



CHAPTER 6

Creating Custom Signatures

This chapter explains how to use the Custom Signature wizard to create custom signatures. For more information on the individual signature engines, see [Appendix B, “Signature Engines.”](#)

This chapter contains the following sections:

- [About Custom Signature Wizard, page 6-1](#)
- [Supported User Role, page 6-4](#)
- [Field Definitions, page 6-4](#)
- [Creating Custom Signatures, page 6-22](#)

About Custom Signature Wizard

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 5.1 does not support creating custom signatures based on the following signature engines:

- AIC FTP
- AIC HTTP
- Atomic ARP
- Flood Host
- Flood Net
- Meta
- Multi String
- Normalizer
- Service DNS
- Service FTP
- Service Generic
- Service H224
- Service IDENT
- Service MSSQL

- Service NTP
- Service SMB
- Service SNMP
- Service SSH
- Sweep TCP Other

To create custom signatures based on these existing signature engines, clone an existing signature from the engine you want by choosing Configuration > Signature Configuration > Clone. For more information, see [Cloning Signatures, page 5-19](#).

For more information on using the CLI to create custom signatures using these signature engines, refer to [Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1](#).

This section contains the following topics:

- [Using a Signature Engine, page 6-2](#)
- [Not Using a Signature Engine, page 6-3](#)

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 identifiers:

- 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 or change it by clicking **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** Click the **No** radio button in the Welcome window.
- Step 2** Choose the protocol you want to use:
- IP—Go to Step 4.
 - ICMP—Go to Step 3.
 - UDP—Go to Step 3.
 - TCP—Go to Step 3.
- Step 3** For ICMP and UDP protocols, choose the traffic type and inspect data type. For TCP protocol, choose the traffic type.
- Step 4** Assign the signature identifiers:
- Signature ID
 - SubSignature ID
 - Signature Name
 - Alert Notes (optional)
 - User Comments (optional)
- Step 5** 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 6** Assign the alert response:
- Signature Fidelity Rating
 - Severity of the alert
- Step 7** Assign the alert behavior.
- You can accept the default alert behavior or change it by clicking **Advanced**, which opens the Advanced Alert Behavior wizard. With this wizard you can configure how you want to handle alerts for this signature.
- Step 8** Click **Finish**.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator or Operator to create custom signatures.

Field Definitions

The following section describes the Custom Signature wizard field definitions window by window. It contains the following topics:

- [Welcome Field Definitions, page 6-5](#)
- [Protocol Type Field Definitions, page 6-5](#)
- [Signature Identification Field Definitions, page 6-6](#)
- [Atomic IP Engine Parameters Field Definitions, page 6-6](#)
- [Service HTTP Engine Parameters Field Definitions, page 6-8](#)
- [Service MSRPC Engine Parameters Field Definitions, page 6-9](#)
- [Service RPC Engine Parameters Field Definitions, page 6-9](#)
- [State Engine Parameters Field Definitions, page 6-10](#)
- [String ICMP Engine Parameters Field Definitions, page 6-11](#)
- [String TCP Engine Parameters Field Definitions, page 6-12](#)
- [String UDP Engine Parameters Field Definitions, page 6-13](#)
- [Sweep Engine Parameters Field Definitions, page 6-14](#)
- [ICMP Traffic Type Field Definitions, page 6-14](#)
- [UDP Traffic Type Field Definitions, page 6-15](#)
- [TCP Traffic Type Field Definitions, page 6-15](#)
- [UDP Sweep Type Field Definitions, page 6-16](#)
- [TCP Sweep Type Field Definitions, page 6-16](#)
- [Service Type Field Definitions, page 6-16](#)
- [Inspect Data Field Definitions, page 6-17](#)
- [Alert Response Field Definitions, page 6-17](#)
- [Alert Behavior Field Definitions, page 6-18](#)
- [Advanced Alert Behavior Wizard, page 6-18](#)

Welcome Field Definitions

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

Field Descriptions:

- 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 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.

Button Functions:

- 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.

Protocol Type Field Definitions

You can define a signature that looks for malicious behavior in a certain protocol. You can have the following protocols decoded and inspected by your signature:

- IP
- ICMP
- UDP
- TCP

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

Field Descriptions:

- 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.

Button Functions:

- 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.

Signature Identification Field Definitions

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

Field Descriptions:

- 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.
A subsignature ID is used to identify 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.

Button Functions:

- 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.

Atomic IP Engine Parameters Field Definitions

The following fields and buttons 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.

Field Descriptions:

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



Tip To choose 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 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 Total IP Length**—(Optional) Lets you specify the total IP length.
- **Specify IP Option Inspection Options**—(Optional) Lets you specify the IP inspection options.

Choose 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.
 - **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.

Button Functions:

- **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.

Service HTTP Engine Parameters Field Definitions

The following fields and buttons 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.

Field Descriptions:

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



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

- De Obfuscate—Specifies whether or not to apply anti-evasive HTTP deobfuscation before searching.

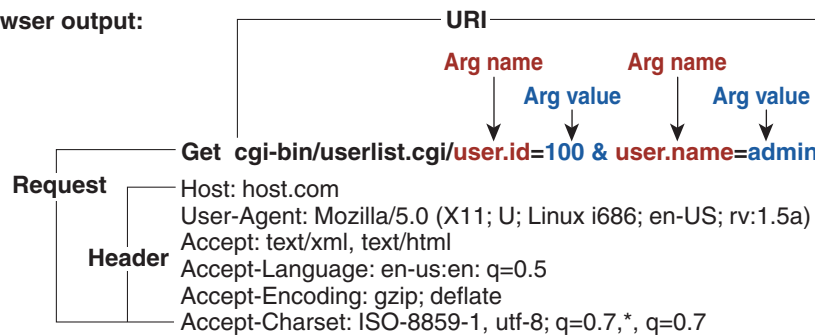
The default is Yes.

- 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.

Button Functions:

- 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.

Service MSRPC Engine Parameters Field Definitions

The following fields and buttons 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.

Field Descriptions:

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



Tip To choose 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.

Button Functions:

- **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.

Service RPC Engine Parameters Field Definitions

The following fields and buttons 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 choose 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 comma-separated list of ports or port ranges.
- 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 Spool 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 alarm. 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.

Button Functions:

- 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.

State Engine Parameters Field Definitions

The following fields and buttons 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.

Field Descriptions:

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



Tip To choose 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.
- 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.
The valid range is 0 to 65535.
If you choose No, you can set the minimum and maximum match offset.
The valid range is 1 to 65535.

Button Functions:

- 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.

String ICMP Engine Parameters Field Definitions

The following fields and buttons 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.

Field Descriptions:

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



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

The valid range for the maximum match offset is 1 to 65535. The valid range for the minimum match offset is 0 to 65535.

Button Functions:

- 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.

String TCP Engine Parameters Field Definitions

The following fields and buttons 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.

Field Descriptions:

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



Tip To choose 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 No, you can set the minimum and maximum match offset. The valid range for the maximum match offset is 1 to 65535. The valid range for the minimum match offset is 0 to 65535.

- 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.

Button Functions:

- 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.

String UDP Engine Parameters Field Definitions

The following fields and buttons 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.

Field Descriptions:

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

The default is Produce Alert.



Tip To choose 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.

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

The valid range is 0 to 65535.

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

The valid range is 1 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.

Button Functions:

- 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.

Sweep Engine Parameters Field Definitions

The following fields and buttons 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.

Field Descriptions:

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



Tip To choose 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
- 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.

Button Functions:

- 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.

ICMP Traffic Type Field Definitions

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

Field Descriptions:

- 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.

Button Functions:

- 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.

UDP Traffic Type Field Definitions

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

Field Descriptions:

- 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.

Button Functions:

- 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.

TCP Traffic Type Field Definitions

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

Field Descriptions:

- 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.

Button Functions:

- 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.

UDP Sweep Type Field Definitions

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

Field Descriptions:

- 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.

Button Functions:

- 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.

TCP Sweep Type Field Definitions

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

Field Descriptions:

- 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.

Button Functions:

- 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.

Service Type Field Definitions

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

Field Descriptions:

- 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.

Button Functions:

- 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.

Inspect Data Field Definitions

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

Field Descriptions:

- 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.

Button Functions:

- 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.

Alert Response Field Definitions

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

Field Descriptions:

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

SFR 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 SFR 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.

Button Functions:

- 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.

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 6-18](#)
- [Alert Summarization Field Definitions, page 6-19](#)
- [Alert Dynamic Response Summary Field Definitions, page 6-19](#)
- [Alert Dynamic Response Fire All Field Definitions, page 6-20](#)
- [Alert Dynamic Response Fire Once Field Definitions, page 6-21](#)
- [Global Summarization Field Definitions, page 6-21](#)

Event Count and Interval Field Definitions

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

Field Descriptions:

- **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, choose 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 each other.
- **Event Interval (seconds)**—Identifies the time interval during which the sensor counts events for rate-based counting.

Button Functions:

- Back—Returns you to the previous window in the Alert Behavior wizard.
- Next—Advances you to the next window in the Alert Behavior wizard.
- Finish—Completes the Alert Behavior wizard and saves the signature you created.
- Cancel—Exits the Alert Behavior wizard.
- Help—Displays the help topic for this feature.

Alert Summarization Field Definitions

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

Field Descriptions:

- 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.

Button Functions:

- Back—Returns you to the previous window in the Alert Behavior wizard.
- Next—Advances you to the next window in the Alert Behavior wizard.
- Finish—Completes the Alert Behavior wizard and saves the signature you created.
- Cancel—Exits the Alert Behavior wizard.
- Help—Displays the help topic for this feature.

Alert Dynamic Response Summary Field Definitions

The following fields and buttons are found in the Alert Dynamic Response Summary window of the Advanced Alert Behavior wizard.

Field Descriptions:

- 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, choose 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.

Button Functions:

- Back—Returns you to the previous window in the Alert Behavior wizard.
- Next—Advances you to the next window in the Alert Behavior wizard.
- Finish—Completes the Alert Behavior wizard and saves the signature you created.
- Cancel—Exits the Alert Behavior wizard.
- Help—Displays the help topic for this feature.

Alert Dynamic Response Fire All Field Definitions

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

Field Descriptions:

- Use Dynamic Summarization—Lets the sensor dynamically adjust the volume of alerts it sends based on the summary parameters you configure.
- Summary Threshold—Identifies the minimum number of hits the sensor must receive before sending a summary alert for this signature.
- 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.
- 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.

- Specify Global Summary Threshold—Lets the sensor dynamically enter global 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.

- Global Summary Threshold—Identifies the minimum number of hits the sensor must receive before sending a global summary alert.

Button Functions:

- Back—Returns you to the previous window in the Alert Behavior wizard.
- Next—Advances you to the next window in the Alert Behavior wizard.

- **Finish**—Completes the Alert Behavior wizard and saves the signature you created.
- **Cancel**—Exits the Alert Behavior wizard.
- **Help**—Displays the help topic for this feature.

Alert Dynamic Response Fire Once Field Definitions

The following fields and buttons are found in the Alert Dynamic Response window of the Advanced Alert Behavior wizard when you chose 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, choose 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.

Button Functions:

- **Back**—Returns you to the previous window in the Alert Behavior wizard.
- **Next**—Advances you to the next window in the Alert Behavior wizard.
- **Finish**—Completes the Alert Behavior wizard and saves the signature you created.
- **Cancel**—Exits the Alert Behavior wizard.
- **Help**—Displays the help topic for this feature.

Global Summarization Field Definitions

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

Field Descriptions:

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

Button Functions:

- **Back**—Returns you to the previous window in the Alert Behavior wizard.
- **Next**—Advances you to the next window in the Alert Behavior wizard.
- **Finish**—Completes the Alert Behavior wizard and saves the signature you created.
- **Cancel**—Exits the Alert Behavior wizard.
- **Help**—Displays the help topic for this feature.

Creating Custom Signatures

This section provides examples of custom signatures. It contains the following topics:

- [Signature Engines Not Supported in the Custom Signature Wizard, page 6-22](#)
- [Master Custom Signature Procedure, page 6-23](#)
- [Example String TCP Signature, page 6-28](#)
- [Example Service HTTP Signature, page 6-33](#)

Signature Engines Not Supported in the Custom Signature Wizard

The Custom Signature wizard in IPS 5.1 does not support creating custom signatures based on the following signature engines:

- AIC FTP
- AIC HTTP
- Atomic ARP
- Flood Host
- Flood Net
- Meta
- Multi String
- Normalizer
- Service DNS
- Service FTP
- Service Generic
- Service H224
- Service IDENT
- Service MSSQL
- Service NTP
- Service SMB
- Service SNMP
- Service SSH
- Sweep TCP Other

To create custom signatures based on these existing signature engines, clone an existing signature from the engine you want by choosing Configuration > Signature Configuration > Clone. For more information, see [Cloning Signatures, page 5-19](#).

For more information on using the CLI to create custom signatures using these signature engines, refer to [Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1](#).

Master Custom Signature Procedure

The Custom Signature wizard provides a step-by-step procedure for configuring custom signatures. For more information on the individual signature engines, see [Appendix B, “Signature Engines.”](#)

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 > Signature Definition > 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**.

The Welcome window appears.

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 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**.

The Protocol Type window appears.

Step 5 Choose the protocol that best matches the type of traffic you want this signature to inspect and then click **Next**:

- IP (If you choose IP, go to Step 13.)
- ICMP (If you choose ICMP, go to Step 6.)
- UDP (If you choose UDP, go to Step 7.)
- TCP (If you choose TCP, go to Step 9.)

Step 6 In the ICMP Traffic Type window, choose one of the following options, 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, choose one of the following options, 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, choose one of the following options, 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, choose one of the following options, 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, choose one of the following options, 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, choose one of the following options, 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 For a single packet, choose one of the following inspection options:

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

- a. Type a number in the Signature ID field.

Custom signatures are in the range of 60000 to 65000.

- b. Type a number in the SubSignature ID field.

The default is 0.

You can assign a subsignature ID if you are grouping signatures together that are similar.

- c. Type a name in the Signature Name field.

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 are reported to the event viewer when an alert is generated.

- d. (Optional) Type text in the Alert Notes field

You can add text to be included in alarms associated with this signature. These notes are reported to the event viewer when an alert is generated.

- e. (Optional) Type text in the User Comments field.

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 + icon indicates that more parameters are available for this signature. Click the + icon to expand the section and view the remaining parameters.

**Tip**

A green icon indicates that the parameter is using the default value. Click the green icon to activate the parameter field and edit the value.

Step 15 Specify the following alert response options:

- a. Specify a value in the Signature Fidelity Rating field.

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

- b. Choose the severity to be reported by the event viewer when the sensor sends an alert:

- High
- Informational
- Low
- Medium

Step 16 To change the default alert behavior, click **Advanced**.

The Advanced Alert Behavior wizard Event Count and Interval window appears.

**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 into 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. Type a value for the event count in the Event Count field.

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

- b. 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 Use Event Interval and then specify 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, choose one of the following options:

- 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.
Go to Step 22.

Step 19 To configure the Alert Every Time the Signature Fires:

- a. **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. **Use Dynamic Summarization**
Lets the sensor dynamically adjust the volume of alerts it sends based on the summary parameters you configure.
- c. **Summary Threshold**
Identifies the minimum number of hits the sensor must receive before sending a summary alert for this signature.
- d. **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.
- e. **Specify Global Summary Threshold**
Lets the sensor dynamically enter global summarization mode.
- f. **Global Summary Threshold**
Identifies the minimum number of hits the sensor must receive before sending a global summary alert.

Step 20 To configure Alert the First Time the Signature Fires:

- a. **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. **Use Dynamic Global Summarization**
Lets the sensor dynamically enter global summarization mode.

c. 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.

d. Global Summary Interval (seconds)

Identifies the time interval during which the sensor counts events for summarization

Step 21 To configure Send Summary Alerts, choose one of the following options

a. Summary Interval (seconds)

Identifies the time interval during which the sensor counts events for summarization.

b. 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. Use Dynamic Global Summarization

Lets the sensor dynamically enter global summarization mode.

d. 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.

Step 22 To configure Global Summarization, specify the time interval during which the sensor should count events for summarization

Step 23 Click **Next** to continue.

Step 24 Click **Finish** to save your changes.

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.

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

**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 > Signature Definition > 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**.
The Welcome window appears.
- Step 4** Click the **Yes** radio button, choose String TCP from the Select Engine 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**:
- a. Type a number in the Signature ID field.
Custom signatures range from 60000 to 65000.
 - b. Type a number in the SubSignature ID field.
The default is 0.
You can assign a subsignature ID if you are grouping signatures together that are similar.
 - c. Type a name in the Signature Name field.
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 are reported to the Event Viewer when an alert is generated.

- d. (Optional) Type text in the Alert Notes field
You can add text to be included in alarms associated with this signature. These notes are reported to the event viewer when an alert is generated. The default is My Sig Info.
- e. (Optional) Type text in the User Comments field.
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**.
The Engine Specific Parameters window appears.

**Tip**

A + icon indicates that more options are available for this parameter. Click the + icon to expand the section and view the remaining parameters.

**Tip**

A green icon indicates that the parameter is using the default value. Click the green icon to change it to red, which activates the parameter field so you can edit the value.

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

Step 7 Click the green icon next to Direction and 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 8 In the Regexp String field specify the string this signature will be looking for in the TCP packet.**Step 9** In the Service Ports field, specify the port, for example, 23.

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

Step 10 (Optional) You can configure the following optional parameters for this signature:

- Specify Exact Match Offset—Enables exact match offset, the exact stream offset the regular expression string must report for a match to be valid (0 to 65535).
- Specify Min Match Length—Enables minimum match length, the minimum number of bytes the regular expression string must match (0 to 65535).
- Strip Telnet Options—Strips the Telnet option characters from the data before the pattern is searched.
- Swap Attacker Victim—Swaps the address (and ports) source and destination in the alert message.

Step 11 Click **Next**.

The Alert Response window appears.

Step 12 Change the following default alert response options if desired:**a.** Specify a value in the Signature Fidelity Rating field.

The SFR 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. Choose the severity to be reported by the event viewer when the sensor sends an alert. The default is Medium.

- High
- Informational
- Low
- Medium

Step 13 Click **Next**.

The Alert Behavior window appears.

Step 14 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 15 through 21. Otherwise click **Finish** and your custom signature is created.



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 into 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 15 Configure the event count, key, and interval:

- a. Type a value for the event count in the Event Count field.

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

- b. 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 Use Event Interval and then specify the number of seconds that you want to use for your interval.

- d. Click **Next** to continue.

The Alert Summarization window appears.

Step 16 To control the volume of alerts and to configure how the sensor summarizes alerts, choose one of the following options and then click **Next**:

- 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 17a.

- 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 17b.

- 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 17c.

- 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.

Go to Step 17d.

The Alert Dynamic Response window appears.

Step 17 Configure the alert dynamic response:

- a. To configure the Alert Every Time the Signature Fires, choose one of the following options:

- 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.

- Use Dynamic Summarization

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

- Summary Threshold

Identifies the minimum number of hits the sensor must receive before sending a summary alert for this signature.

- 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 Global Summary Threshold

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.

- b. To configure Alert the First Time the Signature Fires, choose one of the following options:

- 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.

- 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

- c. To configure Send Summary Alerts, choose one of the following options
 - 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, choose 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 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.
- d. To configure Global Summarization, specify the time interval during which the sensor should count events for summarization

Step 18 Click **Finish** to save your changes.

The Alert Behavior window appears.

Step 19 Click **Finish**.

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

Step 20 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.

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 today's networks. In addition, it requires the most amount of preprocessing time and has the most number of signatures requiring inspection making it critical to the system's overall performance.

The Service HTTP engine uses a Regex library that can combine multiple patterns into 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. For more information on the Service HTTP engine, see [Service HTTP Engine, page B-23](#).

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 > Signature Definition > 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**.

The Welcome window appears.

Step 4 Click the **Yes** radio button, choose Service HTTP from the Select Engine 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**:

- a. Type a number in the Signature ID field.

Custom signatures range from 60000 to 65000.

- b. Type a number in the SubSignature ID field.

The default is 0.

You can assign a subsignature ID if you are grouping signatures together that are similar.

- c. Type a name in the Signature Name field.

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 are reported to the event viewer when an alert is generated.

- d. (Optional) Type text in the Alert Notes field

You can add text to be included in alarms associated with this signature. These notes are reported to the event viewer when an alert is generated. The default is My Sig Info.

- e. (Optional) Type text in the User Comments field.

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**.

The Engine Specific Parameters window appears.

**Tip**

A + icon indicates that more options are available for this parameter. Click the + icon to expand the section and view the remaining parameters.

**Tip**

A green icon indicates that the parameter is using the default value. Click the green icon to change it to red, which activates the parameter field so you can edit the value.

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

Step 7 Click the green icon next to De Obfuscate and choose Yes 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. Choose Yes for Specify URI Regex.
- b. Specify the URI Regex in the URI Regex field, 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, specify the port, for example, use the web ports variable, \$WEBPORTS. Service Ports 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) Change the following default alert response options:

- a. Specify a value in the Signature Fidelity Rating field.

The SFR 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. Choose the severity to be reported by the event viewer when the sensor sends an alert. The default is Medium.
 - High
 - Informational
 - Low
 - Medium

Step 14 Click **Next**.

The Alert Behavior window appears.

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 15 through 21. Otherwise click **Finish** and your custom signature is created.



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 into 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 16 Configure the event count, key, and interval:

- a. Type a value for the event count in the Event Count field.

This is the minimum number of hits the sensor must receive before sending one alert for this signature.
- b. 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 Use Event Interval and then specify the number of seconds that you want to use for your interval.
- d. Click **Next** to continue.

The Alert Summarization window appears.

Step 17 To control the volume of alerts and to configure how the sensor summarizes alerts, choose one of the following options and then click **Next**:

- 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 17a.
- 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 17b.

- 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 17c.

- 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.

Go to Step 17d.

The Alert Dynamic Response window appears.

Step 18 Configure the alert dynamic response:

a. To configure the Alert Every Time the Signature Fires, choose one of the following options:

- 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.

- Use Dynamic Summarization

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

- Summary Threshold

Identifies the minimum number of hits the sensor must receive before sending a summary alert for this signature.

- 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 Global Summary Threshold

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.

b. To configure Alert the First Time the Signature Fires, choose one of the following options:

- 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.

- 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

- c. To configure Send Summary Alerts, choose one of the following options

- 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, choose 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 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.

- d. To configure Global Summarization, specify the time interval during which the sensor should count events for summarization

Step 19 Click **Finish** to save your changes.

The Alert Behavior window appears.

Step 20 Click **Finish**.

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

Step 21 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.