CHAPTER 17

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.

Examples

This following example first configures a new trustpoint and then configures it for WebVPN Java object signing. The following command creates a new trustpoint called my mytrustpoint:

```
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:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	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.

keepout

To present a keepout webpage rather than a login page for new user sessions when the security appliance 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 mode	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the keepout command to communicate unavailability of the security appliance.

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 SSLVPN 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 security appliance 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)	Introduced in this release.

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 security appliance 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

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, 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	•	•	•	•	—

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 that is the same value as the key on the TACACS+ server. Any characters entered past 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 security appliance to the AAA server.

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

The **key** parameter of the **aaa-server** command in earlier PIX firewall versions is automatically converted to the equivalent **key** command.

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 you can configure AAA server parameters that are host-specific.
clear configure aaa-server	Removes all AAA command statements from the configuration.
show running-config aaa-server	Displays AAA server configuration.

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	This command was introduced.

Examples

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

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

Related Commands

Command	Description
crypto ca trustpoint	Enters 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, the 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 CA Server Configuration mode CLI 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 configure the size of the CAs own 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, the 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 CAs own 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 CAs own 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 CA Server Configuration mode CLI 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:

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

Command History

Release	Modification
Preexisting	This command was preexisting.

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 security appliance 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 security appliance.
who	Displays a list of active Telnet sessions.