The ability to add an alarm is available to users with administrator privileges and any user belonging to an access group with the Alarm Management privilege. To create an alarm, do the following:

2. Click on Alarms on the System Properties menu. The Alarms dialog will open listing the existing alarms on the system.
3. Click on Add. The Alarm Settings dialog opens showing the Summary, Condition, Actions, and Escalation tabs.
4. On the Summary tab, enter the name for the alarm in the Name field. The Condition field will be blank because there is no default condition selected for a new alarm (see Step 7 to add a condition). The Actions field will say Log event, which is the default action setting for a new alarm (see Step 10 to change).
5. Select the person or group to whom this alarm is assigned in the Assignee field. The drop-down list will show the users and groups that have alarm management privileges.
6. Select the severity of this alarm, which will determine the priority given to the notification it generates in the Alarm log.
7. If you want to disable the alarm, deselect the Enabled checkbox. The alarm is enabled by default.
8. Click on Next or on the Condition tab. The Condition dialog will open. Conditions can be thought of as triggers that cause an alarm to be generated when a specified criterion is met.
9. In the Type field, select the type of alarm on the drop-down list. When you do so, further details will be requested based on the type of alarm you selected. Below is information regarding each of these additional fields:

<table>
<thead>
<tr>
<th>Section</th>
<th>Alarm Types</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Rate</td>
<td>Device Failure, FIPS</td>
<td>Select how often the system should check to see if this type of condition exists.</td>
</tr>
<tr>
<td></td>
<td>Failure, Deviation from Baseline, HA Failure</td>
<td></td>
</tr>
<tr>
<td>Deviation</td>
<td>Deviation from Baseline</td>
<td>This condition allows you to specify a percentage threshold to check above baseline and/or a different percentage below baseline.</td>
</tr>
</tbody>
</table>
• In the **Query** field, select the type of data that you will be querying.

• Click on the **Filter** icon (✓) and select the values to filter the data for this alarm. Values containing commas must be used inside of a Watchlist (see **Watchlists** section) in order to work properly.

  ![Refer to the Alarm UCF filters section if you wish to set up regulation compliance filters.]

• In the **Time Frame** field, select whether you want it to query the last or the previous period of time that you select in the number field and type field.

• Select how far above and/or below the baseline you want the deviation to be before an alarm is triggered.

<table>
<thead>
<tr>
<th>Event Rate</th>
<th>Specified Event Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Enter the number of the events that need to occur before an alarm is generated in the <strong>Event Count</strong> field.</td>
<td></td>
</tr>
<tr>
<td>• Click on the <strong>Filter</strong> icon (✓) and select the values to filter the data for this alarm. Values containing commas must be used inside of a Watchlist (see <strong>Watchlists</strong> section) in order to work properly.</td>
<td></td>
</tr>
<tr>
<td>• Refer to the Alarm UCF filters section if you wish to set up regulation compliance filters.</td>
<td></td>
</tr>
<tr>
<td>• In the <strong>Time Frame</strong> field, select the amount of time in which the number of events you selected must occur for an alarm to be generated.</td>
<td></td>
</tr>
<tr>
<td>• Since the rate data for an event will include a sharp increase at the end created by aggregation, select the amount of time by which you want the time frame offset in the <strong>Offset By</strong> field so that it won't include that sharp increase. For example, if your ESM pulls events every 5 minutes, the last 1 minute of the events retrieved will contain the aggregated events. You would, therefore, want to offset the time frame by that period of time so the last 1 minute would not be included in the data measurement. If you don't do this, the values in</td>
<td></td>
</tr>
</tbody>
</table>
Create a New Alarm

the aggregated data will be included in the event count, very likely causing a false positive.

<table>
<thead>
<tr>
<th>Field Match</th>
<th>Field Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Select <em>Trigger when value does not match</em> to trigger an alarm if the value in the event is not in the corresponding watchlist or list of values.</td>
<td></td>
</tr>
<tr>
<td>• Click on the <em>Use Watchlist</em> checkbox if you have set up a watchlist that contains all of the values on which you want this alarm to notify you, then select the watchlist from the drop-down list.</td>
<td></td>
</tr>
<tr>
<td>• If you do not select <em>Use Watchlist</em>, select the type of data that this alarm will be monitoring on the <em>Field</em> drop-down list. If you are setting up an alarm that will trigger when a health monitor event is generated, refer to the Health Monitor Alarms section for details.</td>
<td></td>
</tr>
<tr>
<td>Values containing commas must be used inside of a Watchlist (see Watchlists section) in order to work properly.</td>
<td></td>
</tr>
<tr>
<td>• In the <em>Value(s)</em> field, enter the specific values of the types that you selected in <em>Field</em>. For example, if you selected Source IP in <em>Field</em>, enter the actual source IP addresses on which you want this alarm to trigger.</td>
<td></td>
</tr>
<tr>
<td>The values field is limited to 1000 characters. If you need to enter more values, create a watchlist with the needed values (see Add a Watchlist) and apply it to the <em>Field Match</em> condition.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Maximum Condition</th>
<th>All except for Deviation from Baseline</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trigger Frequency</td>
<td>Since events can be experienced on a sustained basis, select the amount of time to allow between each condition is defined to prevent a flood of notifications from being sent.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Health Monitor Status</th>
<th>Device Status Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the types of device status changes about which you want to be notified. For example, if you select only <em>Critical</em>, you will not be notified if there is a health monitor status change that is at the <em>Warning</em> level.</td>
<td></td>
</tr>
<tr>
<td>For more details, refer to the Health Monitor</td>
<td></td>
</tr>
</tbody>
</table>
9. Select the device(s) that you want this alarm to monitor in the Select Device section.

10. Click on Next or the Actions tab. The Actions dialog will open.

11. Select the type(s) of action(s) to be taken when an alarm is triggered by the condition you defined on the Condition tab. You can select more than one action. Following are the options:

   • **Log event** - This is selected by default. When this option is selected, an event will be logged on the ESM.
   
   • **Visual alert** - If you select this option, a message, looking as follows, will pop up on the bottom right of the screen when the alarm is triggered. When you click on the Visual Alert checkbox, you will be allowed to select whether or not you want a sound to be played when the message pops up. When you click on the down arrow, a list of the audio files on the system will appear. Select the sound that you want associated with the visual alert. (Refer to Additional Alarm Options section for details on adding audio files to the system.)

   When you click on the Visual Alert checkbox, you will be allowed to select whether or not you want a sound to be played when the message pops up. When you click on the down arrow, a list of the audio files on the system will appear. Select the sound that you want associated with the visual alert. (Refer to Additional Alarm Options section for details on adding audio files to the system.)

   • **Create a case for** - When you select this option, a case will be created for the person or group that you select from the drop-down list. The case will show the severity and associated event, and the alarm event will be added so the user can trace the case back to its source. The alarm summary will be the name/summary of the case created. Can not be used when escalating an alarm (see step 19).

   • **Update Watchlist** - This option is only available if Field Match is selected as the condition type. It allows you to modify watchlists by adding or removing values based on the information contained in up to 10 alarm triggering events. When you click on the Manage button in the Update Watchlist field, the Update Watchlist dialog will open.

     o **Action** - Select whether you want the value to be appended to or removed from the watchlist.
     o **Field** - Select the field from which you want the data retrieved in the triggered alarm.
     o **Watchlist** - Select the watchlist to which you want to append or remove the data.
     o **Add New Watchlist** - Allows you to add a new watchlist to the system.

You can add up to 5 actions per alarm. To add more than one, click on Add Action. To delete an action, click on Delete to the right of the action to be deleted. When a watchlist is
modified as a result of these settings, the Actions tab of the triggered alarm will say something like Added SrcIP to “Bad IPs” Watchlist or Removed DestIP from “Clean IPs” Watchlist.

- **Generate reports, views and queries** - You can select this alarm to generate a report, view, or query. To do so, click on the Add button. The Add Report editor opens. For details regarding filling out the editor, start at Step 7 of the Add a Report section. When you click Save on the Add Report dialog, the report type and layout will be added to the list of reports on the Actions tab.

- **Send Message** - If this option is selected, a text or email message will be sent to the recipient(s) that you choose. To choose the recipients:
  1. Click on Add recipient. The Recipients dialog will open.
  2. Select the email, email Groups, Users, or SMS.
  3. Click on the checkbox(s) of the recipient(s) to whom you want this message sent or click on Select All or Select None.
  4. Click on OK. This dialog also allows you to add, edit, or remove recipients. Refer to the following sections for details.
    - Email Recipients
    - Email Group Recipients
    - SMS Recipients
    - Add, Edit, and Remove Users

- **Execute script** - Provides you with the ability to execute a script on any device that accepts SSH connections. This could then initiate actions on other software applications. When you click on the Setup button, the Execute Script Configuration dialog opens. Fill in the Host, Port, Username, Password, and Command String fields.

  Executing scripts can be used in all alarm types, but only the Field Match alarm type tracks specific events and will have variables to insert into the command string. To access these variables, click on the Insert Variable icon ( ).

- **Send to Remedy** - This option is only available if Field Match is selected as the condition type. You can send up to 10 events to Remedy per triggered alarm, if Remedy is set up. When you click on Setup, the Send to Remedy dialog will open allowing you to add the Remedy prefix, keyword, and user ID for sending emails to the Remedy system. When an event is sent to Remedy as a result of this setting, Sent events to Remedy will be added to the Actions tab of the triggered alarm.

- **Blacklist** - This action will only be available if Field Match is selected as the condition. Select this option if you want the destination IP, source IP, or IP address on the device you select to be added to the global blacklist.
Create a New Alarm

1. Click the Configure button. The Blacklist dialog box will open.
2. Select the IP address field you want to blacklist.
3. Select the device you want the address blacklisted on.
4. Select how long you want this blacklisting to last.
5. (Optional) Enter a description.
6. Click OK.

12. Click on Next or the Escalation tab. The Escalation dialog will open.
13. If you want to escalate the alarm if it is not acknowledged within a specified period of time, click on the Escalate after check box.
14. Select the number of hours and/or minutes after which the alarm should be escalated if it isn't acknowledged.
15. In the Escalated assignee field, select the person or group who should receive notification.
16. Select the severity that this alarm should have when it has been escalated. Default is 50.
17. Select the action that should be taken when the alarm has been escalated. Refer to Step 11 for details regarding these options. Keep in mind that you can't use the Update Watchlist, Send to Remedy, or Create a Case actions in the Escalation tab.
18. Click on Finish. The name, condition, and status of the alarm will be added to the table of alarms on the Alarms dialog.

Once an alarm has been added, it will begin to trigger when the conditions are met. For example, if the Maximum Condition Trigger Frequency is set to 15 minutes, the alarm will trigger for the first time when the number of events specified in the Event Count field occur within a 15-minute period. Events that come in during the first 15 minutes will not trigger the alarm.

For more information regarding managing alarms, refer to the Alarms Management section.

Alarm UCF Filters

One of the challenges for regulation compliance support is the ever-changing nature of regulations. Unified Compliance Framework (UCF) is an organization that maps the specifics of each regulation to harmonized control IDs. As regulations change, these IDs are updated and pushed to the McAfee ESM. The Compliance ID filter option allows you to select the required compliance or specific subcomponents and apply the filter so that only the appropriate events are displayed.

If you select the Deviation from Baseline or Specified Event Rate condition type, you will need to set values by which to filter by clicking on the filter icon ( darken). When you do so, the Filter Values dialog will open. If you need to set up compliance filters:

1. Click on the filter icon ( darken) to the right of the Compliance ID field. The Filter Variables dialog opens.
2. Select the compliance value(s) by which you want to filter.

3. Click OK. The *Filter Variables* dialog will close and the UCF IDs will be added to the *Compliance ID* field.

4. Click OK to save the settings.

**Health Monitor Alarms**

Health monitor rules generate events that appear under a base device in the System Navigation Tree. The Signature IDs of the health monitor events can be used in the *Values* field of a *Field Match* alarm to generate an alarm based off health monitor events. The *Health Monitor Event Summary* report can be generated as an alarm action in order to receive more details concerning health monitor events on the system (see *Generate reports, views and queries* above).

To set up an alarm before any health monitor events have been generated, do the following:

1. Follow the process to create an alarm (see *Create an Alarm* above).
2. On the *Condition* tab, select the *Field Match* type.
3. On the *Field* line, select *Signature ID*.
4. In the *Value(s)* field, enter the signature ID(s) for the health monitor rule(s) (see *Health Monitor SigIDs*).
5. Complete the remaining information as described in *Create an Alarm*.

If a health monitor event already exists, do the following to create an alarm:

1. Click on the event.
   a. Click the node for the base device (e.g., ![Node Icon](NRC-1100)).
   b. Select a view that displays the health monitor event (e.g., *Event Analysis, Default Summary*).
2. Click on the *Menu* icon (⃗).
3. Highlight *Create new alarm from*, then select *Signature ID*. The Alarm Settings dialog opens and the Field Match section on the Condition tab will contain the signature ID for the event.
4. Fill out the remaining settings for the alarm (see *Create an Alarm*).