug aaa** command displays detailed information about AAA activity. The **no debug all** and **undebug all** commands turn off all enabled debugging commands.

Examples

The following is sample output from the **debug aaa internal** command:

```
hostname(config)# debug aaa internal
debug aaa internal enabled at level 1
hostname(config)# uap allocated. remote address: 10.42.15.172, Session_id: 2147483841
uap freed for user . remote address: 10.42.15.172, session id: 2147483841
```

Related Commands

Command	Description
show running-config aaa	Displays the running configuration related to AAA.

debug acl filter

To enable VPN filter debugging, use the **debug acl filter** command in privileged EXEC mode. To disable VPN filter debugging, use the **no** form of this command.

debug acl filter

no debug acl filter

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
8.2(2)	This command was introduced.

Usage Guidelines

Use the **debug acl filter** command to help troubleshoot installation of the VPN filters into the ASP Filter table and removal of the VPN filters from the ASP Filter table.

Examples

The following is sample output from the **debug acl filter** command when a user 1 connects:

```
hostname(config)# debug acl filter
ACL FILTER INFO: first reference to inbound filter vpnfilter(2): Installing rule into NP.
 ACL FILTER INFO: first reference to outbound filter vpnfilter(2): Installing rule into
NP.
```

The following is sample output from the **debug acl filter** command when a user 1 disconnects:

```
hostname(config)# debug acl filter

ACL FILTER INFO: releasing last reference from inbound filter vpnfilter(2): Removing rule
into NP.
 ACL FILTER INFO: releasing last reference from outbound filter vpnfilter(2): Removing
rule into NP.
```

Related Commands

Command	Description
show asp table filter	Debugs the accelerated security path filter tables.
clear asp table filter	Clears the hit counters for the ASP filter table entries.

debug appfw

To display detailed information about application inspection, use the **debug appfw** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug appfw [**chunk** | **event** | **eventverb** | **regex**]

no debug appfw [**chunk** | **event** | **eventverb** | **regex**]

Syntax Description

chunk	(Optional) Displays runtime information about processing of chunked transfer encoded packets.
event	(Optional) Displays debug information about packet inspection events.
eventverb	(Optional) Displays the action taken by the ASA in response to an event.
regex	(Optional) Displays information about matching patterns with predefined signatures.

Defaults

All options are enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **debug appfw** command displays detailed information about HTTP application inspection. The **no debug all** and **undebug all** commands turn off all enabled **debug** commands.

Examples

The following example enables the display of detailed information about application inspection:

```
hostname# debug appfw
```

Related Commands

Commands	Description
http-map	Defines an HTTP map for configuring enhanced HTTP inspection.
inspect http	Applies a specific HTTP map to use for application inspection.

debug arp

To show debugging messages for ARP, use the **debug arp** command in privileged EXEC mode. To stop showing debugging messages for ARP, use the **no** form of this command.

debug arp

no debug arp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

The following example enables debugging messages for ARP:

```
hostname# debug arp
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
show arp statistics	Shows ARP statistics.
show debug	Shows all enabled debuggers.

debug arp-inspection

To show debugging messages for ARP inspection, use the **debug arp-inspection** command in privileged EXEC mode. To stop showing debugging messages for ARP inspection, use the **no** form of this command.

debug arp-inspection

no debug arp-inspection

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	—	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

The following example enables debugging messages for ARP inspection:

```
hostname# debug arp-inspection
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
arp-inspection	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
show debug	Shows all enabled debuggers.

debug asdm history

To view debugging information for ASDM, use the **debug asdm history** command in privileged EXEC mode.

debug asdm history *level*

Syntax Description

level	(Optional) Specifies the debugging level.

Defaults

The default debugging level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was changed from the **debug pdm history** command to the **debug asdm history** command.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example enables level 1 debugging of ASDM:

```
hostname# debug asdm history
debug asdm history enabled at level 1

hostname#
```

Related Commands

Command	Description
show asdm history	Displays the contents of the ASDM history buffer.

debug auto-update

To display auto-update client and server debugging information, use the **debug auto-update** command in privileged EXEC mode. To disable the display of auto-update client and server debugging information, use the **no** form of this command.

debug auto-update client | server [*level*]

no debug auto-update client | server [*level*]

Syntax Description

client	Identifies the auto-update client.
level	(Optional) Sets the level at which to display debugging messages. The range of values is between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.
server	Identifies the auto-update server.

Defaults

The default value for the debugging level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following is sample output from the **debug auto-update** and the **show debug auto-update** commands.

```
hostname# debug auto-update client
hostname# debug auto-update server
hostname# show debug auto-update
debug auto-update client enabled at level 1
debug auto-update server enabled at level 1
```

Related Commands

Command	Description
show debug auto	Displays the current auto-update debugging configuration.

debug boot-mem

To display boot memory debugging information, use the **debug boot-mem** command in privileged EXEC mode. To disable the display of debugging information, use the **no** form of this command.

debug boot-mem [*level*]

no debug boot-mem [*level*]

Syntax Description

level	(Optional) Sets the level at which to display debugging messages. The range of values is between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default value for the debugging level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following is sample output from the **debug boot-mem** and the **show debug boot-mem** commands.

```
hostname# debug boot-mem
debug boot-mem enabled at level 1
hostname# show debug boot-mem
debug boot-mem enabled at level 1
```

Related Commands

Command	Description
show debug boot	Displays the current boot memory debugging configuration.

debug boot-module

To display boot module (SSM) debugging information, use the **debug boot-module** command in privileged EXEC mode. To disable the display of debugging information, use the **no** form of this command.

debug boot-module [*level*]

no debug boot-module [*level*]

Syntax Description

level	(Optional) Sets the level to display debugging messages. The range of values is between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default value for the debugging level is 1.

Command Modes

The following table shows the modes in which you can enter the command.

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
8.0(2)	This command was introduced.
8.6(1)	Supports software modules such as IPS. Supports the ASA 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following is sample output from the **debug boot-module** command:

```
hostname# debug boot-module
debug boot-module enabled at level 1
```

Related Commands

Command	Description
show debug boot-mem	Displays the current boot memory debugging configuration.

debug cluster

To display ASA cluster debug information, use the **debug cluster** command in privileged EXEC mode. To disable the display of debug information, use the **no** form of this command.

debug cluster [**ccp** | **datapath** | **fsm** | **general** | **hc** | **license** | **rpc** | **transport**] [*level*]

no debug cluster [**ccp** | **datapath** | **fsm** | **general** | **hc** | **license** | **rpc** | **transport**]

Syntax Description

level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.
ccp	(Optional) Displays debug messages for the cluster control protocol.
datapath	(Optional) Displays debug messages for the datapath.
fsm	(Optional) Displays debug messages for the finite state machine.
general	(Optional) Displays general clustering debug messages.
hc	(Optional) Displays debug messages for the health check.
license	(Optional) Displays debug messages for the cluster license.
rpc	(Optional) Displays debug messages for the RPC module.
transport	(Optional) Displays debug messages for the transport service.

Command Default

If you do not specify a debug type when enabling debug messages, then all types are enabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
9.0(1)	We introduced this command.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example enables debug messages for all types:

```
hostname# debug cluster
```

Related Commands

Command	Description
debug lacp cluster	Enables debug messages for cluster Link Aggregation Control Protocol (cLACP).

debug context

To show debugging messages when you add or delete a security context, use the **debug context** command in privileged EXEC mode. To stop showing debugging messages for contexts, use the **no** form of this command.

debug context [*level*]

no debug context [*level*]

Syntax Description

level	(Optional) Sets the debugging message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

The following example enables debug messages for context management:

```
hostname# debug context
```

Related Commands

Command	Description
context	Creates a security context in the system configuration and enters context configuration mode.
show context	Shows context information.
show debug	Shows all enabled debuggers.

debug cplane

To show debugging messages about the control plane that connects internally to an SSM, use the **debug cplane** command in privileged EXEC mode. To stop showing debugging messages for the control plane, use the **no** form of this command.

debug cplane [*level*]

no debug cplane [*level*]

Syntax Description

level	(Optional) Sets the debugging message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

The following example enables debugging messages for the control plane:

```
hostname# debug cplane
```

Related Commands

Command	Description
hw-module module recover	Recovers an intelligent SSM by loading a recovery image from a TFTP server.
hw-module module reset	Shuts down an SSM and performs a hardware reset.
hw-module module reload	Reloads the intelligent SSM software.

Command	Description
hw-module module shutdown	Shuts down the SSM software in preparation for being powered off without losing configuration data.
show module	Shows SSM information.

debug crypto ca

To show debugging messages for PKI activity (used with CAs), use the **debug crypto ca** command in privileged EXEC mode. To disable the display of debugging messages for PKI, use the **no** form of this command.

debug crypto ca [**messages** | **transactions**] [*level*]

no debug crypto ca [**messages** | **transactions**] [*level*]

Syntax Description

messages	(Optional) Shows only debugging messages for PKI input and output messages.
transactions	(Optional) Shows only debugging messages for PKI transactions.
level	(Optional) Sets the level to display debugging messages.The range is between 1 and 255. To display additional messages at higher levels, set the level to a higher number. Level 1 (the default) shows messages only when errors occur. Level 2 shows warnings. Level 3 shows informational messages. Levels 4 and up show additional information for troubleshooting.

Defaults

By default, this command shows all debugging messages. The default level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

The following example enables debugging messages for PKI:

```
hostname# debug crypto ca
```

Related Commands

Command	Description
debug crypto engine	Shows debugging messages for the crypto engine.
debug crypto ipsec	Shows debugging messages for IPsec.
debug crypto isakmp	Shows debugging messages for ISAKMP.

debug crypto condition

To filter debugging messages for IPSec and ISAKMP based on the specified conditions, use the **debug crypto condition** command in privileged EXEC mode. To disable a single filtering condition without affecting other conditions, use the **no** form of this command.

debug crypto condition [[**peer [address** *peer_addr*] **subnet** *subnet_mask*]] | [**user** *user_name*] | [**group** *group_name*] | [spi *spi*] | [**reset**]

[no] debug crypto condition [[**peer [address** *peer_addr*] **subnet** *subnet_mask*]] | [**user** *user_name*] | [**group** *group_name*] | [**spi** *spi*] | [**reset**]

Syntax Description

group *group_name*	Specifies the group being used and the client group name.
peer *peer_addr*	Specifies the IPsec peer and its IP address
reset	Clears all filtering conditions and disables filtering.
spi *spi*	Specifies the IPsec SPI.
subnet *subnet_mask*	Specifies the subnet and subnet mask that are associated with the specified IP address.
user *user_name*	Specifies the client being used and the client username.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The **debug crypto condition** command does not affect the display or logging of syslog messages. This feature is not stored in the configuration, and must be reset after each power cycle.

Examples

The following examples configure a filter for the network, 10.1.1.0 and for the peer, 10.2.2.2:

```
hostname# debug crypto condition peer address 10.1.1.0 subnet 255.255.255.0
hostname# debug crypto condition peer address 10.2.2.2
```

The following example configures a filter for the user, “example_user”:

```
hostname# debug crypto condition user example_user
```

The following example clears the debugging filters:

```
hostname# debug crypto condition reset
```

Related Commands

Command	Description
debug crypto condition error	Shows debugging messages whether or not filtering conditions have been specified.
debug crypto condition unmatched	Shows debugging messages for IPsec and ISAKMP that do not include sufficient context information for filtering.
show crypto debug-condition	Shows the configured filters for IPsec and ISAKMP debugging messages.

debug crypto condition error

To show debugging messages for IPSec and ISAKMP whether or not they match any of the configured filters, use the **debug crypto condition error** command in privileged EXEC mode. To disable the display of debugging messages for IPsec and ISAKMP whether or not they match any of the configured filters, use the **no** form of this command.

debug crypto condition error [[**ipsec | isakmp**]

[**no**] **debug crypto condition error** [**ipsec | isakmp**]

Syntax Description

ipsec	Specifies the IPsec debugging messaging system.
isakmp	Specifies the ISAKMP debugging messaging system.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The **debug crypto condition error** command does not affect the display or logging of syslog messages. This feature is not stored in the configuration, and must be reset after each power cycle.

Examples

The following example configures IPsec messages to appear whether or not filtering conditions have been specified:

```
hostname# debug crypto condition error ipsec
```

Related Commands

Command	Description
debug crypto condition	Sets filtering conditions for IPsec and ISAKMP debugging messages.

Command	Description
debug crypto condition unmatched	Shows debugging messages for IPsec and ISAKMP that do not include sufficient context information for filtering.
show crypto debug-condition	Shows the configured filters for IPsec and ISAKMP debugging messages.

debug crypto condition unmatched

To show debugging messages for IPsec and ISAKMP that do not include sufficient context information for filtering, use the **debug crypto condition unmatched** command in privileged EXEC mode. To filter debugging messages for IPSec and ISAKMP that do not include sufficient context information, use the **no** form of this command.

debug crypto condition unmatched [[**ipsec | isakmp**]

[**no**] **debug crypto condition unmatched** [**ipsec | isakmp**]

Syntax Description

ipsec	Specifies the IPSec debugging messaging system.
isakmp	Specifies the ISAKMP debugging messaging system.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The **debug crypto condition unmatched** command does not affect the display or logging of syslog messages. This feature is not stored in the configuration, and must be reset after each power cycle.

Examples

The following example configures the filter to allow IPsec messages with insufficient context to appear:

```
hostname# debug crypto condition unmatched ipsec
```

Related Commands

Command	Description
debug crypto condition	Sets filtering conditions for IPsec and ISAKMP debugging messages.

Command	Description
debug crypto condition error	Shows debugging messages whether or not filtering conditions have been specified.
show crypto debug-condition	Shows the configured filters for IPsec and ISAKMP debugging messages.

debug crypto ca server

To set the local CA server debugging message level and begin listing associated debugging messages, use the **debug crypto ca server** command in ca server configuration mode. To disable the display of all debugging messages, use the **no** form of the command.

debug crypto ca server [*level*]

no debug crypto ca server [*level*]

Syntax Description

level	Sets the level to display associated debugging messages. The range of values is between 1 and 255.

Defaults

The default debugging level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Ca server configuration	•	—	•	—	—
Global configuration	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks. Levels 5 and higher are reserved for raw data dumps and should be avoided during normal debugging because of excessive debugging output.

Examples

The following example sets the debugging level to 3:

```
hostname(config-ca-server)# debug crypto ca server 3
hostname(config-ca-server)#
```

The following example turns off all debugging:

```
hostname(config-ca-server)# no debug crypto ca server
hostname(config-ca-server)#
```

Related Commands

Command	Description
cdp-url	Specifies the certificate revocation list (CRL) distribution point (CDP) to be included in the certificates issued by the CA.
crypto ca server	Provides access to the ca server configuration mode CLI command set, which allows you to configure and manage the local CA.
database path	Specifies a path or location for the local CA server database.
show crypto ca server	Displays the characteristics of the certificate authority configuration on the ASA in ASCII text format.
show crypto ca server certificate	Displays the local CA configuration in base64 format.
show crypto ca server crl	Displays the current CRL of the local CA.

debug crypto condition error

To show debugging messages for IPsec and ISAKMP whether or not they match any of the configured filters, use the **debug crypto condition error** command in privileged EXEC mode. To disable the display of debugging messages for IPsec and ISAKMP whether or not they match any of the configured filters, use the **no** form of this command.

debug crypto condition error [**ipsec | isakmp**]

[**no**] **debug crypto condition error** [**ipsec | isakmp**]

Syntax Description

ipsec	Specifies the IPsec debugging messaging system.
isakmp	Specifies the ISAKMP debugging messaging system.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The **debug crypto condition error** command does not affect the display or logging of syslog messages. This feature is not stored in the configuration, and must be reset after each power cycle.

Examples

The following example configures IPsec messages to appear whether or not filtering conditions have been specified:

```
hostname# debug crypto condition error ipsec
```

Related Commands

Command	Description
debug crypto condition	Sets filtering conditions for IPsec and ISAKMP debugging messages.
debug crypto condition unmatched	Shows debugging messages for IPsec and ISAKMP that do not include sufficient context information for filtering.
show crypto debug-condition	Shows the configured filters for IPsec and ISAKMP debugging messages.

debug crypto engine

To show debugging messages for the crypto engine, use the **debug crypto engine** command in privileged EXEC mode. To disable the display of debugging messages for the crypto engine, use the **no** form of this command.

debug crypto engine [*level*]

no debug crypto engine [*level*]

Syntax Description

level	(Optional) Sets the level to display debugging messages. The range of values is between 1 and 255. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

The following example enables debugging messages for the crypto engine:

```
hostname# debug crypto engine
```

Related Commands

Command	Description
debug crypto ca	Shows debugging messages for the CA.
debug crypto ipsec	Shows debugging messages for IPsec.
debug crypto ikev1	Shows debugging messages for IKEv1.
debug crypto ikev2	Shows debugging messages for IKEv2.

debug crypto ike-common

To show debugging processes that involve the IKE protocol, use the **debug crypto ike-common** command in privileged EXEC mode. To stop showing the debugging messages, use the **no** form of this command:

debug crypto ike-common [*level*]

no debug crypto ike-common [*level*]

Syntax Descriptiong

level	(Optional) Sets the debugging message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number. Level 1 (the default) shows messages only when errors occur. Levels 2 through 7 show additional information. Level 254 shows decrypted IKE packets in a human readable format. Level 255 shows hexadecimal dumps of decrypted IKE packets.

ing

Defaults

The default level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
8.4(1)	The command was introduced.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

The following example enables debugging messages processes involving the IKE protocol:

```
hostname# debug crypto ike-common
```

Related Commands

Command	Description
debug crypto ca	Shows debugging messages for the CA.
debug crypto engine	Shows debugging messages for the crypto engine.

Command	Description
debug crypto ipsec	Shows debugging messages for IPsec.
debug crypto ikev1	Shows debugging messages for IKEv1.
debug crypto ikev2	Shows debugging messages for IKEv2.

debug crypto ikev1

To show debug messages for IKEv1, use the **debug crypto ikev1** command in privileged EXEC mode. To stop showing the debugging messages, use the **no** form of this command:

debug crypto ikev1 [*level*] [**timers**]

no debug crypto ikev1 [*level*] [**timers**]

Syntax Description

level	(Optional) Sets the debugging message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number. Level 1 (the default) shows messages only when errors occur. Levels 2 through 7 show additional information. Level 254 shows decrypted IKEv1 packets in a human readable format. Level 255 shows hexadecimal dumps of decrypted IKEv1 packets.
timers	(Optional) Shows debugging messages for IKEv1 timer expiration.

Defaults

The default level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.
8.4(1)	The command name changed from **debug crypto isakmp** to **debug crypto ikev1**.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

The following example enables debugging messages for IKEv1:

```
hostname# debug crypto ikev1
```

Related Commands

Command	Description
debug crypto ca	Shows debugging messages for the CA.
debug crypto engine	Shows debugging messages for the crypto engine.
debug crypto ipsec	Shows debugging messages for IPsec.
debug crypto ikev2	Shows debugging messages for IKEv2.

debug crypto ikev2

To show debugging messages for IKEv2, use the **debug crypto ikev2** command in privileged EXEC mode. To stop showing the debugging messages, use the **no** form of this command:

debug crypto ikev2 {**ha** | **platform** | **protocol** | **timers**} [*level*]

no debug crypto ikev2 {**ha** | **platform** | **protocol** | **timers**} [*level*]

Syntax Description

ha	Shows debugging messages for IKEv1 high availability.
level	(Optional) Sets the debugging message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number. Level 1 (the default) shows messages only when errors occur. Levels 2 through 7 show additional information. Level 254 shows decrypted IKEv1 packets in a human-readable format. Level 255 shows hexadecimal dumps of decrypted IKEv1 packets.
platform	Shows debugging messages about ASA processing of IKEv2 vs. protocol specific exchanges, such as AAA interfacing, session manager, and the ASA cryptographic module performing encryption and decryption.
protocol	Shows debugging messages about the IKEv1 protocol.
timers	(Optional) Shows debugging messages for IKEv1 timer expiration.

Defaults

The default level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
8.4(1)	The command was introduced.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

The following example enables debug messages for IKEv2 protocol:

```
hostname# debug crypto ikev1 protocol
```

Related Commands

Command	Description
debug crypto ca	Shows debugging messages for the CA.
debug crypto engine	Shows debugging messages for the crypto engine.
debug crypto ipsec	Shows debugging messages for IPsec.
debug crypto ikev1	Shows debugging messages for IKEv1.

debug crypto ss-api

To show debugging messages for the crypto secure socket API, use the **debug crypto ss-api** command in privileged EXEC mode. To disable the display of these debugging messages, use the **no** form of this command.

debug crypto ss-api [*level*]

no debug crypto ss-api [*level*]

Syntax Description

level	(Optional) Sets the debugging message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
9.0(1)	This command was introduced.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

The following example enables debugging messages for the crypto secure socket API:

```
hostname# debug crypto ss-api
```

Related Commands

Command	Description
debug crypto ca	Shows debugging messages for the CA.
debug crypto engine	Shows debugging messages for the crypto engine.
debug crypto ikev1	Shows debugging messages for IKEv1.
debug crypto ikev2	Shows debugging messages for IKEv2.

debug crypto vpnclient

To show crypto debugging messages for the EasyVPN client, use the **debug crypto vpnclient** command in privileged EXEC mode. To stop showing the debugging messages, use the **no** form of this command:

debug crypto vpnclient [*level*]

no debug crypto vpnclient [*level*]

Syntax Description

level	(Optional) Sets the debugging message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

The following example enables crypto debugging messages for the Easy VPN client:

```
hostname# debug crypto vpnclient
```

Related Commands

Command	Description
debug crypto ca	Shows debugging messages for the CA.
debug crypto engine	Shows debugging messages for the crypto engine.
debug crypto ikev1	Shows debugging messages for IKEv1.
debug crypto ikev2	Shows debugging messages for IKEv2.

debug crypto ipsec

To show debugging messages for IPsec, use the **debug crypto ipsec** command in privileged EXEC mode. To stop showing debugging messages for IPsec, use the **no** form of this command.

debug crypto ipsec [*level*]

no debug crypto ipsec [*level*]

Syntax Description

level	(Optional) Sets the debugging message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

The following example enables debugging messages for IPsec:

```
hostname# debug crypto ipsec
```

Related Commands

Command	Description
debug crypto ca	Shows debugging messages for the CA.
debug crypto engine	Shows debugging messages for the crypto engine.
debug crypto ikev1	Shows debugging messages for IKEv1.
debug crypto ikev2	Shows debugging messages for IKEv2.

debug ctiqbe

To show debugging messages for CTIQBE application inspection, use the **debug ctiqbe** command in privileged EXEC mode. To stop showing debugging messages for CTIQBE application inspection, use the **no** form of this command.

debug ctiqbe [*level*]

no debug ctiqbe [*level*]

Syntax Description

level	(Optional) Sets the debugging message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default value for the debugging level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

To see the current debugging command settings, enter the **show debug** command. To stop the debugging output, enter the **no debug** command. To stop all debugging messages from being displayed, enter the **no debug all** command.

Note Enabling the **debug ctiqbe** command may slow down traffic on busy networks.

Examples

The following example enables debugging messages at the default level (1) for CTIQBE application inspection:

```
hostname# debug ctiqbe
```

Related Commands

Command	Description
inspect ctiqbe	Enables CTIQBE application inspection.
show ctiqbe	Displays information about CTIQBE sessions established through the ASA.
show conn	Displays the connection state for different connection types.
timeout	Sets the maximum idle time duration for different protocols and session types.

debug ctl-provider

To show debugging messages for Certificate Trust List (CTL) providers, use the **debug ctl-provider** command in privileged EXEC mode. To stop showing debugging messages, use the **no** form of this command.

debug ctl-provider [**errors** | **events** | **parser**]

no debug ctl-provider [**errors** | **events** | **parser**]

Syntax Description

errors	Specifies CTL provider error debugging.
events	Specifies CTL provider event debugging.
parser	Specifies CTL provider parser debugging.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

The following example enables debugging messages for CTL provider:

```
hostname# debug ctl-provider
```

Related Commands

Command	Description
ctl	Parses the CTL file from the CTL client and install trustpoints.
ctl-provider	Configures a CTL provider instance in CTL provider mode.
export	Specifies the certificate to be exported to the client.
service	Specifies the port to which the CTL provider listens.

debug cxsc

To show debugging messages for the ASA CX module, use the **debug cxsc** command in privileged EXEC mode. To stop showing debugging messages, use the **no** form of this command.

debug cxsc [**error** | **event** | **message**]

no debug cxsc [**error** | **event** | **message**]

Syntax Description

error	Enables error-level debugging.
event	Enables event-level debugging.
message	Enables message-level debugging.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
8.4(4.1)	This command was introduced.
9.1(3)	You can now configure ASA CX policies per context.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

When you enable the authentication proxy, the ASA generates a debugging messge when it sends an authentication proxy TLV to the ASA CX module, giving details of the IP and port:

```
DP CXSC Event: Sent Auth proxy tlv for adding Auth Proxy on interface: inside4.
DP CXSC Event: Sent Auth proxy tlv for adding Auth Proxy on interface: cx_inside.
DP CXSC Event: Sent Auth proxy tlv for adding Auth Proxy on interface: cx_outside.
```

When the interface IP address is changed, auth-proxy tlv updates are sent to CXSC:

```
DP CXSC Event: Sent Auth proxy tlv for removing Auth Proxy for interface inside.
DP CXSC Event: Sent Auth proxy tlv for adding Auth Proxy on interface: inside.
```

When a flow is freed on the ASA, the ASA CX module is notified so it can clean up the flow:

```
DP CXSC Msg: Notifying CXSC that flow (handle:275233990) is being freed  for
192.168.18.5:2213 -> 10.166.255.18:80.
```

When the ASA CX module sends a redirect to a client to authenticate, and that redirect is sent to the ASA, the ASA sends it to the ASA CX module. In this example, 192.168.18.3 is the interface address and port 8888 is the authentication proxy port reserved on that interface for the authentication proxy feature:

```
DP CXSC Msg: rcvd authentication proxy data from 192.168.18.5:2214 -> 192.168.18.3:8888,
forwarding to cx
```

When a VPN connection is established on the ASA, and the ASA sends connection information to the ASA CX module:

```
CXSC Event:   Dumping attributes from the vpn session record
CXSC Event:   tunnel->Protocol:        17
CXSC Event:   tunnel->ClientVendor:    SSL VPN Client
CXSC Event:   tunnel->ClientVersion:   Cisco AnyConnect VPN Agent for Windows 2.4.1012
CXSC Event:   Sending VPN RA session data to CXSC
CXSC Event:   sess index:      0x3000
CXSC Event:   sess type id:    3
CXSC Event:   username:        devuser
CXSC Event:   domain:          CN=Users,DC=test,DC=priv
CXSC Event:   directory type:  1
CXSC Event:   login time:      1337124762
CXSC Event:   nac result:      0
CXSC Event:   posture token:
CXSC Event:   public IP:       172.23.34.108
CXSC Event:   assigned IP:     192.168.17.200
CXSC Event:   client OS id:    1
CXSC Event:   client OS:
CXSC Event:   client type:     Cisco AnyConnect VPN Agent for Windows 2.4.1012
CXSC Event:   anyconnect data: , len: 0
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
class-map	Identifies traffic for use in a policy map.
cxsc	Redirects traffic to the ASA CX module.
cxsc auth-proxy port	Sets the authentication proxy port.
hw-module module password-reset	Resets the module password to the default.
hw-module module reload	Reloads the module.
hw-module module reset	Performs a reset and then reloads the module.
hw-module module shutdown	Shuts down the module.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
session do get-config	Gets the module configuration.
session do password-reset	Resets the module password to the default.
session do setup host ip	Configures the module management address.
show asp table classify domain cxsc	Shows the NP rules created to send traffic to the ASA CX module.
show asp table classify domain cxsc-auth-proxy	Shows the NP rules created for the authentication proxy for the ASA CX module.
show module	Shows the module status.

Command	Description
show running-config policy-map	Displays all current policy map configurations.
show service-policy	Shows service policy statistics.