Configuring Event Action Rules

Note From 4.17, though Cisco Security Manager continues to support IPS features/functionality, it does not support any enhancements as IPS is now End of Life. For more information, see EOL notice.

An IPS event is an IPS message that contains an alert, a block request, a status message, or an error message. An event action is the sensor's response to an event. An event action happens only if the event is not filtered. Possible event actions are TCP reset, block host, block connection, IP logging, and capturing the alert trigger packet. Event actions were known as alarms in Cisco IPS versions earlier than 5.x.

The IPS Event Actions folder is where you configure settings for the event action processing component of the sensor. These settings define the actions for the sensor to take when an event is detected.

Note You cannot use IPv6 addresses in Event Action policies in Security Manager. For more information on IPv6 support in Security Manager, see IPv6 Support in Security Manager, page 1-8.

This chapter contains the following topics:

Understanding the IPS Event Action Process

The IPS event action rules dictate the actions that the sensor performs when an event occurs. Although each signature is configured with specific actions that should be taken, the actual actions performed also depend on other factors.

Following is the general process that occurs when inspection identifies a signature event:

1. A signature alert occurs with actions specified by the signature. A risk rating for the alert is calculated.

For a detailed explanation of how risk rating is calculated, see Calculating the Risk Rating in *Installing and Using Cisco Intrusion Prevention System Device Manager 7.0* on Cisco.com.

You can influence risk ratings by configuring target value ratings and OS mappings; see Configuring IPS Event Action Network Information, page 40-17.

2. The **Event Action Overrides** policy is processed. If the risk rating of the event matches an override rule, the actions identified in the override rule are **added** to the actions defined in the signature. The overrides do not replace the actions specified in the signature.

   For information on configuring overrides, see Configuring Event Action Overrides, page 40-13.

3. The **Event Action Filters** policy is processed. If rules apply to the event, the rules **subtract** actions from the event. Thus, an action you added in a signature policy or override rule might be removed by one of your filter rules.

   For information on creating filter rules, see Configuring Event Action Filters, page 40-4.

4. Event summarization occurs, unless you turn off the summarization feature as described in Configuring Settings for Event Actions, page 40-23.

5. The actions are performed. For an explanation of possible actions, see Edit, Add, Replace Action Dialog Boxes, page 39-12.

6. A list of denied attackers is maintained, and subsequent access prevented, based on configurable settings. To change the default settings, see Configuring Settings for Event Actions, page 40-23.

Understanding IPS Event Actions

When you configure an event action filter or override, or a signature, you specify an action for events that meet the rule. For signatures and overrides, you are specifying an action to add to the event; for filters, you are specifying an action to remove from the event.

The most common action is Produce Alert, which generates an alert that you can view in your network management system, such as the Security Manager Event Viewer or CS MARS. However, there are a wide variety of actions that you can assign to an event. When looking over the possible actions, keep the following in mind:

- Many actions produce alerts in addition to the other action performed. The description for each action explains whether an alert is also produced.
- Cisco IOS IPS supports fewer actions for event action override or filter rules. The actions supported are Deny Attacker Inline, Deny Connection Inline, Deny Packet Inline, Product Alert, and Reset TCP Connection.
- Not all actions are necessarily available on all combinations of IPS software version and device type. Whenever you need to select an action, only those actions that are valid are available for selection.
- For deny and block actions, use the event actions settings policy to set the period of time for which addresses or packets are denied. For more information, see Configuring Settings for Event Actions, page 40-23.

The following table explains the possible actions.

Table 40-1 IPS Event Actions

Menu Command	Description
Deny Attacker Inline	Terminates the current packet and future packets from this attacker address for a specified period of time. The IPS must be operating in inline mode. For Cisco IOS IPS devices, no connection can be established from the attacker to the router until the shun time expires. **Tip** This is the most severe of the deny actions. It denies current and future packets from a single attacker address. For IPS appliances and service modules, you can use the IPS Device Manager to see a list of denied attackers and clear the list if necessary.
Deny Attacker/Service Pair Inline	Does not transmit this packet and future packets on the attacker address victim port pair for a specified period of time. The IPS must be operating in inline mode.
Deny Attacker/Victim Pair Inline	Does not transmit this packet and future packets on the attacker/victim address pair for a specified period of time. The IPS must be operating in inline mode.
Deny Connection Inline	Terminates the current packet and future packets on this TCP flow. Other connections from the attacker can be established. The IPS must be operating in inline mode.
Deny Packet Inline	Terminates the packet. The IPS must be operating in inline mode. For Cisco IOS IPS devices, this action discards the packet without sending a reset. Cisco recommends using “drop and reset” in conjunction with alarm. **Tip** For IPS appliances and service modules, there is an event action override that adds this action to high risk events. You cannot delete the override. If you do not want to use it, disable the override. For more information, see Configuring Event Action Overrides, page 40-13.
Log Attacker Packets	Starts IP logging on packets that contain the attacker address and sends an alert. This action causes an alert to be written to the Event Store, even if Produce Alert is not selected.
Log Pair Packets	Starts IP Logging on packets that contain the attacker/victim address pair. This action causes an alert to be written to the Event Store, even if Produce Alert is not selected.
Log Victim Packets	Starts IP Logging on packets that contain the victim address and sends an alert. This action causes an alert to be written to the Event Store, even if Produce Alert is not selected.
Modify Packet Inline	Modifies packet data to remove ambiguity about what the endpoint might do with the packet. **Tip** This option is not available for event action override or filter rules. It is available in signatures.

Table 40-1 IPS Event Actions (continued)

Menu Command	Description
Product Alert	Writes the event to the Event Store as an alert. For Cisco IOS IPS devices, the notification is sent through syslog or SDEE. **Note** A Produce Alert event action is added for an event when global correlation has increased the risk rating of an event, and has added either the Deny Packet Inline or Deny Attacker Inline event action.
Produce Verbose Alert	Includes an encoded dump of the offending packet in the alert. This action causes an alert to be written to the Event Store, even if Produce Alert is not selected.
Request Block Connection	Sends a request to block this connection. You must have blocking devices configured to implement this action. For more information, see Configuring IPS Blocking and Rate Limiting, page 43-7.
Request Block Host	Sends a request to block this attacker host. You must have blocking devices configured to implement this action.
Request Rate Limit	Sends a rate limit request to perform rate limiting. You must have rate limiting devices configured to implement this action.
Request SNMP Trap	Requests that the sensor send an SNMP trap notification to the configured trap destinations. This action causes an alert to be written even if Produce Alert is not selected. You must have SNMP configured on the sensor for traps to actually be sent. For more information, see Configuring SNMP, page 36-8.
Reset TCP Connection	Sends TCP resets to hijack and terminate the TCP flow, sending a reset to both the source and destination addresses. Reset TCP Connection works only on TCP signatures that analyze a single connection, for example, half-open SYN attacks. It does not work for sweeps or floods.

Related Topics

- Configuring Event Action Filters, page 40-4
- Configuring Event Action Overrides, page 40-13
- Configuring Signatures, page 39-4

Configuring Event Action Filters

You can configure event action filters to remove specific actions from an event or to discard an entire event and prevent further processing by the sensor.

Filters let the sensor perform certain actions in response to the event without requiring the sensor to perform all actions or remove the entire event. Filters work by removing actions from an event. A filter that removes all actions from an event effectively consumes the event. Before configuring filter rules, read Tips for Managing Event Action Filter Rules, page 40-6.

Note When filtering sweep signatures, we recommend that you do not filter the destination addresses. If there are multiple destination addresses, only the last address is used for matching the filter.

Related Topics

- Understanding the IPS Event Action Process, page 40-1

Step 1 Do one of the following to open the Event Action Filters policy:

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

The table shows the existing filter rules organized into sections. The Local section is for rules defined specifically for a selected device (in Device view). For shared or inherited policies, there are also sections for mandatory and default rules. For more information about the contents of this policy, see Event Action Filters Page, page 40-7.

Step 2 Select the row after which you want to create the filter rule and click the **Add Row** button or right-click and select **Add Row**. This opens the Add Filter Item dialog box. For detailed information about the options in this dialog box, see Filter Item Dialog Box, page 40-9.

Tips

- If you do not select a row, the new rule is added at the end of the local scope.
- You can also select an existing row and edit either the entire row (by clicking the **Edit Row** button) or specific cells. To edit a specific cell, right-click the cell and select the **Edit** command related to the cell from the top of the context menu.
- You can delete a rule by selecting it and clicking the **Delete Row** button.
- You can export the entire list of filter rules to a comma-separated values (CSV) file. Click **Export to File**, navigate to an appropriate folder on the Security Manager server, change the file name if you do not like the default name, and click **Save**.

Step 3 Configure the filter rule. Following are the highlights of what you typically need to configure. For specific information on configuring the fields, and for information on fields not mentioned here, see Filter Item Dialog Box, page 40-9.

- Name—You must enter a name for the rule. Use a name that is meaningful to you.
- Signature, Subsignature ID—If the filter should apply to all signatures, use the default values. If you are targeting a specific signature, enter its signature and subsignature identifiers. You can obtain these values by finding the signature in the Signatures policy (see Signatures Page, page 39-4).
- Attacker and Victim Addresses and Ports—If the filter should apply no matter who is attacking, or who is the victim, use the default values. If you are creating a filter specific to an attacker or victim, update these fields to match the appropriate address and port.
- Risk Rating—You are most likely to want to change this value. The filter is applied to events that are within the minimum-maximum range you configure here. The default value, 0-100, will apply the filter rule to all events. If you configure a specific signature ID, the rating applies only to events for that signature (in which case the default risk rating might be acceptable).

  For example, you might want to target only high-risk events, such as 90-100.
- Actions to Subtract—Select the actions that you want to subtract from the event. Use Ctrl+click to select more than one action. If you select an action that is not actually assigned to an event, the filter rule essentially has no effect on the event. For more information about the actions, see Edit, Add, Replace Action Dialog Boxes, page 39-12.

- Stop on Match—Whether to define this filter rule as a stop rule. This setting determines how the remaining rules in the event action filter rules table are processed:
  - If you select this option, and an event meets the conditions of the rule, this rule is the final rule tested for the event. The actions identified by this rule are removed from the event, and the device moves on to perform all remaining actions assigned to the event.
  - If you do not select this option, then events that meet the conditions of this filter rule are also compared to subsequent rules in the event actions filters table. Subsequent rules are tested until either all rules are tested, or the event matches a stop rule.

Click **OK** when you are finished defining your filter rule.

Step 4 If you did not select the right row before adding the rule, select the new rule and use the up and down arrow buttons to position the rule appropriately. Ensure that stop rules are placed after other rules that you want applied prior to the stop.

Tips for Managing Event Action Filter Rules

Following are some tips that might help you effectively manage your event action filter rules:

- Disabled rules are shown with hash marks covering the table row. To change the enabled/disabled status of a rule, right click the rule and select **Enable** or **Disable** as appropriate. You can also change the status when editing the rule.

  Disabling a rule is useful if you want to stop using the rule, but you might want to start using it again in the future. Disabled rules remain in the table so that you do not need to recreate them.

- For existing rules, you can edit most of the fields directly from the event actions filter rules table by right-clicking the cell and selecting the appropriate Edit command from the top portion of the context menu. For example, you can right click the Attacker Ports cell and select **Edit Attacker Ports**.

  Many of these right-click commands open a version of the Edit Filter Item dialog box that contains only the selected property. Other commands simply change a value, or open a sub-menu from which you can select a value to add or remove. For example, right-clicking the Action cell provides four commands:
  - **Add to Actions**—Select from a list of actions to add to those already defined in the rule.
  - **Delete from Actions**—Select from a list of actions defined in the rule to remove from the rule.
  - **Replace Actions With**—Select from a list the action that you want to completely replace those defined in the rule.
  - **Edit Actions**—Opens a dialog box where you can select all actions for the rule. Your selection replaces the cell contents.

- Although filter rules are configured as an ordered list, the rules are not processed as a “first match wins” list, even through they are processed and applied top to bottom. Instead, each rule has a Stop property: the rule is either a stop rule or it is not a stop rule. Processing ends only if an event matches a stop rule. If an event matches a non-stop rule, the event is compared to subsequent filter rules. Thus, more than one filter rule can apply to an event. If you decide to create stop rules, ensure that you place them below all other rules that you want processed for an event.

  If you define no stop rules, each event is compared to all filter rules, and all matching rules are applied to the event in top-to-bottom order.

- You can inherit event action filter rules policies. Thus, you could configure a shared policy in Policy view that includes filter rules that you want to share among all of your devices, inherit that rule for each device (in Device view), and in Device view configure local filter rules that are unique to each device. For more information on inheriting policies, see:
  - Creating a New Shared Policy, page 5-54
  - Inheritance vs. Assignment, page 5-6
  - Inheriting or Uninheriting Rules, page 5-47

Related Topics

- Configuring Event Action Filters, page 40-4
- Event Action Filters Page, page 40-7

Event Action Filters Page

Use the Event Actions Filters page to configure event action filter rules. Filter rules can remove specific actions from an event or they can discard an entire event and prevent further processing by the sensor.

Event action filters are processed as an ordered list and you can move filters up or down in the list. Filters let the sensor perform certain actions in response to the event without requiring the sensor to perform all actions or remove the entire event. Filters work by removing actions from an event. A filter that removes all actions from an event effectively consumes the event.

Before configuring event action filter rules, read the following topics:

- Configuring Event Action Filters, page 40-4
- Tips for Managing Event Action Filter Rules, page 40-6
- Understanding the IPS Event Action Process, page 40-1

Tip Disabled rules are shown with hash marks covering the table row. To change the enabled/disabled status of a rule, right click the rule and select **Enable** or **Disable** as appropriate. You can also change the status when editing the rule.

Navigation Path

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

Field Reference

Table 40-2 Event Action Filters Page

Element	Description
Name	The name of the filter rule.
Active	Whether the signature is active. This cell is not available for Cisco IOS IPS policies.

Table 40-2 Event Action Filters Page (continued)

Element	Description
IDs	The signature identifiers to which this rule applies.
Subs	The subsignature identifiers.
Attackers	The IP address of the attacker that triggers the filter rule, which can be a host address, an address range (such as 0.0.0.0-255.255.255.255 in the case of IPv4 or ::0-FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF in the case of IPv6), or a network/host policy object. **Tip** If you use a network/host object, you can see the contents of the object by right-clicking it and selecting **Show Contents**. **Note** Do not create an IPv4 object and an IPv6 object with the same name; doing so leads to deployment failure.
Attack Ports	The port used by the attacker host that triggers the filter.
Victims	The IP address of the victim that triggers the filter rule, which can be a host address, an address range (such as 0.0.0.0-255.255.255.255 in the case of IPv4 or ::0-FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF in the case of IPv6), or a network/host policy object. **Tip** If you use a network/host object, you can see the contents of the object by right-clicking it and selecting **Show Contents**. **Note** Do not create an IPv4 object and an IPv6 object with the same name; doing so leads to deployment failure.
Victim Ports	The port targeted by the attacker host that triggers the filter.
Actions	The actions that should be removed from the event when the filter is triggered.
RR	The risk rating range that triggers this event action filter. For a detailed explanation of how risk rating is calculated, see Calculating the Risk Rating in *Installing and Using Cisco Intrusion Prevention System Device Manager 7.0* on Cisco.com.
Stop	Whether this is a stop rule. If Yes, then when an event meets the conditions of this rule, the filter is applied to the event but the event is not tested against the remaining rules in the event action filter rules policy.
Export to File button	Click this button to export the event action filters summary 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.

Table 40-2 Event Action Filters Page (continued)

Element	Description
Up Row and Down Row buttons (arrow icons)	Click these buttons to move the selected rules up or down within a scope. Filter rules are processed in order top to bottom for each event. If the conditions of an event match those defined for a filter, and the filter has the Stop field set to Yes, that filter is applied and no additional filters are considered. Ensure that stop rules are placed after the other rules you want applied to an event. You should order the more restrictive rules before general rules in the table.
Add Row button	Click this button to add a filter rule to the table after the selected row using the Add Filter Item dialog box (see Filter Item Dialog Box, page 40-9). If you do not select a row, the rule is added at the end of the local scope.
Edit Row button	Click this button to edit the selected rule. You can also edit individual cells by right-clicking the cell and selecting the appropriate Edit command.
Delete Row button	Click this button to delete the selected rule. **Tip** Instead of removing the rule, you can right-click the rule and select **Disable**. This prevents the rule from being used, but leaves it in the table in case you want to use it again at a later time.

Filter Item Dialog Box

Use the Add or Edit Filter Item dialog box to configure an event action filter rule.

Tip For existing rules, you can edit most of these fields directly from the event actions filter rules table by right-clicking the cell and selecting the appropriate command from the top portion of the context menu. For example, you can right click the Attacker Ports cell and select **Edit Attacker Ports**. Many of these right-click commands open a version of the Edit Filter Item dialog box that contains only the selected property. When seeking help for these context-editing dialog boxes, look for the property description in the table below.

Navigation Path

From the Event Action Filters page (see Event Action Filters Page, page 40-7), click the **Add Row** button, or select a filter rule and click the **Edit Row** button.

Related Topics

- Configuring Event Action Filters, page 40-4
- Tips for Managing Event Action Filter Rules, page 40-6

Field Reference

Table 40-3 Filter Item Dialog Box

Element	Description
Active Enabled (Active does not apply to Cisco IOS IPS devices.)	Whether the filter rule is active and enabled. Active means that the filter has been put into the filter list and will take effect on filtering events. The default is that the rule is both active and enabled, which means that the rule is used when events are processed. **Tips** • If a filter is active but not enabled, it will still be included in the ordering list; it will be processed, but it will not be used. • If a filter is not active, then it will not be included at all in the ordering of the filters; it will not be processed at all. • Disabled rules are shown in the event action filters table with cross-hatching.
Name	The name of the filter rule. The following characters are allowed in filter names: a-z, A-Z, 0-9, -, . (dot or period), : (colon), and _ (underscore).
Signature IDs	The numerical signature IDs to which the filter rule applies. You can enter a single signature ID, a comma-separated list, or a range of IDs. The default is to apply the rule to signatures in the range 900-65535.
SubSignature ID	The subsignature ID for the specified signature to which the filter rule applies. The subsignature ID identifies a more granular version of a broad signature, but it is not used for all signatures. Enter a subsignature ID appropriate for the signature ID you specified, or enter a range of subsignature IDs. The default value is the range of 0-255.
Attacker IPv4 Address	The IP address of the host that sent the offending packet. You can specify a single host IP address, a range of addresses, or the name of a network/host policy object that identifies the address or address range. Click **Select** to select a network/host object from a list or to create a new object. **Note** Do not create an IPv4 object and an IPv6 object with the same name; doing so leads to deployment failure. The default value is a range of all IPv4 addresses (0.0.0.0-255.255.255.255).
Attacker IPv6 Address	The IP address of the host that sent the offending packet. You can specify a single host IP address, a range of addresses, or the name of a network/host policy object that identifies the address or address range. Click **Select** to select a network/host object from a list or to create a new object. **Note** Do not create an IPv4 object and an IPv6 object with the same name; doing so leads to deployment failure. The default value is a range of all IPv6 addresses (::0-FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF).

Table 40-3 Filter Item Dialog Box (continued)

Element	Description
Attacker Port	The port used by the attacker host. This is the port from which the offending packet originated. You can also enter a range of ports. The default value is a range of all ports (0-65535).
Victim IPv4 Address	The IP address of the host being attacked (the recipient of the offending packet). You can specify a single host IP address, a range of addresses, or the name of a network/host policy object that identifies the address or address range. Click **Select** to select a network/host object from a list or to create a new object. **Note** Do not create an IPv4 object and an IPv6 object with the same name; doing so leads to deployment failure. The default value is a range of all IPv4 addresses (0.0.0.0-255.255.255.255).
Victim IPv6 Address	The IP address of the host being attacked (the recipient of the offending packet). You can specify a single host IP address, a range of addresses, or the name of a network/host policy object that identifies the address or address range. Click **Select** to select a network/host object from a list or to create a new object. **Note** Do not create an IPv4 object and an IPv6 object with the same name; doing so leads to deployment failure. The default value is a range of all IPv6 addresses (::0-FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF).
Victim Port	The port of the host being attacked (the recipient of the offending packet). This is the port to which the offending packet was sent. You can also enter a range of ports. The default value is a range of all ports (0-65535).
Risk Rating Min. and Max.	The risk rating range, between 0 and 100, that should be used to trigger this event action filter. The default value is the complete range (0-100). If an event occurs with a risk rating that falls within the minimum-maximum range you configure here, the event is processed against the rules of this event filter.
OS Relevance	Indicates whether the alert is relevant to the OS that has been identified for the victim. Possible values include one or more of the following: Not Relevant, Relevant, Unknown. Use Ctrl+click to select multiple values. The default is all values selected. **Note** OS Relevance is applicable only to appliances and service modules running IPS 6.x+ software. For Cisco IOS IPS devices, this field is read-only and cannot be edited, and for IPS 5.x devices, this field is blank.
Comments	The user comments associated with this filter, such as an explanation of the purpose of the rule.

Table 40-3 Filter Item Dialog Box (continued)

Element	Description
Actions to Subtract	The actions that should be removed from the event, should the conditions of the event meet the criteria of the event action filter. You can select one or more actions in this list box. All selected actions are removed from the event. Use Ctrl+click to select multiple values. For more information about the possible actions, see Edit, Add, Replace Action Dialog Boxes, page 39-12. For IOS IPS devices, the possible values are restricted to the following: • *Deny Attacker Inline* blocks the attacker's source IP address completely. No connection can be established from the attacker to the router until the shun time expires. You can configure this time in the Event Actions Settings policy as described in Configuring Settings for Event Actions, page 40-23. • *Deny Connection Inline* blocks the appropriate TCP flow from the attacker. Other connections from the attacker can be established to the router. • *Deny Packet Inline* discards the packet without sending a reset. Cisco recommends using "drop and reset" in conjunction with alarm. • *Produce Alert* sends a notification about the attack through syslog or SDEE. • *Reset TCP Connection* is effective for TCP-based connections and sends a reset to both the source and destination addresses. For example, in case of a half-open SYN attack, Cisco IOS IPS can reset the TCP connections.
% to Deny	The percentage of packets to deny for deny attacker features. The range is 0 to 100. The default is 100 percent. **Note** For IOS IPS devices, this field is read only and cannot be edited.
Stop on Match	Whether to define this filter rule as a stop rule. This setting determines how the remaining rules in the event action filter rules table are processed: • If you select this option, and an event meets the conditions of the rule, this rule is the final rule tested for the event. The actions identified by this rule are removed from the event, and the device moves on to perform all remaining actions assigned to the event. • If you do not select this option, then events that meet the conditions of this filter rule are also compared to subsequent rules in the event actions filters table. Subsequent rules are tested until either all rules are tested, or the event matches a stop rule.

Configuring Event Action Overrides

You can add an event action override to change the actions associated with an event based on the risk rating of that event. Event action overrides are a way to add event actions globally without having to configure each signature individually.

Each event action has an associated risk rating range. If a signature event occurs and the risk rating for that event falls within the range for an event action, that action is added to the event. For example, if you want any event with a risk rating of 85 or more to generate an SNMP trap, you can create an event action override for Request SNMP Trap with the risk rating 85-100.

Tip If you want to prevent the use of action overrides, you can disable the entire event action override component as described in Configuring Settings for Event Actions, page 40-23.

Related Topics

- Understanding the IPS Event Action Process, page 40-1

Step 1 Do one of the following to open the Event Action Overrides policy:

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

The table shows the existing overrides, including the action, the risk rating of the alerts the action will be added to, and whether the rule is enabled. The order of the rules does not matter: all overrides that apply to an alert add the associated actions.

The table can have at most a single entry for each possible action.

Step 2 Configure the desired overrides:

- To add a new override, click the **Add Row (+)** button beneath the table and fill in the Add Event Action Rule dialog box. In the dialog box, select the action you want to add, enter the rating range of the alerts to which you are adding the action (for example, 90-100), and click **OK**. For more information, see Add or Edit Event Action Rule Dialog Box, page 40-14.

  The risk rating range must be between 0 and 100. Separate the low and high of the range with a hyphen, for example, 80-90.

  When adding a new override, you can define your own risk rating, or you can use a pre-defined Risk Rating policy object; beginning with Version 4.5, Security Manager has several pre-defined Risk Rating policy objects:

  - Extreme Risk (90-100)
  - High Risk (76-90)
  - Medium-High Risk (61-75)
  - Medium Risk (46-60)
  - Medium-Low Risk (30-45)
  - Low Risk (16-30)
  - Very Low Risk (1-15)

For more information on these pre-defined policy objects, refer to Configuring Risk Rating Policy Objects, page 40-15.

These pre-defined policy objects cannot be edited, but you can add and edit any of your own policy objects that you have defined.

- To edit an override, to disable it or to change the risk rating, select the override and click the **Edit Row (pencil)** button. You cannot change the event action.

  Note Re-discovery of an IPS device will replace the Risk Rating policy object's value with its inline value. For example, if you assign the High Risk policy object (80-89) to any of the event actions and deploy it to the device, then after re-discovery that policy object's value will be replaced with its inline value of 80-89.

- To remove an override, select it and click the **Delete Row** button.

  Note Policies for IPS appliances and service modules include a default override for Deny Packet Inline, which you cannot delete. If you do not want to use that override, disable it.

- To export the entire list of overrides to a comma-separated values (CSV) file, click **Export to File**, navigate to an appropriate folder on the Security Manager server, change the file name if you do not like the default name, and click **Save**.

Add or Edit Event Action Rule Dialog Box

Use the Add or Edit Event Action Rule dialog box to add an event action rule based on one of the pre-defined Risk Rating policy objects that are available in Security Manager beginning with Version 4.5.

Navigation Path

From the Event Action Overrides policy, click the **Add Row** button beneath the overrides table, or select a row in the table and click the **Edit Row** button. For information on opening the Event Action Overrides policy, see Configuring Event Action Overrides, page 40-13.

Field Reference

Table 40-4 Add or Edit Event Action Rule Dialog Box

Element	Description
Risk Rating	One of several pre-defined Risk Rating policy objects that are available in Security Manager beginning with Version 4.5: • Extreme Risk (90-100) • High Risk (76-90) • Medium-High Risk (61-75) • Medium Risk (46-60) • Medium-Low Risk (30-45) • Low Risk (16-30) • Very Low Risk (1-15) For more information on using one of these pre-defined Risk Rating policy objects, or defining your own, refer to Configuring Event Action Overrides, page 40-13.
Assigned	Whether a particular action is assigned to at least one of the Risk Rating policy objects.
Action Name	The action to be taken for a particular Risk Rating when assigned.
Enabled	Whether a particular action is enabled. Deselect this option to temporarily disable an action without deleting it.

Configuring Risk Rating Policy Objects

Use the Risk Rating Policy Object Dialog Box to configure policy objects for IPS. Seven pre-defined policy objects are available for risk rating; you can also define your own.

Navigation Path

Select **Manage > Policy Objects > All Object Types**, then select **Risk Rating** from the Object Type selector. Right-click inside the work area, then select **New Object** or right-click a row and select **Edit Object**. You cannot edit the pre-defined policy objects, however.

Depending upon whether you selected **New Object** or **Edit Object**, the Add Risk Rating or Edit Risk Rating dialog box appears: refer to Add or Edit Event Action Rule Dialog Box, page 40-14

The remainder of this topic describes the fields that you see in the Risk Rating Policy Object dialog box.

Related Topics

- Configuring Event Action Overrides, page 40-13
- Add or Edit Event Action Rule Dialog Box, page 40-14

Field Reference

Table 40-5 Risk Rating Policy Object Dialog Box

Element	Description
Name	The name of a pre-defined policy object, such as "High Risk," or the name of a policy object that you have defined.
Range	The Risk Rating of a particular policy object, expressed as a numerical range.
Category	Allows you to select Cat-A through Cat-G. This is the category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Overrides	Whether any IPS event action overrides have been configured for this policy object
Description	A text description that you can provide; applies to policy objects that you have defined, not to pre-defined policy objects.
Last Ticket(s)	The last ticket used for this policy object.
Last Modified Date	The last date on which this policy object was modified.

Add or Edit Risk Rating Dialog Box

Use the Add or Edit Risk Rating dialog box to define policy objects for IPS Risk Rating.

Navigation Path

Select **Manage > Policy Objects > All Object Types**, then select **Risk Rating** from the Object Type selector. Right-click inside the work area, then select **New Object** or right-click a row and select **Edit Object**. You cannot edit the pre-defined policy objects, however.

Related Topics

- Configuring Event Action Overrides, page 40-13
- Add or Edit Event Action Rule Dialog Box, page 40-14

Field Reference

Table 40-6 Add or Edit Risk Rating Dialog Box

Element	Description
Name	The name of a pre-defined policy object, such as "High Risk," or the name of a policy object that you have defined.
Description	A text description that you can provide; applies to policy objects that you have defined, not to pre-defined policy objects.
Range	The Risk Rating of a particular policy object, expressed as a numerical range.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.

Table 40-6 Add or Edit Risk Rating Dialog Box (continued)

Element	Description
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

Configuring IPS Event Action Network Information

Use the Event Actions Network Information policy to configure these features:

- **Target value ratings (IPv4 Target Value Ratings tab and IPv6 Target Value Ratings tab)**—You can configure the target value ratings of your network assets. The sensor uses these ratings when calculating the overall risk rating of an alert. By identifying your mission-critical assets, you can trigger more severe signature event actions. As the names indicate, you can use IPv4 or IPv6 by selecting the appropriate tab.

  Target value rating is available on IPS appliances, service modules, and Cisco IOS IPS devices.

  For more information, see Configuring Target Value Ratings, page 40-17.

- **Passive OS fingerprinting and OS mappings (OS Identification tab)**—You can enable the sensor to use information about the operating system running on a device to determine the attack relevance rating, which is a component of the overall risk rating.

  Passive OS fingerprinting and OS mappings are available on devices running IPS 6.x+ software only, and are not available on Cisco IOS IPS devices.

  For more information, see:

  - Understanding Passive OS Fingerprinting, page 40-19
  - Configuring OS Identification (Cisco IPS 6.x and Later Sensors Only), page 40-21

To open the Network Information policy, do one of the following:

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

Configuring Target Value Ratings

You can assign target value ratings to your network assets. The target value rating is one of the factors used to calculate the risk rating value for each alert. It identifies the perceived importance of a network asset, which you identify by its IP address.

You can develop a security policy that is more stringent for valuable corporate resources and looser for less important resources. For example, you could assign a target value rating to the company web server that is higher than the target value rating you assign to a desktop node. In this example, attacks against the company web server have a higher risk rating than attacks against the desktop node. Events with a higher risk rating trigger more severe signature event actions.

You can configure four value ratings. From highest value to lowest: Mission Critical, High, Medium, Low, No Value (zero value).

For a detailed explanation of how risk rating is calculated, see Calculating the Risk Rating in *Installing and Using Cisco Intrusion Prevention System Device Manager 7.0* on Cisco.com.

Tip If you are configuring target value ratings on a device that uses IPS 6.0 software lower than 6.0(5), you might also want to update the OS Identification tab of the Network Information policy to get around a software bug, even if you do not need to create OS maps. For detailed information, see Configuring OS Identification (Cisco IPS 6.x and Later Sensors Only), page 40-21.

Related Topics

- Configuring IPS Event Action Network Information, page 40-17
- Understanding the IPS Event Action Process, page 40-1

Step 1 Do one of the following to open the Network Information policy:

- (Device view) Select **IPS > Event Actions > Network Information** from the Policy selector, then click the **IPv4 Target Value Ratings** tab or the **IPv6 Target Value Ratings** tab.
- (Policy view, IPS appliances and service modules) Select **IPS > Event Actions > Network Information**, then select an existing policy or create a new one. Click the **IPv4 Target Value Ratings** tab or the **IPv6 Target Value Ratings** tab.
- (Policy view, Cisco IOS IPS devices) Select **IPS (Router) > Event Actions > Network Information**, then select an existing policy or create a new one. Click the **IPv4 Target Value Ratings** tab.

Note Cisco IOS IPS devices do not support IPv6.

The tab shows the target value ratings that are already configured, showing the IP addresses associated with each configured ratings category. The table can have at most five entries, one per rating category.

Step 2 Configure the desired target value ratings categories:

- To add a new ratings category, click the **Add Row (+)** button beneath the table and fill in the Add Target Value Rating dialog box. In the dialog box, select the rating you want to add, enter the host, network, and address ranges to associate with the category, and click **OK**. For more information, see Target Value Rating Dialog Box, page 40-19.

  For IPv4 addresses, you can specify a single network/host object, or a comma-separated list of host, network, or address ranges, such as 10.10.10.10, 10.10.10.0/24, or 10.10.10.2-10.10.10.254. Addresses that you enter in the network format are converted to address ranges. For IPv6 addresses, use IPv6 addressing conventions.
- To edit the IP addresses in an existing ratings category, select the category and click the **Edit Row (pencil)** button. You cannot change the value rating.

- To remove a rating, select it and click the **Delete Row** button.

Target Value Rating Dialog Box

Use the Add or Edit Target Value Rating dialog box to associate the IP addresses of your assets to a ratings category. IP addresses are IPv4 when you open the Target Value Rating dialog box from the IPv4 Target Value Ratings tab; they are IPv6 from the IPv6 tab.

Navigation Path

From the IPv4 Target Value Rating tab or the IPv6 Target Value Rating tab of the IPS Event Actions Network Information policy, click the **Add Row** button beneath the Target Value Ratings table, or select a row in the table and click the **Edit Row** button. For information on opening the IPv4 Target Value Rating tab or the IPv6 Target Value Rating tab, see Configuring Target Value Ratings, page 40-17.

Field Reference

Table 40-7 Target Value Rating Dialog Box

Element	Description
Value	The target value rating to associate with the specified addresses. From highest to lowest importance: Mission Critical, High, Medium, Low, No Value. This list includes only those value ratings that you have not already configured in the target value ratings table. You change this option when editing a ratings category.
target-address	The IP addresses of the network assets assigned to this value rating. You can specify addresses using the following techniques: • Enter the name of a single network/host object, or click **Select** to select an object from a list or to create a new one. The object can contain a group of networks, hosts, and address ranges. • A comma-separated list of host or network addresses or address ranges. For example, using IPv4, 10.10.10.0/24, 10.10.10.10, 10.10.10.2-10.10.10.254. Addresses that you enter in the network format are converted to address ranges; for example, 10.10.10.0/24 is converted to 10.10.10.0-10.10.10.255.

Understanding Passive OS Fingerprinting

Passive operating system (OS) fingerprinting is enabled by default on IPS 6.0+ sensors and the IPS contains a default vulnerable OS list for each signature.

Passive OS fingerprinting lets the sensor determine the OS that hosts are running. The sensor analyzes network traffic between hosts and stores the OS of these hosts with their IP addresses. The sensor inspects TCP SYN and SYNACK packets exchanged on the network to determine the OS type.

The sensor then uses the OS of the target host OS to determine the relevance of the attack to the victim by computing the attack relevance rating component of the risk rating. Based on the relevance of the attack, the sensor may alter the risk rating of the alert for the attack or the sensor may filter the alert for

the attack. You can then use the risk rating to reduce the number of false positive alerts (a benefit in IDS mode) or definitively drop suspicious packets (a benefit in IPS mode). Passive OS fingerprinting also enhances the alert output by reporting the victim OS, the source of the OS identification, and the relevance to the victim OS in the alert.

Passive OS fingerprinting consists of three components:

- Passive OS learning.

  Passive OS learning occurs as the sensor observes traffic on the network. Based on the characteristics of TCP SYN and SYNACK packets, the sensor makes a determination of the OS running on the host of the source IP address.

- User-configurable OS identification.

  You can configure OS host mappings, which take precedence over learned OS mappings.

- Computation of attack relevance rating and risk rating.

  The sensor uses OS information to determine the relevance of the attack signature to the targeted host. The attack relevance is the attack relevance rating component of the risk rating value for the attack alert.

There are three sources of OS information. The sensor ranks the sources of OS information in the following order:

1. Configured OS mappings—OS mappings that you enter on the OS Identification tab of the Event Actions Network Information policy. You can configure different mappings for each virtual sensor. For more information, see Configuring OS Identification (Cisco IPS 6.x and Later Sensors Only), page 40-21.

   We recommend configuring OS mappings to define the identity of the OS running on critical systems. It is best to configure OS mappings when the OS and IP address of the critical systems are unlikely to change.

2. Imported OS mappings—OS mappings imported from Management Center for Cisco Security Agents (CSA MC).

   Imported OS mappings are global and apply to all virtual sensors. For information on configuring the sensor to use CSA MC, see Configuring the External Product Interface, page 36-26.

3. Learned OS mappings—OS mappings observed by the sensor through the fingerprinting of TCP packets with the SYN control bit set.

   Learned OS mappings are local to the virtual sensor that sees the traffic.

When the sensor needs to determine the OS for a target IP address, it consults the configured OS mappings. If the target IP address is not in the configured OS mappings, the sensor looks in the imported OS mappings. If the target IP address is not in the imported OS mappings, the sensor looks in the learned OS mappings. If it cannot find it there, the sensor treats the OS of the target IP address as unknown.

Tip You can configure Event Action Filter rules to use the OS relevancy value of the target, and configure signatures to identify the OSes vulnerable to a signature.

Configuring OS Identification (Cisco IPS 6.x and Later Sensors Only)

Use the OS Identification tab on the Event Actions Network Information policy to configure operating system (OS) host mappings, which take precedence over learned OS mappings. On the OS Identifications tab you can add, edit, and delete configured OS maps. You can move them up and down in the list to change the order in which the sensor computes the attack relevance rating and risk rating for that particular IP address and OS type combination.

Note OS Identification applies to IPS 6.0+ sensors only and does not apply to Cisco IOS IPS devices.

You can also move them up and down in the list to change the order in which the sensor resolves the OS associated with a particular IP address. Configured OS mappings allow for ranges, so for network 192.168.1.0/24 you might define the following:

IP Address Range Set	OS
192.168.1.1	IOS
192.168.1.2-192.168.1.10,192.168.1.25	UNIX
192.168.1.1-192.168.1.255	Windows

More specific mappings should be at the beginning of the list. Overlap in the IP address range sets is allowed, but the entry closest to the beginning of the list takes precedence.

Tip There is a bug in IPS 6.0 versions lower than 6.0(5) related to the Network Information policy. Even if you change nothing on the OS Identification tab, but you make configuration changes to the Threat Value Ratings tab, Security Manager configures the device to use the **any** variable for restricting OS mappings to addresses. This can result in your monitoring application showing “any” as the event locality for all events. The solution is to upgrade the IPS version on your sensor. The workaround is to enter a non-default value in the **Restrict to these IP Addresses** field on the OS Identification tab, even if you are not configuring specific OS mappings. For example, enter 0.0.0.1-255.255.255.255 instead of “any” or 0.0.0.0-255.255.255.255.

Navigation Path

- (Device view) Select **IPS > Event Actions > Network Information** from the Policy selector, then click the **OS Identification** tab.
- (Policy view, IPS appliances and service modules) Select **IPS > Event Actions > Network Information**, then select an existing policy or create a new one. Click the **OS Identification** tab.

Related Topics

- Configuring IPS Event Action Network Information, page 40-17
- Understanding the IPS Event Action Process, page 40-1

Field Reference

Table 40-8 OS Identification Tab

Element	Description
Enable Passive OS Fingerprinting	When selected, lets the sensor perform passive OS analysis. You must enable this option for any of the maps configured on this page to be used. Passive OS fingerprinting functions as part of the sensor. As the sensor analyzes network traffic between hosts, the sensor stores the identity of the OS running on the hosts alongside the IP addresses of the hosts. The sensor determines the identity of the OSes on the hosts by inspecting characteristics of the packets exchanged on the network. The sensor then uses the target system's OS information to compute the ARR (Attack Relevance Rating) component for the RR (Risk Rating). The RR can then be used to drop suspicious packets. For more information about passive OS fingerprinting, see Understanding Passive OS Fingerprinting, page 40-19.
Restricted to these IP Addresses	Restricts attack relevance rating calculation to the specified addresses. You can specify addresses using the following techniques: • Enter the name of a single network/host object, or click **Select** to select an object from a list or to create a new one. The object can contain a group of networks, hosts, and address ranges. • A comma-separated list of host or network addresses or address ranges. For example, 10.10.10.0/24, 10.10.10.10, 10.10.10.2-10.10.10.254.
OS Maps table	The list of OS mappings, showing the IP addresses of the hosts and the operating systems to which they are mapped. When looking for a match, the sensor goes from top to bottom and selects the first rule that matches the IP address. • To add a mapping, click the **Add Row** button and fill in the Add OS Map dialog box (see OS Map Dialog Box, page 40-22). • To edit a mapping, select the rule and click the **Edit Row** button. • To delete a map, select it and click the **Delete Row** button. • To change the priority of a rule, select it and click the **Up** or **Down** arrow buttons until the rule is positioned correctly.

OS Map Dialog Box

Use the Add or Edit OS Map dialog box to map a host through its IP address to an OS type. Create mappings only if you want to statically assign an OS type to an IP address. Because the sensor uses passive OS fingerprinting to discover the OS associated with an IP address, you might not want to create any mappings, or create mappings only for mission-critical devices that have static IP addresses. Update any mappings that you create if you install devices with different operating systems on the address.

Navigation Path

From the OS Identification tab of the IPS Event Actions Network Information policy, click the **Add Row** button beneath the OS Maps table, or select a row in the table and click the **Edit Row** button. For information on opening the OS Identification tab, see Configuring OS Identification (Cisco IPS 6.x and Later Sensors Only), page 40-21.

Field Reference

Table 40-9 OS Map Dialog Box

Element	Description
IP Addresses	The IP addresses for this mapping. You can specify addresses using the following techniques: • Enter the name of a single network/host object, or click **Select** to select an object from a list or to create a new one. The object can contain a group of networks, hosts, and address ranges. • A comma-separated list of host or network addresses or address ranges. For example, 10.10.10.0/24, 10.10.10.10, 10.10.10.2-10.10.10.254.
OS Type	The operating system running on the identified hosts. Select the most appropriate option from the list. You can select multiple options (using Ctrl+click) to indicate that there is more than one possible OS. **Tip** Because these mappings take precedence over learned mappings, you probably are better off not assigning General OS, Other, or Unknown OS. The sensor might be able to learn the actual OS through passive OS fingerprinting and provide a better matching. For more information, see Understanding Passive OS Fingerprinting, page 40-19.

Configuring Settings for Event Actions

Use the Event Actions Settings policy to configure general settings that apply globally to event action rules. The defaults for these options are appropriate for most situations, so change them only if you are certain that your situation requires non-default behavior.

To configure the Event Actions Settings policy, do one of the following:

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

The following table describes the options you can configure. Note that the options available for Cisco IOS IPS devices are more limited than those available for IPS appliances and service modules.

Tip Do not disable the Summarizer except for troubleshooting purposes. If you disable the Summarizer, every signature is set to Fire All with no summarization. Note that you do not need to change the state of the Meta Event Generator. Cisco has discontinued the use of Meta signatures, and they have all been retired.

Table 40-10 Event Actions Settings Policy

Element	Description
Enable Event Action Override (All device types.)	When selected, enables override rules as defined on the Event Action Overrides page. You can add an event action override to add actions to an event based on specific details about that event. For configuring override rules, see Configuring Event Action Overrides, page 40-13.
Enable Event Action Filters (All device types.)	When selected, enables the filter rules as defined on the Event Action Filters page. You can configure event action filters to remove specific actions from an event or to discard an entire event and prevent further processing by the sensor. For configuring event action filters rules, see Configuring Event Action Filters, page 40-4.
Enable Event Action Summarizer (IPS appliances and service modules only.)	When selected, enables the Summarizer component. The Summarizer groups events into a single alert, thus decreasing the number of alerts the sensor sends out. By default, the Summarizer is enabled. If you disable it, all signatures are set to Fire All with no summarization. If you configure individual signatures to summarize, this configuration is ignored when the Summarizer is not enabled. The Report Manager component of Cisco Security Manager reports events individually. The Event Viewer component of Cisco Security Manager displays alerts. As stated above, the Summarizer groups events into a single alert, thus decreasing the number of alerts the sensor sends out. **Tip** Cisco IPS Manager Express (IME) and Cisco Security Manager do not summarize events in precisely the same way.
Enable Meta Event Generator (IPS appliances and service modules only.)	Cisco recommends that you do not change the state of the Meta Event Generator. Cisco has discontinued the use of Meta signatures, and they have all been retired.

Table 40-10 Event Actions Settings Policy (continued)

Element	Description
Enable Threat Rating Adjustment (IPS appliances and service modules only.)	When selected, enables threat rating adjustment, which adjusts the risk rating. If disabled, risk rating is equal to threat rating. Available in sensors running IPS 6.0+ software only. The Threat Rating feature provides a single view of the threat environment of the network. Threat Rating minimizes alarms and events through a customized view that shows only events with a high Threat Rating value. The Threat Rating value is derived as follows: • Dynamic adjustment of event Risk Rating based on success of response action • If response action was applied, Risk Rating is deprecated (Threat Rating < Risk Rating) • If response action was not applied, Risk Rating remains unchanged (Threat Rating = Risk Rating) The result is a single value by which the threat risk is determined.
Deny Attacker Duration in seconds (All device types.)	The number of seconds to deny the attacker inline. The range is 0 to 518400. The default is 3600.
Block Attack Duration in minutes (IPS appliances and service modules only.)	The number of minutes to block a host or connection. The range is 0 to 10000000. The default is 30.
Maximum Number of Denied Attackers (IPS appliances and service modules only.)	Limits the number of denied attackers possible in the system at any one time. The range is 0 to 100000000. The default is 10000.
Enable One Way TCP Reset (IPS appliances and service modules only.)	When selected, enables a one-way TCP reset for deny packet inline actions for TCP-based alerts. Available only for sensors running IPS 6.1+ software. The one-way TCP reset operates for inline mode only and is an automatic addition to the deny packet inline actions. It sends a TCP reset to the victim of the alert, thus creating a black hole for the attacker and clearing the TCP resources of the victim. **Tips** • In inline mode, all packets entering or leaving the network must pass through the sensor. • An inline sensor denies packets for any alert with a risk rating of greater than or equal to 90. It also issues a one-way TCP reset on TCP alerts with a risk rating of greater than or equal to 90.