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

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:

Step 1   Log in to the CLI.

Step 2   Display the current configuration:

```
sensor# show configuration
! ------------------------------
! Version 5.1(0.7)
! Current configuration last modified Thu Jul 14 21:49:58 2005
! ------------------------------
display-serial
! ------------------------------
service interface
exit
! ------------------------------
service analysis-engine
exit
! ------------------------------
service authentication
exit
! ------------------------------
```

```
service event-action-rules rules0
exit
! -----------------------------
service host
network-settings
host-ip 10.89.149.27/25,10.89.149.126
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 logger
exit
! -----------------------------
service network-access
user-profiles test
exit
exit
! -----------------------------
service notification
exit
! -----------------------------
service signature-definition sig0
signatures 60000 0
alert-severity medium
sig-fidelity-rating 75
sig-description
sig-name My Sig
sig-string-info My Sig Info
sig-comment Sig Comment
exit
engine string-tcp
event-action produce-alert
direction to-service
regex-string My Regex String
service-ports 23
exit
event-counter
event-count 1
event-count-key Axxx
specify-alert-interval no
exit
alert-frequency
summary-mode summarize
summary-interval 15
summary-key Axxx
specify-global-summary-threshold yes
global-summary-threshold 75
exit
exit
exit
exit
exit
! -----------------------------
service ssh-known-hosts
exit
! -----------------------------
service trusted-certificates
```

```
exit
! -----------------------------
service web-server
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 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 4   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: 256, 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>
      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 5   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: 10.89.149.27/25,10.89.149.126 default: 10.1.9.201/24,10.1.9.1
      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
      ----------------------------------------------
      ----------------------------------------------
   -----------------------------------------------
   summertime-option
   -----------------------------------------------
      disabled
      ----------------------------------------------
      ----------------------------------------------
   -----------------------------------------------
```

```
      auto-upgrade-option
      -----------------------------------------------
         disabled
         ----------------------------------------------
         ----------------------------------------------
      -----------------------------------------------
      crypto
      -----------------------------------------------
         key (min: 0, max: 10, current: 2)
         -----------------------------------------------
            <protected entry>
            name: realm-cisco.pub <defaulted>
            type
            -----------------------------------------------
               rsa-pubkey
               -----------------------------------------------
                  length: 2048 <defaulted>
                  exponent: 65537 <defaulted>
                  modulus: 2444218998935774708387485533523262884359996893419855964 8
63019947387841151932503911172668940194754549155390407658020393330611891292508300
85940304031186014499632568812428068058089581614196337399623060624990057049103055
90153955935086060000867977680807364018606343572325237557529312630455806870430186 3
80562114437439289069456670922074995827390284761610591515752008405140243673083189
77822469964934598367010389389888297490802884118543730076293589703535912161993319
47093130298688830012547215572646349623539468838641064915313947806852904082351955
13217273138099965383039716130153270715220046567107828128924197692417332033911704
3 <defaulted>
               -----------------------------------------------
               -----------------------------------------------
            <protected entry>
            name: realm-trend.pub <defaulted>
            type
            -----------------------------------------------
               rsa-pubkey
               -----------------------------------------------
                  length: 2048 <defaulted>
                  exponent: 65537 <defaulted>
                  modulus: 2176556142257302131415985535141872303162509338077705369 6
63817289527060570932551065489818190713745672148260527030060667208366606603802679
30439066724143390626495479300550101618179584637287052936465692146572612651375969
20354521585644221602944203520804404212975401970895119903756769601133853673296766
45289795777973491984056587045214514820063366950731346400044308491594626434706999
47608668822814014830063399534204647069509052443439525363706527255224510771122235
80181150460544783251498481432705991010069844368525754878413669427639752950801767
99905309235232456295580086724203297914095984224328444391582223138423799100838191
9 <defaulted>
               -----------------------------------------------
               -----------------------------------------------
            -----------------------------------------------
         -----------------------------------------------
   sensor(config-hos)# exit
   sensor(config)# exit
   sensor#
```

Step 6   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>
                 -----------------------------------------------
                    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 7   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 8   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 9 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>
    snmp-agent-port: 161 <defaulted>
    snmp-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#
```

Step 10 Display the current configuration for the signature definitions 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: 80-80,3128-3128,8000-8000,8010-8010,8080-8080,8888-8888,2432
6-24326 <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,
24326-24326 <defaulted>
       -----------------------------------------------
       ftp-enable: false <defaulted>
```

```
          ---------------------------------------------
          fragment-reassembly
          ---------------------------------------------
             ip-reassemble-mode: nt <defaulted>
          ---------------------------------------------
          stream-reassembly
          ---------------------------------------------
       --MORE--
```

Step 11   Display the current configuration for the SSH known hosts submode:

```
sensor# configure terminal
sensor(config)# service ssh-known-hosts
sensor(config-ssh)# show settings
   rsa1-keys (min: 0, max: 500, current: 0)
   ---------------------------------------------
   ---------------------------------------------
sensor(config-ssh)# exit
sensor(config)# exit
sensor#
```

Step 12   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
      certificate: MIICJDCCAY0CCPbSkgXUchJIMA0GCSqGSIb3DQEBBQUAMFcxCzAJBgNVBAYTA
lVTMRwwGgYDVQQKExNDaXNjbyBTeXN0ZW1zLCBJbmMuMRIwEAYDVQQLEwlTU00tSVBTMjAxFjAUBgNVB
AMTDTEwLjg5LjEzMC4xMDgwHhcNMDMwMTAzMDE1MjEwWhcNMDUwMTAzMDE1MjEwWjBXMQswCQYDVQQGE
wJVUzEcMBoGA1UEChMTQ2lzY28gU3lzdGVtcywgSW5jLjESMBAGA1UECxMJU1NNLlQUzIwMRYwFAYDV
QQDEw0xMC44OS4xMzAuMTA4MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCzldqLFG4MT4bfgh3mJ
fP/DCilnnaLfzHK9FdnhmWI4FY+9MVvAI7MOhAcuV6HYfyp6n6cYvH+Eswzl9uv7H5nouID9St9GI3Yr
SUtlIQAJ4QVL2DwWP230x6KdHrYqcj+Nmhc7AnnPypjidwGSfF+VetIJLEeRFh/mI2JcmwF2QIDAQABM
A0GCSqGSIb3DQEBBQUAA4GBAAUI2PLANTOehxvCfwd6UAFXvy8uifbjqKMC1jrrF+f9KGkxmR+XZvUaG
OS83FYDXlXJvB5Xyxms+Y01wGjzKKpxegBoan8OB8o193Ueszdpvz2xYmiEgywCDyVJRsw3hAFMXWMS5
XsBUiHtw0btHH0j7ElFZxUjZv12fGz8hlnY
   ---------------------------------------------
sensor(config-tru)# exit
sensor(config)# exit
sensor#
```

Step 13   Display the current configuration for the web server submode:

```
sensor# configure terminal
sensor(config)# service web-server
sensor(config-web)# show settings
   enable-tls: true <defaulted>
   port: 443 <defaulted>
   server-id: HTTP/1.1 compliant <defaulted>
sensor(config-web)# exit
sensor(config)# exit
sensor#
```

Filtering the Current Configuration Output

Use the **show configuration | [begin | exclude | include]** *regular_expression* command to search or filter the output of the contents of the current configuration.

> **Note** Users with operator or viewer privileges can search or filter the **current-config** only.

The following options apply:

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

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

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

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

Step 2 Search the configuration output beginning with the regular expression "ssh," for example

> **Note** The **show configuration | begin** *regular_expression* command begins unfiltered output of the **show** command with the first line that contains the specified regular expression.

```
sensor# show configuration | begin ssh
communication ssh-3des
profile-name test1
block-vlans 234
pre-vacl-name aaaa
post-vacl-name bbbb
exit
exit
exit
! ----------------------------
service notification
exit
! ----------------------------
service signature-definition sig0
signatures 2200 0
engine service-generic
specify-payload-source yes
payload-source l2-header
exit
exit
exit
signatures 12300 0
```

```
status
enabled true
retired true
--MORE--
```

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

Step 3 Filter the current configuration so that you exclude lines that contain a regular expression, for example, "service":

```
sensor# show configuration | exclude service
! ----------------------------
! Version 5.1(0.7)
! Current configuration last modified Thu Jul 14 21:49:58 2005
! ----------------------------
display-serial
! ----------------------------
exit
! ----------------------------
exit
! ----------------------------
exit
! ----------------------------
exit
! ----------------------------
network-settings
host-ip 10.89.149.27/25,10.89.149.126
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!
--MORE--
```

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

Step 4 Filter the current configuration so that you include lines that contain a regular expression, for example, "service":

```
sensor# show configuration | include service
service analysis-engine
service authentication
service event-action-rules rules0
service host
service interface
service logger
service network-access
service notification
service signature-definition sig0
```

```
engine service-generic
service ssh-known-hosts
service trusted-certificates
service web-server
sensor#
```

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*—Any regular expression found in the **show settings** command output.

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

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: 10.89.149.124
         -----------------------------------------------
            password: <hidden>
            port: 443 default: 443
            tls: 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: 10.89.149.185/25,10.89.149.254 default: 10.1.9.201/24,10.1.9.1
sensor(config-hos)#
```

Displaying the Contents of a Logical File

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*—Either the current-config or the backup-config.

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

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

✎

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

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. For the procedure for using the **terminal** command, see Modifying Terminal Properties, page 13-3.

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:

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

The current configuration is displayed.

```
! ----------------------------
! Version 5.1(0.7)
! Current configuration last modified Thu Jul 14 21:49:58 2005
! ----------------------------
display-serial
! ----------------------------
service interface
exit
! ----------------------------
service analysis-engine
exit
! ----------------------------
service authentication
exit
! ----------------------------
service event-action-rules rules0
exit
! ----------------------------
service host
network-settings
host-ip 10.89.149.27/25,10.89.149.126
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 logger
exit
! ----------------------------
service network-access
user-profiles test
exit
exit
! ----------------------------
service notification
exit
! ----------------------------
service signature-definition sig0
signatures 60000 0
alert-severity medium
sig-fidelity-rating 75
```

```
sig-description
sig-name My Sig
sig-string-info My Sig Info
sig-comment Sig Comment
exit
engine string-tcp
event-action produce-alert
direction to-service
regex-string My Regex String
service-ports 23
exit
event-counter
event-count 1
event-count-key Axxx
specify-alert-interval no
exit
alert-frequency
summary-mode summarize
summary-interval 15
summary-key Axxx
specify-global-summary-threshold yes
global-summary-threshold 75
exit
exit
exit
exit
exit
! ----------------------------
service ssh-known-hosts
exit
! ----------------------------
service trusted-certificates
exit
! ----------------------------
service web-server
exit
sensor#
```

Copying and Restoring the Configuration File Using a Remote Server

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.

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

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.

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

- http:—Source URL for the web server. The syntax for this prefix is:

  http:[[/[username@]location]/directory]/filename

- https:—Source URL for the web server. The syntax for this prefix is:

  https:[[/[username@]location]/directory]/filename

> **Note**   If you use FTP or SCP protocol, you are prompted for a password.

The following keywords are used to designate the file location on the sensor:

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

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

To back up and restore your current configuration, follow these steps:

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

Step 2   To back up the current configuration to the remote server:

```
sensor# copy current-config ftp://qa_user@10.89.146.1//tftpboot/update/qmaster89.cfg
Password: ********
```

Step 3   To restore the configuration file that you copied to the remote server:

```
sensor# copy ftp://qa_user@10.89.146.1//tftpboot/update/qmaster89.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 4   Press **Enter** to copy the configuration file or enter **no** to stop.

Chapter 12   Working With Configuration Files

■ Creating and Using a Backup Configuration File

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:

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

The current configuration is saved in a backup file.

Step 3   Display the backup configuration file:

```
sensor# more backup-config
```

The backup configuration file is displayed.

Step 4   You can either merge the backup configuration with the current configuration, or you can overwrite the current configuration.

- To merge the backup configuration into the current configuration:

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

- To 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.

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.
```

Cisco Intrusion Prevention System Sensor CLI Configuration Guide for IPS 5.1

12-18

OL-8677-01

```
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.