

KeySecure
Command Line Interface
Version 6.2.0

Reference Guide



Software Version: 6.2.0
Documentation Version: 20121030
Part Number: 007-012125-001

© 2012 SafeNet, Inc. All rights reserved

Preface

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording or otherwise without the prior written permission of SafeNet.

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address below.

4690 Millennium Drive
Belcamp, Maryland 21017
USA

Disclaimers

The foregoing integration was performed and tested only with specific versions of equipment and software and only in the configuration indicated. If your setup matches exactly, you should expect no trouble, and Customer Support can assist with any missteps. If your setup differs, then the foregoing is merely a template and you will need to adjust the instructions to fit your situation. Customer Support will attempt to assist, but cannot guarantee success in setups that we have not tested.

This product contains software that is subject to various public licenses. The source code form of such software and all derivative forms thereof can be copied from the following website: <http://c3.safenet-inc.com/>

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

Technical Support

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, please contact your supplier or SafeNet support.

SafeNet support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Technical Support Contact Information:

Phone: 800-545-6608, 410-931-7520
Email: support@safenet-inc.com

Table of Contents

CHAPTER 1	OVERVIEW OF THE COMMAND LINE INTERFACE	3
CHAPTER 2	ADMINISTRATOR CONFIGURATION	7
CHAPTER 3	AUTO-LOGOUT	18
CHAPTER 4	BACKUP & RESTORE	19
CHAPTER 5	CERTIFICATE CONFIGURATION	22
CHAPTER 6	CERTIFICATE AUTHORITY CONFIGURATION	28
CHAPTER 7	CERTIFICATE REVOCATION LIST CONFIGURATION	41
CHAPTER 8	CLUSTER CONFIGURATION	45
CHAPTER 9	DATE & TIME CONFIGURATION	46
CHAPTER 10	HEALTH CHECK CONFIGURATION	49
CHAPTER 11	HELP	50
CHAPTER 12	HISTORY	52
CHAPTER 13	HSM CONFIGURATION	53
CHAPTER 14	LOG CONFIGURATION	59
CHAPTER 15	LOG VIEWING & ROTATION CONFIGURATION	72
CHAPTER 16	SERVER CONFIGURATION	82
CHAPTER 17	NETWORK CONFIGURATION	83
CHAPTER 18	NETWORK DIAGNOSTICS	98
CHAPTER 19	SNMP CONFIGURATION	100

CHAPTER 20	SSKM CONFIGURATION	106
CHAPTER 21	SSL CONFIGURATION	110
CHAPTER 22	SECURITY CONFIGURATION	115
CHAPTER 23	SERVICES	119
CHAPTER 24	STATISTICS CONFIGURATION	121
CHAPTER 25	SYSTEM HEALTH	124
CHAPTER 26	SYSTEM INFORMATION & UPGRADE	126

Chapter 1

Overview of the Command Line Interface

The KeySecure's command line interface (CLI) enables you to perform administrative functions either at the KeySecure's serial console or remotely using SSH on tcp port 22. Only administrator accounts with the Admin Access via SSH access control can use the CLI. Administrator access controls are set on the Administrator Configuration

The serial console must use a terminal emulation program such as HyperTerminal. Remote CLI administration requires a terminal emulation program that supports SSH (PuTTY, Teraterm, or SecureCRT, for example). The SSH client should connect to the IP address defined in the first-time initialization process.

CLI Keyboard Shortcuts

The CLI supports a few standard linux shell commands that allow you to perform search, cut and paste operations.

- Ctrl-C - cancel the current command.
- Ctrl-R - search backward through the command history. Type Ctrl-R to retrieve the search prompt. Type the first few letters of a command and press Ctrl-R repeatedly to search through the previously executed commands that match those letters.
- Ctrl-K - delete the text from the cursor to the end of the line.
- Ctrl-U - erase the entire line.
- Ctrl-Y - pastes text erased by Ctrl-K or Ctrl-U.
- Ctrl-P - move backwards through the command history.

Use quotes when passing an argument that will contain spaces. For example, to create a certificate request called `another request`, do the following:

```
certificate request "another request"
```

You can also use single quotes:

```
certificate request 'another request'
```

The **tab completion** feature allows you to type part of a command and use the tab key to fill in the remainder of the word. If the command is unambiguous, the CLI will fill in the rest of the command up until the next point of ambiguity or to the end of the current word.

For example, type `sh` and TAB and the CLI will complete the word `show`, as this is the only possible ending to that word.

Type `tim` and TAB and the CLI will complete the word `timezone`. Type TAB again and the CLI will complete the word `set`.

Because the majority of commands include multiple words, you will most likely type the beginning of one word, press tab to complete the word, start another word, and press tab again. Tab completion is available as long as the CLI knows you can only be referring to one word or command.

If the text you have entered can refer to multiple commands, tab completion will not work, but you can press the return key to view the possible commands.

For example, type `show sys` and then RETURN and the CLI will display the commands that begin with `show sys`: `show system health`, `show system log`, `show system syslog`.

To search for a command without executing it, type the command, or part of the command, and include a question mark (?). The CLI will display the commands that match the pattern you typed.

For example, type `sh au l ?` on the command line and the CLI displays `show audit log` and `show audit log signing`.

Type `system l ?` and the CLI indicates that `system log rotate` is the only command that can be called by `system l`.

Note: Include a space before the question mark. Otherwise, the CLI interprets the punctuation as part of the command, and returns an error.

View Mode

This is the default mode. It allows viewing of current configuration and system status; you cannot write to the system. View mode requires secure shell (SSH) administration privilege.

The view mode prompt is the hostname of the KeySecure followed by #:

```
hostname#
```

Configure Mode

Configure mode allows both viewing and configuration. The system is in configure mode when the following prompt is displayed on the screen:

```
hostname (config)#
```

To enter config mode, type `config`:

```
hostname# config  
hostname (config)#
```

To exit config mode and return to view mode, type `exit`:

```
hostname (config)# exit  
hostname#
```

Script Mode

Script mode allows you to create and run scripts containing view and/or configure mode CLI commands. To enter script mode, you must first enter configure mode, then type `script`.

```
hostname# config
hostname (config)# script
hostname (script)#
```

The system is in script mode when the following prompt is displayed:

```
hostname (script)#
```

To exit script mode and return to configure mode, type `exit`:

```
hostname (script)# exit
hostname (config)#
```

Creating Scripts

There are essentially two different ways to create CLI scripts: manually or via the Script Recorder.

Manual Creation

This is done using the command `create script <script name>`, as shown here:

```
hostname (script)# create script testscript
```

Perform the following actions to create the script:

- 1 Type OR Paste the script immediately after the question mark.
- 2 Press **Return** twice when you have finished.

After you type the command, you are presented with the above directions. You can either enter your script line by line or create it using another editor and just paste it after the question mark. Note that when you manually create scripts, you must format the script file correctly. For example, when scripting an interactive command (i.e. one that asks for input), the command often prompts the user multiple times to enter input. You must ensure that each response to a prompt for input is entered on a separate line in the script file.

Note: The Script Recorder takes care of all such formatting issues and hence is probably the best way to create scripts initially.

Script Recorder

The Script Recorder is started by typing in the command `record <script name>` as shown here:

```
hostname(script)# record testscript
Recording to script testscript.
```

You can then type any view or configure mode CLI commands and they will automatically be written to the script specified in the correct format.

To stop the Script Recorder, type `no record` as show here:

```
hostname(script)# no record  
Recording successfully stopped.
```

Executing Scripts

To execute a script, you must first load it using the command `load <script name>`, as shown here:

```
hostname(script)# load testscript  
Script testscript successfully loaded.
```

Once loaded, a script can either be stepped through (executed one line at a time), or the entire script can be run. To step through a script, use the command `step`, as shown here:

```
hostname(script)# step
```

To run the entire script, use the command `go`, as shown here:

```
hostname(script)# go
```

Displaying and Deleting Scripts

To display the current scripts that have been created on the system, use the command `show script`. To display the contents of a specified script, use the command `show script <script name>`, as shown here:

```
hostname(script)# show script testscript
```

If you want to delete an existing script, use the command `no script <script name>` as shown here:

```
hostname(script)# no script testscript
```

Installing Certificates

When you attempt to enter a command in a script that requires a certificate to be pasted in, the actual certificate will not be stored in the script. Instead, the script will prompt you when it is run to paste in the certificate.

Entering Passwords

Whenever a command that requires a password is executed in a script, the actual password will not be stored in the script. Instead, when the script is run, it will prompt you to enter the password.

Chapter 2

Administrator Configuration

Using the CLI, you can:

- view a list of all administrator accounts or view a specific account (`show administrator`)
- view and configure ldap server settings (`show ldap server administrators`, `ldap server administrator`, `no ldap server administrator`, `ldap test administrator`)
- view and configure password settings (`show password settings`, `password settings`)
- display and configure the multiple credentials settings (`show credential settings`, `credential settings`)
- grant credentials, view granted credentials, and cancel grants (`grant credential`, `show granted credential`, `no granted credential`)
- view and edit remote administration settings (`show ras settings`, `edit ras settings`)
- create, edit, and delete administrator accounts (`administrator`, `edit administrator`, `no administrator`)
- change passwords (`passwd`)
- recreate the ssh key (`recreate ssh key`)
- recreate the webadmin cert (`reissue webadmin certificate`).

administrator - create a new local or LDAP administrator on the system

Syntax: **administrator** <username>

For example:

```
DemoBox (config)# administrator admin2
Administrator Type:
  1. Local
  2. LDAP
Enter a number (1 - 2) [1]: 1
Full Name: administrator 2
Description: administrator 2
Password:
Confirm Password:
High Access Administrator (y/n) [n]: y

Access Control - Security Configuration
  Keys and Authorization Policies (y/n) [n]: y
  Users and Groups (y/n) [n]: y
  Certificates (y/n) [n]: y
  Certificate Authorities (y/n) [n]: y
```

```
Advanced Security (y/n) [n]: y
SSL (y/n) [n]: y
ProtectFile Manager (y/n) [n]: y
Access Control - Device Configuration
NAE Server (y/n) [n]: y
Cluster (y/n) [n]: y
Network and Date/Time (y/n) [n]: y
High Availability (y/n) [n]: y
SNMP (y/n) [n]: y
Logging (y/n) [n]: y
Access Control - Backup & Restore
Backup Configuration (y/n) [n]: y
Backup Keys & Certificates (y/n) [n]: y
Backup Local CAs (y/n) [n]: y
Restore Configuration (y/n) [n]: y
Restore Keys & Certificates (y/n) [n]: y
Restore Local CAs (y/n) [n]: y
Access Control - Maintenance
Services (y/n) [n]: y
Software Upgrade and System Health (y/n) [n]: y
Access Control - Administrative Access
Admin Access via Web (y/n) [n]: y
Admin Access via SSH (y/n) [n]: y
Warning: High access administrators may grant themselves other access rights
Administrator successfully added.
```

credential settings - establish the multiple credential settings

Syntax: **credential settings**

For example:

```
DemoBox (config)# credential settings
Require Multiple Credentials [n]: y
Num of Admins Required for Operations:
    1: 2
    2: 3
    3: 4
Enter a number (1 - 3) [1]: 2
Allow Time-Limited Credentials [n]: y
Maximum Duration for Credentials (minutes) [0]: 5
```

As a security precaution, approval from multiple administrators is required to commit the requested changes. These changes may adversely affect the functionality of this device.

```
Current Administrator: admin
Authorization is required from 2 additional administrators
Valid Administrators to choose from:
    admin2
```

admin3

```
Administrator: admin2
Administrator Password:
Authorization successfully granted by: admin2
```

```
Administrator: admin3
Administrator Password:
Authorization successfully granted by: admin3
```

Changed Multiple Credentials settings

edit administrator - modify settings for a specified administrator

The system prompts for all user access controls.

Syntax: **edit administrator <username>**

For example:

```
DemoBox (config)# edit administrator admin2
Username [admin2]:
Full Name [administrator 2]:
Description [administrator 2]:
Password [*****]:
High Access Administrator (y/n) [y]: n

Access Control - Security Configuration
  Keys and Authorization Policies (y/n) [y]: y
  Users and Groups (y/n) [y]: y
  Certificates (y/n) [y]: y
  Certificate Authorities (y/n) [y]: y
  Advanced Security (y/n) [y]: n
  SSL (y/n) [y]: n
  ProtectFile Manager (y/n) [y]: n

Access Control - Device Configuration
  NAE Server (y/n) [y]: n
  Cluster (y/n) [y]: n
  Network and Date/Time (y/n) [y]: n
  High Availability (y/n) [y]: n
  SNMP (y/n) [y]: n
  Logging (y/n) [y]: n

Access Control - Backup & Restore
  Backup Configuration (y/n) [y]: y
  Backup Keys & Certificates (y/n) [y]: y
  Backup Local CAs (y/n) [y]: y
  Restore Configuration (y/n) [y]: y
  Restore Keys & Certificates (y/n) [y]: y
  Restore Local CAs (y/n) [y]: y

Access Control - Maintenance
  Services (y/n) [y]: n
  Software Upgrade and System Health (y/n) [y]: n
```

Access Control - Administrative Access
Admin Access via Web (y/n) [y]: y
Admin Access via SSH (y/n) [y]: y
Administrator successfully modified.

edit ras settings - edit the Remote Administration Settings

If you make changes to the remote administration settings via secure shell, you will be logged out of your secure shell client after you have entered all the necessary information.

Syntax: **edit ras settings**

For example:

```
DemoBox (config)# edit ras settings
Available IP addresses:
  1. All
  2. 172.17.7.29
Web Admin Server IP (1-2)[1]:1
Web Admin Server Port [9443]: 9443
Web Admin Client Certificate Authentication (y/n) [n]: n
Available IP addresses:
  1. All
  2. 172.17.7.29
SSH Admin Server IP (1-2)[1]:1
SSH Admin Server Port [22]: 22
Successfully changed Remote Admin Settings.
nightly-7-29 (config)# Connection to 172.17.7.29 closed by remote host.
Connection to 172.17.7.29 closed.
```

grant credential - grant credentials to another administrator

The duration of the credential grant cannot be longer than the Maximum Duration for Credentials (specified in credential settings).

Syntax: **grant credential**

For example:

```
DemoBox (config)# grant credential
Grant to:
  1: admin2
  2: admin3
Enter a number (1 - 2) [1]: 1
Duration (minutes): 5
Allowed Operations:
  Add/Modify Keys [n]: n
  Delete Keys [n]: n
  Add/Modify Users & Groups [n]: y
  Delete Users & Groups [n]: y
  Modify Auth Policies [n]: y
```

Modify LDAP Server for Users & Groups [n]: y
Credential granted

ldap server administrators - display and configure LDAP administrator server settings for primary, schema, or failover servers

Syntax: **ldap server administrators** <primary | schema | failover>

For example:

```
DemoBox (config)# ldap server administrators primary
Hostname or IP Address [everest1.qa.ingrian.com]:
Port [389]: 389
Use SSL [n]: n
Trusted Certificate Authority:
    1: None
    2: Known: ProtectFile_PKI_CA
    3: Known: SSL-CA
    4: Local: Ingrian
Enter a number (1 - 4) [1]: 1
Timeout (sec) [3]: 3
Bind DN: cn=Administrator, cn=Users, dc=win, dc=qa, dc=ingrian, dc=com
Bind Password: *****
LDAP administrator server successfully saved.
```

ldap test administrators - connect to the failover or primary LDAP server and print connection debugging information

Requires config mode.

Syntax: **ldap test administrators** <primary | failover>

For example:

```
DemoBox (config)# ldap test administrators primary
Testing LDAP Administrator Directory Default
Primary Server
----- BEGIN TEST -----
ldap_create
ldap_url_parse_ext(ldap://volvo.qa.ingrian.com:389)
ldap_bind
ldap_simple_bind
ldap_sasl_bind
ldap_send_initial_request
ldap_new_connection 1 1 0
ldap_int_open_connection
ldap_connect_to_host: TCP volvo.qa.ingrian.com:389
ldap_new_socket: 25
ldap_prepare_socket: 25
ldap_connect_to_host: Trying 172.17.6.102:389
ldap_connect_timeout: fd: 25 tm: 3 async: 0
```

```
ldap_ndelay_on: 25
ldap_is_sock_ready: 25
ldap_ndelay_off: 25
ldap_open_defconn: successful
ldap_send_server_request
ldap_result ld 0x91694d0 msgid 1
ldap_chkResponseList ld 0x91694d0 msgid 1 all 1
ldap_chkResponseList returns ld 0x91694d0 NULL
wait4msg ld 0x91694d0 msgid 1 (timeout 3000000 usec)
wait4msg continue ld 0x91694d0 msgid 1 all 1
ldap_chkResponseList ld 0x91694d0 msgid 1 all 1
ldap_chkResponseList returns ld 0x91694d0 NULL
ldap_int_select
readlmsg: ld 0x91694d0 msgid 1 all 1
readlmsg: ld 0x91694d0 msgid 1 message type bind
new result: res_errno: 0, res_error: <>, res_matched: <>
readlmsg: ld 0x91694d0 0 new referrals
readlmsg: mark request completed, ld 0x91694d0 msgid 1
request done: ld 0x91694d0 msgid 1
res_errno: 0, res_error: <>, res_matched: <>
ldap_free_request (origid 1, msgid 1)
ldap_free_connection 0 1
ldap_free_connection: refcnt 1
ldap_parse_result
ldap_msgfree
ldap_free_connection 1 1
ldap_send_unbind
ldap_free_connection: actually freed
----- END TEST -----
Successfully connected to user directory
```

no administrator - delete an administrator

Syntax: **no administrator** <username>

For example:

```
DemoBox (config)# show administrator
    admin
    admin2
    admin3
DemoBox (config)# no administrator admin3
```

As a security precaution, approval from multiple administrators is required to commit the requested changes. These changes may adversely affect the functionality of this device.

```
Current Administrator: admin
Authorization is required from 1 additional administrator
Valid Administrators to choose from:
    admin2
    admin3
```

```
Administrator: admin2
Administrator Password:
Authorization successfully granted by: admin2
Administrator successfully removed.
DemoBox (config)# show administrator
    admin
    admin2
```

no granted credential - cancel an existing credential grant

Syntax: **no granted credential** <credential #>

For example:

```
DemoBox (config)# show granted credential
1.   Grant to:          admin2
     Grant by:          admin
     Expiration:        Fri Dec 17 16:15:16 2010
     Allowed Operations: Add/Modify Users & Groups

2.   Grant to:          admin3
     Grant by:          admin
     Expiration:        Fri Dec 17 16:16:24 2010
     Allowed Operations: Add/Modify Keys, Delete Keys
```

```
DemoBox (config)# no granted credential 1
Credential removed
```

```
DemoBox (config)# show granted credential
1.   Grant to:          admin3
     Grant by:          admin
     Expiration:        Fri Dec 17 16:16:24 2010
     Allowed Operations: Add/Modify Keys, Delete Keys
```

no ldap server administrators - delete the LDAP settings for the primary, schema or failover servers

Syntax: **no ldap server administrators** <primary | schema | failover>

For example:

```
DemoBox (config)# no ldap server administrators failover
Cleared LDAP administrator server failover properties
```

passwd - change your password

Syntax: **passwd**

For example:

```
DemoBox (config)# passwd
Username: admin
```

```
Current Password:
New Password:
Confirm New Password:
Password successfully changed.
```

password settings - edit the password settings for all administrators

Requires config mode.

Syntax: **password settings**

For example:

```
DemoBox (config)# password settings
Enable Password Expiration (y/n) [n]: y
Maximum Password Age (days) [0]: 180
Enable Password History (y/n) [n]: y
Num Passwords to Remember [0]: 5
Minimum Password Length [8]: 8
Must Passwords Contain At Least One:
  Lower Case Letter (y/n) [n]: y
  Upper Case Letter (y/n) [n]: y
  Number (y/n) [n]: y
  Special Character (y/n) [n]: y
Password settings successfully saved.
```

recreate ssh key - recreate the Secure Shell key

If you execute this command from a secure shell client, the system will log you out of your SSH session.

Syntax: **recreate ssh key**

For example:

```
DemoBox (config)# recreate ssh key
Are you sure you want to recreate the SSH key? (y/n) [n]: y
SSH key successfully re-created.
DemoBox (config)# Connection to 172.17.7.29 closed by remote host.
Connection to 172.17.7.29 closed.
```

reissue webadmin certificate - recreate the web administration certificate

This action is performed when initializing the device. The optional duration parameter allows you to specify in days the duration that the webadmin certificate is valid.

Syntax: **reissue webadmin certificate <certification duration>**

For example:

```
DemoBox (config)# reissue webadmin certificate 10
Are you sure you want to reissue the cert? [n]: y
Warning: Please quit your browser now to use web certificate
```


Web administrator certificate successfully re-issued.

show administrator - view the settings for a specific administrator

Syntax: **show administrator** to view a list of all administrator accounts
show administrator <username> to view a specific account

For example:

```
DemoBox# show administrator  
admin  
admin2  
admin3
```

```
DemoBox# show administrator admin2  
Username: admin2  
Administrator Type: Local  
Full Name: administrator 2  
Description: administrator 2  
Password Expiration: Password must be changed after next login  
High Access Admin: yes
```

```
Access Control - Security Configuration  
yes - Keys and Authorization Policies  
yes - Users and Groups  
yes - Certificates  
yes - Certificate Authorities  
yes - Advanced Security  
yes - SSL  
yes - ProtectFile Manager
```

```
Access Control - Device Configuration  
yes - NAE Server  
yes - Cluster  
yes - Network and Date/Time  
yes - High Availability  
yes - SNMP  
yes - Logging
```

```
Access Control - Backup & Restore  
yes - Backup Configuration  
yes - Backup Keys & Certificates  
yes - Backup Local CAs  
yes - Restore Configuration  
yes - Restore Keys & Certificates  
yes - Restore Local CAs
```

```
Access Control - Maintenance  
yes - Services  
yes - Software Upgrade and System Health
```

```
Access Control - Administrative Access  
yes - Admin Access via Web  
yes - Admin Access via SSH
```

show credential settings - display the multiple credential settings

Syntax: **show credential settings**

For example:

```
DemoBox# show credential settings
  Require Multiple Credentials:          yes
  Num of Admins Required for Operations: 2
  Allow Time-Limited Credentials:       yes
  Maximum Duration for Credentials (minutes): 5
```

show granted credential - display the existing credential grants

Syntax: **show granted credential**

For example:

```
DemoBox (config)# show granted credential
1. Grant to:          admin2
   Grant by:          admin
   Expiration:        Fri Dec 17 15:48:30 2010
   Allowed Operations: Add/Modify Keys, Delete Keys, Add/Modify Users
                       & Groups, Delete Users & Groups, Modify Auth
                       Policies, Modify LDAP Server for Users & Groups
```

show ldap server administrators - display the LDAP administrator server settings, schema properties, and the failover server properties

Syntax: **show ldap server administrators**

For example:

```
DemoBox# show ldap server administrators
LDAP Administrator Server Properties
  Hostname or IP Address: [None]
  Port:                   [None]
  Use SSL:                 no
  Trusted Certificate Authority: [None]
  Timeout (sec):          3
  Bind DN:                 [None]
  Bind Password:          [None]

LDAP Schema Properties
  User Base DN:           [None]
  User ID Attribute:      [None]
  User Object Class:      [None]
  User List Filter:       [None]
  Search Scope:           One Level

LDAP Failover Server Properties
  Failover Hostname or IP Address: [None]
  Failover Port:             [None]
```

show password settings - view the password settings for all administrators

Syntax: **show password settings**

For example:

```
DemoBox# show password settings
Password Expiration:      Never
Password History:        Disabled
Minimum Password Length: 8
Passwords Must Contain At Least One:
  Lower Case Letter:     no
  Upper Case Letter:     no
  Number:                no
  Special Character:     no
```

Note: In addition to the restrictions above, passwords must contain at least 5 different characters, cannot be based on a dictionary word, and cannot contain too many sequential characters. Password length and character requirements also apply to local user, cluster, and backup passwords.

show ras settings - display the current remote administration settings

Syntax: **show ras settings**

For example:

```
DemoBox# show ras settings
Web Admin Server IP:           [All]
Web Admin Server Port:         9443
Web Admin Client Cert Authentication: Disabled
Web Admin Trusted CA List Profile: [None]
SSH Admin Server IP:           [All]
SSH Admin Server Port:         22
```

Chapter 3

Auto-logout

Using the CLI, you can:

- configure and view the automatic logout time for the current administrator for the current session (autologout, show autologout)

autologout - set the number of minutes the system remains inactive prior to logging off the current user

The autologout setting applies to the current administrator and the current session. The setting can be between 0 and 720. Use 0 to disable the feature.

Syntax: **autologout** <minutes>

For example:

```
DemoBox (config)# autologout 45  
Autologout successfully set to 45 minutes.
```

show autologout - display the current autologout setting for this session

Syntax: **show autologout**

For example:

```
DemoBox# show autologout  
The autologout time is set to 45 minutes.
```

Chapter 4

Backup & Restore

Using the CLI, you can:

- view the backups on the device (`show backup`)
- create backups (`backup`)
- restore backups (`restore backup`)
- delete backups (`no backup`)

The same functionality is available through the Management Console.

backup - create a system backup

After executing the backup command, the system prompts you to provide a name and description for the file. You can specify which configurations to include.

Syntax: **backup**

For example:

```
DemoBox (config)# backup
Enter the backup name: FullBackup
Enter a backup description: Backup of all config, keys, and certs
Please indicate below which Security items are to be backed up:
    ProtectFile Manager (y/n): y
Which keys would you like to back up?
    1: All keys
    2: No keys
    3: Prompt me for each key
Enter a number (1 - 3): 1
    Key Query and Options (y/n): y
    Authorization Policies (y/n): y
    Local Users & Groups (y/n): y
    LDAP Server for Users & Groups (y/n): y
Would you like to back up all the certificates (y/n): y
Would you like to back up all the local certificate authorities (y/n): y
    Known CAs, CRLs, Trusted CA Lists (y/n): y
    High Security (y/n): y
    FIPS Status Server (y/n): y
Please indicate below which Device items are to be backed up:
    NTP (y/n): y
    Network (y/n): y
    IP Authorization (y/n): y
    High Availability (y/n): y
    Administrators (y/n): y
    SNMP (y/n): y
```

```
Logging (y/n): y
SSL (y/n): y
NAE Server (y/n): y
Services (y/n): y
Log Signing Certificate (y/n): y
Enter the backup password:
Please enter the password again:
Please pick one of the following types of backup:
    1) Internal    2) FTP    3) SCP
Backup Type (1-3): 1
Backup successful.
```

no backup - remove a specified system backup file

Syntax: **no backup** <name>

For example:

```
DemoBox# show backup
Internal Backup List
    Backup Name                Backup Date
    FullBackup                 Fri Dec 17 2010 14:01:28 PST
    WeeklyBackup               Fri Dec 17 2010 14:00:19 PST
```

```
DemoBox (config)# no backup WeeklyBackup
Backup removal successful.
```

```
DemoBox (config)# show backup
Internal Backup List
    Backup Name                Backup Date
    FullBackup                 Fri Dec 17 2010 14:01:28 PST
```

restore backup - restore a backup file

You must know the backup file password. The system displays the configuration items that were included in the backup you selected to restore. After restoring the backup, we recommend that you restart the device. This command requires config mode.

Syntax: **restore backup**

For example:

```
DemoBox (config)# show backup
Internal Backup List
    Backup Name                Backup Date
    FullBackup                 Fri Dec 17 2010 14:01:28 PST
```

```
DemoBox (config)# restore backup
Please pick the type of backup to restore:
    1) Internal    2) FTP    3) SCP
Backup Type (1-3): 1
Enter the source filename: FullBackup
Enter the backup password:
```

The following describes the backup you are going to restore:

Backup Name: FullBackup

Description: Backup of all configuration, keys, and certs

Archive Date: 2010-12-17 14:01:28

Would you like to restore this configuration item? (yes or no):

NTP (y/n): y

Network (y/n): y

IP Authorization (y/n): y

High Availability (y/n): y

Administrators (y/n): y

SNMP (y/n): y

Logging (y/n): y

SSL (y/n): y

High Security (y/n): y

FIPS Status Server (y/n): y

NAE Server (y/n): y

Key Query and Options (y/n): y

Authorization Policies (y/n): y

Local Users & Groups (y/n): y

LDAP Server for Users & Groups (y/n): y

ProtectFile Manager (y/n): y

Services (y/n): y

Log Signing Certificate (y/n): y

Certificates:

Would you like to restore all the certificates (y/n): y

Local Certificate Authorities:

Would you like to restore all the certificate authorities (y/n): y

Keys:

Would you like to restore all the keys (y/n): y

Enter the backup password again to restore this backup:

Backup successfully restored.

Warning: Restart your system for changes to take effect.

show backup - view a list of the backup files stored on the device

Syntax: **show backup**

For example:

DemoBox# **show backup**

Internal Backup List

Backup Name

FullBackup

WeeklyBackup

Backup Date

Fri Dec 17 2010 14:01:28 PST

Fri Dec 17 2010 14:00:19 PST

Chapter 5

Certificate Configuration

Using the CLI, you can:

- view certificates (show certificate)
- view certificate requests (show request)
- install certificates (certificate install)
- import certificates (certificate import)
- create a certificate request (certificate request)
- install a selfsigned certificate (certificate selfsign install)
- delete an installed certificate (no certificate)
- delete a certificate request (no request)

certificate install - install a certificate

During the installation session, the system will prompt for the certificate.

Syntax: **certificate install <cert name>**

For example:

```
DemoBox (config)# certificate install "Client Cert"
Please perform these 2 steps to install the certificate:
  1) Paste the certificate immediately after the question mark
  2) Press return twice when you have finished
?-----BEGIN CERTIFICATE-----
MIIDoZCCAougAwIBAgIC0lEwDQYJKoZIhvcNAQELBQAwfzELMAkGA1UEBhMCVVMx
EDAoBgNVBAgTB2sxNTAuY2ExEDAoBgNVBAcTB2sxNTAuY2ExEDAoBgNVBAoTB2sx
NTAuY2ExEDAoBgNVBAcTB2sxNTAuY2ExEDAoBgNVBAMTB2sxNTAuY2ExFjAUBGkq
hkiG9w0BCQEWB2sxNTAuY2EwHhcNMTEwMzI0MDM1MTM2WhcNMjEwMzAzMDM1MTM2
WjCBhZELMAkGA1UEBhMCVVMx CzAJBgNVBAGTAkNBMRewDwYDQVQHEwhTYW4gSm9z
ZTEQMA4GA1UEChMHQ29tcGFueTERMA8GA1UECXMIRGl2aXNpb24xFDASBgNVBAMT
C0NsaWVudCBDZXXJ0MR0wGwYJKoZIhvcNAQkBFg51c2VyQGVTYWlsLmNvbTCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKeQ2jrzcEF4Bk036sIY+DrgRMQc
hRzwbWITahtkQSNX1SjxkjivGEZvORiDmarPhfmv/neMqo+CaTH8uoVThuCBKvt
rea3Kvh21l6TdSsOY/VoSRA92LzMNcWv2ZduQI+6z7km+G9hGIyFu9939xDqDxYf
HSu3KjAdvxdCRA/ywYweEFXYEGmWanpGYPeAgb1tAYvlV0GRtDaWqXUyOGFu47n0
5ZsK6b9o39h/DwtqhGYEZJkViET8bHa4FlJ4BuC25U2Vk5tUUsUCbeAqCD3Gn6Nb
RHPEG5xyrRHGHmA26JrYJXuuvRuyUOqa8FxaSR7EakXkPO2wHQHN4dP8xnECAwEA
AaMgMB4wCQYDVR0TBAlwADARBgIghkgBhvCAQEEBAMCB4AwDQYJKoZIhvcNAQEL
BQADggEBAIcxrbECLXyo/WbT0DvJFLTdyCxx9nPFzXaE2Y9K/Ns2Jsnz34MQ72mK
bqj27XZGyeTVAvCDYHPDQiEEnk/p5AiKqorCIaOdVzEvH4NEQ5mSCJa8AODPvtme
D9PFTA/270YHgXoMS50pgOsXGYOJOPjtZXwauXJzjZi19KyYZ9zbExirApVMNj4v
```



```
ZWd3p3MdQIEkgZvbXjaBjmfPry5cgq/Vz9TZa7SJuoZ1AEdX/5VhUJKIZuY8IHYA
5szVXhRZ2zDMJ5Pbd3nw6ccDhNvBj47Ph09HXMYfdfqFgFNIw/LNO2sr7lcCzk7M
9GLoq8c1deS0LoxIxqkuCf6HXzaKI8M=
-----END CERTIFICATE-----
```

Warning: Certificates should be backed up for protection
Certificate successfully installed.

certificate import - import a certificate

Syntax: **certificate import**

For example:

```
DemoBox (config)# certificate import
Please pick the upload option for uploading your certificate:
  1) Console Paste (PEM certs only)
  2) FTP
  3) SCP
Upload Type (1-3)? : 1
Enter cert name: TestThree
Enter the password protecting the private key:
Please perform these 2 steps to finish importing a PEM encoded
certificate and key:
  1) Paste the PEM encoded certificate and private
     key (in any order) immediately after the question mark
  2) Press return three times when you are done
?-----BEGIN CERTIFICATE-----
MIIDDozCCAougAwIBAgIC0lEwdQYJKoZIhvcNAQELBQAwfzELMAkGA1UEBhMCVVMx
EDA0BgNVBAGTB2sxNTAuY2ExEDA0BgNVBACTB2sxNTAuY2ExEDA0BgNVBAoTB2sx
NTAuY2ExEDA0BgNVBAsTB2sxNTAuY2ExEDA0BgNVBAMTB2sxNTAuY2ExFjAUBGkq
hkiG9w0BCQEWB2sxNTAuY2EwHhcNMTEwMDM1MTM2WhcNMjEwMzAzMDM1MTM2
WjCBhzELMAkGA1UEBhMCVVMxChAJBgNVBAGTAkNBMRERwDwYDVRQHEwhTYW4gSm9z
ZTEQMA4GA1UEChMHQ29tcGFueTERMA8GA1UECXMIRG12aXNpb24xFDASBgNVBAMT
C0NsaWVudCBDZXJ0MR0wGwYJKoZIhvcNAQkBFg51c2VyQGVTYWlsLmNvbTCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKeQ2jrzcEF4Bk036sIY+DrgRMQc
hrZwBWiTahtkQSNX1SjKxjiqvGEZvORiDmarPhfmv/neMqo+CaTH8uoVThuCBKvt
rea3Kvh2116TdSsOY/VoSRA92LzMNCwV2ZduQI+6z7km+G9hGIyFu9939xDqDxYf
HSu3KjAdvxdCRA/ywYweEFXYEGmWanpGYPeAgbltAYvlVOgRtDaWqXUyOGFu47nO
5ZsK6b9o39h/DwtqhGYEZJkViET8bHa4FlJ4BuC25U2Vk5tUUsUCbeAqCD3Gn6Nb
RHPEG5xyrRHGHmA26JrYJXuuvRuyUOqa8FxaSR7EakXkPO2wHQHN4dP8xnECAwEA
AaMgMB4wCQYDVR0TBAlwADARBgIghkgBhvCAQEEBAMCB4AwDQYJKoZIhvcNAQEL
BQADggEBAIcxrbECLXyo/WbT0DvJFLTdyCxX9nPFzXaE2Y9K/Ns2Jsnz34MQ72mK
bqj27XZGyeTVAvCDYHPDQiEEnk/p5AiKqorCIaOdVzEvH4NEQ5mSCJa8AODPvtme
D9PFTA/270YHgXoMS50pgOsXGYOJOPjtZXwauXJzjZi19KyYZ9zbExirApVMNj4v
ZWd3p3MdQIEkgZvbXjaBjmfPry5cgq/Vz9TZa7SJuoZ1AEdX/5VhUJKIZuY8IHYA
5szVXhRZ2zDMJ5Pbd3nw6ccDhNvBj47Ph09HXMYfdfqFgFNIw/LNO2sr7lcCzk7M
9GLoq8c1deS0LoxIxqkuCf6HXzaKI8M=
-----END CERTIFICATE-----

Certificate successfully installed.
```

certificate request - create a certificate request

Syntax: **certificate request** <cert name>

For example:

```
DemoBox (config)# certificate request CertTwo
Common Name: CertTwo
Organization Name: Company
Organizational Unit Name: Division
Locality Name: Chico
State or Province Name: CA
Country Name [US]: US
Email Address: user@company.com
```

Key Size (2048, 3072, 4096) [2048]: 2048

Warning: Certificate requests should be backed up for protection
The certificate request was successfully created (text shown below).

TEXT:

```
-----BEGIN CERTIFICATE REQUEST-----
MIICyDCCAbACAQAwYIxEDAOBgNVBAMTB0NlcnRud28xEDA0BgNVBAoTB0NvbXBh
bnkxETAPBgNVBAsTCERpdmlzaW9uMQ4wDAYDVQQHEwVDaGljbzELMAkGA1UECBMC
Q0ExCzAJBgNVBAYTALVTMR8wHQYJKoZIhvcNAQkBFhBlc2VyQGNvbXBhbnkuY29t
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAMT7TZohCwGQDQiiObMp
uKM4xifrITQUM9ewd6EARxDKtXm4JOkH2lnFcowQrnOZPWdigpkLraacZXqlaW8m
5mHBw/qkW7MfD0pZmK8IeEi5TldZYdtZaPwiNgpIqQhVvoSG71lwkg+PSkGgWV9q
muvYqdEucvp2KSxL6U/XxqfYfAbtqbz/eSoA+B3LDKN9NP1CuAEpkmLRPtAvOThU
1NQilA121qFmcgnJTc9rrtquIEwfV0ynk2sqd8Ke2YHFBT4JXCzX/dHZhp941UE3
c2bwfPd4WKVrb0cuf4Jl9P2tLckqPI8FBtqiFaEYqXSRGYlkK0noFzXZq5EhFbz9
5wIDAQABAAAwDQYJKoZIhvcNAQELBQADggEBAEzJSvItZ4P0WpXroaxc9zv96wtO
+7toLF1c80WdiuuMkr7lk3q9BI2lztH+dG+9YM5E980qzbjyniISZviypGUoxz4
JIQvm/tAcOu2c5sVsJVcDJAWSj36qwrowHa7sHsQwaiJ/LfLp5+W9tXMzGiB0qCH
XMYd3Ma7ie3DMEhPG0dl0I6lieMx2cTwHha+bEM/CiNkBvgJ8j762wWBaXGtMB2R
LA6Hh3Qvcx6K8OD8HUMyYctSlHkGqcKwPJ5fbGNzcea5AK/56azd6W0pSibKNeYW
yeZzmeS8xz29tLvsBpXxJYL0M7aCy+H/ICiQtIl6a4S4h8N+yXwi+rYoZDQ=
-----END CERTIFICATE REQUEST-----
```

certificate selfsign install - install a test certificate

This command allows you to set up a self-signed certificate. The optional duration parameter allows you to specify in days the duration that the certificate is valid.

Syntax: **certificate selfsign install** <cert name> <cert duration>

For example:

```
DemoBox (config)# certificate selfsign install CertTwo 3056
Self sign certificate successfully created.
```

no certificate - delete an installed certificate

Syntax: **no certificate** <cert name>

For example:

```
DemoBox (config)# no certificate SelfTest-selfsign
Are you sure you want to delete the cert? [n]: y
Certificate successfully deleted.
```

no request - delete a certificate request

Syntax: **no request** <cert name>

For example:

```
DemoBox (config)# no request TestOne
Are you sure you want to delete the cert request? [n]: y
Certificate Request successfully deleted.
```

show certificate - view either specific certificate details or all installed certificates

Syntax: **show certificate** to view a list of all certificates

show certificate <cert name> to view a specific cert

For example:

```
DemoBox# show certificate
Server Certificates Installed
                Name                Status
                SelfTest-selfsign    Active

Client Certificates Installed
                Name                Status
                Client Cert          Active
                SelfTest-selfsign    Active

DemoBox# show certificate "Client Cert"
PROPERTIES:
Certificate Name: Client Cert
Serial Number:   0x3A51 (0)
Key Size:       2048
Start Date:     Mar 24 03:51:36 2011 GMT
Expiration:     Mar 3 03:51:36 2021 GMT

Issuer:
C:              US
ST:             k460.ca
L:              k460.ca
O:              k460.ca
OU:             k460.ca
CN:             k460.ca
emailAddress:   k460.ca
```

```
Subject:
C:          US
ST:         CA
L:          San Jose
O:          Company
OU:         Division
CN:         Client Cert
emailAddress: user@email.com
```

```
Purpose:
SSL client
CRL signing
```

```
TEXT:
-----BEGIN CERTIFICATE-----
MIIDoZCCAougAwIBAgICOlEwDQYJKoZIhvcNAQELBQAwfzELMAkGA1UEBhMCVVMx
EDA0BgNVBAGTB2sxNTAuY2ExEDA0BgNVBAcTB2sxNTAuY2ExEDA0BgNVBAoTB2sx
NTAuY2ExEDA0BgNVBAsTB2sxNTAuY2ExEDA0BgNVBAMTB2sxNTAuY2ExFjAUBGkq
hkiG9w0BCQEWB2sxNTAuY2EwHhcNMTEwMzI0MDM1MTM2WhcNMjEwMzAzMDM1MTM2
WjCBhzELMAkGA1UEBhMCVVMxCzAJBgNVBAGTAkNBMRewDwYDVQQHEwhTYW4gSm9z
ZTEQMA4GA1UEChMHQ29tcGFueTERMA8GA1UECXMIRG12aXNpb24xFDASBgNVBAMT
C0NsaWVudCBDZXXJ0MR0wGwYJKoZIhvcNAQkBFg51c2VyQGVTYWlsLmNvbTCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAAkeQ2jrzcEF4Bk036sIY+DrgRMQc
hRzWBWitAhtkQSNX1SjKxjiqvGEZvORiDmarPhfmv/neMqo+CaTH8uoVThuCBKVT
rea3Kvh21l6TdSsOY/VoSRA92LzMNcWV2ZduQI+6z7km+G9hGIyFu9939xDqDxYf
HSu3KjAdvxdCRA/ywYweEFXYEGmWanpGYPeAgbltAYv1VOgRtDaWqXUyOGFu47nO
5ZsK6b9o39h/DwtqhGYEZJkViET8bHa4FlJ4BuC25U2Vt5tUUsUCbeAqCD3Gn6Nb
RHPEG5xyrRHGHmA26JrYJXuuvRuyUOqa8FxaSR7EakXkPO2wHQHN4dP8xnECAwEA
AaMgMB4wCQYDVR0TBAlwADARBgIghkgBhvhCAQEEBAMCB4AwDQYJKoZIhvcNAQEL
BQADggEBAIcxrbeCLXyo/WbT0DvJFLtdyCx9nPFzXaE2Y9K/Ns2Jsnz34MQ72mK
bqj27XZGyeTVAvCDYHPDQiEEnk/p5AiKqorCIaOdVzEvH4NEQ5mSCJa8AODPvtme
D9PFTA/270YHgXoMS50pgOsXGYOJOPjtZXwauXJzjZi19KyYZ9zbExirApVMNj4v
Zwd3p3MdQIEkgZvbXjaBjmFpRy5cgq/Vz9Tza7SJuoZ1AedX/5VhUJKIZuY8IHYA
5szVXhRZ2zDMJ5Pbd3nw6ccDhNvBj47PhO9HXMYfdfqGfFNIw/LNO2sr7lcCzk7M
9GLoq8c1deS0LoxIxqkuCf6HXzaKI8M=
-----END CERTIFICATE-----
```

show request - view specific, or all certificate request details

Syntax: **show request** to view a list of all requests
show request <cert name> to view a specific request

For example:

```
DemoBox# show request
Certificate Requests
Name          Status
SelfTest     Request Pending
TestOne      Request Pending

DemoBox# show request TestOne
PROPERTIES:
```

Certificate Name: TestOne
Key Size: 2048

Subject:
CN=TestOne
O=Company
OU=Division
L=Naples
ST=Florida
C=US
emailAddress=user@email.com

TEXT:

```
-----BEGIN CERTIFICATE REQUEST-----  
MIICzDCCAbQCAQAwgYYxEDAObgNVBAMTB1Rlc3RPbmUxEDAObgNVBAoTB0NvbXBh  
bnkxETAPBgNVBAsTCERpdmlzaW9uMQ8wDQYDVQQHEwZOYXBsZXMxEDAObgNVBAgT  
B0Zsb3JpZGExCzAJBgNVBAYTAlVTMR0wGwYJKoZIhvcNAQkBFg51c2VyQGgtYWls  
LmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAAOUeKYM4AGKqV8lO  
E14N3gsIJ8BJqHcDePy6Ov8JZBCdbULi6hxZrnY92Jkcj3gJxFXBepoZqw0Phv1M  
PAYz4MWZv4UDcHhnqr0fe+S3pvAO5bz0sovnDNNaTVBGnE9RDYKNGq+JMCvn6h+d  
7+M3ZXmHr4SinLaM9SXcW/zumPFB5Ui7+U8sdi jY5gGZEcUoer6KdMzv11KE24Gb  
CCcpeeMlRYJMhIWBmU13sZSh7u+ILpywO9QMqDTEs82zRIxlxuGr5CvVZgmcskgF  
PJsU1VyXaF0sg3HThrAxQVcR1PwwGyE55WsBfPNBKMmWBulun5s/PIKI7/mP0rMH  
ub3fBb8CAwEAaAAMA0GCSqGSIb3DQEBCwUAA4IBAQC4lOjs9DmwNsFTiQDk33Rc  
oAR49jW3pmlKd0/RzbZ/o5hYVMLAjMV92Bcpg7IZhdCtOc9ca6BRhkinjM6oXRh  
JT0KKhqDoI9COB8bv1LzrpKG7EoQ0WWVQCTNjm8DNtHIAWbRFN2iJnHAM9a6tYtAD  
TQYsyb5SFfonFkL/D/DsZ2RXg3BLDCTiOKgV8Xx25ZXR2DMMLHnYznqcULG22Htz  
WzTc8jgi6pPYsdTVWX1vFI5eTicsCOD0Ym+uPp0ndX7Dn0liSi184tyHemnV+qTb  
Y8rkYsVIK76TKftNs4rs8I1hgNxVwtgchOzERSgbKyV1Bb0klP9WR4v3FnbbBVxr  
-----END CERTIFICATE REQUEST-----
```

Chapter 6

Certificate Authority Configuration

Using the CLI, you can:

- view a list of all CA certificate or specific certs (`show ca certificate`)
- view a list of local CAs or the details of a specific CA (`show local ca`)
- view a list of trusted CA list profiles or the details of a specific list (`show ca profile`)
- view the certificates signed by a CA (`show signed certificate`)
- install and remove a CA certificate (`ca certificate install`, `no ca certificate`)
- generate a local CA (`local ca`)
- install and remove a local CA (`local ca install`, `no local ca`)
- sign a certificate request (`sign request`)
- revoke and renew certificates signed by a local CA (`certificate revoke`, `certificate renew`)
- create and populate a trusted CA list profile (`ca profile`, `ca profile entry`, `ca profile duplicate`)
- rename a trusted CA list profile (`ca profile rename`)
- delete a CA from a trusted CA list (`no ca profile entry`)
- delete a trusted CA list profile (`no ca profile`)

ca certificate install - install a CA certificate

Syntax: **ca certificate install** <certificate name>

For example:

```
DemoBox (config)# ca certificate install NewCaCert
Please perform these 2 steps to install the CA certificate:
    1) Paste the CA certificate immediately after the question mark
    2) Press return twice when you have finished
?-----BEGIN CERTIFICATE-----
MIIEmjCCA4KgAwIBAgICLtoWdQYJKoZIhvcNAQELBQAwfzELMAkGA1UEBhMCVVMx
EDA0BgNVBAGTB2sxNTAuY2ExEDA0BgNVBACjB2sxNTAuY2ExEDA0BgNVBAoTB2sx
NTAuY2ExEDA0BgNVBAsTB2sxNTAuY2ExEDA0BgNVBAMTB2sxNTAuY2ExFjAUBGkq
hkiG9w0BCQEWB2sxNTAuY2EwHhcNMTEwMzA4MTc1NzU0WhcNMjEwMzAyMTc1NzU0
WjB/MQswCQYDVQQGEwJVUzEQMA4GA1UECBMHQ2Vydc44NzEQMA4GA1UEBxMHQ2Vy
dc44NzEQMA4GA1UEChMHQ2Vydc44NzEQMA4GA1UECjxMHQ2Vydc44NzEQMA4GA1UE
AxMHQ2Vydc44NzEQMA4GA1UEC3GSIb3DQEJARYHQ2Vydc44NzEQMA4GA1UEC3Fqm0EzKt
7HBgILBQZk7oqu+Q0jIRsy5JOWznXFrh4a4mVcEz/+a57PjJPJCNz2N8K8V+Tfs
```

```
hLMNSQB8iHOyAPbnsbQD1SGPtsafPGCaOHsxVSdG33o3qRHEuyQTjppqRFj0BsnLg
1IL6GbDEjjf1tk7ekkwhaeIH9FDV0/ulFHhHjBEAMubgDlwopMHe/xai1tEHUZOD
ofc3TkQy7Wm+eoTnWcA+h1RVW/w3+SdTP2CeB2Ji2ilKy7xhuxcP4Zsx00rC4DRa
MY8QCKopsce0XRCLnNlea04y6DMLcgUyq7ScFaRUJF5Aa7NQnBk9MQThh+j1GXyn
k0daSWdB/S5hOLAswOB1I1vXjpnKH1yIv25hVu7n4/8hDzNcg0qGo4OYYQs7CRqP
lhdL+rbC29UsvHfoObSBRma4q88/9OamZ2Yqkg8IuJ66zkX9Y4oinXIzPyy3NTXV
BAHRqoVn3Wl3B6Xz5vE1U3vNimhdeW4uWE8mWvYN4um+bvueVsaYZDoIFM9Roxw8
mPk3RRbRO+LbDcoDrlgUqlrV4FOjDNbQfh9pRy8zJqva5LMMIhZXuevoUousk9Of
ejJKzaZkSL7qRmstXy2grb8ArcHI0cbJrYfykGkTsW/WqRL96fsQ9DxbBMb4M4IF
hTAFAGMBAAGjIDAeMAkGA1UdEwQCMAAwEQYJYIZIAAYb4QgEBBAQDAgeAMA0GCSqG
S1b3DQEBCwUAA4IBAQA9HixwDAX2x/KwxsgtomqL6wz8JBC4mfGLSBeV3+0CxxuT
c95i962slgrcYrAsL2U53aCgw7tSL4YOaharm3KIgzP88qQEhQVfYN82+Vy9tuwQQ
n0NnZdvneJeRwnzxxk0ZokvfCroP9dYNVT42W3qdPYZcJXu5JS7XzTNGW3QDT2Qcj
bSljcxbtWJD3HI0+/MDC4/8IoW0NZY6y8f26/OUqGiD4ZqsJZ8cyCAu5cYRpjVxc
JnOy6fndPqXJwmluXA/eTxDqjL5Pdea30q1bqqyuD1lUe0ATeB3n0wQ0D1hQ46oi
jvl+AoiRDDyDsTB2OWCNq/k6VhE8uqDd5uRv3CXb
-----END CERTIFICATE-----
```

CA Certificate successfully installed.

ca profile - create an empty Trusted CA List profile

The profile is only useful when populated. Populate it using the `ca profile` entry and `ca profile duplicate` commands

Syntax: `ca profile <profile name>`

For example:

```
DemoBox (config)# ca profile ThirdProfile
Trusted CA list profile successfully added.
```

ca profile duplicate - copy the Trusted CA List from one profile and populate the Trusted CA list of another profile

Syntax: `ca profile duplicate <source profile> <target profile>`

For example:

```
DemoBox (config)# ca profile duplicate Default "Second Profile"
Trusted CA list profile successfully duplicated.
```

ca profile entry - add a CA to a Trusted CA List

Syntax: `ca profile entry <profile name> <ca name>`

For example:

```
DemoBox (config)# ca profile entry "Second Profile" k460.ca
CA successfully added to trusted CA list profile.
```

ca profile rename - rename a Trusted CA List profile

Syntax: **ca profile rename** <old name> <new name>

For example:

```
DemoBox (config)# ca profile rename "Second Profile" SecondProfile  
Trusted CA list profile successfully renamed.
```

certificate renew - renew a certificate that has been signed and revoked by a local CA

Syntax: **certificate renew** <local ca name> <serial number>

For example:

```
DemoBox (config)# show signed certificate k460.ca  
Serial Number      Status      Subject Name  
0x0                 Active      /C=US/ST=k460.ca/L=k460.ca/O=k460.ca/OU=k460.ca/CN=  
k460.ca/emailAddress=k460.ca  
0x2EDA             Active      /C=US/ST=Cert.87/L=Cert.87/O=Cert.87/OU=Cert.87/CN=  
Cert.87/emailAddress=Cert.87  
0x335A             Active      /C=US/ST=CA/L=Redwood City/O=SafeNet/OU=SafeNet  
West/CN=Certificate 47/emailAddress=safenet@safenet-inc.com  
0x3627             Active      /C=US/ST=CA/L=Redwood City/O=SafeNet/OU=SafeNet  
West/CN=Certificate 32/emailAddress=safenet@safenet-inc.com  
0x3A51             Active      /C=US/ST=CA/L=San Jose/O=Company/OU=Division/CN=  
Client Cert/emailAddress=user@email.com  
0x3F92             Revoked     /C=US/ST=SelfTest/L=SelfTest/O=SelfTest/OU=SelfT-  
est/CN=SelfTest/emailAddress=SelfTest
```

```
DemoBox (config)# certificate renew k460.ca 0x3F92  
Certificate renewed successfully
```

```
DemoBox (config)# show signed certificate k460.ca  
Serial Number      Status      Subject Name  
0x0                 Active      /C=US/ST=k460.ca/L=k460.ca/O=k460.ca/OU=k460.ca/CN=  
k460.ca/emailAddress=k460.ca  
0x2EDA             Active      /C=US/ST=Cert.87/L=Cert.87/O=Cert.87/OU=Cert.87/CN=  
Cert.87/emailAddress=Cert.87  
0x335A             Active      /C=US/ST=CA/L=Redwood City/O=SafeNet/OU=SafeNet  
West/CN=Certificate 47/emailAddress=safenet@safenet-inc.com  
0x3627             Active      /C=US/ST=CA/L=Redwood City/O=SafeNet/OU=SafeNet  
West/CN=Certificate 32/emailAddress=safenet@safenet-inc.com  
0x3A51             Active      /C=US/ST=CA/L=San Jose/O=Company/OU=Division/CN=  
Client Cert/emailAddress=user@email.com  
0x3F92             Active      /C=US/ST=SelfTest/L=SelfTest/O=SelfTest/OU=SelfT-  
est/CN=SelfTest/emailAddress=SelfTest
```


certificate revoke - revoke a certificate signed by a local CA

Syntax: **certificate revoke** <local ca name> <serial number>

For example:

```
DemoBox (config)# show signed certificate k460.ca
Serial Number      Status      Subject Name
0x0                 Active     /C=US/ST=k460.ca/L=k460.ca/O=k460.ca/OU=k460.ca/CN=
k460.ca/emailAddress=k460.ca
0x2EDA             Active     /C=US/ST=Cert.87/L=Cert.87/O=Cert.87/OU=Cert.87/CN=
Cert.87/emailAddress=Cert.87
0x335A             Active     /C=US/ST=CA/L=Redwood City/O=SafeNet/OU=SafeNet
West/CN=Certificate 47/emailAddress=safenet@safenet-inc.com
0x3627             Active     /C=US/ST=CA/L=Redwood City/O=SafeNet/OU=SafeNet
West/CN=Certificate 32/emailAddress=safenet@safenet-inc.com
0x3A51             Active     /C=US/ST=CA/L=San Jose/O=Company/OU=Division/CN=
Client Cert/emailAddress=user@email.com
0x3F92             Active     /C=US/ST=SelfTest/L=SelfTest/O=SelfTest/OU=SelfT-
est/CN=SelfTest/emailAddress=SelfTest
```

```
DemoBox (config)# certificate revoke k460.ca 0x3F92
Certificate revoked successfully
```

```
DemoBox (config)# show signed certificate k460.ca
Serial Number      Status      Subject Name
0x0                 Active     /C=US/ST=k460.ca/L=k460.ca/O=k460.ca/OU=k460.ca/CN=
k460.ca/emailAddress=k460.ca
0x2EDA             Active     /C=US/ST=Cert.87/L=Cert.87/O=Cert.87/OU=Cert.87/CN=
Cert.87/emailAddress=Cert.87
0x335A             Active     /C=US/ST=CA/L=Redwood City/O=SafeNet/OU=SafeNet
West/CN=Certificate 47/emailAddress=safenet@safenet-inc.com
0x3627             Active     /C=US/ST=CA/L=Redwood City/O=SafeNet/OU=SafeNet
West/CN=Certificate 32/emailAddress=safenet@safenet-inc.com
0x3A51             Active     /C=US/ST=CA/L=San Jose/O=Company/OU=Division/CN=
Client Cert/emailAddress=user@email.com
0x3F92             Revoked    /C=US/ST=SelfTest/L=SelfTest/O=SelfTest/OU=SelfT-
est/CN=SelfTest/emailAddress=SelfTest
```

local ca - generate a local CA certificate

Syntax: **local ca**

For example:

```
DemoBox (config)# local ca
Enter the certificate name: NewCA
Enter the common name: NewCA
Enter the organization name: Company
Enter the organization unit name: Division
Enter the locality name: Chicago
Enter the state name: IL
Enter the country name [US]: US
```

```

Enter the email address: user@company.com
Key Size (2048, 3072, 4096) [2048]: 2048
Please pick the Certificate Authority Type to create:
    1) Self-signed Root CA
    2) Intermediate CA Request
Certificate Type (1-2) [1]: 1
Enter a number of days for CA certificate duration [3650]: 3650
Enter a number of days for maximum user certificate duration [3650]: 3650

```

Warning: Local CA certificates must be added to a trusted CA list in order to be recognized by the NAE Server. Local CA certificates should be backed up for protection.

Local CA certificate successfully generated.

local ca install - install a local CA

Syntax: **local ca install**

For example:

```

DemoBox (config)# show local ca TestTwo
PROPERTIES:
Certificate Name: TestTwo
Key Size:      2048

Subject:
  CN:          TestTwo
  O:           Company
  OU:          Division
  L:           Boston
  ST:          MA
  C:           US
  emailAddress: user@company.com

```

```

TEXT:
-----BEGIN CERTIFICATE REQUEST-----
MIIC6DCCAdACAQAwwYMxEDAObgNVBAMTB1Rlc3RUd28xEDAObgNVBAoTB0NvbXBh
bnkxETAPBgNVBAsTCERpdmlzaW9uMQ8wDQYDVQQHEwZCb3N0b24xCzAJBgNVBAGT
Ak1BMQswCQYDVQQGEwJVUzEfMB0GCSqGSIb3DQEJARYQdXNlckBjb21wYW55LmNv
bTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAN1Ko69iG/1414iJRh2l
wAlYEaXhrrEaYlC6Imaa3X2fEPoilJzDsTIM8TA4MrlMAIH8UcmAYeSVRKTZjacE
91hvb27vmZwAEJO/1kVLnpo3iuNKGNDJiVl5xSks12k1L3kzbiCUwpFdydB0jpxL
k3sGPoRNQWScflzWoi+BJJaKUlDh+nEs0wwFCWesrtg6x+cnxdX9+a2EQvan2pO/
T+66TP0/b9Mpi8gI/Nvw/S22uROS4mDRgtQTZtoQADjq5AQQ9Z/aHy1/cEsse7uE
rYcIhEQzTNrwyq4mh+t0jMQPaNbjt/OV+S1Tnj/tSAGK3gYuVySPD6cYeP7sJLWn
eDcCAwEAaAfMB0GCSqGSIb3DQEJJDjEQMA4wDAYDVR0TBAUwAwEB/zANBgkqhkiG
9w0BAQsFAAOCAQEAWCH9WS2Z6r0/bmbx8Gqx+nMqhdYSVY8qz0GFKaiaOQuaDszQ
TAacP0B3Jtg7pkfzAbYJ4NdIWaw8rwwfPyogCLlJ+pAXDFr5VNIInlOm9t+gPA+wL
sxpUuY6doUnWSMBcMPgdmYl8skNwaYwDH4hArk+On3QVyH/zEurlhSxhxQujEP3m
WaXRKdQt79HBr8rMmQVwCQta+Y28f8MxkWq3s2dgOHZ3E/v3M7wB/mIfkrQtLahf
GHQA0ejyw1ER1owPg8I6QK+jEXycCbY633FAf5zL1Miko+X5EyZ/vWYvDHSYzUyB
xzfyylr6/OUtKvRtD0wHNNXWJcvNULemwQLgg==

```

-----END CERTIFICATE REQUEST-----

DemoBox (config)# **local ca install**

Enter the Local CA request that this certificate is for: TestTwo

Enter a number of days for maximum user certificate duration [3650]: 3650

Please perform these 2 steps to install the certificate:

1) Paste the certificate immediately after the question mark

2) Press return twice when you have finished

?-----BEGIN CERTIFICATE REQUEST-----

```
MIIC6DCCAdACAQAwwYMxEDAObgNVBAMTB1Rlc3RUd28xEDAObgNVBAoTB0NvbXBh
bnkxETAPBgNVBAsTCERpdmlzaW9uMQ8wDQYDVQQHEwZCb3N0b24xCzAJBgNVBAGT
Ak1BMQswCQYDVQQGEwJVUzEfMB0GCSqGSIb3DQEJARYQdXNlckBjb21wYW55LmNv
bTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAN1Ko69iG/1414iJRh2l
wAlYEaXhrrEaYlC6Imaa3X2fEPoilJzDsTIM8TA4MrLMAlH8UcmAYeSVRKTZjacE
91hvB27vmZwAEJO/1kVLnpo3iuNKGNDJiVl5xSks12k1L3kzbiCUwpFdydB0jpxL
k3sGPoRNQWScflzWoi+BJJaKuldh+nEs0wwFCWesrtg6x+cnxdX9+a2EQvan2pO/
T+66TP0/b9Mpi8gI/Nvw/S22uROS4mDRgtQTZtoQADjq5AQQ9Z/aHy1/cEsse7uE
rYcIhEQzTNrwyq4mh+t0jMQPaNbjt/OV+S1Tnj/tSAGK3gYuVySPD6cYeP7sJLWn
eDcCAwEAAaAfMB0GCSqGSIb3DQEJJDjEQMA4wDAYDVR0TBAAUwAwEB/zANBgkqhkiG
9w0BAQsFAAOCAQEAWCh9WS2Z6r0/bmbx8Gqx+nMqhdYSVY8qz0GFKaiaOQuaDszQ
TAacP0B3Jtg7pkfzAbYJ4NdIWaw8rwwfPyogCL1J+pAXDFr5VNIIn1oM9t+gPA+wL
sxpUuY6doUnWSMBcMPgdmYl8skNwaYwDH4hArk+On3QVyH/zEurlhSxhxQujEP3m
WaXRKdQt79HBr8rMmQVwCQta+Y28f8MxkWq3s2dgOHZ3E/v3M7wB/mIfkrQtLahf
GHQA0ejyw1ER1OwPg8I6QK+jEXycCbY633FAf5zL1Miko+X5EYZ/vWYvdHSYzUyB
xZfyylr6/OUtKvRtD0wHNNXWJcvNULemwQLgg==
```

-----END CERTIFICATE REQUEST-----

Certificate has been successfully installed.

no ca certificate - remove a CA certificate

Syntax: **no ca certificate** <ca name>

For example:

DemoBox (config)# **no ca certificate NewCaCert**

Are you sure you want to delete the CA cert? [n]: y

CA certificate successfully removed.

no ca profile - delete a Trusted CA List profile

Syntax: **no ca profile** <profile name>

For example:

DemoBox (config)# **no ca profile ThirdProfile**

Trusted CA list profile successfully removed.

no ca profile entry - delete a CA from a Trusted CA List

Syntax: **no ca profile entry** <profile name> <ca name>

For example:

```
DemoBox (config)# no ca profile entry "Second Profile" k460.ca  
CA successfully removed from trusted CA list profile.
```

no local ca - remove a specified local CA certificate

Syntax: **no local ca** <ca name>

For example:

```
DemoBox (config)# no local ca NewCA  
Are you sure you want to delete the Local CA? [n]: y  
Local CA certificate successfully removed.
```

show ca certificate - view the names of all CA certificates or view the details of a specific certificate

Syntax: **show ca certificate** to view the list of all CA certs
show ca certificate <ca name> to view a specific cert

For example:

```
DemoBox# show ca certificate  
CA Certificates  
  Name                Status  
  Another CA          Certificate Active  
  SelfTest-selfsign   Certificate Active
```

```
DemoBox# show ca certificate "Another CA"  
PROPERTIES:  
Certificate Name: Another CA  
Serial Number:    0x00 (0)  
Key Size:         2048  
Start Date:       Mar 24 03:49:59 2011 GMT  
Expiration:       Mar 22 03:49:59 2021 GMT
```

```
Issuer:  
  C:                US  
  ST:               CA  
  L:                Redwood City  
  O:                SafeNet  
  OU:               SafeNet West  
  CN:               SafeNet Local CA  
  emailAddress:     safenet@safenet-inc.com
```

```
Subject:  
  C:                US  
  ST:               CA  
  L:                Redwood City
```

```
O: SafeNet
OU: SafeNet West
CN: SafeNet Local CA
emailAddress: safenet@safenet-inc.com
```

```
Purpose:
SSL client & CA
SSL server & CA
Netscape SSL server & CA
S/MIME signing & CA
S/MIME encryption & CA
CRL signing & CA
```

```
TEXT:
-----BEGIN CERTIFICATE-----
MIIEtTCCA52gAwIBAgIBADANBgkqhkiG9w0BAQsFADCbnTElMAkGA1UEBhMCVVMx
CzAJBgNVBAGTAkNBMRUwEwYDVQQHEwxsZWR3b29kIENpdHkxEDAObGVBAAoTB1Nh
ZmVOZXQxFTATBgNVBAsTDFNhZmVOZXQgV2VzdDEZMBCGA1UEAxMQU2FmZU5ldCBM
b2NhbCBDQTEEmMCQGCSqGSIB3DQEJARYXc2FmZW5ldEBzYWZlbnV0LWluYy5jb20w
HhcNMTEwMzI0MDM0OTU5WhcNMjEwMzIyMDM0OTU5WjCBnTElMAkGA1UEBhMCVVMx
CzAJBgNVBAGTAkNBMRUwEwYDVQQHEwxsZWR3b29kIENpdHkxEDAObGVBAAoTB1Nh
ZmVOZXQxFTATBgNVBAsTDFNhZmVOZXQgV2VzdDEZMBCGA1UEAxMQU2FmZU5ldCBM
b2NhbCBDQTEEmMCQGCSqGSIB3DQEJARYXc2FmZW5ldEBzYWZlbnV0LWluYy5jb20w
ggEiMA0GCSqGSIB3DQEBAAUAA4IBDwAwggEKAoIBAQC7AcmvvungAJKoVLMTLu
99tMaCiTtJiFT7f+yex+XjVxp9k09X1EHfzNhWmiGuJ/MfE6PHJJBQsmLMn7tNaW
fsKLn3rjSNFbHmiHN6PskJ4e/9kHQJJ1CGym98zJZuTPefuVvre/fJurnJxvrH/u
CaPyT7wGqEmqwhdxID+NqO3LTeGDPGU8Kr5ncNQp+m/8d5ZzgmZbrg00+Sic3Jil
ZTFZ4Erd00arY96k/bRaN9E34iUbIODClRhIDpn1F/utko2dVO/RAjtWy/VS68Wx
xWbFsrfgax5u8wW8uHvx+Ztf8+yod8ngio5ixMNYnjMftQLSz0+BR503oJvqflUf
AgMBAAGjgJf0wgfowHQYDVR0OBByEFDIz1YZ9/S629zZvKCKZe7eXZqMfMIHKBgNV
HSMEGcIwgb+AFDIZ1YZ9/S629zZvKCKZe7eXZqMfoYGjpIGgMIGdMQswCQYDVOQG
EwJVUzELMAkGA1UECBMCQ0ExFTATBgNVBACTDFJlZHdvd2QgQ2l0eTEQMA4GA1UE
ChMHU2FmZU5ldDEVMBMGA1UECXMUMU2FmZU5ldCBXZXN0MRkwFwYDVQQDExBTYWZl
TmV0IEExvY2FsIENBMSYwJAYJKoZIhvcNAQkBFhdzYWZlbnV0QHNhZmVuZXQtaW5j
LmNvbYIBADAMBGNVHRMEBTADAQH/MA0GCSqGSIB3DQEBCwUAA4IBAQA/droSg58L
pxn3MANrkttcAEikG2gsDfom49Kp7n58zFBGs+7UBUsvUej8h05mAlKkbU7znLnt
Fwb8WdVbsQXXYvxYL5vnUrfJF06u3HiB/7zPFaSDuI+7HDD1vgdTTg4Xa/Z7Ro4U
PuPPqcmZxiajqr7LE2dmY9PZmUA3qAn0cvhe7ABIseyExXokwMr7oooRGgGnKL8h4
cSeHYorP6vKXgFlIi8wkyabdEr4QCnrSF+r02vui+1BDa+Wr4MFs5JhYEFW+XRw
0ixxhv3VtjtsVgEg3BWPm9zCbYOTxGHgdqI7Ewyczxl4PTvrEMN38X2HEj4KmkV2
uxRFP0n1CjM2
-----END CERTIFICATE-----
```

show ca profile - display a list of Trusted Certificate Authority List profiles or view the trusted CA list for a profile

Syntax: **show ca profile** to view the list of profiles
show ca profile <profile name> to view a profile's trusted CA list

For example:

```
DemoBox# show ca profile
          Default
          Second Profile
```

```
DemoBox# show ca profile Default
Local Certificate Authorities:
          k460.ca
          SafeNet Local CA
```

```
CA Certificates:
          SelfTest-selfsign
```

show local ca - view the list of all currently configured local CA certificates, or details for a specified local CA certificate

Syntax: **show local ca** to view the list of all local CAs
show local ca <ca name> to view a specific CA

For example:

```
DemoBox# show local ca
CA Certificates
          Name                      Status
          k460.ca                   CA Certificate Active
          SafeNet Local CA          CA Certificate Active
```

```
DemoBox# show local ca k460.ca
PROPERTIES:
Certificate Name: k460.ca
Serial Number:   0x00 (0)
Key Size:        2048
Start Date:      Mar 5 00:23:26 2011 GMT
Expiration:      Mar 3 00:23:26 2021 GMT
```

```
Issuer:
C:          US
ST:         k460.ca
L:          k460.ca
O:          k460.ca
OU:         k460.ca
CN:         k460.ca
emailAddress: k460.ca
```

```
Subject:
C:          US
ST:         k460.ca
L:          k460.ca
O:          k460.ca
OU:         k460.ca
CN:         k460.ca
emailAddress: k460.ca
```

```
Purpose:
  SSL client & CA
  SSL server & CA
  Netscape SSL server & CA
  S/MIME signing & CA
  S/MIME encryption & CA
  CRL signing & CA
```

```
TEXT:
```

```
-----BEGIN CERTIFICATE-----
MIIEWDCCA0CgAwIBAgIBADANBgkqhkiG9w0BAQsFADB/MQswCQYDVQQGEwJVUzEQ
MA4GA1UECBMHazE1MC5jYTEQMA4GA1UEBxMHazE1MC5jYTEQMA4GA1UEChMHazE1
MC5jYTEQMA4GA1UECXMhazE1MC5jYTEQMA4GA1UEAxMHazE1MC5jYTEWMBQGCsQG
S1b3DQEJARYHazE1MC5jYTAeFw0xMTAzMDUwMDIzMjZaFw0yMTAzMDMwMDIzMjZa
MH8xCzAJBgNVBAYTAlVTMRAwDgYDVQQIEwdrMTUwLmNhMRAwDgYDVQQHEwdrMTUw
LmNhMRAwDgYDVQQKEwdrMTUwLmNhMRAwDgYDVQQLEwdrMTUwLmNhMRAwDgYDVQQD
EwdrMTUwLmNhMRYwFAYJKoZIhvcNAQkBFgdrMTUwLmNhMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAKxRjNtK60qalE0RhJr8ge8Js9UEht2NC87IQwhUy
5RzPWxZQPZBwpiJAIRUCr7w/msu7LVQRDaRtF8H+KMVAiFrUiEwwokKESyTGH1
VE3AReakmkz7C+8wHXD6fQ70EdHgqiC4C5LpKESys35yx1MwByTSQQwsv/yjpdX
078dlyXHHy2J9TtJfLXXCFyBOABiN4ci2e5IxISPipmunNta7SOM/pDqQxFylrQf
8aD0+v95dsu8aBPtmUOPUwAqIwKzn5Jp4uKXH4sbrUJ4YZZkrnAKhl0snhYnUEeC
Yz4TjLnDsPGLy0kmBmHxeGIhSggB3zOStZ+bmjIyXs63hwIDAQABO4HeMIHbMB0G
A1UdDgQWBBQfZbh8Y7XAbhYHejvG45ATdQJXHkGBhKSBgTB/MQswCQYDVQQGEwJVUzEQMA4GA1UECBMH
azE1MC5jYTEQMA4GA1UEBxMHazE1MC5jYTEQMA4GA1UEChMHazE1MC5jYTEQMA4G
A1UECXMhazE1MC5jYTEQMA4GA1UEAxMHazE1MC5jYTEWMBQGCsQGS1b3DQEJARYH
azE1MC5jYYIBADAMBgNVHRMBETADAQH/MA0GCSqGSIb3DQEBwUAA4IBAQAActXty
VHurEA283QqKHRTU0e0MH7+6ei9wgKmfJmYS4cnyF7JofPP5VFUSPbX97jFnIk4m
4wzBNJ8bWEGEcWCAm4j1SfvV/F1JQMX/0Vwj6+TMjHvcTZu9W+0Ymj42IAL/Q9D
mvN3mD3ie5l/UK5Jk4E3AN7qgkZtiOtfyq7Bn3I6AxMlQvPm6RzWhwDo2BU5WcQr
CeMCA2rGDQFI7s2Vubx1kX89JReWwGgP1L5SmzjPRhoUoebhodc41q9w/tGWHh11
Mao6t0fCrmC8CnjYXE7m8zOSB4lc0jazH5QjV8v2FyXB7aGZcalkcPFtX6cYZYst
IW4yEVoHqZDQCbFD
-----END CERTIFICATE-----
```

show signed certificate - display information about certificates signed by local CAs on the device

If you specify a local CA after the show signed certificate command, the system will display all of the certificates signed by that CA. If you specify a local CA and the serial number of a certificate signed by that CA, the system will show specific certificate information for that signed certificate.

```
Syntax: show signed certificate <local ca name>
        show signed certificate <local ca name> <serial number>
```

For example:

```
DemoBox# show signed certificate k460.ca
Serial Number      Status      Subject Name
0x0                Active     /C=US/ST=k460.ca/L=k460.ca/O=k460.ca/OU=k460.ca/
```

```

0x2EDA      Active      CN=k460.ca/emailAddress=k460.ca
              /C=US/ST=Cert.87/L=Cert.87/O=Cert.87/OU=Cert.87/
0x335A      Active      CN=Cert.87/emailAddress=Cert.87
              /C=US/ST=CA/L=Redwood City/O=SafeNet/OU=SafeNet
0x3627      Active      West/CN=Certificate 47/emailAddress=
              safenet@safenet-inc.com
0x3A51      Active      /C=US/ST=CA/L=Redwood City/O=SafeNet/OU=SafeNet
              West/CN=Certificate 32/emailAddress=
              safenet@safenet-inc.com
0x3A51      Active      /C=US/ST=CA/L=San Jose/O=Company/OU=Division/CN=
              Client Cert/emailAddress=user@email.com

```

DemoBox# show signed certificate k460.ca 0x2EDA

PROPERTIES:

```

Serial Number: 0x2EDA (11994)
Key Size:      4096
Start Date:    Mar 8 17:57:54 2011 GMT
Expiration:    Mar 2 17:57:54 2021 GMT

```

Issuer:

```

C:             US
ST:            k460.ca
L:             k460.ca
O:             k460.ca
OU:            k460.ca
CN:            k460.ca
emailAddress:  k460.ca

```

Subject:

```

C:             US
ST:            Cert.87
L:             Cert.87
O:             Cert.87
OU:            Cert.87
CN:            Cert.87
emailAddress:  Cert.87

```

Purpose:

```

SSL client
CRL signing

```

Text:

-----BEGIN CERTIFICATE-----

```

MIIEmjCCA4KgAwIBAgICLtoWdQYJKoZIhvcNAQELBQAwfzELMAkGA1UEBhMCVVMx
EDA0BgNVBAGTB2sxNTAuY2ExEDA0BgNVBAcTB2sxNTAuY2ExEDA0BgNVBAoTB2sx
NTAuY2ExEDA0BgNVBAsTB2sxNTAuY2ExEDA0BgNVBAMTB2sxNTAuY2ExFjAUBgkq
hkiG9w0BCQEWB2sxNTAuY2EwHhcNMTEwMzA4MTc1NzU0WhcNMjEwMzAyMTc1NzU0
WjB/MQswCQYDVQQGEwJVUzEQMA4GA1UECBMHQ2VydC44NzEQMA4GA1UEBxMHQ2Vy
dC44NzEQMA4GA1UEChMHQ2VydC44NzEQMA4GA1UECXMHQ2VydC44NzEQMA4GA1UE
AxMHQ2VydC44NzEQMA4GA1UEC3QGSiB3DQEJARYHQ2VydC44NzCCAiIwDQYJKoZIhvcN
AQEBBQADggIPADCCAgcCggIBAMAMersrwnC1J8Cbrm9b/LavnGHInMC3Fqm0EzKt
7HBgILBQQfk7oqu+Q0jIRsy5JOWznxFrh4a4mVcEz/+a57PjJPJCNz2N8K8V+Tfs
hLMNSQB8iHOyAPbnsbQD1SGPtsafPGCaOHsxVSdG33o3qRHEuyQTjppRFj0BsnLg
1IL6GbDEjjf1tk7ekkwhaeIH9FDV0/ulFhHjBEAMubgDlwopMHe/xailtEHUZOD

```



```

ofc3TkQy7Wm+eoTnWcA+h1RVW/w3+SdTP2CeB2Ji2ilKy7xhuxcP4Zsx00rC4DRa
MY8QCKopsce0XRCLnNlea04y6DMLcgUyq7ScFaRUJF5Aa7NQnBk9MQThh+j1GXyn
k0daSWdB/S5hOLAswOB1i1vXjpnKH1yIv25hVu7n4/8hDzNcg0qGo4OYYQs7CRqP
1hdL+rbC29UsvHfoObSBRma4q88/9OamZ2Yqkg8IuJ66zkX9Y4oinXIzPyy3NTXV
BAHRqoVn3Wl3B6Xz5vE1U3vNimhdeW4uWE8mWvYN4um+bvueVsaYZDoIFM9Roxw8
mPk3RRbRO+LbDcoDrlgUqlrV4FOjDNbQfh9pRy8zJqva5LMMIhZXuevoUousk9Of
ejJKzaZkSL7qRmstXy2grb8ArchI0cbJrYfykGkTsW/WqRL96fsQ9DxbBmB4M4IF
hTAFAGMBAAGjIDAeMAKGA1UdEwQCMAAwEQYJYIZIAAYb4QgEBBAQDAgeAMA0GCSqG
S1b3DQEBCwUAA4IBAQA9HixwDAX2x/KwxsgtomqL6wz8JBC4mfGLSBeV3+0CxxuT
c95i962s1grcYrAsL2U53aCgw7tSL4YOharm3KIgzP88qQEhQVfYN82+Vy9tuwQQ
n0NnZdvneJeRwnzxk0ZokvfCroP9dYNVT42W3qdPYZcJXu5JS7XzTNGW3QDT2Qcj
bSljcxBTwJD3HI0+/MDC4/8IoW0NZY6y8f26/OUqGiD4ZqsJZ8cyCAu5cYRpjVxc
JnOy6fndPqXJwmluXA/eTxDqjL5Pdea30q1bqqyuD11Ue0ATeB3n0wQ0DlhQ46oi
jvl+AoiRDDyDsTB2OWCNq/k6VhE8uqDd5uRv3CXb
-----END CERTIFICATE-----

```

sign request - sign a certificate request using a local CA

Syntax: **sign request**

For example:

```

DemoBox (config)# sign request
Enter the Local CA certificate to sign this request with: k460.ca
Enter the certificate purpose of this request:
    1) Server          2) Client          3) Intermediate CA
Enter a number (1 - 3): 2
Enter a number of days for the certificate duration [3631]: 3630
Please perform these 2 steps to sign the request:
    1) Paste the request immediately after the question mark
    2) Press return twice when you have finished
?-----BEGIN CERTIFICATE REQUEST-----
MIICyzCCAbMCAQAwwYUxETAPBgNVBAMTCFNlbGZUZXR0MREwDwYDVQQKEWhTZWxm
VGZvdDERMA8GA1UECXMlU2VsZlRlc3QxETAPBgNVBAcTCFNlbGZUZXR0MREwDwYD
VQIIEwhTZWxmVGZvdDELMAKGA1UEBhMCVVMxMzFzAVBkqkqhkig9w0BCQEWCFNlbGZU
ZXN0MIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5L0y/8OeITiAJanb
ZPR2WhfThINZrZmz19g5VTlF5xkU+hmnPkgJD7/zfzKRvX45UnhE55xejyY2ieg
n42lS2TQTqrGBZWI/DP69kqTWWKN6FZ8C8SNKCZANjnoWYBtXCmRB02GoX88xwo+
p6sPuXnD8nC5OQBloNi9cQeHG0kiq+GuIGPdBKY+wI60HsFFLd4yXhKU8jPVsxCh
0EpyL/c3lHqPoeyabfj4lW8Q3uquxrwthFB8WBG/z21nmXZCzljlHu4ejKzsKv9
AvWXe4RA80G7JRkqNUiTqXpUrRBwn5tw3RX4tLEWVv7Bi04cqFfscEYEanWJj7lM
94ToowIDAQABoAAwDQYJKoZIhvcNAQELBQADggEBAC0ZtDNa2NJpAunn11vp30Yp
FXQbgOr2BYGPDPT5ajuCsy9pb0twcqFDenOy3uxCsBQ0R5uLoUg+HW+/a5ZanVoG
R94LyCm+TsAWavblbDI/87WzjkrVussQuaGBLZgexlRiHLoCBQEJjB8XS6BDgQlB
6aswZQVknJUZCep4tYfJ2tCxGi9F+W7lsmyl3kGgS36sT7LtrqOGj09XqMZmW402
NdoFU2C07t/41T5LvXCwJ+pgNhomJD1786TBGWr8IKdAYLuhPbcbId2E07xQ39EB
+LOTdpwtoRab9mEQpfdNXEVAW7NnlupfS/3XpXnlXt5qpy8r0u17PonJlpWBpBc=
-----END CERTIFICATE REQUEST-----

Certificate request successfully signed.
The signed certificate is shown below:

```

-----BEGIN CERTIFICATE-----

```
MIIDoTCCAomgAwIBAgICP5IwDQYJKoZIhvcNAQELBQAwfzELMAkGA1UEBhMCVVMx
EDA0BgNVBAGTB2sXNTAuY2ExEDA0BgNVBACTB2sXNTAuY2ExEDA0BgNVBAoTB2sX
NTAuY2ExEDA0BgNVBAsTB2sXNTAuY2ExEDA0BgNVBAMTB2sXNTAuY2ExFjAUBgkq
hkiG9w0BCQEWB2sXNTAuY2EwHhcNMTEwMzI0MDQxNzQ1WhcNMjEwMzAyMDQxNzQ1
WjCBhTELMAkGA1UEBhMCVVMxETAPBgNVBAGTCFNlbGZUZXR0MREwDwYDVQQHEwhT
ZWxmVGZzdDERMA8GA1UEChMIU2VsZlRlc3QxETAPBgNVBAsTCFNlbGZUZXR0MREw
DwYDVQQDEwhTZWxmVGZzdDEXMBUGCSqGSIb3DQEJARYIU2VsZlRlc3QwggEiMA0G
CSqGSIb3DQEBAAQ4IBDwAwggEKAoIBAQDkvTL/w54hOIALqdtk9HZaF90Eg1mt
mbPX2DlVOUWzGRT6GaGc+SakPv/N/MpG9fj1SeETnnF6PJjaJ6CfjaVLZNB0qsYF
lyj8M/r2SpNZYo3oVnwLxI0oJkA2OehZgG1cKZEHTYahfzzHCj6nqw+5ecPycLk5
AGWg2LlxB4cbSSKr4a4gY90Epj7AjrQewUUt3jJeEpTyM9WzEKHQSnIv9zeUeo+h
7Jpt+PiVbxDe6q7GvC0cUHxYeb/PbWeZdkLOWOWce7h6MrOwq/0C9Zd7hEDzQbsl
GSolSJOpelStEHCfm3DdFfi2URZW/sGLThyoV+xwRgRqdYmPuUz3hOijAgMBAAGj
IDAeMAkGA1UdEwQCMAAwEQYJYIZIAAYb4QgEBBAQDAgeAMA0GCSqGSIb3DQEBcWUA
A4IBAQBxI9QtrhHyHu9sDoytgkmdGFDwHdcb526m6geMiQnu6MB2+pfCIkO17npf
uZPKuJ2hmHbMmm4IiZPcEqF4eKJayhyzrPVkmzK9I+dtq+JyGG6dXZiWja8MZw4P
BoTraFjXvlainfi5/cjoy8Qyx0t3mb1UJpBSprJq7K/EPkeaCWCYPhklFvTidJyu
JBQUaRVtp1XokGxu9ryJjmqjHa9CdxgslDSacMyJCWvzw2Xtlllaehiou4V7CLcE
LEYizv1tpIexy2/K22oLXAjMrsWNV2EpuroL/RuhpOQ+j3YrjzBou2HjgnlXbIbm
66ffze2wpXNcxD/E8YoZzAn4ejg
```

-----END CERTIFICATE-----

Chapter 7

Certificate Revocation List Configuration

Using the CLI, you can:

- enable, configure, disable, and view the status of the crl auto-update feature (`crl auto-update`, `crl settings`, `no crl auto-update`, `show crl auto-update`)
- export a crl (`crl list send`)
- manually update a crl (`crl list update`)
- delete a crl (`no crl list`)
- find a certificate on a crl (`show crl entry`)
- view all serial numbers on a crl (`show crl list`)
- view the crl settings for a CA (`show crl settings`)
- view the general information associated with a crl (`show crl status`)

crl auto-update - enable the auto-update feature

Syntax: **crl auto-update**

For example:

```
DemoBox (config)# crl auto-update  
CRL auto-update enabled successfully.
```

crl list send - export a CRL

Syntax: **crl list send <ca name>**

For example:

```
DemoBox (config)# crl list send Local_CA  
      Transport Method:  
        1) FTP  2) SCP  
Enter a number (1 - 2): 1  
      Host: 172.17.40.247  
      Filename: Local_CA.crl  
      Username: user1  
      Password:  
      Confirm password:  
Success
```

crl list update - manually update a CRL

You must have already run the `crl settings` command. This command cannot be applied to a local CA.

Syntax: **crl list update** <ca name>

For example:

```
DemoBox (config)# crl list update Some_CA
CRL updated successfully.
```

crl settings - configure the device to automatically download the CRL for a CA

This command is only effective when Auto-Update is enabled. This command cannot be used for local CAs.

Note: The Next Update prompt is used to set the Next Update field in the CRL, not to change the actual update time. The actual update time follows the normal 5:00 AM procedures.

Syntax: **crl settings** <ca name>

For example:

```
DemoBox (config)# crl settings Verisign_Class_2_Public_Primary_CA_-_G3
Transport Method:
  1) FTP  2) SCP  3) HTTP
Enter a number (1 - 3): 3
Host: crl.verisign.com
Filename: pca2-g3.crl
Enter a date as Month Day HH:MM:SS Year TZ
For example, Jan 29 00:00:00 1996 GMT
Next Update: Apr 16 23:37:00 2011 PST
Force a periodic update of the CRL? [n]: y
Force Update Interval (min): 60
CRL settings updated successfully.
```

no crl auto-update - disable the Auto-Update feature

Syntax: **no crl auto-update**

For example:

```
DemoBox (config)# no crl auto-update
CRL auto-update disabled successfully.
```

no crl list - delete the CRL published by the known CA

When you use the `no crl list` command with a local CA, the device renews all revoked certificates signed by that local CA.

Syntax: **no crl list** <ca name>

For example:

```
DemoBox (config)# no crl list Local_CA  
CRL has been deleted successfully.
```

show crl auto-update - see if the Auto-Update feature is enabled

Syntax: **show crl auto-update**

For example:

```
DemoBox# show crl auto-update  
CRL auto-update: Disabled.
```

show crl entry - see if a certificate is on a CRL

Syntax: **show crl entry <ca name> <serial number>**

For example:

```
DemoBox# show crl entry Local_CA 0x0660  
  Serial Number: 0x0660 (1632)  
Revocation Date: Apr 21 17:55:25 2011 GMT
```

show crl list - display the serial number and revocation date of all revoked certificates in the CRL

Syntax: **show crl list <ca name>**

For example:

```
DemoBox# show crl list Local_CA  
  Serial Number: 0x0660 (1632)  
Revocation Date: Apr 21 17:55:25 2011 GMT  
  Serial Number: 0x0F0B (3851)  
Revocation Date: Apr 21 21:54:39 2011 GMT
```

show crl settings - display the CRL settings for a CA

When you execute this command, the information you see should be similar to what is shown here.

Syntax: **show crl settings <ca name>**

For example:

```
DemoBox# show crl settings k460.ca  
  CA Name: k460.ca  
  CDP:  
  Username:  
  Next Update: Apr 5 00:23:21 2011 GMT
```

show crl status - display the general information associated with a CRL

General information includes:

- complete DN of the issuer
- last update and next update value for the CRL.
- signature algorithm for the CRL.

Syntax: **show crl status <ca name>**

For example:

```
DemoBox (config)# show crl status Local_CA
Issuer (DN): /C=US/ST=CA/L=RWC/O=hdfsg/OU=gsga/CN=comm/emailAddress=ho@on.com
Version: 2 (0x1)
Last Update: Apr 21 17:55:25 2011 GMT
Next Update: Oct 10 10:10:10 2011 GMT
Signature Algorithm: sha1WithRSAEncryption

Signature Data:
3c:3a:94:a7:6b:49:e8:76:89:f7:c4:7c:89:91:55:ec:7c:55:
56:64:31:b2:56:15:db:e8:6c:62:77:9e:b2:f5:a2:13:c0:47:
1a:a5:01:d7:e2:40:67:1c:99:9c:87:d7:ac:0a:2a:90:5f:cc:
12:70:92:dd:71:86:64:00:82:c6:b5:39:61:8a:92:6e:17:54:
eb:76:d8:89:a2:e5:5b:63:a4:b4:bb:21:a4:f2:4b:0c:48:98:
23:b3:f1:7e:b7:7f:1a:92:0c:9c:66:36:a7:0e:86:51:47:6c:
df:9b:49:b8:21:74:37:27:35:d1:e6:6c:30:dc:83:29:56:ac:
86:d6:cc:f3:fa:57:d7:b7:f3:11:89:14:9b:2e:96:90:b3:30:
12:f0:cd:76:6f:af:da:6f:4c:17:d8:7d:c1:e1:a8:77:50:c7:
da:c8:96:f5:37:8a:20:42:b5:30:52:f3:2e:e5:b4:97:5f:0b:
97:83:0c:cd:ad:af:10:7c:43:dd:25:5e:b8:a3:84:1c:c2:67:
96:82:f5:c1:88:74:e5:ce:bc:76:37:bb:d6:d9:be:b2:d2:77:
00:f6:f3:cf:d3:60:b0:c7:5a:93:c9:27:af:72:b8:55:b2:07:
25:10:cf:61:60:c2:ed:70:1b:fd:94:50:b6:b3:4c:a5:56:5b:
5e:bd:9b:1c
```

Chapter 8

Cluster Configuration

Using the CLI, you can:

- view and configure the local IP and port used for the device's cluster settings (`show cluster settings`, `cluster settings`)

To join or remove a device from a cluster, you must use the Management Console.

cluster settings - change the cluster's IP and port

Syntax: **cluster settings**

For example:

```
DemoBox (config)# cluster settings
Available IP addresses:
    1. 172.17.17.120
Local IP (1-1)[1]:1
Local Port [9001]: 9001
Successfully changed Cluster Settings
```

When the device is not in a cluster, you cannot change the cluster settings.

```
DemoBox (config)# cluster settings
This device doesn't belong to a cluster.
```

show cluster settings - view the local IP and port used by the cluster

Syntax: **show cluster settings**

For example:

```
DemoBox# show cluster settings
Local IP:    172.17.17.120
Local Port:  9001
```

If the device does not belong to a cluster, No values are returned.

```
DemoBox# show cluster settings
This device doesn't belong to a cluster.
```

Chapter 9

Date & Time Configuration

Using the CLI, you can:

- configure and view the device's date and time settings (`show clock`, `clock set`, `timezone set`)
- synchronization with ntp servers (`ntp synchronize`)
- view and configure ntp settings (`show ntp`, `ntp`, `no ntp server`)

clock set - set the date, time and timezone for the device

Syntax: **clock set** <mm/dd/yy> <hh:mm:ss> <timezone>

For example:

```
DemoBox (config)# clock set 12/14/2010 14:45:58 PST
```

To return the list of valid time zone abbreviations, type `timezone set help`.

You must use one of the following time zone abbreviations, otherwise you'll see an error.

Abbreviation	Description
SST	Samoa Time Zone
HST, HDT	Hawaii Time Zone
HAST, HADT	Aleutian Time Zone
AKST, AKDT	Alaska Time Zone
PST, PDT	Pacific Time Zone
AZST, AZDT	Arizona Time Zone
MST, MDT	Mountain Time Zone
SASK	Saskatchewan Time Zone
CST, CDT	Central Time Zone
ISST, ISDT	Indiana Starke Time Zone
IEST, IEDT	Indiana East Time Zone
EST, EDT	Eastern Time Zone
AST, ADT	Atlantic Time Zone
NST, NDT	Newfoundland Time Zone
BRT, BRST	Brasilia Time Zone
AMT, AMST	Amazon Time Zone
ACT	Acre Time Zone
GMT	Greenwich Mean Time
IRISH	Irish Time Zone
BST	British Time Zone
WET, WEST	Western Europe Time Zone
CET, CEST	Central Europe Time Zone
EET, EEST	Eastern Europe Time Zone
IST, IDT	Israel Time Zone
SAST	South Africa Time Zone

MSK, MSD	Moscow Time Zone
GST	Gulf Time Zone
INDIA	India Time Zone
JAVT, WIB	Western Indonesia Time Zone
BORT, WITA	Central Indonesia Time Zone
JAYT, WIT	Eastern Indonesia Time Zone
HKT	Hong Kong Time Zone
JST	Japan Time Zone
KST	Korea Time Zone
AWST	Australian Western Time Zone
ACST	Australian Central Time Zone (Northern Terr.)
ACDT	Australian Central Time Zone (South Aust.)
AEDT	Australian Eastern Time Zone (ACT, NSW, Vic.)
AEST	Australian Eastern Time Zone (Queensland)

Note: The abbreviations for the IRISH and INDIA time zones are not standard. Normally, they are IST; however, because IST is also used for the Israel time zone, the alternate abbreviations are necessary for the Irish and India time zones to eliminate ambiguity.

no ntp server - delete an NTP server from the list

There can be at most three ntp servers configured.

Syntax: **no ntp server <ip>**

For example:

```
DemoBox (config)# no ntp server 172.20.1.149
NTP server successfully removed
```

ntp - enable and disable NTP, add NTP servers. and set the polling interval

Syntax: **ntp**

For example:

```
DemoBox (config)# ntp
Enable NTP [n]: y
NTP Server 1 [None]: 172.20.1.150
NTP Server 2 [None]: 172.20.1.149
NTP Server 3 [None]: 172.20.1.106
Poll Interval (min) [30]: 20
```

NTP settings successfully saved

ntp synchronize - immediately synchronize the device clock with the NTP server

Synchronization adjust the time and date only. It does not change the timezone.

Syntax: **ntp synchronize**

For example:

```
DemoBox (config)# show clock
01/01/2010 08:08:34 Eastern Time Zone
```

```
DemoBox (config)# ntp synchronize
Successfully stepped time by 30190404.000000 seconds using server 172.17.34.149
```

```
DemoBox (config)# show clock
12/16/2010 18:22:14 Eastern Time Zone
```

show clock - view the current date, time, and time zone on the device

Syntax: **show clock**

For example:

```
DemoBox# show clock
12/14/2010 14:39:42 Pacific Time Zone
```

show ntp - show the NTP settings

Syntax: **show ntp**

For example:

```
DemoBox# show ntp
  Enable NTP:                no
  NTP Server 1:              [None]
  NTP Server 2:              [None]
  NTP Server 3:              [None]
  Poll Interval (min):       30
```

timezone set - set the timezone

Syntax: **timezone set**

For example:

```
DemoBox (config)# timezone set EST
DemoBox (config)# show clock
12/14/2010 17:51:23 Eastern Time Zone
```

To return the list of valid timezone abbreviations, type `timezone set help`. Otherwise see the list above.

Chapter 10

Health Check Configuration

Using the CLI, you can:

- view, enable, and configure the health check feature (`show health check`, `health check`)

health check - enable and configure the health check feature

Syntax: **health check**

For example:

```
DemoBox (config)# health check
Enable Health Check [n]: y
Local IP:
    1: All
    2: 172.17.7.29
Enter a number (1 - 2) [1]: 1
Local Port [9080]: 9080
Health check settings successfully saved. Health check is enabled.
```

show health check - view the health check settings

Syntax: **show health check**

For example:

```
DemoBox# show health check
    Enable Health Check:    no
    Local IP:               [All]
    Local Port:             9080
```

Chapter 11

Help

Using the CLI, you can:

- view the list of help categories or show the list of commands for a specific help category (`help`)

help - view the list of help categories or show the list of commands for a specific help category

Syntax: **help**
help <alias>

For example:

```
DemoBox (config)# help
```

The commands available in Config Mode are grouped under the following categories:

Alias	Category
mode	Mode Changes
datetime	Date & Time Configuration
network	Network Configuration
nae	NAE Server Configuration
snmp	SNMP Configuration
admin	Administrator Configuration
healthcheck	Health Check Configuration
ssl	SSL Configuration
cert	Certificate Configuration
ca	Certificate Authority Configuration
crl	Certificate Revocation List Configuration
cluster	Cluster
security	Security
enterprise	Enterprise Manager Configuration
log	Log Configuration
logview	Log Viewing & Rotation
protectfile	ProtectFile
stats	Statistics
backup	Backup & Restore
services	Services
sysinfo	System Information & Upgrade
health	System Health
diag	Network Diagnostics
auto	Auto-logout
history	History
help	Help

```
DemoBox (config)# help datetime
  show clock
  show ntp
  clock set <mm/dd/yy> <hh:mm:ss> <timezone>
  timezone set <timezone>
  ntp
  no ntp server <ip>
  ntp synchronize
```

Note: The results of the `help <alias>` command differ depending on which CLI mode you are using (view or config). For example, here is `help datetime` in view mode:

```
DemoBox# help datetime
  show clock
  show ntp
```

Chapter 12

History

Using the CLI, you can:

- view the history of commands executed by the current administrator during the current session (`history`)

history - view the history of commands executed by the current administrator during the current session

Syntax: **history**

For example:

```
DemoBox# history
1 config
2 ntp
3 show clock
4 no ntp server
5 no ntp server 172.20.1.149
6 show ntp
7 show clock
8 ntp synchronize
9 ping 172.20.1.150
10 traceroute 172.20.1.150
11 ntp
12 show clock
13 set clock
14 clock set 04/18/2009 10:10:10 HKT
15 show clock
16 ntp synchronize
17 show clock
18 show nae-server settings
19 nae-server settings
20 show health check
21 health check
22 show cluster settings
23 cluster settings
24 show cluster settings
25 cluster settings
26 show cluster settings
```

Chapter 13

HSM Configuration

Using the CLI, you can:

- initialize the hsm - this involves (hsm initialize, hsm create partition, hsm generate certificates, hsm set password)
- log in and log out as the hsm crypto user (hsm login crypto user, hsm logout crypto user)
- log in and log out as the hsm security officer (hsm login security officer, hsm logout security officer)
- view hsm status (show hsm status)
- view hsm configuration information (hsm show info)
- set the auto-activation feature (hsm auto-activation)
- initialize and connect to the remote PED (hsm remote ped init, hsm remote ped connect)

hsm auto-activation - enable or disable the auto-activation feature

Syntax: **hsm auto-activation** <on|off>

For example:

```
DemoBox (config)# hsm auto-activation on  
'partition changePolicy' successful.
```

```
Policy "Allow auto-activation" is now set to: 1
```

```
Notice: Auto activation parameters will be stored during next activation.  
It is recommended you activate this partition now.
```

Note: To activate the partition, log in as the crypto user after running this command.

hsm create partition - create a partition on the hsm

Syntax: **hsm create partition**

For example:

```
DemoBox (config)# hsm create partition
```

```
Please ensure that you copy the password from the Luna PED and that you keep it  
in a safe place.
```

```
Luna PED operation required to create a partition - use User or Partition Owner  
(black) PED key.
```

```
Luna PED operation required to generate cloning domain on the partition - use  
Domain (red) PED key.
```

```
'partition create' successful.
```

hsm generate certificates - generate the certificates used by the sskm and the KeySecure to communicate with the hsm

Syntax: **hsm generate certificates**

For example:

```
DemoBox (config)# hsm generate certificates
HSM private link parameters:
    Server IP: 192.168.187.214/24
    Client IP: 192.168.187.219/24
Checking for any internal-external IP conflicts with HSM private network...
Would wait for ping reply for each IP for max 3 seconds...
No conflicts with HSM private network
Gathering state.....
HSM link set with Server-IP: 192.168.187.214/24

/usr/local/ingrian/watched/bin/luna_regen_cert.sh successful. NTLS must be
(re)started before clients can connect.

Server Cert Gen succeeded, rc=0
copying server cert to local client
copying server cert to remote client

Bind succeeded, rc=0

watcher restart succeeded, rc=0

Client configuration file must be in /etc/saclient/Chrystoki.conf
Exporting the env variable ChrystokiConfigurationPath=/etc/saclient/

Private Key created and written to: /usr/lunasa/cert/client/
192.168.187.219Key.pem
Certificate created and written to: /usr/lunasa/cert/client/192.168.187.219.pem
Remote client 192.168.187.219 cert gen succeeded, rc=0

Private Key created and written to: /usr/lunasa/cert/client/
192.168.187.214Key.pem
Certificate created and written to: /usr/lunasa/cert/client/192.168.187.214.pem
Local client 192.168.187.214 cert gen succeeded, rc=0

New server 192.168.187.214 successfully added to server list.

addServer 192.168.187.214 succeeded, rc=0
Force option used. All proceed prompts bypassed.

'client register' successful.

Local client 192.168.187.214 cert registration succeeded, rc=0
Force option used. All proceed prompts bypassed.

'client register' successful.

Remote client 192.168.187.219 cert registration succeeded, rc=0
'client assignPartition' successful.

Partition default assignment to local_hsm_client succeeded, rc=0
'client assignPartition' successful.
```



```
Partition default assignment to remote_hsm_client succeeded, rc=0
watcher restart succeeded, rc=0
HSM certificates generated successfully
Waiting till HSM environment updates.....
HSM environment updated successfully
Applications would be able to use HSM when crypto-user logs-in
```

If a conflict occurs between your external network and the hsm's private network, the command displays a message and enables you to change the hsm's network settings.

Note: Prior to running this command, SSKM must be shut down and the Crypto User must be logged out. You can do this manually using the `sskm halt` and `hsm logout crypto user` commands.

hsm initialize - initialize the hsm

This command requires that the security officer iKey (blue) and the domain iKey (red) be inserted in the PED.

Syntax: **hsm initialize**

For example:

```
DemoBox (config)# hsm initialize
```

```
Luna PED operation required to initialize HSM - use Security Officer (blue) PED key.
```

```
Luna PED operation required to login as HSM Administrator - use Security Officer (blue) PED key.
```

```
Luna PED operation required to generate cloning domain - use Domain (red) PED key.
```

```
'hsm init' successful.
```

hsm login crypto user - login as the hsm crypto user

This command requires that the black iKey be inserted in the ped.

Syntax: **hsm login crypto user**

For example:

```
DemoBox (config)# hsm login crypto user
Crypto user successfully logged into the HSM
```

hsm login security officer - login as the hsm security officer

This command requires that the blue iKey be inserted in the ped.

Syntax: **hsm login security officer**

For example:

DemoBox (config)# **hsm login security officer**

Luna PED operation required to login as HSM Administrator - use Security Officer (blue).

'hsm login' successful.

hsm logout crypto user - logout as the hsm crypto user

Syntax: **hsm logout crypto user**

For example:

DemoBox (config)# **hsm logout crypto user**

Are you sure, you want to log-out?

Logging-Out could make applications using HSM to fail
yes/no?

yes

Logged out of HSM partition successfully

Important! To log out, you must enter **yes**. The CLI does not accept **y**.

hsm logout security officer - logout as the security officer

Syntax: **hsm logout security officer**

For example:

DemoBox (config)# **hsm logout security officer**

'hsm logout' successful.

hsm remote ped connect - connect to the remote ped

The ped must first be initialized. After running this command, the orange Remote PED iKey must be inserted into the remote PED within 480 seconds, otherwise the command will fail.

Syntax: **hsm remote ped connect <ip> <port>**

For example:

DemoBox (config)# **hsm remote ped connect 172.17.40.247 1503**

Luna PED operation required to connect to Remote PED - use orange PED key.

Ped Client Version 1.0.5 (10005)

Ped Client launched in forced startup mode.

Ped Client is not currently running.

Shutdown passed.

Ped Client launched in startup mode.

Starting background process

Background process started

Ped Client Process created, exiting this process.

hsm remote ped init - initialize the remote PED

Prior to running this command, you must have installed and configured the PED on a device running Windows XP. For more information on this, see the *KeySecure User Guide*.

Syntax: **hsm remote ped init**

For example:

```
DemoBox (config)# hsm remote ped init
Luna PED operation required to initialize remote PED key vector - use orange PED
key(s).

Ped Client Version 1.0.5 (10005)
Ped Client launched in shutdown mode.
Shutdown passed.
```

hsm set password - input the hsm password

The password is displayed at the ped after reading the domain (red) iKey) during the hsm initialization.

Syntax: **hsm set password <password>**

For example:

```
DemoBox (config)# hsm set password xdE3-ENGs-xE79-4XKq
```

hsm show info - view the hsm configuration information including the firmware, remote ped vector (rpv) status, partition name, and storage usage

Syntax: **hsm show info**

For example:

```
DemoBox# hsm show info

HSM Details:
=====
HSM Label:                " "
Serial #:                  150170
Firmware:                  6.0.8
Hardware Model:            Luna K6
Authentication Method:     PED keys
HSM Admin login status:    Logged In
HSM Admin login attempts left: 3 before HSM zeroization!
RPV Initialized:           Yes
Manually Zeroized:         No

Partitions created on HSM:
=====
Partition: 150170008,      Name: default

FIPS 140-2 Operation:
```

```
=====
The HSM is NOT in FIPS 140-2 approved operation mode.
HSM Storage Information:
=====
Maximum HSM Storage Space (Bytes):    2097152
Space In Use (Bytes):                  2097152
Free Space Left (Bytes):                0
```

show hsm status - view the status of the hsm

Possible statuses are:

- Initialized - the hsm has been initialized and is ready for use.
- Partition created but missing certificates - the hsm has been initialized, the partition created, but the certificates have not been created
- Initialized without partition - the hsm has been initialized, but a partition has not been created
- Uninitialized - the hsm has not been initialized

This command also checks that the internal private network used by the hsm does not conflict with your organization's external network.

Syntax: **show hsm status**

For example:

```
DemoBox# show hsm status
HSM Status:      Initialized
Crypto-user logged in: yes
HSM private link parameters:
    Server IP: 192.168.187.214/24
    Client IP: 192.168.187.219/24
Checking for any internal-external IP conflicts with HSM private network...
Will wait for ping reply for each IP for max 3 seconds...
No conflicts with HSM private network.
```

If a conflict occurs between your external network and the hsm's private network, the command displays one of the following messages:

```
Default gateway 172.25.18.3 conflicts with HSM server IP on private network
Host 172.25.18.21 conflicts with the HSM server IP on private network
It may not be able to access this device
```

If either of these errors occur, you must run the `hsm generate certificates` command to reconfigure the hsm's private network. For more information, consult the release notes.

hsm enable secure-key-cache - start applying the key-caching functions

Secure key caching improves performance by providing faster access to the managed keys on i460 and k460 platforms, while maintaining security. In SafeNet test environments, some key management operations ran 2 -3 times faster when key caching was enabled.

Secure key caching stores the HSM master keys in the process memory of internal servers. To ensure security, these keys are obfuscated, and they are never swapped to disk. On a KeySecure, only the HSM keys that are specific to KeySecure VM are cached; SSKM VM keys are not.

You do not violate FIPS requirements by enabling secure-key-caching.

Note: This setting is not replicated across a cluster; it must be set via CLI for each node in the cluster, if needed.

For this command to work, the crypto user must be logged in.

Note the following characteristics regarding secure-key-caching:

- Secure key caching is available only on k460 and i460 platforms. The two related CLI commands, `hsm disable secure-key-cache` and `hsm disable secure-key-cache`, should not be used with the i150, k150 or i450 platforms.
- Even though the master keys are cached, the master keys are not available for use when the crypto user is logged out. So, the system behavior is the same as without secure key caching.
- When a box is freshly imaged, it will start with secure-key-caching disabled by default.
- The secure-key-caching configuration is not maintained by Backup or Restore capabilities.
- If Reset Factory Setting (RFS) or Restore Default Configuration (RDC) is run, secure key caching will be disabled, by default: keys will no longer be cached.

You can discover the current state of the secure-key-cache by using `show hsm status`. For example:

```
DemoBox# show hsm status
HSM Status:      Initialized
Crypto-user logged in: yes
HSM secure-key-cache: Enabled
```

When you run the this command, the response tells you if it failed or succeeded, or if it is already in the state requested by the command. For example:

Here is confirmation of a successful use of `enable secure-key-cache`:

```
DemoBox# hsm enable secure-key-cache
Successfully enabled HSM secure-key-cache.
```

Here is the result when secure-key-caching is already enabled:

```
DemoBox# hsm enable secure-key-cache
HSM secure-key-cache is already enabled.
```

hsm disable secure-key-cache - stop the key-caching functions

Secure key caching improves performance by providing faster access to the managed keys on i460 and k460 platforms, while maintaining security. In SafeNet test environments, some key management operations ran 2 -3 times faster when key caching was enabled.

Secure key caching stores the HSM master keys in the process memory of internal servers. To ensure security these keys are obfuscated, and they are never swapped to disk. On a KeySecure, only the HSM keys that are specific to KeySecure VM are cached; SSKM VM keys are not.

You do not violate FIPS requirements by enabling secure-key-caching.

Note: This setting is not replicated across a cluster; it must be set via CLI for each node in the cluster if needed.

For this command to work, the crypto user must be logged in. This command, `disable secure-key-cache`, complements `enable secure-key-cache`.

Note the following characteristics regarding secure-key-caching:

- Secure key caching is available only on k460 and i460 platforms. The two related CLI commands, `hsm disable secure-key-cache` and `hsm disable secure-key-cache`, should not be used with the i150, k150 or i450 platforms.
- Even though the master keys are cached, the master keys are not available for user when the crypto user is logged out. So, the system behavior is the same as without secure key caching.
- When a box is freshly imaged, it will start with secure-key-caching disabled by default.
- The secure-key-caching configuration is not maintained by Backup or Restore capabilities.
- If Reset Factory Setting (RFS) or Restore Default Configuration (RDC) is run, secure key caching will be disabled, by default: keys will no longer be cached.

You can discover the current state of the secure-key-cache by using `show hsm status`. For example:

```
DemoBox# show hsm status
HSM Status:      Initialized
Crypto-user logged in: yes
HSM secure-key-cache: Enabled
```

When you run the this command, the response tells you if it failed or succeeded, or if it is already in the state requested by the command. For example:

Here is confirmation of a successful use of `disable secure-key-cache`:

```
DemoBox# hsm disable secure-key-cache
Successfully disabled HSM secure-key-cache.
```

Here is the result when secure-key-caching is already disabled:

```
DemoBox# hsm disable secure-key-cache
HSM secure-key-cache is already disabled.
```

Chapter 14

Log Configuration

Using the CLI, you can:

- view and set the audit log level (audit log level, show audit log level)
- view and configure log rotation settings for all logs (show log rotation, edit log rotation)
- view and recreate the log signing certificate (show logsigning certificate, recreate logsigning certificate)
- view and configure log signing for all logs (show log signing, log signing)
- show and configure log levels for the activity and sql logs (show activity log level, activity log level, show sql log level, sql log level)
- view, configure, and erase syslog settings for all logs (show system syslog, show audit syslog, show activity syslog, show clientevent syslog, show dbencrypt syslog, show sql syslog, show failover syslog, system syslog, audit syslog, activity syslog, clientevent syslog, dbencrypt syslog, sql syslog, failover syslog, no system syslog, no audit syslog, no activity syslog, no client syslog, no dbencrypt syslog, no sql syslog, no failover syslog)

activity log level - set the activity log level

Syntax: **activity log level**

For example:

```
DemoBox (config)# activity log level
Log Level:
    1: Normal
    2: Low
Enter a number (1 - 2) [1]: 2
Activity Log settings successfully saved.
```

activity syslog - enable the device to use the syslog protocol to send activity log messages to an external machine

Syntax: **activity syslog**

For example:

```
DemoBox (config)# activity syslog
Enable Syslog [n]: y
Syslog Server #1 IP: 172.168.18.51
Syslog Server #1 Port [514]: 514
Server #1 Proto:
```

```
1. udp
2. tcp
Enter a number (1 - 2) [1]: 1
Syslog Server #2 IP: 10.20.15.81
Syslog Server #2 Port [514]: 514
Server #2 Proto:
1. udp
2. tcp
Enter a number (1 - 2) [1]: 1
Syslog Facility:
1: local0
2: local1
3: local2
4: local3
5: local4
6: local5
7: local6
8: local7
Enter a number (1 - 8) [2]: 2
Activity Log syslog settings successfully saved. Syslog is enabled.
Warning: The syslog protocol insecurely transfers logs in cleartext
```

audit log level - set the audit log level

Syntax: **audit log level**

For example:

```
DemoBox (config)# audit log level
Please pick one of the following log levels:
1) Maximum
2) Medium
2) Minimum
Log Level (1-3): 2
Audit log level successfully set.
```

audit syslog - enable the device to use the syslog protocol to send audit log messages to an external machine

Syntax: **audit syslog**

For example:

```
DemoBox (config)# audit syslog
Enable Syslog [n]: y
Syslog Server #1 IP: 172.168.18.51
Syslog Server #1 Port [514]: 514
Server #1 Proto:
1. udp
2. tcp
Enter a number (1 - 2) [1]: 1
```



```
Syslog Server #2 IP: 10.20.15.81
Syslog Server #2 Port [514]: 514
Server #2 Proto:
  1. udp
  2. tcp
```

```
Enter a number (1 - 2) [1]: 1
```

```
Syslog Facility:
  1: local0
  2: local1
  3: local2
  4: local3
  5: local4
  6: local5
  7: local6
  8: local7
```

```
Enter a number (1 - 8) [2]: 2
```

```
Audit Log syslog settings successfully saved. Syslog is enabled.
Warning: The syslog protocol insecurely transfers logs in cleartext
```

clientevent syslog - enable the device to use the syslog protocol to send client event log messages to an external machine

Syntax: **clientevent syslog**

For example:

```
DemoBox (config)# clientevent syslog
Enable Syslog [n]: y
Syslog Server #1 IP: 172.168.18.51
Syslog Server #1 Port [514]: 514
Server #1 Proto:
  1. udp
  2. tcp
```

```
Enter a number (1 - 2) [1]: 1
```

```
Syslog Server #2 IP: 10.20.15.81
Syslog Server #2 Port [514]: 514
Server #2 Proto:
  1. udp
  2. tcp
```

```
Enter a number (1 - 2) [1]: 1
```

```
Syslog Facility:
  1: local0
  2: local1
  3: local2
  4: local3
  5: local4
  6: local5
  7: local6
  8: local7
```

```
Enter a number (1 - 8) [2]: 2
```

```
Client Event Log syslog settings successfully saved. Syslog is enabled.
```

Warning: The syslog protocol insecurely transfers logs in cleartext

dbencrypt syslog - enable the device to use the syslog protocol to send database encryption log messages to an external machine

Syntax: **dbencrypt syslog**

For example:

```
DemoBox (config)# dbencrypt syslog
Enable Syslog [n]: y
Syslog Server #1 IP: 172.168.18.51
Syslog Server #1 Port [514]: 514
Server #1 Proto:
    1. udp
    2. tcp
Enter a number (1 - 2) [1]: 1
Syslog Server #2 IP: 10.20.15.81
Syslog Server #2 Port [514]: 514
Server #2 Proto:
    1. udp
    2. tcp
Enter a number (1 - 2) [1]: 1
Syslog Facility:
    1: local0
    2: local1
    3: local2
    4: local3
    5: local4
    6: local5
    7: local6
    8: local7
Enter a number (1 - 8) [2]: 2
Database Encryption Log syslog settings successfully saved. Syslog is enabled.
Warning: The syslog protocol insecurely transfers logs in cleartext
```

edit log rotation <log name> - edit the log rotation settings for the specified log

Syntax: **edit log rotation <log name>**

For example:

```
DemoBox (config)# edit log rotation activity
Please pick one of the following rotation schedules:
    1) Daily      2) Weekly      3) Monthly
Rotation Schedule [1]: 1
Enter the time (HH:MM) for log rotation to occur: 02:33
Enter the num logs archived: 6
Enter the max log file size (MB): 75
Please pick one of the following types of transfer:
    1) None      2) FTP      3) SCP
```

```
Transfer Type [1]: 3
Enter the host: 127.18.32.9
Enter the directory: /activity
Enter the username: host-user
Enter the password:
Successfully edited log configuration.
```

failover syslog - enable the device to use the syslog protocol to send failover log messages to an external machine

Syntax: **failover syslog**

For example:

```
DemoBox (config)# failover syslog
Enable Syslog [n]: y
Syslog Server #1 IP: 172.168.18.51
Syslog Server #1 Port [514]: 514
Server #1 Proto:
    1. udp
    2. tcp
Enter a number (1 - 2) [1]: 1
Syslog Server #2 IP: 10.20.15.81
Syslog Server #2 Port [514]: 514
Server #2 Proto:
    1. udp
    2. tcp
Enter a number (1 - 2) [1]: 1
Syslog Facility:
    1: local0
    2: local1
    3: local2
    4: local3
    5: local4
    6: local5
    7: local6
    8: local7
Enter a number (1 - 8) [2]: 2
Failover Log syslog settings successfully saved. Syslog is enabled.
Warning: The syslog protocol insecurely transfers logs in cleartext
```

log signing - enable the secure log feature for a given log

Syntax: **log signing <log name>**

For example:

```
DemoBox (config)# log signing Audit
Sign Log [y]: y
```

no activity syslog - disable the use of the syslog protocol to send activity log messages to an external machine and clear all values in the activity log settings

Syntax: **no activity syslog**

For example:

```
DemoBox (config)# no activity syslog  
Activity Log syslog settings cleared. Syslog is disabled.
```

no audit syslog - disable the use of the syslog protocol to send audit log messages to an external machine and clear all values in the audit log settings

Syntax: **no audit syslog**

For example:

```
DemoBox (config)# no audit syslog  
Audit Log syslog settings cleared. Syslog is disabled.
```

no clientevent syslog - disable the use of the syslog protocol to send client event Log messages to an external machine and clear all values in the client event log settings

Syntax: **no clientevent syslog**

For example:

```
DemoBox (config)# no clientevent syslog  
Client Event Log syslog settings cleared. Syslog is disabled.
```

no dbencrypt syslog - disable the use of the syslog protocol to send database encryption log messages to an external machine and clear all values in the database encryption log settings

Syntax: **no dbencrypt syslog**

For example:

```
DemoBox (config)# no dbencrypt syslog  
Database Encryption Log syslog settings cleared. Syslog is disabled.
```

no failover syslog - disable the use of the syslog protocol to send failover log messages to an external machine

Syntax: **no failover syslog**

For example:

```
DemoBox (config)# no failover syslog  
Failover Log syslog settings cleared. Syslog is disabled.
```

no sql syslog - disable the use of the syslog protocol to send sql log messages to an external machine and clear all values in the sql log settings

Syntax: **no sql syslog**

For example:

```
DemoBox (config)# no sql syslog  
SQL Log syslog settings cleared. Syslog is disabled.
```

no system syslog - disable the use of the syslog protocol to send system log messages to an external machine and clear all values in the system log settings

Syntax: **no system syslog**

For example:

```
DemoBox (config)# no system syslog  
System Log syslog settings cleared. Syslog is disabled.
```

recreate logsigning certificate - recreate the log signing certificate

Syntax: **recreate logsigning certificate** create a cert with the default duration of 365 days
recreate logsigning certificate <days> creates a cert with the specified duration

For example:

```
DemoBox (config)# recreate logsigning certificate  
Backup old log signing certificates for verifying previously signed logs  
Are you sure you want to recreate the logsigning cert? [n]: y  
Warning: Logs transferred in the future will be signed with the new cert  
Log Signing certificate successfully recreated.
```

```
DemoBox (config)# recreate logsigning certificate 30  
Backup old log signing certificates for verifying previously signed logs  
Are you sure you want to recreate the logsigning cert? [n]: y  
Warning: Logs transferred in the future will be signed with the new cert  
Log Signing certificate successfully recreated.
```

show activity log level - view the activity log level

Syntax: **show activity log level**

For example:

```
DemoBox# show activity log level  
Log Level: Normal
```

show activity syslog - display the syslog settings for the activity log

Syntax: **show activity syslog**

For example:

```
DemoBox# show activity syslog
  Enable Syslog:          yes
  Syslog Server #1 IP:    172.17.6.121
  Syslog Server #1 Port:  514
  Syslog Server #2 IP:    172.17.6.2
  Syslog Server #2 Port:  514
  Syslog Facility:        local7
```

show audit log level - display the current audit log level

Syntax: **show audit log level**

For example:

```
DemoBox# show audit log level
The audit log level is Medium
```

show audit syslog - display the syslog settings of the audit log

Syntax: **show audit syslog**

For example:

```
DemoBox# show audit syslog
  Enable Syslog:          yes
  Syslog Server #1 IP:    172.17.6.121
  Syslog Server #1 Port:  514
  Syslog Server #2 IP:    172.17.6.2
  Syslog Server #2 Port:  514
  Syslog Facility:        local6
```

show clientevent syslog - display the syslog settings for the client event log

Syntax: **show clientevent syslog**

For example:

```
DemoBox# show clientevent syslog
  Enable Syslog:          yes
  Syslog Server #1 IP:    172.17.6.121
  Syslog Server #1 Port:  514
  Syslog Server #2 IP:    172.17.6.2
  Syslog Server #2 Port:  514
  Syslog Facility:        local5
```

show dbencrypt syslog - display the syslog settings for the database encryption log

Syntax: **show dbencrypt syslog**

For example:

```
DemoBox# show dbencrypt syslog
  Enable Syslog:      yes
  Syslog Server #1 IP: 172.17.6.121
  Syslog Server #1 Port: 514
  Syslog Server #2 IP: 172.17.6.2
  Syslog Server #2 Port: 514
  Syslog Facility:    local5
```

show failover syslog - display the syslog settings for the failover log

Syntax: **show failover syslog**

For example:

```
DemoBox# show failover syslog
  Enable Syslog:      yes
  Syslog Server #1 IP: 172.17.6.121
  Syslog Server #1 Port: 514
  Syslog Server #2 IP: 172.17.6.2
  Syslog Server #2 Port: 514
  Syslog Facility:    local6
```

show log rotation - either show all the current logs and some general information on them, or specify a log name to see the detailed settings for the specified log

Syntax: **show log rotation**
show log rotation <log name>

For example:

```
DemoBox# show log rotation
```

Log Name	Rotation Schedule	Num Logs Archived / Max File Size (MB)	Transfer Dest
System	Weekly 03:15 Sun	6 / 100	None
Audit	Weekly 03:15 Sun	6 / 100	None
Activity	Daily 03:05	4 / 100	None
Client Event	Daily 03:05	4 / 100	None

```
DemoBox# show log rotation system
Rotation Schedule:    Weekly on Sunday
Rotation Time:        03:15
Num Logs Archived:    6
Max Log File Size (MB): 100
```

Transfer Type: None
Host: None
Directory: None
Username: None
Password: None

show log signing - see whether the secure log feature is enabled for a given log

Syntax: **show log signing <log name>**

For example:

```
DemoBox# show log signing system
Log Name:      System
Sign Log:      yes
```

show logsigning certificate - show the log signing certificate

Syntax: **show logsigning certificate**

For example:

```
DemoBox# show logsigning certificate
Certificate Name: logsigner
Serial Number: 0x00
Key Size: 1024
Start Date: Aug 31 21:32:02 2009 GMT
Expiration: Sep  1 21:32:02 2010 GMT

Issuer:
C=US
ST=undefined
L=undefined
O=Security Appliance
OU=Security Appliance Log Signer
CN=suchitra-18
emailAddress=logsigner@user-18

Subject:
C=US
ST=undefined
L=undefined
O=Security Appliance
OU=Security Appliance Log Signer
CN=suchitra-18
emailAddress=logsigner@user-18

Purpose:
SSL client & CA
SSL server & CA
Netscape SSL server & CA
S/MIME signing CA
S/MIME encryption CA
```


CRL signing & CA

```
-----BEGIN CERTIFICATE-----
MIIDBzCCAnCgAwIBAgIBADANBgkqhkiG9w0BAQUFADCbt jELMAkGA1UEBhMCVVMx
EjAQBgNVBAGTCXVuZGVmaW5lZDESMBAGA1UEBxMJdW5kZWZpbmVkbMRswGQYDVQQK
ExJTZW51cm10eSBBcHBsaWFnY2UxJjAkBgNVBAsTHVnlY3VyaXR5IEFwcGxpYW5j
ZSBMb2cgU2lnbmVybWQwEgYDVQQDEwtzdWNoaXRyYS0xODEkMCIGCSqGSIb3DQEJ
QwYqr3YBp+ZH08DgMnXVvkQqN1vBSdpq+eaU/v8AbX2zcBw0YHylRQhQfVjfMI0G
G1o4Yeq9XnZXLYk=
-----END CERTIFICATE-----
```

show sql log level - show the log level for the sql log

Syntax: **show sql log level**

For example:

```
DemoBox# show sql log level
      Log Level: Normal
```

show sql syslog - display the syslog setting for the sql log

Syntax: **show sql syslog**

For example:

```
DemoBox# show sql syslog
      Enable Syslog:          yes
      Syslog Server #1 IP:    172.17.6.121
      Syslog Server #1 Port:  514
      Syslog Server #2 IP:    172.17.6.2
      Syslog Server #2 Port:  514
      Syslog Facility:        local5
```

show system syslog - display the syslog settings for the system log

Syntax: **show system syslog**

For example:

```
DemoBox# show system syslog
      Enable Syslog:          yes
      Syslog Server #1 IP:    172.17.6.121
      Syslog Server #1 Port:  514
      Syslog Server #2 IP:    172.17.6.2
      Syslog Server #2 Port:  514
      Syslog Facility:        local5
```

sql log level - set the sql log level

Syntax: **sql log level**

For example:

```
DemoBox (config)# sql log level
Log Level:
    1: Debug
    2: Normal
    3: Low
Enter a number (1 - 3) [2]: 1
SQL Log settings successfully saved.
```

sql syslog - enable the device to use the syslog protocol to send sql log messages to an external machine

Syntax: **sql syslog**

For example:

```
DemoBox (config)# sql syslog
Enable Syslog [n]: y
Syslog Server #1 IP: 172.168.18.51
Syslog Server #1 Port [514]: 514
Server #1 Proto:
    1. udp
    2. tcp
Enter a number (1 - 2) [1]: 1
Syslog Server #2 IP: 10.20.15.81
Syslog Server #2 Port [514]: 514
Server #2 Proto:
    1. udp
    2. tcp
Enter a number (1 - 2) [1]: 1
Syslog Facility:
    1: local0
    2: local1
    3: local2
    4: local3
    5: local4
    6: local5
    7: local6
    8: local7
Enter a number (1 - 8) [2]: 2
SQL Log syslog settings successfully saved. Syslog is enabled.
Warning: The syslog protocol insecurely transfers logs in cleartext
```

system syslog - enable the device appliance to use the syslog protocol to send system log messages to an external machine

Syntax: **system syslog**

For example:

```
DemoBox (config)# system syslog
Enable Syslog [n]: y
Syslog Server #1 IP: 172.168.18.51
Syslog Server #1 Port [514]: 514
Server #1 Proto:
    1. udp
    2. tcp
Enter a number (1 - 2) [1]: 1
Syslog Server #2 IP: 10.20.15.81
Syslog Server #2 Port [514]: 514
Server #2 Proto:
    1. udp
    2. tcp
Enter a number (1 - 2) [1]: 1
Syslog Facility:
    1: local0
    2: local1
    3: local2
    4: local3
    5: local4
    6: local5
    7: local6
    8: local7
Enter a number (1 - 8) [2]: 2
System Log syslog settings successfully saved. Syslog is enabled.
Warning: The syslog protocol insecurely transfers logs in cleartext
```

Chapter 15

Log Viewing & Rotation Configuration

Using the CLI, you can:

- view a list of all logs or view specific logs (show system log, show audit log, show activity log, show clientevent log, show dbencrypt log, show sql log, show failover log)
- transfer specific logs off of the device (transfer system log, transfer audit log, transfer activity log, transfer clientevent log, transfer dbencrypt log, transfer sql log, transfer failover log)
- rotate the latest log (system log rotate, activity log rotate, clientevent log rotate, dbencrypt log rotate, sql log rotate, failover log rotate)
- delete specific logs (no system log, no activity log, no clientevent log, no dbencrypt log, no sql log, no failover log)

activity log rotate - rotate the activity log

Syntax: **activity log rotate**

For example:

```
DemoBox (config)# activity log rotate  
Activity Log successfully rotated.
```

clientevent log rotate - rotate the client event log

Syntax: **clientevent log rotate**

For example:

```
DemoBox (config)# clientevent log rotate  
Client Event Log successfully rotated.
```

dbencrypt log rotate - rotate the database encryption log

Syntax: **dbencrypt log rotate**

For example:

```
DemoBox (config)# dbencrypt log rotate  
Database Encryption Log successfully rotated.
```

failover log rotate - rotate the failover log

Syntax: **failover log rotate**

For example:

```
DemoBox (config)# failover log rotate  
Failover Log successfully rotated.
```

no activity log - delete an activity log

Syntax: **no activity log** <log name>

For example:

```
DemoBox# show activity log  
Activity Log file names:  
Current  
1.2011-03-22_030501  
2.2011-03-21_030501
```

```
DemoBox# c
```

```
DemoBox (config)# no activity log 2.2011-03-21_030501  
Are you sure you want to clear the Activity Log "2.2011-03-21_030501"? [n]: y  
Activity Log "2.2011-03-21_030501" successfully cleared.
```

no clientevent log - delete a client event log

Syntax: **no clientevent log** <log name>

For example:

```
DemoBox# show clientevent log  
Client Event Log file names:  
Current  
1.2011-03-22_030501  
2.2011-03-21_030501
```

```
DemoBox# c
```

```
DemoBox (config)# no clientevent log 2.2011-03-21_030501  
Are you sure you want to clear the Client Event Log "2.2011-03-21_030501"? [n]: y  
Client Event Log "2.2011-03-21_030501" successfully cleared.
```

no dbencrypt log - delete a dbencrypt log

Syntax: **no dbencrypt log** <log name>

For example:

```
DemoBox# show dbencrypt log  
Database Encryption Log file names:  
Current  
1.2011-03-24_143527  
2.2011-03-01_032501
```

```
DemoBox# c
```

```
DemoBox (config)# no dbencrypt log 2.2011-03-01_032501
Are you sure you want to clear the Database Encryption Log "2.2011-03-01_032501"? [n]: y
Database Encryption Log "2.2011-03-01_032501" successfully cleared.
```

no failover log - delete a failover log

Syntax: **no failover log <log name>**

For example:

```
DemoBox# show failover log
Failover Log file names:
    Current
    1.2011-02-20_031501
    2.2011-02-13_031501
```

```
DemoBox# c
```

```
DemoBox (config)# no failover log 2.2011-02-13_031501
Are you sure you want to clear the Failover Log "2.2011-02-13_031501"? [n]: y
Failover Log "2.2011-02-13_031501" successfully cleared.
```

no sql log - delete a sql log

Syntax: **no sql log <log name>**

For example:

```
DemoBox# show sql log
SQL Log file names:
    Current
    1.2011-03-24_143501
    2.2011-03-01_032501
```

```
DemoBox# c
```

```
DemoBox (config)# no sql log 2.2011-03-01_032501
Are you sure you want to clear the SQL Log "2.2011-03-01_032501"? [n]: y
SQL Log "2.2011-03-01_032501" successfully cleared.
```

no system log - delete a system log

Syntax: **no system log <log name>**

For example:

```
DemoBox# show system log
System Log file names:
    Current
    1.2011-02-20_031501
    2.2011-02-13_031501
```

```
DemoBox# c
```

```
DemoBox (config)# no system log 2.2011-02-13_031501
Are you sure you want to clear the System Log "2.2011-02-13_031501"? [n]: y
System Log "2.2011-02-13_031501" successfully cleared.
```

show activity log - view an activity log

Syntax: **show activity log** for a list of all logs
show activity log <log name> for a specific log
show activity log <log name> <number of lines> for part of a log

For example:

```
DemoBox# show activity log
Activity Log file names:
    Current
    1.2011-04-18_030501
    2.2011-04-17_030501
    3.2011-04-16_030501
DemoBox# show activity log 3.2011-04-16_030501 10
[2011-04-15 11:46:06] INFO 172.17.6.121 [-] stats XMLID546 KeyDel
RANDOM_KEY_1731625354322856302613303801943047507970 [-] - [Success] [-]
[2011-04-15 11:46:06] INFO 172.17.6.121 [-] stats XMLID547 Auth - [stats] -
[Success] [-]
[2011-04-15 11:46:06] ERROR 172.17.6.121 [-] stats - - - [-] 100 [Unrecognizable
client request] [-]
[2011-04-15 11:46:06] INFO 172.17.6.121 [-] stats XMLID550 Auth - [stats] -
[Success] [-]
[2011-04-15 11:46:06] INFO 172.17.6.121 [-] stats XMLID551 KeyDel
RANDOM_KEY_95299797105954945003865651177125670408 [-] - [Success] [-]
```

show audit log - display all audit log names

Specify a log name to display a specific log. Include the log name and a number to display that number of lines in the specified log.

Syntax: **show audit log** for a list of all logs
show audit log <log name> for a specific log
show audit log <log name> <number of lines> for part of a log

For example:

```
DemoBox# show audit log
Audit Log file names:
    Current
    1.2011-03-20_031501
    2.2011-03-13_031501
    3.2011-03-06_031501
    4.2011-02-27_031501
DemoBox# show audit log 4.2011-02-27_031501 5
2011-02-25 17:21:12 [admin] [ConfigInfo] [Initialization]: Starting first time
```


show dbencrypt log - view a database encryption log

Syntax: **show dbencrypt log** for a list of all logs
show dbencrypt log <log name> for a specific log
show dbencrypt log <log name> <number of lines> for part of a log

For example:

```
DemoBox# show dbencrypt log
Database Encryption Log file names:
Current
1.2011-03-01_032501
```

show failover log - view a failover log

Syntax: **show failover log** for a list of all logs
show failover log <log name> for a specific log
show failover log <log name> <number of lines> for part of a log

For example:

```
DemoBox# show failover log
Failover Log file names:
Current
1.2011-03-20_031501
2.2011-03-13_031501
```

```
DemoBox# show failover log 2.2011-03-13_031501 5
[2011-03-07 00:46:27] ERROR 172.17.6.121 [-] ES-36 East103 XMLID1 Crypto
ldap_aap-des-56 [-] 221 [User is not authorized to perform this operation at
this time] [-]
[2011-03-07 00:46:40] INFO 172.17.6.121 [-] ES-37 East103 XMLID0 Auth -
[East103] - [Success] [-]
```

show sql log - view a sql log

Syntax: **show sql log** for a list of all logs
show sql log <log name> for a specific log
show sql log <log name> <number of lines> for part of a log

For example:

```
DemoBox# show sql log
SQL Log file names:
Current
1.2011-03-01_032501
```

show system log - view the system log

Syntax: **show system log** for a list of all logs
show system log <log name> for a specific log
show system log <log name> <number of lines> for part of a log

For example:

```
DemoBox# show system log
System Log file names:
  Current
  1.2011-03-20_031501
  2.2011-03-13_031501
```

```
DemoBox# show system log 1.2011-03-20_031501 5
2011-03-20 02:40:01 nightly-7-23 NTP: Synchronized clock via NTP: Successfully
slewed time by 0.261629 seconds using server 172.17.6.2
2011-02-25 17:21:08 localhost System: Device starting up. Software version:
6.1.0.
```

sql log rotate - rotate the sql log

Syntax: **sql log rotate**

For example:

```
DemoBox (config)# sql log rotate
SQL Log successfully rotated.
```

system log rotate - rotate a system log

Syntax: **system log rotate**

For example:

```
DemoBox (config)# system log rotate
System Log successfully rotated.
```

transfer activity log - transfer a log file off of the device

Syntax: **transfer activity log <log name>**

For example:

```
DemoBox# show activity log
Activity Log file names:
  Current
  1.2011-03-22_030501
  2.2011-03-21_030501
```

```
DemoBox# transfer activity log 2.2011-03-21)030501
Please pick one of the following types of transfer:
  1) FTP    2) SCP
Transfer Type (1-2): 2
Enter the host: 10.20.15.81
Enter the directory: /logs
Enter the username: user1
Enter the password:
Success.
```

transfer audit log - transfer a log file off of the device

Syntax: **transfer audit log** <log name>

For example:

```
DemoBox# show audit log
Audit Log file names:
  Current
  1.2011-03-20_031501
  2.2011-03-13_031501
  3.2011-03-06_031501
  4.2011-02-27_031501
  5.2011-02-20_031501
  6.2011-02-13_031501

DemoBox# transfer audit log 6.2011-02-13_031501
Please pick one of the following types of transfer:
  1) FTP    2) SCP
Transfer Type (1-2): 2
Enter the host: 10.20.15.81
Enter the directory: /logs
Enter the username: user1
Enter the password:
Success.
```

transfer clientevent log - transfer a client event log off of the device

Syntax: **transfer clientevent log** <log name>

For example:

```
DemoBox# show clientevent log
Client Event Log file names:
  Current
  1.2011-03-24_143551
  2.2011-03-24_030501
  3.2011-03-23_030501
  4.2011-03-22_030501

DemoBox# transfer clientevent log 4.2011-03-22_030501
Please pick one of the following types of transfer:
  1) FTP    2) SCP
Transfer Type (1-2): 2
Enter the host: 10.20.15.81
Enter the directory: /logs
Enter the username: user1
Enter the password:
Success.
```

transfer dbencrypt log - transfer a database encryption log off of the device

Syntax: **transfer dbencrypt log <log name>**

For example:

```
DemoBox# show dbencrypt log
Database Encryption Log file names:
Current
1.2011-03-24_143551
2.2011-03-24_030501
3.2011-03-23_030501
4.2011-03-22_030501

DemoBox# transfer dbencrypt log 4.2011-03-22_030501
Please pick one of the following types of transfer:
1) FTP    2) SCP
Transfer Type (1-2): 2
Enter the host: 10.20.15.81
Enter the directory: /logs
Enter the username: user1
Enter the password:
Success.
```

transfer failover log - transfer a failover log off of the device

Syntax: **transfer failover log <log name>**

For example:

```
DemoBox# show failover log
Failover Log file names:
Current
1.2011-03-24_143551
2.2011-03-24_030501
3.2011-03-23_030501
4.2011-03-22_030501

DemoBox# transfer failover log 4.2011-03-22_030501
Please pick one of the following types of transfer:
1) FTP    2) SCP
Transfer Type (1-2): 2
Enter the host: 10.20.15.81
Enter the directory: /logs
Enter the username: user1
Enter the password:
Success.
```

transfer sql log - transfer a sql log file off of the device

Syntax: **transfer sql log <log name>**

For example:

```
DemoBox# show sql log
SQL Log file names:
  Current
  1.2011-03-24_143551
  2.2011-03-24_030501
  3.2011-03-23_030501
  4.2011-03-22_030501
```

```
DemoBox# transfer sql log 4.2011-03-22_030501
Please pick one of the following types of transfer:
  1) FTP    2) SCP
Transfer Type (1-2): 2
Enter the host: 10.20.15.81
Enter the directory: /logs
Enter the username: user1
Enter the password:
Success.
```

transfer system log - transfer a system log off of the device

Syntax: **transfer system log <log name>**

For example:

```
DemoBox# show system log
System Log file names:
  Current
  1.2011-03-20_031501
  2.2011-03-13_031501
  3.2011-03-06_031501
  4.2011-02-27_031501
  5.2011-02-20_031501
  6.2011-02-13_031501
```

```
DemoBox# transfer system log 6.2011-02-13_031501
Please pick one of the following types of transfer:
  1) FTP    2) SCP
Transfer Type (1-2): 2
Enter the host: 10.20.15.81
Enter the directory: /logs
Enter the username: user1
Enter the password:
Success.
```

Chapter 16

Server Configuration

Using the CLI, you can:

- configure and view the key server settings for the NAE-XML server (`nae-server settings`, `show nae-server settings`)

nae-server settings - configure the nae server settings

Syntax: **nae-server settings** <ip address> <port>

For example:

```
DemoBox (config)# nae-server settings 172.17.17.20 9002
IP:
    1: All
    2: 172.17.17.20
Enter a number (1 - 2) [1]: 2
Port [9000]:9002
Use SSL [n]:y
Server Certificate:
    1: Cert.150
Enter a number (1 - 1) [1]: 1
Connection Timeout (sec) [3600]: 3600
Allow Key and Policy Configuration Operations [y]: y
Allow Key Export [n]: y
NAE server settings successfully saved.
Warning: For high security it is strongly recommended to use SSL when allowing
key export
```

show nae-server settings - view the nae server settings

Syntax: **show nae-server settings**

For example:

```
DemoBox# show nae-server settings
1.      Protocol:      NAE-XML
        IP:            [All]
        Port:          9000
        Use SSL:       no
        Server Certificate: [None]
2.      Protocol:      KMIP
        IP:            [All]
        Port:          9002
        Use SSL:       yes
        Server Certificate: CertTwo
```

Chapter 17

Network Configuration

Using the CLI, you can:

- add and remove an ip address (`ip address`, `no ip address`)
- configure the outgoing gateway (`outgoing gateway`)
- show and edit the hostname (`show hostname`, `hostname`)
- view, create, and delete static routes (`show static route`, `static route`, `no static route`)
- view and edit the network interface port speed/duplex settings (`show ethernet port`, `ethernet port`)
- view, create, edit, and delete vlan tags (`show vlan tag`, `vlan tag`, `edit vlan tag`, `no vlan tag`)
- view and configure high availability settings (`show high-availability`, `high-availability`) and configure and remove high-availability interfaces (`high-availability ip address`, `no high-availability ip address`)
- view, configure, and delete the default gateway interfaces (`show gateway`, `gateway`, `no gateway`)
- view, add, and remove domain name servers (`show hosts`, `ip name-server`, `no ip name-server`)
- view network interfaces (`show interfaces`, `show interface ethernet`)
- view the device's mac address (`show mac address`)
- view, configure, and manage the ip authorization settings (`show ip authorization`, `ip authorization`, `edit ip authorization allowed`, `no ip authorization allowed`)

edit ip authorization allowed - edit the IP authorization settings for a particular IP

This command requires that you provide the index number of the IP address you want to edit, rather than the actual IP itself. You might find it useful to use the `show ip authorization allowed` command to find the appropriate index number.

Syntax: **edit ip authorization allowed <ip #>**

For example:

```
DemoBox (config)# show ip authorization allowed
1.      IP Address, Range, or Subnet: 172.17.40.37
       NAE Server:                    no
       Web Administration:            no
       SSH Administration:            yes
```

- 2. IP Address, Range, or Subnet: 172.17.40.247
 NAE Server: yes
 Web Administration: yes
 SSH Administration: no
- 3. IP Address, Range, or Subnet: 172.18.18.0
 NAE Server: yes
 Web Administration: no
 SSH Administration: no

```
DemoBox (config)# edit ip authorization allowed 3
IP Address, Range, or Subnet [172.18.18.0]:
NAE Server [y]: y
Web Administration [n]: y
SSH Administration [n]: y
IP successfully saved.
```

```
DemoBox (config)# show ip authorization allowed
1. IP Address, Range, or Subnet: 172.17.40.37
   NAE Server: no
   Web Administration: no
   SSH Administration: yes
2. IP Address, Range, or Subnet: 172.17.40.247
   NAE Server: yes
   Web Administration: yes
   SSH Administration: no
3. IP Address, Range, or Subnet: 172.18.18.0
   NAE Server: yes
   Web Administration: yes
   SSH Administration: yes
```

edit vlan tag - modify the description of a VLAN tagged interface on the device

Syntax: **edit vlan tag <number>**

For example:

```
DemoBox (config)# show vlan tag
Physical Interface Tag Description
=====
1. Ethernet #1 100 VLAN Tagged Interface #1
2. Ethernet #2 200 vlan 200
```

```
DemoBox (config)# edit vlan tag 2
Enter the description: VLAN Tagged Interface #2
VLAN tagged interface Ethernet #2 Tag 200 successfully modified.
```

```
DemoBox (config)# show vlan tag
Physical Interface Tag Description
=====
1. Ethernet #1 100 VLAN Tagged Interface #1
2. Ethernet #2 200 VLAN Tagged Interface #2
```


ethernet port - change the Network Interface Port Speed/Duplex settings

Syntax: **ethernet port**

For example:

```
DemoBox (config)# show ethernet port
Interface           Requested Speed/Duplex   Current Speed/Duplex
=====
Gigabit Ethernet #1   Auto-Negotiate          100 Mbps/Full Duplex
Gigabit Ethernet #2   Auto-Negotiate          Unknown or not connected
Gigabit Ethernet #3   Auto-Negotiate          Unknown or not connected
Gigabit Ethernet #4   Auto-Negotiate          Unknown or not connected
```

```
DemoBox (config)# ethernet port
Enter the port speed and duplex for Gigabit Ethernet #1:
  1: Auto-Negotiate
  2: 10 Mbps/Half Duplex
  3: 10 Mbps/Full Duplex
  4: 100 Mbps/Half Duplex
  5: 100 Mbps/Full Duplex
  6: 1000 Mbps/Full Duplex
Enter a number (1 - 6) [1]: 4
Enter the port speed and duplex for Gigabit Ethernet #2:
  1: Auto-Negotiate
  2: 10 Mbps/Half Duplex
  3: 10 Mbps/Full Duplex
  4: 100 Mbps/Half Duplex
  5: 100 Mbps/Full Duplex
  6: 1000 Mbps/Full Duplex
Enter a number (1 - 6) [1]: 6
```

Note: The changes will take a few moments to take effect.
Continue (y/n)? [n]: y

```
DemoBox (config)# show ethernet port
Interface           Requested Speed/Duplex   Current Speed/Duplex
=====
Gigabit Ethernet #1   100 Mbps/Half Duplex    100 Mbps/Half Duplex
Gigabit Ethernet #2   1000 Mbps/Full Duplex   Unknown or not connected
Gigabit Ethernet #3   1000 Mbps/Full Duplex   Unknown or not connected
Gigabit Ethernet #4   1000 Mbps/Full Duplex   Unknown or not connected
```

gateway <ip> <interface #> - define the default gateway used by the device

Syntax: **gateway <ip> <interface #>**

For example:

```
DemoBox (config)# gateway 172.17.17.1 1
Gateway for interface 1 successfully set.
```

You can also pass the IP, interface number and vlan tag as arguments to the command in order to define the default gateway using a VLAN tag.

Syntax: `gateway <ip> <interface #> <vlan tag>`

For example:

```
DemoBox (config)# gateway 172.17.17.1 1 100
Gateway for interface 1 successfully set.
```

high-availability - configure high availability

Syntax: **high-availability**

For example:

```
DemoBox (config)# high-availability
Enable High Availability (y/n) [n]: y
Set as Master (y/n) [n]: y
Monitor IP Address:
    1: 172.17.17.120
Enter a number (1 - 1): 1
Ethernet #1 Group ID [1]: 1
Ethernet #2 Group ID [2]: 2
High Availability settings successfully updated.
```

high-availability ip address - add a high-availability interface

You can specify the ip, subnet mask, interface, and vlan tag at the command line. The vlan tag must already be configured. (You can use the `vlan tag` command for that.)

Syntax: **high-availability ip address**

```
high-availability ip address <ip> <subnet mask> <interface #>
high-availability ip address <ip> <subnet mask> <interface #> <vlan tag>
```

For example:

```
DemoBox (config)# high-availability ip address
Enter the IP address: 172.18.18.100
Enter the subnet mask: 255.255.255.0
Available interfaces:
    1. Ethernet #1
    2. Ethernet #2
    3. Ethernet #1 Tag 100
Enter the interface (1-3): 1
IP address 172.18.18.100 successfully added.

DemoBox (config)# high-availability ip address 172.18.18.100 255.255.255.0 1
IP address 172.18.18.100 successfully added.

DemoBox (config)# high availability ip address 172.17.17.121 255.255.255.0 1 100
IP address 172.17.17.121 successfully added.
```

hostname - define the device's hostname

Syntax: **hostname <name>**

For example:

```
DemoBox (config)# hostname DemoBox2
Successfully set hostname.
DemoBox2 (config)#
```

ip address - add an IP address, subnet mask, and interface number to the network settings

Syntax: **ip address**

For example:

```
DemoBox (config)# ip address
Enter the IP address: 172.17.17.121
Enter the subnet mask: 255.255.255.0
Available interfaces:
    1. Ethernet #1
    2. Ethernet #2
    3. Virtual Interface
    4. Ethernet #1 Tag 100
Enter the interface (1-4): 2
IP address 172.17.17.121 successfully added.
```

You can also pass the IP, subnet mask, and interface as arguments to the command in order to skip the subsequent input prompts.

Syntax: **ip address <ip> <subnet mask> <interface #>**

For example:

```
DemoBox (config)# ip address 172.17.17.121 255.255.255.0 2
IP address 172.17.17.121 successfully added.
```

Similarly, you can pass the IP, subnet mask, interface, and vlan tag as arguments to the command. The vlan tag must already be configured. (You can use the `vlan tag` command for that.)

Syntax: **ip address <ip> <subnet mask> <interface #> <vlan tag>**

For example:

```
DemoBox (config)# ip address 172.17.17.121 255.255.255.0 1 100
IP address 172.17.17.121 successfully added.
```

ip authorization - edit the IP authorization settings

Use the `ip authorization allowed` and `edit ip authorization allowed` commands to configure the IPs referred to in the second option "Only Allow IPs Specified".

Syntax: **ip authorization**

For example:

```
DemoBox (config)# ip authorization
NAE Server:
```

```
Please select from the following options:
    1) Allow All Connections          2) Only Allow IPs Specified
NAE Server [1]: 2
Web Administration:
Please select from the following options:
    1) Allow All Connections          2) Only Allow IPs Specified
Web Administration [1]: 1
SSH Administration:
Please select from the following options:
    1) Allow All Connections          2) Only Allow IPs Specified
SSH Administration [1]: 1
IP Authorization settings successfully saved.
```

ip authorization allowed - add a new IP address to the list of authorized IP addresses

Syntax: **ip authorization allowed**

For example:

```
DemoBox (config)# ip authorization allowed
IP Address, Range, or Subnet: 172.18.18.0
NAE Server [n]: y
Web Administration [n]: n
SSH Administration [n]: n
IP successfully saved.
```

ip name-server - add one or more domain name servers

Syntax: **ip name-server <ip1> [ip2...ipN]**

For example:

```
DemoBox (config)# ip name-server 172.18.18.1 172.18.18.2
DNS Server successfully added.
DNS Server successfully added.
```

no gateway - remove the default gateway setting for an interface

Syntax: **no gateway <interface #>**

For example:

```
DemoBox (config)# show gateway
Ethernet #1 default gateway: 172.17.17.1
Ethernet #2 default gateway: 172.17.18.1
Ethernet #3 default gateway: None
Ethernet #4 default gateway: None
Ethernet #1 Tag 100 default gateway: 172.34.20.1
Outgoing gateway is set to Ethernet #1

DemoBox (config)# no gateway 2
Gateway for interface 2 successfully cleared.
```

```
DemoBox (config)# show gateway
Ethernet #1 default gateway: 172.17.17.1
Ethernet #2 default gateway: None
Ethernet #3 default gateway: None
Ethernet #4 default gateway: None
Ethernet #1 Tag 100 default gateway: 172.34.20.1
Outgoing gateway is set to Ethernet #1
```

Pass the vlan tag as an argument when removing the default gateway for a vlan tagged interface

Syntax: `no gateway <interface #> <vlan tag>`

For example:

```
DemoBox (config)# show gateway
Ethernet #1 default gateway: 172.17.17.1
Ethernet #2 default gateway: 172.17.18.1
Ethernet #3 default gateway: None
Ethernet #4 default gateway: None
Ethernet #1 Tag 100 default gateway: 172.34.20.1
Outgoing gateway is set to Ethernet #1

DemoBox (config)# no gateway 1 100
Gateway for interface 1 Tag 100 successfully cleared.
```

```
DemoBox (config)# show gateway
Ethernet #1 default gateway: 172.17.17.1
Ethernet #2 default gateway: 172.17.18.1
Ethernet #3 default gateway: None
Ethernet #4 default gateway: None
Ethernet #1 Tag 100 default gateway: None
Outgoing gateway is set to Ethernet #1
```

no high-availability ip address - delete one or more high availability interfaces

Syntax: `no high-availability ip address <ip1>...<ipN>`

For example:

```
DemoBox (config)# no high-availability ip address 172.18.18.100
IP address 172.18.18.100 successfully removed.
```

no ip address - delete one or multiple IP addresses from the network settings

Syntax: `no ip address <ip1> [ip2...ipN]`

For example:

```
DemoBox (config)# show interfaces
Configured Interfaces:
      IP Address      Subnet Mask      Interface
      172.17.17.120   255.255.255.0    Ethernet #1
      172.17.17.121   255.255.255.0    Ethernet #1 Tag 100
```

```

High Availability Interfaces:
  No network interfaces.

Available Physical and VLAN Tagged Interfaces:
  Ethernet #1
  Ethernet #2
  Ethernet #1 Tag 100

DemoBox (config)# no ip address 172.17.17.121
IP address 172.17.17.121 successfully removed.

DemoBox (config)# show interfaces
Configured Interfaces:
  IP Address      Subnet Mask      Interface
  172.17.17.120   255.255.255.0    Ethernet #1

High Availability Interfaces:
  No network interfaces.

Available Physical and VLAN Tagged Interfaces:
  Ethernet #1
  Ethernet #2
  Ethernet #1 Tag 100

```

no ip authorization allowed - delete an IP address from the list of authorized IP addresses

The `no ip authorization allowed` command requires that you provide the index number of the IP address you want to edit, rather than the actual IP address itself. You might find it helpful to use the `show ip authorization allowed` command to find the appropriate index number.

Syntax: `no ip authorization allowed <allowed ip #>`

For example:

```

DemoBox (config)# show ip authorization allowed
1.   IP Address, Range, or Subnet: 172.17.40.37
     NAE Server:                    no
     Web Administration:            no
     SSH Administration:            yes

2.   IP Address, Range, or Subnet: 172.17.40.247
     NAE Server:                    yes
     Web Administration:            yes
     SSH Administration:            no

3.   IP Address, Range, or Subnet: 172.18.18.0
     NAE Server:                    yes
     Web Administration:            yes
     SSH Administration:            yes

DemoBox (config)# no ip authorization allowed 3
IP successfully removed.

DemoBox (config)# show ip authorization allowed
1.   IP Address, Range, or Subnet: 172.17.40.37
     NAE Server:                    no

```

```

        Web Administration:          no
        SSH Administration:         yes
2.    IP Address, Range, or Subnet: 172.17.40.247
        NAE Server:                 yes
        Web Administration:         yes
        SSH Administration:         no

```

no ip name-server - delete a domain name server

Syntax: **no ip name-server** <ip1> [ip2...ipN]

For example:

```

DemoBox (config)# no ip name-server 172.18.18.1 172.18.18.2
DNS Server successfully deleted.
DNS Server successfully deleted.

```

no static route - delete a static route

Syntax: **no static route** <route #>

For example:

```

DemoBox (config)# show static route
Static Routes:
      Destination IP      Subnet Mask      Gateway      Interface
1.  172.17.17.0          255.255.255.0    172.17.17.1  Ethernet #1
2.  172.18.18.0          255.255.255.0    172.17.17.1  Ethernet #1

```

```

DemoBox (config)# no static route 2
Static route successfully removed.

```

```

DemoBox (config)# show static route
Static Routes:
      Destination IP      Subnet Mask      Gateway      Interface
1.  172.17.17.0          255.255.255.0    172.17.17.1  Ethernet #1

```

no vlan tag - delete a VLAN tagged interface

Syntax: **no vlan tag** <number>

For example:

```

DemoBox (config)# show vlan tag
      Physical Interface  Tag  Description
=====
1.  Ethernet #1          100  VLAN Tagged Interface #1
2.  Ethernet #2          200  VLAN Tagged Interface #2

```

```

DemoBox (config)# no vlan tag 2
VLAN tagged interface Ethernet #2 Tag 200 deleted.

```

```

DemoBox (config)# show vlan tag

```


Physical Interface	Tag	Description
1. Ethernet #1	100	VLAN Tagged Interface #1

outgoing gateway - designate an interface to handle outgoing connections initiated by the device

Syntax: **outgoing gateway <interface #>**

For example:

```
DemoBox (config)# show gateway
Ethernet #1 default gateway: 172.17.17.1
Ethernet #2 default gateway: 172.17.18.1
Ethernet #3 default gateway: None
Ethernet #4 default gateway: None
Ethernet #1 Tag 100 default gateway: None
Outgoing gateway is set to Ethernet #2
```

```
DemoBox (config)# outgoing gateway 1
Warning: Outgoing Gateway is already set to the specified interface.
Outgoing gateway set successfully.
```

```
DemoBox (config)# show gateway
Ethernet #1 default gateway: 172.17.17.1
Ethernet #2 default gateway: 172.17.18.1
Ethernet #3 default gateway: None
Ethernet #4 default gateway: None
Ethernet #1 Tag 100 default gateway: None
Outgoing gateway is set to Ethernet #1
```

You can also pass the interface number and vlan tag as arguments to the command.

Syntax: **outgoing gateway <interface #> <vlan tag>**

For example:

```
DemoBox (config)# show gateway
Ethernet #1 default gateway: 172.17.17.1
Ethernet #2 default gateway: 172.17.18.1
Ethernet #3 default gateway: None
Ethernet #4 default gateway: None
Ethernet #1 Tag 100 default gateway: 172.34.20.1
Outgoing gateway is set to Ethernet #2
```

```
DemoBox (config)# outgoing gateway 1 100
Warning: Outgoing Gateway is already set to the specified interface.
Outgoing gateway set successfully.
```

```
DemoBox (config)# show gateway
Ethernet #1 default gateway: 172.17.17.1
Ethernet #2 default gateway: 172.17.18.1
Ethernet #3 default gateway: None
Ethernet #4 default gateway: None
Ethernet #1 Tag 100 default gateway: 172.34.20.1
```

Outgoing gateway is set to Ethernet #1 Tag 100

show ethernet port - view the network interface port speed/duplex settings

Syntax: **show ethernet port**

For example:

```
DemoBox# show ethernet port
Interface                Requested Speed/Duplex    Current Speed/Duplex
=====
Gigabit Ethernet #1     Auto-Negotiate           1000 Mbps/Full Duplex
```

show gateway - show the current gateway

Syntax: **show gateway**

For example:

```
DemoBox# show gateway
Ethernet #1 default gateway: 172.17.7.1
Outgoing gateway is set to Ethernet #1
```

show high-availability - display the high availability settings

Syntax: **show high-availability**

For example:

```
DemoBox# show high-availability
Enable High Availability:      False
Set as Master:                 False
Monitor IP Address:           [None]
Slave Advertisement Timeout (sec): 3
Ethernet #1 Group ID:         1
```

show hostname - view the device's hostname

Syntax: **show hostname**

For example:

```
DemoBox# show hostname
The hostname is DemoBox.
```

show hosts - view currently configured domain name server

Syntax: **show hosts**

For example:

```
DemoBox# show hosts
```

```
Name Servers
    172.17.6.12
    172.17.6.2
```

show interface ethernet - view interface detail for a specified ethernet port

Syntax: **show internet ethernet <interface # | virtual>**

For example:

```
DemoBox# show interface ethernet 1
```

```
Configured Interfaces:
    IP Address      Subnet Mask      Interface
    172.17.7.29     255.255.255.0   Ethernet #1
```

```
High Availability Interfaces:
    No network interfaces.
```

show interfaces - view all network interfaces

Syntax: **show interfaces**

For example:

```
DemoBox# show interfaces
```

```
Configured Interfaces:
    IP Address      Subnet Mask      Interface
    172.17.7.29     255.255.255.0   Ethernet #1
```

```
High Availability Interfaces:
    No network interfaces.
```

```
Available Physical and VLAN Tagged Interfaces:
    Ethernet #1
```

show ip authorization - display whether each server grants access to all IPs or only grants access to specific IPs

Syntax: **show ip authorization**

For example:

```
DemoBox# show ip authorization
    NAE Server:      Allow All Connections
    Web Administration:  Allow All Connections
    SSH Administration: Allow All Connections
```

show ip authorization allowed - display the IP authorization settings for all authorized IP addresses

You can view the settings for a particular IP address by passing in the index number of the IP address as a parameter.

Syntax: **show ip authorization allowed**
show ip authorization allowed <ip address index number>

For example:

```
DemoBox# show ip authorization allowed
1.      IP Address, Range, or Subnet: 172.17.40.37
        NAE Server:                  no
        Web Administration:          no
        SSH Administration:          yes
2.      IP Address, Range, or Subnet: 172.17.40.247
        NAE Server:                  yes
        Web Administration:          yes
        SSH Administration:          no
```

```
DemoBox# show ip authorization allowed 1
        IP Address, Range, or Subnet: 172.17.40.37
        NAE Server:                  no
        Web Administration:          no
        SSH Administration:          yes
```

show mac address - view the device's MAC address

Syntax: **show mac address**

For example:

```
DemoBox# show mac address
Ethernet #1: d4:be:d9:ed:96:1d
Ethernet #2: d4:be:d9:ed:96:1f
```

show static route - view the static route settings

Syntax: **show static route**

For example:

```
DemoBox# show static route
Static Routes:
      Destination IP      Subnet Mask      Gateway      Interface
1. 172.17.17.0           255.255.255.0    172.17.17.1  Ethernet #1
```

show vlan tag - view the VLAN Tagged Interfaces

Syntax: **show vlan tag**

For example:

```
DemoBox# show vlan tag
      Physical Interface  Tag  Description
=====
```

1. Ethernet #1 100 VLAN Tagged Interface #1

static route - configure a static route

Syntax: **static route**

For example:

```
DemoBox (config)# show static route
Static Routes:
      Destination IP      Subnet Mask      Gateway      Interface
1. 172.17.17.0          255.255.255.0    172.17.17.1    Ethernet #1

DemoBox (config)# static route
Enter the destination IP address: 172.18.18.0
Enter the subnet mask: 255.255.255.0
Enter the gateway: 172.17.17.1
Available interfaces:
  1. Ethernet #1
  2. Ethernet #2
  3. Ethernet #1 Tag 100
Enter the interface (1-3): 1
Static route successfully added.

DemoBox (config)# show static route
Static Routes:
      Destination IP      Subnet Mask      Gateway      Interface
1. 172.17.17.0          255.255.255.0    172.17.17.1    Ethernet #1
2. 172.18.18.0          255.255.255.0    172.17.17.1    Ethernet #1
```

vlan tag - configure a VLAN tagged interface

Syntax: **vlan tag**

For example:

```
DemoBox (config)# vlan tag
Select the physical interface from the following list:
  1. Ethernet #1
  2. Ethernet #2
Enter a number (1-2): 2
Enter the tag (2-4094): 200
Enter the description (0-256 characters): vlan 200
VLAN tagged interface Ethernet #2 Tag 200 successfully created.
```

Chapter 18

Network Diagnostics

Using the CLI, you can:

- ping a device on the network (`ping run`)
- print the route to a network device (`tracerout run`)
- lookup the hostname for an IP address (`host run`)
- generate a list of active connections (`netstat run`)

The same functionality is available through the Management Console.

host run - look up the host specified using the domain server

Syntax: **host run <ip>**

For example:

```
DemoBox (config)# host run 172.17.6.12  
12.6.17.172.in-addr.arpa domain name pointer server1.qa.company.com.
```

netstat run - generate a list of all active connections

Use this tool to identify problems in the network and determine the amount of network traffic.

Syntax: **netstat run**

For example:

```
DemoBox (config)# netstat run  
Active Internet connections (w/o servers)  
Proto Recv-Q Send-Q Local Address Foreign Address State  
tcp 0 0 172.17.17.120:22 172.17.40.37:32850 ESTABLISHED  
udp 0 0 127.0.0.1:23362 127.0.0.1:23362 ESTABLISHED
```

Heading	Description
Proto	The protocol used by the connection. Either tcp, udp, or raw.
Recv-Q	The number of bytes received from the remote host waiting to be read.
Send-Q	The number of bytes awaiting acknowledgement by the remote host.
Local Address	The local address/hostname and port number of the connection.
Foreign Address	The remote address/hostname and port number of the connection.
State	The state of the connection.

ping run - send ICMP ECHO_REQUEST packets to the specified network host

Syntax: **ping run <ip>**

For example:

```
DemoBox (config)# ping run 172.17.6.27
PING 172.17.6.27 (172.17.6.27) 56(84) bytes of data.
64 bytes from 172.17.6.27: icmp_seq=0 ttl=127 time=1.46 ms
64 bytes from 172.17.6.27: icmp_seq=1 ttl=127 time=2.91 ms
64 bytes from 172.17.6.27: icmp_seq=2 ttl=127 time=1.90 ms
64 bytes from 172.17.6.27: icmp_seq=3 ttl=127 time=0.775 ms
64 bytes from 172.17.6.27: icmp_seq=4 ttl=127 time=0.875 ms

--- 172.17.6.27 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 0.775/1.587/2.918/0.782 ms, pipe 2
```

traceroute run - print the route packets take to the specified network host

Syntax: **traceroute run <ip>**

For example:

```
DemoBox(config)# traceroute run 172.17.6.27
 1 172.17.3.1    0.401 ms  0.335 ms  0.351 ms
 2 172.17.6.27  2.727 ms  0.244 ms  0.169 ms
```

Chapter 19

SNMP Configuration

Using the CLI, you can:

- view and edit the snmp agent settings (`show snmp agent`, `snmp agent`)
- view, add, edit, and delete communities (`show community`, `community`, `edit community`, `no community`)
- view, create, edit, and delete SNMPv3 usernames (`show snmp username`, `snmp username`, `edit snmp username`, `no snmp username`)
- view, add, edit, and remove stations (`show station`, `station`, `edit station`, `no station`)
- send test traps (`snmp test`)

community - add a community

Syntax: **community**

For example:

```
DemoBox (config)# community
Community Name: YourCommunity
Source IP/Subnet Mask(s): 172.17.45.15/255.255.255.255
MIB Access:
    Enterprise [y]: y
    Standard [y]: y
SNMP community successfully saved.
```

edit community - edit a community

Syntax: **edit community** <community name>

For example:

```
DemoBox (config)# edit community YourCommunity
Community Name [YourCommunity]:
Source IP/Subnet Mask(s) [172.17.45.15/255.255.255.255]:
MIB Access:
    Enterprise [y]: n
    Standard [y]: y
SNMP community successfully saved.
```

edit snmp username - edit an existing SNMPv3 username

Syntax: **edit snmp username** <username>

For example:

```
DemoBox (config)# edit snmp username SNMP.User2
Username [SNMP.User2]:
Security Level:
    1: noAuth, noPriv
    2: auth, noPriv
    3: auth, priv
Enter a number (1 - 3) [2]:
Auth Protocol:
    1: None
    2: MD5
    3: SHA
Enter a number (1 - 3) [2]:
Auth Password [*****]:
MIB Access:
    Enterprise [n]: y
    Standard [y]: n
SNMP username successfully saved.
```

edit station - edit an SNMP management station

Syntax: **edit station <station number>**

For example:

```
DemoBox (config)# edit station 2
Manager Type:
    1: SNMPv1
    2: SNMPv2
    3: SNMPv3
Enter a number (1 - 3) [2]:
Trap Type:
    1: Trap
    2: Inform
Enter a number (1 - 2) [2]: 1
Hostname or IP [172.17.17.80]:
Port [162]:
Manager Community [public]:
SNMP management station successfully saved.
```

no community - remove a community from the system SMNP configuration

Syntax: **no community <community name>**

For example:

```
DemoBox (config)# no community YourCommunity
SNMP community successfully removed.
```

no snmp username - delete an existing SNMPv3 username

Syntax: **no snmp username <username>**

For example:

```
DemoBox (config)# no snmp username SNMP.User3  
SNMP username successfully removed.
```

no station - remove an SNMP management station

Syntax: **no station <station number>**

For example:

```
DemoBox (config)# no station 2  
SNMP management station successfully removed.  
DemoBox (config)# show station  
1.      Manager Type:                SNMPv1  
      Trap Type:                    Trap  
      Hostname or IP:                172.17.40.37  
      Port:                          162  
      Manager Community or Username: Community: public
```

show community - view either all current communities configured on the device, or detail about a specific community

Syntax: **show community**
show community <community name>

For example:

```
DemoBox (config)# show community  
1.      Community Name:              public  
      Source IP/Subnet Mask(s): Any  
      MIB Access:                    Enterprise, Standard  
  
DemoBox (config)# show community SomeCommunity  
Community Name:                    SomeCommunity  
Source IP/Subnet Mask(s): Any  
MIB Access:                          Standard
```

show snmp agent - display the SNMP agent settings

Syntax: **show snmp agent**

For example:

```
DemoBox (config)# show snmp agent  
SNMP Agent IP:                      [All]  
SNMP Agent Port:                    161  
Enable SNMP Traps:                  yes
```

show snmp username - view the list of existing SNMPv3 usernames or view a specific user

Syntax: **show snmp username**
show snmp username <username>

For example:

```
DemoBox# show snmp username
1.      Username:          SNMP.User1
        Security Level:    auth, priv
        Auth Protocol:     SHA
        Auth Password:     *****
        Priv Password:     *****
        MIB Access:       Enterprise, Standard

2.      Username:          SNMP.User2
        Security Level:    auth, noPriv
        Auth Protocol:     MD5
        Auth Password:     *****
        Priv Password:     [None]
        MIB Access:       Standard
```

```
DemoBox# show snmp username SNMP.User2
Username:          SNMP.User2
Security Level:    auth, noPriv
Auth Protocol:     MD5
Auth Password:     *****
Priv Password:     [None]
MIB Access:       Standard
```

show station - view all SNMP management stations of the details of a specific station

Syntax: **show station**
show station <station number>

For example:

```
DemoBox# show station
1.      Manager Type:      SNMPv1
        Trap Type:        Trap
        Hostname or IP:    172.17.40.37
        Port:              162
        Manager Community or Username: Community: public
```

```
DemoBox# show station 1
Manager Type:      SNMPv1
Trap Type:        Trap
Hostname or IP:    172.17.40.37
Port:              162
Manager Community: public
Username:          [None]
Security Level:    [None]
Auth Protocol:     [None]
```

```
Auth Password:          [None]
Priv Password:          [None]
Manager Engine ID:      [None]
```

snmp agent - set the SNMP agent settings

Syntax: **snmp agent**

For example:

```
DemoBox (config)# snmp agent
SNMP Agent IP:
  1: All
  2: 172.17.7.80
Enter a number (1 - 2) [1]: 2
SNMP Agent Port [161]: 161
Enable SNMP Traps [y]: y
SNMP agent settings successfully saved.
```

snmp test - send an SNMP test trap

Syntax: **snmp test**

For example:

```
DemoBox (config)# snmp test
SNMP test trap successfully sent. Check SNMP Management Stations to confirm.
```

snmp username - create an SNMPv3 username

Syntax: **snmp username**

For example:

```
DemoBox (config)# snmp username
Username: SNMP.User3
Security Level:
  1: noAuth, noPriv
  2: auth, noPriv
  3: auth, priv
Enter a number (1 - 3) [1]: 3
Auth Protocol:
  1: None
  2: MD5
  3: SHA
Enter a number (1 - 3) [1]: 2
Auth Password:
Priv Password:
MIB Access:
  Enterprise [y]: y
  Standard [y]: y
SNMP username successfully saved.
```

station - add an SNMP management station

Syntax: **station**

For example:

```
DemoBox (config)# station
Manager Type:
    1: SNMPv1
    2: SNMPv2
    3: SNMPv3
Enter a number (1 - 3) [1]: 2
Trap Type:
    1: Trap
    2: Inform
Enter a number (1 - 2) [1]: 2
Hostname or IP: 172.17.17.80
Port [162]:
Manager Community: public
SNMP management station successfully saved.
```

Chapter 20

SSKM Configuration

Using the CLI, you can:

- configure and view the sskm interface (`sskm interface`, `show sskm interface`)
- view sskm status information (`show sskm status`)
- start, halt, and restart the sskm (`sskm start`, `sskm halt`, `sskm restart`)
- ping the sskm (`sskm ping`)

show sskm interface - show the ip, netmask, and interface used by the sskm

Syntax: **show sskm interface**

For example:

```
DemoBox# show sskm interface
SSKM is running now
External IP from SSKM config file=172.17.7.189
External IP from network template=172.17.7.189
Netmask: 255.255.0.0
Physical interface mapping: eth0
Default Gateway = 172.17.7.1
```

show sskm status - view sskm status information

Syntax: **show sskm status**

For example:

```
DemoBox# show sskm status
SSKM is running. State is-
-----
Name    ID Mem(MiB) VCPUs State    Time(s)
SSKM    1    4103    2 -b----- 4597.5
-----
Detailed state is:
(domain
  (domid 1)
  (uuid de93beed-7cc5-11cb-55e7-9126d05072ff)
  (vcpus 2)
  (cpu_cap 0)
  (cpu_weight 256)
  (memory 4096)
  (shadow_memory 34)
  (maxmem 4096)
```

```

(features)
(name SSKM)
(on_poweroff destroy)
(on_reboot restart)
(on_crash restart)
(image
  (hvm
    (kernel /usr/lib/xen/boot/hvmloader)
    (device_model /usr/lib/xen/bin/qemu-dm)
    (pae 1)
    (vcpus 2)
    (boot c)
    (timer_mode 1)
    (serial pty)
    (vncunused 1)
    (xauthority /root/.Xauthority)
    (acpi 1)
    (apic 1)
    (usb 1)
    (usbdevice tablet)
    (keymap en-us)
  )
)
)
(cpus ())
(device
  (vif
    (backend 0)
    (script vif-bridge)
    (ip 172.17.7.189)
    (bridge xenbr0)
    (mac 00:16:3e:6c:25:5d)
    (vifname external_sskm_link)
  )
)
)
(device
  (vif
    (backend 0)
    (script vif-bridge)
    (ip 10.0.0.1/32)
    (bridge xenbr-pr)
    (mac 00:16:3e:5c:52:b5)
    (vifname ds_sskm_link)
  )
)
)
(device (vbd (backend 0) (dev hda:disk) (uname phy:/dev/md10) (mode w)))
(device (vbd (backend 0) (dev hdb:disk) (uname phy:/dev/md11) (mode w)))
(device
  (vbd
    (backend 0)
    (dev hdc:disk)
  )
)

```

```
(uname file:/SSKM_WORK/images/SSKM_hdc.img)
(mode w)
)
)
(state -b----)
(shutdown_reason poweroff)
(cpu_time 4597.47401091)
(online_vcpus 2)
(up_time 189925.900305)
(start_time 1305067095.97)
(store_mfn 983038)
)
-----
```

sskm halt - shutdown the sskm

Syntax: **sskm halt**

For example:

```
DemoBox (config)# sskm halt
Info: SSKM shutdown command issued. It may take some time to actually shutdown
Waiting to shut down SSKM...
SUCCESS: SSKM shutdown done
```

sskm interface - configure the ip, and interface to use for the sskm

Note: You cannot execute this command while the SSKM is running. Execute `sskm halt` first.

Syntax: **sskm interface <ip> <interface>**

For example:

```
DemoBox (config)# sskm halt
Info: SSKM shutdown command issued. It may take some time to actually shutdown
Waiting to shut down SSKM...
SUCCESS: SSKM shutdown done
```

```
DemoBox (config)# sskm interface 172.17.7.189 eth0
Network Templates generated OK
IP address 172.17.7.189 scheduled for assignment to SSKM
Warning:If SSKM is not started soon, IP 172.17.7.189 may become stale
SUCCESS: Configured network interface with ip=172.17.7.189, netmask=255.255.0.0
and interface=eth0
```

```
DemoBox (config)# sskm start
SUCCESS: SSKM Started OK
```

sskm ping - ping the sskm

Syntax: **sskm ping**

For example:

```
DemoBox# sskm ping
SSKM is running
IP address is: 172.17.7.189
Press Ctrl+c to stop
PING 172.17.7.189 (172.17.7.189) 56(84) bytes of data.
64 bytes from 172.17.7.189: icmp_seq=1 ttl=64 time=2.61 ms
64 bytes from 172.17.7.189: icmp_seq=2 ttl=64 time=0.175 ms
64 bytes from 172.17.7.189: icmp_seq=3 ttl=64 time=0.179 ms

--- 172.17.7.189 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.175/0.990/2.618/1.151 ms
```

sskm restart - stop and start the sskm

Syntax: **sskm restart**

For example:

```
DemoBox (config)# sskm restart
Info: SSKM shutdown command issued. It may take some time to actually shutdown
Waiting to shut down SSKM...
SUCCESS: SSKM shutdown done
SUCCESS: SSKM Restarted OK
```

sskm start - start the sskm

Syntax: **sskm start**

For example:

```
DemoBox (config)# sskm start
SUCCESS: SSKM Started OK
```

Chapter 21

SSL Configuration

Using the CLI, you can:

- view the allowed ssl protocols and the session key timeout (`show ssl`)
- enable and remove ssl protocols (`ssl protocol` and `no ssl protocol`)
- set the session key timeout (`ssl timeout`)
- view the priority of all ciphers on the system (`show cipherspec`)
- enable and disable a cipherspec (`cipherspec` and `no cipherspec`)
- change the cipherspec priority list (`cipherspec priority`)
- restore the default cipherspec priority list (`restore cipherspec`)
- disable cipherspec export (`no export cipherspec`)

cipherspec - enable a cipherspec

Unless you know the priority of the disabled cipher you want to enable, you can use the `show cipherspec` command to display the ciphers on the system.

Note: The cipher order pertains to the communication channel between the client and the device. It does not affect the keys that might be used to encrypt data by the device.

Syntax: `cipherspec <disabled cipherspec number>`

For example:

```
DemoBox (config)# show cipherspec
```

The SSL cipher order is:

Priority	Key Exchange	Cipher	Keysize	Hash
1	RSA	AES128	128	SHA-1
2	RSA	AES256	256	SHA-1
3	RSA	3DES	168	SHA-1
Disabled (1)	RSA	RC4	128	SHA-1
Disabled (2)	RSA	RC4	128	MD5

```
DemoBox (config)# cipherspec 2
```

SSL cipher successfully enabled.

```
DemoBox (config)# show cipherspec
```

The SSL cipher order is:

Priority	Key Exchange	Cipher	Keysize	Hash
1	RSA	AES128	128	SHA-1
2	RSA	AES256	256	SHA-1
3	RSA	3DES	168	SHA-1
Disabled (1)	RSA	RC4	128	SHA-1
4	RSA	RC4	128	MD5

cipherspec priority - prioritize the cipher spec

Note: The cipher order pertains to the communication channel between the client (application, database, etc.) and the device. It does not affect the keys that might be used to encrypt data by the nae server.

Syntax: **cipherspec priority**

For example:

```
DemoBox (config)# cipherspec priority  
CURRENT PRIORITIES
```

The SSL cipher order is shown below:

Priority	Key Exchange	Cipher	Keysize	Hash
1	RSA	AES128	128	SHA-1
2	RSA	AES256	256	SHA-1
3	RSA	3DES	168	SHA-1
Disabled (1)	RSA	RC4	128	SHA-1
4	RSA	RC4	128	MD5

NEW PRIORITY CONFIGURATION

Please use the current priority from above to reference each item.

Which item will have priority #1 (1...4): 3

Which item will have priority #2: 1

Which item will have priority #3: 2

Which item will have priority #4: 4

SSL cipher order priorities successfully changed.

```
DemoBox (config)# show cipherspec
```

The SSL cipher order is:

Priority	Key Exchange	Cipher	Keysize	Hash
1	RSA	3DES	168	SHA-1
2	RSA	AES128	128	SHA-1
3	RSA	AES256	256	SHA-1
Disabled (1)	RSA	RC4	128	SHA-1
4	RSA	RC4	128	MD5

no cipherspec - disable a cipherspec

Unless you know the priority of the cipher you want to disable, you can use the show cipherspec command to display the ciphers on the system.

Syntax: **no cipherspec <priority of enabled cipherspec>**

For example:

```
DemoBox (config)# show cipherspec
```

The SSL cipher order is:

Priority	Key Exchange	Cipher	Keysize	Hash
1	RSA	3DES	168	SHA-1
2	RSA	AES128	128	SHA-1
3	RSA	AES256	256	SHA-1
Disabled (1)	RSA	RC4	128	SHA-1
4	RSA	RC4	128	MD5

```
DemoBox (config)# no cipherspec 4
SSL cipher successfully disabled.
```

```
DemoBox (config)# show cipherspec
The SSL cipher order is:
```

Priority	Key Exchange	Cipher	Keysize	Hash
1	RSA	3DES	168	SHA-1
2	RSA	AES128	128	SHA-1
3	RSA	AES256	256	SHA-1
Disabled (1)	RSA	RC4	128	SHA-1
Disabled (2)	RSA	RC4	128	MD5

no export cipherspec - disable export cipherspecs (128-bit and below)

By executing this command, you are basically mandating that only high security ciphers (128-bit and above) are used during ssl sessions. Please note that the cipher order pertains to the communication channel between the client (application, database, etc.) and the device. It does not affect the keys that might be used to encrypt data by the nae server.

You can restore the original ssl cipher order by executing the restore cipherspec command.

Syntax: **no export cipherspec**

For example:

```
DemoBox (config)# no export cipherspec
SSL low security (export) ciphers successfully disabled.
```

no ssl protocol - remove the specified protocol

Syntax: **no ssl protocol <protocol>**

For example:

```
DemoBox (config)# no ssl protocol ssl3
Warning: This change affects the NAE Server and the Web Administration service.
Some Web browsers, including Internet Explorer 6.0, do not have TLS 1.0 enabled
by default. If your browser is no longer able to make a connection to this de-
vice, please check that it has TLS 1.0 enabled. (In Internet Explorer, select
Internet Options from the Tools menu, click the Advanced tab, scroll down to the
Security section, and make sure the "Use TLS 1.0" checkbox is checked.)
SSL protocol successfully disabled.
```

restore cipherspec - restore the cipherspecs to their default values

Syntax: **restore cipherspec**

For example:

```
DemoBox (config)# restore cipherspec
SSL cipher order defaults successfully restored.
DemoBox (config)# show cipherspec
```

The SSL cipher order is:

Priority	Key Exchange	Cipher	Keysize	Hash
1	RSA	AES128	128	SHA-1
2	RSA	AES256	256	SHA-1
3	RSA	3DES	168	SHA-1
Disabled (1)	RSA	RC4	128	SHA-1
Disabled (2)	RSA	RC4	128	MD5

show cipherspec - view the priority of all ciphers on the system

Syntax: **show cipherspec**

For example:

```
DemoBox# show cipherspec
```

The SSL cipher order is:

Priority	Key Exchange	Cipher	Keysize	Hash
1	RSA	AES128	128	SHA-1
2	RSA	AES256	256	SHA-1
3	RSA	3DES	168	SHA-1
Disabled (1)	RSA	RC4	128	SHA-1
Disabled (2)	RSA	RC4	128	MD5

ssl protocol - enable the use of a particular ssl protocol

The valid protocols are ssl3 and tls1.

Syntax: **ssl protocol <protocol>**

For example:

```
DemoBox (config)# ssl protocol ssl3  
SSL protocol successfully enabled.
```

show ssl - view all client-side ssl settings

Syntax: **show ssl**

For example:

```
DemoBox# show ssl  
Allowed Protocols:  
  SSL3: yes  
  TLS1: yes  
Session Key Timeout (sec): 7200
```

ssl timeout - set the session key timeout for incoming ssl client connections to the device

The default value is 7200 seconds (2 hours).

Syntax: **ssl timeout <timeout in seconds>**

For example:

```
DemoBox (config)# ssl timeout 3600  
SSL timeout successfully set.
```

Chapter 22

Security Configuration

Using the CLI, you can:

- view and configure the device's security settings, including the status of security-related functionality like global keys, use of ssl protocols and ciphers, and certificate import and export mechanisms (`security settings, show security settings`)
- make the device FIPS compliant and view the FIPS status (`fips compliant, show fips status`)
- configure and view the IP and port of the FIPS status server (`fips server, show fips server`)
- zeroize keys (`zeroize all keys`)
- zeroize keys and restore the device to its initial, factory state (`reset factory settings zeroize`)

The same functionality is available through the Management Console, however, only the CLI enables you to zeroize keys, using the `zeroize all keys` and `reset factory settings zeroize` commands, which is required before entering or leaving FIPS mode.

fips compliant - make the device FIPS compliant

This will alter the server settings listed with the `show security settings` command.

WARNING! According to FIPS requirements, you cannot enable or disable FIPS when there are keys on the device. You must *manually* delete all keys before enabling and disabling FIPS compliance. Keys are zeroized upon deletion. *We strongly recommend that you back up your keys before deleting.*

WARNING! Setting this device to be FIPS compliant forces SSL connections to the NAE Server and to the Web Administration service to use TLS 1.0 only. Some Web browsers, including Internet Explorer 6.0, do not have TLS 1.0 enabled by default. If your browser is no longer able to make a connection to this device, please check that it has TLS 1.0 enabled. (In Internet Explorer, select Internet Options from the Tools menu, click the Advanced tab, scroll down to the Security section, and make sure the "Use TLS 1.0" checkbox is checked.)

Syntax: **fips compliant**

For example:

```
DemoBox (config)# fips compliant
```

```
Warning: Setting this device to be FIPS compliant forces SSL connections to the NAE Server and to the Web Administration service to use TLS 1.0 only. Some Web browsers, including Internet Explorer 6.0, do not have TLS 1.0 enabled by default. If your browser is no longer able to make a connection to this device, please check that it has TLS 1.0 enabled. (In Internet Explorer, select Internet Options from the Tools menu, click the Advanced tab, scroll down to the Security section, and make sure the "Use TLS 1.0" checkbox is checked.)
```

```
This device is now FIPS compliant.
```

fips server - enable the FIPS status server and assign it an IP and a port

You can view the FIPS Status Report by accessing <http://<local ip>/status.html>.

Syntax: **fips server**

For example:

```
DemoBox (config)# fips server
Enable FIPS Status Server [y]: y
Available IP addresses:
    1. All
    2. 172.17.7.29
Local IP (1-2)[1]:1
Local Port [9081]: 9081
```

reset factory settings zeroize - zeroize all keys and passwords on the device

Note: For security purposes, this command can only be run from the CLI at the console. You cannot execute this command remotely via the CLI over SSH or from the Management Console.

Syntax: **reset factory settings zeroize**

For example:

```
DemoBox (config)# reset factory settings zeroize
WARNING!
This command will reset your system to its original factory
state. All configuration settings, ALL KEYS, software upgrades,
internal backup files, and log will be deleted.

In addition, all keys on the device will be zeroized,
a process that may require additional time but will render the
keys irrecoverable.

The system will automatically reboot to apply these changes.
Are you sure you want to continue? y

Are you REALLY sure you want to continue? y

Reset Factory Settings initiated
The system is rebooting.
```


security settings - change the status of security-related functionality on the device

This functionality must be disabled for FIPS compliance. These settings are automatically configured when you select **Set FIPS Compliance** in the FIPS Compliance section.

WARNING! When you enable FIPS compliance on the device, the functionality displayed here is disabled. Modifying *any* of the items in the High Security Settings section immediately takes the device out of FIPS compliance. This section should be used to *review* the key and device security functionality that has been disabled for full FIPS compliance. When the device is FIPS compliant, you should not alter these settings.

Important! According to FIPS requirements, you cannot enable or disable FIPS when there are keys on the device. You must *manually* delete all keys before enabling and disabling FIPS compliance. Keys are zeroized upon deletion. *We strongly recommend that you back up your keys before deleting.*

For more information, see the *KeySecure User Guide*.

Syntax: **security settings**

For example:

```
DemoBox (config)# security settings
Disable Creation and Use of Global Keys [y]: y
Disable Non-FIPS Algorithms and Key Sizes [y]: y
Disable FTP for Certificate Import, Backup and Restore [y]: y
Disable Certificate Import through Serial Console Paste [y]: y
Disable Hotswappable RAID Drives [y]: y
```

show fips server - view the status of the FIPS Status Server and its IP and port

You can view the FIPS Status Report by accessing <http://<Local IP>:<Local Port>/status.html>.

Syntax: **show fips server**

For example:

```
DemoBox# show fips server
    Enable FIPS Status Server:      Yes
    Local IP:                       [All]
    Local Port:                     9081
```

show fips status - view if the device is FIPS compliant

Syntax: **show fips status**

For example:

```
DemoBox# show fips status
FIPS Compliant: No
```

show security settings - view the status of security-related functionality on the device

This functionality must be disabled for FIPS compliance. These settings are automatically configured when you select **Set FIPS Compliance** in the FIPS Compliance section.

Syntax: **show security settings**

For example:

```
DemoBox# show security settings
```

```
Key Security
```

```
  Disable Creation and Use of Global Keys:           Yes
  Disable Non-FIPS Algorithms and Key Sizes:         Yes
```

```
Device Security
```

```
  Disable FTP for Certificate Import, Backup and Restore: Yes
  Disable Certificate Import through Serial Console Paste: Yes
```

```
Other Security
```

```
  Allow Key and Policy Configuration Operations: Disabled (FIPS compliant)
  Allow Key Export:                               Disabled (FIPS compliant)
  User Directory:                                 Local (FIPS compliant)
  LDAP Administrator Server Configured:          No (FIPS compliant)
  Allowed SSL Protocols:                         SSL 3.0, TLS 1.0 (not FIPS
                                                    compliant due to SSL 3.0)
  Enabled SSL Ciphers:                           Only FIPS compliant ciphers
```

zeroize all keys - delete all keys from the device and irrevocably remove all key bits from your system

Keys are not recoverable after using this command. Device configuration will remain intact. We recommend contacting customer support prior to using this command.

When executed from the KeySecure's serial console, this command also zeroizes the keys on the HSM card. You will not be able to create keys or use any key management functionality until the HSM has been initialized. Refer to the *KeySecure Quick Start Guide* for HSM initialization instructions.

When executed from the remote CLI, the HSM keys are not zeroized. You can create new keys and use other key management functionality immediately after zeroizing from the remote CLI.

Note: This command will only remove keys from the local device. To zeroize keys from an entire cluster, you must run the zeroize all keys command on each cluster member.

Syntax: **zeroize all keys**

For example:

```
DemoBox (config)# zeroize all keys
```

```
This command will delete 42 keys. Are you sure you want to continue? [n]: y
Are you REALLY sure you want to continue? [n]: y
Zeroized HSM keys.
All keys have been successfully zeroized.
```

Chapter 23

Services

Using the CLI, you can:

- view the status of the `nae-server`, `snmp`, `sshadmin`, and `webadmin` services (`show services`)
- start the services (`<nae-server | snmp | sshadmin | webadmin> run`)
- stop the services (`no <nae-server | snmp | sshadmin | webadmin> run`)
- launch the services at startup (`<nae-server | snmp | sshadmin | webadmin> startup`)
- disable their launch at startup (`no <nae-server | snmp | sshadmin | webadmin> startup`)
- halt (`halt`) and reboot (`reboot`) the device

The same functionality is available using the Management Console.

halt - halt the device

Syntax: **halt**

For example:

```
DemoBox (config)# halt
Are you sure you want to halt? [n]: y
The system is going down for system halt NOW!
The system is being halted.
Exiting command line interface.
Connection to DemoBox closed.
```

<nae-server | snmp | sshadmin | webadmin> run - activate the nae, snmp, sshadmin, or webadmin server

Syntax: **<nae-server | snmp | sshadmin | webadmin> run**

For example:

```
DemoBox (config)# nae-server run
Are you sure you want to start the NAE Server? (y/n) [n]: y
Warning: Service already started
The NAE Server successfully started.
```

<nae-server | snmp | sshadmin | webadmin> startup - activate the nae, snmp, sshadmin, or webadmin server at startup

Syntax: **<nae-server | snmp | sshadmin | webadmin> startup**

For example:

```
DemoBox (config)# snmp startup
SNMP successfully enabled on startup.
```

reboot - reboot the device

Syntax: **reboot**

For example:

```
DemoBox (config)# reboot
Are you sure you want to reboot? [n]: y
The system is going down for reboot NOW!
The system is being rebooted.
Exiting command line interface.
Connection to DemoBox closed.
```

show services - view the current service status

Syntax: **show services**

For example:

```
DemoBox# show services
Service Group  Service                Status      Startup
nae-server     NAE Server            Started    Enabled
webadmin       Web Administration     Started    Enabled
sshadmin       SSH Administration     Started    Enabled
snmp           SNMP Agent            Stopped    Disabled
```

no <nae-server | snmp | sshadmin | webadmin> run - halt the nae, snmp, sshadmin, or webadmin server

Syntax: **no <nae-server | snmp | sshadmin | webadmin> run**

For example:

```
DemoBox (config)# no sshadmin run
Are you sure you want to stop the SSH Admin service? (y/n) [n]: y
SSH Admin service successfully stopped.
DemoBox (config)# Connection to DemoBox closed by remote host.
Connection to DemoBox closed.
```

no <nae-server | snmp | sshadmin | webadmin> startup - disable the nae, snmp, sshadmin, or webadmin server at startup

Syntax: **no <nae-server | snmp | sshadmin | webadmin> startup**

For example:

```
DemoBox (config)# no webadmin startup
Web administration successfully disabled on startup.
```

Chapter 24

Statistics Configuration

Using the CLI, you can:

- view the device's operation statistics (`show statistics`)
- show the number of licenses in use (`show license usage`), and the number of licenses available (`show license`)

The same functionality is available through the Management Console.

show license - show the number of licenses currently in use

Syntax: **show license**

For example:

```
DemoBox (config)# show license
Application Server Licenses: 1
Database Licenses:          1
```

show license usage - show the number of open connections

Syntax: **show license usage**

For example:

```
DemoBox# show license usage
Client IP Address      Number of Connections
=====
172.17.17.89           1
```

show statistics - view operation statistics

The refresh interval is an optional parameter to specify how frequently the statistic information should be updated. The default refresh interval is 3 seconds. The value specified from the CLI does not affect the refresh interval on the Management Console. The `show statistics` command displays the system, connection, throughput, server, and KMIP statistics. Push the spacebar to update the statistics immediately. Use the following navigation to scroll through the statistics:

```
1: System & Connection Statistics
2: Throughput Statistics
3: Server Statistics (1)
4: Server Statistics (2)
5: KMIP Statistics
```

Syntax: **show statistics [interval]**

For example:

```
DemoBox(config)# show statistics
```

```
SafeNet i426: DemoBox Fri Dec 17 13:05:25 2010
```

```
System Statistics
```

```
CPU Utilization (%): CPU #1: 0 CPU #3: 0
                      CPU #2: 0 CPU #4: 0
```

```
System Uptime:      8 days, 14:56:17
```

```
NAE Server Connection Statistics
```

	Current/sec	Max/sec	Open	Total
Total Connections:	0	6	0	225
Non-SSL Conn:	0	6	0	225
SSL Conn:	0	0	0	0
Handshakes:	0	0		0
Resumes:	0	0		0
Failed:	0	0		0

```
NAE Server Throughput Statistics
```

	Incoming	Outgoing	Total
NAE Server (Mbits/s):	0	0	0

```
Interface Throughput Statistics
```

	Incoming	Outgoing	Total
Ethernet #1 (Mbits/s):	0	0	0

```
Server Statistics (1)
```

	Current/sec	Max/sec	Success	Failed
Total Operations	0	27	1047	28
Key Generate	0	5	86	0
Key Version Generate	0	6	46	0
Key Delete	0	13	143	10
Key Query	0	0	28	0
Key Information	0	5	57	0
Key Import	0	4	33	0
Key Export	0	4	43	0
Key Modify	0	8	64	0
Key Version Modify	0	2	10	0
Key Clone	0	3	24	0
Cryptographic Operation	0	11	238	8

```
Server Statistics (2)
```

	Current/sec	Max/sec	Success	Failed
Total Operations	0	27	1047	28
Public Key Export	0	1	10	0
Certificate Export	0	3	10	0
CA Export	0	3	10	0
Key Certificate Export	0	0	0	10
Random Generate	0	3	10	0
Record Event	0	3	10	0
Authenticate	0	6	225	0

KMIP Statistics

	Current/sec	Max/sec	Success	Failed
Total Operations	0	0	0	0
Locate	0	0	0	0
Register	0	0	0	0
Get	0	0	0	0
Get Attributes	0	0	0	0
Query	0	0	0	0

Chapter 25

System Health

Using the CLI, you can:

- view the status of the RAID disks, power supplies and cooling fans (`show system health`)
- add and remove RAID disks (`raid add`, `raid remove`)

The same functionality is available through the Management Console.

raid add - add a disk to the device

Syntax: **raid add** <disk slot number>

For example:

```
DemoBox (config)# raid add 2
Warning: Adding a RAID disk is a potentially dangerous operation that can
result in system instability.
```

```
Are you sure you want to add the disk? [n]: y
Disk addition may take several moments to perform. Please be patient and
wait for the operation to complete.
```

```
Are you sure you want to proceed? [n]: y
Adding RAID disk...
```

```
RAID disk successfully added.
```

If RAID is not supported on the device, or if no more disks are allowed, you will see an error message.

raid remove - remove a disk from the device

Syntax: **raid remove** <disk slot number>

For example:

```
DemoBox (config)# raid remove 2
Warning: Removing a RAID disk is a potentially dangerous operation that can
result in system instability.
```

```
Are you sure you want to remove the disk? [n]: y
Disk removal may take several moments to perform. Please be patient and
wait for the operation to complete.
```

```
Are you sure you want to proceed false? [n]: y
Removing RAID disk...
```

```
RAID disk removed.
```


show system health - view the status of RAID disks, power supply units and cooling fans

Syntax: **show system health**

For example:

```
DemoBox# show system health
```

```
RAID Status
```

```
=====
```

```
    Disk Slot #0:      Operational
```

```
    Disk Slot #1:      Operational
```

```
Power Supply Status
```

```
=====
```

```
    Power Supply #1:    Not receiving power
```

```
    Power Supply #2:    Operational
```

```
Warning: A power supply is not plugged in or is malfunctioning
```

```
Cooling Fan Status
```

```
=====
```

```
    Fan Status:         Operational
```

Chapter 26

System Information & Upgrade

Using the CLI, you can:

- view the device's model number and box ID (`show device`)
- view software licenses (`show license`)
- view the software copyright (`show copyright`)
- view software version and installation date (`show software`)
- display the list of activated features (`show activate feature`)
- install a new version of the server software (`software install`)
- rollback to a previous version (`software rollback`)

The same functionality is available through the Management Console - except for the `software rollback` command. You cannot use the Management Console to rollback to a previous software version.

show activated feature - display a list of all the activated features on the device or the details of a specific feature

Syntax: **show activated feature**
show activated feature "<name>"

For example:

```
DemoBox# show activated feature
ProtectFile Manager
  Activation Date:      N/A
  Expiration Date:     Never
  Status:              Active
```

```
DemoBox# show activated feature "ProtectFile Manager"
ProtectFile Manager
  Activation Date:      N/A
  Expiration Date:     Never
  Status:              Active
```

show copyright - view the software copyright

Syntax: **show copyright**

For example:

```
DemoBox# show copyright
Copyright (c) 2000-2012 SafeNet, Inc.
```

show device - view the device's model number and box ID

Syntax: **show device**

For example:

```
DemoBox (config)# show device
Product: SafeNet k460
Box ID: 4ME2NO99
Software Version: 6.1.0
Software Install Date: Sat Apr 30 19:33:28 EST 2011
```

show license - view the licenses currently active on the device

Syntax: **show license**

For example:

```
DemoBox# show license
Application Server Licenses: 1
Database Licenses:          1
Transform Utility Licenses: 1
```

show software - view information about the current system software

Syntax: **show software**

For example:

```
DemoBox# show software
Core Software
  Version:          6.1.0
  Description:      Core Software
  Install Date:    Wed Dec 8 03:35:27 PST 2010
Content Encryption Service Engine
  Version:          6.1.0
  Description:      Content Encryption Service Engine
  Install Date:    Wed Dec 8 03:35:27 PST 2010
```

software install - install new software or a software patch

The device will reboot after the upgrade.

Syntax: **software install**

For example:

```
DemoBox (config)# software install
Please pick one of the following installation sources:
  1) FTP    2) SCP
Source (1-2): 2
Enter the host: 172.20.40.33
Enter the filename: 009848-001_keysecure_server_upgrade_v6.1.0-08.iou
```

Enter the username: YourUser
Enter the password:

Warning: Applying the software upgrade/install may take a long time and the system will automatically reboot.

Are you sure you want to apply a software upgrade? [n]: y
Step 1 of 18 steps completed.
Step 2 of 18 steps completed.
Step 3 of 18 steps completed.
Step 4 of 18 steps completed.
Step 5: preparing to install. This may take a few minutes
Step 5 of 18 steps completed.
Step 6 of 18 steps completed.
Step 7: installing patch. This may take a few minutes
Step 7 of 18 steps completed.
Step 8 of 18 steps completed.
Step 9 of 18 steps completed.
Step 10 of 18 steps completed.
Step 11 of 18 steps completed.
Step 12: doing post install. This may take a few minutes
Step 12 of 18 steps completed.
Step 13 of 18 steps completed.
Step 14 of 18 steps completed.
Step 15 of 18 steps completed.
Step 16 of 18 steps completed.
Step 17 of 18 steps completed.
Step 18 of 18 steps completed.
Patch installer: Patch installed successfully.
System will reboot automatically...
The system is going down for reboot NOW!
Connection to DemoBox closed by remote host.
Connection to DemoBox closed.

software rollback - roll back one version of the server software

Software rollbacks can only be performed using the CLI, this functionality is not available through the Management Console. The device will reboot after the rollback.

Syntax: **software rollback**

For example:

```
DemoBox (config)# software rollback
```


WARNING: Preparing to ROLL BACK SOFTWARE!

This action will remove the current software version and restore the previous version.

It will also remove all configuration changes made since the last software upgrade.

For example:

All new keys will be lost.



All modifications to existing keys will be undone.
All new license files will be lost.
All new administrator accounts will be removed.
All modifications to existing administrator accounts - including password changes - will be lost.

To avoid data loss, make an EXTERNAL backup of the device's current configuration before rolling back the software. After the software rollback, restore the configuration backup.

You must manually upload any missing license files after the rollback.

Once the software rollback completes, you can only access the device using an administrator account and password that were valid in the previous version. Otherwise, you will be LOCKED OUT OF YOUR DEVICE.

Please type "rollback" to initiate rollback or "q" to quit.

rollback

Patch rollback started. This should take less than 1 minute.
Patch installer: Patch rollback is successful.
System will reboot...
The system is going down for reboot NOW!
Software rollback successful.