Defining IPS Signatures

You can use Security Manager to configure IPS signatures for dedicated IPS appliances and service modules or Cisco IOS IPS devices. When configuring signatures for Cisco IOS IPS, keep in mind that the router cannot use as many signatures as a dedicated appliance or service module.

This chapter contains the following topics:
- Understanding Signatures, page 35-1
- Configuring Signatures, page 35-3
- Configuring Signature Settings, page 35-26

Understanding Signatures

Network intrusions are attacks on, or other misuses of, network resources. Cisco IPS sensors and Cisco IOS IPS devices use a signature-based technology to detect network intrusions. A signature specifies the types of network intrusions that you want the sensor to detect and report. As sensors scan network packets, they use signatures to detect known types of attacks, such as denial of service (DoS) attacks, and respond with actions that you define.

On a basic level, signature-based intrusion detection technology can be compared to virus-checking programs. Cisco IPS contains a set of signatures that the sensor compares with network activity. When a match is found, the sensor takes some action, such as logging the event or sending an alarm to the Security Manager Event Viewer.

Signatures can produce false positives, because certain normal network activity can be construed as malicious. 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 editing your signature parameters (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 such as Event Viewer. By default the sensor logs all Informational alerts or higher.

Some signatures have subsignatures, that is, the signature is divided into 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.
Cisco IPS contains over 10,000 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.

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.

For more about signatures, see:
- Obtaining Detailed Information About a Signature, page 35-2
- Understanding Signature Inheritance, page 35-2

Related Topics
- Configuring Signatures, page 35-3
- Chapter 38, “Configuring Global Correlation”

### Obtaining Detailed Information About a Signature

You can find detailed information about each signature from the Cisco Security Intelligence Operations web site. The web site includes a wealth of information and best practice recommendations for network security, and you can set up IntelliShield alerts. There is education on advanced security topics to help you protect your network, prioritize remediation, and structure your systems to reduce organizational risk.

When you edit the Signatures policy in Security Manager (see Signatures Page, page 35-4), the signature ID is linked directly into the Cisco Security Intelligence Operations database of IPS signatures. Clicking a signature ID opens a page containing information about the signature, including a description, the vulnerabilities on which the signature is based, when the signature was created, and so forth. You can search this database yourself at [http://tools.cisco.com/security/center/search.x?search=Signature](http://tools.cisco.com/security/center/search.x?search=Signature). (The database was formerly called the Cisco Network Security Database or NSDB.)

If you do not have access to Cisco.com, then the signature ID is linked to a local copy of the signature database information. Security Manager detects whether you have access to Cisco.com and makes the appropriate link for you without your having to set a preference.

The database includes information only for built-in, default signatures. You cannot find information about custom (user-defined) signatures.

### Understanding Signature Inheritance

Signature inheritance for IPS devices is different than for any other Security Manager rules-based policy. Inheritance refers to the capability of Security Manager to enforce hierarchical lists of first-match, rule-based policies such as access rules. Signature inheritance is different because for IPS devices, Security Manager allows inheritance on a per-signature basis.
This example shows what is meant by inheritance on a per-signature basis:

### Step 1
In Policy View, select **IPS > Signatures > Signatures**.

### Step 2
Create a policy named test1.

### Step 3
Create a second policy, named test2.

### Step 4
Right-click **test2** and select **Inherit Signatures**. The Inherit Rules—test 2 dialog box appears.

### Step 5
Select **test1** and click the **OK** button.

### Step 6
Select **test1** and edit a signature. Note the edit that you made and save your change.

### Step 7
Select **test2** and select the signature that you just edited. Observe that test2 inherited the editing that you did on test1.

---

**IPS Signature Purge**

Beginning with Security Manager 4.1, old signature versions (defined as being older than the lowest signature level deployed) are purged during a periodic purge operation, the purpose of which is to optimize the database.

**Note**
As a result of the purge operation, you may notice the deletion of some of your unused tuning contexts.

Some of the purged signatures may be restored during your next download of IPS signature packages from Cisco.com.

IPS signature purge is disabled by default. To enable IPS signature purge,

### Step 1
Stop the Cisco Security Manager Daemon Manager: At the command prompt, enter `net stop crmdmgtd`.

### Step 2
Navigate to `NMSROOT\MDC\ips\etc\sensorupdate.properties` file, where `NMSROOT` is the path to the Security Manager installation directory. The default is C:\Program Files\CSCOpx.

### Step 3
In `sensorupdate.properties`, change `purgeUnusedSignautesEntriesinDB=false` to `purgeUnusedSignautesEntriesinDB=true`.

### Step 4
Re-start the Cisco Security Manager Daemon Manager: At the command prompt, enter `net start crmdmgtd`.

IPS signature purge now runs at midnight every day.

---

**Configuring Signatures**

The Signatures policy is where you configure signatures for Cisco IPS sensors and Cisco IOS IPS devices.

This section contains the following topics:

- **Signatures Page, page 35-4**
- **Viewing Signature Update Levels, page 35-9**
Signatures Page

Use the Signatures page to display the signature summary table, in which you can add, edit, and delete IPS signatures. From this page you can tune the active signature set in a policy by enabling or disabling signatures. You can also use this page to unload signatures from the engine.

Tips

- Disabled signatures are shown with hash marks covering the table row. When you deploy the configuration, disabled signatures are removed from the device. For more information, see Enabling and Disabling Signatures, page 35-10.
- For many columns, you can right-click the column and edit the property directly. Your edits apply to all rows that you have selected. If you select multiple rows, the options that you can select are limited to those that are valid for all selected rows. The contents of the right-click menu differ based on the cell that you right click. For more information on the available commands, see Signature Shortcut Menu, page 35-7.

Navigation Path

- (Device view) Select IPS > Signatures > Signatures from the Policy selector.
- (Policy view, IPS appliances and service modules) Select IPS > Signatures > Signatures, then select an existing policy or create a new one.
- (Policy view, Cisco IOS IPS devices) Select IPS (Router) > Signatures, then select an existing policy or create a new one.

Related Topics

- Filtering Tables, page 1-37
- Table Columns and Column Heading Features, page 1-38
- Understanding Signatures, page 35-1
- Understanding Signature Inheritance, page 35-2
- Enabling and Disabling Signatures, page 35-10
- Cloning Signatures, page 35-18
- Editing Signature Parameters (Tuning Signatures), page 35-18
- Configuring Event Action Filters, page 36-4
- Chapter 36, “Configuring Event Action Rules”
### Field Reference

**Table 35-1 Signature Policy**

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>The signature ID, which is the unique numerical value assigned to this signature. This value lets the sensor identify a particular signature. Click the ID number to open a page in your web browser with detailed information about the signature, as explained in Obtaining Detailed Information About a Signature, page 35-2.</td>
</tr>
<tr>
<td>Sub</td>
<td>The subsignature ID, which is the unique numerical value assigned to this subsignature. A Subsignature ID identifies a more granular version of a broad signature.</td>
</tr>
<tr>
<td>Name</td>
<td>The name assigned to the signature.</td>
</tr>
<tr>
<td>Action</td>
<td>The actions the sensor takes when this signature fires.</td>
</tr>
<tr>
<td>Severity</td>
<td>The severity level that the signature reports: High, Medium, Low, or Informational.</td>
</tr>
<tr>
<td>Fidelity</td>
<td>The weight associated with how well this signature might perform in the absence of specific knowledge of the target.</td>
</tr>
</tbody>
</table>
| Source  | The lowest policy in the inheritance hierarchy that overrides the settings for a signature. Values can be:  
- **Default**—The signature uses the default Cisco-defined settings.  
- **Local**—The signature is defined specifically for the selected device (Device view only.)  
- **Policy name**—The lowest shared policy in the inheritance hierarchy. You can see policy names in Policy view, or in Device view if you assign a shared signature policy to the device. |
| Enabled | Whether the signature is enabled in this policy; true signifies that it is enabled, false that it is disabled. A signature must be enabled for the sensor to protect against the traffic specified by the signature. |
| Base Risk Rating | The base risk rating value of the signature. |
### Configuring Signatures

#### Retired

The conditions under which the signature is retired, if any. A retired signature is removed from the signature engine. You can activate a retired signature to place it back in the signature engine.

**Timesaver**

Use the retired field to unload disabled signatures on your IOS-IPS device to achieve the most favorable memory consumption of that device.

If the engine level of a signature policy is less than E-4, the Retired field has two possible values: false and true. False means that the signature is not retired; true means that the signature is retired.

If the engine level of a signature policy is equal to E-4, the Retired field has four possible values:

- **false**—The signature is not retired.
- **low-mem-retired**—The signature should be retired on low-memory platforms. A low-memory device is one that has 2 MB RAM or less.
- **med-mem-retired**—The signature should be retired on both low-end and medium platforms. A medium-memory device is one that has 4 MB RAM or less, but more than 2 MB RAM. (Any device with more than 4 MB RAM is considered a high-memory platform.)
- **true**—The signature is retired on all platforms.

When you select low-mem-retired or med-mem-retired, Security Manager configures the device with those signatures. Whether the signature is actually retired on the device depends on amount of memory installed on the device; the device makes the decision on which signatures are actually retired.

**Tip**

The term *engine level* used here is not the same as the term *engine* in the row above.

#### Obsolete

Whether the signature is obsolete. An obsolete signature is removed from the signature engine. It cannot be re-activated. This column is read only.

#### Engine

The engine that parses and inspects the traffic specified by this signature.

#### View Update Level button

(Admin view only.)

Click this button to view the signature update level for this device. For more information, see Viewing Signature Update Levels, page 35-9.

#### Export to File button

Click this button to export the signature summary for the current device to a comma-separated values (CSV) file. You are prompted to select the folder on the Security Manager server and to specify a file name.

#### Add button

Click this button to add a custom signature. For more information, see the following topics:

- Adding Custom Signatures, page 35-15
- Edit Signature or Add Custom Signature Dialog Boxes, page 35-12

### Table 35-1 Signature Policy (Continued)

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retired</td>
<td>The conditions under which the signature is retired, if any. A retired signature is removed from the signature engine. You can activate a retired signature to place it back in the signature engine.</td>
</tr>
<tr>
<td><strong>Timesaver</strong></td>
<td>Use the retired field to unload disabled signatures on your IOS-IPS device to achieve the most favorable memory consumption of that device.</td>
</tr>
<tr>
<td>Obsolete</td>
<td>Whether the signature is obsolete. An obsolete signature is removed from the signature engine. It cannot be re-activated. This column is read only.</td>
</tr>
<tr>
<td>Engine</td>
<td>The engine that parses and inspects the traffic specified by this signature.</td>
</tr>
<tr>
<td>View Update Level button (Device view only.)</td>
<td>Click this button to view the signature update level for this device. For more information, see Viewing Signature Update Levels, page 35-9.</td>
</tr>
<tr>
<td>Export to File button</td>
<td>Click this button to export the signature summary for the current device to a comma-separated values (CSV) file. You are prompted to select the folder on the Security Manager server and to specify a file name.</td>
</tr>
<tr>
<td>Add button</td>
<td>Click this button to add a custom signature. For more information, see the following topics:</td>
</tr>
<tr>
<td></td>
<td>• Adding Custom Signatures, page 35-15</td>
</tr>
<tr>
<td></td>
<td>• Edit Signature or Add Custom Signature Dialog Boxes, page 35-12</td>
</tr>
</tbody>
</table>
Configuring Signatures

Chapter 35  Defining IPS Signatures

Table 35-1  Signature Policy (Continued)

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
</table>
| Edit button  | Click this button to edit the selected signature. You can edit one signature at a time. For more information, see the following topics:  
  - Editing Signatures, page 35-11  
  - Edit Signature or Add Custom Signature Dialog Boxes, page 35-12 |
| Delete button| Click this button to delete the selected custom signatures. You cannot delete Cisco-defined signatures. If you do not want to deploy a Cisco-defined signature, you can retire it or disable it. |

Signature Shortcut Menu

Right-clicking inside the signature summary table in the Signatures policy displays a shortcut menu for performing various functions on the selected signatures. Some commands appear only if you select a single signature, while some commands can be used on more than one signature at a time; your changes apply to all selected signatures. For more information about the Signatures policy, see Signatures Page, page 35-4.

Additionally, the available commands differ depending on which cell you right click. Some commands are available when right-clicking any cell, while others are specific to a single cell.

When you use a right-click command to change the value in a cell of a Default signature, the signature is converted to a Local signature in Device view or a shared-policy-specific signature in Policy view.

The following table explains the available commands.

Table 35-2  Signature Shortcut Menu

<table>
<thead>
<tr>
<th>Menu Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| Add Row      | Adds a custom signature. For more information, see the following topics:  
  - Adding Custom Signatures, page 35-15  
  - Edit Signature or Add Custom Signature Dialog Boxes, page 35-12 |
| Edit Row     | Edits the selected signature. You can edit one signature at a time. For more information, see the following topics:  
  - Editing Signatures, page 35-11  
  - Edit Signature or Add Custom Signature Dialog Boxes, page 35-12 |
| Delete Row   | Deletes the selected custom signatures. You cannot delete Cisco-defined signatures. If you do not want to deploy a Cisco-defined signature, you can retire it or disable it. |
| Clone        | Creates a new custom signature that contains the same properties as the selected signature. For more information, see Cloning Signatures, page 35-18. |
Configuring Signatures

Chapter 35  Defining IPS Signatures

Configuring Signatures

Edit, Add, Replace Action Dialog Boxes

Use the Edit, Add, or Replace Action dialog boxes to change the actions defined for a signature. These
dialog boxes are available only when you edit the Action cell using the right click menu as explained in
Signature Shortcut Menu, page 35-7. The behavior differs depending on the dialog box name:

- Add Actions—The actions that you select are added to those already defined in the signature. To
  open this dialog box, right-click the Actions cell of a signature and select Add to Actions > More.

Table 35-2  Signature Shortcut Menu (Continued)

<table>
<thead>
<tr>
<th>Menu Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable, Disable</td>
<td>Places the signature in the enabled or disabled state, respectively. Disabled signatures appear with crosshatching over them. For more information, see Enabling and Disabling Signatures, page 35-10.</td>
</tr>
<tr>
<td>Show Events</td>
<td>Enables navigation to the Cisco Security MARS application to view the realtime or historical events detected by the selected signature. For more information, see Viewing CS-MARS Events for an IPS Signature, page 65-28.</td>
</tr>
</tbody>
</table>

Action Cell Commands

<table>
<thead>
<tr>
<th>Menu Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add to Actions</td>
<td>Adds an action to the current list of actions for the selected signature.</td>
</tr>
<tr>
<td>Delete from Actions</td>
<td>Deletes an action from the current list of actions for the selected signature.</td>
</tr>
<tr>
<td>Replace Actions With</td>
<td>Replace the current set of actions for the selected signature with the single action selected. If you want to select more than one action, select More from the submenu, then use Ctrl+click to select the desired actions.</td>
</tr>
<tr>
<td>Edit Actions</td>
<td>Opens the Edit Actions dialog box, where you can select the desired actions for the signature. Your selection replaces the current list of actions for the signature. For more information, see Edit, Add, Replace Action Dialog Boxes, page 35-8.</td>
</tr>
</tbody>
</table>

Severity Cell Commands

- High
- Medium
- Low
- Informational
Changes the severity level of the signature to the level you select.

Fidelity Cell Commands

Edit Fidelity
Changes the fidelity rating of the signature, which is the weight associated with how well this signature might perform in the absence of specific knowledge of the target.

Retired Cell Commands

- Retire
- Activate
- Retire on Low Memory
- Retire on Medium Memory
Changes the retired status of the signature to the selected status. For more information about the retired status categories, see Edit Signature or Add Custom Signature Dialog Boxes, page 35-12.
Replace Actions—The actions that you select completely replace those defined in the signature. To open this dialog box, right-click the Actions cell of a signature and select Replace Actions With > More.

Edit Actions—The actions that you select completely replace those defined in the signature. To open this dialog box, right-click the Actions cell of a signature and select Edit Actions.

For an explanation of the available actions, see Understanding IPS Event Actions, page 36-2. You can select multiple actions using Ctrl-click.

**Note**

When you open dialog box, the list of actions that you see varies. The list of actions depends upon whether you right-click in only one signature row in the Actions column or select more than one signature row before right-clicking in the Actions column. If you right-click in only one signature row in the Actions column, the list of actions is that of the engine for that signature. If you select more than one signature row before right-clicking in the Actions column, the list of actions is that which is available for each affected engine. (It is the list of common actions, not the union of actions.)

### Edit Fidelity Dialog Box

Use the Edit Fidelity dialog box to make changes in the Fidelity Rating for a particular signature. The Fidelity Rating, or Signature Fidelity Rating (SFR), identifies the weight associated with how well this signature might perform in the absence of specific knowledge of the target. This rating can be any number from 0 to 100, with 100 indicating the most confidence in the signature.

**Navigation Path**

In the Signatures policy, right-click the Fidelity cell in a signature and select Edit Fidelity. For information on opening the Signatures policy, see Signatures Page, page 35-4. For more information on the signature shortcut menu, see Signature Shortcut Menu, page 35-7.

### Viewing Signature Update Levels

In Device view, you can determine the current signature update packages applied to the device in Security Manager and compare it to the one deployed on the device.

Differences between the applied and deployed update levels can occur when:

- The device is updated outside of Security Manager.
- An update is applied to the policy in Security Manager but not yet published to the device.
- During initial Security Manager deployment before the devices are under Security Manager control.

To view the signature update level, select the IPS > Signatures > Signatures policy for an IPS device in Device view. Then, click the View Update Level button to open the Update Level dialog box.

The following table describes the information displayed in the dialog box.

<table>
<thead>
<tr>
<th>Table 35-3</th>
<th>Update Level Dialog Box</th>
</tr>
</thead>
<tbody>
<tr>
<td>Element</td>
<td>Description</td>
</tr>
<tr>
<td>Applied Level</td>
<td>This column displays the patch level that is applied to this device in Security Manager.</td>
</tr>
</tbody>
</table>
Configuring Signatures

Chapter 35  Defining IPS Signatures

Table 35-3   Update Level Dialog Box (Continued)

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployed Level</td>
<td>This column displays the patch level that is currently running on the selected device.</td>
</tr>
<tr>
<td>Major Update</td>
<td>Identifies the major update level.</td>
</tr>
<tr>
<td>Minor Update</td>
<td>Identifies the minor update level.</td>
</tr>
<tr>
<td>Service Pack</td>
<td>Identifies the service pack level.</td>
</tr>
<tr>
<td>Patch</td>
<td>Identifies the patch level.</td>
</tr>
<tr>
<td>Engine</td>
<td>Identifies the engine level.</td>
</tr>
<tr>
<td>Signature Update</td>
<td>Identifies the signature update level.</td>
</tr>
</tbody>
</table>

**Note** This field is the only field on this page that applies to the IOS IPS devices; all of the other fields are exclusive to IPS devices.

| Revert button   | If you mistakenly modify Applied Level, allows you to discard that new Applied Level; clicking Revert syncs the Applied Level to the Deployed Level. |
| Tip            | A warning dialog appears before performing Revert. Also, a warning dialog appears asking you to submit the activity. |

Enabling and Disabling Signatures

You can enable and disable individual signatures. Your change takes effect when you redeploy the configuration to the device.

If a signature is disabled, it appears in the table overlain with hash marks. When you deploy the configuration, disabled signatures are removed from the device.

Disabling signatures is useful when you want to reduce the number of signatures used by a device, or if you want to temporarily stop using a custom signature without deleting it. You can later re-enable a signature that you disabled.

**Note** You can enable a signature that is retired, but it then is not used to scan traffic, because it is not in the signature micro-engine. If you want a sensor to scan network traffic for a particular signature, you must enable it and not retire it. The AIP-SSC-5 does not support enabling a signature that is retired.

**Step 1** Do one of the following:

- (Device view) Select **IPS > Signatures > Signatures** from the Policy selector.
- (Policy view, IPS appliances and service modules) Select **IPS > Signatures > Signatures**, then select an existing policy or create a new one.
- (Policy view, Cisco IOS IPS devices) Select **IPS (Router) > Signatures**, then select an existing policy or create a new one.

The Signature page appears; see **Signatures Page, page 35-4**.
Step 2   Right-click the signature whose enabled status you want to change and select **Enable** or **Disable**, as appropriate.

---

### Editing Signatures

You can edit signatures to change their behavior. For example, you can change the action that should be taken when a signature fires, or the severity and fidelity ratings used to calculate the risk rating of the signature.

Some signatures have special requirements. For example, to configure a sensor to detect ACL violation signatures, you must first configure one or more Cisco IOS routers to log ACL violations. Then, you must configure those routers to communicate with the sensor. Finally, you must configure the sensor to accept syslog traffic from those routers.

#### Tip
This procedure describes how to edit an entire signature. You can also selectively edit individual properties of a signature using the right-click menu in the Signatures policy. For information on the available commands, see **Signature Shortcut Menu**, page 35-7.

---

**Related Topics**
- Understanding Signatures, page 35-1
- Understanding IPS Event Actions, page 36-2
- Enabling and Disabling Signatures, page 35-10
- Cloning Signatures, page 35-18
- Configuring Event Action Filters, page 36-4
- Chapter 36, “Configuring Event Action Rules”

---

**Step 1**   Do one of the following:
- (Device view) Select **IPS > Signatures > Signatures** from the Policy selector.
- (Policy view, IPS appliances and service modules) Select **IPS > Signatures > Signatures**, then select an existing policy or create a new one.
- (Policy view, Cisco IOS IPS devices) Select **IPS (Router) > Signatures**, then select an existing policy or create a new one.

The Signature page appears; see **Signatures Page**, page 35-4.

**Step 2**   Right-click the signature you want to edit and select **Edit Row**. You can also select the signature and click the Edit Row (pencil) button beneath the signatures table. The Edit Signature dialog box opens.

#### Tip
Use the filter fields above the table to help you find the desired signature. For information on filtering tables, see **Filtering Tables**, page 1-37.

**Step 3**   Make the desired changes to the signature. For specific details about each option, see **Edit Signature or Add Custom Signature Dialog Boxes**, page 35-12.

When editing signatures, keep the following in mind:
You cannot edit a Default signature. Default signatures are the Cisco-defined version of a signature. Before you can edit a Default signature, you must convert it either to a Local signature (one defined specifically on the selected device) or a shared-policy-specific signature (one defined in a shared policy). You must select either Local or the shared policy name from the Source Policy field before you can change any field on the Edit Signature dialog box.

You cannot change every characteristic of a signature. For example, you cannot change the signature or subsignature IDs. These fields are read-only.

If you want to change the detailed parameters of a signature, follow the procedure described in Editing Signature Parameters (Tuning Signatures), page 35-18.

Step 4  Click OK to save your changes.

Edit Signature or Add Custom Signature Dialog Boxes

The Edit Signature and Add Custom Signature dialog boxes are essentially the same. Most of the fields are identical, although there are some layout differences. Use these dialog boxes as follows:

- Use the Edit Signature dialog box to edit the characteristics of a non-default signature (you can only view the characteristics of a default signature in read-only mode).
  
  You cannot edit default signatures. To make any changes to a signature, you must select something other than Default in the Source Policy field at the top of the dialog box.

- Use the Add Custom Signature dialog box to create a custom signature. In the Add Custom Signature dialog box, you enter a name and then select an existing engine from a drop-down list. The signature ID and subsignature ID are assigned by Security Manager. After you finish selecting the remaining parameters, the new signature is added to the Signatures page in the appropriate numerical location, and it is selected.

Navigation Path

From the Signatures page:

- To edit a signature, right-click the policy you want to edit and select Edit Row.
- To add a custom signature, click the Add Row (+) button beneath the table, or right-click any row and select Add Row.

For information on opening the Signature page, see Signatures Page, page 35-4.

Related Topics

- Edit, Add, Replace Action Dialog Boxes, page 35-8
- Edit Signature Parameters Dialog Box, page 35-20
- Engine Options, page 35-16
### Table 35-4 Edit Signature or Add Custom Signature Dialog Boxes

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Policy</td>
<td>The policy in which you are editing the signature:</td>
</tr>
<tr>
<td>(Edit signature only.)</td>
<td>- Default—The default Cisco-defined signature, which you cannot edit. You must select something other than Default to edit the signature.</td>
</tr>
<tr>
<td></td>
<td>- Local—The signature is a local signature defined specifically for the selected device. This option is not available in Policy view.</td>
</tr>
<tr>
<td></td>
<td>- Policy name (variable)—The name of a shared policy. In Device view, a policy name is available only if you assign a shared policy to the device. In Policy view, this is the name of the policy you are editing. Select the policy name to edit the signature and to have your edits reflected on all devices that are assigned the shared policy.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the signature.</td>
</tr>
<tr>
<td>(Add only.)</td>
<td>You cannot change the name after you create the signature. If you want to change the name, you must create a clone of the signature.</td>
</tr>
<tr>
<td>Inheritance Mandatory</td>
<td>When selected, forces any policy that inherits from this policy to use the signature settings defined.</td>
</tr>
<tr>
<td>(Edit signature only.)</td>
<td></td>
</tr>
<tr>
<td>Enabled</td>
<td>Whether the signature is enabled.</td>
</tr>
<tr>
<td>Severity</td>
<td>The severity level that the signature will report: High, Medium, Low, or Informational.</td>
</tr>
<tr>
<td>Fidelity Rating</td>
<td>The weight associated with how well this signature might perform in the absence of specific knowledge of the target.</td>
</tr>
<tr>
<td>Actions</td>
<td>The actions that the sensor will take when this signature fires. For a complete list of actions, see the Understanding IPS Event Actions, page 36-2. Use Ctrl+click to select multiple actions.</td>
</tr>
</tbody>
</table>

**Base Risk Rating**

**Risk Rating**

(Fields have slightly different names when adding or editing signatures.)

The base risk rating value of the signature, which is calculated by multiplying the fidelity rating and the severity factor and dividing them by 100 (Fidelity Rating x Severity Factor /100). This value is read only; you cannot directly change it. To change the value, alter the Severity and Fidelity fields.

The Severity Factor has the following values based on what you select in the Severity field:

- High = 100
- Medium = 75
- Low = 50
- Informational = 25
### Chapter 35  Defining IPS Signatures

#### Configuring Signatures

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engine</td>
<td>The engine that parses and inspects the traffic specified by this signature. For a description of the engines, see <a href="#">Engine Options</a>, page 35-16. When adding a custom signature, you must select the appropriate engine. For detailed information about each engine, and the parameters available, see the “Signature Engines” section in the <em>Installing and Using Cisco Intrusion Prevention System Device Manager</em> document for the IPS Software release you are using.</td>
</tr>
</tbody>
</table>
| Retired       | The conditions under which the signature is retired, if any. A retired signature is removed from the signature engine. You can activate a retired signature to place it back in the signature engine. Timesaver: Use the retired field to unload disabled signatures on your IOS-IPS device to achieve the most favorable memory consumption of that device. If the engine level of a signature policy is less than E-4, the Retired field has two possible values: false and true. False means that the signature is not retired; true means that the signature is retired. If the engine level of a signature policy is equal to E-4, the Retired field has four possible values:  
  - **false**—The signature is not retired.  
  - **low-mem-retired**—The signature should be retired on low-memory platforms. A low-memory device is one that has 2 MB RAM or less.  
  - **med-mem-retired**—The signature should be retired on both low-end and medium platforms. A medium-memory device is one that has 4 MB RAM or less, but more than 2 MB RAM. (Any device with more than 4 MB RAM is considered a high-memory platform.)  
  - **true**—The signature is retired on all platforms. When you select low-mem-retired or med-mem-retired, Security Manager configures the device with those signatures. Whether the signature is actually retired on the device depends on amount of memory installed on the device; the device makes the decision on which signatures are actually retired. Tip: The term *engine level* used here is not the same as the term *engine* in the row above. |
| Obsolete      | Identifies whether the signature is obsolete. An obsolete signature is removed from the signature engine. It cannot be re-activated. (Edit signature only.)                                                                 |

---

**Table 35-4  Edit Signature or Add Custom Signature Dialog Boxes (Continued)**

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
</table>
Chapter 35      Defining IPS Signatures

Configuring Signatures

Adding Custom Signatures

If you want to look for traffic patterns that are not identified by the built-in signatures, you can create your own custom signatures to define the traffic patterns.

Even if a built-in signature covers the traffic pattern, you might want to create a custom signature to edit the detailed signature parameters without altering the default signature. If you are creating a custom signature that is similar to an existing signature, the easiest way to do it is to clone the signature as described in Cloning Signatures, page 35-18.

Note

The AIP-SSC-5 does not support custom signatures.

Step 1

Do one of the following:

- (Device view) Select IPS > Signatures > Signatures from the Policy selector.
- (Policy view, IPS appliances and service modules) Select IPS > Signatures > Signatures, then select an existing policy or create a new one.
- (Policy view, Cisco IOS IPS devices) Select IPS (Router) > Signatures, then select an existing policy or create a new one.

The Signature page appears; see Signatures Page, page 35-4.

Step 2

Click the Add Row (+) button beneath the signature table to open the Add Custom Signature dialog box.

Step 3

Configure the desired settings. For specific details about each option, see Edit Signature or Add Custom Signature Dialog Boxes, page 35-12.

When creating signatures, keep the following in mind:

- You cannot change the signature name after you define the signature. If you later want to change the name, you must clone the signature and change it while creating the clone.
- Select the appropriate signature engine for the signature. For a description of the signature engines, see Engine Options, page 35-16. You cannot change the engine after you create the signature; if you select the wrong engine and click OK to save the signature, you must start over and create an entirely new signature.
- The default is to create an enabled signature, but you can deselect the Enabled check box to initially create a disabled signature. You might want to disable the signature if you have not finished editing its parameters.
Follow the procedure described in Editing Signature Parameters (Tuning Signatures), page 35-18 to define the detailed signature parameters. You must select the desired engine before you edit the parameters, because many of the parameters are determined by the signature engine.

Whether you can save the signature before configuring parameters differs based on the engine that you select. At minimum, you must click **Edit Parameters** to open the Edit Signature Parameters dialog box, and then click **OK** in the Edit Signature Parameters dialog box, before you can save the signature definition. However, to create a meaningful signature, you will need to configure the parameters to identify the desired traffic pattern.

**Step 4**  Click **OK** to save your changes.

The custom signature is added to the end of the table and given the next available signature ID starting at 60000.

---

### Engine Options

The following list identifies the options you can specifying in the Engine field of the Edit Signature Parameters dialog box. For detailed information about each engine, and the parameters available, see the “Signature Engines” section in the *Installing and Using Cisco Intrusion Prevention System Device Manager* document for the IPS Software release you are using.

- 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.

The Service Generic engine allows programmatic signatures to be issued in a config-file-only signature update. It has a simple machine and assembly language that is defined in the configuration file. It runs the machine code (distilled from the assembly language) through its virtual machine, which processes the instructions and pulls the important pieces of information out of the packet and runs them through the comparisons and operations specified in the machine code. It is intended as a rapid signature response engine to supplement the String and State engines.

You cannot use the Service Generic engine to create custom signatures.
Note: Due to the proprietary nature of this complex language, we do not recommend that you edit the Service Generic engine signature parameters. Change only the severity and event action for these signatures.

- 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.
Cloning Signatures

If you want to create a custom signature that is similar to an existing signature, you can create a clone, or copy, of the signature. You can then edit the parameters to make the clone perform according to your requirements.

For example, you might want to create a clone of a Cisco-defined signature to customize it to your needs. You might find this preferable to converting the Cisco signature to a Local or shared policy signature and directly editing its parameters.

To clone a signature, follow these steps:

Step 1  Do one of the following:
• (Device view) Select IPS > Signatures > Signatures from the Policy selector.
• (Policy view, IPS appliances and service modules) Select IPS > Signatures > Signatures, then select an existing policy or create a new one.
• (Policy view, Cisco IOS IPS devices) Select IPS (Router) > Signatures, then select an existing policy or create a new one.

The Signature page appears; see Signatures Page, page 35-4.

Step 2  Right-click the signature that you want to clone and select Clone.

Security Manager takes some time to make the copy, and might warn you that some attributes are read-only and cannot be copied. If you receive a warning, click OK. The Add Custom Signature dialog box then appears.

Step 3  Edit the properties of the cloned signature, as described in Adding Custom Signatures, page 35-15.

Step 4  Click OK. The clone appears in the summary table on the Signatures page as the last signature.

Cloned signatures are enabled and active by default.

Editing Signature Parameters (Tuning Signatures)

If you cannot alter the behavior of a signature to fit your needs using the Event Action Filters and Overrides policies, or by changing the actions associated with a signature, you might need to fine-tune the signature parameters. You should considered editing parameters to be your last option, however, because these parameters can be complex and frequently require that you have a deep understanding of packet characteristics.

The reason you would want to edit parameters is to reduce false positives and false negatives:

• A false positive occurs when legitimate network activity, such as virus scanning, is interpreted and reported as an attack. This happens when network activity meets criteria that were specified to identify an attack before the attack occurred. You can decrease the number false positives by tuning your sensor configurations.
• A false negative occurs when an attack was not detected. Tuning your sensor configurations will help you decrease the number of false negatives.
Tip

You cannot edit the parameters of a default signature. Before editing the parameters of a default signature, you must convert the signature to a local- or shared-policy signature. In some cases, such as regular expression editing, you must clone the signature and convert it to a custom signature.

This procedure describes how to edit signature parameters to tune a signature.

Related Topics

- Editing Signatures, page 35-11
- Understanding Signatures, page 35-1
- Configuring Event Action Filters, page 36-4
- Configuring Event Action Overrides, page 36-12

Step 1

Do one of the following:

- (Device view) Select **IPS > Signatures > Signatures** from the Policy selector.
- (Policy view, IPS appliances and service modules) Select **IPS > Signatures > Signatures**, then select an existing policy or create a new one.
- (Policy view, Cisco IOS IPS devices) Select **IPS (Router) > Signatures**, then select an existing policy or create a new one.

The Signature page appears; see Signatures Page, page 35-4.

Step 2

Right-click the signature whose parameters you want to edit and select **Edit Row**. The Edit Signature dialog box appears (see Edit Signature or Add Custom Signature Dialog Boxes, page 35-12).

Step 3

If the Source Policy field shows Default, you must change it to Local or to the name of a shared policy before you can edit the parameters. The Local option is available in Device view only, and makes your changes apply to the device you are editing and to no other devices. If you select the name of a shared policy, your changes apply to all devices that are assigned the policy.

Step 4

Click **Edit Parameters**. The Edit Signature Parameters dialog box appears.

The Edit Signature Parameters dialog box contains a folder tree structure, with the parameter names in the left side tree, and the values of the parameters shown on the right side.

Values that you can change contain a little box in the name; this is a check box. An empty check box indicates that the default value is being used for the parameter. Check the check box to configure that parameter. Click the value field to change the parameter. A green check indicates that a user-defined value is being used. Click the green check to change the value back to the default. (Editing the field typically adds a check mark to the box.)

To change a parameter, click in the associated field in the right side. The behavior of clicking on a parameter differs based on the parameter type:

- **Read-only parameters**—Many parameters are read-only and cannot be changed, such as signature ID. Clicking these parameters typically has no effect, although parameter lists will open a dialog box (such as the Obsoletes list).

- **Text or Numeric parameters**—When you click a parameter that requires that you type in a value, whether alphanumeric or numeric, the field becomes an edit box. Type in the desired value and either press enter or click outside the edit box.

- **Predefined value parameters**—Many parameters have a small set of possible values, such as Yes/No. When you click these parameters, you activate a drop-down list. Select the desired option and click outside the field.
- List parameters—Some parameters contain a list of items. These parameters are represented by a pencil icon in the parameter value along with a word, such as Set or List. When you click in the field, a dialog box opens where you can configure the list associated with the item. The Meta engine component list is an example; for more information, see Editing the Component List for Meta Engine Signatures, page 35-25.

- Variable parameters—Some parameters allow you to select policy objects to identify the contents of the parameters. For example, you can select port list objects to identify ports in some signature engines. When you click these parameters, an edit box with a Select button appears. You can type the items directly into the edit box, including the name of the policy object, or click Select to select the policy object from a list or to create a new object.

For more information about the Edit Signature Parameters dialog box, see Edit Signature Parameters Dialog Box, page 35-20.

**Step 5** Change the settings as desired, then click OK to save your changes. You are returned to the Edit Signature dialog box.

**Step 6** Click OK in the Edit Signature dialog box to save your changes to the signature.

### Tip
If you decide that your edits did not have the desired effect, or you suspect that you made a mistake, you can click the Restore Defaults button in the Edit Signature dialog box to erase your changes. You can then start over.

---

**Edit Signature Parameters Dialog Box**

Use the Edit Signature Parameters dialog box to edit (also called tune) the built-in micro-engine parameters for a particular signature. Different engines have different parameters, so the appearance of the Edit Signature Parameters dialog box varies. For more information about editing signature parameters, see Editing Signature Parameters (Tuning Signatures), page 35-18.

The Edit Signature Parameters dialog box contains a folder tree structure, with the parameter names in the left side tree, and the values of the parameters shown on the right side.

Values that you can change contain a little box in the name; this is a check box. An empty check box indicates that the default value is being used for the parameter. Check the check box to configure that parameter. Click the value field to change the parameter. A green check indicates that a user-defined value is being used. Click the green check to change the value back to the default. (Editing the field typically adds a check mark to the box.)

To change a parameter, click in the associated filed in the right side. The behavior of clicking on a parameter differs based on the parameter type:

- **Read-only parameters**—Many parameters are read-only and cannot be changed, such as signature ID. Clicking these parameters typically has no effect, although parameter lists will open a dialog box (such as the Obsoletes list).

- **Text or Numeric parameters**—When you click a parameter that requires that you type in a value, whether alphanumeric or numeric, the field becomes an edit box. Type in the desired value and either press enter or click outside the edit box.

- **Predefined value parameters**—Many parameters have a small set of possible values, such as Yes/No. When you click these parameters, you activate a drop-down list. Select the desired option and click outside the field.
• List parameters—Some parameters contain a list of items. These parameters are represented by a pencil icon in the parameter value along with a word, such as Set or List. When you click in the field, a dialog box opens where you can configure the list associated with the item. The Meta engine component list is an example; for more information, see Editing the Component List for Meta Engine Signatures, page 35-25.

• Variable parameters—Some parameters allow you to select policy objects to identify the contents of the parameters. For example, you can select port list objects to identify ports in some signature engines. When you click these parameters, an edit box with a Select button appears. You can type the items directly into the edit box, including the name of the policy object, or click Select to select the policy object from a list or to create a new object.

Navigation Path
From the Edit Signature or Add Custom Signature dialog boxes, click the Edit Parameters button. For information on opening these dialog boxes, see Edit Signature or Add Custom Signature Dialog Boxes, page 35-12.

Tip
If the button is not active, you must first select Local or the name of a shared policy from the Source Policy field, or clone the signature to create a custom policy. The Local option is available in Device view only, and makes your changes apply to the device you are editing and to no other devices. If you select the name of a shared policy, your changes apply to all devices that are assigned the policy.
### Field Reference

#### Table 35-5 Edit Signature Parameters Dialog Box

<table>
<thead>
<tr>
<th>Elements</th>
<th>Description</th>
</tr>
</thead>
</table>
| Tuning Context (Policy view only) | Displays the information needed by Security Manager to uniquely describe how the signature parameters were edited (tuned) for a particular signature policy. The Tuning Context field is a character string that contains the following items:  
  - **Context** — The identification given by the Security Manager server for the unique definition of this micro-engine.  
  - **SigLevel (IPS) or Version (IOS IPS)** — For IPS policies, the range of signature update levels to which this definition of the signature micro-engine applies. For IOS IPS, this is the IOS IPS version.  
  - **Engine** — The name of the IPS engine.  
  **Tip** As an example, the Tuning Context field could contain the following character string: Context:9, SigLevel:302-449, Engine:atomic-ip.  
  For any particular signature policy, the Tuning Context field can contain one or many tuning contexts:  
  - The tuning context with the highest signature level is prepended with “Reference context.”  
  - If you modify the shared policy that is prepended with “Reference context,” Security Manager may ask you if you want to copy the policy to other applicable contexts. (A particular device may appear in more than one context.)  
  - If you choose to copy the policy to other applicable contexts, an error message informs you if some parameters cannot be copied.  
  **Note** Beginning with Security Manager 4.1, old signature versions (defined as being older than the lowest signature level deployed) are purged during a periodic purge operation, the purpose of which is to optimize the database. As a result, you may notice the deletion of some of your unused tuning contexts. |
| Signature ID               | 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            | 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. |
| Promiscuous Delta          | Modifies the seriousness of an alert when operating in promiscuous mode. The value is subtracted from an alert’s overall risk rating. The promiscuous delta is ignored when operating in inline mode. The value can be 0 to 30. |
### Table 35-5  Edit Signature Parameters Dialog Box (Continued)

<table>
<thead>
<tr>
<th>Elements</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sig Description</td>
<td>A description of the signature to help you distinguish this signature from other signatures:</td>
</tr>
<tr>
<td></td>
<td>• Alert Notes—Additional information about this signature that will be included in the alert message.</td>
</tr>
<tr>
<td></td>
<td>• User Comments—Your comments about the signature.</td>
</tr>
<tr>
<td></td>
<td>• Alarm Traits—Traits you want to document about this signature. The value is 0 to 65535. The default is 0.</td>
</tr>
<tr>
<td></td>
<td>• Release—The release in which the signature was most recently updated.</td>
</tr>
<tr>
<td></td>
<td>• Signature Creation Date—The date on which the signature was created.</td>
</tr>
<tr>
<td></td>
<td>• Signature Type—The type of signature: Anomaly, Component, Exploit, Vulnerability, or Other.</td>
</tr>
<tr>
<td>Engine</td>
<td>The engine that parses and inspects the traffic specified by this signature. The engine determines which parameters are available in the Engines folder. For a description of the engines, see Engine Options, page 35-16.</td>
</tr>
<tr>
<td></td>
<td>For detailed information about each engine, and the parameters available, see the “Signature Engines” section in the Installing and Using Cisco Intrusion Prevention System Device Manager document for the IPS Software release you are using.</td>
</tr>
<tr>
<td>Tip</td>
<td>Many engines include the Fragment Status parameter, which lets you identify whether packet fragments should be inspected. You can elect to not inspect fragments, to inspect fragments, or to apply the signature to any packet status.</td>
</tr>
<tr>
<td>Event Counter</td>
<td>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. Configure the following values:</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• Specify Alert Interval—Whether you want to specify the time between alerts for resetting the event count, Yes or No. If you select Yes, enter the time in seconds from 2 to 1000.</td>
</tr>
</tbody>
</table>
### Configuring Signatures

#### Chapter 35      Defining IPS Signatures

**Table 35-5  Edit Signature Parameters Dialog Box (Continued)**

<table>
<thead>
<tr>
<th>Elements</th>
<th>Description</th>
</tr>
</thead>
</table>
| Alert Frequency              | How often the sensor alerts you when this signature is firing. Specify the following parameters for this signature. These parameters are explained below.  
  - Summary Mode  
  - Summary Interval  
  - Summary Key  
  - Specify Global Summary Threshold |
| Summary Mode (Alert Frequency group) | The mode of alert summarization. There are four modes: Fire All, Fire Once, Summarize, and Global Summarize. The summary mode is changed dynamically to adapt to the current alert volume. For example, you can configure the signature to Fire All, but after a certain threshold is reached, it starts summarizing. Your selection of summary mode controls which other parameters are available in the Summary Mode group.  
  - Fire All—Fires an alert on all events.  
  - Fire Once—Fires an alert only once.  
  - Summarize—Summarizes alerts.  
  - Global Summarize—Summarizes an alert so that it only fires once regardless of how many attackers or victims.  
  **Note** When multiple contexts from an ASA device 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. |
| Specify Summary Threshold (Summary Mode group.) | When you select Fire All, you can select whether you want to configure the summary threshold settings that will be used if the device dynamically changes to summary mode. If you select Yes, you can configure the summary interval, key, or global summary thresholds. |
| Summary Interval (Summary Mode group.) | The time in seconds used in each summary alert. The value is 1 to 65535. The default is 15. |
| Summary Key (Summary Mode group.) | 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 (Summary Mode group.) | Whether to specify the threshold number of events to take the alert into global summary, Yes or No. If you select Yes, enter the threshold number of events, from 1 to 65535. The default is 240. |
Use the Edit Signature Parameter—Component List dialog box to edit the component list for a 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.

The Meta engine is different from other engines in that it takes alerts as input where most engines take packets as input. Thus, in a Meta engine signature, you must identify the signatures that the Meta signature should be looking for. This list of signatures is contained in the Component list.

The Component list is part of the signature parameters. To edit the parameters, follow the procedure described in Editing Signature Parameters (Tuning Signatures), page 35-18. When you open the Edit Signature Parameters dialog box for a signature that uses the Meta engine, look for the Engine > Component List parameter. The parameter value contains a pencil icon and the word List. Click List to open the Edit Signature Parameter—Component List dialog box.

The dialog box is divided into two lists, an Inactive list (on the left) and an active list (on the right). The active list defines the signatures that the Meta engine signature is looking for.

To modify the components list:

- **Add new components**—Click the Add Entry (+) button to the left of the inactive list. The Add Signature Parameter—List Entry dialog box opens. Configure the following values:
  - **Entry Key**—A name for the component.
  - **Component Sig ID**—The signature ID of the signature you are looking for.
  - **Component SubSig ID**—The subsignature ID; enter 0 if there are no subsignatures.
Configuring Signature Settings

Use the Signature Settings page to define settings for IPS appliances and service modules (but not Cisco IOS IPS devices). These settings define the following policies:

- **Application policy**—Enable or disable HTTP, determine and specify the maximum number of HTTP requests, specify AIC web ports, and enable or disable FTP.

- **Fragment reassembly policy**—Configure the sensor to reassemble a datagram that has been fragmented over more than one packet by selecting the IP reassembly mode.
- **Stream reassembly policy**—Configure the sensor to monitor only TCP sessions that have been established by a complete three-way handshake by specifying whether a TCP handshake is required and by selecting the TCP reassembly mode.

- **IP logging policy**—Configure the sensor to generate an IP session log when the sensor detects an attack by determining and selecting the maximum allowable number of log packets, the IP log time and the maximum allowable size of the IP log.

All of these settings have default values, so configure this policy only if you need to use a non-default value.

To configure the Signature Settings policy, do one of the following:

- (Device view) Select **IPS > Signatures > Settings** from the Policy selector.
- (Policy view) Select **IPS > Signatures > Settings**, then select an existing policy or create a new one.

You can then configure the options that are explained in the following table.

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable HTTP</td>
<td>Enables protection for web services. Select <strong>Yes</strong> to require the sensor to inspect HTTP traffic for compliance with the RFC.</td>
</tr>
<tr>
<td>Max HTTP Requests</td>
<td>The maximum number of outstanding HTTP requests per connection.</td>
</tr>
<tr>
<td>AIC Web Ports</td>
<td>The ports on which to look for AIC traffic. Enter a comma-separated list of port numbers or port list objects that define the ports. You can click <strong>Select</strong> to select a port list object from a list or to create a new object.</td>
</tr>
<tr>
<td>Enable FTP</td>
<td>Enables protection for FTP services. Select <strong>Yes</strong> to require the sensor to inspect FTP traffic.</td>
</tr>
<tr>
<td>IP Reassembly Mode</td>
<td>The method the sensor uses to reassemble the fragments, based on the operating system.</td>
</tr>
<tr>
<td>TCP Handshake Required</td>
<td>Whether the sensor should only track sessions for which the three-way handshake is completed.</td>
</tr>
<tr>
<td>TCP Reassembly Mode</td>
<td>The mode the sensor should use to reassemble TCP sessions with the following options:</td>
</tr>
<tr>
<td></td>
<td>• Asymmetric—May only be seeing one direction of bidirectional traffic flow.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> 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.</td>
</tr>
<tr>
<td></td>
<td>• Loose—Use in environments where packets might be dropped.</td>
</tr>
<tr>
<td></td>
<td>• Strict—If a packet is missed for any reason, all packets after the missed packet are not processed.</td>
</tr>
<tr>
<td>Max IP Log Packets</td>
<td>The number of packets you want logged.</td>
</tr>
<tr>
<td>IP Log Time</td>
<td>The duration you want the sensor to log, from 1 to 60 minutes. The default is 30 minutes.</td>
</tr>
</tbody>
</table>
### Configuring Signature Settings

#### Table 35-6 Signature Settings Page (Continued)

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max IP Log Bytes</td>
<td>The maximum number of bytes you want logged.</td>
</tr>
</tbody>
</table>