



## join-failover-group through kill Commands

---

# 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

<i>group_num</i>	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		
	Routed	Transparent	Single	Multiple	
				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
<b>context</b>	Enters context configuration mode for the specified context.
<b>failover group</b>	Defines a failover group for Active/Active failover.
<b>show context detail</b>	Displays context detail information, including name, class, interfaces, failover group association, and configuration file URL.

# 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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				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**

<b>Command</b>	<b>Description</b>
<b>aaa-server host</b>	Enter AAA server host configuration submode so you can configure AAA server parameters that are host-specific.
<b>clear configure aaa-server</b>	Remove all AAA command statements from the configuration.
<b>show running-config aaa-server</b>	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 mode. Aaa-server host configuration mode is accessible from aaa-server protocol configuration mode. To remove the key, use the **no** form of this command. The key (server secret) value authenticates the security appliance to the AAA server.

**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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				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.

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 “svrgrp1” 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
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>aaa-server host</b>	Enters AAA server host configuration mode so you can configure AAA server parameters that are host-specific.
	<b>clear configure aaa-server</b>	Removes all AAA command statements from the configuration.
	<b>show running-config aaa-server</b>	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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				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 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
<a href="#">crypto ca trustpoint</a>	Enters trustpoint configuration mode.
<a href="#">crypto key generate dsa</a>	Generates DSA keys.
<a href="#">crypto key generate rsa</a>	Generates RSA keys.
<a href="#">default enrollment</a>	Returns enrollment parameters to their defaults.

# kill

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

```
kill telnet_id
```

<b>Syntax Description</b>	<i>telnet_id</i> Specifies the Telnet session ID.
---------------------------	---

<b>Defaults</b>	No default behaviors or values.
-----------------	---------------------------------

<b>Command Modes</b>	The following table shows the modes in which you can enter the command:
----------------------	---

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Preexisting	This command was preexisting.

<b>Usage Guidelines</b>	The <b>kill</b> command lets you terminate a Telnet session. Use the <b>who</b> 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.
-------------------------	--

<b>Examples</b>	The following example shows how to terminate a Telnet session with the ID “2”. First, the <b>who</b> command is entered to display the list of active Telnet sessions. Then the <b>kill 2</b> command is entered to terminate the Telnet session with the ID “2”.
-----------------	---

```
hostname# who
2: From 10.10.54.0

hostname# kill 2
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">telnet</a>	Configures Telnet access to the security appliance.
	<a href="#">who</a>	Displays a list of active Telnet sessions.

