Working With Configuration Files

This chapter describes how to use commands that show, copy, and erase the configuration file. It contains the following sections:

- Displaying the Current Configuration, page 16-1
- Displaying the Current Submode Configuration, page 16-3
- Filtering the Current Configuration Output, page 16-16
- Filtering the Current Submode Configuration Output, page 16-18
- Displaying the Contents of a Logical File, page 16-19
- Backing Up and Restoring the Configuration File Using a Remote Server, page 16-21
- Creating and Using a Backup Configuration File, page 16-23
- Erasing the Configuration File, page 16-23

Displaying the Current Configuration

Note

The CLI output is an example of what your configuration may look like. It will not match exactly due to the optional setup choices, sensor model, and IPS 7.1 version you have installed.

Use the `show configuration` or the `more current-config` command to display the contents of the current configuration. To display the contents of the current configuration, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Log in to the CLI.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Display the current configuration.</td>
</tr>
</tbody>
</table>

```
sensor# show configuration
! ------------------------------
! Current configuration last modified Fri Apr 10 13:29:06 2010
! ------------------------------
! Version 7.1(1)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S383.0   2009-02-20
!     Virus Update        V1.4     2007-03-02
! ------------------------------
service interface
```
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 192.0.2.0/24,192.0.2.17
telnet-option enabled
access-list 0.0.0.0/0
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
service external-product-interface
exit
! ------------------------------
service health-monitor
exit
! ------------------------------
service global-correlation
exit
! ------------------------------
service analysis-engine
exit
sensor#
Displaying the Current Submode Configuration

Use the `show settings` command in a submode to display the current configuration of that submode. To display the current configuration of a submode, follow these steps:

**Step 1** Log in to the CLI.

**Step 2** Display the current configuration of the service analysis engine submode.

```
sensor# configure terminal
sensor(config)# service analysis-engine
sensor(config-ana)# show settings
          global-parameters
            ip-logging
              max-open-iplog-files: 20 <defaulted>
            virtual-sensor (min: 1, max: 255, current: 1)
              <protected entry>
                name: vs0 <defaulted>
                  description: default virtual sensor <defaulted>
                  signature-definition: sig0 <protected>
                  event-action-rules: rules0 <protected>
                  physical-interface (min: 0, max: 999999999, current: 0)
                  logical-interface (min: 0, max: 999999999, current: 0)
          sensor(config-ana)# exit
          sensor(config)# exit
          sensor# 
```

**Step 3** Display the current configuration of the service anomaly detection submode.

```
sensor(config)# service anomaly-detection ad0
sensor(config-ano)# show settings
          worm-timeout: 600 seconds <defaulted>
          learning-accept-mode
            auto
            action: rotate <defaulted>
            schedule
              periodic-schedule
                start-time: 10:00:00 <defaulted>
                interval: 24 hours <defaulted>
            internal-zone
              enabled: true <defaulted>
          sensor(config-ano)# exit
          sensor(config)# exit
          sensor# 
```
ip-address-range: 0.0.0.0 <defaulted>
tcp
-----------------------------------------------
dst-port (min: 0, max: 65535, current: 0)
-----------------------------------------------
default-thresholds
-----------------------------------------------
scanner-threshold: 100 <defaulted>
threshold-histogram (min: 0, max: 3, current: 3)
-----------------------------------------------
<protected entry>
dest-ip-bin: low <defaulted>
num-source-ips: 10 <defaulted>
<protected entry>
dest-ip-bin: medium <defaulted>
num-source-ips: 1 <defaulted>
<protected entry>
dest-ip-bin: high <defaulted>
num-source-ips: 1 <defaulted>
-----------------------------------------------
enabled: true <defaulted>
-----------------------------------------------
udp
-----------------------------------------------
dst-port (min: 0, max: 65535, current: 0)
-----------------------------------------------
default-thresholds
-----------------------------------------------
scanner-threshold: 100 <defaulted>
threshold-histogram (min: 0, max: 3, current: 3)
-----------------------------------------------
<protected entry>
dest-ip-bin: low <defaulted>
num-source-ips: 10 <defaulted>
<protected entry>
dest-ip-bin: medium <defaulted>
num-source-ips: 1 <defaulted>
<protected entry>
dest-ip-bin: high <defaulted>
num-source-ips: 1 <defaulted>
-----------------------------------------------
enabled: true <defaulted>
-----------------------------------------------
other
-----------------------------------------------
protocol-number (min: 0, max: 255, current: 0)
-----------------------------------------------
default-thresholds
-----------------------------------------------
scanner-threshold: 100 <defaulted>
threshold-histogram (min: 0, max: 3, current: 3)
-----------------------------------------------
<protected entry>
dest-ip-bin: low <defaulted>
num-source-ips: 10 <defaulted>
<protected entry>
dest-ip-bin: medium <defaulted>
num-source-ips: 1 <defaulted>
<protected entry>
dest-ip-bin: high <defaulted>
num-source-ips: 1 <defaulted>
<protected entry>
dest-ip-bin: high <defaulted>
num-source-ips: 1 <defaulted>
-----------------------------------------------
-----------------------------------------------
enabled: true <defaulted>
-----------------------------------------------
-----------------------------------------------
illegal-zone

 enabled: true <defaulted>
 ip-address-range: 0.0.0.0 <defaulted>
tcp
-----------------------------
dst-port (min: 0, max: 65535, current: 0)
-----------------------------------------------
-----------------------------------------------
default-thresholds

 scanner-threshold: 100 <defaulted>
 threshold-histogram (min: 0, max: 3, current: 3)

<protected entry>
dest-ip-bin: low <defaulted>
num-source-ips: 10 <defaulted>
<protected entry>
dest-ip-bin: medium <defaulted>
num-source-ips: 1 <defaulted>
<protected entry>
dest-ip-bin: high <defaulted>
num-source-ips: 1 <defaulted>
-----------------------------------------------
-----------------------------------------------
enabled: true <defaulted>
-----------------------------------------------
-----------------------------------------------
udp
-----------------------------
dst-port (min: 0, max: 65535, current: 0)
-----------------------------------------------
-----------------------------------------------
default-thresholds

 scanner-threshold: 100 <defaulted>
 threshold-histogram (min: 0, max: 3, current: 3)

<protected entry>
dest-ip-bin: low <defaulted>
num-source-ips: 10 <defaulted>
<protected entry>
dest-ip-bin: medium <defaulted>
num-source-ips: 1 <defaulted>
<protected entry>
dest-ip-bin: high <defaulted>
num-source-ips: 1 <defaulted>
-----------------------------------------------
-----------------------------------------------
enabled: true <defaulted>
-----------------------------------------------
-----------------------------------------------
other
-----------------------------
protocol-number (min: 0, max: 255, current: 0)
-----------------------------------------------
default-thresholds
scanner-threshold: 100 <defaulted>
threshold-histogram (min: 0, max: 3, current: 3)

<protected entry>
dest-ip-bin: low <defaulted>
num-source-ips: 10 <defaulted>
<protected entry>
dest-ip-bin: medium <defaulted>
num-source-ips: 1 <defaulted>
<protected entry>
dest-ip-bin: high <defaulted>
num-source-ips: 1 <defaulted>

enabled: true <defaulted>

-----------------------------------------------

dest-ip-bin: low <defaulted>
num-source-ips: 10 <defaulted>
<protected entry>
dest-ip-bin: medium <defaulted>
num-source-ips: 1 <defaulted>
<protected entry>
dest-ip-bin: high <defaulted>
num-source-ips: 1 <defaulted>

-----------------------------------------------

enabled: true <defaulted>

-----------------------------------------------

default-thresholds

scanner-threshold: 100 <defaulted>
threshold-histogram (min: 0, max: 3, current: 3)

<protected entry>
dest-ip-bin: low <defaulted>
num-source-ips: 10 <defaulted>
<protected entry>
dest-ip-bin: medium <defaulted>
num-source-ips: 1 <defaulted>
<protected entry>
dest-ip-bin: high <defaulted>
num-source-ips: 1 <defaulted>

-----------------------------------------------

enabled: true <defaulted>

-----------------------------------------------

tcp

dst-port (min: 0, max: 65535, current: 0)

default-thresholds

scanner-threshold: 100 <defaulted>
threshold-histogram (min: 0, max: 3, current: 3)

<protected entry>
dest-ip-bin: low <defaulted>
num-source-ips: 10 <defaulted>
<protected entry>
dest-ip-bin: medium <defaulted>
num-source-ips: 1 <defaulted>
<protected entry>
dest-ip-bin: high <defaulted>
num-source-ips: 1 <defaulted>

-----------------------------------------------

enabled: true <defaulted>

-----------------------------------------------

udp

dst-port (min: 0, max: 65535, current: 0)

default-thresholds

scanner-threshold: 100 <defaulted>
threshold-histogram (min: 0, max: 3, current: 3)

<protected entry>
dest-ip-bin: low <defaulted>
num-source-ips: 10 <defaulted>
<protected entry>
dest-ip-bin: medium <defaulted>
num-source-ips: 1 <defaulted>
<protected entry>
dest-ip-bin: high <defaulted>
num-source-ips: 1 <defaulted>

-----------------------------------------------
Step 4  Display the current configuration of the service authentication submode.

sensor# configure terminal
sensor(config)# service authentication
sensor(config-aut)# show settings
            attemptLimit: 0 <defaulted>
sensor(config-aut)# exit
sensor(config)# exit
sensor#

Step 5  Display the current configuration of the service event action rules submode.

sensor# configure terminal
sensor(config)# service event-action-rules rules0
sensor(config-rul)# show settings
            variables (min: 0, max: 255, current: 0)
            overrides (min: 0, max: 12, current: 0)
            filters (min: 0, max: 4096, current: 0 - 0 active, 0 inactive)
            general
            global-overrides-status: Enabled <defaulted>
global-filters-status: Enabled <defaulted>
global-summarization-status: Enabled <defaulted>
Displaying the Current Submode Configuration

global-metaevent-status: Enabled <defaulted>
global-deny-timeout: 3600 <defaulted>
global-block-timeout: 30 <defaulted>
max-denied-attackers: 10000 <defaulted>

-----------------------------------------------
target-value (min: 0, max: 5, current: 0)
-----------------------------------------------

sensor(config-rul)# exit
sensor(config)# exit
sensor# exit

Step 6  Display the current configuration of the external product interface submode.

sensor(config)# service external-product-interface
sensor(config-ext)# show settings
cisco-security-agents-mc-settings (min: 0, max: 2, current: 0)

-----------------------------------------------

sensor(config-ext)# exit
sensor(config)# exit
sensor#

Step 7  Display the current configuration of the service global-correlation submode.

sensor# configure terminal
sensor(config)# service global-correlation
sensor(config-glo)# show settings
network-participation: off <defaulted>
global-correlation-inspection: on <defaulted>
global-correlation-inspection-influence: standard <defaulted>
reputation-filtering: on <defaulted>
test-global-correlation: off <defaulted>

sensor(config-glo)# exit
sensor(config)# exit
sensor#

Step 8  Display the current configuration of the service health-monitor submode.

sensor# configure terminal
sensor(config)# service health-monitor
sensor(config-hea)# show settings
enable-monitoring: true <defaulted>
persist-security-status: 5 minutes <defaulted>
heartbeat-events

---
enable: 300 seconds <defaulted>

---
application-failure-policy

---
enable: true <defaulted>
status: red <defaulted>

---
bypass-policy

---
enable: true <defaulted>
status: red <defaulted>

---
interface-down-policy

---
enable: true <defaulted>
status: red <defaulted>

---
inspection-load-policy

---
enable: true <defaulted>
yellow-threshold: 80 percent <defaulted>
red-threshold: 91 percent <defaulted>

missed-packet-policy

enable: true <defaulted>
yellow-threshold: 1 percent <defaulted>
red-threshold: 6 percent <defaulted>

memory-usage-policy

enable: false <defaulted>
yellow-threshold: 80 percent <defaulted>
red-threshold: 91 percent <defaulted>

signature-update-policy

enable: true <defaulted>
yellow-threshold: 30 days <defaulted>
red-threshold: 60 days <defaulted>

license-expiration-policy

enable: true <defaulted>
yellow-threshold: 30 days <defaulted>
red-threshold: 0 days <defaulted>

event-retrieval-policy

enable: true <defaulted>
yellow-threshold: 300 seconds <defaulted>
red-threshold: 600 seconds <defaulted>

global-correlation-policy

enable: true <defaulted>
yellow-threshold: 86400 seconds <protected>
red-threshold: 259200 seconds <protected>

network-participation-policy

enable: false <defaulted>
yellow-threshold: 1 connection failures <protected>
red-threshold: 6 connection failures <protected>

Step 9  Display the current configuration of the service host submode.

sensor# configure terminal
sensor(config)# service host
sensor(config-hos)# show settings
network-settings
-----------------------------------------------
host-ip: 192.0.2.0/24,192.0.2.17 default: 192.168.1.2/24,192.168.1.1
host-name: sensor default: sensor
telnet-option: enabled default: disabled
access-list (min: 0, max: 512, current: 2)
-----------------------------------------------
network-address: 10.0.0.0/8
-----------------------------------------------
network-address: 64.0.0.0/8

ftp-timeout: 300 seconds <defaulted>
login-banner-text: <defaulted>

time-zone-settings

offset: 0 minutes default: 0
standard-time-zone-name: UTC default: UTC

ntp-option
disabled

t summertime-option
disabled

auto-upgrade-option
disabled

crypto

key (min: 0, max: 10, current: 2)

rsa-pubkey

<protected entry>
name: realm-cisco.pub <defaulted>
type

rsa-pubkey

length: 2048 <defaulted>

rsa-pubkey

<protected entry>
name: realm-trend.pub <defaulted>
type

rsa-pubkey

length: 2048 <defaulted>

rsa-pubkey

<protected entry>
name: realm-cisco.pub <defaulted>
type

rsa-pubkey

length: 2048 <defaulted>

rsa-pubkey

<protected entry>
name: realm-trend.pub <defaulted>
type

rsa-pubkey

length: 2048 <defaulted>

rsa-pubkey
Displaying the Current Submode Configuration

```
4528979577973491984056587045214514820063366950731346400044308491594626434706999
47608668228140148300633995342046447695090524434952536370652725224510771122235
80181150460544783251498481432705991010069844368525754878413669427639752950801767
9990530923523245629558008672420329791409598422432844391582223138423799100838191
9 <defaulted>

Step 10  Display the current configuration of the service interface submode.

sensor# configure terminal
sensor(config)# service interface
sensor(config-int)# show settings

physical-interfaces (min: 0, max: 999999999, current: 4)

<protected entry>
name: GigabitEthernet0/0 <defaulted>

-----------------------------------------------
media-type: tx <protected>
description: <defaulted>
admin-state: disabled <defaulted>
duplex: auto <defaulted>
speed: auto <defaulted>
alt-tcp-reset-interface

none

-----------------------------------------------
subinterface-type

none

-----------------------------------------------

<protected entry>
name: GigabitEthernet0/1 <defaulted>

-----------------------------------------------
media-type: tx <protected>
description: <defaulted>
admin-state: disabled <protected>
duplex: auto <defaulted>
speed: auto <defaulted>
alt-tcp-reset-interface

none

-----------------------------------------------
subinterface-type

none

-----------------------------------------------

<protected entry>
name: GigabitEthernet2/0 <defaulted>
```
Chapter 16  Working With Configuration Files

Displaying the Current Submode Configuration

---
media-type: xl <protected>
description: <defaulted>
admin-state: disabled <defaulted>
duplex: auto <defaulted>
speed: auto <defaulted>
alt-tcp-reset-interface
---

none
---

subinterface-type
---

none
---

------

<protected entry>

name: GigabitEthernet2/1 <defaulted>

---
media-type: xl <protected>
description: <defaulted>
admin-state: disabled <defaulted>
duplex: auto <defaulted>
speed: auto <defaulted>
alt-tcp-reset-interface
---

none
---

subinterface-type
---

none
---

------

command-control: GigabitEthernet0/1 <protected>
inline-interfaces (min: 0, max: 999999999, current: 0)
---
bypass-mode: auto <defaulted>
interface-notifications
---
missed-percentage-threshold: 0 percent <defaulted>
notification-interval: 30 seconds <defaulted>
idle-interface-delay: 30 seconds <defaulted>
---
sensor(config-int)# exit
sensor(config)# exit
sensor#

Step 11  Display the current configuration for the service logger submode.

sensor# configure terminal
sensor(config)# service logger
sensor(config-log)# show settings
master-control
---
enable-debug: false <defaulted>
individual-zone-control: false <defaulted>
-----------------------------------------------
zone-control (min: 0, max: 999999999, current: 14)
-----------------------------------------------
<protected entry>
zone-name: Cid
severity: debug <defaulted>
<protected entry>
zone-name: AuthenticationApp
severity: warning <defaulted>
<protected entry>
zone-name: Cli
severity: warning <defaulted>
<protected entry>
zone-name: csi
severity: warning <defaulted>
<protected entry>
zone-name: ctlTransSource
severity: warning <defaulted>
<protected entry>
zone-name: IdapiCtlTrans
severity: warning <defaulted>
<protected entry>
zone-name: IdsEventStore
severity: warning <defaulted>
<protected entry>
zone-name: MpInstaller
severity: warning <defaulted>
<protected entry>
zone-name: nac
severity: warning <defaulted>
<protected entry>
zone-name: sensorApp
severity: warning <defaulted>
<protected entry>
zone-name: tls
severity: warning <defaulted>
<protected entry>
zone-name: intfc
severity: warning <defaulted>
<protected entry>
zone-name: cmgr
severity: warning <defaulted>
<protected entry>
zone-name: cplane
severity: warning <defaulted>
-----------------------------------------------
sensor(config-log)# exit
sensor(config)# exit
sensor#

Step 12 Display the current configuration for the service network access submode.

sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)# show settings
general
-----------------------------------------------
log-all-block-events-and-errors: true <defaulted>
enable-nvram-write: false <defaulted>
enable-acl-logging: false <defaulted>
allow-sensor-block: false <defaulted>
block-enable: true <defaulted>
block-max-entries: 250 <defaulted>
max-interfaces: 250 <defaulted>
rate-limit-max-entries: 250 <defaulted>
master-blocking-sensors (min: 0, max: 100, current: 0)
never-block-hosts (min: 0, max: 250, current: 0)
never-block-networks (min: 0, max: 250, current: 0)
block-hosts (min: 0, max: 250, current: 0)
block-networks (min: 0, max: 250, current: 0)
user-profiles (min: 0, max: 250, current: 1)
profile-name: test

enable-password: <hidden>
password: <hidden>
username: <defaulted>
cat6k-devices (min: 0, max: 250, current: 0)
router-devices (min: 0, max: 250, current: 0)
firewall-devices (min: 0, max: 250, current: 0)

sensor(config-net)# exit
sensor(config)# exit
sensor#

Step 13  Display the current configuration for the notification submode.

sensor# configure terminal
sensor(config)# service notification
sensor(config-not)# show settings
trap-destinations (min: 0, max: 10, current: 0)
error-filter: error|fatal <defaulted>
enable-detail-traps: false <defaulted>
enable-notifications: false <defaulted>
enable-set-get: false <defaulted>
smn-agent-port: 161 <defaulted>
smn-agent-protocol: udp <defaulted>
read-only-community: public <defaulted>
read-write-community: private <defaulted>
trap-community-name: public <defaulted>
system-location: Unknown <defaulted>
system-contact: Unknown <defaulted>
sensor(config-not)# exit
sensor(config)# exit
sensor#
Chapter 16  Working With Configuration Files

Displaying the Current Submode Configuration

Step 14 Display the current configuration for the signature definition submode.

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# show settings
variables (min: 0, max: 256, current: 1)
-----------------------------------------------
<protected entry>
variable-name: WEBPORTS
-----------------------------------------------
web-ports: 80-80,3128-3128,8000-8000,8010-8010,8080-8080,8888-8888,824326 <defaulted>
-----------------------------------------------
application-policy
-----------------------------------------------
http-policy
-----------------------------------------------
http-enable: false <defaulted>
max-outstanding-http-requests-per-connection: 10 <defaulted>
aic-web-ports: 80-80,3128-3128,8000-8000,8010-8010,8080-8080,8888-8888,824326 <defaulted>
-----------------------------------------------
ftp-enable: false <defaulted>
-----------------------------------------------
fragment-reassembly
-----------------------------------------------
ip-reassemble-mode: nt <defaulted>
-----------------------------------------------
stream-reassembly
-----------------------------------------------
```

Step 15 Display the current configuration for the SSH known hosts submode.

```
sensor# configure terminal
sensor(config)# service ssh-known-hosts
sensor(config-ssh)# show settings
real-keys (min: 0, max: 500, current: 0)
-----------------------------------------------
sensor(config-ssh)# exit
sensor(config)# exit
```

Step 16 Display the current configuration for the trusted certificates submode.

```
sensor# configure terminal
sensor(config)# service trusted-certificate
sensor(config-tru)# show settings
trusted-certificates (min: 0, max: 500, current: 1)
-----------------------------------------------
common-name: 10.89.130.108
```

Cisco Intrusion Prevention System CLI Sensor Configuration Guide for IPS 7.1
Filtering the Current Configuration Output

Use the `more` keyword | [begin | exclude | include] `regular-expression` command to search the output of the more command. The following options apply:

- **keyword**—Specifies either the current-config or the backup-config:
  - `current-config`—Specifies the current running configuration. This configuration becomes persistent as the commands are entered.
  - `backup-config`—Specifies the storage location for the configuration backup file.
- `|`—The pipe symbol indicates that an output processing specification follows.
- **begin**—Begins unfiltered output of the `more` command with the first line that contains the regular expression specified.
- **exclude**—Excludes lines in the output of the `more` command that contain a particular regular expression.
- **include**—Includes only the lines in the output of the `more` command that contain the regular expression you specify.
- **regular-expression**—Specifies any regular expression found in the `more` command output.

---

Note The `regular-expression` option is case sensitive and allows for complex matching requirements.

Filtering Using the More Command

To filter the more command, follow these steps:

**Step 1** Log in to the CLI using an account with administrator privileges.

**Step 2** Filter the current-config output beginning with the regular expression “ip,” for example.

```
sensor# more current-config | begin ip
generating current config:
host-ip 192.0.2.0/24,192.0.2.17
host-name sensor
telnet-option enabled
access-list 10.0.0.0/8
access-list 64.0.0.0/8
```
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
exit
! ------------------------------
service interface
exit
! ------------------------------
service logger
master-control
enable-debug true
exit
exit
! ------------------------------
service network-access
general
log-all-block-events-and-errors true
--MORE--

Note Press Ctrl-C to stop the output and return to the CLI prompt.

Step 3 Exclude the regular expression “ip” from the current-config output.
sensor# more current-config | exclude ip
generating current config:
! ------------------------------
! Version 7.0(1)
! Current configuration last modified Fri Feb 11 15:10:57 2009
! ------------------------------
service analysis-engine
virtual_sensor vs0
physical_interface FastEthernet0/1
exit
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host_name sensor
telnet-option enabled
access-list 10.0.0.0/8
access-list 64.0.0.0/8
exit
time-zone-settings
--MORE--

Note Press Ctrl-C to stop the output and return to the CLI prompt.

Step 4 Include the regular expression “ip” in the current-config output.
sensor# more current-config | include ip
generating current config:
Filtering the Current Submode Configuration Output

Use the `show settings | [begin | exclude | include] regular_expression` command in the submode you are interested in to search or filter the output of the contents of the submode configuration. The following options apply:

- `|`—The pipe symbol indicates that an output processing specification follows.
- `begin`—Begins unfiltered output of the `show settings` command with the first line that contains the regular expression specified.
- `exclude`—Excludes lines in the output of the `show settings` command that contain a particular regular expression.
- `include`—Includes only the lines in the output of the `show settings` command that contain the regular expression you specify.
- `regular_expression`—Specifies any regular expression found in the `show settings` command output.

**Note** The `regular_expression` option is case sensitive and allows for complex matching requirements.

Filtering the Submode Output

To search or filter the output of the contents of the submode configuration, follow these steps:

**Step 1**
Log in to the CLI using an account with administrator privileges.

**Step 2**
Search the output of the event action rules settings for the regular expression, “filters,” for example.

```
sensor# configure terminal
sensor(config)# service event-action-rules
sensor(config-rul)# show settings | begin filters
filters (min: 0, max: 4096, current: 0 - 0 active, 0 inactive)
-----------------------------------------------
general
-----------------------------------------------
global-overrides-status: Enabled <defaulted>
global-filters-status: Enabled <defaulted>
global-summarization-status: Enabled <defaulted>
global-metaevent-status: Enabled <defaulted>
global-deny-timeout: 3600 <defaulted>
global-block-timeout: 15 default: 30
max-denied-attackers: 10000 <defaulted>
-----------------------------------------------
target-value (min: 0, max: 5, current: 0)
-----------------------------------------------
sensor(config-rul)#
```

**Step 3**
Filter the output of the network access settings to exclude the regular expression.

```
sensor# configure terminal
sensor(config)# service network-access
```
sensor(config-net)# show settings | exclude false

general
-----------------------------------------------
   log-all-block-events-and-errors: true default: true
   block-enable: true default: true
   block-max-entries: 11 default: 250
   max-interfaces: 13 default: 250
   master-blocking-sensors (min: 0, max: 100, current: 1)
-----------------------------------------------
   ipaddress: 192.0.2.0
-----------------------------------------------
   password: <hidden>
   port: 443 default: 443
   tis: true default: true
   username: cisco default:
-----------------------------------------------
-----------------------------------------------
   never-block-hosts (min: 0, max: 250, current: 1)
-----------------------------------------------
   ip-address: 10.89.146.112
-----------------------------------------------
   never-block-networks (min: 0, max: 250, current: 1)
-----------------------------------------------
   ip-address: 88.88.88.0/24
--MORE--

Step 4  Filter the output of the host settings to include the regular expression “ip.”

sensor# configure terminal
sensor(config)# service host
sensor(config-hos)# show settings | include ip
   host-ip: 192.0.2.0/24,192.0.2.17 default: 192.168.1.2/24,192.168.1.1
sensor(config-hos)#

---Displaying the Contents of a Logical File---

Note  Operators and viewers can only display the current configuration. Only administrators can view hidden fields such as passwords.

Use the more keyword command to display the contents of a logical file, such as the current system configuration or the saved backup system configuration. The following options apply:

- keyword—Specifies either the current-config or the backup-config:
  - current-config—Specifies the current running configuration. This configuration becomes persistent as the commands are entered.
  - backup-config—Specifies the storage location for the configuration backup file.

You can disable the more prompt in more current-config or more backup-config by setting the terminal length to zero using the terminal length 0 command. The more command then displays the entire file content without pausing.
Displaying the Logical File Contents

To display the contents of a logical file, follow these steps:

**Step 1**
Log in to the CLI using an account with administrator privileges.

**Step 2**
Display the contents of the current configuration file.

```bash
sensor# more current-config
Generating current config:

The current configuration is displayed.

! -----------------------------------------------
! Current configuration last modified Fri Apr 10 13:29:06 2011
! -----------------------------------------------
! Version 7.1(1)
! Host:
!   Realm Keys          key1.0
! Signature Definition:
!   Signature Update    S383.0   2009-02-20
!   Virus Update        V1.4     2007-03-02
! -----------------------------------------------
-service interface
exit
! -----------------------------------------------
-service authentication
exit
! -----------------------------------------------
-service event-action-rules rules0
exit
! -----------------------------------------------
-service host
network-settings
host-ip 192.168.1.2/24,192.168.1.1
telnet-option enabled
access-list 0.0.0.0/0
exit
exit
! -----------------------------------------------
-service logger
exit
! -----------------------------------------------
-service network-access
exit
! -----------------------------------------------
-service notification
exit
! -----------------------------------------------
-service signature-definition sig0
exit
! -----------------------------------------------
-service ssh-known-hosts
exit
! -----------------------------------------------
-service trusted-certificates
exit
! -----------------------------------------------
-service web-server
exit
! -----------------------------------------------
-service anomaly-detection ad0
exit
! -----------------------------------------------
```
Chapter 16      Working With Configuration Files

Back Up and Restore the Configuration File Using a Remote Server

We recommend copying the current configuration file to a remote server before upgrading.

Use the copy [/erase] source_url destination_url keyword command to copy the configuration file to a remote server. You can then restore the current configuration from the remote server. You are prompted to back up the current configuration first. The following options apply:

- **/erase**—Erases the destination file before copying.
  This keyword only applies to the current-config; the backup-config is always overwritten. If this keyword is specified for destination current-config, the source configuration is applied to the system default configuration. If it is not specified for the destination current-config, the source configuration is merged with the current-config.

- **source_url**—The location of the source file to be copied. It can be a URL or keyword.

- **destination_url**—The location of the destination file to be copied. It can be a URL or a keyword.

- **current-config**—The current running configuration. The configuration becomes persistent as the commands are entered.

- **backup-config**—The storage location for the configuration backup.

The exact format of the source and destination URLs varies according to the file. Here are the valid types:

- **ftp:**—Source or destination URL for an FTP network server. The syntax for this prefix is:
  ftp://[[username@] location]/relativeDirectory[/filename]
  ftp://[[username@]location]/absoluteDirectory[/filename]

- **scp:**—Source or destination URL for the SCP network server. The syntax for this prefix is:
  scp://[[username@] location]/relativeDirectory[/filename]
  scp://[[username@] location]/absoluteDirectory[/filename]
Chapter 16  Working With Configuration Files

Back up and restoring the configuration file using a remote server

### Note
If you use FTP or SCP protocol, you are prompted for a password. If you use SCP protocol, you must also add the remote host to the SSH known hosts list.

- **http**—Source URL for the web server. The syntax for this prefix is:
  ```plaintext
  http://[[username@]location]/directory/filename
  ```
- **https**—Source URL for the web server. The syntax for this prefix is:
  ```plaintext
  https://[[username@]location]/directory/filename
  ```

### Note
HTTP and HTTPS prompt for a password if a username is required to access the website. If you use HTTPS protocol, the remote host must be a TLS trusted host.

### Caution
Copying a configuration file from another sensor may result in errors if the sensing interfaces and virtual sensors are not configured the same.

### Backing up the current configuration to a remote server

To back up your current configuration to a remote server, follow these steps:

**Step 1** Log in to the CLI using an account with administrator privileges.

**Step 2** Back up the current configuration to the remote server.

```plaintext
sensor# copy current-config scp://user@192.0.2.0/configuration/cfg current-config
```

Password: ********

Warning: Copying over the current configuration may leave the box in an unstable state.
Would you like to copy current-config to backup-config before proceeding? [yes]:

**Step 3** Enter yes to copy the current configuration to a backup configuration.

```plaintext
cfg 100% |*******************************************************************| 36124 00:00
```

### Restoring the current configuration from a backup file

To restore your current configuration from a backup file, follow these steps:

**Step 1** Log in to the CLI using an account with administrator privileges.

**Step 2** Back up the current configuration to the remote server.

```plaintext
sensor# copy scp://user@192.0.2.0/configuration/cfg current-config
```

Password: ********

Warning: Copying over the current configuration may leave the box in an unstable state.
Would you like to copy current-config to backup-config before proceeding? [yes]:

**Step 3** Enter yes to copy the current configuration to a backup configuration.

```plaintext
cfg 100% |*******************************************************************| 36124 00:00
```

Warning: Replacing existing network-settings may leave the box in an unstable state.
Would you like to replace existing network settings (host-ipaddress/netmask/gateway/access-list) on sensor before proceeding? [no]:

```plaintext
sensor#
```
Creating and Using a Backup Configuration File

To protect your configuration, you can back up the current configuration and then display it to confirm that is the configuration you want to save. If you need to restore this configuration, you can merge the backup configuration file with the current configuration or overwrite the current configuration file with the backup configuration file.

To back up your current configuration, follow these steps:

Step 1 Log in to the CLI using an account with administrator privileges.
Step 2 Save the current configuration. The current configuration is saved in a backup file.

```
sensor# copy current-config backup-config
```
Step 3 Display the backup configuration file. The backup configuration file is displayed.

```
sensor# more backup-config
```
Step 4 You can either merge the backup configuration with the current configuration, or you can overwrite the current configuration:

- Merge the backup configuration into the current configuration.

```
sensor# copy backup-config current-config
```
- Overwrite the current configuration with the backup configuration.

```
sensor# copy /erase backup-config current-config
```

Erasing the Configuration File

Use the `erase {backup-config | current-config}` command to delete a logical file. The following options apply:

- `current-config`—The current running configuration. The configuration becomes persistent as the commands are entered.
- `backup-config`—The storage location for the configuration backup.

For More Information

- For the procedure for adding the remote host to the SSH known host list, see Adding Hosts to the SSH Known Hosts List, page 4-46.
- For the procedure for adding the remote host to the TLS trusted hosts list, see Adding TLS Trusted Hosts, page 4-52.
To erase the current configuration and return all settings back to the default, follow these steps:

**Step 1** Log in to the CLI using an account with administrator privileges.

sensor# erase current-config

Warning: Removing the current-config file will result in all configuration being reset to default, including system information such as IP address. User accounts will not be erased. They must be removed manually using the "no username" command.

Continue? []:

**Step 2** Press **Enter** to continue or enter **no** to stop.