



Configuring Virtual Sensors

This chapter explains the function of the Analysis Engine and how to create, edit, and delete virtual sensors. It also explains how to assign interfaces to a virtual sensor. It contains the following sections:

- [Virtual Sensor Notes and Caveats, page 6-1](#)
- [Understanding the Analysis Engine, page 6-2](#)
- [Understanding Virtual Sensors, page 6-2](#)
- [Advantages and Restrictions of Virtualization, page 6-2](#)
- [Inline TCP Session Tracking Mode, page 6-3](#)
- [Normalization and Inline TCP Evasion Protection Mode, page 6-4](#)
- [HTTP Advanced Decoding, page 6-4](#)
- [Adding, Editing, and Deleting Virtual Sensors, page 6-5](#)
- [Configuring Global Variables, page 6-12](#)

Virtual Sensor Notes and Caveats

The following notes and caveats apply to configuring the virtual sensor:

- The Cisco IPS does not support more than four virtual sensors. You cannot delete the default virtual sensor vs0.
- The ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP) do not support the inline TCP session tracking mode.
- For the ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP), normalization is performed by the adaptive security appliance and not the IPS.
- Anomaly detection is disabled by default. You must enable it to configure or apply an anomaly detection policy. Enabling anomaly detection results in a decrease in performance.

Understanding the Analysis Engine

The Analysis Engine performs packet analysis and alert detection. It monitors traffic that flows through specified interfaces.

You create virtual sensors in the Analysis Engine. Each virtual sensor has a unique name with a list of interfaces, inline interface pairs, inline VLAN pairs, and VLAN groups associated with it. To avoid definition ordering issues, no conflicts or overlaps are allowed in assignments. You assign interfaces, inline interface pairs, inline VLAN pairs, and VLAN groups to a specific virtual sensor so that no packet is processed by more than one virtual sensor. Each virtual sensor is also associated with a specifically named signature definition, event action rules, and anomaly detection configuration. Packets from interfaces, inline interface pairs, inline VLAN pairs, and VLAN groups that are not assigned to any virtual sensor are disposed of according to the inline bypass configuration.

**Note**

The Cisco IPS does not support more than four virtual sensors. You cannot delete the default virtual sensor vs0.

Understanding Virtual Sensors

The sensor can receive data inputs from one or many monitored data streams. These monitored data streams can either be physical interface ports or virtual interface ports. For example, a single sensor can monitor traffic from in front of the firewall, from behind the firewall, or from in front of and behind the firewall concurrently. And a single sensor can monitor one or more data streams. In this situation a single sensor policy or configuration is applied to all monitored data streams.

A virtual sensor is a collection of data that is defined by a set of configuration policies. The virtual sensor is applied to a set of packets as defined by interface component.

A virtual sensor can monitor multiple segments, and you can apply a different policy or configuration for each virtual sensor within a single physical sensor. You can set up a different policy per monitored segment under analysis. You can also apply the same policy instance, for example, sig0, rules0, or ad0, to different virtual sensors. You can assign interfaces, inline interface pairs, inline VLAN pairs, and VLAN groups to a virtual sensor.

**Note**

The default virtual sensor is vs0. You cannot delete the default virtual sensor. The interface list, the anomaly detection operational mode, the inline TCP session tracking mode, and the virtual sensor description are the only configuration features you can change for the default virtual sensor. You cannot change the signature definition, event action rules, or anomaly detection policies.

Advantages and Restrictions of Virtualization

Virtualization has the following advantages:

- You can apply different configurations to different sets of traffic.
- You can monitor two networks with overlapping IP spaces with one sensor.
- You can monitor both inside and outside of a firewall or NAT device.

Virtualization has the following restrictions:

- You must assign both sides of asymmetric traffic to the same virtual sensor.
- Using VACL capture or SPAN (promiscuous monitoring) is inconsistent with regard to VLAN tagging, which causes problems with VLAN groups.
 - When using Cisco IOS software, a VACL capture port or a SPAN target does not always receive tagged packets even if it is configured for trunking.
 - When using the MSFC, fast path switching of learned routes changes the behavior of VACL captures and SPAN.
- Persistent store is limited.

Virtualization has the following traffic capture requirements:

- The virtual sensor must receive traffic that has 802.1q headers (other than traffic on the native VLAN of the capture port).
- The sensor must see both directions of traffic in the same VLAN group in the same virtual sensor for any given sensor.

The following sensors support virtualization:

- ASA 5500-X IPS SSP
- ASA 5585-X IPS SSP
- IPS 4345
- IPS 4345-DC
- IPS 4360
- IPS 4510
- IPS 4520
- IPS 4520-XL

Inline TCP Session Tracking Mode



Note

The ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP) do not support the inline TCP session tracking mode.

When you choose to modify packets inline, if the packets from a stream are seen twice by the Normalizer engine, it cannot properly track the stream state and often the stream is dropped. This situation occurs most often when a stream is routed through multiple VLANs or interfaces that are being monitored by the IPS. A further complication in this situation is the necessity of allowing asymmetric traffic to merge for proper tracking of streams when the traffic for either direction is received from different VLANs or interfaces. To deal with this situation, you can set the mode so that streams are perceived as unique if they are received on separate interfaces and/or VLANs (or the subinterface for VLAN pairs).

The following inline TCP session tracking modes apply:

- Interface and VLAN—All packets with the same session key (AaBb) in the same VLAN (or inline VLAN pair) and on the same interface belong to the same session. Packets with the same key but on different VLANs are tracked separately.

- VLAN Only—All packets with the same session key (AaBb) in the same VLAN (or inline VLAN pair) regardless of the interface belong to the same session. Packets with the same key but on different VLANs are tracked separately.
- Virtual Sensor—All packets with the same session key (AaBb) within a virtual sensor belong to the same session. This is the default and almost always the best option to choose.

Normalization and Inline TCP Evasion Protection Mode



Note

For the ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP), normalization is performed by the adaptive security appliance and not the IPS.

Normalization only applies when the sensor is operating in inline mode. The default is strict evasion protection, which is full enforcement of TCP state and sequence tracking. The Normalizer enforces duplicate packets, changed packets, out-of-order packets, and so forth, which helps prevent attackers from evading the IPS.

Asymmetric mode disables most of the Normalizer checks. Use asymmetric mode only when the entire stream cannot be inspected, because in this situation, attackers can now evade the IPS.

HTTP Advanced Decoding

HTTP advanced decoding facilitates analysis of encoded HTTP return web traffic by using on-the-fly decoding. Changes to HTTP advanced decoding take effect immediately and only affect the new traffic flows.

Restrictions

The following restrictions apply when you enable HTTP advanced decoding:

- Although HTTP advanced decoding does not fire any new signatures, drop packets, or modify traffic, it allows existing signatures to match on content that was previously not detectable because of encodings.
- HTTP advanced decoding only acts on return web response traffic.



Caution

Enabling HTTP advanced decoding severely impacts system performance.



Note

Because HTTP advanced decoding requires the Regex card and the String XL engine, it is available only to those platforms that have them. HTTP advanced decoding is supported on the ASA 5585-X IPS SSP, ASA 5525-X IPS SSP, ASA 5545-X IPS SSP, ASA 5555-X IPS SSP, IPS 4345, IPS 4360, IPS 4510, IPS 4520, and IPS 4520-XL.

Adding, Editing, and Deleting Virtual Sensors

This section describes how to add, edit, and delete virtual sensors, and contains the following topics:

- [Adding Virtual Sensors, page 6-5](#)
- [Editing and Deleting Virtual Sensors, page 6-9](#)

Adding Virtual Sensors

Use the **virtual-sensor** *name* command in service analysis engine submode to create a virtual sensor. You can create up to four virtual sensors. You assign policies (anomaly detection, event action rules, and signature definition) to the virtual sensor. Then you assign interfaces (promiscuous, inline interface pairs, inline VLAN pairs, and VLAN groups) to the virtual sensor. You must configure the inline interface pairs and VLAN pairs before you can assign them to a virtual sensor.



Note

Anomaly detection is disabled by default. You must enable it to configure or apply an anomaly detection policy. Enabling anomaly detection results in a decrease in performance.

The following commands apply:

- **http-advanced-decoding {true | false}**—Enables deeper inspection of HTTP traffic. The default is disabled. Valid for IPS 7.1(5)E4 and later.



Caution

Enabling HTTP advanced decoding severely impacts system performance.



Note

HTTP advanced decoding is supported on the ASA 5585-X IPS SSP, ASA 5525-X IPS SSP, ASA 5545-X IPS SSP, ASA 5555-X IPS SSP, IPS 4345, IPS 4360, IPS 4510, IPS 4520, and IPS 4520-XL.

- **anomaly-detection**—Specifies the anomaly detection parameters:
 - **anomaly-detection-name** *name*—Specifies the name of the anomaly detection policy.
 - **operational-mode**—Specifies the anomaly detection mode (**inactive**, **learn**, **detect**).
- **description**—Description of the virtual sensor.
- **event-action-rules**—Specifies the name of the event action rules policy.
- **inline-TCP-evasion-protection-mode**—Lets you choose which type of normalization you need for traffic inspection:
 - **asymmetric** —Specifies that the sensor can only see one direction of bidirectional traffic flow. Asymmetric mode protection relaxes the evasion protection at the TCP layer.



Note

Asymmetric mode lets the sensor synchronize state with the flow and maintain inspection for those engines that do not require both directions. Asymmetric mode lowers security because full protection requires both sides of traffic to be seen.

- **strict**—Specifies that if a packet is missed for any reason, all packets after the missed packet are not processed. Strict evasion protection provides full enforcement of TCP state and sequence tracking.



Note Any out-of-order packets or missed packets can produce Normalizer engine signatures 1300 or 1330 firings, which try to correct the situation, but can result in denied connections.



Note For the ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP), normalization is performed by the adaptive security appliance and not the IPS.

- **inline-TCP-session-tracking-mode**—Enables an advanced method used to identify duplicate TCP sessions in inline traffic. The default is virtual sensor, which is almost always the best choice.
 - **virtual-sensor** —Specifies that all packets with the same session key (AaBb) within a virtual sensor belong to the same session.
 - **interface-and-vlan**—Specifies that all packets with the same session key (AaBb) in the same VLAN (or inline VLAN pair) and on the same interface belong to the same session. Packets with the same key but on different VLANs or interfaces are tracked independently.
 - **vlan-only**—Specifies that all packets with the same session key (AaBb) in the same VLAN (or inline VLAN pair) regardless of the interface belong to the same session. Packets with the same key but on different VLANs are tracked independently.



Note The ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP) do not support the inline TCP session tracking mode.

- **signature-definition**—Specifies the name of the signature definition policy.
- **logical-interfaces**—Specifies the name of the logical interfaces (inline interface pairs).
- **physical-interfaces**—Specifies the name of the physical interfaces (promiscuous, inline VLAN pairs, and VLAN groups):
 - **subinterface-number**—Specifies the physical subinterface number. If the subinterface-type is none, the value of 0 indicates the entire interface is assigned in promiscuous mode.
- **no**—Removes an entry or selection.

Adding a Virtual Sensor

To add a virtual sensor, follow these steps:

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

Step 2 Enter service analysis mode.

```
sensor# configure terminal
sensor(config)# service analysis-engine
sensor(config-ana)#
```

Step 3 Add a virtual sensor.

```
sensor(config-ana)# virtual-sensor vs1
sensor(config-ana-vir)#
```

Step 4 Add a description for this virtual sensor.

```
sensor(config-ana-vir)# description virtual sensor 1
```

Step 5 Assign an anomaly detection policy and operational mode to this virtual sensor.

```
sensor(config-ana-vir)# anomaly-detection
sensor(config-ana-vir-ano)# anomaly-detection-name ad1
sensor(config-ana-vir-ano)# operational-mode learn
```

Step 6 Assign an event action rules policy to this virtual sensor.

```
sensor(config-ana-vir-ano)# exit
sensor(config-ana-vir)# event-action-rules rules1
```

Step 7 Assign a signature definition policy to this virtual sensor.

```
sensor(config-ana-vir)# signature-definition sig1
```

Step 8 Enable HTTP advanced decoding.

```
sensor(config-ana-vir)# http-advanced-decoding true
```



Caution

Enabling HTTP advanced decoding severely impacts system performance.

Step 9 Assign the inline TCP session tracking mode. The default is virtual sensor mode, which is almost always the best option to choose.

```
sensor(config-ana-vir)# inline-TCP-session-tracking-mode virtual-sensor
```

Step 10 Assign the inline TCP evasion protection mode. The default is strict mode, which is almost always the best option to choose.

```
sensor(config-ana-vir)# inline-TCP-evasion-protection-mode strict
```

Step 11 Enable HTTP advanced decoding.

```
sensor(config-ana-vir)# http-advanced-decoding true
```

Step 12 Display the list of available interfaces.

```
sensor(config-ana-vir)# physical-interface ?
GigabitEthernet0/0    GigabitEthernet0/0 physical interface.
GigabitEthernet0/1    GigabitEthernet0/1 physical interface.
GigabitEthernet2/0    GigabitEthernet0/2 physical interface.
GigabitEthernet2/1    GigabitEthernet0/3 physical interface.
sensor(config-ana-vir)# physical-interface
```

```
sensor(config-ana-vir)# logical-interface ?
<none available>
```

Step 13 Assign the promiscuous mode interfaces you want to add to this virtual sensor. Repeat this step for all the promiscuous interfaces that you want to assign to this virtual sensor.

```
sensor(config-ana-vir)# physical-interface GigabitEthernet0/3
```

Step 14 Assign the inline interface pairs you want to add to this virtual sensor. You must have already paired the interfaces.

```
sensor(config-ana-vir)# logical-interface inline_interface_pair_name
```

- Step 15** Assign the subinterfaces of the inline VLAN pairs or groups you want to add to this virtual sensor. You must have already subdivided any interfaces into VLAN pairs or groups.

```
sensor(config-ana-vir)# physical-interface GigabitEthernet2/0 subinterface-number
subinterface_number
```

- Step 16** Verify the virtual sensor settings.

```
sensor(config-ana-vir)# show settings
name: vs1
-----
description: virtual sensor 1 default:
signature-definition: sig1 default: sig0
event-action-rules: rules1 default: rules0
anomaly-detection
-----
anomaly-detection-name: ad1 default: ad0
operational-mode: learn default: detect
-----
physical-interface (min: 0, max: 999999999, current: 2)
-----
name: GigabitEthernet0/3
subinterface-number: 0 <defaulted>
-----
inline-TCP-session-tracking-mode: virtual-sensor default: virtual-sensor
-----
logical-interface (min: 0, max: 999999999, current: 0)
-----
-----
sensor(config-ana-vir)#
```

- Step 17** Exit analysis engine mode.

```
sensor(config-ana-vir)# exit
sensor(config-ana)# exit
sensor(config)#
Apply Changes:[yes]:
```

- Step 18** Press **Enter** to apply the changes or enter **no** to discard them.

For More Information

- For the procedure for creating virtual sensors on the ASA 5500-X IPS SSP, see [Creating Virtual Sensors for the ASA 5500-X IPS SSP, page 18-3](#).
- For the procedure for creating virtual sensors on the ASA 5585-X IPS SSP, see [Creating Virtual Sensors for the ASA 5585-X IPS SSP, page 19-4](#).
- For more information on creating and configuring anomaly detection policies, see [Working With Anomaly Detection Policies, page 9-8](#).
- For more information on creating and configuring event action rules policies, see [Working With Event Action Rules Policies, page 8-8](#).
- For more information on creating and configuring signature definition policies, see [Working With Signature Definition Policies, page 7-2](#).
- For more information about normalization, see [Normalization and Inline TCP Evasion Protection Mode, page 6-4](#).
- For more information about inline TCP session tracking mode, see [Inline TCP Session Tracking Mode, page 6-3](#).

- For the procedure for pairing inline interfaces, see [Configuring Inline Interface Pairs, page 5-17](#). Repeat Step 11 for all the inline interface pairs that you want to assign to this virtual sensor.
- For the procedure for pairing and grouping inline VLANs, see [Configuring Inline VLAN Pairs, page 5-22](#) and [Configuring VLAN Groups, page 5-28](#). Repeat Step 12 for all inline VLAN pairs or VLAN groups that you want to assign to this virtual sensor.
- For the procedure for enabling anomaly detection, see [Enabling Anomaly Detection, page 9-8](#).

Editing and Deleting Virtual Sensors

You can edit the following parameters of a virtual sensor:

- Signature definition policy
- Event action rules policy
- Anomaly detection policy



Note

Anomaly detection is disabled by default. You must enable it to configure or apply an anomaly detection policy. Enabling anomaly detection results in a decrease in performance.

- Anomaly detection operational mode
- Inline TCP session tracking mode



Note

The ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP) do not support the inline TCP session tracking mode.

- Description
- Interfaces assigned

Editing or Deleting a Virtual Sensor

To edit or delete a virtual sensor, follow these steps:

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

Step 2 Enter analysis engine mode.

```
sensor# configure terminal
sensor(config)# service analysis-engine
sensor(config-ana)#
```

Step 3 Edit the virtual sensor, vs1.

```
sensor(config-ana)# virtual-sensor vs1
sensor(config-ana-vir)#
```

Step 4 Edit the description of this virtual sensor.

```
sensor(config-ana-vir)# description virtual sensor A
```

Step 5 Change the anomaly detection policy and operational mode assigned to this virtual sensor.

```
sensor(config-ana-vir)# anomaly-detection
sensor(config-ana-vir-ano)# anomaly-detection-name ad0
sensor(config-ana-vir-ano)# operational-mode learn
```

Step 6 Change the event action rules policy assigned to this virtual sensor.

```
sensor(config-ana-vir-ano)# exit
sensor(config-ana-vir)# event-action-rules rules0
```

Step 7 Change the signature definition policy assigned to this virtual sensor.

```
sensor(config-ana-vir)# signature-definition sig0
```

Step 8 Change the inline TCP session tracking mode. The default is virtual sensor mode, which is almost always the best option to choose.

```
sensor(config-ana-vir)# inline-TCP-session-tracking-mode interface-and-vlan
```

Step 9 Display the list of available interfaces.

```
sensor(config-ana-vir)# physical-interface ?
GigabitEthernet0/0    GigabitEthernet0/0 physical interface.
GigabitEthernet0/1    GigabitEthernet0/1 physical interface.
GigabitEthernet2/0    GigabitEthernet0/2 physical interface.
GigabitEthernet2/1    GigabitEthernet0/3 physical interface.
sensor(config-ana-vir)# physical-interface

sensor(config-ana-vir)# logical-interface ?
<none available>
```

Step 10 Change the promiscuous mode interfaces assigned to this virtual sensor.

```
sensor(config-ana-vir)# physical-interface GigabitEthernet0/2
```

Step 11 Change the inline interface pairs assigned to this virtual sensor. You must have already paired the interfaces.

```
sensor(config-ana-vir)# logical-interface inline_interface_pair_name
```

Step 12 Change the subinterface with the inline VLAN pairs or groups assigned to this virtual sensor. You must have already subdivided any interfaces into VLAN pairs or groups.

```
sensor(config-ana-vir)# physical-interface GigabitEthernet2/0 subinterface-number
subinterface_number
```

Step 13 Verify the edited virtual sensor settings.

```
ssensor(config-ana-vir)# show settings
name: vs1
-----
description: virtual sensor 1 default:
signature-definition: sig1 default: sig0
event-action-rules: rules1 default: rules0
anomaly-detection
-----
anomaly-detection-name: ad1 default: ad0
operational-mode: learn default: detect
-----
physical-interface (min: 0, max: 999999999, current: 2)
-----
name: GigabitEthernet0/3
subinterface-number: 0 <defaulted>
-----
inline-TCP-session-tracking-mode: interface-and-vlan default: virtual-sensor
```

```
-----
logical-interface (min: 0, max: 999999999, current: 0)
-----
-----
```

```
sensor(config-ana-vir)#
```

Step 14 Delete a virtual sensor.

```
sensor(config-ana-vir)# exit
sensor(config-ana)# no virtual-sensor vs1
```

Step 15 Verify the deleted virtual sensor. Only the default virtual sensor, vs0, is present.

```
sensor(config-ana)# show settings
global-parameters
-----
ip-logging
-----
max-open-iplog-files: 20 <defaulted>
-----
virtual-sensor (min: 1, max: 255, current: 2)
-----
<protected entry>
name: vs0 <defaulted>
-----
description: default virtual sensor <defaulted>
signature-definition: sig0 <protected>
event-action-rules: rules0 <protected>
anomaly-detection
-----
anomaly-detection-name: ad0 <protected>
operational-mode: detect <defaulted>
-----
physical-interface (min: 0, max: 999999999, current: 0)
-----
logical-interface (min: 0, max: 999999999, current: 0)
-----
sensor(config-ana)#
```

Step 16 Exit analysis engine mode.

```
sensor(config-ana)# exit
sensor(config)#
Apply Changes:[yes]:
```

Step 17 Press **Enter** to apply the changes or enter **no** to discard them.

For More Information

- For more information on creating and configuring anomaly detection policies, see [Working With Anomaly Detection Policies, page 9-8](#).
- For more information on creating and configuring event action rules policies, see [Working With Event Action Rules Policies, page 8-8](#).
- For more information on creating and configuring signature definition policies, see [Working With Signature Definition Policies, page 7-2](#).

- For the procedure for pairing inline interfaces, see [Configuring Inline Interface Pairs, page 5-17](#). Repeat Step 11 for all the inline interface pairs that you want to assign to this virtual sensor.
- For the procedure for pairing and grouping inline VLANs, see [Configuring Inline VLAN Pairs, page 5-22](#) and [Configuring VLAN Groups, page 5-28](#). Repeat Step 12 for all inline VLAN pairs or VLAN groups that you want to assign to this virtual sensor.
- For the procedure for enabling anomaly detection, see [Enabling Anomaly Detection, page 9-8](#).

Configuring Global Variables

Use the **global-parameters** command in service analysis engine submode to create global variables, such as IP logging, service activity, and specifying the flow depth. Flow depth is used for String, Multi-String, Service HTTP, and State engines. It does not apply to the XL String engine and the platforms that support it.



Note

The IPS 4345, IPS 4360, IPS 4510, IPS 4520, IPS 4520-XL, ASA 5525-X IPS SSP, ASA 5545-X IPS SSP, ASA 5555-X IPS SSP, and ASA 5585-X IPS SSP support the String XL engines and the Regex accelerator card.

The following commands apply:

- **ip-logging**—Enables global IP logging parameters.
 - **max-open-iplog-files**—Specifies the maximum number of concurrently open log files. The range is 20 to 100. The default is 20.
- **serviceActivity**—Lets you gather information about service activities for diagnostic purposes. The details are more granular and have port level details.



Note

Enabling service activity impacts system performance. Enable service activity collection temporarily for diagnostic purposes only. You must reboot the sensor after you enable service activity for the change to take affect.

- **enable-serviceactivity [1 | 0]**—Set to 1 to enable, set to 0 to disable. The default is disabled.
- **serviceActivityLimit limit**—Sets the limit for how many services you want to enable. The valid range is from 10 to 65536. The default is 15.
- **specify-flow-depth**—Lets you specify the inspection depth of the flow. Flow depth is the number of bytes inspected in a flow. The new value applies for new flows only. The valid range is from 0 to 429496296. The default is 0, which is infinite. Creating a Global Variable

To create a global variable, follow these steps:

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

Step 2 Enter service analysis mode.

```
sensor# configure terminal
sensor(config)# service analysis-engine
sensor(config-ana)#
```

Step 3 Create the variable for the maximum number of open IP logs.

```
sensor(config-ana)# global-parameters
```

```

sensor(config-ana-glo)# ip-logging
sensor(config-ana-glo-ip)# max-open-iplog-files 50
sensor(config-ana-glo-ip)# exit
sensor(config-ana-glo)#

```

Step 4 Create the variable for service activity.

```

sensor(config-ana-glo)# serviceActivity
sensor(config-ana-glo-ser)# enable-serviceactivity 1
sensor(config-ana-glo-ser)# serviceActivityLimit 25
sensor(config-ana-glo-ser)# exit
sensor(config-ana-glo)#

```

Step 5 Create the flow depth variable.

```

sensor(config-ana-glo)# specify-flow-depth 500
sensor(config-ana-glo)# exit
sensor(config-ana)#

```

Step 6 Verify the global variable settings.

```

sensor(config-ana-glo)# show settings
global-parameters
-----
specify-flow-depth: 500 default: 0
serviceActivity
-----
enable-serviceactivity: 1 default: 0
serviceActivityLimit: 25 default: 15
-----
ip-logging
-----
max-open-iplog-files: 50 default: 20
-----
sensor(config-ana-glo)#

```

Step 7 Exit analysis engine mode.

```

sensor(config-ana)# exit
sensor(config)#
Apply Changes:[yes]:

```

Step 8 Press **Enter** to apply the changes or enter **no** to discard them.

For More Information

For detailed information about String, Multi-String, Service HTTP, and State engines, see [Appendix B, “Signature Engines.”](#)

