



## CHAPTER 5

# Policies—Signature Definitions

---

This chapter explains how to create signature definition policies and how to configure signatures. It contains the following sections:

- [Understanding Security Policies, page 5-1](#)
- [Configuring Signature Definition Policies, page 5-1](#)
- [Signature Definition Policy sig0, page 5-3](#)
- [Understanding Signatures, page 5-3](#)
- [Configuring Signatures, page 5-4](#)
- [Example Meta Engine Signature, page 5-23](#)
- [Using the Custom Signature Wizard, page 5-27](#)
- [Configuring Signature Variables, page 5-55](#)
- [Miscellaneous Tab, page 5-57](#)

## Understanding Security Policies

You can create multiple security policies and apply them to individual virtual sensors. A security policy is made up of a signature definition policy, an event action rules policy, and an anomaly detection policy. IPS 6.0 contains a default signature definition policy called sig0, a default event action rules policy called rules0, and a default anomaly detection policy called ad0. You can assign the default policies to a virtual sensor or you can create new policies.

The use of multiple security policies lets you create security policies based on different requirements and then apply these customized policies per VLAN or physical interface.

## Configuring Signature Definition Policies

This section describes how to create signature definition policies, and contains the following topics:

- [Signature Definitions Pane, page 5-2](#)
- [Signature Definitions Pane Field Definitions, page 5-2](#)
- [Add and Clone Policy Dialog Boxes Field Definitions, page 5-2](#)
- [Adding, Cloning, and Deleting Signature Policies, page 5-2](#)

## Signature Definitions Pane

**Note**

You must be administrator or operator to add, clone, or delete signature policies.

In the Signature Definitions pane, you can add, clone, or delete a signature definition policy. The default signature definition policy is called sig0. When you add a policy, a control transaction is sent to the sensor to create the policy instance. If the response is successful, the new policy instance is added under Signature Definitions. If the control transaction fails, for example because of resource limitations, an error message appears.

If your platform does not support virtual policies, this means you can only have one instance for each component and you cannot create new ones or delete the existing one. In this case, the Add, Clone, and Delete buttons are disabled.

**Caution**

IDS-4215, AIM IPS, and NM CIDS do not support sensor virtualization and therefore do not support multiple policies.

## Signature Definitions Pane Field Definitions

The following fields are found in the Signature Definitions pane:

- Policy Name—Identifies the name of this signature definition policy.
- Assigned Virtual Sensor—Identifies the virtual sensor that this signature definition policy is assigned to.

## Add and Clone Policy Dialog Boxes Field Definitions

The following field is found in the Add and Clone Policy dialog boxes:

- Policy Name—Lets you create a unique name for the new policy.

## Adding, Cloning, and Deleting Signature Policies

To add, clone, or delete a signature definition policy, follow these steps:

- Step 1** Log in to IDM using an account with administrator or operator privileges.
- Step 2** Choose **Configuration > Policies > Signature Definitions**, and then click **Add**.
- Step 3** In the Policy Name field, enter a name for the signature definition policy.
- Step 4** Click **OK**.

The signature definition policy appears in the list in the Signature Definitions pane.

- Step 5** To clone an existing signature definition policy, select it in the list, and then click **Clone**.  
The Clone Policy dialog box appears with “\_copy” appended to the existing signature definition policy name.
- Step 6** In the Policy Name field, enter a unique name.

**Step 7** Click **OK**.

The cloned signature definition policy appears in the list in the Signature Definitions pane.

**Step 8** To remove a signature definition policy, select it, and then click **Delete**.

The Delete Policy dialog box appears asking if you are sure you want to delete this policy permanently.



**Caution**

You cannot delete the default signature definition policy, sig0.

**Step 9** Click **Yes**.

The signature definition policy no longer appears in the list in the Signature Definitions pane.

**Step 10** Click **Apply** to apply your changes and save the revised configuration.

## Signature Definition Policy sig0

The sig0 pane (default) contains the signature policy configuration and the tools to configure signatures. There are four tabs:

- Signature Configuration—Lets you enable and disable signatures, add, edit and clone signatures, restore signature defaults, and assign actions to signatures.
- Custom Signature Wizard—Lets you use a wizard to create custom signatures.
- Configuring Signature Variables—Lets you set up variables to use within multiple signatures.
- Miscellaneous—Lets you configure application policy signatures, set up the mode for IP fragmentation and TCP stream reassembly, and configure IP logging.

## Understanding Signatures

Attacks or other misuses of network resources can be defined as network intrusions. Sensors that use a signature-based technology can detect network intrusions. A signature is a set of rules that your sensor uses to detect typical intrusive activity, such as DoS attacks. As sensors scan network packets, they use signatures to detect known attacks and respond with actions that you define.

The sensor compares the list of signatures with network activity. When a match is found, the sensor takes an action, such as logging the event or sending an alert. Sensors let you modify existing signatures and define new ones.

Signature-based intrusion detection can produce false positives because certain normal network activity can be misinterpreted as malicious activity. For example, some network applications or operating systems may send out numerous ICMP messages, which a signature-based detection system might interpret as an attempt by an attacker to map out a network segment. You can minimize false positives by tuning your signatures.

To configure a sensor to monitor network traffic for a particular signature, you must enable the signature. By default, the most critical signatures are enabled when you install the signature update. When an attack is detected that matches an enabled signature, the sensor generates an alert, which is stored in the Event Store of the sensor. The alerts, as well as other events, may be retrieved from the Event Store by web-based clients. By default the sensor logs all Informational alerts or higher.

Some signatures have subsignatures, that is, the signature is divided in to subcategories. When you configure a subsignature, changes made to the parameters of one subsignature apply only to that subsignature. For example, if you edit signature 3050 subsignature 1 and change the severity, the severity change applies to only subsignature 1 and not to 3050 2, 3050 3, and 3050 4.

IPS 6.0 contains over 1000 built-in default signatures. You cannot rename or delete signatures from the list of built-in signatures, but you can retire signatures to remove them from the sensing engine. You can later activate retired signatures; however, this process requires the sensing engines to rebuild their configuration, which takes time and could delay the processing of traffic. You can tune built-in signatures by adjusting several signature parameters. Built-in signatures that have been modified are called tuned signatures.

**Note**


---

We recommend that you retire any signatures that you are not using. This improves sensor performance.

---

You can create signatures, which are called custom signatures. Custom signature IDs begin at 60000. You can configure them for several things, such as matching of strings on UDP connections, tracking of network floods, and scans. Each signature is created using a signature engine specifically designed for the type of traffic being monitored.

## Configuring Signatures

This section describes the Signature Configuration tab, and how to configure signatures. It contains the following topics:

- [Signature Configuration Tab, page 5-4](#)
- [Signature Configuration Tab Field Definitions, page 5-5](#)
- [Add, Clone, and Edit Signatures Dialog Boxes Field Definitions, page 5-6](#)
- [Assign Actions Dialog Box Field Definitions, page 5-11](#)
- [Enabling and Disabling Signatures, page 5-13](#)
- [Adding Signatures, page 5-14](#)
- [Cloning Signatures, page 5-16](#)
- [Tuning Signatures, page 5-17](#)
- [Assigning Actions to Signatures, page 5-18](#)
- [Configuring Alert Frequency, page 5-21](#)

## Signature Configuration Tab

**Note**


---

You must be administrator or operator to add, clone, enable, disable, tune, and delete signatures.

---

You can perform the following tasks on the Signature Configuration tab:

- Sort and view all signatures stored on the sensor.
- Edit (tune) an existing signature to change the value(s) associated with the parameter(s) for that signature.

- Create a signature, either by cloning an existing signature and using the parameters of that signature as a starting point for the new signature, or by adding a new signature from scratch.

You can also use the Custom Signature Wizard to create a signature. The wizard guides you through the parameters that you must select to configure a custom signature, including selection of the appropriate signature engine.

- Enable, disable, or retire an existing signature.
- Restore the factory defaults to the signature.
- Delete a custom signature.




---

**Note** You cannot delete built-in signatures.

---

- Assign actions to a signature.

#### For More Information

- For the procedure for tuning signatures, see [Tuning Signatures, page 5-17](#).
- For the procedure for adding signatures, see [Adding Signatures, page 5-14](#).
- For the procedure for cloning signatures, see [Cloning Signatures, page 5-16](#).
- For more information on using the Custom Signature Wizard, see [Using the Custom Signature Wizard, page 5-27](#).
- For the procedure for enabling, disabling, and retiring signatures, see [Enabling and Disabling Signatures, page 5-13](#).
- For the procedure for assigning actions to signatures, see [Assigning Actions to Signatures, page 5-18](#).

## Signature Configuration Tab Field Definitions

The following fields are found on the Signature Configuration tab:

- **Select By**—Lets you sort the list of signatures by selecting an attribute to sort on.
- **Sig ID**—Identifies the unique numerical value assigned to this signature.  
This value lets the sensor identify a particular signature.
- **Subsig ID**—Identifies the unique numerical value assigned to this subsignature.  
A SubSig ID is used to identify a more granular version of a broad signature.
- **Name**—Identifies the name assigned to the signature.
- **Enabled**—Identifies whether or not the signature is enabled.  
A signature must be enabled for the sensor to protect against the traffic specified by the signature.
- **Severity**—Identifies the severity level that the signature will report: High, Informational, Low, Medium.
- **Fidelity Rating**—Identifies the weight associated with how well this signature might perform in the absence of specific knowledge of the target.
- **Base RR**—Displays the base risk rating value of each signature. IDM automatically calculates the base risk rating by multiplying the fidelity rating and the severity factor and dividing them by 100 (Fidelity Rating x Severity Factor /100).

Severity Factor has the following values:

- Severity Factor = 100 if the severity level of the signature is high
- Severity Factor = 75 if severity level of the signature is medium
- Severity Factor = 50 if severity level of the signature is low
- Severity Factor = 25 if severity level of the signature is informational
- Action—Identifies the actions the sensor will take when this signature fires.
- Type—Identifies whether this signature is a default (built-in), tuned, or custom signature.
- Engine—Identifies the engine that parses and inspects the traffic specified by this signature.
- Retired—Identifies whether or not the signature is retired.

A retired signature is removed from the signature engine. You can activate a retired signature to place it back in the signature engine.




---

**Note** We recommend that you retire any signatures that you are not using. This improves sensor performance.

---

Right-Click Menu:

- NSDB Link—Takes you to the description of that signature on the MySDN site (formerly known as NSDB) on Cisco.com.
- Set Severity To—Lets you set the severity level that the signature will report: High, Medium, Low or Informational.
- Actions—Opens the Assign Actions dialog box.
- Edit—Opens the Edit Signature dialog box. In the Edit Signature dialog box, you can change the parameters associated with the selected signature and effectively *tune* the signature. You can edit only one signature at a time
- Restore Defaults—Returns all parameters to the default settings for the selected signature.
- Enable—Enables the selected signature.
- Disable—Disables the selected signature.
- Change Status To—Lets you change the status to retired or active.

## Add, Clone, and Edit Signatures Dialog Boxes Field Definitions



**Tip**

---

A square green icon indicates the default value is being used. Click the green icon to configure that parameter. Click the value field to change the parameter.

---



**Tip**

---

A red diamond icon indicates that a user-defined value is being used. Click the icon to change the value back to the default.

---

The following fields are found in the Add, Clone, and Edit Signature dialog boxes:

- Signature Definition
  - Signature ID—Identifies the unique numerical value assigned to this signature. This value lets the sensor identify a particular signature.  
The value is 1000 to 65000.
  - SubSignature ID—Identifies the unique numerical value assigned to this subsignature. The subsignature ID identifies a more granular version of a broad signature.  
The value is 0 to 255.
  - Alert Severity—Lets you choose the severity level of the signature: High, Informational, Low, Medium.
  - Promiscuous Delta—Lets you determine the seriousness of the alert.
  - Sig Fidelity Rating—Lets you choose the weight associated with how well this signature might perform in the absence of specific knowledge of the target.  
The value is 0 to 100. The default is 75.
- Sig Description—Lets you specify the following attributes that help you distinguish this signature from other signatures:
  - Signature Name—Name your signature. The default is MySig.
  - Alert Notes—Add alert notes in this field.
  - User Comments—Add your comments about this signature in this field.
  - Alarm Traits—Add the alarm trait in this field. The value is 0 to 65535. The default is 0.
  - Release—Add the software release in which the signature first appeared.
- Engine—Lets you choose the engine that parses and inspects the traffic specified by this signature.
  - AIC FTP—Inspects FTP traffic and lets you control the commands being issued.
  - AIC HTTP—Provides granular control over HTTP sessions to prevent abuse of the HTTP protocol.
  - Atomic ARP—Inspects Layer-2 ARP protocol. The Atomic ARP engine is different because most engines are based on Layer-3-IP.
  - Atomic IP—Inspects IP protocol packets and associated Layer-4 transport protocols.
  - Atomic IPv6—Detects IOS vulnerabilities that are stimulated by malformed IPv6 traffic.
  - Flood Host—Detects ICMP and UDP floods directed at hosts.
  - Flood Net—Detects ICMP and UDP floods directed at networks.
  - Meta—Defines events that occur in a related manner within a sliding time interval. This engine processes events rather than packets.
  - Multi String—Defines signatures that inspect Layer 4 transport protocol (ICMP, TCP, and UDP) payloads using multiple string matches for one signature. You can specify a series of regular expression patterns that must be matched to fire the signature.
  - Normalizer—Configures how the IP and TCP normalizer functions and provides configuration for signature events related to the IP and TCP normalizer. Allows you to enforce RFC compliance.
  - Service DNS—Inspects DNS (TCP and UDP) traffic.
  - Service FTP—Inspects FTP traffic.

- Service Generic—Decodes custom service and payload.
- Service Generic Advanced—Generically analyzes network protocols.
- Service H225— Inspects VoIP traffic.
- Service HTTP—Inspects HTTP traffic. The WEBPORTS variable defines inspection port for HTTP traffic.
- Service IDENT—Inspects IDENT (client and server) traffic.
- Service MSRPC—Inspects MSRPC traffic.
- Service MSSQL—Inspects Microsoft SQL traffic.
- Service NTP—Inspects NTP traffic.
- Service RPC—Inspects RPC traffic.
- Service SMB—Inspects SMB traffic.
- Service SMB Advanced—Processes Microsoft SMB and Microsoft RPC over SMB packets.
- Service SNMP—Inspects SNMP traffic.
- Service SSH—Inspects SSH traffic.
- Service TNS—Inspects TNS traffic.
- State—Stateful searches of strings in protocols such as SMTP.
- String ICMP—Searches on Regex strings based on ICMP protocol.
- String TCP—Searches on Regex strings based on TCP protocol.
- String UDP—Searches on Regex strings based on UDP protocol.
- Sweep—Analyzes sweeps of ports, hosts, and services, from a single host (ICMP and TCP), from destination ports (TCP and UDP), and multiple ports with RPC requests between two nodes.
- Sweep Other TCP—Analyzes TCP flag combinations from reconnaissance scans that are trying to get information about a single host. The signatures look for flags A, B, and C. When all three are seen, an alert is fired.
- Traffic ICMP—Analyzes nonstandard protocols, such as TFN2K, LOKI, and DDOS. There are only two signatures with configurable parameters.
- Traffic Anomaly—Analyzes TCP, UDP, and other traffic for worm-infested hosts.
- Trojan Bo2k—Analyzes traffic from the nonstandard protocol BO2K. There are no user-configurable parameters in this engine.
- Trojan Tfn2k—Analyzes traffic from the nonstandard protocol TFN2K. There are no user-configurable parameters in this engine.
- Trojan UDP—Analyzes traffic from the UDP protocol. There are no user-configurable parameters in this engine.
- Event Action—Lets you assign the actions the sensor takes when it responds to events.
  - Deny Attacker Inline—(Inline only) Terminates the current packet and future packets from this attacker address for a specified period of time.

The sensor maintains a list of attackers being denied by the system. To remove an entry from the denied attacker list, you can view the list of attackers and clear the entire list, or you can wait for the timer to expire. The timer is a sliding timer for each entry. Therefore, if attacker A



is being denied, but issues another attack, the timer for attacker A is reset and attacker A remains in the denied attacker list until the timer expires. If the denied attacker list is at capacity and cannot add a new entry, the packet is still denied.



**Note** This is the most severe of the deny actions. It denies current and future packets from a single attacker address. To clear all denied attacker entries, choose **Monitoring > Denied Attackers > Clear List**, which permits the addresses back on the network.

- Deny Attacker Service Pair Inline—(Inline only) Does not transmit this packet and future packets on the attacker address victim port pair for a specified period of time.
- Deny Attacker Victim Pair Inline—(Inline only) Does not transmit this packet and future packets on the attacker/victim address pair for a specified period of time.



**Note** For deny actions, to set the specified period of time and maximum number of denied attackers, choose **Configuration > Policies > Event Action Rules > rules0 > General Settings**.

- Deny Connection Inline—(Inline only) Terminates the current packet and future packets on this TCP flow.
- Deny Packet Inline—(Inline only) Terminates the packet.



**Note** You cannot delete the event action override for Deny Packet Inline because it is protected. If you do not want to use that override, disable it.

- Log Attacker Packets—Starts IP logging on packets that contain the attacker address and sends an alert. This action causes an alert to be written to the Event Store, even if Produce Alert is not selected.
- Log Pair Packets—Starts IP Logging on packets that contain the attacker/victim address pair. This action causes an alert to be written to the Event Store, even if Produce Alert is not selected.
- Log Victim Packets—Starts IP Logging on packets that contain the victim address and sends an alert. This action causes an alert to be written to the Event Store, even if Produce Alert is not selected.
- Modify Packet Inline— Modifies packet data to remove ambiguity about what the end point might do with the packet.



**Note** Modify Packet Inline is not an option for Add Event Action Filter or Add Event Action Override.

- Produce Alert—Writes the event to the Event Store as an alert.
- Produce Verbose Alert—Includes an encoded dump of the offending packet in the alert. This action causes an alert to be written to the Event Store, even if Produce Alert is not selected.
- Request Block Connection—Sends a request to ARC to block this connection. You must have blocking devices configured to implement this action.
- Request Block Host—Sends a request to ARC to block this attacker host. You must have blocking devices configured to implement this action.




---

**Note** For block actions, to set the duration of the block, choose **Configuration > Policies > Event Action Rules > rules0 > General Settings**.

---

- Request Rate Limit—Sends a rate limit request to ARC to perform rate limiting. You must have rate limiting devices configured to implement this action.




---

**Note** Request Rate Limit applies to a select set of signatures.

---

- Request SNMP Trap—Sends a request to the Notification Application component of the sensor to perform SNMP notification. This action causes an alert to be written to the Event Store, even if Produce Alert is not selected. You must have SNMP configured on the sensor to implement this action.
- Reset TCP Connection—Sends TCP resets to hijack and terminate the TCP flow. Reset TCP Connection only works on TCP signatures that analyze a single connection. It does not work for sweeps or floods.
- Event Counter—Lets you configure how the sensor counts events. For example, you can specify that you want the sensor to send an alert only if the same signature fires 5 times for the same address set:
  - Event Count—The number of times an event must occur before an alert is generated. The value is 1 to 65535. The default is 1.
  - Event Count Key—The storage type used to count events for this signature. Choose attacker address, attacker address and victim port, attacker and victim addresses, attacker and victim addresses and ports, or victim address. The default is attacker address.
  - Specify Alert Interval—Specifies the time in seconds before the event count is reset. Choose Yes or No from the drop-down list and then specify the amount of time.
- Alert Frequency—Lets you configure how often the sensor alerts you when this signature is firing. Specify the following parameters for this signature:
  - Summary Mode—The mode of alert summarization. Choose Fire All, Fire Once, Global Summarize, or Summarize.




---

**Note** When multiple contexts from the adaptive security appliance are contained in one virtual sensor, the summary alerts contain the context name of the last context that was summarized. Thus, the summary is the result of all alerts of this type from all contexts that are being summarized.

---

- Summary Interval—The time in seconds used in each summary alert. The value is 1 to 65535. The default is 15.
- Summary Key—The storage type used to summarize alerts. Choose Attacker address, Attacker address and victim port, Attacker and victim addresses, Attacker and victim addresses and ports, or Victim address. The default is Attacker address.
- Specify Global Summary Threshold—Lets you specify the threshold number of events to take the alert in to global summary. Choose Yes or No and then specify the threshold number of events.
- Status—Lets you enable or disable a signature, or retire or unretire a signature:
  - Enabled—Lets you choose whether the signature is enabled or disabled. The default is yes (enabled).

- Retired—Let you choose whether the signature is retired or not. The default is no (not retired).
- Obsoletes—Lists the signatures that are obsoleted by this signature.

#### For More Information

- For the procedure for clearing all denied attacker entries, see [Monitoring the Denied Attackers List, page 12-2](#).
- For the procedure for configuring the general settings, see [Configuring the General Settings, page 6-32](#).
- For more information on blocking, see [Chapter 9, “Configuring Attack Response Controller for Blocking and Rate Limiting.”](#)
- For the list of signatures for which you can request a rate limit, see [Understanding Rate Limiting, page 12-7](#).
- For more information on configuring SNMP, see [Chapter 8, “Configuring SNMP.”](#)

## Assign Actions Dialog Box Field Definitions

An event action is the response of the sensor to an event. Event actions are configurable on a per-signature basis.

The following fields are found in the Assign Actions dialog box:

- Product Alert—Writes the event to the Event Store as an alert.



#### Note

The Product Alert action is not automatic when you enable alerts for a signature. To have an alert created in the Event Store, you must select Product Alert. If you add a second action, you must include Product Alert if you want an alert sent to the Event Store. Also, every time you configure the event actions, a new list is created and it replaces the old list. Make sure you include all the event actions you need for each signature.



#### Note

There are other event actions that force a Product Alert. These actions use Product Alert as the vehicle for performing the action. Even if Product Alert is not selected or is filtered, the alert is still produced. The actions are the following: Produce Verbose Alert, Request SNMP Trap, Log Attacker Packets, Log Victim Packets, and Log Pair Packets.



#### Note

A Produce Alert event action is added for an event when global correlation has increased the risk rating of an event, and has added either the Deny Packet Inline or Deny Attacker Inline event action.

- Produce Verbose Alert—Includes an encoded dump of the offending packet in the alert. This action causes an alert to be written to the Event Store, even if Product Alert is not selected.
- Log Attacker Packets—Starts IP logging on packets that contain the attacker address and sends an alert. This action causes an alert to be written to the Event Store, even if Product Alert is not selected.
- Log Victim Packets—Starts IP logging on packets that contain the victim address and sends an alert. This action causes an alert to be written to the Event Store, even if Product Alert is not selected.

- Log Pair Packets—Starts IP logging on packets that contain the attacker/victim address pair. This action causes an alert to be written to the Event Store, even if Product Alert is not selected.
- Request SNMP Trap—Sends a request to the Notification Application component of the sensor to perform SNMP notification. This action causes an alert to be written to the Event Store, even if Product Alert is not selected. You must have SNMP configured on the sensor to implement this action.
- Deny Packet Inline (inline only)—Terminates the packet.




---

**Note** You cannot delete the event action override for Deny Packet Inline because it is protected. If you do not want to use that override, disable it.

---

- Deny Connection Inline (inline only)—Terminates the current packet and future packets on this TCP flow.
- Deny Attacker Victim Pair Inline (inline only)—Does not transmit this packet and future packets on the attacker/victim address pair for a specified period of time.
- Deny Attacker Service Pair Inline (inline only)—Does not transmit this packet and future packets on the attacker address victim port pair for a specified period of time.
- Deny Attacker Inline (inline only)—Terminates the current packet and future packets from this attacker address for a specified period of time.
- The sensor maintains a list of attackers being denied by the system. To remove an entry from the denied attacker list, you can view the list of attackers and clear the entire list, or you can wait for the timer to expire. The timer is a sliding timer for each entry. Therefore, if attacker A is being denied, but issues another attack, the timer for attacker A is reset and attacker A remains in the denied attacker list until the timer expires. If the denied attacker list is at capacity and cannot add a new entry, the packet is still denied.
- Modify Packet Inline (inline only)—Modifies packet data to remove ambiguity about what the end point might do with the packet.




---

**Note** You cannot use Modify Packet Inline as an action when adding event action filters or overrides.

---

- Request Block Connection—Sends a request to ARC to block this connection. You must have blocking devices configured to implement this action.




---

**Note** Connection blocks and network blocks are not supported on adaptive security appliances. Adaptive security appliances only support host blocks with additional connection information.

---




---

**Note** IPv6 does not support Request Block Connection.

---

- Request Block Host—Sends a request to ARC to block this attacker host. You must have blocking devices configured to implement this action.




---

**Note** IPv6 does not support Request Block Host.

---

- Request Rate Limit—Sends a rate limit request to ARC to perform rate limiting. You must have rate limiting devices configured to implement this action.




---

**Note** Request Rate Limit applies to a select set of signatures.

---




---

**Note** IPv6 does not support Request Rate Limit.

---

- Reset TCP Connection—Sends TCP resets to hijack and terminate the TCP flow. Reset TCP Connection only works on TCP signatures that analyze a single connection. It does not work for sweeps or floods.

#### For More Information

- For detailed descriptions of the event actions, see [Event Actions, page 6-7](#).
- For the procedure for clearing all denied attacker entries, see [Monitoring the Denied Attackers List, page 12-2](#).
- For the procedure for configuring the general settings, see [Configuring the General Settings, page 6-32](#).
- For more information on blocking, see [Chapter 9, “Configuring Attack Response Controller for Blocking and Rate Limiting.”](#)
- For the list of signatures for which you can request a rate limit, see [Understanding Rate Limiting, page 12-7](#).
- For more information on configuring SNMP, see [Chapter 8, “Configuring SNMP.”](#)

## Enabling and Disabling Signatures

To enable and disable signatures, follow these steps:

- 
- Step 1** Log in to IDM using an account with administrator or operator privileges.
- Step 2** Choose **Configuration > Policies > Signature Definitions > sig0 > Signature Configuration**.
- Step 3** To locate a signature, choose a sorting option from the Select By drop-down list.  
For example, if you are searching for a Flood Host signature, chose **Engine** from the drop-down list, then **Flood Host** and then select the individual signature.  
The Signature Configuration tab refreshes and displays only those signatures that match your sorting criteria.
- Step 4** To enable or disable an existing signature, select the signature, and follow these steps:
- a. View the Enabled column to determine the status of the signature. A signature that is enabled has the value Yes in this column.
  - b. To enable a signature that is disabled, select the signature, and click **Enable**.  
The Enabled column now reads Yes.
  - c. To disable a signature that is enabled, select the signature, and click **Disable**.  
The Enabled column now reads No.
  - d. To retire one or more signatures, select the signature(s), and click **Retire**.

**Note**

We recommend that you retire any signatures that you are not using. This improves sensor performance.

**Tip**

To discard your changes, click **Reset**.

**Step 5**

Click **Apply** to apply your changes and save the revised configuration.

## Adding Signatures

On the Signature Configuration tab, you can add a custom signature. You can also add custom signatures through the Custom Signature Wizard.

**Tip**

A square green icon indicates the default value is being used. Click the green icon to configure that parameter. Click the value field to change the parameter.

**Tip**

A red diamond icon indicates that a user-defined value is being used. Click the icon to change the value back to the default.

To create a custom signature that is not based on an existing signature, follow these steps:

- Step 1** Log in to IDM using an account with administrator or operator privileges.
- Step 2** Choose **Configuration > Policies > Signature Definitions > sig0 > Signature Configuration**, and then click **Add**.
- Step 3** In the Signature ID field, enter a unique signature ID for the new signature.
- Step 4** In the Subsignature field, enter a unique subsignature ID for the new signature.
- Step 5** From the Alert Severity drop-down list, choose the severity you want to associate with this signature.
- Step 6** In the Promiscuous Delta field, enter the promiscuous delta (between 0 and 30) that you want to associate with this signature.
- Step 7** In the Sig Fidelity Rating field, enter a value between 1 and 100 to represent the signature fidelity rating for this signature.
- Step 8** Complete the Sig Description fields and add any comments about this signature.
- Step 9** In the Select Item(s) dialog box, choose the vulnerable OS(es) and click **OK**.

**Tip**

To select more than one OS, hold down the **Ctrl** key.

- Step 10** From the Engine drop-down list, choose the engine the sensor will use to enforce this signature.



---

**Note** If you do not know which engine to select, use the Custom Signature Wizard to help you create a custom signature.

---

**Step 11** Configure Event Counter:

- a. In the Event Count field, enter the number of events you want counted (1 to 65535).
- b. From the Event Count Key drop-down list, choose the key you want to use.
- c. From the Specify Alert Interface drop-down list, choose whether you want to specify the alert interval (Yes or No).
- d. If you chose Yes, enter the alert interval (2 to 1000) in the Alert Interval field.

**Step 12** Configure the alert frequency.

**Step 13** Configure the status of the signature:

- a. From the Enabled drop-down list, choose **Yes** to enable the signature.



---

**Note** A signature must be enabled for the sensor to actively detect the attack specified by the signature.

---

- b. From the Retired drop-down list, choose **Yes** to make sure the signature is active.  
This places the signature in the engine.



---

**Note** A signature must not be retired for the sensor to actively detect the attack specified by the signature.

---



---

**Tip** To discard your changes and close the Add Signature dialog box, click **Cancel**.

---

**Step 14** Click **OK**.

The new signature appears in the list with the Type set to Custom.

**Step 15** Assign actions to this signature.



---

**Tip** To discard your changes, click **Reset**.

---

**Step 16** Click **Apply** to apply your changes and save the revised configuration.

---

**For More Information**

- For the procedure for using the Custom Signature Wizard to add signatures, see [Master Custom Signature Procedure, page 5-44](#).
- For the procedure for configuring alert frequency, see [Configuring Alert Frequency, page 5-21](#).
- For the procedure for assigning actions to a signature, see [Assigning Actions to Signatures, page 5-18](#).

## Cloning Signatures

On the Signature Configuration tab, you can create a signature by cloning an existing signature. This task can save you time when you are creating signatures that are similar.



**Tip**

A square green icon indicates the default value is being used. Click the green icon to configure that parameter. Click the value field to change the parameter.



**Tip**

A red diamond icon indicates that a user-defined value is being used. Click the icon to change the value back to the default.

To create a signature by using an existing signature as the starting point, follow these steps:

- Step 1** Log in to IDM using an account with administrator or operator privileges.
- Step 2** Choose **Configuration > Policies > Signature Definitions > sig0 > Signature Configuration**.
- Step 3** To locate a signature, choose a sorting option from the Select By drop-down list.  
For example, if you are searching for a Flood Host signature, choose **Engine** from the drop-down list, then **Flood Host**, and then select the individual signature.  
The Signature Configuration tab refreshes and displays only those signatures that match your sorting criteria.
- Step 4** Select the signature and click **Clone**. The Clone Signature dialog box appears.
- Step 5** In the Signature field, enter a unique signature ID for the new signature.
- Step 6** In the Subsignature field, enter a unique subsignature ID for the new signature.
- Step 7** Review the parameter values and change the value of any parameter you want to be different for this new signature.



**Tip**

To select more than one OS or event action, hold down the **Ctrl** key.

- Step 8** Configure the status of the signature:
  - a. From the Enabled drop-down list, choose **Yes** to enable the signature.



**Note**

A signature must be enabled for the sensor to actively detect the attack specified by the signature.

- b. From the Retired drop-down list, choose **Yes** to make sure the signature is active.  
This places the signature in the engine.



**Note**

A signature must not be retired for the sensor to actively detect the attack specified by the signature.





**Tip** To discard your changes and close the Clone Signature dialog box, click **Cancel**.

c. Click **OK**.

The cloned signature now appears in the list with the Type set to Custom.



**Tip** To discard your changes, click **Reset**.

**Step 9** Click **Apply** to apply your changes and save the revised configuration.

#### For More Information

- For the procedure for using the Custom Signature Wizard to add signatures, see [Master Custom Signature Procedure, page 5-44](#).
- For the procedure for configuring alert frequency, see [Configuring Alert Frequency, page 5-21](#).
- For the procedure for assigning actions to a signature, see [Assigning Actions to Signatures, page 5-18](#).

## Tuning Signatures

On the Signature Configuration tab, you can edit, or *tune* a signature.



**Note** You can tune built-in signatures by adjusting several signature parameters. Built-in signatures that have been modified are called *tuned* signatures.



**Tip** A square green icon indicates the default value is being used. Click the green icon to configure that parameter. Click the value field to change the parameter.



**Tip** A red diamond icon indicates that a user-defined value is being used. Click the icon to change the value back to the default.

To tune an existing signature, follow these steps:

**Step 1** Log in to IDM using an account with administrator or operator privileges.

**Step 2** Choose **Configuration > Policies > Signature Definitions > sig0 > Signature Configuration**.

**Step 3** To locate a signature, choose a sorting option from the Select By drop-down list.

For example, if you are searching for a Flood Host signature, choose **Engine** from the drop-down list, then **Flood Host**, and then select the individual signature.

The Signature Configuration tab refreshes and displays only those signatures that match your sorting criteria.

**Step 4** Select the signature and click **Edit**. The Edit Signature dialog box appears.

**Step 5** Review the parameter values and change the value of any parameter you want to tune.



**Tip** To select more than one OS or event action, hold down the **Ctrl** key.

**Step 6** Configure the status of the signature:

- a. From the Enabled drop-down list, choose **Yes** to enable the signature.



**Note** A signature must be enabled for the sensor to actively detect the attack specified by the signature.

- b. From the Retired drop-down list, choose **Yes** to make sure the signature is active.

This places the signature in the engine.



**Note** A signature must not be retired for the sensor to actively detect the attack specified by the signature.



**Tip** To discard your changes and close the Edit Signature dialog box, click **Cancel**.

**Step 7** Click **OK**. The edited signature now appears in the list with the Type set to Tuned.



**Tip** To discard your changes, click **Reset**.

**Step 8** Click **Apply** to apply your changes and save the revised configuration.

#### For More Information

- For the procedure for using the Custom Signature Wizard to add signatures, see [Master Custom Signature Procedure, page 5-44](#).
- For the procedure for configuring alert frequency, see [Configuring Alert Frequency, page 5-21](#).
- For the procedure for assigning actions to a signature, see [Assigning Actions to Signatures, page 5-18](#).

## Assigning Actions to Signatures

On the Signature Configuration tab, you can assign actions to a signature.

To assign actions to a signature or a set of signatures, follow these steps:

**Step 1** Log in to IDM using an account with administrator or operator privileges.

**Step 2** Choose **Configuration > Policies > Signature Definitions > sig0 > Signature Configuration**.

**Step 3** To locate a signature, choose a sorting option from the Select By drop-down list.

For example, if you are searching for a Flood Host signature, chose **Engine** from the drop-down list, then **Flood Host**, and then select the individual signature.

The Signature Configuration tab refreshes and displays only those signatures that match your sorting criteria.

**Step 4** Select the signature(s), and click **Actions**.

The Assign Actions dialog box appears.

**Step 5** Check the check boxes next to the actions you want to assign to the signature(s). Click **Select All** to select all actions. Click **Select None** to clear the check boxes.



**Note** A check mark indicates that the action is assigned to the selected signature(s). No check mark indicates that the action is not assigned to any of the selected signatures. A gray check mark indicates that the action is assigned to some of the selected signatures.



**Tip** To select more than one action, hold down the **Ctrl** key.

Choose from the following actions:

- Deny Attacker Inline—(Inline only) Terminates the current packet and future packets from this attacker address for a specified period of time.  
The sensor maintains a list of attackers being denied by the system. To remove an entry from the denied attacker list, you can view the list of attackers and clear the entire list, or you can wait for the timer to expire. The timer is a sliding timer for each entry. Therefore, if attacker A is being denied, but issues another attack, the timer for attacker A is reset and attacker A remains in the denied attacker list until the timer expires. If the denied attacker list is at capacity and cannot add a new entry, the packet is still denied.
- Deny Attacker Service Pair Inline—(Inline only) Does not transmit this packet and future packets on the attacker address victim port pair for a specified period of time.
- Deny Attacker Victim Pair Inline—(Inline only) Does not transmit this packet and future packets on the attacker/victim address pair for a specified period of time.
- Deny Connection Inline—(Inline only) Terminates the current packet and future packets on this TCP flow.
- Deny Packet Inline—(Inline only) Terminates the packet.
- Log Attacker Packets—Starts IP logging on packets that contain the attacker address and sends an alert. This action causes an alert to be written to the Event Store, even if Produce Alert is not selected.
- Log Pair Packets—Starts IP Logging on packets that contain the attacker/victim address pair. This action causes an alert to be written to the Event Store, even if Produce Alert is not selected.
- Log Victim Packets—Starts IP Logging on packets that contain the victim address and sends an alert. This action causes an alert to be written to the Event Store, even if Produce Alert is not selected.
- Modify Packet Inline— Modifies packet data to remove ambiguity about what the end point might do with the packet.
- Produce Alert—Writes the event to the Event Store as an alert.

- Produce Verbose Alert—Includes an encoded dump of the offending packet in the alert. This action causes an alert to be written to the Event Store, even if Produce Alert is not selected.
- Request Block Connection—Sends a request to ARC to block this connection. You must have blocking devices configured to implement this action.
- Request Block Host—Sends a request to ARC to block this attacker host. You must have blocking devices configured to implement this action.
- Request Rate Limit—Sends a rate limit request to ARC to perform rate limiting. You must have rate limiting devices configured to implement this action.
- Request SNMP Trap—Sends a request to the Notification Application component of the sensor to perform SNMP notification. This action causes an alert to be written to the Event Store, even if Produce Alert is not selected. You must have SNMP configured on the sensor to implement this action.
- Reset TCP Connection—Sends TCP resets to hijack and terminate the TCP flow. Reset TCP Connection only works on TCP signatures that analyze a single connection. It does not work for sweeps or floods.




---

**Tip** To discard your changes and close the Assign Actions dialog box, click **Cancel**.

---

- Step 6** Click **OK** to save your changes and close the dialog box.  
The new action(s) now appears in the Action column.




---

**Tip** To discard your changes, click **Reset**.

---

- Step 7** Click **Apply** to apply your changes and save the revised configuration.
- 

#### For More Information

- For detailed descriptions of the event actions, see [Event Actions, page 6-7](#).
- For the procedure for clearing all denied attacker entries, see [Monitoring the Denied Attackers List, page 12-2](#).
- For the procedure for configuring the general settings, see [Configuring the General Settings, page 6-32](#).
- For more information on blocking, see [Chapter 9, “Configuring Attack Response Controller for Blocking and Rate Limiting.”](#)
- For the list of signatures for which you can request a rate limit, see [Understanding Rate Limiting, page 12-7](#).
- For more information on configuring SNMP, see [Chapter 8, “Configuring SNMP.”](#)
- For detailed information about event actions, see [Event Actions, page 6-7](#).

## Configuring Alert Frequency

You can control how often a signature fires. For example, you may want to decrease the volume of alerts sent out from the sensor. Or you may want the sensor to provide basic aggregation of signature firings in to a single alert. Or you may want to counter anti-IPS tools such as “stick,” which are designed to send bogus traffic so that the IPS produces thousands of alerts during a very short time.



### Note

When multiple contexts from the adaptive security appliance are contained in one virtual sensor, the summary alerts contain the context name of the last context that was summarized. Thus, the summary is the result of all alerts of this type from all contexts that are being summarized.



### Tip

A square green icon indicates the default value is being used. Click the green icon to configure that parameter. Click the value field to change the parameter.



### Tip

A red diamond icon indicates that a user-defined value is being used. Click the icon to change the value back to the default.

To configure the alert frequency of a signature, follow these steps:

- Step 1** Log in to IDM using an account with administrator or operator privileges.
- Step 2** Choose **Configuration > Policies > Signature Definitions > sig0 > Signature Configuration**.  
The Signature Configuration tab appears.
- Step 3** Click **Add** to add a signature, or choose a signature to edit, and click **Edit**.  
The Add Signature or Edit Signature dialog box appears.
- Step 4** Configure the event count, key, and alert interval:
  - a.** In the Event Count field, enter a value for the event count.  
This is the minimum number of hits the sensor must receive before sending one alert for this signature.
  - b.** From the Event Count Key drop-down list, choose an attribute to use as the Event Count Key.  
For example, if you want the sensor to count events based on whether or not they are from the same attacker, choose Attacker address as the Event Count Key.
  - c.** If you want to count events based on a rate, choose **Yes** from the Specify Event Interval drop-down list, and then in the Alert Interval field, enter the number of seconds that you want to use for your interval.
- Step 5** To control the volume of alerts and configure how the sensor summarizes alerts, choose one of the following options from the Summary Mode drop-down list:
  - **Fire All**  
Specifies that you want the sensor to send an alert every time the signature detects malicious traffic. You can then specify additional thresholds that let the sensor dynamically adjust the volume of alerts.  
Go to Step 6.

- **Fire Once**  
Specifies that you want the sensor to send an alert the first time the signature detects malicious traffic. You can then specify additional thresholds that let the sensor dynamically adjust the volume of alerts.  
Go to Step 7.
- **Summarize**  
Specifies that you want the sensor to only send summary alerts for this signature instead of sending alerts every time the signature fires. You can then specify additional thresholds that let the sensor dynamically adjust the volume of alerts.  
Go to Step 8.
- **Global Summarize**  
Specifies that you want the sensor to send an alert the first time a signature fires on an address set, and then only send a global summary alert that includes a summary of all alerts for all address sets over a given time interval.  
Go to Step 9.

**Step 6** Configure the Fire All option:

- a. From the Specify Summary Threshold drop-down list, choose **Yes**.
- b. In the Summary Threshold field, enter the minimum number of hits the sensor must receive before sending a summary alert for this signature.
- c. In the Summary Interval field, enter the number of seconds that you want to use for the time interval.
- d. To have the sensor enter global summarization mode, choose **Yes** from the Specify Global Summary Threshold drop-down list.
- e. In the Global Summary Threshold field, enter the minimum number of hits the sensor must receive before sending a global summary alert.
- f. From the Summary Key drop-down list, choose the type of summary key.  
The summary key identifies the attribute to use for counting events. For example, if you want the sensor to count events based on whether or not they are from the same attacker, choose Attacker address as the summary key.

**Step 7** Configure the Fire Once option:

- a. From the Summary Key drop-down list, choose the type of summary key.  
The summary key identifies the attribute to use for counting events. For example, if you want the sensor to count events based on whether or not they are from the same attacker, choose Attacker address as the summary key.
- b. To have the sensor use global summarization, choose **Yes** from the Specify Global Summary Threshold drop-down list.
- c. In the Global Summary Threshold field, enter the minimum number of hits the sensor must receive before sending a global summary alert.  
When the alert rate exceeds a specified number of signatures in a specified number of seconds, the sensor changes from sending a single alert the first time a signature fires to sending a single global summary alert. When the rate during the interval drops below this threshold, the sensor reverts to its configured alert behavior.

**Note**

When multiple contexts from the adaptive security appliance are contained in one virtual sensor, the summary alerts contain the context name of the last context that was summarized. Thus, the summary is the result of all alerts of this type from all contexts that are being summarized.

- d. In the Summary Interval field, enter the number of seconds during which the sensor counts events for summarization.

**Step 8** Configure the Summarize option:

- a. In the Summary Interval field, enter the number of seconds during which the sensor counts events for summarization.
- b. From the Summary Key drop-down list, choose the type of summary key.

The summary key identifies the attribute to use for counting events. For example, if you want the sensor to count events based on whether or not they are from the same attacker, choose Attacker address as the summary key.

- c. To have the sensor use dynamic global summarization, choose **Yes** from the Specify Global Summary Threshold drop-down list.
- d. In the Global Summary Threshold field, enter the minimum number of hits the sensor must receive before sending a global summary alert.

When the alert rate exceeds a specified number of signatures in a specified number of seconds, the sensor changes from sending a single alert the first time a signature fires to sending a single global summary alert. When the rate during the interval drops below this threshold, the sensor reverts to its configured alert behavior.

**Step 9** To configure the Global Summarize option, in the Summary Interval field, enter the number of seconds during which the sensor counts events for summarization.

**Step 10** Click **OK** to save your alert behavior changes.

You are returned to the Signature Configuration tab.

**Tip**

To discard your changes, click **Reset**.

**Step 11** To apply your alert behavior changes to the signature configuration, click **Apply**.

The signature you added or edited is enabled and added to the list of signatures.

## Example Meta Engine Signature

The Meta engine defines events that occur in a related manner within a sliding time interval. This engine processes events rather than packets. As signature events are generated, the Meta engine inspects them to determine if they match any or several Meta definitions. The Meta engine generates a signature event after all requirements for the event are met.

All signature events are handed off to the Meta engine by the Signature Event Action Processor. The Signature Event Action Processor hands off the event after processing the minimum hits option. Summarization and event action are processed after the Meta engine has processed the component events.

**Caution**

A large number of Meta signatures could adversely affect overall sensor performance.

The following example demonstrates how to create a signature based on the Meta engine.

For example, signature 64000 subsignature 0 fires when it sees the alerts from signature 2000 subsignature 0 and signature 3000 subsignature 0 on the same source address. The source address selection is a result of the meta key default value of Axxx. You can change the behavior by changing the meta key setting to xxBx (destination address) for example.

**Note**

The Meta engine is different from other engines in that it takes alerts as input where most engines take packets as input.

**Tip**

A square green icon indicates the default value is being used. Click the green icon to configure that parameter. Click the value field to change the parameter.

**Tip**

A red diamond icon indicates that a user-defined value is being used. Click the icon to change the value back to the default.

To create a signature based on the Meta engine, follow these steps:

- Step 1** Log in to IDM using an account with administrator or operator privileges.
- Step 2** Choose **Configuration > Policies > Signature Definitions > sig0 > Signature Configuration**, and then click **Add**.
- Step 3** In the Signature ID field, enter a unique signature ID for the new signature.
- Step 4** In the Subsignature field, enter a unique subsignature ID for the new signature.
- Step 5** From the Alert Severity drop-down list, choose the severity you want to associate with this signature.
- Step 6** In the Signature Fidelity Rating field, enter a value between 1 and 100 to represent the signature fidelity rating for this signature.
- Step 7** Leave the default value for the Promiscuous Delta field.
- Step 8** Complete the signature description fields and add any comments about this signature.
- Step 9** From the Vulnerable OS List drop-down list, choose the operating systems that are vulnerable to this signature.

**Tip**

To choose more than one action, hold down the **Ctrl** key.

- Step 10** From the Engine drop-down list, choose **Meta**.
- Step 11** Configure the Meta engine-specific parameters:
  - a.** From the Event Action drop-down list, choose the actions you want the sensor to take when it responds to an event.





---

**Tip** To choose more than one action, hold down the **Ctrl** key.

---

- b. From the Swap Attacker Victim drop-down list, choose **Yes** to swap the attacker and victim addresses and ports (destination and source) in the alert message and for any actions taken.
- c. In the Meta Reset Interval field, enter the time in seconds to reset the Meta signature.  
The valid range is 0 to 3600 seconds. The default is 60 seconds.
- d. Click the pencil icon next to Component List to insert the new signature.  
The Component List dialog box appears.
- e. Click **Add** to insert the first Meta signature.  
The Add List Entry dialog box appears.
- f. In the Entry Key field, enter a name for the entry, for example, Entry1.  
The default is MyEntry.
- g. In the Component Sig ID field, enter the signature ID of the signature (2000 in this example) on which to match this component.
- h. In the Component SubSig ID field, specify the subsignature ID of the signature (0 in this example) on which to match this component.
- i. In the Component Count field, enter the number of times this component must fire before it is satisfied.
- j. Click **OK**.  
You are returned to the Add List Entry dialog box.
- k. Select your entry and click **Select** to move it to the Selected Entries list.
- l. Click **OK**.
- m. Click **Add** to insert the next Meta signature.
- n. In the Entry Key field, enter a name for the entry, for example Entry2.
- o. In the Component Sig ID field, enter the signature ID of the signature (3000 in this example) on which to match this component.
- p. In the Component SubSig ID field, enter the subsignature ID of the signature (0 in this example) on which to match this component.
- q. In the Component Count field, enter the number of times this component must fire before it is satisfied.
- r. Click **OK**.  
You are returned to the Add List Entry dialog box.
- s. Select your entry and click **Select** to move it to the Selected Entries list.
- t. Select the new entry and click **Move Up** or **Move Down** to order the new entry.



---

**Tip** To return the entries to the Entry Key list, click **Reset Ordering**.

---

- u. Click **OK**.
- v. From the Meta Key drop-down list, choose the storage type for the Meta signature:

- Attacker address
  - Attacker and victim addresses
  - Attacker and victim addresses and ports
  - Victim address
- w. In the Unique Victims field, enter the number of unique victims required for this Meta signature. The valid value is 1 to 256. The default is 1.
- x. From the Component List in Order drop-down list, choose **Yes** to have the component list fire in order.

**Step 12** Configure Event Counter:

- a. In the Event Count field, enter the number of events you want counted (1 to 65535).
- b. From the Event Count Key drop-down list, choose the key you want to use.
- c. From the Specify Alert Interface drop-down list, choose whether you want to specify the alert interval (Yes or No).
- d. If you chose Yes, enter the alert interval (2 to 1000) in the Alert Interval field.

**Step 13** Configure the alert frequency.**Step 14** Configure the status of the signature:

- a. From the Enabled drop-down list, choose **Yes** to enable the signature.




---

**Note** A signature must be enabled for the sensor to actively detect the attack specified by the signature.

---

- b. From the Retired drop-down list, choose **Yes** to make sure the signature is active. This places the signature in the engine.




---

**Note** A signature must not be retired for the sensor to actively detect the attack specified by the signature.

---




---

**Tip** To discard your changes and close the Add Signature dialog box, click **Cancel**.

---

**Step 15** Click **OK**.

The new signature appears in the list with the Type set to Custom.




---

**Tip** To discard your changes, click **Reset**.

---

**Step 16** Click **Apply** to apply your changes and save the revised configuration.

**For More Information**

- For detailed descriptions of the event actions, see [Event Actions, page 6-7](#).
- For more information about the Signature Event Action Processor, see [Signature Event Action Processor, page 6-5](#).
- For more information on the Meta engine, see [Meta Engine, page A-16](#).
- For the procedure for configuring alert frequency, see [Configuring Alert Frequency, page 5-21](#).

## Using the Custom Signature Wizard

This section describes the Custom Signature Wizard tab and how to create custom signatures. It contains the following topics:

- [Understanding the Custom Signature Wizard, page 5-27](#)
- [Using a Signature Engine, page 5-28](#)
- [Not Using a Signature Engine, page 5-29](#)
- [Custom Signature Wizard Field Definitions, page 5-30](#)

## Understanding the Custom Signature Wizard

**Note**

---

You must be administrator or operator to create custom signatures.

---

The Custom Signature wizard guides you through a step-by-step process for creating custom signatures. There are two possible sequences—using a signature engine to create your custom signature or creating the custom signature without a signature engine.

The Custom Signature wizard in IPS 6.0 does not support creating custom signatures based on the following signature engines:

- AIC FTP
- AIC HTTP
- Atomic ARP
- Atomic IP6
- Flood Host
- Flood Net
- Meta
- Multi String
- Normalizer
- Service DNS
- Service FTP
- Service Generic
- Service Generic Advanced
- Service H225

- Service IDENT
- Service MSSQL
- Service NTP
- Service SMB
- Service SMB Advanced
- Service SNMP
- Service SSH
- Service TNS
- Sweep Other TCP
- Traffic ICMP
- Traffic Anomaly
- Trojan Bo2k
- Trojan Tfn2k
- Trojan UDF

You can create custom signatures based on these existing signature engines by cloning an existing signature.

**For More Information**

- For more information on the individual signature engines, see [Appendix B, “Signature Engines.”](#)
- For more information on cloning existing signatures, see [Cloning Signatures, page 5-16.](#)
- For more information on using the CLI to create custom signatures using the signature engines not supported by the Custom Signature Wizard, refer to [Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 6.0.](#)

## Using a Signature Engine

The following sequence applies if you use a signature engine to create your custom signature:

---

**Step 1** Choose a signature engine:

- Atomic IP
- Service HTTP
- Service MSRPC
- Service RPC
- State (SMTP, ...)
- String ICMP
- String TCP
- String UDP
- Sweep

**Step 2** Assign the signature identification parameters:

- Signature ID

- Subsignature ID
  - Signature Name
  - Alert Notes (optional)
  - User Comments (optional)
- Step 3** Assign the engine-specific parameters.
- The parameters differ for each signature engine, although there is a group of master parameters that applies to each engine.
- Step 4** Assign the alert response:
- Signature Fidelity Rating
  - Severity of the Alert
- Step 5** Assign the alert behavior.
- You can accept the default alert behavior. To change it, click **Advanced**, which opens the Advanced Alert Behavior wizard. With this wizard you can configure how you want to handle alerts for this signature.
- Step 6** Click **Finish**.
- 

## Not Using a Signature Engine

The following sequence applies if you are not using a signature engine to create your custom signature:

---

- Step 1** Specify the protocol you want to use:
- IP—Go to Step 3.
  - ICMP—Go to Step 2.
  - UDP—Go to Step 2.
  - TCP—Go to Step 2.
- Step 2** For ICMP and UDP protocols, select the traffic type and inspect data type. For TCP protocol, select the traffic type.
- Step 3** Assign the signature identification parameters:
- Signature ID
  - Subsignature ID
  - Signature Name
  - Alert Notes (optional)
  - User Comments (optional)
- Step 4** Assign the engine-specific parameters.
- The parameters differ for each signature engine, although there is a group of master parameters that applies to each engine.
- Step 5** Assign the alert response:
- Signature Fidelity Rating
  - Severity of the Alert

**Step 6** Assign the alert behavior.

You can accept the default alert behavior. To change it, click **Advanced**, which opens the Advanced Alert Behavior wizard. With this wizard you can configure how you want to handle alerts for this signature.

**Step 7** Click **Finish**.

---

## Custom Signature Wizard Field Definitions

This section lists the field definitions for the Custom Signature wizard, and contains the following topics:

- [Welcome Field Definitions, page 5-31](#)
- [Protocol Type Field Definitions, page 5-31](#)
- [Signature Identification Field Definitions, page 5-31](#)
- [Atomic IP Engine Parameters Field Definitions, page 5-32](#)
- [Service HTTP Engine Parameters Field Definitions, page 5-33](#)
- [Service MSRPC Engine Parameters Field Definitions, page 5-34](#)
- [Service RPC Engine Parameters Field Definitions, page 5-34](#)
- [State Engine Parameters Field Definitions, page 5-35](#)
- [String ICMP Engine Parameters Field Definitions, page 5-35](#)
- [String TCP Engine Parameters Field Definitions, page 5-36](#)
- [String UDP Engine Parameters Field Definitions, page 5-37](#)
- [Sweep Engine Parameters Field Definitions, page 5-37](#)
- [ICMP Traffic Type Field Definitions, page 5-38](#)
- [UDP Traffic Type Field Definitions, page 5-38](#)
- [TCP Traffic Type Field Definitions, page 5-38](#)
- [UDP Sweep Type Field Definitions, page 5-38](#)
- [TCP Sweep Type Field Definitions, page 5-39](#)
- [Service Type Field Definitions, page 5-39](#)
- [Inspect Data Field Definitions, page 5-39](#)
- [Alert Response Field Definitions, page 5-39](#)
- [Alert Behavior Field Definitions, page 5-40](#)
- [Advanced Alert Behavior Wizard, page 5-40](#)

## Welcome Field Definitions

The following fields are found in the Welcome window of the Custom Signature wizard.

- Yes—Activates the Select Engine field and lets you choose from a list of signature engines.
- Select Engine—Displays the list of available signature engines. If you know which signature engine you want to use to create a signature, click **Yes**, and choose the engine type from the drop-down list.
  - Atomic IP—Lets you create an Atomic IP signature.
  - Service HTTP—Lets you create a signature for HTTP traffic.
  - Service MSRPC—Lets you create a signature for MSRPC traffic.
  - Service RPC—Lets you create a signature for RPC traffic.
  - State SMTP—Lets you create a signature for SMTP traffic.
  - String ICMP—Lets you create a signature for an ICMP string.
  - String TCP—Lets you create a signature for a TCP string.
  - String UDP—Lets you create a signature for a UDP string.
  - Sweep—Lets you create a signature for a sweep.
- No—Lets you continue with the advanced engine selection screens of the Custom Signature wizard.

## Protocol Type Field Definitions

The following fields are found in the Protocol Type window of the Custom Signature wizard.

- IP—Creates a signature to decode and inspect IP traffic.
- ICMP—Creates a signature to decode and inspect ICMP traffic.
- UDP—Creates a signature to decode and inspect UDP traffic.
- TCP—Creates a signature to decode and inspect TCP traffic.

## Signature Identification Field Definitions

The following fields are found in the Signature Identification window of the Custom Signature wizard.

- Signature ID—Identifies the unique numerical value assigned to this signature.

The signature ID lets the sensor identify a particular signature. The signature ID is reported to the Event Viewer when an alert is generated. The valid range is between 60000 and 65000.
- SubSignature ID—Identifies the unique numerical value assigned to this subsignature.

The subsignature ID identifies a more granular version of a broad signature. The valid value is between 0 and 255. The subsignature is reported to the Event Viewer when an alert is generated.
- Signature Name—Identifies the name assigned to this signature.

Reported to the Event Viewer when an alert is generated.
- Alert Notes—(Optional) Specifies the text that is associated with the alert if this signature fires.

Reported to the Event Viewer when an alert is generated.
- User Comments—(Optional) Specifies notes or other comments about this signature that you want stored with the signature parameters.

## Atomic IP Engine Parameters Field Definitions

The following fields are found in the Atomic IP Engine Parameters window of the Custom Signature wizard. These options let you create a signature to detect a very general or very specific type of traffic.

- Event Action—Specifies the actions you want the sensor to perform if this signature is detected.

The default is Produce Alert.




---

**Tip** To select more than one action, hold down the **Ctrl** key.

---

- Fragment Status—Indicates if you want to inspect fragmented or unfragmented traffic.
- Specify Layer 4 Protocol—(Optional) Lets you choose whether or not a specific protocol applies to this signature. If you choose Yes, you can choose from the following protocols:
  - ICMP Protocol—Lets you specify an ICMP sequence, type, code, identifier, and total length.
  - Other IP Protocols—Lets you specify an identifier.
  - TCP Protocol—Lets you set the TCP flags, window size, mask, payload length, urgent pointer, header length, reserved attribute, and port range for the source and destination.
  - UDP Protocol—Lets you specify a valid UDP length, length mismatch, and port range for the source and destination.
- Specify Payload Inspection—(Optional) Lets you specify the following payload inspection options.
- Specify IP Payload Length—(Optional) Lets you specify the payload length.
- Specify IP Header Length—(Optional) Lets you specify the header length.
- Specify IP Type of Service—(Optional) Lets you specify the type of service.
- Specify IP Time-to-Live—(Optional) Lets you specify the time-to-live for the packet.
- Specify IP Version—(Optional) Lets you specify the IP version.
- Specify IP Identifier—(Optional) Lets you specify an IP identifier.
- Specify IP Total Length—(Optional) Lets you specify the total IP length.
- Specify IP Option Inspection—(Optional) Lets you specify the IP inspection options.
 

Select from the following:

  - IP Option—IP option code to match.
  - IP Option Abnormal Options—Malformed list of options.
- Specify IP Addr Options—(Optional) Lets you specify the following IP Address options:
  - Address with Localhost—Identifies traffic where the local host address is used as either the source or destination.
  - IP Addresses—Lets you specify the source or destination address. Use the following syntax: x.x.x.x-z.z.z.z, for example, 10.10.10.1-10.10.10.254.
  - RFC 1918 Address—Identifies the type of address as RFC 1918.
  - Src IP Equal Dst IP—Identifies traffic where the source and destination addresses are the same.



## Service HTTP Engine Parameters Field Definitions

The following fields are found in the Service HTTP Engine Parameters window of the Custom Signature wizard. These options let you create a signature to detect a very general or very specific type of traffic.

- **Event Action**—Specifies the actions you want the sensor to perform if this signature is detected. The default is Produce Alert.



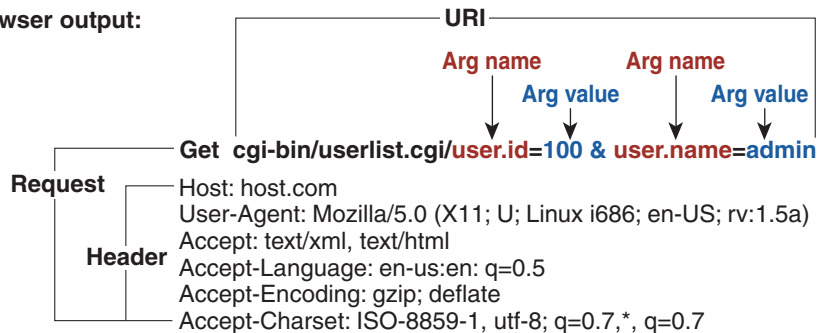
**Tip** To select more than one action, hold down the **Ctrl** key.

- **De Obfuscate**—Specifies whether or not to apply anti-evasive HTTP deobfuscation before searching. The default is Yes.
- **Max Field Sizes**—(Optional) Lets you specify maximum URI, Arg, Header, and Request field lengths.

The following figure demonstrates the maximum field sizes:

**User Input:** <http://10.20.35.6/cgi-bin/userlist.cgi/user.id=100&user.name=admin>

**Browser output:**



**Note\*:** Individual arguments are separated by '&' Argument name and value are separated by "="

- **Regex**—Lets you specify a regular expression for the URI, Arg, Header, and Request Regex.
- **Service Ports**—Identifies the specific service ports used by the traffic. The value is a comma-separated list of ports.
- **Swap Attacker Victim**—Specifies whether to swap the source and destination addresses that are reported in the alert when this signature fires. The default is No.

## Service MSRPC Engine Parameters Field Definitions

The following fields are found in the MSRPC Engine Parameters window of the Custom Signature wizard. These options enable you to create a signature to detect a very general or very specific type of traffic.

- Event Action—Specifies the actions you want the sensor to perform if this signature is detected. The default is Produce Alert.




---

**Tip** To select more than one action, hold down the **Ctrl** key.

---

- Specify Regex String—(Optional) Lets you specify an exact match offset, including the minimum and maximum match offset, Regex string, and minimum match length.
- Protocol—Lets you specify TCP or UDP as the protocol.
- Specify Operation—(Optional) Lets you specify an operation.
- Specify UUID—(Optional) Lets you specify a UUID.

## Service RPC Engine Parameters Field Definitions

The following fields are found in the Service RPC Engine Parameters window of the Custom Signature wizard. These options allow you to create a signature to detect a very general or very specific type of traffic.

- Event Action—Specifies the actions you want the sensor to perform if this signature is detected. The default is Produce Alert.




---

**Tip** To select more than one action, hold down the **Ctrl** key.

---

- Direction—Indicates whether the sensor is watching traffic destined to or coming from the service port. The default is To Service.
- Protocol—Lets you specify TCP or UDP as the protocol.
- Service Ports—Identifies ports or port ranges where the target service may reside. The valid value is a comma-separated list of ports or port ranges.
- Specify Regex String—Lets you specify a Regex string to search for.
- Specify Port Map Program—Identifies the program number sent to the port mapper of interest for this signature. The valid range is 0 to 999999999.
- Specify RPC Program—Identifies the RPC program number of interest for this signature. The valid range is 0 to 1000000.
- Specify Spoof Src—Fires the alarm when the source address is set to 127.0.0.1.
- Specify RPC Max Length—Identifies the maximum allowed length of the whole RPC message. Lengths longer than this cause an alert. The valid range is 0 to 65535.

- Specify RPC Procedure—Identifies the RPC procedure number of interest for this signature. The valid range is 0 to 1000000.

## State Engine Parameters Field Definitions

The following fields are found in the State Engine Parameters window of the Custom Signature wizard. These options allow you to create a signature to detect a very general or very specific type of traffic.

- Event Action—Specifies the actions you want the sensor to perform if this signature is detected. The default is Produce Alert.




---

**Tip** To select more than one action, hold down the **Ctrl** key.

---

- State Machine—Identifies the name of the state to restrict the match of the regular expression string. The options are: Cisco Login, LPR Format String, and SMTP.
  - State Name—Identifies the name of the state. The options are: Abort, Mail Body, Mail Header, SMTP Commands, and Start.
- Specify Min Match Length—Identifies the minimum number of bytes the regular expression string must match from the start of the match to end of the match. The valid range is 0 to 65535.
- Regex String—Identifies the regular expression string that triggers a state transition.
- Direction—Identifies the direction of the data stream to inspect for the transition. The default is To Service.
- Service Ports—Identifies ports or port ranges where the target service may reside. The valid value is a comma-separated list of ports or port ranges.
- Swap Attacker Victim—Specifies whether to swap the source and destination addresses that are reported in the alert when this signature fires. The default is No.
- Specify Exact Match Offset—Identifies the exact stream offset in bytes in which the regular expression string must report the match. If you choose Yes, you can set the exact match offset. The valid range is 0 to 65535. If you choose No, you can set the minimum and maximum match offset.

## String ICMP Engine Parameters Field Definitions

The following fields are found in the String ICMP Engine Parameters window of the Custom Signature wizard. These options allow you to create a signature to detect a very general or very specific type of traffic.

- Event Action—Specifies the actions you want the sensor to perform if this signature is detected. The default is Produce Alert.




---

**Tip** To select more than one action, hold down the **Ctrl** key.

---

- **Specify Min Match Length**—Identifies the minimum number of bytes the regular expression string must match from the start of the match to the end of the match.  
The valid range is 0 to 65535.
- **Regex String**—Identifies the regular expression string to search for in a single packet.
- **Direction**—Identifies the direction of the data stream to inspect for the transition.  
The default is To Service.
- **ICMP Type**—The ICMP header TYPE value.  
The valid range is 0 to 18. The default is 0-18.
- **Swap Attacker Victim**—Specifies whether to swap the source and destination addresses that are reported in the alert when this signature fires.  
The default is No.
- **Specify Exact Match Offset**—Identifies the exact stream offset in bytes in which the regular expression string must report the match.  
If you choose Yes, you can set the exact match offset. The valid range is 0 to 65535.  
If you choose No, you can set the minimum and maximum match offsets.

## String TCP Engine Parameters Field Definitions

The following fields are found in the String TCP Engine Parameters window of the Custom Signature wizard. These options allow you to create a signature to detect a very general or very specific type of traffic.

- **Event Action**—Specifies the actions you want the sensor to perform if this signature is detected.  
The default is Produce Alert.



**Tip** To select more than one action, hold down the **Ctrl** key.

- **Strip Telnet Options**—Strips the Telnet option control characters from the data stream before the pattern is searched.  
This is primarily used as an anti-evasion tool. The default is No.
- **Specify Min Match Length**—Identifies the minimum number of bytes the regular expression string must match from the start of the match to end of the match.  
The valid range is 0 to 65535.
- **Regex String**—Identifies the regular expression string to search for in a single packet.
- **Service Ports**—Identifies ports or port ranges where the target service may reside.  
The valid value is a comma-separated list of ports or port ranges.
- **Direction**—Identifies the direction of the data stream to inspect for the transition.  
The default is To Service.
- **Specify Exact Match Offset**—Identifies the exact stream offset in bytes in which the regular expression string must report the match.  
If you choose Yes, you can set the exact match offset. The valid range is 0 to 65535.  
If you choose No, you can set the minimum and maximum match offsets.

- Swap Attacker Victim—Specifies whether to swap the source and destination addresses that are reported in the alert when this signature fires.

The default is No.

## String UDP Engine Parameters Field Definitions

The following fields are found in the String UDP Engine Parameters window of the Custom Signature wizard. These options allow you to create a signature to detect a very general or very specific type of traffic.

- Event Action—Specifies the actions you want the sensor to perform if this signature is detected.

The default is Produce Alert.




---

**Tip** To select more than one action, hold down the **Ctrl** key.

---

- Specify Min Match Length—Identifies the minimum number of bytes the regular expression string must match from the start of the match to end of the match.

The valid range is 0 to 65535.

- Regex String—Identifies the regular expression string to search for in a single packet.

- Service Ports—Identifies ports or port ranges where the target service may reside.

The valid value is a comma-separated list of ports or port ranges.

- Direction—Identifies the direction of the data stream to inspect for the transition.

- Swap Attacker Victim—Specifies whether to swap the source and destination addresses that are reported in the alert when this signature fires.

The default is No.

- Specify Exact Match Offset—Identifies the exact stream offset in bytes in which the regular expression string must report the match.

If you choose Yes, you can set the exact match offset. The valid range is 0 to 65535.

If you choose No, you can set the minimum and maximum match offset.

## Sweep Engine Parameters Field Definitions

The following fields are found in the Sweep Engine Parameters window in the Custom Signature wizard. These options allow you to create a signature to detect a very general or very specific type of traffic.

- Event Action—Specifies the actions you want the sensor to perform if this signature is detected.

The default is Produce Alert.




---

**Tip** To select more than one action, hold down the **Ctrl** key.

---

- Unique—Identifies the threshold number of unique host connections.

The alarm fires when the unique number of host connections is exceeded during the interval.

- Protocol—Identifies the protocol:
  - ICMP—Lets you specify the ICMP storage type and choose one of these storage keys: attacker address, attacker address and victim port, or attacker and victim addresses.
  - TCP—Lets you choose suppress reverse, inverted sweep, mask, TCP flags, fragment status, storage key, or specify a port range.
  - UDP—Lets you choose a storage key, or specify a port range
- Src Addr Filter—Processes packets that do not have a source IP address (or addresses) defined in the filter values.
- Dst Addr Filter—Processes packets that do not have a destination IP address (or addresses) defined in the filter values.
- Swap Attacker Victim—Specifies whether to swap the source and destination addresses that are reported in the alert when this signature fires.

The default is No.

## ICMP Traffic Type Field Definitions

The following fields are found in the ICMP Traffic Type window of the Custom Signature wizard.

- Single Packet—Specifies that you are creating a signature to inspect a single packet for an attack.
- Sweeps—Specifies that you are creating a signature to detect a sweep attack.

## UDP Traffic Type Field Definitions

The following fields are found in the UDP Traffic Type window of the Custom Signature wizard.

- Single Packet—Specifies that you are creating a signature to inspect a single packet for an attack.
- Sweeps—Specifies that you are creating a signature to detect a sweep attack.

## TCP Traffic Type Field Definitions

The following fields are found in the TCP Traffic Type window of the Custom Signature wizard.

- Single Packet—Specifies that you are creating a signature to inspect a single packet for an attack.
- Single TCP Connection—Specifies that you are creating a signature to inspect a single TCP connection for an attack.
- Multiple Connections—Specifies that you are creating a signature to inspect multiple connections for an attack.

## UDP Sweep Type Field Definitions

The following fields are found in the UDP Sweep Type window of the Custom Signature wizard.

- Host Sweep—Identifies a sweep that searches for hosts on a network.
- Port Sweep—Identifies a sweep that searches for open ports on a host.

## TCP Sweep Type Field Definitions

The following fields are found in the TCP Sweep Type window of the Custom Signature wizard.

- Host Sweep—Identifies a sweep that searches for hosts on a network.
- Port Sweep—Identifies a sweep that searches for open ports on a host.

## Service Type Field Definitions

The following fields are found in the Service Type window of the Custom Signature wizard.

- HTTP—Specifies you are creating a signature to describe an attack that uses the HTTP service.
- SMTP—Specifies you are creating a signature to describe an attack that uses the SMTP service.
- RPC—Specifies you are creating a signature to describe an attack that uses the RPC service.
- MSRPC—Specifies you are creating a signature to describe an attack that uses the MSRPC service.
- Other—Specifies you are creating a signature to describe an attack that uses a service other than HTTP, SMTP, RPC, or MSRPC.

## Inspect Data Field Definitions

The following fields are found in the Inspect Data window of the Custom Signature wizard.

- Header Data Only—Specifies the header as the portion of the packet you want the sensor to inspect.
- Payload Data Only—Specifies the payload as the portion of the packet you want the sensor to inspect.

## Alert Response Field Definitions

The following fields are found in the Alert Response window of the Custom Signature wizard.

- Signature Fidelity Rating—A weight associated with how well this signature might perform in the absence of specific knowledge of the target.

The signature fidelity rating is calculated by the signature author on a per-signature basis. A signature that is written with very specific rules (specific Regex) will have a higher signature fidelity rating than a signature that is written with generic rules.

- Severity of the Alert—The severity at which the alert is reported.

You can choose from the following options:

- High—The most serious security alert.
- Medium—A moderate security alert.
- Low—The least security alert.
- Information—Denotes network activity, not a security alert.

## Alert Behavior Field Definitions

The following buttons are found in the Alert Behavior window of the Custom Signature wizard.

- **Advanced**—Opens the Advanced Alert Behavior window from which you can change the default alert behavior and configure how often the sensor sends alerts.
- **Back**—Returns you to the previous window in the Custom Signature wizard.
- **Next**—Advances you to the next window in the Custom Signature wizard.
- **Finish**—Completes the Custom Signature wizard and saves the signature you created.
- **Cancel**—Exits the Custom Signature wizard.
- **Help**—Displays the help topic for this feature.

## Advanced Alert Behavior Wizard

The following section describes the field definitions for the Advanced Alert Behavior wizard. It contains the following topics:

- [Event Count and Interval Field Definitions, page 5-40](#)
- [Alert Summarization Field Definitions, page 5-41](#)
- [Alert Dynamic Response Summary Field Definitions, page 5-41](#)
- [Alert Dynamic Response Fire All Field Definitions, page 5-42](#)
- [Alert Dynamic Response Fire Once Field Definitions, page 5-42](#)
- [Global Summarization Field Definitions, page 5-42](#)

### Event Count and Interval Field Definitions

The following fields are found in the Event Count and Interval window of the Advanced Alert Behavior wizard.

- **Event Count**—Identifies the minimum number of hits the sensor must receive before sending one alert for this signature.
- **Event Count Key**—Identifies the attribute to use for counting events.  
For example, if you want the sensor to count events based on whether or not they are from the same attacker, select Attacker Address as the Event Count Key.
- **Use Event Interval**—Specifies that you want the sensor to count events based on a rate.  
For example, if set your Event Count to 500 events and your Event Interval to 30 seconds, the sensor sends you one alert if 500 events are received within 30 seconds of one another.
- **Event Interval (seconds)**—Identifies the time interval during which the sensor counts events for rate-based counting.



## Alert Summarization Field Definitions

The following fields are found in the Alert Summarization window of the Advanced Alert Behavior wizard.

- **Alert Every Time the Signature Fires**—Specifies that you want the sensor to send an alert every time the signature detects malicious traffic.  
You can then specify additional thresholds that allow the sensor to dynamically adjust the volume of alerts.
- **Alert the First Time the Signature Fires**—Specifies that you want the sensor to send an alert the first time the signature detects malicious traffic.  
You can then specify additional thresholds that allow the sensor to dynamically adjust the volume of alerts.
- **Send Summary Alerts**—Specifies that you want the sensor to only send summary alerts for this signature, instead of sending alerts every time the signature fires.  
You can then specify additional thresholds that allow the sensor to dynamically adjust the volume of alerts.
- **Send Global Summary Alerts**—Specifies that you want the sensor to send an alert the first time a signature fires on an address set, and then only send a global summary alert that includes a summary of all alerts for all address sets over a given time interval.

## Alert Dynamic Response Summary Field Definitions

The following fields are found in the Alert Dynamic Response window of the Advanced Alert Behavior wizard when you choose Summary.

- **Summary Interval (seconds)**—Identifies the time interval during which the sensor counts events for summarization.
- **Summary Key**—Identifies the attribute to use for counting events.  
For example, if you want the sensor to count events based on whether or not they are from the same attacker, select Attacker Address as the Summary Key.
- **Use Dynamic Global Summarization**—Allows the sensor to dynamically enter global summarization mode.
  - **Global Summary Threshold**—Identifies the minimum number of hits the sensor must receive before sending a global summary alert.

When the alert rate exceeds a specified number of signatures in a specified number of seconds, the sensor changes from sending a single summary alert to sending a single global summary alert. When the rate during the interval drops below this threshold, the sensor reverts to its configured alert behavior.

**Note**

When multiple contexts from the adaptive security appliance are contained in one virtual sensor, the summary alerts contain the context name of the last context that was summarized. Thus, the summary is the result of all alerts of this type from all contexts that are being summarized.

### Alert Dynamic Response Fire All Field Definitions

The following fields are found in the Alert Dynamic Response window of the Advanced Alert Behavior wizard when you choose Alert Every Time the Signature Fires.

- **Summary Key**—Identifies the attribute to use for counting events.  
For example, if you want the sensor to count events based on whether or not they are from the same attacker, select Attacker Address as the Summary Key.
- **Use Dynamic Summarization**—Lets the sensor dynamically enter summarization mode.  
When the alert rate exceeds a specified number of signatures in a specified number of seconds, the sensor changes from sending a single alert for each signature to sending a single global summary alert. When the rate during the interval drops below this threshold, the sensor reverts to its configured alert behavior. A global summary counts signature firings on all attacker IP addresses and ports and all victim IP addresses and ports.
  - **Summary Threshold**—Identifies the minimum number of hits the sensor must receive before sending a summary.
  - **Summary Interval (seconds)**—Specifies that you want to count events based on a rate and identifies the number of seconds that you want to use for the time interval.
- **Specify Summary Threshold**—Lets you choose a summary threshold.
  - **Global Summary Threshold**—Identifies the minimum number of hits the sensor must receive before sending a global summary alert.

### Alert Dynamic Response Fire Once Field Definitions

The following fields are found in the Alert Dynamic Response window of the Advanced Alert Behavior wizard when you choose Alert the First Time the Signature Fires.

Field Descriptions:

- **Summary Key**—Identifies the attribute to use for counting events.  
For example, if you want the sensor to count events based on whether or not they are from the same attacker, select Attacker Address as the Summary Key.
- **Use Dynamic Global Summarization**—Lets the sensor dynamically enter global summarization mode.
  - **Global Summary Threshold**—Identifies the minimum number of hits the sensor must receive before sending a global summary alert.  
When the alert rate exceeds a specified number of signatures in a specified number of seconds, the sensor changes from sending a single alert the first time a signature fires to sending a single global summary alert. When the rate during the interval drops below this threshold, the sensor reverts to its configured alert behavior.
  - **Global Summary Interval (seconds)**—Identifies the time interval during which the sensor counts events for summarization.

### Global Summarization Field Definitions

The following field is found in the Global Summarization window of the Advanced Alert Behavior wizard.

- **Global Summary Interval (seconds)**—Identifies the time interval during which the sensor counts events for summarization.

## Custom Signature Examples

This section provides examples of custom signatures, and contains the following topics:

- [Signature Engines Not Supported in the Custom Signature Wizard, page 5-43](#)
- [Master Custom Signature Procedure, page 5-44](#)
- [Example String TCP Signature, page 5-50](#)
- [Example Service HTTP Signature, page 5-52](#)

## Signature Engines Not Supported in the Custom Signature Wizard

The Custom Signature wizard in IPS 6.0 does not support creating custom signatures based on the following signature engines:

- AIC FTP
- AIC HTTP
- Atomic ARP
- Atomic IP6
- Flood Host
- Flood Net
- Meta
- Multi String
- Normalizer
- Service DNS
- Service FTP
- Service Generic
- Service Generic Advanced
- Service H225
- Service IDENT
- Service MSSQL
- Service NTP
- Service SMB
- Service SMB Advanced
- Service SNMP
- Service SSH
- Service TNS
- Sweep Other TCP
- Traffic ICMP
- Traffic Anomaly
- Trojan Bo2k

- Trojan Tfn2k
- Trojan UDF

You can create custom signatures based on these existing signature engines by cloning an existing signature from the engine you want.

#### For More Information

- For more information about cloning existing signatures, see [Cloning Signatures, page 5-16](#).
- For more information on using the CLI to create custom signatures using the signature engines not supported by IDM, refer to [Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 6.0](#).

## Master Custom Signature Procedure

The Custom Signature wizard provides a step-by-step procedure for configuring custom signatures.

To create custom signatures using the Custom Signature wizard, follow these steps:

- 
- Step 1** Log in to IDM using an account with administrator or operator privileges.
- Step 2** Choose **Configuration > Policies > Signature Definitions > sig0 > Custom Signature Wizard**.  
The Start window appears.




---

**Caution** A custom signature can affect the performance of your sensor. Test the custom signature against a baseline sensor performance for your network to determine the overall impact of the signature.

---

- Step 3** Click **Start the Wizard**.
- Step 4** If you know the specific signature engine you want to use to create the new signature, click the **Yes** radio button, choose the engine from the Select Engine drop-down list, and then click **Next**. Go to Step 13.  
If you do not know what engine you should use, click the **No** radio button, and then click **Next**.
- Step 5** Click the radio button that best matches the type of traffic you want this signature to inspect, and then click **Next**:
- IP (for IP, go to Step 13.)
  - ICMP (for ICMP, go to Step 6.)
  - UDP (for UDP, go to Step 7.)
  - TCP (for TCP, go to Step 9.)
- Step 6** In the ICMP Traffic Type window, click one of the following radio buttons, and then click **Next**:
- Single Packet  
You are creating a signature to inspect a single packet for an attack using either the Atomic IP engine (for Header Data) or the String ICMP engine.  
Go to Step 12.
  - Sweeps  
You are creating a signature to detect a sweep attack using the sweep engine for your new signature.  
Go to Step 13.

- Step 7** In the UDP Traffic Type window, click one of the following radio buttons, and then click **Next**:
- **Single Packet**  
You are creating a signature to inspect a single packet for an attack using either the Atomic IP engine (for Header Data) or the String UDP engine.  
Go to Step 12.
  - **Sweeps**  
You are creating a signature to detect a sweep attack using the sweep engine for the signature.  
Go to Step 8.
- Step 8** In the UDP Sweep Type window, click one of the following radio buttons, and then click **Next**:
- **Host Sweep**  
You are creating a signature that uses a sweep to search for open ports on a host. The sweep engine is used to create the new signature and the storage key is set to Axxx.  
Go to Step 13.
  - **Port Sweep**  
You are creating a signature that uses a sweep to search for hosts on a network. The sweep engine is used to create the new signature and the storage key is set to AxBx.  
Go to Step 13.
- Step 9** In the TCP Traffic Type window, click one of the following radio buttons, and then click **Next**:
- **Single Packet**  
You are creating a signature to inspect a single packet for an attack. The atomic IP engine is used to create the signature.  
Go to Step 13.
  - **Single TCP Connection**  
You are creating a signature to detect an attack in a single TCP connection.  
Go to Step 10.
  - **Multiple Connections**  
You are creating a signature to inspect multiple connections for an attack.  
Go to Step 11.
- Step 10** In the Service Type window, click one of the following radio buttons, and then click **Next**:
- **HTTP**  
You are creating a signature to detect an attack that uses the HTTP service. The service HTTP engine is used to create the signature.
  - **SMTP**  
You are creating a signature to detect an attack that uses the SMTP service. The SMTP engine is used to create the signature.
  - **RPC**  
You are creating a signature to detect an attack that uses the RPC service. The service RPC engine is used to create the signature.

- MSRPC  
You are creating a signature to detect an attack that uses the MSRPC service. The service MSRPC engine is used to create the signature.
- Other  
You are creating a signature to detect an attack that uses a service other than HTTP, SMTP, or RPC. The string TCP engine is used to create the signature.

Go to Step 13.

**Step 11** On the TCP Sweep Type window, click one of the following radio buttons, and then click **Next**:

- Host Sweep  
You are creating a signature that uses a sweep to search for open ports on a host. The sweep engine is used to create the signature and the storage key is set to Axxx.
- Port Sweep  
You are creating a signature that uses a sweep to search for hosts on a network. The Sweep engine is used to create the new signature and the storage key is set to AxBx.

Go to Step 13

**Step 12** In the Inspect Data window, for a single packet, click one of the following radio buttons, and then click **Next**:

- Header Data Only  
Specifies the header as the portion of the packet you want the sensor to inspect.
- Payload Data Only  
Specifies the payload as the portion of the packet you want the sensor to inspect.

Go to Step 13.

**Step 13** In the Signature Identification window, specify the attributes that uniquely identify this signature, and then click **Next**:

- a. In the Signature ID field, enter a number for this signature.  
Custom signatures are range from 60000 to 65000.
- b. In the Subsignature ID field, enter a number for this signature.  
The default is 0.  
You can assign a subsignature ID if you are grouping signatures together that are similar.
- c. In the Signature Name field, enter a name for this signature.  
A default name appears in the Signature Name field. Change it to a name that is more specific for your custom signature.




---

**Note** The signature name, along with the signature ID and subsignature ID, is reported to Event Viewer when an alert is generated.

---

- d. (Optional) In the Alert Notes field, enter text to be added to the alert.  
You can add text to be included in alerts associated with this signature. These notes are reported to Event Viewer when an alert is generated.
- e. (Optional) In the User Comments field, enter text that describes this signature.

You can add any text that you find useful here. This field does not affect the signature or alert in any way.

**Step 14** Assign values to the engine-specific parameters, and then click **Next**.



**Tip**

A square green icon indicates the default value is being used. Click the green icon to configure that parameter. Click the value field to change the parameter.



**Tip**

A red diamond icon indicates that a user-defined value is being used. Click the icon to change the value back to the default.

**Step 15** In the Alert Response window, specify the following alert response options:

- a. In the Signature Fidelity Rating field, enter a value.

The signature fidelity rating is a valid value between 0 and 100 that indicates your confidence in the signature, with 100 being the most confident.

- b. From the Severity of the Alert drop-down list, choose the severity to be reported by Event Viewer when the sensor sends an alert:
  - High
  - Informational
  - Low
  - Medium

**Step 16** To accept the default alert behavior, click **Finish** and go to Step 24. To change the default alert behavior, click **Advanced** and continue with Step 17.



**Note**

You can control how often this signature fires. For example, you may want to decrease the volume of alerts sent out from the sensor. Or you may want the sensor to provide basic aggregation of signature firings in to a single alert. Or you may want to counter anti-IPS tools such as “stick,” which are designed to send bogus traffic so that the IPS produces thousands of alerts during a very short time.

**Step 17** Configure the event count, key, and interval:

- a. In the Event Count field, enter a value for the event count.

This is the minimum number of hits the sensor must receive before sending one alert for this signature.

- b. From the Event Count Key drop-down list, choose an attribute to use as the event count key.

For example, if you want the sensor to count events based on whether or not they are from the same attacker, choose Attacker address as the event count key.

- c. If you want to count events based on a rate, check the **Use Event Interval** check box, and then in the Event Interval (seconds) field, enter the number of seconds that you want to use for your interval.
- d. Click **Next** to continue.

The Alert Summarization window appears.

**Step 18** To control the volume of alerts and configure how the sensor summarizes alerts, click one of the following radio buttons:

- Alert Every Time the Signature Fires

Specifies that you want the sensor to send an alert every time the signature detects malicious traffic. You can then specify additional thresholds that let the sensor dynamically adjust the volume of alerts.

Go to Step 19.

- Alert the First Time the Signature Fires

Specifies that you want the sensor to send an alert the first time the signature detects malicious traffic. You can then specify additional thresholds that let the sensor dynamically adjust the volume of alerts.

Go to Step 20.

- Send Summary Alerts

Specifies that you want the sensor to only send summary alerts for this signature instead of sending alerts every time the signature fires. You can then specify additional thresholds that let the sensor dynamically adjust the volume of alerts.

Go to Step 21.

- Send Global Summary Alerts

Specifies that you want the sensor to send an alert the first time a signature fires on an address set, and then only send a global summary alert that includes a summary of all alerts for all address sets over a given time interval.




---

**Note** When multiple contexts from the adaptive security appliance are contained in one virtual sensor, the summary alerts contain the context name of the last context that was summarized. Thus, the summary is the result of all alerts of this type from all contexts that are being summarized.

---

Go to Step 22.

**Step 19** Configure the Alert Every Time the Signature Fires option:

- a. From the Summary Key drop-down list, choose the type of summary key.

The summary key identifies the attribute to use for counting events. For example, if you want the sensor to count events based on whether or not they are from the same attacker, choose Attacker address as the summary key.

- b. To use dynamic summarization, check the **Use Dynamic Summarization** check box.

Dynamic summarization lets the sensor dynamically adjust the volume of alerts it sends based on the summary parameters you configure.

- c. In the Summary Threshold field, enter the minimum number of hits the sensor must receive before sending a summary alert for this signature.

- d. In the Summary Interval (seconds) field, enter the number of seconds that you want to use for the time interval.

- e. To have the sensor enter global summarization mode, check the **Specify Global Summary Threshold** check box.

- f. In the Global Summary Threshold field, enter the minimum number of hits the sensor must receive before sending a global summary alert.



**Step 20** Configure the Alert the First Time the Signature Fires option:

- a. From the Summary Key drop-down list, choose the type of summary key.

The summary key identifies the attribute to use for counting events. For example, if you want the sensor to count events based on whether or not they are from the same attacker, choose Attacker address as the summary key.

- b. To have the sensor use dynamic global summarization, check the **Use Dynamic Global Summarization** check box.

- c. In the Global Summary Threshold field, enter the minimum number of hits the sensor must receive before sending a global summary alert.

When the alert rate exceeds a specified number of signatures in a specified number of seconds, the sensor changes from sending a single alert the first time a signature fires to sending a single global summary alert. When the rate during the interval drops below this threshold, the sensor reverts to its configured alert behavior.

- d. In the Global Summary Interval (seconds) field, enter the number of seconds during which the sensor counts events for summarization.

**Step 21** Configure the Send Summary Alerts option:

- a. In the Summary Interval (seconds) field, enter the number of seconds during which the sensor counts events for summarization.

- b. From the Summary Key drop-down list, choose the type of summary key.

The summary key identifies the attribute to use for counting events. For example, if you want the sensor to count events based on whether or not they are from the same attacker, choose Attacker address as the summary key.

- c. To have the sensor use dynamic global summarization, check the **Use Dynamic Global Summarization** check box.

- d. In the Global Summary Threshold field, enter the minimum number of hits the sensor must receive before sending a global summary alert.

When the alert rate exceeds a specified number of signatures in a specified number of seconds, the sensor changes from sending a single alert the first time a signature fires to sending a single global summary alert. When the rate during the interval drops below this threshold, the sensor reverts to its configured alert behavior.

**Step 22** In the Global Summary Interval (seconds) field, enter the number of seconds during which the sensor counts events for summarization.

**Step 23** Click **Finish** to save your alert behavior changes.

The Alert Behavior window appears.

**Step 24** Click **Finish** to save your custom signature.

The Create Custom Signature dialog box appears.

**Step 25** Click **Yes** to create the custom signature.



**Tip**

To discard your changes, click **Cancel**.

The signature you created is enabled and added to the list of signatures.

**For More Information**

For more information on the individual signature engines, see [Appendix B, “Signature Engines.”](#)

**Example String TCP Signature**

The String engine is a generic-based pattern-matching inspection engine for ICMP, TCP, and UDP protocols. The String engine uses a regular expression engine that can combine multiple patterns in to a single pattern-matching table allowing for a single search through the data.

There are three String engines: String ICMP, String TCP, and String UDP.

Use the Custom Signature wizard to create a custom String TCP signature.

**Note**

The following procedure also applies to creating custom String ICMP and UDP signatures.

To create a custom String TCP signature, follow these steps:

- Step 1** Log in to IDM using an account with administrator or operator privileges.
- Step 2** Choose **Configuration > Policies > Signature Definitions > sig0 > Custom Signature Wizard**.

**Caution**

A custom signature can affect the performance of your sensor. Test the custom signature against a baseline sensor performance for your network to determine the overall impact of the signature.

- Step 3** Click **Start the Wizard**.
- Step 4** Click the **Yes** radio button, choose **String TCP** from the Select Engine drop-down list, and then click **Next**.

The Signature Identification window appears.

- Step 5** To specify the attributes that uniquely identify this signature, complete the following required values, and then click **Next**:
- In the Signature ID field, enter a number for the signature.  
Custom signatures range from 60000 to 65000.
  - In the Subsignature ID field, enter a number for the signature.  
The default is 0. You can assign a subsignature ID if you are grouping signatures together that are similar.
  - In the Signature Name field, enter a name for the signature.  
A default name, My Sig, appears in the Signature Name field. Change it to a name that is more specific for your custom signature.

**Note**

The signature name, along with the signature ID and subsignature ID, is reported to Event Viewer when an alert is generated.

- (Optional) In the Alert Notes field, enter text to be added to the alert.  
You can add text to be included in alerts associated with this signature. These notes are reported to Event Viewer when an alert is generated. The default is My Sig Info.
- (Optional) In the User Comments field, enter text that describes this signature.

You can add any text that you find useful here. This field does not affect the signature or alert in any way. The default is Sig Comment.

Click **Next**.



**Tip**

A square green icon indicates the default value is being used. Click the green icon to configure that parameter. Click the value field to change the parameter.



**Tip**

A red diamond icon indicates that a user-defined value is being used. Click the icon to change the value back to the default.

**Step 6** Assign the event actions.

The default is Produce Alert. You can assign more actions, such as deny or block, based on your security policy.



**Tip**

To select more than one action, hold down the **Ctrl** key.

**Step 7** (Optional) In the Strip Telnet Options field, choose **Yes** from the drop-down list to strip the Telnet option characters from the data before the pattern is searched.

**Step 8** (Optional) In the Specify Min Match Length field, choose **Yes** from the drop-down list to enable minimum match length, and then in the Min Match Length field, enter the minimum number of bytes the regular expression string must match (0 to 65535).

**Step 9** In the Regex String field, enter the string this signature will be looking for in the TCP packet.

**Step 10** In the Service Ports field, enter the port number, for example, 23.

The value is a comma-separated list of ports or port ranges where the target service resides.

**Step 11** From the Direction drop-down list, choose the direction of the traffic:

- From Service—Traffic from service port destined to client port.
- To Service—Traffic from client port destined to service port.

**Step 12** (Optional) In the Specify Exact Match Offset field, choose **Yes** from the drop-down list to enable exact match offset.

The exact match offset is the exact stream offset the regular expression string must report for a match to be valid (0 to 65535).

- a. In the Specify Max Match Offset field, enter the maximum value.
- b. In the Specify Min Match Offset field, enter the minimum value.

**Step 13** From the Swap Attacker Victim drop-down list, choose **Yes** to swap the attacker and victim addresses and ports (destination and source) in the alert message and for any actions taken.

**Step 14** Click **Next**.

The Alert Response window appears.

**Step 15** (Optional) You can change the following default alert response options:

- a. In the Signature Fidelity Rating field, enter a value.

The signature fidelity rating is a valid value between 0 and 100 that indicates your confidence in the signature, with 100 being the most confident. The default is 75.

- b. In the Severity of the Alert field, choose the severity to be reported by Event Viewer when the sensor sends an alert. The default is Medium.

**Step 16** Click **Next**.

The Alert Behavior window appears.

**Step 17** To change the default alert behavior, click **Advanced**.

The Advanced Alert Behavior wizard Event Count and Interval window appears. To change the default alert behavior, follow Steps 16 through 23 of [Master Custom Signature Procedure, page 5-44](#). Otherwise click **Finish** and your custom signature is created.

The Create Custom Signature dialog box appears and asks if you want to create and apply this custom signature to the sensor.

**Step 18** Click **Yes** to create the custom signature.



**Tip** To discard your changes, click **Cancel**.

The signature you created is enabled and added to the list of signatures.

#### For More Information

For more information on the String engines, see [String Engines, page A-42](#)

## Example Service HTTP Signature

The Service HTTP engine is a service-specific string-based pattern-matching inspection engine. The HTTP protocol is one of the most commonly used in networks of today. In addition, it requires the most amount of preprocessing time and has the most number of signatures requiring inspection making it critical to the overall performance of the system.

The Service HTTP engine uses a Regex library that can combine multiple patterns in to a single pattern-matching table allowing a single search through the data. This engine searches traffic directed to web services only to web services, or HTTP requests. You cannot inspect return traffic with this engine. You can specify separate web ports of interest in each signature in this engine.

HTTP deobfuscation is the process of decoding an HTTP message by normalizing encoded characters to ASCII equivalent characters. It is also known as ASCII normalization.

Before an HTTP packet can be inspected, the data must be deobfuscated or normalized to the same representation that the target system sees when it processes the data. It is ideal to have a customized decoding technique for each host target type, which involves knowing what operating system and web server version is running on the target. The Service HTTP engine has default deobfuscation behavior for the Microsoft IIS web server.

Use the Custom Signature wizard to create a custom Service HTTP signature.

To create a custom Service HTTP signature, follow these steps:

**Step 1** Log in to IDM using an account with administrator or operator privileges.

**Step 2** Choose **Configuration > Policies > Signature Definitions > sig0 > Custom Signature Wizard**.

**Caution**

A custom signature can affect the performance of your sensor. Test the custom signature against a baseline sensor performance for your network to determine the overall impact of the signature.

**Step 3** Click **Start the Wizard**.

**Step 4** Click the **Yes** radio button, choose **Service HTTP** from the Select Engine drop-down list, and then click **Next**.

**Step 5** To specify the attributes that uniquely identify this signature, complete the following required values, and then click **Next**:

- a. In the Signature ID field, enter a number for the signature.

Custom signatures range from 60000 to 65000.

- b. In the Subsignature ID field, enter a number for the signature.

The default is 0. You can assign a subsignature ID if you are grouping signatures together that are similar.

- c. In the Signature Name field, enter a name for the signature.

A default name, My Sig, appears in the Signature Name field. Change it to a name that is more specific for your custom signature.

**Note**

The signature name, along with the signature ID and subsignature ID, is reported to Event Viewer when an alert is generated.

- d. (Optional) In the Alert Notes field, enter text to be added to the alert.

You can add text to be included in alerts associated with this signature. These notes are reported to Event Viewer when an alert is generated. The default is My Sig Info.

- e. (Optional) In the User Comments field, enter text that describes this signature.

You can add any text that you find useful here. This field does not affect the signature or alert in any way. The default is Sig Comment.

Click **Next**.

**Tip**

A square green icon indicates the default value is being used. Click the green icon to configure that parameter. Click the value field to change the parameter.

**Tip**

A red diamond icon indicates that a user-defined value is being used. Click the icon to change the value back to the default.

**Step 6** Assign the event actions.

The default is Produce Alert. You can assign more actions, such as deny or block, based on your security policy.

**Tip**

To select more than one action, hold down the **Ctrl** key.

- Step 7** In the De Obfuscate field, choose **Yes** from the drop-down list to configure the signature to apply anti-evasive deobfuscation before searching.
- Step 8** (Optional) Under Max Field Sizes you can configure the following optional parameters for maximum field sizes:
- Specify Max URI Field Length—Enables the maximum URI field length.
  - Specify Max Arg Field Length—Enables maximum argument field length.
  - Specify Max Header Field Length—Enables maximum header field length.
  - Specify Max Request Field Length—Enables maximum request field length.
- Step 9** Under Regex, configure the Regex parameters:
- a. In the Specify URI Regex field, choose **Yes** from the drop-down list.
  - b. In the URI Regex field, enter the URI Regex, for example, [Mm][Yy][Ff][Oo][Oo].
  - c. You can specify values for the following optional parameters:
    - Specify Arg Name Regex—Enables searching the Arguments field for a specific regular expression.
    - Specify Header Regex—Enables searching the Header field for a specific regular expression.
    - Specify Request Regex—Enables searching the Request field for a specific regular expression.
- Step 10** In the Service Ports field, enter the port number. For example, you can use the web ports variable, \$WEBPORTS.
- The value is a comma-separated list of ports or port ranges where the target service resides.
- Step 11** (Optional) From the Swap Attacker Victim drop-down list, choose **Yes** to swap the attacker and victim addresses and ports (destination and source) in the alert message and for any actions taken.
- Step 12** Click **Next**.
- The Alert Response window appears.
- Step 13** (Optional) You can change the following default alert response options:
- a. In the Signature Fidelity Rating field, enter a value.  
The signature fidelity rating is a valid value between 0 and 100 that indicates your confidence in the signature, with 100 being the most confident. The default is 75.
  - b. In the Severity of the Alert field, choose the severity to be reported by Event Viewer when the sensor sends an alert. The default is Medium.
- Step 14** Click **Next**.
- Step 15** To change the default alert behavior, click **Advanced**.
- The Advanced Alert Behavior wizard Event Count and Interval window appears. To change the default alert behavior, follow Steps 16 through 23 of [Master Custom Signature Procedure, page 5-44](#). Otherwise click **Finish** and your custom signature is created.
- The Create Custom Signature dialog box appears and asks if you want to create and apply this custom signature to the sensor.
- Click **Yes** to create the custom signature. The signature you created is enabled and added to the list of signatures.

**Tip**

To discard your changes, click **Cancel**.

**For More Information**

For more information on the Service HTTP engine, see [Example Service HTTP Signature, page 5-52](#).

## Configuring Signature Variables

This section describes the Signature Variables tab and how to create signature variables. It contains the following topics:

- [Signature Variables Tab, page 5-55](#)
- [Signature Variables Tab Field Definitions, page 5-55](#)
- [Add and Edit Signature Variable Dialog Boxes Field Definitions, page 5-56](#)
- [Adding, Editing, and Deleting Signature Variables, page 5-56](#)

## Signature Variables Tab

**Note**

You must be administrator or operator to configure signature variables.

When you want to use the same value within multiple signatures, use a variable. When you change the value of a variable, that variable is updated in all signatures in which it appears. This saves you from having to change the variable repeatedly as you configure signatures.

**Note**

You must preface the variable with a dollar (\$) sign to indicate that you are using a variable rather than a string.

Some variables cannot be deleted because they are necessary to the signature system. If a variable is protected, you cannot select it to edit it. You receive an error message if you try to delete protected variables. You can edit only one variable at a time.

## Signature Variables Tab Field Definitions

The following fields are found on the Signature Variables tab:

- **Name**—Identifies the name assigned to this variable.
- **Type**—Identifies the variable as a web port or IP address range.
- **Value**—Identifies the value(s) represented by this variable.

To designate multiple port numbers for a single variable, place a comma between the entries. For example, 80, 3128, 8000, 8010, 8080, 8888, 24326.

## Add and Edit Signature Variable Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Signature Variable dialog boxes:

- Name—Identifies the name assigned to this variable.
- Type—Identifies the variable as a web port or IP address range.
- Value—Identifies the value(s) represented by this variable.

To designate multiple port numbers for a single variable, place a comma between the entries. For example, 80, 3128, 8000, 8010, 8080, 8888, 24326.

### Adding, Editing, and Deleting Signature Variables

To add, edit, and delete signature variables, follow these steps:

- 
- Step 1** Log in to IDM using an account with administrator or operator privileges.
- Step 2** Choose **Configuration > Policies > Signature Definitions > sig0 > Signature Variables**, and then click **Add**.
- Step 3** In the Name field, enter the name of the signature variable.



**Note** A valid name can only contain numbers or letters. You can also use a hyphen (-) or underscore (\_).

- Step 4** From the Type drop-down list, choose the type of signature variable.
- Step 5** In the Value field, enter the value for the new signature variable.



**Note** You can use commas as delimiters. Make sure there are no trailing spaces after the comma. Otherwise, you receive a `Validation failed` error.

WEBPORTS has a predefined set of ports where web servers are running, but you can edit the value. This variable affects all signatures that have web ports. The default is 80, 3128, 8000, 8010, 8080, 8888, 24326.

- Step 6** Click **OK**.
- The new variable appears in the signature variables list on the Signature Variables tab.
- Step 7** To edit an existing variable, select it in the signature variables list, and then click **Edit**.
- The Edit Signature Variable dialog box appears for the variable that you chose.
- Step 8** Make any necessary changes in the Value field.
- Step 9** Click **OK**.
- The edited variable appears in the signature variables list on the Signature Variables tab.
- Step 10** To delete a variable, select it in the signature variables list, and then click **Delete**.
- The variable no longer appears in the signature variables list on the Signature Variables tab.



**Tip** To discard your changes, click **Reset**.



**Step 11** Click **Apply** to apply your changes and save the revised configuration.

---

## Miscellaneous Tab

This section describes the Miscellaneous tab and how to configure AIC signatures, IP fragment reassembly signatures, TCP stream reassembly signatures, and IP logging. It contains the following topics:

- [Miscellaneous Tab, page 5-57](#)
- [Miscellaneous Tab Field Definitions, page 5-58](#)
- [Configuring Application Policy Signatures, page 5-59](#)
- [Configuring IP Fragment Reassembly Signatures, page 5-69](#)
- [Configuring TCP Stream Reassembly Signatures, page 5-73](#)
- [Configuring IP Logging, page 5-80](#)

## Miscellaneous Tab



### Note

---

You must be administrator or operator to configure the parameters on the Miscellaneous tab.

---

On the Miscellaneous tab, you can perform the following tasks:

- Configure the application policy parameters (also known as AIC signatures)

You can configure the sensor to provide Layer 4 to Layer 7 packet inspection to prevent malicious attacks related to web services. You first set up the AIC parameters, then you can either use the default AIC signatures or tune them.

- Configure IP fragment reassembly options

You can configure the sensor to reassemble a datagram that has been fragmented over multiple packets. You can specify boundaries that the sensor uses to determine how many datagrams and how long to wait for more fragments of a datagram. The goal is to ensure that the sensor does not allocate all its resources to datagrams that cannot be completely reassembled, either because the sensor missed some frame transmissions or because an attack has been launched that is based on generating random fragment datagrams. You first choose the method the sensor will use to perform IP fragment reassembly, then you can tune the IP fragment reassembly signatures, which are part of the Normalizer engine.

- Configure TCP stream reassembly

You can configure the sensor to monitor only TCP sessions that have been established by a complete three-way handshake. You can also configure how long to wait for the handshake to complete, and how long to keep monitoring a connection where no more packets have been seen. The goal is to prevent the sensor from creating alerts where a valid TCP session has not been established. There are known attacks against sensors that try to get the sensor to generate alerts by simply replaying pieces of an attack. The TCP session reassembly feature helps to mitigate these types of attacks against the sensor. You first choose the method the sensor will use to perform TCP stream reassembly, then you can tune TCP stream reassembly signatures, which are part of the Normalizer engine.

**Caution**

For signature 3050 Half Open SYN Attack, if you choose modify packet inline as the action, you can see as much as 20 to 30% performance degradation while the protection is active. The protection is only active during an actual SYN flood.

- Configure IP logging options  
You can configure a sensor to generate an IP session log when the sensor detects an attack. When IP logging is configured as a response action for a signature and the signature is triggered, all packets to and from the source address of the alert are logged for a specified period of time.

**For More Information**

- For the procedure for setting up the AIC parameters, see [Configuring Application Policy Signatures, page 5-59](#).
- For an example of an AIC signature, see [Example Recognized Define Content Type \(MIME\) Signature, page 5-68](#).
- For the procedure to configure the mode for IP fragment reassembly, see [Configuring the Mode for IP Fragment Reassembly, page 5-71](#).
- For an example of an IP fragment reassembly signature, see [Configuring IP Fragment Reassembly Signatures, page 5-72](#).
- For the procedure to configure the mode for TCP stream reassembly, see [Configuring the Mode for TCP Stream Reassembly, page 5-78](#).
- For an example of a TCP stream reassembly signature, see [Configuring TCP Stream Reassembly Signatures, page 5-79](#).
- For the procedure for configuring IP logging, see [Configuring IP Logging, page 5-80](#).

## Miscellaneous Tab Field Definitions


The following fields are found on the Miscellaneous tab:

- Application Policy—Lets you configure application policy enforcement.
  - Enable HTTP —Enables protection for web services. Check the Yes check box to require the sensor to inspect HTTP traffic for compliance with the RFC.
  - Max HTTP Requests—Specifies the maximum number of outstanding HTTP requests per connection.
  - AIC Web Ports—Specifies the variable for ports to look for AIC traffic.



**Note** We recommend that you not configure AIC web ports, but rather use the default web ports.

- Enable FTP—Enables protection for web services. Check the Yes check box to require the sensor to inspect FTP traffic.
- Fragment Reassembly—Lets you configure IP fragment reassembly.
  - IP Reassembly Mode—Identifies the method the sensor uses to reassemble the fragments, based on the operating system.

- Stream Reassembly—Lets you configure TCP stream reassembly.
    - TCP Handshake Required—Specifies that the sensor should only track sessions for which the three-way handshake is completed.
    - TCP Reassembly Mode—Specifies the mode the sensor should use to reassemble TCP sessions with the following options:
      - Asymmetric—Can only see one direction of bidirectional traffic flow.
- 
-  **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—If a packet is missed for any reason, all packets after the missed packet are not processed.
  - Loose—Use in environments where packets might be dropped.
- IP Log—Lets you configure the sensor to stop IP logging when any of the following conditions are met:
    - Max IP Log Packets—Identifies the number of packets you want logged.
    - IP Log Time—Identifies the duration you want the sensor to log. A valid value is 1 to 60 seconds. The default is 30 seconds.
    - Max IP Log Bytes—Identifies the maximum number of bytes you want logged.

## Configuring Application Policy Signatures

This section describes Application Inspection and Control (AIC) signatures and how to configure them. It contains the following topics:

- [Understanding the AIC Engine, page 5-59](#)
- [AIC Engine and Sensor Performance, page 5-61](#)
- [AIC Request Method Signatures, page 5-61](#)
- [AIC MIME Define Content Type Signatures, page 5-63](#)
- [AIC Transfer Encoding Signatures, page 5-66](#)
- [AIC FTP Commands Signatures, page 5-66](#)
- [Configuring Application Policy, page 5-67](#)
- [Example Recognized Define Content Type \(MIME\) Signature, page 5-68](#)

## Understanding the AIC Engine

AIC provides detailed analysis of web traffic. It provides granular control over HTTP sessions to prevent abuse of the HTTP protocol. It also allows administrative control over applications that attempt to tunnel over specified ports, such as instant messaging, and tunneling applications such as, gotomypc. Inspection and policy checks for P2P and instant messaging is possible if these applications are running over HTTP.

AIC also provides a way to inspect FTP traffic and control the commands being issued. You can enable or disable the predefined signatures or you can create policies through custom signatures.

The AIC engine runs when HTTP traffic is received on AIC web ports. If traffic is web traffic, but not received on the AIC web ports, the Service HTTP engine is executed. AIC inspection can be on any port if it is configured as an AIC web port and the traffic to be inspected is HTTP traffic.

**Caution**

The AIC web ports are regular HTTP web ports. You can turn on AIC web ports to distinguish which ports should watch for regular HTTP traffic and which ports should watch for AIC enforcement. You might use AIC web ports, for example, if you have a proxy on port 82 and you need to monitor it. We recommend that you do not configure separate ports for AIC enforcement.

AIC has the following categories of signatures:

- HTTP request method
  - Define request method
  - Recognized request methods
- MIME type
  - Define content type
  - Recognized content type

- Define web traffic policy

There is one predefined signature, 12674, that specifies the action to take when noncompliant HTTP traffic is seen. The parameter Alarm on Non HTTP Traffic enables the signature. By default this signature is enabled.

- Transfer encodings
  - Associate an action with each method
  - List methods recognized by the sensor
  - Specify which actions need to be taken when a chunked encoding error is seen
- FTP commands
 

Associates an action with an FTP command.

**For More Information**

- For more information on the AIC signature engine, see [AIC Engine, page A-10](#).
- For a list of signature IDs and descriptions of request method signatures, see [AIC Request Method Signatures, page 5-61](#).
- For a list of signature IDs and descriptions of MIME type signatures, see [AIC MIME Define Content Type Signatures, page 5-63](#).
- For the procedure for creating a custom MIME signature, see [Configuring Application Policy, page 5-67](#).
- For a list of signature IDs and descriptions for transfer encoding signatures, see [AIC Transfer Encoding Signatures, page 5-66](#).
- For a list of signature IDs and descriptions for FTP command signatures, see [AIC FTP Commands Signatures, page 5-66](#).

## AIC Engine and Sensor Performance

Application policy enforcement is a unique sensor feature. Rather than being based on traditional IPS technologies that inspect for exploits, vulnerabilities, and anomalies, AIC policy enforcement is designed to enforce HTTP and FTP service policies. The inspection work required for this policy enforcement is extreme compared with traditional IPS inspection work. A large performance penalty is associated with using this feature. When AIC is enabled, the overall bandwidth capacity of the sensor is reduced.

AIC policy enforcement is disabled in the IPS default configuration. If you want to activate AIC policy enforcement, we highly recommend that you carefully choose the exact policies of interest and disable those you do not need. Also, if your sensor is near its maximum inspection load capacity, we recommend that you not use this feature since it can oversubscribe the sensor. We recommend that you use the adaptive security appliance firewall to handle this type of policy enforcement.

## AIC Request Method Signatures

The HTTP request method has two categories of signatures:

- Define request method—Allows actions to be associated with request methods. You can expand and modify the signatures (Define Request Method).
- Recognized request methods—Lists methods that are recognized by the sensor (Recognized Request Methods).

[Table 5-1](#) lists the predefined define request method signatures. Enable the signatures that have the predefined content type you need.

**Table 5-1** Request Method Signatures

Signature ID	Define Request Method
12676	Request Method Not Recognized
12677	Define Request Method PUT
12678	Define Request Method CONNECT
12679	Define Request Method DELETE
12680	Define Request Method GET
12681	Define Request Method HEAD
12682	Define Request Method OPTIONS
12683	Define Request Method POST
12685	Define Request Method TRACE
12695	Define Request Method INDEX
12696	Define Request Method MOVE
12697	Define Request Method MKDIR
12698	Define Request Method COPY
12699	Define Request Method EDIT
12700	Define Request Method UNEDIT
12701	Define Request Method SAVE
12702	Define Request Method LOCK

**Table 5-1** Request Method Signatures (continued)

<b>Signature ID</b>	<b>Define Request Method</b>
12703	Define Request Method UNLOCK
12704	Define Request Method REVLABEL
12705	Define Request Method REVLOG
12706	Define Request Method REVADD
12707	Define Request Method REVNUM
12708	Define Request Method SETATTRIBUTE
12709	Define Request Method GETATTRIBUTE
12710	Define Request Method GETPROPERTIES
12711	Define Request Method STARTENV
12712	Define Request Method STOPREV

**For More Information**

For the procedure for enabling signatures, see [Enabling and Disabling Signatures, page 5-13](#).

## AIC MIME Define Content Type Signatures

There are two policies associated with MIME types:

- Define content type—Associates specific actions for the following cases (Define Content Type):
  - Deny a specific MIME type, such as an image/jpeg
  - Message size violation
  - MIME-type mentioned in header and body do not match
- Recognized content type (Recognized Content Type)

Table 5-2 lists the predefined define content type signatures. Enable the signatures that have the predefined content type you need. You can also create custom define content type signatures.

**Table 5-2 Define Content Type Signatures**

Signature ID	Signature Description
12621	Content Type image/gif Invalid Message Length
12622 2	Content Type image/png Verification Failed
12623 0	Content Type image/tiff Header Check
12623 1	Content Type image/tiff Invalid Message Length
12623 2	Content Type image/tiff Verification Failed
12624 0	Content Type image/x-3ds Header Check
12624 1	Content Type image/x-3ds Invalid Message Length
12624 2	Content Type image/x-3ds Verification Failed
12626 0	Content Type image/x-portable-bitmap Header Check
12626 1	Content Type image/x-portable-bitmap Invalid Message Length
12626 2	Content Type image/x-portable-bitmap Verification Failed
12627 0	Content Type image/x-portable-graymap Header Check
12627 1	Content Type image/x-portable-graymap Invalid Message Length
12627 2	Content Type image/x-portable-graymap Verification Failed
12628 0	Content Type image/jpeg Header Check
12628 1	Content Type image/jpeg Invalid Message Length
12628 2	Content Type image/jpeg Verification Failed
12629 0	Content Type image/cgf Header Check
12629 1	Content Type image/cgf Invalid Message Length
12631 0	Content Type image/x-xpm Header Check
12631 1	Content Type image/x-xpm Invalid Message Length
12633 0	Content Type audio/midi Header Check
12633 1	Content Type audio/midi Invalid Message Length
12633 2	Content Type audio/midi Verification Failed
12634 0	Content Type audio/basic Header Check
12634 1	Content Type audio/basic Invalid Message Length
12634 2	Content Type audio/basic Verification Failed
12635 0	Content Type audio/mpeg Header Check
12635 1	Content Type audio/mpeg Invalid Message Length
12635 2	Content Type audio/mpeg Verification Failed

**Table 5-2 Define Content Type Signatures (continued)**

<b>Signature ID</b>	<b>Signature Description</b>
12636 0	Content Type audio/x-adpcm Header Check
12636 1	Content Type audio/x-adpcm Invalid Message Length
12636 2	Content Type audio/x-adpcm Verification Failed
12637 0	Content Type audio/x-aiff Header Check
12637 1	Content Type audio/x-aiff Invalid Message Length
12637 2	Content Type audio/x-aiff Verification Failed
12638 0	Content Type audio/x-ogg Header Check
12638 1	Content Type audio/x-ogg Invalid Message Length
12638 2	Content Type audio/x-ogg Verification Failed
12639 0	Content Type audio/x-wav Header Check
12639 1	Content Type audio/x-wav Invalid Message Length
12639 2	Content Type audio/x-wav Verification Failed
12641 0	Content Type text/html Header Check
12641 1	Content Type text/html Invalid Message Length
12641 2	Content Type text/html Verification Failed
12642 0	Content Type text/css Header Check
12642 1	Content Type text/css Invalid Message Length
12643 0	Content Type text/plain Header Check
12643 1	Content Type text/plain Invalid Message Length
12644 0	Content Type text/richtext Header Check
12644 1	Content Type text/richtext Invalid Message Length
12645 0	Content Type text/sgml Header Check
12645 1	Content Type text/sgml Invalid Message Length
12645 2	Content Type text/sgml Verification Failed
12646 0	Content Type text/xml Header Check
12646 1	Content Type text/xml Invalid Message Length
12646 2	Content Type text/xml Verification Failed
12648 0	Content Type video/flc Header Check
12648 1	Content Type video/flc Invalid Message Length
12648 2	Content Type video/flc Verification Failed
12649 0	Content Type video/mpeg Header Check
12649 1	Content Type video/mpeg Invalid Message Length
12649 2	Content Type video/mpeg Verification Failed
12650 0	Content Type text/xmcd Header Check
12650 1	Content Type text/xmcd Invalid Message Length
12651 0	Content Type video/quicktime Header Check
12651 1	Content Type video/quicktime Invalid Message Length
12651 2	Content Type video/quicktime Verification Failed
12652 0	Content Type video/sgi Header Check
12652 1	Content Type video/sgi Verification Failed
12653 0	Content Type video/x-avi Header Check
12653 1	Content Type video/x-avi Invalid Message Length



**Table 5-2 Define Content Type Signatures (continued)**

Signature ID	Signature Description
12654 0	Content Type video/x-flv Header Check
12654 1	Content Type video/x-flv Invalid Message Length
12654 2	Content Type video/x-flv Verification Failed
12655 0	Content Type video/x-mng Header Check
12655 1	Content Type video/x-mng Invalid Message Length
12655 2	Content Type video/x-mng Verification Failed
12656 0	Content Type application/x-msvideo Header Check
12656 1	Content Type application/x-msvideo Invalid Message Length
12656 2	Content Type application/x-msvideo Verification Failed
12658 0	Content Type application/ms-word Header Check
12658 1	Content Type application/ms-word Invalid Message Length
12659 0	Content Type application/octet-stream Header Check
12659 1	Content Type application/octet-stream Invalid Message Length
12660 0	Content Type application/postscript Header Check
12660 1	Content Type application/postscript Invalid Message Length
12660 2	Content Type application/postscript Verification Failed
12661 0	Content Type application/vnd.ms-excel Header Check
12661 1	Content Type application/vnd.ms-excel Invalid Message Length
12662 0	Content Type application/vnd.ms-powerpoint Header Check
12662 1	Content Type application/vnd.ms-powerpoint Invalid Message Length
12663 0	Content Type application/zip Header Check
12663 1	Content Type application/zip Invalid Message Length
12663 2	Content Type application/zip Verification Failed
12664 0	Content Type application/x-gzip Header Check
12664 1	Content Type application/x-gzip Invalid Message Length
12664 2	Content Type application/x-gzip Verification Failed
12665 0	Content Type application/x-java-archive Header Check
12665 1	Content Type application/x-java-archive Invalid Message Length
12666 0	Content Type application/x-java-vm Header Check
12666 1	Content Type application/x-java-vm Invalid Message Length
12667 0	Content Type application/pdf Header Check
12667 1	Content Type application/pdf Invalid Message Length
12667 2	Content Type application/pdf Verification Failed
12668 0	Content Type unknown Header Check
12668 1	Content Type unknown Invalid Message Length
12669 0	Content Type image/x-bitmap Header Check
12669 1	Content Type image/x-bitmap Invalid Message Length
12673 0	Recognized content type

**For More Information**

- For the procedure for enabling signatures, see [Enabling and Disabling Signatures, page 5-13](#).
- For the procedure for creating custom define type signatures, see [Configuring Application Policy Signatures, page 5-59](#).

## AIC Transfer Encoding Signatures

There are three policies associated with transfer encoding:

- Associate an action with each method (Define Transfer Encoding)
- List methods recognized by the sensor (Recognized Transfer Encodings)
- Specify which actions need to be taken when a chunked encoding error is seen (Chunked Transfer Encoding Error)

[Table 5-3](#) lists the predefined transfer encoding signatures. Enable the signatures that have the predefined transfer encoding method you need.

**Table 5-3** *Transfer Encoding Signatures*

Signature ID	Transfer Encoding Method
12686	Recognized Transfer Encoding
12687	Define Transfer Encoding Deflate
12688	Define Transfer Encoding Identity
12689	Define Transfer Encoding Compress
12690	Define Transfer Encoding GZIP
12693	Define Transfer Encoding Chunked
12694	Chunked Transfer Encoding Error

### For More Information

For the procedure for enabling signatures, see [Enabling and Disabling Signatures, page 5-13](#).

## AIC FTP Commands Signatures

[Table 5-4](#) lists the predefined FTP commands signatures. Enable the signatures that have the predefined FTP command you need.

**Table 5-4** *FTP Commands Signatures*

Signature ID	FTP Command
12900	Unrecognized FTP command
12901	Define FTP command abor
12902	Define FTP command acct
12903	Define FTP command allo
12904	Define FTP command appe
12905	Define FTP command cdup
12906	Define FTP command cwd
12907	Define FTP command dele
12908	Define FTP command help
12909	Define FTP command list
12910	Define FTP command mkd

**Table 5-4** *FTP Commands Signatures (continued)*

<b>Signature ID</b>	<b>FTP Command</b>
12911	Define FTP command mode
12912	Define FTP command nlst
12913	Define FTP command noop
12914	Define FTP command pass
12915	Define FTP command pasv
12916	Define FTP command port
12917	Define FTP command pwd
12918	Define FTP command quit
12919	Define FTP command rein
12920	Define FTP command rest
12921	Define FTP command retr
12922	Define FTP command rmd
12923	Define FTP command rnfr
12924	Define FTP command rnto
12925	Define FTP command site
12926	Define FTP command smnt
12927	Define FTP command stat
12928	Define FTP command stor
12929	Define FTP command stou
12930	Define FTP command stru
12931	Define FTP command syst
12932	Define FTP command type
12933	Define FTP command user

**For More Information**

For the procedure for enabling signatures, see [Enabling and Disabling Signatures, page 5-13](#).

**Configuring Application Policy****Tip**

A square green icon indicates the default value is being used. Click the green icon to configure that parameter. Click the value field to change the parameter.

**Tip**

A red diamond icon indicates that a user-defined value is being used. Click the icon to change the value back to the default.

To configure the application policy parameters, follow these steps:

- 
- Step 1** Log in to IDM using an account with administrator or operator privileges.
  - Step 2** Choose **Configuration > Policies > Signature Definitions > sig0 > Miscellaneous**.
  - Step 3** In the Enable HTTP field, choose **Yes** from the drop-down list to enable inspection of HTTP traffic.
  - Step 4** In the Max HTTP Requests field, enter the number of outstanding HTTP requests per connection that can be outstanding without having received a response from the server.
  - Step 5** In the AIC Web Ports field, enter the ports that you want to be active.




---

**Note** We recommend that you not configure AIC web ports, but rather use the default web ports.

---

- Step 6** In the Enable FTP field choose **Yes** from the drop-down list to enable inspection of FTP traffic.




---

**Note** If you enable the application policy for HTTP or FTP, the sensor checks to be sure the traffic is compliant with the RFC.

---




---

**Tip** To discard your changes, click **Reset**.

---

- Step 7** Click **Apply** to apply your changes and save the revised configuration.
- 

## Example Recognized Define Content Type (MIME) Signature

The following example demonstrates how to tune an AIC signature, a Recognized Content Type (MIME) signature, specifically, signature 12,623 1 Content Type image/tiff Invalid Message Length.

To tune a MIME-type policy signature, follow these steps:

- 
- Step 1** Log in to IDM using an account with administrator or operator privileges.
  - Step 2** Choose **Configuration > Policies > Signature Definitions > sig0 > Signature Configuration**.
  - Step 3** From the Select By drop-down list, choose **Engine** and then choose **AIC HTTP** as the engine.
  - Step 4** Scroll down the list and select Sig ID 12,623 Subsig ID 1 Content Type image/tiff Invalid Message Length, and click **Edit**.




---

**Tip** You can click the Sig ID column head to have the signature IDs appear in order.

---




---

**Tip** A square green icon indicates the default value is being used. Click the green icon to configure that parameter. Click the value field to change the parameter.

---

**Tip**

A red diamond icon indicates that a user-defined value is being used. Click the icon to change the value back to the default.

**Step 5** Under Status, choose **Yes** from the drop-down list in the Enabled field.

**Step 6** Under Engine, choose one of the options, for example, **Length**, in the Content Type Details field.

**Step 7** In the Length field, make the length smaller by changing the default to 30,000.

**Tip**

To discard your changes and close the Edit Signature dialog box, click **Cancel**.

**Step 8** Click **OK**.

**Tip**

To discard your changes, click **Reset**.

**Step 9** Click **Apply** to save the changes.

## Configuring IP Fragment Reassembly Signatures

This section describes IP fragment reassembly, lists the IP fragment reassembly signatures with their configurable parameters, and describes how to configure them. It contains the following topics:

- [Understanding IP Fragment Reassembly Signatures, page 5-69](#)
- [IP Fragment Reassembly Signatures and Configurable Parameters, page 5-70](#)
- [Configuring the Mode for IP Fragment Reassembly, page 5-71](#)
- [Configuring IP Fragment Reassembly Signatures, page 5-72](#)

## Understanding IP Fragment Reassembly Signatures

You can configure the sensor to reassemble a datagram that has been fragmented over multiple packets. You can specify boundaries that the sensor uses to determine how many datagram fragments it reassembles and how long to wait for more fragments of a datagram. The goal is to ensure that the sensor does not allocate all its resources to datagrams that cannot be completely reassembled, either because the sensor missed some frame transmissions or because an attack has been launched that is based on generating random fragmented datagrams.

You configure the IP fragment reassembly per signature.

### For More Information

- For more information on the Normalizer engine, see [Normalizer Engine, page A-19](#).
- For more information on the AIP SSM and the Normalizer engine, see [Normalizer Engine, page A-19](#).

## IP Fragment Reassembly Signatures and Configurable Parameters

Table 5-5 lists IP fragment reassembly signatures with the parameters that you can configure for IP fragment reassembly. The IP fragment reassembly signatures are part of the Normalizer engine.

**Table 5-5** IP Fragment Reassembly Signatures

Signature ID and Name	Description	Parameter With Default Value and Range	Default Action
1200 IP Fragmentation Buffer Full	Fires when the total number of fragments in the system exceeds the threshold set by Max Fragments.	Specify Max Fragments 10000 (0-42000)	Deny Packet Inline Produce Alert <sup>1</sup>
1201 Fragment Overlap	Fires when the fragments queued for a datagram overlap each other.	None <sup>2</sup>	
1202 Datagram Too Long	Fires when the fragment data (offset and size) exceeds the threshold set with Max Datagram Size.	Specify Max Datagram Size 65536 (2000-65536)	Deny Packet Inline Produce Alert <sup>3</sup>
1203 Fragment Overwrite	Fires when the fragments queued for a datagram overlap each other and the overlapping data is different. <sup>4</sup>	None	Deny Packet Inline Produce Alert <sup>5</sup>
1204 No Initial Fragment	Fires when the datagram is incomplete and missing the initial fragment.	None	Deny Packet Inline Produce Alert <sup>6</sup>
1205 Too Many Datagrams	Fires when the total number of partial datagrams in the system exceeds the threshold set by Max Partial Datagrams.	Specify Max Partial Datagrams 1000 (0-10000)	Deny Packet Inline Produce Alert <sup>7</sup>
1206 Fragment Too Small	Fires when there are more than Max Small Frags of a size less than Min Fragment Size in one datagram. <sup>8</sup>	Specify Max Small Frags 2 (8-1500) Specify Min Fragment Size 400 (1-8)	Deny Packet Inline Produce Alert <sup>9</sup>
1207 Too Many Fragments	Fires when there are more than Max Fragments per Datagram in one datagram.	Specify Max Fragments per Datagram 170 (0-8192)	Deny Packet Inline Produce Alert <sup>10</sup>
1208 Incomplete Datagram	Fires when all of the fragments for a datagram have not arrived during the Fragment Reassembly Timeout. <sup>11</sup>	Specify Fragment Reassembly Timeout 60 (0-360)	Deny Packet Inline Produce Alert <sup>12</sup>
1220 Jolt2 Fragment Reassembly DoS attack	Fires when multiple fragments are received all claiming to be the last fragment of an IP datagram.	Specify Max Last Fragments 4 (1-50)	Deny Packet Inline Produce Alert <sup>13</sup>
1225 Fragment Flags Invalid	Fires when a bad combination of fragment flags is detected.	None <sup>14</sup>	

1. Modify Packet Inline and Deny Connection Inline have no effect on this signature. Deny Packet Inline drops the packets and all associated fragments for this datagram. If you disable this signature, the default values are still used and packets are dropped (inline mode) or not analyzed (promiscuous mode) and no alert is sent.
2. This signature does not fire when the datagram is an exact duplicate. Exact duplicates are dropped in inline mode regardless of the settings. Modify Packet Inline removes the overlapped data from all but one fragment so there is no ambiguity about how the endpoint treats the datagram. Deny Connection Inline has no effect on this signature. Deny Packet Inline drops the packet and all associated fragments for this datagram.

3. Modify Packet Inline and Deny Connection Inline have no effect on this signature. Deny Packet Inline drops the packet and all associated fragments for this datagram. Regardless of the actions set the datagram is not processed by the IPS if the datagram is larger than the Max Datagram size.
4. This is a very unusual event.
5. Modify Packet Inline removes the overlapped data from all but one fragment so there is no ambiguity about how the endpoint treats the datagram. Deny Connection Inline has no effect on this signature. Deny Packet Inline drops the packets and all associated fragments for this datagram.
6. IPS does not inspect a datagram missing the first fragments regardless of the settings. Modify Packet Inline and Deny Connection Inline have no effect on this signature. Deny Packet Inline drops the packet and all associated fragments for this datagram.
7. Modify Packet Inline and Deny Connection Inline have no effect on this signature. Deny Packet Inline drops the packet and all associated fragments for this datagram.
8. IPS does not inspect the datagram if this signature is on and the number of small fragments is exceeded.
9. Modify Packet Inline and Deny Connection Inline have no effect on this signature. Deny Packet Inline drops the packet and all associated fragments for this datagram.
10. Modify Packet Inline and Deny Connection Inline have no effect on this signature. Deny Packet Inline drops the packet and all associated fragments for this datagram.
11. The timer starts when the packet for the datagram arrives.
12. Modify Packet Inline and Deny Connection Inline have no effect on this signature. Deny Packet Inline drops the packet and all associated fragments for this datagram.
13. Modify Packet Inline and Deny Connection Inline have no effect on this signature. Deny Packet Inline drops the packet and all associated fragments for this datagram.
14. Modify Packet Inline modifies the flags to a valid combination. Deny Connection Inline has no effect on this signature. Deny Packet Inline drops the packet and all associated fragments for this datagram.

#### For More Information

For more information on the Normalizer Engine and a list of Normalizer engine signatures with automatic safeguards that you cannot override with configuration settings, see [Normalizer Engine, page A-19](#).

## Configuring the Mode for IP Fragment Reassembly



#### Note

You can configure this option if your sensor is operating in promiscuous mode. If your sensor is operating in line mode, the method is NT only.

To configure the mode the sensor uses for IP fragment reassembly, follow these steps:

**Step 1** Log in to IDM using an account with administrator or operator privileges.

**Step 2** Choose **Configuration > Policies > Signature Definitions > sig0 > Miscellaneous**.



#### Tip

A square green icon indicates the default value is being used. Click the green icon to configure that parameter. Click the value field to change the parameter.



#### Tip

A red diamond icon indicates that a user-defined value is being used. Click the icon to change the value back to the default.

**Step 3** Under Fragment Reassembly, from the IP Reassembly Mode field choose the operating system you want to use to reassemble the fragments.




---

**Tip** To discard your changes, click **Reset**.

---

**Step 4** Click **Apply** to apply your changes and save the revised configuration.

---

## Configuring IP Fragment Reassembly Signatures

The following procedure demonstrates how to tune an IP fragment reassembly signature, specifically, signature 1200 0 IP Fragmentation Buffer Full.

To tune an IP fragment reassembly signature, follow these steps:

- 
- Step 1** Log in to IDM using an account with administrator or operator privileges.
- Step 2** Choose **Configuration > Policies > Signature Definitions > sig0 > Signature Configuration**.
- Step 3** In the Select By field, choose **Engine** from the drop-down list, and then choose **Normalizer** as the engine.
- Step 4** Select the IP fragment reassembly signature you want to configure in the list, for example, Sig ID 1200 Subsig ID 0 IP Fragmentation Buffer Full, and then click **Edit**. The Edit Signature dialog box appears.




---

**Tip** A square green icon indicates the default value is being used. Click the green icon to configure that parameter. Click the value field to change the parameter.

---




---

**Tip** A red diamond icon indicates that a user-defined value is being used. Click the icon to change the value back to the default.

---

- Step 5** Change the default setting of any IP fragment reassembly parameters that can be configured for signature 1200. For example, in the Max Fragments field change the setting from the default of 10000 to 20000.

For signature 1200, you can also change the parameters of these options:

- Specify TCP Idle Timeout
- Specify Service Ports
- Specify SYN Flood Max Embryonic




---

**Tip** To discard your changes, click **Reset**.

---

- Step 6** Click **Apply** to apply your changes and save the revised configuration.
-



## Configuring TCP Stream Reassembly Signatures

This section describes TCP stream reassembly, lists the TCP stream reassembly signatures with the configurable parameters, describes how to configure TCP stream signatures, and how to configure the mode for TCP stream reassembly. It contains the following topics:

- [Understanding TCP Stream Reassembly Signatures, page 5-73](#)
- [TCP Stream Reassembly Signatures and Configurable Parameters, page 5-73](#)
- [Configuring the Mode for TCP Stream Reassembly, page 5-78](#)
- [Configuring TCP Stream Reassembly Signatures, page 5-73](#)

### Understanding TCP Stream Reassembly Signatures

You can configure the sensor to monitor only TCP sessions that have been established by a complete three-way handshake. You can also configure how long to wait for the handshake to complete, and how long to keep monitoring a connection where no more packets have been seen. The goal is to prevent the sensor from creating alerts where a valid TCP session has not been established. There are known attacks against sensors that try to get the sensor to generate alerts by simply replaying pieces of an attack. The TCP session reassembly feature helps to mitigate these types of attacks against the sensor.

You configure TCP stream reassembly parameters per signature. You can configure the mode for TCP stream reassembly.

#### For More Information

- For more information on the Normalizer Engine and a list of Normalizer engine signatures with automatic safeguards that you cannot override with configuration settings, see [Normalizer Engine, page A-19](#).
- For more information on the AIP SSM and the Normalizer engine, see [Normalizer Engine, page A-19](#).

### TCP Stream Reassembly Signatures and Configurable Parameters

[Table 5-6](#) lists TCP stream reassembly signatures with the parameters that you can configure for TCP stream reassembly. TCP stream reassembly signatures are part of the Normalizer engine.

**Table 5-6** TCP Stream Reassembly Signatures

Signature ID and Name	Description	Parameter With Default Value and Range	Default Actions
1301 TCP Session Inactivity Timeout <sup>1</sup>	Fires when a TCP session has been idle for a TCP Idle Timeout.	TCP Idle Timeout 3600 (15-3600)	— <sup>2</sup>
1302 TCP Session Embryonic Timeout <sup>3</sup>	Fires when a TCP session has not completes the three-way handshake in TCP embryonic timeout seconds.	TCP Embryonic Timeout 15 (3-300)	— <sup>4</sup>

Table 5-6 TCP Stream Reassembly Signatures (continued)

Signature ID and Name	Description	Parameter With Default Value and Range	Default Actions
1303 TCP Session Closing Timeout <sup>5</sup>	Fires when a TCP session has not closed completely in TCP Closed Timeout seconds after the first FIN.	TCP Closed Timeout 5 (1-60)	— <sup>6</sup>
1304 TCP Session Packet Queue Overflow	This signature allows for setting the internal TCP Max Queue size value for the Normalizer engine. As a result it does not function in promiscuous mode. By default this signature does not fire an alert. If a custom alert event is associated with this signature and if the queue size is exceeded, an alert fires.  <b>Note</b> The IPS signature team discourages modifying this value.	TCP Max Queue 32 (0-128) TCP Idle Timeout 3600	— <sup>7</sup>
1305 TCP Urg Flag Set <sup>8</sup>	Fires when the TCP urgent flag is seen	TCP Idle Timeout 3600	Modify Packet Inline <sup>9</sup>
1306 0 TCP Option Other	Fires when a TCP option in the range of TCP Option Number is seen. All 1306 signatures fire an alert and do not function in promiscuous mode.	TCP Option Number 6-7,9-255 (Integer Range Allow Multiple 0-255 constraints) TCP Idle Timeout 3600	Modify Packet Inline Produce Alert <sup>10</sup>
1306 1 TCP SACK Allowed Option	Fires when a TCP selective ACK allowed option is seen. All 1306 signatures fire an alert and do not function in promiscuous mode.	TCP Idle Timeout 3600	Modify Packet Inline <sup>11</sup>
1306 2 TCP SACK Data Option	Fires when a TCP selective ACK data option is seen. All 1306 signatures fire an alert and do not function in promiscuous mode.	TCP Idle Timeout 3600	Modify Packet Inline <sup>12</sup>
1306 3 TCP Timestamp Option	Fires when a TCP timestamp option is seen. All 1306 signatures fire an alert and do not function in promiscuous mode.	TCP Idle Timeout 3600	Modify Packet Inline <sup>13</sup>

Table 5-6 TCP Stream Reassembly Signatures (continued)

Signature ID and Name	Description	Parameter With Default Value and Range	Default Actions
1306 4 TCP Window Scale Option	Fires when a TCP window scale option is seen. All 1306 signatures fire an alert and do not function in promiscuous mode.	TCP Idle Timeout 3600	Modify Packet Inline <sup>14</sup>
1306 5 TCP MSS Option	Fires when a TCP MSS option is detected. All 1306 signatures fire an alert and do not function in promiscuous mode.	TCP Idle Timeout 3600	Modify Packet Inline
1306 6 TCP option data after EOL option	Fires when the TCP option list has data after the EOL option. All 1306 signatures fire an alert and do not function in promiscuous mode.	TCP Idle Timeout 3600	Modify Packet Inline
1307 TCP Window Variation	Fires when the right edge of the recv window for TCP moves to the right (decreases).	TCP Idle Timeout 3600	Deny Connection Inline Produce Alert <sup>15</sup>
1308 TTL Evasion <sup>16</sup>	Fires when the TTL seen on one direction of a session is higher than the minimum that has been observed.	TCP Idle Timeout 3600	Modify Packet Inline <sup>17</sup>
1309 TCP Reserved Flags Set	Fires when the reserved bits (including bits used for ECN) are set on the TCP header.	TCP Idle Timeout 3600	Modify Packet Inline Produce Alert <sup>18</sup>
1311 TCP Packet Exceeds MSS	Fires when a packet exceeds the MSS that was exchanged during the three-way handshake.	TCP Idle Timeout 3600	Produce Alert <sup>19</sup>
1312 TCP MSS Below Minimum	Fires when the MSS value in a packet containing a SYN flag is less than TCP Min MSS.	TCP Min MSS 400 (0-16000) TCP Idle Timeout 3600	Modify Packet Inline <sup>20</sup>
1313 TCP Max MSS	Fires when the MSS value in a packet containing a SYN flag exceed TCP Max MSS	TCP Max MSS1460 (0-16000)	Modify Packet Inline disabled <sup>21</sup>
1314 TCP Data SYN	Fires when TCP payload is sent in the SYN packet.	—	Deny Packet Inline disabled <sup>22</sup>
1315 ACK Without TCP Stream	Fires when an ACK packet is sent that does not belong to a stream.	—	Produce Alert disabled <sup>23</sup>

Table 5-6 TCP Stream Reassembly Signatures (continued)

Signature ID and Name	Description	Parameter With Default Value and Range	Default Actions
1317 Zero Window Probe	Fires when a zero window probe packet is detected.	Modify Packet Inline removes data from the Zero Window Probe packet.	Modify Packet Inline
1330 <sup>24</sup> 0 TCP Drop - Bad Checksum	Fires when TCP packet has bad checksum.	Modify Packet Inline corrects the checksum.	Deny Packet Inline
1330 1 TCP Drop - Bad TCP Flags	Fires when TCP packet has bad flag combination.	—	Deny Packet Inline
1330 2 TCP Drop - Urgent Pointer With No Flag	Fires when TCP packet has a URG pointer and no URG flag.	Modify Packet Inline clears the pointer.	Modify Packet Inline disabled
1330 3 TCP Drop - Bad Option List	Fires when TCP packet has a bad option list.	—	Deny Packet Inline
1330 4 TCP Drop - Bad Option Length	Fires when TCP packet has a bad option length.	—	Deny Packet Inline
1330 5 TCP Drop - MSS Option Without SYN	Fires when TCP MSS option is seen in packet without the SYN flag set.	Modify Packet Inline clears the MSS option.	Modify Packet Inline
1330 6 TCP Drop - WinScale Option Without SYN	Fires when TCP window scale option is seen in packet without the SYN flag set.	Modify Packet Inline clears the window scale option.	Modify Packet Inline
1330 7 TCP Drop - Bad WinScale Option Value	Fires when a TCP packet has a bad window scale value.	Modify Packet Inline sets the value to the closest constraint value.	Modify Packet Inline
1330 8 TCP Drop - SACK Allow Without SYN	Fires when the TCP SACK allowed option is seen in a packet without the SYN flags set.	Modify Packet Inline clears the SACK allowed option.	Modify Packet Inline
1330 9 TCP Drop - Data in SYN/ACK	Fires when TCP packet with SYN and ACK flags set also contains data.	—	Deny Packet Inline
1330 10 TCP Drop - Data Past FIN	Fires when TCP data is sequenced after FIN.	—	Deny Packet Inline
1330 11 TCP Drop - Timestamp not Allowed	Fires when TCP packet has timestamp option when timestamp option is not allowed.	—	Deny Packet Inline
1330 12 TCP Drop - Segment Out of Order	Fires when TCP segment is out of order and cannot be queued.	—	Deny Packet Inline
1330 13 TCP Drop - Invalid TCP Packet	Fires when TCP packet has invalid header.	—	Deny Packet Inline

Table 5-6 TCP Stream Reassembly Signatures (continued)

Signature ID and Name	Description	Parameter With Default Value and Range	Default Actions
1330 14 TCP Drop - RST or SYN in window	Fires when TCP packet with RST or SYN flag was sent in the sequence window but was not the next sequence.	—	Deny Packet Inline
1330 15 TCP Drop - Segment Already ACKed	Fires when TCP packet sequence is already ACKed by peer (excluding keepalives).	—	Deny Packet Inline
1330 16 TCP Drop - PAWS Failed	Fires when TCP packet fails PAWS check.	—	Deny Packet Inline
1330 17 TCP Drop - Segment out of State Order	Fires when TCP packet is not proper for the TCP session state.	—	Deny Packet Inline
1330 18 TCP Drop - Segment out of Window	Fires when TCP packet sequence number is outside of allowed window.	—	Deny Packet Inline
3050 Half Open SYN Attack		syn-flood-max-embryonic 5000	
3250 TCP Hijack		max-old-ack 200	
3251 TCP Hijack Simplex Mode		max-old-ack 100	

- The timer is reset to 0 after each packet on the TCP session. By default, this signature does not produce an alert. You can choose to produce alerts for expiring TCP connections if desired. A statistic of total number of expired flows is updated any time a flow expires.
- Modify Packet Inline, Deny Connection Inline, and Deny Packet Inline have no effect on this signature.
- The timer starts with the first SYN packet and is not reset. State for the session is reset and any subsequent packets for this flow appear to be out of order (unless it is a SYN).
- Modify Packet Inline, Deny Connection Inline, and Deny Packet Inline have no effect on this signature.
- The timer starts with the first FIN packet and is not reset. State for the session is reset and any subsequent packets for this flow appear to be out of order (unless it is a SYN).
- Modify Packet Inline, Deny Connection Inline, and Deny Packet Inline have no effect on this signature.
- Modify Packet Inline and Deny Packet Inline have no effect on this signature. Deny Connection Inline drops the current packet and the TCP session.
- Phrak 57 describes a way to evade security policy using URG pointers. You can normalize the packet when it is in inline mode with this signature.
- Modify Packet Inline strips the URG flag and zeros the URG pointer from the packet. Deny Connection Inline drops the current packet and the TCP session. Deny Packet Inline drops the packet.
- Modify Packet Inline strips the selected option(s) from the packet. Deny Connection Inline drops the current packet and the TCP session. Deny Packet Inline drops the packet.
- Modify Packet Inline strips the selected ACK allowed option from the packet. Deny Connection Inline drops the current packet and the TCP session. Deny Packet Inline drops the packet.
- Modify Packet Inline strips the selected ACK allowed option from the packet. Deny Connection Inline drops the current packet and the TCP session. Deny Packet Inline drops the packet.
- Modify Packet Inline strips the timestamp option from the packet. Deny Connection Inline drops the current packet and the TCP session. Deny Packet Inline drops the packet.
- Modify Packet Inline strips the window scale option from the packet. Deny Connection Inline drops the current packet and the TCP session. Deny Packet Inline drops the packet.
- Modify Packet Inline has no effect on this signature. Deny Connection Inline drops the current packet and the TCP connection. Deny Packet Inline drops the packet.

16. This signature is used to cause TTLs to monotonically decrease for each direction on a session. For example, if TTL 45 is the lowest TTL seen from A to B, then all future packets from A to B will have a maximum of 45 if Modify Packet Inline is set. Each new low TTL becomes the new maximum for packets on that session.
17. Modify Packet Inline ensures that the IP TTL monotonically decreases. Deny Connection Inline drops the current packet and the TCP session. Deny Packet Inline drops the packet.
18. Modify Packet Inline clears all reserved TCP flags. Deny Connection Inline drops the current packet and the TCP session. Deny Packet Inline drops the packet.
19. Modify Packet Inline has no effect on this signature. Deny Connection Inline drops the current packet and the TCP connection. Deny Packet Inline drops the packet.
20. 2.4.21-15.EL.cisco.1 Modify Packet Inline raises the MSS value to TCP Min MSS. Deny Connection Inline drops the current packet and the TCP session. Deny Packet Inline drops the packet 2.4.21-15.EL.cisco.1.
21. Modify Packet Inline lowers the MSS value to TCP Max MSS. Deny Connection Inline drops the current packet and the TCP session. Deny Packet Inline drops the packet 2.4.21-15.EL.cisco.1.
22. Modify Packet Inline has no effect on this signature. Deny Connection Inline drops the current packet and the TCP session. Deny Packet Inline drops the packet.
23. Modify Packet Inline, Deny Connection Inline, and Deny Packet Inline have no effect on this signature. By default, the 1330 signatures drop packets for which this signature sends alerts.
24. These subsignatures represent the reasons why the Normalizer might drop a TCP packet. By default these subsignatures drop packets. These subsignatures let you permit packets that fail the checks in the Normalizer through the IPS. The drop reasons have an entry in the TCP statistics. By default these subsignatures do not produce an alert.

## Configuring the Mode for TCP Stream Reassembly



### Note

The parameters TCP Handshake Required and TCP Reassembly Mode only impact sensors inspecting traffic in promiscuous mode, not inline mode. To configure asymmetric options for sensors inspecting inline traffic, use the Normalizer Mode parameter.

To configure the TCP stream reassembly mode, follow these steps:

**Step 1** Log in to IDM using an account with administrator or operator privileges.

**Step 2** Choose **Configuration > Policies > Signature Definitions > sig0 > Miscellaneous**.



### Tip

A square green icon indicates the default value is being used. Click the green icon to configure that parameter. Click the value field to change the parameter.



### Tip

A red diamond icon indicates that a user-defined value is being used. Click the icon to change the value back to the default.

**Step 3** Under Stream Reassembly, in TCP Handshake Required field, choose **Yes**. Choosing TCP Handshake Required specifies that the sensor should only track sessions for which the three-way handshake is completed.

**Step 4** In the TCP Reassembly Mode field, from the drop-down list, choose the mode the sensor should use to reassemble TCP sessions:

- **Asymmetric**—Lets the sensor synchronize state with the flow and maintain inspection for those engines that do not require both directions.
- **Strict**—If a packet is missed for any reason, all packets after the missed packet are processed.
- **Loose**—Use in environments where packets might be dropped.



**Tip** To discard your changes, click **Reset**.

**Step 5** Click **Apply** to apply your changes and save the revised configuration.

#### For More Information

For information on asymmetric inspection options for sensors configured in inline mode, see [Inline TCP Session Tracking Mode, page 4-3](#) and [Adding, Editing, and Deleting Virtual Sensors, page 4-5](#).

## Configuring TCP Stream Reassembly Signatures

The following procedure demonstrates how to tune a TCP stream reassembly signatures, for example, signature 1313 0 TCP MSS Exceeds Maximum.



#### Caution

For signature 3050 Half Open SYN Attack, if you choose modify packet inline as the action, you can see as much as 20 to 30% performance degradation while the protection is active. The protection is only active during an actual SYN flood.

To tune a TCP stream reassembly signature, follow these steps:

- Step 1** Log in to IDM using an account with administrator or operator privileges.
- Step 2** Choose **Configuration > Policies > Signature Definitions > sig0 > Signature Configuration**.
- Step 3** From the Select By drop-down list, choose **Engine** and then choose **Normalizer**.
- Step 4** Select the TCP fragment reassembly signature you want to configure in the list, for example, Sig ID 1313 Subsig ID 0 TCP MSS Exceeds Maximum, and click **Edit**.



**Tip** A square green icon indicates the default value is being used. Click the green icon to configure that parameter. Click the value field to change the parameter.



**Tip** A red diamond icon indicates that a user-defined value is being used. Click the icon to change the value back to the default.

- Step 5** Change the default setting of any configurable IP fragment reassembly parameters for signature 1313. For example, in the TCP Max MSS field, change the setting from the default of 1460 to 1380.



**Note** Changing this parameter from the default of 1460 to 1380 helps prevent fragmentation of traffic going through a VPN tunnel.

For signature 1313 0, you can also change the parameters of these options:

- Specify Hijack Max Old Ack
- Specify TCP Idle Timeout
- Specify Service Ports

- Specify SYN Flood Max Embryonic

**Tip**

To discard your changes, click **Reset**.

**Step 6** Click **Apply** to apply your changes and save the revised configuration.

## Configuring IP Logging

You can configure a sensor to generate an IP session log when the sensor detects an attack. When IP logging is configured as a response action for a signature and the signature is triggered, all packets to and from the source address of the alert are logged for a specified period of time.

**Note**

IP logging allows a maximum limit of 20 concurrent IP log files. Once the limit of 20 is reached, you receive the following message in main.log: `Cid/W errWarnIpLogProcessor::addIpLog: Ran out of file descriptors.`

**Tip**

A square green icon indicates the default value is being used. Click the green icon to configure that parameter. Click the value field to change the parameter. A red diamond icon indicates that a user-defined value is being used. Click the icon to change the value back to the default.

**Note**

When the sensor meets any one of the IP logging conditions, it stops IP logging.

To configure IP logging parameters, follow these steps:

- Step 1** Log in to IDM using an account with administrator or operator privileges.
- Step 2** Choose **Configuration > Policies > Signature Definitions > sig0 > Miscellaneous**.
- Step 3** Under IP Log in the Max IP Log Packets field, enter the number of packets you want logged.
- Step 4** In the IP Log Time field, enter the duration you want the sensor to log. A valid value is 1 to 60 minutes. The default is 30 minutes.
- Step 5** In the Max IP Log Bytes field, enter the maximum number of bytes you want logged.

**Tip**

To discard your changes, click **Reset**.

**Step 6** Click **Apply** to apply your changes and save the revised configuration.