CHAPTER 7

Configuring Event Action Rules

This chapter explains how to configure event action rules. It contains the following sections:

Understanding Event Action Rules

Event action rules are a group of settings you configure for the event action processing component of the sensor. These rules dictate the actions the sensor performs when an event occurs.

The event action processing component is responsible for the following functions:

- Calculating the risk rating
- Adding event action overrides
- Filtering event action
- Executing the resulting event action
- Summarizing and aggregating events
- Maintaining a list of denied attackers

This section contains the following topics:

Calculating the Risk Rating

An RR is a value between 0 and 100 that represents a numerical quantification of the risk associated with a particular event on the network. The calculation takes into account the value of the network asset being attacked (for example, a particular server), so it is configured on a per-signature basis (ASR and SFR) and on a per-server basis (TVR).

RRs let you prioritize alerts that need your attention. These RR factors take into consideration the severity of the attack if it succeeds, the fidelity of the signature, and the overall value of the target host to you. The RR is reported in the evIdsAlert.

The following values are used to calculate the RR for a particular event:

- Attack Severity Rating (ASR)—A weight associated with the severity of a successful exploit of the vulnerability.

  The ASR is derived from the alert severity parameter of the signature.

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

  SFR is calculated by the signature author on a per-signature basis. The signature author defines a baseline confidence ranking for the accuracy of the signature in the absence of qualifying intelligence on the target. It represents the confidence that the detected behavior would produce the intended effect on the target platform if the packet under analysis were allowed to be delivered. For example, a signature that is written with very specific rules (specific regular expression) has a higher SFR than a signature that is written with generic rules.

- Target Value Rating (TVR)—A weight associated with the perceived value of the target.

  TVR is a user-configurable value that identifies the importance of a network asset (through 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 TVR to the company web server that is higher than the TVR you assign to a desktop node. In this example, attacks against the company web server have a higher RR than attacks against the desktop node.

Note RR is a product of ASR, SFR, and TVR with an optional PD (promiscuous delta) subtracted in promiscuous mode only.

Event Overrides

You can add an event action override to change the actions associated with an event based on the RR 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 RR range. If a signature event occurs and the RR 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 an RR of 85 or more to generate an SNMP trap, you can set the RR range for Request SNMP Trap to 85-100. If you do not want to use action overrides, you can disable the entire event action override component.

Event Action Filters

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.

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.

Caution Event action filters based on source and destination IP addresses do not function for the Sweep engine, because they do not filter as regular signatures. To filter source and destination IP addresses in sweep alerts, use the source and destination IP address filter parameters in the Sweep engine signatures.

Event Action Summarization and Aggregation

This section explains how event actions are summarized and aggregated. It contains the following topics:

Event Action Summarization

Summarization decreases the volume of alerts sent out from the sensor by providing basic aggregation of events into a single alert. Special parameters are specified for each signature and they influence the handling of the alerts. Each signature is created with defaults that reflect a preferred normal behavior. However, you can tune each signature to change this default behavior within the constraints for each engine type.

The non-alert generating actions (deny, block, TCP reset) go through the filters for each signature event unsummarized. The alert-generating actions are not performed on these summarized alerts; instead the actions are applied to the one summary alert and then put through the filters.

If you choose one of the other alert-generating actions and do not have it filtered out, the alert is created even if you do not choose Produce Alert. To prevent alerts from being created, you must have all alert-generating actions filtered out.

Summarization and event actions are processed after the META engine has processed the component events. This lets the sensor watch for suspicious activity transpiring over a series of events.

Event Action Aggregation

Basic aggregation provides two operating modes. The simple mode involves configuring a threshold number of hits for a signature that must be met before the alert is sent. A more advanced mode is timed-interval counting. In this mode, the sensor tracks the number of hits per second and only sends alerts when that threshold is met. In this example, a *hit* is a term used to describe an event, which is basically an alert, but it is not sent out of the sensor as an alert until the threshold number of hits has been exceeded.

You can choose from the following summarization options:

- Fire All—Fire All mode fires an alert each time the signature is triggered. If the threshold is set for summarization, the following happens: Alerts are fired for each execution until summarization occurs. After summarization starts only one alert every summary interval fires for each address set. Alerts for other address sets are either all seen or separately summarized. The signature reverts to Fire All mode after a period of no alerts of that signature.
- Summary—Summary mode fires an alert the first time a signature is triggered, and then additional alerts for that signature are summarized for the duration of the summary interval. Only one alert every summary interval should fire for each address set. If the global summary threshold is reached, the signature goes into Global Summarization mode.
- Global Summarization—Global Summarization mode fires an alert for every summary interval. Signatures can be preconfigured for global summarization.
- Fire Once—Fire Once mode fires an alert for each address set. You can upgrade this mode to Global Summarization mode.

Signature Event Action Processor

SEAP coordinates the data flow from the signature event in the alarm channel to processing through the SEAO, the SEAF, and the SEAH. It consists of the following components:

- Alarm channel

  The unit that represents the area to communicate signature events from the Sensor App inspection path to signature event handling.

- Signature event action override (SEAO)

  Adds actions based on the RR value. SEAO applies to all signatures that fall into the range of the configured RR threshold. Each SEAO is independent and has a separate configuration value for each action type. For more information, see Calculating the Risk Rating, page 7-2.

- Signature event action filter (SEAF)

  Subtracts actions based on the signature event's signature ID, addresses, and RR. The input to the SEAF is the signature event with actions possibly added by the SEAO.

  Note The SEAF can only subtract actions, it cannot add new actions.

  The following parameters apply to the SEAF:

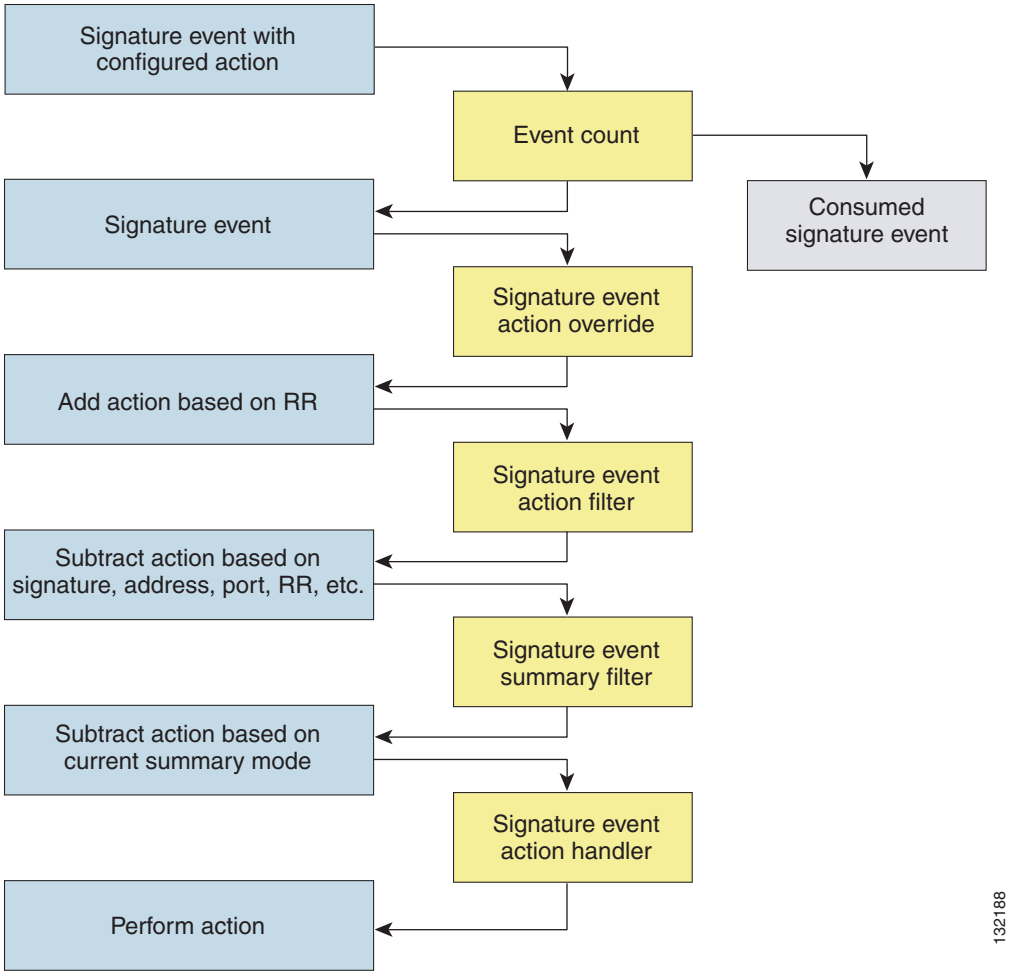
  - Signature ID
  - Subsignature ID
  - Attacker address
  - Attacker port
  - Victim address
  - Victim port
  - RR threshold range
  - Actions to subtract
  - Sequence identifier (optional)

  - Stop-or-continue bit
  - Enable action filter line bit
- Signature event action handler (SEAH)

  Performs the requested actions. The output from the SEAH is the actions being performed and possibly an <evIdsAlert> written to the Event Store.

Figure 7-1 illustrates the logical flow of the signature event through the SEAP and the operations performed on the action for this event. It starts with the signature event with configured action received in the alarm channel and flows top to bottom as the signature event passes through the functional components of the SEAP.

Figure 7-1 Signature Event Through SEAP



Event Actions

Table 7-1 describes the event actions.

Table 7-1 Event Actions

Event Action Name	Description
Deny Attacker Inline	(Inline mode only) Does not transmit this packet and future packets originating from the attacker address for a specified period of time.[1] **Note** This is the most severe of the deny actions. It denies current and future packets from a single attacker address. To clear all denied attacker entries, choose **Monitoring > Denied Attackers > Clear List**, which permits the addresses back on the network.For the procedure, see Monitoring the Denied Attackers List, page 11-2.
Deny Attacker Service Pair Inline	(Inline mode only) Does not transmit this packet and future packets on the attacker address victim port pair for a specified period of time.
Deny Attacker Victim Pair Inline	(Inline mode only) Does not transmit this packet and future packets on the attacker/victim address pair for a specified period of time. **Note** For deny actions, to set the specified period of time and maximum number of denied attackers, choose **Configuration > Event Action Rules > General Settings**. For the procedure, see Configuring the General Settings, page 7-27.
Deny Connection Inline	(Inline mode only) Does not transmit this packet and future packets on the TCP flow.
Deny Packet Inline	(Inline mode only) Does not transmit this packet. **Note** You cannot delete the event action override for Deny Packet Inline because it is protected. If you do not want to use that override, disable it.
Log Attacker Packets	Starts IP logging packets containing the attacker address. **Note** 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 packets containing the attacker-victim address pair. **Note** 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 packets containing the victim address.
Modify Packet Inline	Modifies packet data to remove ambiguity about what the end point might do with the packet. **Note** Modify Packet Inline is not an option for Add Event Action Filter or Add Event Action Override.

Table 7-1 Event Actions (continued)

Event Action Name	Description
Produce Alert	Writes the event to the Event Store as an alert. **Note** The Produce Alert action is not automatic when you enable alerts for a signature. To have an alert created in the Event Store, you must choose Produce Alert. If you add a second action, you must include Produce Alert if you want an alert sent to the Event Store. Also, every time you configure the event actions, a new list is created and it replaces the old list. Make sure you include all the event actions you need for each signature.
Produce Verbose Alert	Includes an encoded dump of the offending packet in the alert. **Note** This action causes an alert to be written to the Event Store, even if Produce Alert is not selected.
Request Block Connection	Sends a request to ARC to block this connection. **Note** You must have blocking devices configured to implement this action. For more information, see Chapter 8, "Configuring Attack Response Controller for Blocking and Rate Limiting."
Request Block Host	Sends a request to ARC to block this attacker host. **Note** You must have blocking devices configured to implement this action. For more information, see Chapter 8, "Configuring Attack Response Controller for Blocking and Rate Limiting." **Note** For block actions, to set the duration of the block, choose **Configuration > Event Action Rules > General Settings**. For the procedure, see Configuring the General Settings, page 7-27.
Request Rate Limit	Sends a rate limit request to ARC to perform rate limiting. You must have rate limiting devices configured to implement this action. For more information, see Chapter 8, "Configuring Attack Response Controller for Blocking and Rate Limiting." **Note** Request Rate Limit applies to a select set of signatures. See Understanding Rate Limiting, page 8-3, for the list of signatures for which you can request a rate limit.
Request SNMP Trap	Sends a request to NotificationApp to perform SNMP notification. **Note** This action causes an alert to be written to the Event Store, even if Produce Alert is not selected. You must have SNMP configured on the sensor to implement this action. For more information, see Chapter 9, "Configuring SNMP."
Reset TCP Connection	Sends TCP resets to hijack and terminate the TCP flow. **Note** Reset TCP Connection only works on TCP signatures that analyze a single connection. It does not work for sweeps or floods.

1. The sensor maintains a list of attackers being denied by the system. To remove an entry from the denied attacker list, you can view the list of attackers and clear the entire list, or you can wait for the timer to expire. The timer is a sliding timer for each entry. Therefore, if attacker A is being denied, but issues another attack, the timer for attacker A is reset and attacker A remains in the denied attacker list until the timer expires. If the denied attacker list is at capacity and cannot add a new entry, the packet will still be denied.

Understanding Deny Packet Inline

For signatures that have Deny Packet Inline configured as an action or for an event action override that adds Deny Packet Inline as an action, the following actions may be taken:

- droppedPacket
- deniedFlow
- tcpOneWayResetSent

The deny packet inline action is represented as a dropped packet action in the alert. When a deny packet inline occurs for a TCP connection, it is automatically upgraded to a deny connection inline action and seen as a denied flow in the alert. If the IPS denies just one packet, the TCP continues to try to send that same packet again and again, so the IPS denies the entire connection to ensure it never succeeds with the resends.

When a deny connection inline occurs, the IPS also automatically sends a TCP one-way reset, which shows up as a TCP one-way reset sent in the alert. When the IPS denies the connection, it leaves an open connection on both the client (generally the attacker) and the server (generally the victim). Too many open connections can result in resource problems on the victim. So the IPS sends a TCP reset to the victim to close the connection on the victim side (usually the server), which conserves the resources of the victim. It also prevents a failover that would otherwise allow the connection to fail over to a different network path and reach the victim. The IPS leaves the attacker side open and denies all traffic from it.

Event Action Rule Example

The following example demonstrates how the individual components of your event action rules work together.

Risk Rating Ranges for Example 1

- Produce Alert—1-100
- Produce Verbose Alert—90-100
- Request SNMP Trap—50-100
- Log Pair Packets—90-100
- Log Victim Packets—90-100
- Log Attacker Packets—90-100
- Reset TCP Connection—90-100
- Request Block Connection—70-89
- Request Block Host—90-100
- Deny Attacker Inline—0-0
- Deny Connection Inline—90-100
- Deny Packet Inline—90-100

Event Action Filters for Example 1

1. SigID=2004, Attacker Address=*, Victim Address=20.1.1.1, Actions to Remove=ALL, Risk Rating Range=1-100, StopOnMatch=True
2. SigID=2004, Attacker Address=30.1.1.1, Victim Address=*, Actions to Remove=ALL, Risk Rating Range=1-100, StopOnMatch=True
3. SigID=2004, Attacker Address=*, Victim Address=*, Actions to Remove=None, Risk Rating Range=95-100, StopOnMatch=True
4. SigID=2004, Attacker Address=*, Victim Address=*, Actions to Remove=denyAttackerInline, requestBlockHost, requestBlockConnection, Risk Rating Range=56-94, StopOnMatch=True
5. SigID=2004, Attacker Address=*, Victim Address=*, Actions to Remove=denyAttackerInline, requestBlockHost, produceAlert, resetTcpConnection, logAttackerPackets, Risk Rating Range=1-55, StopOnMatch=True

Results for Example 1

When SIG 2004 is detected:

- If the attacker address is 30.1.1.1 or the victim address is 20.1.1.1, the event is consumed (ALL actions are subtracted).

If the attacker address is not 30.1.1.1 and the victim address is not 20.1.1.1:

- If the RR is 50, Produce Alert and Request SNMP Trap are added by the event action override component, but Produce Alert is subtracted by the event action filter. However, the event action policy forces the alert action because Request SNMP Trap is dependent on the evIdsAlert.
- If the RR is 89, Request SNMP Trap and Request Block Connection are added by the event action override component. However, Request Block Connection is subtracted by the event action filter.
- If the RR is 96, all actions except Deny Attacker Inline and Request Block Connection are added by the event action override component, and none are removed by the event action filter. The third filter line with the filter action NONE is optional, but is presented as a clearer way to define this type of filter.

Configuring Event Variables

This section describes how to configure event variables, and contains the following topics:

Overview

You can create event variables and then use those variables in event action filters. When you want to use the same value within multiple filters, use a variable. When you change the value of the variable, any filter that uses that variable is updated with the new value.

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

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

When configuring IP addresses, specify the full IP address or ranges or set of ranges. For example:

- 10.89.10.10-10.89.10.23
- 10.90.1.1
- 192.56.10.1-192.56.10.255
- 10.1.1.1-10.2.255.255, 10.89.10.10-10.89.10.23

Timesaver For example, if you have an IP address space that applies to your engineering group and there are no Windows systems in that group, and you are not worried about any Windows-based attacks to that group, you could set up a variable to be the engineering group's IP address space. You could then use this variable to configure a filter that would ignore all Windows-based attacks for this group.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator or Operator to configure event variables.

Field Definitions

This section lists the field definitions for event variables, and contains the following topics:

Event Variables Pane

The following fields and buttons are found in the Event Variables pane.

Field Descriptions:

- Name—Lets you assign a name to this variable.
- Type—Identifies the variable as an address.
- Value—Lets you add the value(s) represented by this variable.

Button Functions:

- Add—Opens the Add Variable dialog box. From this dialog box, you can add a variable and specify the values associated with that variable.
- Edit—Opens the Edit Variable dialog box. From this dialog box, you can change the values associated with this variable.
- Delete—Removes the selected variable from the list of available variables.
- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Add and Edit Event Variable Dialog Boxes

The following fields and buttons are found in the Add and Edit Event Variable dialog boxes.

Field Descriptions:

- Name—Lets you assign a name to this variable.
- Type—Identifies the variable as an address.
- Value—Lets you add the value(s) represented by this variable.

Button Functions:

- OK—Accepts your changes and closes the dialog box.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

Configuring Event Variables

To configure event variables, follow these steps:

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

Step 2 Choose **Configuration > Event Action Rules > Event Variables**.

The Event Variables pane appears.

Step 3 Click **Add** to create a variable.

The Add Variable dialog box appears.

Step 4 Type a name for this variable in the Name field.

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

Step 5 Type the values for this variable in the Value field.

Specify the full IP address or ranges or set of ranges. For example:

- 10.89.10.10-10.89.10.23
- 10.90.1.1
- 192.56.10.1-192.56.10.255

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

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

Step 6 Click **OK**.

The new variable appears in the list in the Event Variables pane.

Step 7 To edit an existing variable, select it in the list, and then click **Edit**.

The Edit Event Variable dialog box appears.

Step 8 Make your changes to the value in the Value field.

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

Step 9 Click **OK**.

The edited event variable now appears in the list in the Event Variables pane.

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

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

Configuring Target Value Ratings

This section describes how to configure target value ratings, and contains the following topics:

Overview

You can assign a TVR to your network assets. The TVR is one of the factors used to calculate the RR value for each alert. You can assign different TVRs to different targets. Events with a higher RR trigger more severe signature event actions.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator or Operator to configure target value ratings.

Field Definitions

This section lists the field definitions for TVR, and contains the following topics:

- Target Value Rating Pane, page 7-13
- Add and Edit Target Value Rating Dialog Boxes, page 7-13

Target Value Rating Pane

The following fields and buttons are found in the Target Value Rating pane.

Field Descriptions:

- Target Value Rating (TVR)—Identifies the value assigned to this network asset. The value can be High, Low, Medium, Mission Critical, or No Value.
- Target IP Address—Identifies the IP address of the network asset you want to prioritize with a TVR.

Button Functions:

- Select All—Selects all configured targets.
- Add—Opens the Add Target Value Rating dialog box. From this dialog box, you add the IP address(es) of the network asset and assign a TVR to the asset.
- Edit—Opens the Edit Target Value Rating dialog box. From this dialog box, you can change the IP address(es) of the network asset.
- Delete—Removes the selected TVR from the list of available ratings.
- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Add and Edit Target Value Rating Dialog Boxes

The following fields and buttons are found in the Add and Edit Target Value Rating dialog boxes.

Field Descriptions:

- Target Value Rating (TVR)—Identifies the value assigned to this network asset. The value can be High, Low, Medium, Mission Critical, or No Value.
- Target IP Address(es)—Identifies the IP address of the network asset you want to prioritize with a TVR.

Button Functions:

- OK—Accepts your changes and closes the dialog box.

- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

Configuring Target Value Ratings

To configure TVR, follow these steps:

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

Step 2 Choose **Configuration > Event Action Rules > Target Value Rating**.

The Target Value Rating pane appears.

Step 3 Click **Add** to create a TVR.

The Add Target Value Rating dialog box appears.

Step 4 To assign a TVR to a new group of assets, follow these steps:

a. Click **Add**. to add a new group of network assets.

b. Choose a rating from the Target Value Rating list box.

The values are High, Low, Medium, Mission Critical, or No Value.

c. Type the IP address of the network asset in the Target IP Address(es) field.

To enter a range of IP addresses, type the lowest address followed by a hyphen and then the highest address in the range. For example: 10.10.2.1-10.10.2.30.

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

Step 5 Click **OK**.

The new TVR for the new asset appears in the list in the Target Value Rating pane.

Step 6 To edit an existing TVR, select it in the list, and then click **Edit**.

The Edit Target Value Rating dialog box appears.

Step 7 Make your changes to the values in the Target IP Address(es) field.

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

Step 8 Click **OK**.

The edited network asset now appears in the list in the Target Value Rating pane.

Step 9 To delete a network asset, select in the list, and then click **Delete**.

The network asset no longer appears in the list in the Target Value Rating pane.

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

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

Configuring Event Action Overrides

This section describes how to configure event action overrides, and contains the following topics:

Overview

You can add an event action override to change the actions associated with an event based on specific details about that event.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator or Operator to configure event action overrides.

Field Definitions

This section lists the field definitions for the event action overrides, and contains the following topics:

Event Action Overrides Pane

The following fields and buttons are found in the Event Action Overrides pane.

Field Descriptions:

- Use Event Action Overrides—If selected, lets you use any event action override that is enabled.
- Event Action—Specifies the event action that will be added to an event if the conditions of this event action override are satisfied.
- Enabled—Indicates whether or not the override is enabled.

- Risk Rating—Indicates the RR range between 0 and 100 that should be used to trigger this event action override.

  If an event occurs with a RR that falls within the minimum-maximum range you configure here, the event action is added to this event.

Button Functions:

- Select All—Selects all event action overrides listed in the table.
- Add—Opens the Add Event Action Override dialog box. From this dialog box, you can add an event action override and specify the values associated with that override.
- Edit—Opens the Edit Event Action Override dialog box. From this dialog box, you can change the values associated with this event action override.
- Enable—Enables the selected event action override. You must check the Use Event Action Overrides check box in the Event Action Overrides pane or none of the event action overrides will be enabled regardless of the value you set here.
- Disable—Disables the selected event action override.
- Delete—Removes the selected event action override from the list of available overrides.
- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Add and Edit Event Action Overrides Dialog Boxes

The following fields and buttons are found in the Add and Edit Event Action Overrides dialog boxes.

Field Descriptions:

- Event Action—Specifies the event action that will be added to an event if the conditions of this event action override are satisfied.
  - Deny Attacker Inline—(Inline only) Terminates the current packet and future packets from this attacker address for a specified period of time.

    The sensor maintains a list of attackers being denied by the system. To remove an entry from the denied attacker list, you can view the list of attackers and clear the entire list, or you can wait for the timer to expire. The timer is a sliding timer for each entry. Therefore, if attacker A is being denied, but issues another attack, the timer for attacker A is reset and attacker A remains in the denied attacker list until the timer expires. If the denied attacker list is at capacity and cannot add a new entry, the packet will still be denied.

    Note This is the most severe of the deny actions. It denies current and future packets from a single attacker address. To clear all denied attacker entries, choose **Monitoring > Denied Attackers > Clear List**, which permits the addresses back on the network. For the procedure, see Monitoring the Denied Attackers List, page 11-2.

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

Note For deny actions, to set the specified period of time and maximum number of denied attackers, choose **Configuration > Event Action Rules > General Settings**. For the procedure, see Configuring the General Settings, page 7-27.

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

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

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

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

- Produce Alert—Writes the event to the Event Store as an alert.
- Produce Verbose Alert—Includes an encoded dump of the offending packet in the alert. This action causes an alert to be written to the Event Store, even if Produce Alert is not selected.
- Request Block Connection—Sends a request to ARC to block this connection. You must have blocking devices configured to implement this action. For more information, see Chapter 8, "Configuring Attack Response Controller for Blocking and Rate Limiting."
- Request Block Host—Sends a request to ARC to block this attacker host. You must have blocking devices configured to implement this action. For more information, see Chapter 8, "Configuring Attack Response Controller for Blocking and Rate Limiting."

Note For block actions, to set the duration of the block, choose **Configuration > Event Action Rules > General Settings**. For the procedure, see Configuring the General Settings, page 7-27.

- Request Rate Limit—Sends a rate limit request to ARC to perform rate limiting. You must have rate limiting devices configured to implement this action. For more information, see Chapter 8, "Configuring Attack Response Controller for Blocking and Rate Limiting."

  - Request SNMP Trap—Sends a request to the Notification Application component of the sensor to perform SNMP notification. This action causes an alert to be written to the Event Store, even if Produce Alert is not selected. You must have SNMP configured on the sensor to implement this action. For more information, see Chapter 9, "Configuring SNMP."
  - Reset TCP Connection—Sends TCP resets to hijack and terminate the TCP flow. Reset TCP Connection only works on TCP signatures that analyze a single connection. It does not work for sweeps or floods.
- Enabled—Check the Yes check box to enable the override, check the No check box to disable the override.
- Risk Rating—Indicates the RR range between 0 and 100 that should be used to trigger this event action override.

  If an event occurs with an RR that falls within the minimum-maximum range you configure here, the event action is added to this event.

Button Functions:

- OK—Accepts your changes and closes the dialog box.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

Understanding Deny Packet Inline

For signatures that have Deny Packet Inline configured as an action or for an event action override that adds Deny Packet Inline as an action, the following actions may be taken:

- droppedPacket
- deniedFlow
- tcpOneWayResetSent

The deny packet inline action is represented as a dropped packet action in the alert. When a deny packet inline occurs for a TCP connection, it is automatically upgraded to a deny connection inline action and seen as a denied flow in the alert. If the IPS denies just one packet, the TCP continues to try to send that same packet again and again, so the IPS denies the entire connection to ensure it never succeeds with the resends.

When a deny connection inline occurs, the IPS also automatically sends a TCP one-way reset, which shows up as a TCP one-way reset sent in the alert. When the IPS denies the connection, it leaves an open connection on both the client (generally the attacker) and the server (generally the victim). Too many open connections can result in resource problems on the victim. So the IPS sends a TCP reset to the victim to close the connection on the victim side (usually the server), which conserves the resources of the victim. It also prevents a failover that would otherwise allow the connection to fail over to a different network path and reach the victim. The IPS leaves the attacker side open and denies all traffic from it.

Configuring Event Action Overrides

To configure event action overrides, follow these steps:

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

Step 2 Choose **Configuration > Event Action Rules > Event Action Overrides**.

The Event Action Overrides pane appears.

Step 3 Click **Add** to create a event action override.

The Add Event Action Override dialog box appears.

Step 4 From the Event Action list, choose the event action this event action override will correspond to.

Step 5 Under Enabled, check the Yes check box.

Step 6 Under Risk Rating assign an RR range to this network asset in the Minimum and Maximum fields.

All values should be between 0 and 100 and the value in the Minimum field must be less than or equal to the value in the Maximum field.

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

Step 7 Click **OK**.

The new event action override now appears in the list in the Event Action Overrides pane.

Step 8 Check the Use Event Action Overrides check box.

Note You must check the Use Event Action Overrides check box in the Event Action Overrides pane or none of the event action overrides will be enabled regardless of the value you set.

Step 9 To edit an existing event action override, select it in the list, and then click **Edit**.

The Edit Event Action Override dialog box appears.

Step 10 Under Enabled, check the Yes check box.

Step 11 Under Risk Rating assign an RR range to this network asset in the Minimum and Maximum fields.

All values should be between 0 and 100 and the value in the Minimum field must be less than or equal to the value in the Maximum field.

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

Step 12 Click **OK**.

The edited event action override now appears in the list in the Event Action Overrides pane.

Step 13 Check the Use Event Action Overrides check box.

Note You must check the Use Event Action Overrides check box in the Event Action Overrides pane or none of the event action overrides will be enabled regardless of the value you set.

Step 14 To delete an event action override, select it in the list, and then click **Delete**.

The event action override no longer appears in the list in the Event Action Overrides pane.

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

Step 15 To enable or disable an event action override, select it in the list, and then click **Enable** or **Disable**.

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

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

Configuring Event Action Filters

This section describes how to configure event action filters, and contains the following topics:

Overview

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. You can use the variables that you defined in the Event Variables pane to group addresses for your filters.

Note You must preface the variable with a dollar sign ($) to indicate that you are using a variable rather than a string. Otherwise, you receive the `Bad source and destination` error.

Caution Event action filters based on source and destination IP addresses do not function for the Sweep engine, because they do not filter as regular signatures. To filter source and destination IP addresses in sweep alerts, use the source and destination IP address filter parameters in the Sweep engine signatures.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator or Operator to configure Event Action Filters.

Field Definitions

This section lists the field definitions for event action filters, and contains the following topics:

Event Action Filters Pane

The following fields and buttons are found in the Event Action Filters pane.

Field Descriptions:

- Use Event Action Filters—Enables the event action filter component.

  You must check this check box to use any filter that is enabled.
- Name—Lets you name the filter you are adding.

  You need to name your filters so that you can move them around in the list and move them to the inactive list if needed.
- Active—Indicates whether the filter has been put into the filter list and will take effect on filtering events.
- Enabled—Indicates whether or not this filter is enabled.
- Sig ID—Identifies the unique numerical value assigned to this signature.

  This value lets the sensor identify a particular signature. You can also enter a range of signatures.
- SubSig ID—Identifies the unique numerical value assigned to this subsignature.

  A subSig ID is used to identify a more granular version of a broad signature. You can also enter a range of subSig IDs.
- Attacker (address/port)—Identifies the IP address and/or port of the host that sent the offending packet.

  You can also enter a range of addresses.
- Attacker (address/port)—Identifies the IP address and/or port used by the attacker host.

  This is the port from where the offending packet originated. You can also enter a range of ports.
- Risk Rating—Indicates the RR range between 0 and 100 that should be used to trigger this Event Action Filter.

  If an event occurs with an RR that falls within the minimum-maximum range you configure here, the event is processed against the rules of this event filter.
- Actions to Subtract—Indicates the actions that should be removed from the event, should the conditions of the event meet the criteria of the event action filter.
- Deny Pct—Indicates the percentage of packets to deny for deny attacker features.
- Stop on Match—Determines whether or not this event will be processed against remaining filters in the event action filters list.

  If set to No, the remaining filters are processed for a match until a Stop flag is encountered.

  If set to Yes, no further processing is done. The actions specified by this filter are removed and the remaining actions are performed.
- Comments—Identifies the user comments associated with this filter.

Button Functions:

- Select All—Selects all event action filters listed.
- Add—Opens the Add Event Action Filter dialog box. From this dialog box, you can add an event action filter and specify the values associated with that filter.
- Insert Before—Lets you add an event action filter above the one you have selected. Opens the Add Event Action Filter dialog box.
- Insert After—Lets you add an event action filter after the one you have selected. Opens the Add Event Action Filter dialog box.
- Move Up—Moves the selected filter up one row in the list and changes the processing order of the filters.
- Move Down—Moves the selected filter down one row in the list and changes the processing order of the filters.
- Edit—Opens the Edit Event Action Filter dialog box. From this dialog box, you can change the values associated with this filter.
- Active—Lets you add a filter to the filter list so that it takes effect on filtering events.
- Inactive—Lets you take a filter out of the list so that it does not take effect on filtering events.
- Enable—Enables the selected event action filter.

  You must check the Use Event Action Filters check box on the Event Action Filters pane or none of the event action filters will be enabled regardless of the value you set here.
- Disable—Disables the selected event action filter.
- Delete—Removes this event action filter from the list of available filters.
- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Add and Edit Event Action Filters Dialog Boxes

The following fields and buttons are found in the Add and Edit Event Action Filters dialog boxes.

Field Descriptions:

- Name—Lets you name the filter you are adding.

  You need to name your filters so that you can move them around in the list and move them to the inactive list if needed.
- Active—Lets you add the filter to the filter list so that it takes effect on filtering events.
- Enabled—Indicates whether or not this filter is enabled.
- Signature ID—Identifies the unique numerical value assigned to this signature.

  This value lets the sensor identify a particular signature. You can also enter a range of signatures.
- SubSignature ID—Identifies the unique numerical value assigned to this subsignature.

  A subSig ID is used to identify a more granular version of a broad signature. You can also enter a range of subSig IDs.
- Attacker Address—Identifies the IP address of the host that sent the offending packet.

  You can also enter a range of addresses.

- Attacker Port—Identifies the port used by the attacker host.

  This is the port from where the offending packet originated. You can also enter a range of ports.
- Victim Address—Identifies the IP address of the host being attacked (the recipient of the offending packet).

  You can also enter a range of addresses.
- Victim Port—Identifies the port through which the offending packet was received.

  You can also enter a range of ports.
- Risk Rating—Indicates the RR range between 0 and 100 that should be used to trigger this event action filter.

  If an event occurs with an RR that falls within the minimum-maximum range you configure here, the event is processed against the rules of this event filter.
- Actions to Subtract—Indicates the actions that should be removed from the event, should the conditions of the event meet the criteria of the event action filter.
  - Deny Attacker Inline—(Inline only) Terminates the current packet and future packets from this attacker address for a specified period of time.

    The sensor maintains a list of attackers being denied by the system. To remove an entry from the denied attacker list, you can view the list of attackers and clear the entire list, or you can wait for the timer to expire. The timer is a sliding timer for each entry. Therefore, if attacker A is being denied, but issues another attack, the timer for attacker A is reset and attacker A remains in the denied attacker list until the timer expires. If the denied attacker list is at capacity and cannot add a new entry, the packet will still be denied.

    Note This is the most severe of the deny actions. It denies current and future packets from a single attacker address. To clear all denied attacker entries, choose **Monitoring > Denied Attackers > Clear List**, which permits the addresses back on the network. For the procedure, see Monitoring the Denied Attackers List, page 11-2.
  - Deny Attacker Service Pair Inline—(Inline only) Does not transmit this packet and future packets on the attacker address victim port pair for a specified period of time.
  - Deny Attacker Victim Pair Inline—(Inline only) Does not transmit this packet and future packets on the attacker/victim address pair for a specified period of time.

    Note For deny actions, to set the specified period of time and maximum number of denied attackers, choose **Configuration > Event Action Rules > General Settings**. For the procedure, see Configuring the General Settings, page 7-27.
  - Deny Connection Inline—(Inline only) Terminates the current packet and future packets on this TCP flow.
  - Deny Packet Inline—(Inline only) Terminates the packet.

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

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

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

- Produce Alert—Writes the event to the Event Store as an alert.
- Produce Verbose Alert—Includes an encoded dump of the offending packet in the alert. This action causes an alert to be written to the Event Store, even if Produce Alert is not selected.
- Request Block Connection—Sends a request to ARC to block this connection. You must have blocking devices configured to implement this action. For more information, see Chapter 8, "Configuring Attack Response Controller for Blocking and Rate Limiting."
- Request Block Host—Sends a request to ARC to block this attacker host. You must have blocking devices configured to implement this action. For more information, see Chapter 8, "Configuring Attack Response Controller for Blocking and Rate Limiting."

Note For block actions, to set the duration of the block, choose **Configuration > Event Action Rules > General Settings**. For the procedure, see Configuring the General Settings, page 7-27.

- Request Rate Limit—Sends a rate limit request to ARC to perform rate limiting. You must have rate limiting devices configured to implement this action. For more information, see Chapter 8, "Configuring Attack Response Controller for Blocking and Rate Limiting."
- Request SNMP Trap—Sends a request to the Notification Application component of the sensor to perform SNMP notification. This action causes an alert to be written to the Event Store, even if Produce Alert is not selected. You must have SNMP configured on the sensor to implement this action. For more information, see Chapter 9, "Configuring SNMP."
- Reset TCP Connection—Sends TCP resets to hijack and terminate the TCP flow. Reset TCP Connection only works on TCP signatures that analyze a single connection. It does not work for sweeps or floods.

- Deny Percentage—Determines the percentage of packets to deny for deny attacker features. The valid range is 0 to 100. The default is 100 percent.
- Stop on Match—Determines whether or not this event will be processed against remaining filters in the event action filters list.

  If set to No, the remaining filters are processed for a match until a Stop flag is encountered.

  If set to Yes, no further processing is done. The actions specified by this filter are removed and the remaining actions are performed.

- Comments—Identifies the user comments associated with this filter.

Button Functions:

- OK—Accepts your changes and closes the dialog box.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

Configuring Event Action Filters

To configure event action filters, follow these steps:

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

Step 2 Choose **Configuration > Event Action Rules > Event Action Filters**.

The Event Action Filters pane appears.

Step 3 To create an event action filter, do one of the following:

- To add a new event action filter, click **Add**.
- Or, to add a filter above or below the current filter, right-click a filter and then choose Insert Before or Insert After.

The Add Event Action Filter dialog box appears.

Step 4 Type the signature IDs of all signatures to which this filter should be applied in the Signature ID field.

You can use a list (2001, 2004), or a range (2001–2004) or one of the SIG variables if you defined them in the Event Variables pane. Preface the variable with $.

Step 5 Type the subsignature IDs of the subsignatures to which this filter should be applied in the SubSignature ID field.

Step 6 Type the IP address of the source host in the Attacker Address field.

You can use one of the variables if you defined them in the Event Variables pane. Preface the variable with $. You can also enter a range of addresses (0.0.0.0-255.255.255.255).

Step 7 Type the port number used by the attacker to send the offending packet in the Attacker Port field.

Step 8 Type the IP address of the recipient host in the Victim Address field.

You can use one of the variables if you defined them in the Event Variables pane. Preface the variable with $. You can also enter a range of addresses (0.0.0.0-255.255.255.255).

Step 9 Type the port number used by the victim host to receive the offending packet in the Victim Port field.

Step 10 Assign an RR range to this filter in the Risk Rating field.

If the RR for an event falls within the range you specify, the event is processed against the criteria of this filter.

Step 11 Select the actions you want this filter to remove from the event from the Actions to Subtract list.

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

Step 12 Type the percentage of packets to deny for deny attacker features in the Deny Percentage field. The default is 100 percent.

Step 13 Next to Stop on Match, check one of the following check boxes:

a. Yes—If you want the Event Action Filters component to stop processing after the actions of this particular filter have been removed.

   Any remaining filters will not be processed; therefore, no additional actions can be removed from the event.

b. No—If you want to continue processing additional filters.

Step 14 Next to Enabled, choose Yes to enable this filter.

Note You must also check the Use Event Action Filters check box in the Event Action Filters pane or none of the event action filters will be enabled regardless of whether you check the Yes check box in the Add Event Action Filter dialog box.

Step 15 Next to Active, choose Yes to add this filter to the list so that it takes effect on filtering events.

Step 16 Type any comments that you want to store with this filter in the Comments field, such as the purpose of this filter or why you have configured this filter in a particular way.

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

Step 17 Click **OK**.

The new event action filter now appears in the list in the Event Action Filters pane.

Step 18 Check the Use Event Action Overrides check box.

Note You must check the Use Event Action Overrides box in the Event Action Overrides pane or none of the event action overrides will be enabled regardless of the value you set in the Add Event Action Filter dialog box.

Step 19 To edit an existing event action filter, select it in the list, and then click **Edit**.

The Edit Event Action Filter dialog box appears.

Step 20 Change any values in the fields that you need to.

See Steps 3 through 14 for information on completing the fields.

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

Step 21 Click **OK**.

The edited event action filter now appears in the list in the Event Action Filter pane.

Step 22 Check the Use Event Action Overrides check box.

Note You must check the Use Event Action Overrides box in the Event Action Overrides pane or none of the event action overrides will be enabled regardless of the value you set in the Edit Event Action Filter dialog box.

Step 23 To delete an event action filter, select it in the list, and then click **Delete**.

The event action filter no longer appears in the list in the Event Action Filters pane.

Step 24 To enable or disable an event action filter, select it in the list, and then click **Enable** or **Disable**.

Step 25 To move an event action filter up or down in the list, select it, and then click **Move Up** or **Move Down**.

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

Step 26 Click **Apply** to apply your changes and save the revised configuration.

Configuring the General Settings

This section describes how to configure the general settings, and contains the following topics:

Overview

You can configure the general settings that apply to event action rules, such as whether you want to use the Summarizer and the Meta Event Generator. The Summarizer groups events into a single alert, thus decreasing the number of alerts the sensor sends out. The Meta Event Generator processes the component events, which lets the sensor watch for suspicious activity transpiring over a series of events.

Caution Do not turn off the Summarizer or Meta Event Generator except for troubleshooting purposes. If you turn off the Summarizer, every signature is set to Fire All with no summarization. If you turn off the Meta Event Generator, all Meta engine signatures are disabled.

You can configure how long you want to deny attackers, the maximum number of denied attackers, and how long you want blocks to last.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator or Operator to configure the general settings for event action rules.

Field Definitions

The following fields and buttons are found in the General Settings pane.

Field Descriptions:

- Use Summarizer—Enables the Summarizer component.

  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 will be ignored if the Summarizer is not enabled.

- Use Meta Event Generator—Enables the meta event generator.

  By default, the Meta Event Generator is enabled. If you disable the Meta Event Generator, all Meta engine signatures will be disabled.

- Deny Attacker Duration—Number of seconds to deny the attacker inline.

  The valid range is 0 to 518400. The default is 3600.

- Block Attack Duration—Number of minutes to block a host or connection.

  The valid range is 0 to 10000000. The default is 30.

- Maximum Denied Attackers—Limits the number of denied attackers possible in the system at any one time.

  The valid range is 0 to 10000000. The default is 10000.

Button Functions:

- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Configuring Event Action Rules General Settings

Caution The Summarizer and Meta Event Generator operate at a global level, so enabling them affects all sensor processing of these features.

To configure the general settings for event action rules, follow these steps:

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

Step 2 Choose **Configuration >Event Action Rules > General Settings**.

The General Settings pane appears.

Step 3 Check the Use Summarizer check box to enable the summarizer feature.

Caution Only disable the Summarizer for troubleshooting purposes. Otherwise, make sure the Summarizer is enabled so that all signatures you configure for summarization will actually summarize.

Step 4 Check the Use Meta Event Generator check box to enable the meta event generator.

Caution Only disable the Meta Event Generator for troubleshooting purposes. Otherwise, make sure the Meta Event Generator is enabled so that all Meta engine signatures are functional.

Step 5 Type the number of seconds you want to deny the attacker inline in the Deny Attacker Duration field.

Step 6 Type the number of minutes you want to block a host or connection in the Block Action Duration field.

Step 7 Type the maximum number of denied attackers you want at any one time in the Maximum Denied Attackers field.

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

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

Monitoring Events

This section describes how to monitor events, and contains the following topics:

Overview

The Events pane lets you filter and view event data. You can filter events based on type, time, or both. By default all alert and error events are displayed for the past one hour. You can access these events by clicking View.

When you click **View**, IDM defines a time range for the events if you have not already configured one. If you do not specify an end time of the range, it is defined as the moment you click **View**.

To prevent system errors when retrieving large numbers of events from the sensor, IDM limits the number of events you can view at one time (the maximum number of rows per page is 500). You can click **Back** and **Next** to view more events.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

Field Definitions

This section lists the field definitions configuring events and viewing events. It contains the following topics:

Events Pane

The following fields and buttons are found in the Events pane.

Field Descriptions:

- Show alert events—Lets you configure the level of alert you want to view:
  - Informational
  - Low
  - Medium
  - High

  The default is all levels enabled.
- Show error events—Lets you configure the type of errors you want to view:
  - Warning
  - Error
  - Fatal

  The default is all levels enabled.
- Show Network Access Controller events—Shows ARC (formally known as Network Access Controller) events.

  The default is disabled.
- Show status events—Shows status events.

  The default is disabled.
- Select the number of the rows per page—Lets you determine how many rows you want to view per page.

  The valid range is 100 to 500. The default is 100.
- Show all events currently stored on the sensor—Retrieves all events stored on the sensor.
- Show past events—Lets you go back a specified number of hours or minutes to view past events.
- Show events from the following time range—Retrieves events from the specified time range.

Button Functions:

- View—Causes the Event Viewer to appear.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Event Viewer Page

The following fields and buttons are found on the Event Viewer page.

- #—Identifies the order number of the event in the results query.
- Type—Identifies the type of event as Error, NAC, Status, or Alert.
- Sensor UTC Time—Identifies when the event occurred.
- Event ID—The numerical identifier the sensor has assigned to the event.
- Events—Briefly describes the event.
- Sig ID—Identifies the signature that fired and caused the alert event.

Button Functions

- Details—Displays the details of the selected event in a separate dialog box.

  Displays the application, attacker, target, and signature details.
- Refresh—Lets you refresh the Event Viewer with new events.
- Back—Displays the previous page in the Event Viewer.
- Next—Displays the next page in the Event Viewer.
- Close—Closes the open dialog box.
- Help—Displays the help topic for this feature.

Configuring Event Display

To configure how you want events to be displayed, follow these steps:

Step 1 Log in to IDM.

Step 2 Choose **Monitoring > Events**.

The Events pane appears.

Step 3 Under Events, choose the levels of alerts you want to be displayed.

Step 4 Under Events, choose the types of errors you want to be displayed.

Step 5 Check the **Show Network Access Controller events** check box if you want ARC (formerly known as Network Access Controller) events to be displayed.

Step 6 Check the **Show status events** check box if you want status events to be displayed.

Step 7 Choose the number of rows per page you want displayed.

The default is 100. The values are 100, 200, 300, 400, or 500.

Step 8 If you want to set a time for events to be displayed, choose one of the following:

- Show all events currently stored on the sensor
- Show past events

  Type in the hours and minutes you want to go back to view past events.
- Show events from the following time range

  Select a start and end time.

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

Step 9 Click **View** to display the events you configured.

The Event Viewer appears.

Step 10 To sort up and down in a column, click the right-hand side to see the up and down arrow.

Step 11 Click **Next** or **Back** to page by one hundred.

Step 12 To view details of an event, select it, and click **Details**.

The details for that event appear in another dialog box. The dialog box has the Event ID as its title.