

database path through debug cxsc Commands

Γ

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.					
	<i>mount-name</i> Specifies the mount name.						
Defaults	By default, the CA	server databa	ise is stored i	in flash memory.			
Command Modes	The following tabl	e shows the m	odes in whic	ch you can enter	the comma	nd:	
			Firewall N	lode	Security (Context	
						Multiple	
	Command Mode		Routed	Transparent	Single	Context	System
	Ca server configu	ration	•		•		
Command History	Release	Modifi	ication				
	8.0(2)	This c	ommand was	s introduced.			
Usage Guidelines	The local CA files PKCS12 files, and for the mount con	stored in the d the current Cl nmand that is u	latabase inclu RL file. The used to speci	ude the certificat <i>mount-name</i> arg fy a file system a	te database, sument is the for the ASA	user database the same as the A.	files, temporary name argument
<u>Note</u>	These CA files are	e internal, store	ed files and s	hould not be mo	odified.		
Examples	The following exa directory on the m hostname(config) hostname(config-	mple defines th ount point as o # crypto ca s ca-server)# .ca-server)#	he mount poi ca_dir/files_c server database pa	nt for the CA da dir: .th cifs_share	tabase as ci ca_dir/fi:	ifs_share and th	ne database files

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 R	Rs.						
Command Modes	The following table shows	the modes in whic	h you can enter	the comma	nd:			
		Firewall N	lode	Security C	Context			
					Multiple			
	Command Mode	Routed	Transparent	Single	Context	System		
	Ddns-update-method	•		•	•			
Command History	Palassa	Modification						
Command mistory	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 use	d to maintain consi	stent informatio	n between	the DNS A and	1 PTR RR types.		
	When issued in ddns-updat is just to a DNS A RR, or	te-method configur to both DNS A and	ation mode, the d I PTR RR types.	ldns comm	and defines wh	ether the update		
Examples	The following example co method named ddns-2:	nfigures updates to	both the DNS A	A and PTR	RRs for the DI	ONS update		
	hostname(config)# ddns hostname(DDNS-update-me	update method ddm thod)# ddns both	ns-2					

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	Specifi	ies a hostnan	ne to be used for	r updates.			
	method-name	<i>od-name</i> Specifies a method name for association with the interface being configured.						
Defaults	No default behavior or v	alues.						
Command Modes	The following table show	ws the m	odes in whic	h you can enter	the comma	nd:		
			Firewall M	lode	Security C	ontext		
				_		Multiple		
	Command Mode		Routed	Iransparent	Single	Context	System	
	Interface configuration		•	—	•	•	—	
Command History	Release	Modifi	cation					
	7.2(1)This command was introduced.							
Usage Guidelines	After defining a DDNS uupdates.	update m	ethod, you n	nust associate it	with an AS	SA interface to	trigger DDNS	
	A hostname could be a F the ASA appends a domain the ASA appends a domain the ASA appender a domain the ASA appender a domain the ASA appender appender a domain the ASA appender appen	⁷ ully Qua ain name	alified Doma to the hostn	in Name (FQD) ame to create a	N) or just a FQDN.	hostname. If ju	ist a hostname,	
Examples	The following example a named ddns-2 and the ho	associate ostname	s the interfac hostname1.e	e GigabitEtherr xample.com:	net0/2 with	the DDNS upc	late method	
	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	<i>name</i> Specifies the name of a method for dynamically updating DNS records.							
Defaults	No default behavior or val	ues.						
Command Modes	The following table shows	ows the modes in which you can enter the command:						
		Firewall M	ode	Security C	ontext			
					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-t method configured by the updates are performed. Of by RFC 2136 and a generi	to-address and addre ddns update meth the two methods for c HTTP method—t	ess-to-name map od command de or performing D he ASA support	pping maint termines w DNS update ts the IETF	tained by DNS hat and how of es—the IETF s method in this	5. The update ften DDNS standard defined s release.		
	Name and address mappin	ig is contained in tw	vo types of resou	urce records	s (RRs):			
	• The A resource record	d contains domain n	ame-to IP-addre	ess mapping	2.			
	• The PTR resource rec	ord contains IP add	ress-to-domain	name mapp	oing.			
	DDNS updates can be use	d to maintain consis	stent informatio	n between t	the DNS A and	l PTR RR types.		
Note	Before the ddns update n server using the dns comm	nethod command w nand with domain lo	ill work, you m ookup enabled c	ust configu on the interf	re a reachable ⁵ ace.	default DNS		
Examples	The following example co hostname(config)# ddns	nfigures the DDNS update method ddr	update method ns-2	named ddn	s-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 of	lebugging messa	ges for acc	ounting only.				
	authentication	(Optional) Show of	lebugging messag	ges for auth	nentication onl	у.			
	authorization	(Optional) Show of	lebugging messa	ges for auth	norization only				
	common	common(Optional) Show debugging messages for different states within the AAA feature.							
	internal	(Optional) Show of local database onl	(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 of	lebugging messag	ges for VPI	N-related AAA	functions only.			
Defaults Command Modes	The default debuggi	ng level is 1. shows the modes in whi	ch you can enter	the comma	ınd:				
		Firewall	Vode	Security (Context				
				t Single	Multiple				
	Command Mode	Routed	Transparent		Context	System			
	Privileged EXEC	•	•	•	•	•			
Command History	Release	Modification							
	7.0(1)	This command wa	s modified to inc	clude new k	keywords.				
Usage Guidelines Examples	The debug aaa com undebug all comma The following is san hostname(config)# debug aaa internal	mand displays detailed inds turn off all enabled nple output from the del	nformation abou debugging comm oug aaa internal	t AAA acti hands. command:	vity. The no d o	ebug all and			

Related Commands	Command	Description
	show running-config	Displays the running configuration related to AAA.
	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 N	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.

I

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	Ink (Optional) Displays runtime information about processing of chunked transfer encoded packets.						
	event	(Option	nal) Displays	debug informa	tion about j	packet inspecti	on events.	
	eventverb	(Option	nal) Displays	the action take	n by the AS	SA in response	to an event.	
	regex	(Option signatur	al) Displays res.	information ab	out matchi	ng patterns wit	h predefined	
Defaults	All options are ena	bled by default	t.					
Command Modes	The following table	e shows the mo	odes in which	n you can enter	the comma	nd:		
			Firewall M	ode	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 debug all and und	command displ ebug all comm	lays detailed aands turn of	information ab f all enabled de	out HTTP : bug comm	application ins ands.	pection. The no	
Examples	The following example enables the display of detailed information about application inspection:							
	hostname# debug a	appfw						
Related Commands	Commands	Descrip	otion					
	http-map	Defines	s an HTTP m	hap for configur	ing enhanc	ed HTTP inspe	ection.	
	inspect http	Applies	s a specific H	HTTP map to us	e for applic	cation inspection	on.	

debug arp

I

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 a	rguments o	r keywords
--------------------	--------------	----------	------------	------------

Defaults No default behavior or values.

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

	Firewall N	Firewall Mode		Security Context		
		Multiple		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 Mod	le	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

Γ

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

debug asdm history level

Syntax Description	level	(Optional) Specific	es the debugging	glevel.				
Defaults	The default debugging	level is 1.						
Command Modes	The following table sh	ows the modes in whic	ch you can enter	the comma	ınd:			
		Firewall	Aode	Security (Context			
					Multiple			
	Command Mode	Routed	Transparent	Single	Context	System		
	Privileged EXEC	•	•	•	•	•		
Command History	Release	Modification						
	7.0(1)	This command wa debug asdm histo	s changed from t ry command.	the debug J	pdm history co	ommand to the		
Usage Guidelines	Because debugging our unusable. For this reas troubleshooting session during periods of lowe likelihood that increase	tput is assigned high p on, use debug comma as with Cisco technica r network traffic and f ed debug command pr	priority in the CP nds only to trout l support staff. M wer users. Debu rocessing overhea	PU process, oleshoot sp loreover, it ugging duri ad will affe	it can render t ecific problem is best to use d ing these perio ect system use.	he system s or during ebug commands ds decreases the		
Examples	The following example	e enables level 1 debug	gging of ASDM:					
	hostname# debug asdm history debug asdm history enabled at level 1							
	hostname#							
Related Commands	Command	Description						
	show asdm history	Displays the conte	ents of the ASDM	l history bu	ıffer.			

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	(Option of value messa	onal) Sets the ues is betwee ges at higher	level at which to n 1 and 255. Th levels, set the le	display de e default is evel to a hig	bugging messa 1. To display gher number.	ages. The range additional	
	server	Identi	fies the auto-	update server.				
Defaults The default value for the debugging level is 1.								
Command Modes	The following table :	shows the m	nodes in whic	h you can enter	the comma	nd:		
			Firewall N	lode	Security C	ontext		
						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 au hostname# debug au hostname# show deb debug auto-update debug auto-update	to-update to-update ug auto-up client ena server ena	client server date bled at leve bled at leve	el 1 el 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	Image:					ages. The range additional	
Defaults	The default value for the	debugging level is 1					
Command Modes	The following table show	s the modes in whic	h you can enter	the comma	nd:		
		Firewall N	lode	Security C	ontext		
					Multiple		
	Command Mode	Routed	Transparent	Single	Context	System	
	Privileged EXEC	•	•	•		•	
Command History	Release Modification						
	8.0(2)	This command was	s introduced.				
Usage Guidelines	Because debugging outpu unusable. For this reason, troubleshooting sessions v during periods of lower no likelihood that increased o	it is assigned high p use debug comman with Cisco technical etwork traffic and for debug command pr	riority in the CP nds only to troub support staff. M ewer users. Debu ocessing overhea	U process, bleshoot spe foreover, it agging duri ad will affe	it can render t ecific problems is best to use d ng these period ct system use.	he system s or during ebug commands ds decreases the	
Examples	The following is sample of hostname# debug boot-me debug boot-mem enabled hostname# show debug bo debug boot-mem enabled	output from the deb em at level 1 oot-mem at level 1	ug boot-mem ar	nd the show	7 debug boot-1	nem commands.	
Related Commands	Command	Description	nt hoot memory	debugging	configuration		
		2.5prays the current	it soot memory		configuration.		

Defaults	The default value for	the debugging level is	1.			
Command Modes	The following table s	hows the modes in wh	ich you can enter	the comma	and.	
		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 5525-X, 5545-X, and 5555-X.					orts the ASA 55	512-X, 5515-X,
Usage Guidelines	Because debugging or unusable. For this rea troubleshooting session during periods of low likelihood that increas	utput is assigned high son, use debug commons ons with Cisco technica er network traffic and sed debug command p	priority in the CP ands only to troub al support staff. M fewer users. Debu processing overhea	PU process, bleshoot sp loreover, it ugging duri ad will affe	it can render t ecific problem is best to use d ing these perio ect system use.	he system s or during ebug commands ds decreases the
Examples	The following is samp hostname# debug boo debug boot-module e	ple output from the de t-module nabled at level 1	bug boot-module	e command	:	

debug boot-module

level

Syntax Description

ſ

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.

higher levels, set the level to a higher number.

(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

debug boot-module [level]

no debug boot-module [level]

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

debug cluster

Γ

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.					
	сср	(Option	al) Display	s debug message	s for the cl	uster control p	protocol.
	datapath	(Option	al) Display	s debug message	s for the da	itapath.	
	fsm	(Option	al) Display	s debug message	es for the fin	nite state mach	nine.
	general	(Option	al) Display	s general cluster	ing debug r	nessages.	
	hc	(Option	al) Display	s debug message	es for the he	ealth check.	
	license	(Option	al) Display	s debug message	es for the cl	uster license.	
	rpc	(Option	al) Display	s debug message	s for the R	PC module.	
	transport	(Option	al) Display	s debug message	es for the tra	ansport service	2.
Command Modes	The following tabl	e shows the mo	odes in whic	h you can enter	the comman	nd: ontext Multiple	
	Command Mode		Routed	Transparent	Single	Context	System
	Privileged EXEC		•	•	•	_	•
Command History	Release	Modific	ation				
	9.0(1)	We intro	oduced this	command.			

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

Γ

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 whic	h you can enter	the comma	ind:			
		Firewall N	lode	Security (Context			
					Multiple			
	Command Mode	Routed	Transparent	Single	Context	System		
	Privileged EXEC	•	•			•		
Command History	Release Modification							
,	7.0(1)	This command was	s introduced.					
Usage Guidelines	Using debug comma	ands might slow down tra	uffic on busy net	works.				
Examples	The following exam	ple enables debug messa	ges for context n	nanagemen	t:			
	hostname# debug cc	ontext						
Related Commands	Command	Description						
	context	Creates a security configuration mod	context in the sy e.	stem config	guration and er	nters context		
	show context	Shows context info	ormation.					
	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 sh	ows the modes in whic	h you can enter	the comma	ind:		
		Context					
					Multiple		
	Command Mode	Routed	Transparent	Single	Context	System	
	Privileged EXEC	•	•	•		•	
Command History	Release	Modification					
	7.0(1)	This command was	s introduced.				
Usage Guidelines Examples	Using debug commands might slow down traffic on busy networks. The following example enables debugging messages for the control plane:						
Related Commands	Command	Description		1		TETD	
	nw-module module recover	server.	gent SSM by loa	ading a reco	overy image fr	om a IFIP	
	hw-module module reset	Shuts down an SSM	A and performs	a hardware	reset.		
	hw-module moduleReloads the intelligent SSM software.reload						

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 of	only debugging i	messages fo	or PKI transact	tions.	
	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 comn	nand shows all debuggir	ng messages. The	e default le	vel is 1.		
Command Modes	The following table s	hows the modes in whic	h you can enter	the comma	ind:		
		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 comman	nds might slow down tra	affic on busy net	works.			
Examples	The following examp hostname# debug cry	le enables debugging m /pto ca	essages for PKI:				

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**]

Syntax Description	group <i>group_name</i> Specifies the group being used and the client group name.					
	peer <i>peer_addr</i>	Specifies the IPsec peer and its IP address				
	reset	Clears all filtering	conditions and c	lisables filt	ering.	
	spi spi	Specifies the IPsec	SPI.			
	subnet subnet_mask	Specifies the subne IP address.	et and subnet ma	sk that are	associated with	h the specified
	user user_name	Specifies the client	being used and	the client u	isername.	
Defaults	No default behavior or	values.				
Command Modes	The following table sho	ows the modes in whic	h you can enter	the comma	ind:	
		Firewall N	lode	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 con feature is not stored in	dition command does the configuration, and	not affect the dis must be reset af	splay or log fter each po	gging of syslog ower cycle.	messages. This
Examples	The following example	es 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

ſ

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 ISAK	MP debugging	messaging	system.		
Defaults	No default behavior o	or values.					
Command Modes	The following table s	shows the modes in whic	h you can enter	the comma	ind:		
		Firewall N	lode	Security C	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 co This feature is not sto	ondition error command ored in the configuration	does not affect to and must be re	the display set after ea	or logging of s ch power cycle	yslog messages. e.	
Examples	The following examp been specified:	ble configures IPsec mes	sages to appear	whether or	not filtering co	onditions have	
	hostname# debug cr	ypto condition error :	ipsec				
Related Commands	Command	Description					
	debug crypto condition	Sets filtering condi	tions for IPsec a	and ISAKM	IP debugging r	nessages.	

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	c debugging mes	saging sys	tem.			
	isakmp	Specifies the ISAk	MP debugging	messaging	system.			
Defaults	No default behavior	or values.						
Command Modes	The following table s	shows the modes in whic	ch you can enter	the comma	and:			
		Firewall N	lode	Security (Context			
					Multiple			
	Command Mode	Routed	Transparent	Single	Context	System		
	Privileged EXEC	•	•	•	•			
Command History	Release Modification							
	8.0(2)	This command wa	s introduced.					
Usage Guidelines	The debug crypto co messages. This featu	ondition unmatched co re is not stored in the co	mmand does not nfiguration, and	affect the must be re	display or logg set after each I	ing of syslog power cycle.		
Examples	The following examp hostname# debug cr	ble configures the filter to ypto condition unmate	o allow IPsec me hed ipsec	essages wit	h insufficient c	ontext to appear:		
Deleted Occurrence 1	0	Description						
Related Commands	Command	Description	tions for IDaga		(D. dahara alara			
	aeoug crypto condition	Sets filtering cond	itions for IPsec a	and ISAKN	iP debugging i	nessages.		

Γ

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 Se is	ts the level to dis between 1 and 2	play associated of 55.	debugging	messages. The	range of values	
Defaults	The default debugging level	is 1.					
Command Modes	The following table shows th	e modes in whic	ch you can enter	the comma	ind:		
		Firewall N	lode	Security (Context		
					Multiple		
	Command Mode	Routed	Transparent	Single	Context	System	
	Ca server configuration	•		•			
	Global configuration	•		•			
	Privileged EXEC	•		•	—		
Command History		dification	introduced				
Usage Guidelines	Using debug commands mig raw data dumps and should be	ht slow down tra e avoided during	ffic on busy netw normal debuggi	vorks. Leve ng because	ls 5 and higher of excessive d	are reserved for ebugging output.	
Examples	The following example sets t	the debugging le	vel to 3: to ca server 3				
	The following example turns	hostname(config-ca-server)# The following example turns off all debugging: hostname(config-ca-server)# no debug crypto ca server					
	hostname(config-ca-server	<u>^</u>)#					

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	c debugging mes	saging syst	em.		
	isakmp	Specifies the ISA	KMP debugging	messaging	system.		
Defaults	No default behavior o	r values.					
Command Modes	The following table sh	nows the modes in which	ch you can enter	the comma	ind:		
		Firewall	Mode	Security (Context		
	Command Mode	Routed	Transparent	Single	Multiple 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 cor This feature is not sto	ndition error command red in the configuration	d does not affect n, and must be re	the display eset after ea	or logging of s ch power cyclo	yslog messages. e.	
Examples	The following exampl been specified:	e configures IPsec mes	ssages to appear	whether or	not filtering co	onditions have	
	hostname# debug cry	pto 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 s	hows the modes in whic	h you can enter	the comma	ınd:		
		Firewall N	lode	Security (Context		
					Multiple		
	Command Mode	Routed	Transparent	Single	Context	System	
	Privileged EXEC	•	•	•	•		
Command History	Release Modification						
	7.0(1)	This command was	s introduced.				
Usage Guidelines Examples	Using debug comman The following examp hostname# debug cry	nds might slow down tra le enables debugging m m to engine	affic on busy net essages for the c	works. crypto engin	ne:		
Related Commands	Command	Description	massagas for the	<u>CA</u>			
	debug crypto ca	Shows debugging 1	nessages for the	sec.			
	debug crypto ikev1	Shows debugging i	nessages for IK	Ev1.			
	debug crypto ikev2	Shows debugging 1	nessages for IK	Ev2.			

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 sho	ws the modes in whic	ch you can enter	the comma	and:		
		Firewall N	lode	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 multip	le context mode	was added	•		
Usage Guidelines	Using debug commands	s might slow down tra	affic on busy net	works.			
Examples	The following example	enables debugging m	essages process	es involving	g the IKE proto	ocol:	
	hostname# debug crypt	o ike-common					
Related Commands	Command	Description					
	debug crypto ca	Shows debugging	messages for the	CA.			
	debug crypto engine	Shows debugging	nessages for the	e crypto eng	gine.		

ſ

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

Γ

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)	al) Shows c	lebugging messa	iges for IKl	Ev1 timer expi	ration.
Defaults	The default level is	1.					
Command Modes	The following table	shows the mo	des in whic	h you can enter	the comma	nd:	
			Firewall M	lode	Security Context		
						Multiple	
	Command Mode		Routed	Iransparent	Single	Context	System
	Privileged EXEC		•	•	•	•	
Command History	Release	Modific	ation				
	7.0(1)	This co	nmand was	introduced.			
	8.4(1)	The command name changed from debug crypto isakmp to debug crypto ikev1 .					
	9.0(1)	Support	for multipl	e context mode	was added.		
Usage Guidelines Examples	Using debug comma The following exam hostname# debug ca	ands might slo ple enables de cypto ikev1	w down tra bugging mo	ffic on busy net essages for IKE	works. v1:		

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.

13-45

debug crypto ikev2

Γ

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 IK	Ev1 high av	vailability.		
	level	(Optional) Sets the debugging message level to display, between 1 and 255.					
		The default is 1. T	o display addition	nal message	es at higher lev	els, set the level	
		to a higher numbe	r. Level 1 (the de	tault) show	vs messages or	ly when errors	
		decrypted IKEv1	packets in a hum	an-readable	e format. Level	255 shows	
		hexadecimal dum	ps of decrypted I	KEv1 pack	ets.		
	platform	Shows debugging	messages about	ASA proce	ssing of IKEv2	2 vs. protocol	
		specific exchange	s, such as AAA ir	nterfacing, s	session manag	er, and the ASA	
		cryptographic mo	dule performing	encryption	and decryption	1.	
	protocol	Shows debugging	messages about	the IKEv1	protocol.		
	timers	(Optional) Shows	debugging messa	ages for IK	Ev1 timer exp	iration.	
Defaulte	The default level is 1						
Delaults	The default level is 1.						
Command Modes	The following table sho	ows the modes in whi	ch vou can enter	the comma	ind:		
	C		5				
		Firewall Mode Security Context					
				Single	Multinle		
	Command Mode	Routed	Transnarent		Context	System	
	Privileged FXFC	•	•	•	oomext	oystem	
0	Deleges	84 - 116 41					
Command History	Kelease		• . 1 1				
	8.4(1)	The command wa	s introduced.				
	9.0(1)	Support for multi	ple context mode	was added	•		
Usage Guidelines	Using debug command	s might slow down th	raffic on busy net	works.			
Framnles	The following example	enables debug mess	ages for IKEy? n	rotocol			
Examples	heathered article		ages for fixev2 p.	1010001.			
	nosiname# depud crvp	LO IKEVI DIOLOCOL					

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

Γ

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 sh	ows the modes in which	ch you can enter	the comma	and:				
		Firewall	Node	Security (Context				
				-	Multiple				
	Command Mode	Routed	Transparent	Single	Context	System			
	Privileged EXEC	•	•	•					
						l			
Command History	Release Modification								
	9.0(1) This command was introduced.								
Usage Guidelines	Using debug command	ds might slow down tr	affic on busy net	works.					
Examples	The following example	e enables debugging m	nessages for the c	ervnto secu	re socket API:				
	hostname# debug crypto ss-api								
Related Commands	Command	Description							
	debug crypto ca	Shows debugging	messages for the	e CA.					
	debug crypto engine	Shows debugging	messages for the	e crypto eng	gine.				
	debug crypto ikev1	Shows debugging	messages for IK	Ev1.					
	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 sho	ows the modes in whic	h you can enter	the comma	nd:				
		Firewall N	lode	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 command	s might slow down tra	ffic on busy net	works.					
Examples	The following example hostname# debug cryp	enables crypto debug to vpnclient	ging messages f	or the Easy	VPN client:				
Related Commands	Command	Description							
	debug crypto ca	Shows debugging t	nessages for the	CA.					
	debug crypto engine	Shows debugging 1	nessages for the	crypto eng	gine.				
	debug crypto ikev1	Shows debugging r	nessages for IK	Ev1.					
	debug crypto ikev2	Shows debugging 1	nessages for IK	Ev2.					

debug crypto ipsec

Γ

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 sho	ws the modes in whic	h you can enter	the comma	ind:					
		Firewall N	lode	Security (Context					
					Multiple					
	Command Mode	Routed	Transparent	Single	Context	System				
	Privileged EXEC	•	•	•						
Command History	Release Modification									
	7.0(1)	This command was	s introduced.							
Usage Guidelines	Using debug command	s might slow down tra	ffic on busy net	works.						
Examples	The following example enables debugging messages for IPsec: hostname# debug crypto ipsec									
Related Commands	Command	Description								
	debug crypto ca	Shows debugging 1	nessages for the	CA.						
	debug crypto engine	Shows debugging 1	nessages for the	crypto eng	gine.					
	debug crypto ikev1	Shows debugging 1	nessages for IK	Ev1.						
	debug crypto ikev2 Shows debugging messages for IKEv2.									

13-49

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 show	s the modes in whic	ch you can enter	the comma	ınd:					
		Firewall N	lode	Security (Context					
					Multiple					
	Command Mode	Routed	Transparent	Single	Context	System				
	Privileged EXEC	•	•	•	•					
Command History	Release	Release Modification								
	7.0(1)	This command was	s introduced.							
Usage Guidelines	To see the current debugg output, enter the no debu no debug all command.	ing command setting g command. To stop	gs, enter the sho o all debugging	w debug co messages fi	ommand. To sto rom being disp	p the debugging layed, enter the				
Note	Enabling the debug ctiq t	e command may sl	ow down traffic	on busy ne	tworks.					
Examples	The following example en inspection:	The following example enables debugging messages at the default level (1) for CTIQBE application inspection:								
	hostname# debug ctiqbe									

Related Commands

Γ

;	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 pro	vider parser deb	ugging.				
Defaults	No default behavior	or values.						
Command Modes	The following table s	shows the modes in which	ch you can enter	the comma	and:			
		Firewall N	Node	Security (Context			
					Multiple			
	Command Mode	Routed	Transparent	Single	Context	System		
	Privileged EXEC	•	•	•	•			
Jsage Guidelines	8.0(2) Using debug comma	This command wa	s introduced. affic on busy net	works.				
Examples	The following examp hostname# debug ct	ole enables debugging m 1-provider	nessages for CTL	. provider:				
Related Commands	Command	Description						
	ctl	Parses the CTL fil	e from the CTL	client and i	nstall trustpoir	nts.		
	ctl-provider	Configures a CTL	provider instanc	e in CTL p	provider mode.			
	export Specifies the certificate to be exported to the client.							
	service Specifies the port to which the CTL provider listens.							

debug cxsc

Γ

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]

error Enables error-level debugging.								
event Enables event-level debugging.								
message	Enable	s message-le	evel debugging.					
No default behavior or	values.							
The following table sho	ows the m	odes in whic	h you can enter	the comma	nd:			
		Firewall N	lode	Security C	Context			
					Multiple			
Command Mode		Routed	Transparent	Single	Context	System		
Privileged EXEC		•	•	•	•			
Release Modification								
8.4(4.1)This command was introduced.								
9.1(3)	You can now configure ASA CX policies per context.							
Using debug command	s might sl	ow down tra	iffic on busy net	works.				
When you enable the at authentication proxy TI	uthenticat LV to the	ion proxy, th ASA CX mc	e ASA generate odule, giving det	s a debugg ails of the l	ing messge wh IP and port:	en it sends an		
DP CXSC Event: Sent A DP CXSC Event: Sent A DP CXSC Event: Sent A	Auth prox Auth prox Auth prox	y tlv for a y tlv for a y tlv for a	adding Auth Pro adding Auth Pro adding Auth Pro	oxy on int oxy on int oxy on int	erface: insid erface: cx_ir erface: cx_ou	de4. nside. ıtside.		
When the interface IP a	ddress is	changed, au	th-proxy tlv upd	ates are ser	nt to CXSC:			
DP CXSC Event: Sent A DP CXSC Event: Sent A	Auth prox Auth prox	y tlv for a y tlv for a	removing Auth 1 adding Auth Pro	Proxy for oxy on int	interface ins erface: insid	side. le.		
When a flow is freed or	n the ASA	, the ASA C	X module is not	ified so it o	can clean up th	e flow:		
DP CXSC Msg: Notifyir 192.168.18.5:2213 ->	.ifying CXSC that flow (handle:275233990) is being freed for .3 -> 10.166.255.18:80.							
	error event message No default behavior or The following table shot Privileged EXEC Release 8.4(4.1) 9.1(3) Using debug command When you enable the at authentication proxy The CXSC Event: Sent of DP CXSC Event Sent of DP CXSC	errorEnableeventEnablemessageEnablemessageEnableNo default behavior or values.The following table shows the meCommand ModePrivileged EXECReleaseModifia8.4(4.1)This co9.1(3)You caUsing debug commands might slWhen you enable the authenticateauthentication proxy TLV to the sectorDP CXSC Event:Sent Auth proxDP CXSC Msg:Notifying CXSC t192.168.18.5:2213 -> 10.166.2	error Enables error-level event Enables event-level message Enables message-level No default behavior or values. The following table shows the modes in which Command Mode Firewall N Firewall N Command Mode Firewall N Privileged EXEC Release Modification 8.4 (4.1) This command was 9.1 (3) Vou can now confi Using debug commands might slow down tradition proxy the authentication proxy the authentication proxy the for a DP CXSC Event: Sent Auth prox	error Enables error-level debugging. event Enables event-level debugging. message Enables message-level debugging. No default behavior or values. Image: State St	error Enables error-level debugging. event Enables event-level debugging. message Enables message-level debugging. No default behavior or values. The following table shows the modes in which you can enter the comma	error Enables error-level debugging. event Enables event-level debugging. message Enables message-level debugging. No default behavior or values. Firewall Mode Security Context firewall Mode Routed Transparent Single Context Privileged EXEC • • • • Release Modification 8.4(4.1) This command was introduced. 9.1(3) You can now configure ASA CX policies per context. Using debug commands might slow down traffic on busy networks. When you enable the authentication proxy, the ASA generates a debugging messee wh authentication proxy TLV to the ASA CX module, giving details of the IP and port: DP CXSC Event: Sent Auth proxy t1v for adding Auth Proxy on interface: inside DP CXSC Event: Sent Auth proxy t1v for adding Auth Proxy on interface: cx, or When the interface IP address is changed, auth-proxy t1v updates are sent to CXSC: DP CXSC Event: Sent Auth proxy t1v for adding Auth Proxy on interface: inside DP CXSC Event: Sent Auth proxy t1v for adding Auth Proxy on interface: inside DP CXSC Event: Sent Auth proxy t1v for adding Auth Proxy on interface: inside DP CXSC Event: Sent Auth proxy t1v for adding Auth Proxy on interface: inside DP CXSC Event: Sent Auth proxy t1v for adding Auth Proxy on interface: inside DP CXSC Event: Sent Auth proxy t1v for adding Auth Proxy on interface: inside DP CXSC Event: Sent Auth proxy t1v for adding Auth Proxy on interface: inside DP CXSC Event: Sent Auth proxy t1v for adding Auth Proxy on interface: inside DP CXS		

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 \mathchar` 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 attribute	es from the vpn session record
CXSC	Event:	tunnel->Protocol:	: 17
CXSC	Event:	tunnel->ClientVer	ndor: SSL VPN Client
CXSC	Event:	tunnel->ClientVer	rsion: Cisco AnyConnect VPN Agent for Windows 2.4.1012
CXSC	Event:	Sending VPN RA se	ession 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

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.