CHAPTER 29

java-trustpoint through kill Commands

java-trustpoint

To configure the WebVPN Java object signing facility to use a PKCS12 certificate and keying material from a specified trustpoint location, use the **java-trustpoint** command in webvpn configuration mode.To remove a trustpoint for Java object signing, use the **no** form of this command.

java-trustpoint *trustpoint*

no java-trustpoint

Syntax Description

trustpoint	Specifies the trustpoint location configured by the **crypto ca import** command.

Defaults

By default, a trustpoint for Java object signing is set to none.

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
Webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.1(2)	This command was introduced.

Usage Guidelines

A trustpoint is a representation of a certificate authority (CA) or identity key pair. For the **java-trustpoint** command, the given trustpoint must contain the X.509 certificate of the application signing entity, the RSA private key corresponding to that certificate, and a certificate authority chain extending up to a root CA. This is typically achieved by using the **crypto ca import** command to import a PKCS12 formatted bundle. You can obtain a PKCS12 bundle from a trusted CA authority or you can manually create one from an existing X.509 certificate and an RSA private key using open source tools such as openssl.

Note An uploaded certificate cannot be used to sign Java objects that are embedded with packages (for example, the CSD package).

Examples

The following example first configures a new trustpoint, then configures it for WebVPN Java object signing:

```
hostname(config)# crypto ca import mytrustpoint pkcs12 mypassphrase
Enter the base 64 encoded PKCS12.
End with the word "quit" on a line by itself.
[ PKCS12 data omitted ]
```

```
quit
INFO: Import PKCS12 operation completed successfully.
hostname(config)#
```

The following example configures the new trustpoint for signing WebVPN Java objects:

```
hostname(config)# webvpn
hostname(config)# java-trustpoint mytrustpoint
hostname(config)#
```

Related Commands

Command	Description
crypto ca import	Imports the certificate and key pair for a trustpoint using PKCS12 data.

join-failover-group

To assign a context to a failover group, use the **join-failover-group** command in context configuration mode. To restore the default setting, use the **no** form of this command.

join-failover-group *group_num*

no join-failover-group *group_num*

Syntax Description

group_num	Specifies the failover group number.

Defaults

Failover group 1.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The admin context is always assigned to failover group 1. You can use the **show context detail** command to display the failover group and context association.

Before you can assign a context to a failover group, you must create the failover group with the **failover group** command in the system context. Enter this command on the unit where the context is in the active state. By default, unassigned contexts are members of failover group 1, so if the context had not been previously assigned to a failover group, you should enter this command on the unit that has failover group 1 in the active state.

You must remove all contexts from a failover group, using the **no join-failover-group** command, before you can remove a failover group from the system.

Examples

The following example assigns a context named ctx1 to failover group 2:

```
hostname(config)# context ctx1
hostname(config-context)# join-failover-group 2
hostname(config-context)# exit
```

Related Commands

Command	Description
context	Enters context configuration mode for the specified context.
failover group	Defines a failover group for Active/Active failover.
show context detail	Displays context detail information, including name, class, interfaces, failover group association, and configuration file URL.

jumbo-frame reservation

To enable jumbo frames for supported models, use the **jumbo-frame reservation** command in global configuration mode. To disable jumbo frames, use the **no** form of this command.

Note Changes in this setting require you to reboot the ASA.

jumbo-frame reservation

no jumbo-frame reservation

Syntax Description

This command has no arguments or keywords.

Defaults

Jumbo frame reservation is disabled by default.

Jumbo frames are supported by default on the ASASM; you do not need to use this command.

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
8.1(1)	This command was introduced for the ASA 5580.
8.2(5)/8.4(1)	We added support for the ASA 5585-X.
8.6(1)	We added support for the ASA 5512-X through ASA 5555-X.

Usage Guidelines

A jumbo frame is an Ethernet packet larger than the standard maximum of 1518 bytes (including Layer 2 header and FCS), up to 9216 bytes. Jumbo frame support requires extra memory, which might limit the maximum use of other features, such as access lists.

Jumbo frames are not supported on the Management *n*/*n* interface.

Be sure to set the MTU for each interface that needs to transmit jumbo frames to a higher value than the default 1500; for example, set the value to 9000 using the **mtu** command. For the ASASM, you do not need to set the **jumbo-frame** reservation command; it supports jumbo frames by default. Just set the MTU to the desired value.

Also, be sure to configure the MSS (maximum segment size) value for TCP when using jumbo frames. The MSS should be 120 bytes less than the MTU. For example, if you configure the MTU to be 9000, then the MSS should be configured to 8880. You can configure the MSS with the **sysopt connection tcpmss** command.

Both the primary and the secondary units require a reboot so that the failover pair supports jumbo frames. To avoid downtime, do the following:

- Issue the command on the active unit.
- Save the running configuration on the active unit.
- Reboot the primary and secondary units, one at a time.

Examples

The following example enables jumbo frame reservation, saves the configuration, and reloads the ASA:

```
hostname(config)# jumbo-frame reservation
WARNING: this command will take effect after the running-config is saved
and the system has been rebooted. Command accepted.

hostname(config)# write memory
Building configuration...
Cryptochecksum: 718e3706 4edb11ea 69af58d0 0a6b7cb5

70291 bytes copied in 3.710 secs (23430 bytes/sec)
[OK]
hostname(config)# reload
Proceed with reload? [confirm] Y
```

Related Commands

Command	Description
mtu	Specifies the maximum transmission unit for an interface.
show jumbo-frame reservation	Shows the current configuration of the **jumbo-frame reservation** command.

kcd-server

To allow the ASA to join an Active Directory domain, use the **kcd-server** command in webvpn configuration mode. To remove the specified behavior for the ASA, use the **no** form of this command.

kcd-server *aaa-server-group_name* **user** *username* **password** *password*

no kcd-server

Syntax Description

user	Specifies the Active Directory user with service level privileges.
password	Specifies the password for the specified user.

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**
Webvpn configuration	•	—	•	—	—

Command History

Release	Modification
8.4(1)	This command was introduced.

Usage Guidelines

Use the **kcd-server** command in webvpn configuration mode to allow the ASA to join an Active Directory domain. The domain controller name and realm are specified in the **aaa-server-groupname** command. The AAA server group has to be a Kerberos server type. The **username** and **password** options do not correspond to a user with Administrator privileges, but they should correspond to a user with service-level privileges on the domain controller. The success or failure status is displayed as the result of this command. The result can also be viewed using the **show webvpn kcd** command.

Kerberos Constrained Delegation, or KCD, in the ASA environment provides WebVPN users Single Sign-on (SSO) access to all web services that are protected by Kerberos. The ASA maintains a credential on behalf of the user (a service ticket) and uses this ticket to authenticate the user to the services.

In order for the **kcd-server** command to function, the ASA must establish a trust relationship between the *source* domain (the domain where the ASA resides) and the *target* or *resource* domain (the domain where the web services reside). The ASA, using its unique format, crosses the certification path from the source to the destination domain and acquires the necessary tickets on behalf of the remote access user to access the services.

This path is called cross-realm authentication. During each phase of cross-realm authentication, the ASA relies on the credentials at a particular domain and the trust relationship with the subsequent domain.

To configure the ASA for cross-realm authentication, you must use the following commands to join the Active Directory domain: **ntp**, **hostname**, **dns domain-lookup, dns server-group**.

Examples

The following example shows the usage of the **kcd-server** command:

```
hostname(config)# aaa-server kcd-grp protocol kerberos
hostname(config-aaa-server-group)# aaa-server kcd-grp host DC
hostname(config-aaa-server-group)# kerberos-realm EXAMPLE.COM
hostname(config)# webvpn
hostname(config-webvpn)# kcd-server kcd-grp user Administrator password Cisco123
hostname(config-aaa-server-group)# exit
hostname(config)#
```

The following is a configuration example of cross-realm authentication, where the Domain Controller is 10.1.1.10 (reachable via inside interface) and the domain name is PRIVATE.NET. Additionally, the Service Account username and password on the domain controller is dcuser and dcuser123! .

```
hostname(config)# config t

-----Create an alias for the Domain Controller-------------

hostname(config)# name 10.1.1.10 DC

----Configure the Name server-----------------------------

hostname(config)# ntp server DC

----Enable a DNS lookup by configuring the DNS server and Domain name --------------

hostname(config)# dns domain-lookup inside
hostname(config)# dns server-group DefaultDNS
hostname(config-dns-server-group)# name-server DC
hostname(config-dns-server-group)# domain-name private.net

----Configure the AAA server group with Server and Realm-------------------------------

hostname(config)# aaa-server KerberosGroup protocol Kerberos
hostname(config-asa-server-group)# aaa-server KerberosGroup (inside) host DC
hostname(config-asa-server-group)# Kerberos-realm PRIVATE.NET

----Configure the Domain Join-----------------------------

hostname(config)# webvpn
hostname(config-webvpn)# kcd-server KerberosGroup username dcuser password dcuser123!
hostname(config)#
```

Related Commands

Command	Description
aaa-server	Enters aaa-server configuration mode, so you can configure AAA server parameters.
aaa-server host	Enters aaa-server host configuration mode, so you can configure AAA server parameters that are host-specific.
clear configure aaa-server	Removes all AAA command statements from the configuration.
dns	Specifies the Domain Name Server.
domain-name	Specifies the domain name of the server.

hostname	Specifies the hostname.
ntp	Specifies the transfer protocol.
show aaa-kerberos	Displays server statistics for all AAA Kerberos servers.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol.

keepout

To present an administrator-defined message rather than a login page for new user sessions (when the ASA undergoes a maintenance or troubleshooting period), use the **keepout** command in webvpn configuration mode. To remove a previously set keepout page, use the **no** version of the command.

keepout

no keepout *string*

Syntax Description

string	An alphanumeric string in double quotation marks.

Defaults

No keepout page.

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
Webvpn configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

When this command is enabled, the clientless WebVPN portal page becomes unavailable. You receive an administrator-defined message stating the unavailability of the portal rather than a login page for the portal. Use the **keepout** command to disable clientless access, but still allow AnyConnect access. You can also use this command to indicate portal unavailability when maintenance is occurring.

Examples

The following example shows how to configure a keepout page:

```
hostname(config)# webvpn
hostname(config-webvpn)# keepout "The system is unavailable until 7:00 a.m. EST."
hostname(config-webvpn)#
```

Related Commands

Command	Description
webvpn	Enters webvpn configuration mode, which lets you configure attributes for clientless SSL VPN connections.

kerberos-realm

To specify the realm name for this Kerberos server, use the **kerberos-realm** command in aaa-server host configuration mode. To remove the realm name, use the **no** form of this command:

kerberos-realm *string*

no kerberos-realm

Syntax Description

string	A case-sensitive, alphanumeric string, up to 64 characters long. Spaces are not permitted in the string. **Note** Kerberos realm names use numbers and upper case letters only. Although the ASA accepts lower case letters in the *string* argument, it does not translate lower case letters to upper case letters. Be sure to use upper case letters only.

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
Aaa-server host configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command is valid only for Kerberos servers.

The value of the *string* argument should match the output of the Microsoft Windows **set USERDNSDOMAIN** command when it is run on the Windows 2000 Active Directory server for the Kerberos realm. In the following example, EXAMPLE.COM is the Kerberos realm name:

```
C:\>set USERDNSDOMAIN
USERDNSDOMAIN=EXAMPLE.COM
```

The *string* argument must use numbers and upper case letters only. The **kerberos-realm** command is case sensitive, and the ASA does not translate lower case letters to upper case letters.

Examples

The following sequence shows the **kerberos-realm** command to set the kerberos realm to "EXAMPLE.COM" in the context of configuring a AAA server host:

```
hostname(config)# aaa-server svrgrp1 protocol kerberos
```

```
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# kerberos-realm EXAMPLE.COM
hostname(config-aaa-server-host)# exit
hostname(config)#
```

Related Commands

Command	Description
aaa-server host	Enter AAA server host configuration submode so you can configure AAA server parameters that are host-specific.
clear configure aaa-server	Remove all AAA command statements from the configuration.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol.

key (aaa-server host)

To specify the server secret value used to authenticate the NAS to the AAA server, use the **key** command in aaa-server host configuration mode. The aaa-server host configuration mode is accessibile from aaa-server protocol configuration mode. To remove the key, use the **no** form of this command.

key *key*

no key

Syntax Description

key	An alphanumeric keyword, which can be up to 127 characters long.

Defaults

No default behaviors 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
Aaa-server host configurationj	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The *key* value is a case-sensitive, alphanumeric keyword of up to 127 characters, which is the same value as the key on the TACACS+ server. Any characters over 127 are ignored. The key is used between the client and the server for encrypting data between them. The key must be the same on both the client and server systems.The key cannot contain spaces, but other special characters are allowed. The key (server secret) value authenticates the ASA to the AAA server.

This command is valid only for RADIUS and TACACS+ servers.

Examples

The following example configures a TACACS+ AAA server named “srvgrp1” on host “1.2.3.4,” sets a timeout of 9 seconds, sets a retry-interval of 7 seconds, and configures the key as “myexclusivemumblekey.”

```
hostname(config)# aaa-server svrgrp1 protocol tacacs+
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# key myexclusivemumblekey
```

Related Commands

Command	Description
aaa-server host	Enters aaa-server host configuration mode, so that you can configure host-specific AAA server parameters.
clear configure aaa-server	Removes all AAA command statements from the configuration.
show running-config aaa-server	Displays the AAA server configuration.

key (cluster group)

To set an authentication key for control traffic on the cluster control link, use the **key** command in ckuster group configuration mode. To remove the key, use the **no** form of this command.

key *shared_secret*

no key [*shared_secret*]

Syntax Description

shared_secret	Sets the shared secret to an ASCII string from 1 to 63 characters. The shared secret is used to generate the key.

Command Default

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
9.0(1)	We introduced this command.

Usage Guidelines

This command does not affect datapath traffic, including connection state update and forwarded packets, which are always sent in the clear.

Examples

The following example sets a shared secret:

```
hostname(config)# cluster group cluster1
hostname(cfg-cluster)# key chuntheunavoidable
```

Related Commands

Command	Description
clacp system-mac	When using spanned EtherChannels, the ASA uses cLACP to negotiate the EtherChannel with the neighbor switch.
cluster group	Names the cluster and enters cluster configuration mode.
cluster-interface	Specifies the cluster control link interface.
cluster interface-mode	Sets the cluster interface mode.
conn-rebalance	Enables connection rebalancing.

Command	Description
console-replicate	Enables console replication from slave units to the master unit.
enable (cluster group)	Enables clustering.
health-check	Enables the cluster health check feature, which includes unit health monitoring and interface health monitoring.
local-unit	Names the cluster member.
mtu cluster-interface	Specifies the maximum transmission unit for the cluster control link interface.
priority (cluster group)	Sets the priority of this unit for master unit elections.

key config-key password-encryption

To set the passphrase used for generation the encryption key, use the **key config-key password-encryption** command in global configuration mode. To decrypt passwords encrypted with the pass phrase, use the **no** form of this command.

key config-key password-encryption [*new pass phrase* [*old pass phrase*]]

no key config-key password-encryption [*current pass phrase*]

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
Global configuration	•	•	•	—	•

Command History

Release	Modification
8.3(1)	This command was introduced.

Usage Guidelines

When this command is enabled it sets the passphrase used for generation the encryption key. If the pass phrase is configured for the first time, then you will not need to enter the current password. Otherwise, you must enter the current password. The new passphrase must be between 8 and 128 character long. All characters except the back space and double quote will be accepted for the passphrase.

The **write erase** command when followed by the **reload** command will remove the master passphrase if it is lost.

Examples

The following example sets the passphrase used for generating the encryption key:

```
hostname(config)# key config-key password-encryption
```

Related Commands

Command	Description
password encryption aes	Enables password encryption.
write erase	Removes the master passphrase if it is lost when followed by the **reload** command.

keypair

To specify the key pair whose public key is to be certified, use the **keypair** command in crypto ca trustpoint configuration mode. To restore the default setting, use the **no** form of the command.

keypair *name*

no keypair

Syntax Description

name	Specify the name of the key pair.

Defaults

The default setting is not to include the key pair.

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
Crypto ca trustpoint configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example enters crypto ca trustpoint configuration mode for the trustpoint central, and specifies a key pair to be certified for the trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# keypair exchange
```

Related Commands

Command	Description
crypto ca trustpoint	Enters crypto ca trustpoint configuration mode.
crypto key generate dsa	Generates DSA keys.
crypto key generate rsa	Generates RSA keys.
default enrollment	Returns enrollment parameters to their defaults.

keysize

To specify the size of the public and private keys generated by the local Certificate Authority (CA) server at user certificate enrollment, use the **keysize** command in ca-server configuration mode. To reset the keysize to the default length of 1024 bits, use the **no** form of this command.

keysize {**512** | **768** | **1024** | **2048**}

no keysize

Syntax Description

512	Specifies a size of 512 bits for the public and private keys generated at certificate enrollment.
768	Specifies a size of 768 bits for the public and private keys generated at certificate enrollment.
1024	Specifies a size of 1024 bits for the public and private keys generated at certificate enrollment.
2048	Specifies a size of 2048 bits for the public and private keys generated at certificate enrollment.

Defaults

By default, each key in the key pair is 1024 bits long.

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.

Examples

The following example specifies a key size of 2048 bits for all public and private key pairs generated for users by the local CA server:

```
hostname(config)# crypto ca server
hostname(config-ca-server))# keysize 2048
hostname(config-ca-server)#
```

The following example resets the key size to the default length of 1024 bits for all public and private key pairs generated for users by the local CA server:

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

Related Commands

Command	Description
crypto ca server	Provides access to the ca-server configuration mode command set, which allows you to configure and manage the local CA.
issuer-name	Specifies the subject name DN of the certificate authority certificate.
subject-name-default	Specifies a generic subject name DN to be used along with the username in all user certificates issued by a CA server.

keysize server

To specify the size of the public and private keys generated by the local Certificate Authority (CA) server for configuring the size of the CA keypair, use the **keysize server** command in ca-server configuration mode. To reset the keysize to the default length of 1024 bits, use the **no** form of this command.

keysize server{**512** | **768** | **1024** | **2048**}

no keysize server

Syntax Description

512	Specifies a size of 512 bits for the public and private keys generated at certificate enrollment.
768	Specifies a size of 768 bits for the public and private keys generated at certificate enrollment.
1024	Specifies a size of 1024 bits for the public and private keys generated at certificate enrollment.
2048	Specifies a size of 2048 bits for the public and private keys generated at certificate enrollment.

Defaults

By default, each key in the key pair is 1024 bits long.

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.

Examples

The following example specifies a key size of 2048 bits for the CA certificate:

```
hostname(config)# crypto ca server
hostname(config-ca-server))# keysize server 2048
hostname(config-ca-server)#
```

The following example resets the key size to the default length of 1024 bits for the CA certificate:

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

Related Commands

Command	Description
crypto ca server	Provides access to the ca-server configuration mode command set, which allows you to configure and manage the local CA.
issuer-name	Specifies the subject name DN of the certificate authority certificate.
keysize	Specifies the key pair size for the user certificate.
subject-name-default	Specifies a generic subject name DN to be used along with the username in all user certificates issued by a CA server.

kill

To terminate a Telnet session, use the **kill** command in privileged EXEC mode.

kill *telnet_id*

Syntax Description

telnet_id	Specifies the Telnet session ID.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **kill** command lets you terminate a Telnet session. Use the **who** command to see the Telnet session ID. When you kill a Telnet session, the ASA lets any active commands terminate and then drops the connection without warning.

Examples

The following example shows how to terminate a Telnet session with the ID "2". First, the **who** command is entered to display the list of active Telnet sessions. Then the **kill 2** command is entered to terminate the Telnet session with the ID "2".

```
hostname# who
2: From 10.10.54.0

hostname# kill 2
```

Related Commands

Command	Description
telnet	Configures Telnet access to the ASA.
who	Displays a list of active Telnet sessions.