

K Commands

- keepalive, on page 2
- kernel core, on page 3
- key, on page 5
- key (sa configuration submode), on page 7
- key-ontape, on page 8

keepalive

To configure the message keepalive interval for the IKE protocol, use the **keepalive** command in IKE configuration submode. To revert to the default, use the **no** form of the command.

keepalive *seconds*
no keepalive *seconds*

Syntax Description

seconds	Specifies the number of seconds for the keepalive interval. The range is 120 to 86400.

Command Default

3600 seconds or 1 hour.

Command Modes

IKE configuration submode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

The keepalive interface only applies to IKE version 2 tunnels.

To use this command, the IKE protocol must be enabled using the **crypto ike enable** command.

Examples

The following example shows how to configure the keepalive interval:

```
switch# config terminal
switch(config)# crypto ike domain ipsec
switch(config-ike-ipsec)# keepalive 7200
```

Related Commands

Command	Description
crypto ike domain ipsec	Enters IKE configuration mode.
crypto ike enable	Enables the IKE protocol.
show crypto ike domain ipsec	Displays IKE information for the IPsec domain.

kernel core

Use the **kernel core** command to generate a core dump for each module. Use the **no** form of this command to negate the command or revert to its factory

kernelcore {**limit***number* | **module***slot* {**force** | **level** {**all** | **header** | **kernel** | **ram** | **used-ram**} | **target***ipaddress*}}
nokernelcore {**limit***number* | **module***slot* {**force** | **level** {**all** | **header** | **kernel** | **ram** | **used-ram**} | **target***ipaddress*}}

Syntax Description

limit *number*	Limits the number of modules for which the core is generated. The range is 1 to 6.
module *slot*	Configures the module requiring the core generation.
force	Forces a module to dump kernel core.
level	Specifies the core dump level for the selected module.
all	Dumps all the memory (requires 1G of space)
header	Dumps kernel header only.
kernel	Dumps all kernel memory pages.
ram	Dumps all the RAM pages.
used-ram	Dumps all the used RAM pages.
target *ipaddress*	Configures the external server IP address on the same physical LAN.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Core dumps performed on the supervisor module can lead to packet loss, even in a dual supervisor configuration.

Examples

The following example limits core generation to two modules:

```
switch(config)# kernel core limit 2
succeeded
```

The following example configures module 5 to generate cores:

```
switch(config)# kernel core module 5
succeeded
```

The following example configures module 5 to generate only header-level cores:

```
switch(config)# kernel core module 5 level header
succeeded
```

The following example configures the external server:

```
switch(config)# kernel core target 10.50.5.5
succeeded
```

Related Commands

Command	Description
show kernel	Displays configured kernel core settings.
show running-config	Displays all switch configurations saved to PSS.

key

To configure the preshared key for the IKE protocol, use the **key** command in IKE configuration submode. To revert to the default, use the **no** form of the command.

key **key-id** { **address** **ip-address** | **hostname** **name** }
no **key** **key-id** { **address** **ip-address** | **hostname** **name** }

Syntax Description

key-id	Specifies the ID for the preshared key. The maximum length is 128 characters.
address *ip-address*	Specifies the peer IP address. The format is *A* . *B* . *C* . *D* .
hostname *name*	Specifies the peer host name. The maximum length is 128 characters.

Command Default

None.

Command Modes

IKE configuration submode.

Command History

Release	Modification
2.0(x)	This command was introduced.
3.0(1)	Added the **hostname** keyword.

Usage Guidelines

To use this command, the IKE protocol must be enabled using the **crypto ike enable** command.

Note The **key** command supports only the IPv4 format for IP address.

Examples

The following example shows how to configure the key:

```
switch# config terminal
switch(config)# crypto ike domain ipsec
switch(config-ike-ipsec)# key ctct address 209.165.200.226
```

The following example shows how to delete the configured key:

```
switch(config-ike-ipsec)# no key ctct address 209.165.200.226
```

The following example shows how to set the preshared key for the specified peer:

```
switch(config-ike-ipsec)# key sample hostname node1
```

The following example shows how to delete the preshared key for the specified peer:

```
switch(config-ike-ipsec)# no key sample hostname node1
```

Related Commands

Command	Description
crypto ike domain ipsec	Enters IKE configuration mode.
crypto ike enable	Enables the IKE protocol.
show crypto ike domain ipsec	Displays IKE information for the IPsec domain.

key (sa configuration submode)

To configure the key for the current Security Association[SA], use the key command. To delete the key from the current SA, use the no form of the command.

key *key*
no key *key*

Syntax Description

key	Specifies the key for encryption as a 16-byte hexadecimal string. The maximum size of the string is 34.

Command Default

None.

Command Modes

Configuration submode.

Command History

Release	Modification
NX-OS 4.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure the key for the current SA:

```
 switch# config t
switch(config)# fcsp esp sa 257
This is a Early Field Trial (EFT) feature.  Please do not use this in a producti
on environment. Continue Y/N ? [no] y
switch(config-sa)# key 0x1234
switch(config-sa)#
```

Related Commands

Command	Description
fcsp enable	Enables FC-SP.
show fcsp interface	Displays FC-SP-related information for a specific interface.

key-ontape

To configure keys on the tape mode and store the encrypted security keys on the backup tapes, use the key-ontape command. To disable this feature, use the no form of the command.

key-ontape
no key-ontape

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Cisco SME cluster configuration submode.

Command History

Release	Modification
3.2(2)	This command was introduced.

Usage Guidelines

This command allows the encrypted security keys to be stored on the backup tapes.

Note This feature is supported only for unique keys.

Before using this command, automatic volume grouping should be disabled by using the auto-volgrp command.

Examples

The following example enables the key-ontape feature:

```
switch# config terminal
switch(config)# sme cluster clustername1
switch(config-sme-cl)# key-ontape
```

The following example disables the key-ontape feature:

```
switch# config terminal
switch(config)# sme cluster clustername1
switch(config-sme0-cl)# no key-ontape
```

Related Commands

Command	Description
no shared-key	Specifies unique key mode.
no auto-volgrp	Disables automatic volume grouping.
show sme cluster key	Displays information about cluster key database.
show sme cluster tape	Displays information about tapes.